# Decluttering the Toolset – Labs and Exercises

In this document, we will delve into a range of open-source and cost-effective technologies and resources to help you curate your cybersecurity architecture toolkit. By carefully evaluating and filtering through available solutions, you can identify the most suitable tools for your specific needs. To enhance your understanding of these tools and their applications, we will provide step-by-step labs and recommended exercises that focus on assessing vulnerabilities and risk profiles. By gaining a deep understanding of potential threats, you can then select and implement appropriate defenses accordingly.

With a well-equipped toolkit at your disposal, you will be able to swiftly and effectively respond to any adversary that emerges, proactively seizing opportunities to fortify your defenses before problems arise. By meticulously preparing the ideal set of tools in advance, you can ensure a strong, resilient cybersecurity posture and confidently tackle any challenges that come your way. This document aims to guide you through the process of assembling a comprehensive and adaptable cybersecurity toolkit, empowering you to safeguard your systems and data with unwavering vigilance.

The document covers the following topics:

- Lab 1: Microsoft Threat Modeling Tool
- Lab 2: OWASP Threat Dragon
- Lab 3: Intrusion detection/prevention systems using Snort
- Lab 4: Firewall configuration using OPNsense
- Lab 5: SIEM solution using Graylog
- Lab 6: Antivirus software implementation using ClamAV
- Lab 7: Endpoint detection and response using Wazuh
- Exercise 1: Setting up and configuring Keycloak for IAM
- Lab 8: Data encryption with VeraCrypt

- Lab 9: Vulnerability scanning with OpenVAS
- Lab 10: Security configuration management using Ansible
- Lab 11: Patch management with WSUS
- Lab 12: Digital forensics with The Sleuth Kit and Autopsy
- Lab 13: Incident response with Security Onion
- Exercise 2: Static application security testing with SonarQube
- Lab 14: Dynamic application security testing with OWASP ZAP
- Lab 15: Setting up and securing an AWS environment
- Lab 16: Implementing and configuring a GRC tool
- Lab 17: Penetration testing with Kali Linux and Metasploit
- Lab 18: Security automation with StackStorm

## What is in the toolbox?

Selecting the right tools is fundamental to building an effective cybersecurity architecture. With the overwhelming array of solutions on the market, architects must thoughtfully curate a toolkit tailored to their organization's specific risks, constraints, and use cases.

As noted in the book, this document is to provide insight to the various types of technology you may need to utilize or experience within an enterprise environment. With this in mind, the technologies discussed within this document are open source or free tools that will help you learn the concepts that can be applied to technologies that you may find within the enterprise. As discussed within the book, understanding the concepts allows you to be a cybersecurity architect that is able to pivot quickly and hit the ground running in any situation.

In addition, even though the book and these labs are meant to provide access to those new to cybersecurity and technology, it does make assumptions that you know how to install Linux and Windows operating systems. It is for this reason that these basic concepts are not covered within the labs, because that would make these labs even longer. With that in mind, I will be placing basic installation guides on my website, www.secdoc.tech, so that if you do not know how to install an operating system, you will not be excluded from continuing on with these labs.

## Threat modeling and risk assessment tools

Let us look at the labs.

## Lab 1: Microsoft Threat Modeling Tool (TMT)

Before diving into the hands-on lab exercise, it is important to understand the value of threat modeling and tools like Microsoft TMT that support the process. As discussed, threat modeling provides a structured system for architects to methodically assess risks and weaknesses. Hands-on practice is key to skill building for threat modeling and attack simulations. This lab will guide you through installing Microsoft TMT, creating a sample model of a 3-tier web application, executing automated threat analysis, assessing and planning mitigations for identified risks, generating documentation, and reviewing how to iterate the model as systems evolve. With firsthand experience of the threat modeling lifecycle, you will be equipped to apply these risk analysis techniques to real-world environments. Now, let's launch into the lab!

The subsequent sections will walk through the step-by-step lab, from downloading and configuring Microsoft TMT to constructing data flow diagrams, analyzing output, documenting findings, and understanding how to continuously update models to meet the dynamic threats and adapting architectures that cybersecurity architects face in their roles.



Figure 1 – Microsoft Ignite Threat Modeling Tool

These are the prerequisites:

- A Windows-based computer system
- Administrative privileges for software installation

With an understanding of the value of threat modeling, we now launch hands-on by installing Microsoft's Threat Modeling Tool. This section will guide you through visiting Microsoft's site to download the latest Threat Modeling Tool installer package, running the package with administrative privileges to install the software, completing the provided on-screen prompts, launching the tool from your start menu or desktop shortcut once setup finishes, and familiarizing yourself with the user interface.

With Microsoft TMT configured on your Windows machine, you have a powerful tool to construct robust threat models that serve as the scaffolding for risk identification and mitigation in your environments. The subsequent sections will build upon TMT's installation by utilizing its automated analysis and templated diagrams to methodically assess sample architecture, surface risks, define mitigating controls, and create shareable documentation - all critical aspects of the threat modeling lifecycle.

So let's get started by downloading the Microsoft Threat Modeling Tool and getting it running on our test system! The installation walkthrough is provided in detail next:

1. First let us look at the installation and initial configuration. Download Microsoft Threat Modeling Tool. Visit the official Microsoft website



Figure 2 – Microsoft Threat Modeling Tool

2. Download the latest version of the TMT installer package:



### Figure 3 – Download Threat Modeling Tool

- 3. To install the tool, run the installer package with administrative privileges.
- 4. Follow the on-screen instructions to complete the installation process:



Figure 4 – Installation of Threat Modeling Tool

- 5. Open TMT and configure the environment. Launch the TMT from the Start Menu or desktop shortcut. Familiarize yourself with the user interface upon opening.
- Now we move on to building the Threat Model. Create a new model. Click on create New Model from the dashboard menu:



Figure 5 – Microsoft Threat Modeling Tool Dashboard

7. The **Add Diagram** window will appear to create the base diagram:

Wew Threat Model - Microsoft Threat Modeling Tool			-		×
File Edit View Settings Diagram Reports Help DiagramReader					
Diagram 1 X	-	Stencils			Ψ×
	^	Search Stenc	ils	u	
		4 🚠 G	eneric Data Flow		<u>^</u>
		· · · ·			- 11
			Request		
			Response		
		4 📃 G	eneric Data Store		
			-		
		1	Azure Cosmos	s DB	
		6	Azure Key Vau	ılt	
			2 .		
			Azure Redis C	ache	
			Azure Storage		
		<			>
		Element Pron	ortios		аx
		content top	cro-ca		
		Diagram			
		Name	Dia	igram 1	
		Add New Cu	stom Attribute		
	>				
Messages - Disabled	ų x				
Description Severity Diagram	Ignore				
Messages - Disabled Notes - no entries					

Figure 6 – Adding a Diagram

 Edit the diagram. Drag and drop elements such as external entities (User Accounts), processes (Web Server, Application Server, Database Server), data stores, and data flows between them:



Figure 7 – Adding Elements to Diagram for Data Flows

9. Define trust boundaries by identifying and outlining the perimeter where trust levels change, e.g., the internet boundary, internal network, etc.:



Figure 8 – Trust Boundary Definition

10. Click **View** and select **Analysis**. Select the ID within the **Threat** list to identify details about the threat properties:



Figure 9 – Threat Analysis

 Review the threats identified by the tool, such as SQL injection, Cross-Site Scripting (XSS), or account hijacking:



Figure 10 – Threat Details

- 12. Now to assess and plan mitigation, for each identified threat, use the tool to assess the potential impact.
- 13. Document remediation options such as input validation, employing parameterized queries, and implementing robust access controls:



Figure 11 – Possible Mitigation Documentation

14. Now, we generate documentation. Create threat modeling reports via the **Report** feature:



Figure 12 – Report Creation

15. Capture the identified risks, their priority, and the status of the mitigations:



**Figure 13 – Report Export** 

16. Save and distribute the threat model documentation among the development and security teams:

Microsoft	🗑 New Threat Model* - Microsoft Threat M	odeling Tool		
Network	Ø Select a file name to save the current th	reat model full report	2	×
	← → × ↑ 🗄 → This PC → Docu	ments→ v õ		]
ampp-wi_	Organize 👻 New folder		lii 👻 💡	
PuTTY (64-bit) Oracle VM VirtualBox PyCharm communi_	Cop Pare 2.2     A     None     Social     Social	Oute modified           V0000000           V000000000000000000000000000000000000	Type         Size           Pila         File folder           AM         File folder           Pila         File folder           Pila         File folder           Pila         File folder           M         File folder           MA         File folder	
	File name:    Save as type: HTML files (*.htm)		Save Cancel	
	STRIDE Category	Short Description	Description V	ustification V Interaction V Possible M
3	adversary car Information Disclosure adversary mi Information Disclosure adversary ca Information Disclosure acker can de Repudiation	Information disclosure happens when the inform Information disclosure happens when the infor Information disclosure happens when the infor Repudiation threats involve an adversary denyi	An adversary can reverse weakly en An adversary may gain access to si An adversary can gain access to se Proper logging of all security even	Request Do not ex Request Ensure th Request Do not ex Request Ensure th
	adversary ca Spoofing adversary ca Spoofing	Spoofing is when a process or entity is somethi Spoofing is when a process or entity is somethi	Ensure that TLS certificate parame Attackers can exploit weaknesses	Request Verify X. Request Explicitly

Figure 14 – Saving Report

17. Iterate as design evolves. Regularly revisit the threat model as system design changes or as new threats emerge:

🖻 🚦 Getting	3 Started - Microsoft The × Threat Modeling Report. × +
← → C	flie:///C:/Users/secdoc/Documents/sample.htm
Threat Mo	deling Report
Created on 1/25/2024 Threat Model Name: Owner: Reviewer: Contributors: Description: Assumptions: External Dependenci	12:13:52 PM
Threat Model Sun	imary:
Not Started	33
Not Applicable	0
Needs Investigation	0
Mitigation Implement	ted 0
Total	33
Total Migrated	0
Diagram: Diag	gram 1
Diagram 1 Diagrar	n Summary:

## Figure 15 – Threat Model Report

18. Update the model and re-run the threat analysis as needed.

## Lab 2: OWASP Threat Dragon

OWASP Threat Dragon is an open-source threat modeling tool that helps cybersecurity professionals and software developers identify, understand, and mitigate potential security threats in their applications and systems. Developed by the **Open Web Application Security Project** (**OWASP**), Threat Dragon provides a user-friendly interface for creating and sharing threat models, promoting collaboration among team members. By visually representing the architecture of a system and its associated threats, Threat Dragon enables users to proactively address security concerns early in the development process. This tool supports various threat modeling methodologies, such as STRIDE and LINDDUN, and allows users to customize threat libraries to suit their specific needs. With its intuitive design and extensive documentation, OWASP Threat Dragon is an essential tool for organizations looking to enhance their application security and build more resilient systems.



Figure 16 – OWASP Threat Dragon

The prerequisites are:

- A computer system with a modern web browser or desktop application support
- Network access for downloading software

Let us look at the lab:

- Download and install OWASP Threat Dragon. Navigate to the OWASP Threat Dragon GitHub page or official website (<u>https://owasp.org/www-project-</u> <u>hreat-dragon/</u>).
- 2. Download the desktop version appropriate for your operating system or access the web application:



Figure 17 – Thread Dragon Download

3. Install the desktop application if applicable, following the instructions provided.

## Note

Version 2 threat models are not backward compatible with Version 1 models, so if you plan to start with version 1 and then move to version 2, realize you will be required to recreate the models.

4. Open Threat Dragon and familiarize yourself with its interface:



Figure 18 – Threat Dragon Dashboard

5. Now let's look at modeling and analysis. First, we look at creating a new project. Start a new project by specifying a name and description for your system under analysis:

	OWASP Threat Diagon Vile Edit View Window Help					-	٥	
Editing: New Threat Model Tite New Threat Model Over Perform P	hreat Dragon v2.1.3 en	ng *		Logged in as local-user	ۥ	?	÷	6
Tor New Threat Model  Preve Research  Preve Research  Preve Research  Preve Research  Preve Research  Start typing to add a contributor  Diagrams  + Add a new dagsm-	Editing: New Threat Model							
New Threat Model  Per  Per  Per  Per  Per  Per  Per  P	Title							
Corer Roleer  ight tool system deorytein  ight tool system deorytein  Contributes  Start typing to add a contributor  Diagrams +Add a new diagram.	New Threat Model							
High level system description         Controlutes         Start typing to add a contributor         Diagrams         + Add a new disgram.	Owner		 Reviewer					
High lovel system decryption Contributors Start typing to add a contributor Diagrams +Add a new diagram.								
Constitutes Scart typing to add a contributor Diagrams + Add a new diagram	High level system description							
Start typing to add a contributor Diagrams + Add a new diagram								
Start typing to add a contributor Diagrams + Add a new diagram. Diagram	Contributors							
Diagrams + Add a new diagram	Start typing to add a contributor							
+ Add a new dagram	Diagrams							
Dispute Py Delaad	+ Add a new diagram							
B Save D Reload								
				B Save				



 Develop a Data Flow Diagram (DFD). Utilize the diagramming features to create a DFD, placing processes, data stores, data flows, actors, and trust boundaries:



Figure 20 – Data Flow Diagram

- 7. Apply threat analysis. Engage threat libraries such as STRIDE or choose from preconfigured Attack Libraries to apply threat rules to your model.
- 8. Execute the threat analysis to identify potential security issues.
- 9. Review and detail threats. Examine each identified threat and assign a risk rating and priority level:

Threat Dragon v2.1.5	Edit Three Hundefined		ar-user				3
	Edit Mileat #underlined						
	Title						
Store	Fake messages could be placed on the queue	1					
	Type						
Actor	•						
		1					
Data Flow	NO Dear Millionard	. 8					
		' 🛛					
undaries	Description						
Trust Boundary	An attacker could put a fake message on queue, causing the Background Worker to do incorrect						
	processing.						
BB-							
Trust Boundary	· · · · · · · · · · · · · · · · · · ·	4					
ender.	Mblgations						
	Restrict access to the queue to the IP addresses of the Web Server and Background Worker.						1
Properties	Implement authentication on the queue endpoint.				+ N	ew Thro	at
						-	
		1					
Results	_			# Fake r	nessage	s	
C challens	Delete Cancel Apply			touid be the que	i piaced	ion	
Bidirectional	✓● STRDE			Spoofin	9	RDE	
Protocol	Encrypted Public Network						

Figure 21 – Editing Threat Information

- 10. Document the mitigation strategies and countermeasures for each threat.
- 11. Generate reports that summarize the threat analysis findings:



Figure 22 – Report Generation

12. Use these reports to communicate with stakeholders, guiding subsequent security hardening efforts:

Threat Dragon v2	:1.5 eng*		cogged in as totar oser 🕞 😈 🏭
Show model Show diagrams threat	mitigated Show out of scope elements	Show empty Threat Dragon elements logo	PDF Report
Jan 25 2024	Denne Theoretical dat		
Inteachiodetreporcion	Demo Infeatimodet		
Owner: Mike Goodwin	Reviewer: Jane Smith	<b>Contributors:</b> Tom Brown, Albert Moneypenny	
Executive Summary			
Executive Summary High level sysl Asample model of a web applice Summary	tem description	) gewend process	Vales
Executive Summary High level syst A sample model of a web applica Summary Name Total Threats	tem description	n grand protein	Wese 14
Executive Summary High level syst Asample model of a web applies Summary Name Total Threats Total MRigated	tem description	n grand protein	Wite 14 4
Executive Summary High level system Asangle model of a web applies Summary Total Threads Total Mitigated Not >Hilligated	tem description	n gewend procesa	Velee 14 4 19
Executive Summary High level syste Summary Name Total Threas Total Mitpaire Open /High Priority	tem description titer, with a queue-drcaupted bed	n gewent process	Votes 14 14 19 4
Executive Summary     High level system     Asampte matchel of a web applica     Summary     Total Margae     Total Margae     Total Margae     Gen / High Philody     Gen / High Philody	tem description	n grund proces.	Votes 14 4 10 4 4
	tem description	) graved process.	Value 14 4 10 4 4 4 4 4 4 2

Figure 23 – Threat Model Report

- 13. Next, for continuous updating—update the threat model regularly, particularly with changes in the system architecture or after the discovery of new vulnerabilities.
- 14. Rerun the analysis and revise the mitigation strategies as required.

In both labs, it is essential to document the learning outcomes and ensure that the threat model remains a living document, iteratively improved upon as the system it represents evolves. Additionally, these tools should be integrated within the SDLC to enhance the security posture from the earliest stages of development.

## Network defense and monitoring tools

Let us look at the labs.

## Lab 1: Intrusion Detection/Prevention System (IDS/IPS) Using Snort in a Virtual Environment

Snort is a widely-used, open-source **intrusion detection system** (**IDS**) that helps network administrators and security professionals monitor and protect their networks from various security threats. Developed by Martin Roesch in 1998 and now maintained by Cisco Systems, Snort is a powerful tool that performs real-time traffic analysis and packet logging on IP networks. It uses a rule-based language to detect and alert users about potential security breaches, such as malware infections, port scans, and attempts to exploit known vulnerabilities. Snort can be configured to work as a passive IDS, simply monitoring network traffic and raising alerts, or as an **intrusion prevention system** (**IPS**), actively blocking suspicious traffic. With its extensive community support, regular rule updates, and compatibility with various platforms, Snort has become an essential component of many organizations' cybersecurity strategies, helping them detect and respond to threats more effectively.



**Figure 24 – Snort Website** 

The link to access it is at https://www.snort.org/.

The prerequisites are:

- Virtualization software (e.g., VirtualBox, VMware)
- A virtual machine (VM) with a Linux-based system installed
- Network access within the virtual environment
- Administrative privileges for software installation within the VM

Let us look at the steps:

- 1. Create a new VM within your virtualization software. Allocate sufficient resources (CPU, Memory, and Network Adapters).
- 2. Install a Linux distribution (such as Ubuntu) on the VM.
- 3. Configure one network adapter in bridged mode and another in host-only or internal network mode for testing.
- 4. Update your system's package database with (for Debian-based systems):

## sudo apt-get update

5. Install Snort using the package manager with sudo apt-get install
snort:

□ secdoc@ubuntu2004.kvm: - Q
Package configuration
This value is usually "etb0", but this may be inappropriate in some network environments; for a dialup connection "popo" might be more appropriate (see the output of "/sbin/ifconfig").
Typically, this is the same interface as the "default route" is on. You can determine which interface is used for this by running "/sbin/route -n" (look for "0.0.0.0").
It is also not uncommon to use an interface with no IP address configured in promiscous mode. For such cases, select the interface in this system that is physically connected to the network that should be inspected, enable provideous mode later on and neke sure that the network rater is sent to this interface (either connected to a "prort structing)spanning" part in a sakton, to a hud, or to a tap).
You can configure multiple interfaces, just by adding more than one interface name separated by spaces. Each interface can have its own specific configuration.
Interface(s) which Snort should listen on:
atha
<0k>

**Figure 25 – Assigning Listening Interface for Snort** 

- 6. During installation, configure the network interface you want Snort to monitor.
- 7. Set up the internal network variable in the Snort configuration file:

## /etc/snort/snort.conf

8. Now, let's look at rule management. Navigate to /etc/snort/rules.

- 9. Create or update Snort rules to define what traffic should be inspected.
- 10. With the configuration and rule files in place, edit the snort.conf to modify a few parameters. Open the configuration file in your favorite text editor, for example using nano with the following command:

#### sudo nano /etc/snort/snort.conf

Find these following sections in the configuration file and change the parameters to reflect the examples here:

# Setup the network addresses you are protecting ipvar HOME\_NET server\_public\_ip/32

# Set up the external network addresses. Leave as "any" in most situations ipvar EXTERNAL NET !\$HOME NET

# Path to your rules files (this can be a relative path) var RULE\_PATH /etc/snort/rules var SO\_RULE\_PATH /etc/snort/so\_rules var PREPROC RULE PATH /etc/snort/preproc rules

```
# Set the absolute path appropriately
var WHITE_LIST_PATH /etc/snort/rules
var BLACK LIST PATH /etc/snort/rules
```

In the same snort.conf file, scroll down to the section 6 and set the output for unified2 to log under filename of snort.log, as follows:

```
# unified2
# Recommended for most installs
output unified2: filename snort.log, limit 128
```

Lastly, scroll down towards the bottom of the file to find the list of included rule sets. You will need to uncomment the local.rules to allow Snort to load any custom rules:

include \$RULE PATH/local.rules

- 11. Once you are done with the configuration file, save the changes and exit the editor.
- 12. Now, next to validating settings. Your Snort should now be ready to run. Test the configuration using the parameter -T to enable test mode:

```
sudo snort -T -c /etc/snort/snort.conf
```

After running the Snort configuration test, you should get a message like the following example:

```
--== Initialization Complete ==--
          -*> Snort! <*-
  11_
  o" )~ Version 2.9.16 GRE (Build 118)
   ....
          By Martin Roesch & The Snort Team:
http://www.snort.org/contact#team
          Copyright (C) 2014-2020 Cisco and/or its
affiliates. All rights reserved.
          Copyright (C) 1998-2013 Sourcefire, Inc.,
et al.
          Using libpcap version 1.8.1
           Using PCRE version: 8.39 2016-06-14
           Using ZLIB version: 1.2.11
          Rules Engine: SF SNORT DETECTION ENGINE
Version 3.1
           Preprocessor Object: SF DCERPC2 Version
1.0
           Preprocessor Object: SF SSH Version 1.1
           Preprocessor Object: SF FTPTELNET
                                             Version
1.2
           Preprocessor Object: SF SDF Version 1.1
           Preprocessor Object: SF DNP3 Version 1.1
           Preprocessor Object: SF REPUTATION Version
1.1
           Preprocessor Object: SF IMAP Version 1.0
           Preprocessor Object: SF SMTP Version 1.1
           Preprocessor Object: SF GTP Version 1.1
           Preprocessor Object: appid Version 1.1
```

```
Preprocessor Object: SF_MODBUS Version 1.1

Preprocessor Object: SF_POP Version 1.0

Preprocessor Object: SF_DNS Version 1.1

Preprocessor Object: SF_SSLPP Version 1.1

Preprocessor Object: SF_SIP Version 1.1

Snort successfully validated the configuration!

Snort exiting
```

This is how it'll look:



#### Figure 26 – Snort Initialization

In case you get an error, the response in the terminal should tell you what the problem was and where to fix it. Most likely problems are missing files or folders, which you can usually resolve by either adding any you might have missed in the setup above, or by commenting out unnecessary inclusion lines in the snort.conf file. Check the configuration part and try again.

- 13. To test if Snort is logging alerts as intended, add a custom detection rule alert on incoming ICMP connections to the local.rules file. Open your local rules in a text editor. Then add the following example line to the file: alert tcp any any -> 192.168.1.0/24 80 (msg:"Possible Web Traffic"; sid:1000001;)
- 14. Run Snort in IDS mode. Execute Snort in console mode with the following:

```
sudo snort -q -A console -i [interface] -c
/etc/snort/snort.conf -l /var/log/snort
```

- 15. Run Snort in IPS mode. Implement inline mode by adding the −Q switch and using appropriate inline-specific rules.
- 16. For testing and validation, use another VM or the host machine to generate network traffic that Snort should detect. Ensure this testing machine is connected to the same virtual network.
- 17. Review the alerts in <a href="https://www.variable.com"/war/log/snort">/war/log/snort</a>.

## Lab 2: Firewall Configuration Using OPNsense in a Virtual Environment

OPNsense is a powerful, open-source firewall and routing platform based on FreeBSD. It provides a feature-rich, user-friendly web interface for managing and securing networks of all sizes. As a fork of pfSense, OPNsense has quickly gained popularity among network administrators and cybersecurity professionals for its stability, performance, and extensive set of built-in security features. These features include a stateful firewall, IDS/IPS, **virtual private network** (**VPN**) support, traffic shaping, and more. OPNsense also offers a plugin system that allows users to extend its functionality with additional security tools and services, such as Suricata, Snort, and OpenVPN. With its active community, regular updates, and commitment to open-source principles, OPNsense has established itself as a reliable and flexible solution for organizations looking to protect their networks from various security threats while maintaining a high level of control and customization.



Figure 27 – OPNsense Website

The prerequisites are a VM to install OPNsense with at least two network interfaces configured. Let us look at the steps:

- 1. Prepare a new VM with at least two network adapters.
- 2. One network adapter should be configured in bridged mode (to simulate the WAN), and the other in internal network mode (to simulate the LAN).
- 3. Download the OPNsense ISO from the official website, https://opnsense.org/
- 4. Burn the ISO to a USB drive or attach it to a VM.
- 5. Boot from the drive or ISO and follow the installation prompts:

>>> Invoking start script 'sysctl'
Service sysctl has been restarted.
>>> Invoking start script 'beep'
Root file system: /dev/iso9660/OPNSENSE_INSTALL
Fri Jan 26 16:02:17 UTC 2024
*** OPNsense.localdomain: OPNsense 23.7 ***
LAN (vtnet0) -> v4: 192.168.1.1/24
°WAN (vtnet1) → v4/DHCP4: 10.13.37.103/24
HTTPS: SHA256 63 BC 53 2E D2 13 12 B9 23 3C A8 11 CB 7C 93 49
8D 75 6B 43 76 DD 3F 50 F7 62 F8 37 0E ED 59 62
/ SSH: SHA256 EzVrSu51spdKDoX4YZsH2QTAB/gB9vBRAs6BJFJb14H (ECDSA)
, SSH: SHA256 GwczxYH1GbcAgqCwGZL8XZ/6QyuiDsU3n2T4nnFbmBE (ED25519)
SSH: SHA256 R7H6+hcjeeDwwH013F7y3tNsQtb2xu7GJmv96QbJhuQ (RSA)
Helcome! UPNsense is running in live mode from install media. Please
login as root to continue in live mode, or as installer to start the
installation. Use the default or previously-imported root password for
both accounts. Remote login via SSH is also enabled.
Treebs0/amu64 (OPAsense.localuomain) ((tyv0)

Figure 28 – Installation of OPNsense

The default password for OPNsense is opnsense and is the password to use for the default root and installer accounts.

Configure a keyboard:

OPNsense Installer 	
Keynap Selection The system console driver for OPNsense defaults to standard "US" keyboard map. Other keymaps can be chosen below.	
<pre>&gt;&gt; Continue with default keynap -&gt;- Test default keynap () Armenian phonetic layout () Belarusian () Belgian () Belgian (accent keys) () Brazilian (accent keys) () Brazilian (uithout accent keys) () Bulgarian (BDS) () Bulgarian (Phonetic) () Canadian Bilingual ())</pre>	
<pre></pre>	

Figure 29 – Keyboard Mapping Configuration

The default is Unix File System (UFS), but I prefer the Zettabyte File System (ZFS), but either are acceptable selections:

Select Vir	ZFS Configuration tual Device type:	
stripe mirror raid10 raidz1 raidz2 raidz3	Stripe - No Redundancy Mirror - n-Way Mirroring RAID 1+0 - n x 2-Way Mirrors RAID-Z1 - Single Redundant RAID RAID-Z2 - Double Redundant RAID RAID-Z3 - Triple Redundant RAID	
[Pr	<pre>Cancel&gt; ess arrows, TAB or ENTER]</pre>	

Figure 30 – ZFS Configuration

If this is a VM using a single disk, the **Stripe – No Redundancy** should the left as the default selection.

6. Press the spacebar to select the drive.

Once you have selected the ZFS configuration, the next screen will allow you select the hard drive that OPNsense will be installed upon. Select the drive and click **OK**:



Figure 31 – Harddrive Selection

At this point, the screen now provides warning that you are about to destroy any data that exists on the disk selected:





7. Click the **TAB** key on the keyboard to select **YES** to continue:



Figure 33 – Select YES to Install

8. At this point you can change the default root account password:

PNsense Installer	
	Please select a password for the system management account (root):
	······
	Cancel>

Figure 34 – Define Root Password

9. Upon changing the password, the following prompt will show up:



Figure 35 – Complete Installation

10. At this point you can change the LAN IP Addressing scheme and recommend that you do in the event there is a conflict with an existing LAN/Network IP range:



Figure 36 – Terminal Login for Initial Configuration

11. Select option 2 to assign LAN Interface IP Address:

   Website:   Handbook:   Forums:   Code:   T⊎itter:	https://opnsense https://docs.opr https://forum.op https://github.c https://twitter	e.org/ nsense.org/ onsense.org/ com/opnsense .com/opnsens	       		0000 000\\ ))))))))) 000// 0000 00000		0000 //000 ((((((() \\000 00000	
*** OPNsense.lo LAN (vtnet0) WAN (vtnet1)	caldomain: OPNser -> v4: 192.168 -> v4/DHCP4: 19	nse 23.7 *** 1.1/24 02.168.2.170	/24					
HTTPS: SHA256	63 BC 53 2E D2 13 8D 75 6B 43 76 DC	3 12 B9 23 3 ) 3F 50 F7 6	C A8 2 F8	11 C 37 Ø	B 7C 93 E ED 59	49 62		
0) Logout		7)	Ping	j hos	t			
1) Assign int	erfaces	8)	Shel	11				
<ol><li>Set interf</li></ol>	ace IP address	9)	pfTo	р				
3) Reset the	root password	10)	Fire	ewall	log			
4) Reset to f	actory defaults	11)	Relo	bad a	ll servi	ces		
5) Power off	system	12)	Upda	ate fi	rom cons	ole		
6) Reboot sys	tem	13)	Rest	tore	a backup			
Enter an option	: 2							

Figure 37 – Interface Configuration

12. Select option 1 to configure LAN Interface and choose N to not assign IP address via DHCP:

LAN (vtnet0) WAN (vtnet1)	-> v4: 192.168 -> v4/DHCP4: 1	8.1.1/24 192.168.2.170/24	
HTTPS: SHA256	63 BC 53 2E D2 1 8D 75 6B 43 76 D	13 12 B9 23 3C A8 11 CB 7C 93 49 DD 3F 50 F7 62 F8 37 0E ED 59 62	
0) Logout 1) Assign int 2) Set interf 3) Reset the 4) Reset to f 5) Power off 6) Reboot sys	erfaces ace IP address root password actory defaults system tem	7) Ping host 8) Shell 9) pfTop 10) Firewall log 11) Reload all services 12) Update from console 13) Restore a backup	
Enter an option: 2			
Available interfaces:			
1 – LAN (vtnet0 – static, track6) 2 – WAN (vtnet1 – dhcp, dhcp6)			
Enter the number of the interface to configure: 1			
Configure IPv4 address LAN interface via DHCP? [y/N] n			

Figure 38 – Define LAN/WAN Interfaces

13. Enter the desired IP Address, such as the example 10.13.37.1, and select the desired CIDR/subnet range such as the /24 or 255.255.255.0 example:

5) Power off system	12) Update from console		
6) Reboot system	13) Restore a backup		
Enter an option: 2			
Available interfaces:			
1 – LAN (vtnet0 – static, track6) 2 – WAN (vtnet1 – dhcp, dhcp6)			
Enter the number of the interface to configure: 1			
Configure IPv4 address LAN interface via DHCP? [y/N] n			
Enter the new LAN IPv4 address. Press <enter> for none: &gt; 10.13.37.1</enter>			
Subnet masks are entered as bit counts e.g. 255.255.255.0 = 24 255.255.0.0 = 16 255.0.0.0 = 8	(like CIDR notation).		
Enter the new LAN IPv4 subnet bit count > 24	(1 to 32):		

Figure 39 – Define LAN Subnet Scheme

14. Press enter since there is no upstream gateway for the LAN:

```
Available interfaces:

1 - LAN (vtnet0 - static, track6)

2 - WAN (vtnet1 - dhcp, dhcp6)

Enter the number of the interface to configure: 1

Configure IPv4 address LAN interface via DHCP? [y/N] n

Enter the new LAN IPv4 address. Press <ENTER> for none:

> 10.13.37.1

Subnet masks are entered as bit counts (like CIDR notation).

e.g. 255.255.0.0 = 24

255.255.0.0 = 16

255.0.0.0 = 8

Enter the new LAN IPv4 subnet bit count (1 to 32):

> 24

For a WAN, enter the new LAN IPv4 upstream gateway address.

For a LAN, press <ENTER> for none:

> 10.13.37.1
```

Figure 40 – LAN Interface Upstream Gateway Configuration

15. While you can configure IPv6 addressing to do further testing, this has been disabled by selecting **No** and pressing *Enter*.



Figure 41 – LAN Interface IPv6 Configuration

16. To enable DCHP server on the LAN for attached devices, select Yes:



Figure 42 – Enabling a DHCP Server on the LAN Interface

17. Enter the starting and ending client IP address range as in the example

```
10.13.37.100-10.13.37.250:
```

```
> 10.13.37.1
Subnet masks are entered as bit counts (like CIDR notation).
e.g. 255.255.255.0 = 24
    255.255.0.0 = 16
    255.0.0.0 = 8
Enter the new LAN IPv4 subnet bit count (1 to 32):
    > 24
For a WAN, enter the new LAN IPv4 upstream gateway address.
For a LAN, press <ENTER> for none:
    >
Configure IPv6 address LAN interface via WAN tracking? [Y/n] n
Configure IPv6 address LAN interface via DHCP6? [y/N]
Enter the new LAN IPv6 address. Press <ENTER> for none:
    >
Do you want to enable the DHCP server on LAN? [y/N] y
Enter the start address of the IPv4 client address range: 10.13.37.100
Enter the end address of the IPv4 client address range: 10.13.37.250
```

Figure 43 – Defining DHCP Scope

18. Select No, when prompted to change web GUI protocol:

```
Subnet masks are entered as bit counts (like CIDR notation).

e.g. 255.255.255.0 = 24

255.255.0.0 = 16

255.0.0.0 = 8

Enter the new LAN IPv4 subnet bit count (1 to 32):

> 24

For a WAN, enter the new LAN IPv4 upstream gateway address.

For a LAN, press (ENTER) for none:

>

Configure IPv6 address LAN interface via WAN tracking? [Y/n] n

Configure IPv6 address LAN interface via DHCP6? [y/N]

Enter the new LAN IPv6 address. Press (ENTER) for none:

>

Do you want to enable the DHCP server on LAN? [y/N] y

Enter the start address of the IPv4 client address range: 10.13.37.100

Enter the end address of the IPv4 client address range: 10.13.37.250

Do you want to change the web GUI protocol from HTTPS to HTTP? [y/N] n
```

#### Figure 44 – HTTP/HTTP Web GUI Protocol

19. Select Yes to generate self-signed certificate:

Subnet masks are entered as bit counts (like CIDR notation). e.g. 255.255.255.8 = 24 255.255.8.8 = 16 255.8.8.8 = 8 Enter the new LAN IPv4 subnet bit count (1 to 32): > 24 For a WAN, enter the new LAN IPv4 upstream gateway address. For a LAN, press <ENTER> for none: > Configure IPv6 address LAN interface via WAN tracking? [Y/n] n Configure IPv6 address LAN interface via DHCP6? [y/N] Enter the new LAN IPv6 address. Press <ENTER> for none: > Do you want to enable the DHCP server on LAN? [y/N] y Enter the start address of the IPv4 client address range: 10.13.37.100 Enter the end address of the IPv4 client address range: 10.13.37.250 Do you want to change the web GUI protocol from HTTPS to HTTP? [y/N] n Do you want to generate a new self-signed web GUI certificate? [y/N] y

Figure 45 – Allow Self-signed Certificate

20. Select No to restore web GUI defaults:
| e.g. 255.255.255.0 = 24<br>255.255.0.0 = 16<br>255.0.0.0 = 8   |
|--|
| Enter the new LAN IPv4 subnet bit count (1 to 32):<br>> 24   |
| For a WAN, enter the new LAN IPv4 upstream gateway address.<br>For a LAN, press <enter> for none:<br/>&gt;</enter>   |
| Configure IPv6 address LAN interface via WAN tracking? [Y/n] n<br>Configure IPv6 address LAN interface via DHCP6? [y/N]  |
| Enter the new LAN IPv6 address. Press <enter> for none:<br/>&gt;</enter>   |
| Do you ⊎ant to enable the DHCP server on LAN? [y/N] y  |
| Enter the start address of the IPv4 client address range: 10.13.37.100<br>Enter the end address of the IPv4 client address range: 10.13.37.250   |
| Do you want to change the web GUI protocol from HTTPS to HTTP? [y/N] n<br>Do you want to generate a new self-signed web GUI certificate? [y/N] y<br>Restore web GUI access defaults? [y/N] ■ |

Figure 46 – Web GUI Access Defaults

21. After installation, access the OPNsense web interface from another machine in the same network using the default IP provided at the end of the installation:

ō			🔶 New Jah				n x
$\leftarrow \rightarrow$	C	0 8⊾ ∾	https://10.13.37.1		ŵ	9 ®	ല്≡
				ZOPDsense			
				Username:			
				Pacounert			
				•••••••			
				Logn			
				OPvicence (c) 2014-2023 Deciso SV.			

Figure 47 – OPNsense Web Management Interface

22. Let us now look at the initial setup wizard:

E Lobby System Market System	· Wizard· General Setun	root@OPNsense.localdomain (	٩	
Lobby System	Wizard' General Setup			
Reporting System	Wizard' General Setun			
System	a manor deneral becup			
Access 🖀	This wizard will guide you through the initial system or	onfiguration. The wizard may be stopped at any time by clicking the logo im	age at the top of the screen.	
Configuration 🕲				
Firmware		Nest		
Сягеманук 🕈				
High/wallability 2				
Routes 🕈				
Sattinga 🛛 😋				
Trust 🔹				
Wizard 🎽				
Log Files 🔹 👁				
Disgnostics				
Interfaces				
Firewall				
E SEN				
Services				
Power				
B Help				

# Figure 48 – OPNsense Setup Wizard

23. Use the setup wizard to configure the basic settings such as **Hostname**, **Domain**, **DNS servers**, and **Time zone**:

🗈 😣 General informatio	an   Wiea	d   S X 🍓 Nov Tab X 🕂				~	_	u.	x
		A https://10.13.37.1/wizard.ohp?cml=system							
ZOPOsense' <				roots30PRsense.localdomain	Q				
🚊 Lobby		System: Wizard: General Info	mation						
System Access	÷	General Information							
Configuration	ວ ພ	Hostname:	DPNsense						
Gateways High Availability	1	Domainc	localdomain						
Routes	=	Language:	English •						
Trust		Primary DNS Server:							
Wizard Log Files	*	Secondary DNS Server:							
Diagnostics	۵	Override DNS:	Allow DNS servers to be overridden by DHCP/PPP on WAN						
A Interfaces		Unbound DNS							
Ø VPN		Enable Resolver:							
Ø Services		Enable DNSSEC Support:							
# Power		Harden DNSSEC data:	D						
D liep			Ked						
		OPhicense (c) 2014-2023 Deciso 5/5							

# Figure 49 – Wizard General Configuration

24. Assign and configure WAN and LAN interfaces, ensuring proper IP address configuration. This should have been configured earlier in the steps, but if you need to adjust you can do so through the initial wizard setup:

	🗇 🐮 Configu	ne LAN Interface   W	fan X 🍁 New Tab X 🕂				×
			A https://10.13.37.1/wizard.php1xml=system				
ş					rootgPOPNsense.localdomain	۹	
	Lobby						_
-	Reporting		System: Wizard: Configure LAN	Interface			
-	System						
	Access	쓭	LAN IP Address:	10.13.37.1			
	Configuration	ອ		(leave empty for none)			
	Firmware		Subset Mark:				
	Gataways	4		24 *			
	High Availability	2 +		Next			
	Routes	+					
	Trust						
	Wittand	×					
	Log Files	۲					
	Diagnostics	D					
dh.	interfaces						
49	Firewall						
9	VPN						
0	Services						
~	Power						
	нар						
			OPNos nos (c) 2014-2025 Deciso B.V.				
		_					

Figure 50 – Wizard LAN Configuration

25. The OPNsense dashboard is then presented:

↓ → C     ↓	A https://131337.1/4 Lobby: Dashbo System Information Name Versions Uptatas Cr Uppe Cr Uppe Load sverage	And An Antonio	root Service Service configi cron dhod login nipol	Description System Configurati Cron DHCPV4 Server Users and Groups Network Time Dae	ion Daemon	ي ا ا	got 2 colu	C C	- ×
Lubby Datiboard 40 Lichos Passend 40 Ligout 40 Lig	Lobby: Dashbo system Information Name Versions Updatas CV 1558 CV 1558 Load sverage	CPTGerms-Accolionam CPTGerms-Accolionam CPTGerms-Accolionam CPTGerms-Accolionam CPTGerms-Accolionam Context for applates. AND Synei SSSXI 15-Care Processor (f cross, 4 threads)	services Service configd cron dhopd login nipd	OFNeeded Jocaldomat Description System Configurati Cron DHCPV4 Server Users and Groups Network Time Dae	n • C	Add wid	get 2 colu	e C	- x
Li Lobby Darboard Ø Litania Pattmend 4, Lagot 10 Mentoria Mentoria File System file Sys	Lobby: Dashbo system Information Name Versions Updates CVU System Load average	Image: Control of the state of the	Services Service configd cron dhapd login nipd	Description System Configuration Cron DHCPv4 Server Users and Groups Network Time Date	lon Daomon	O Add wid	get 2 colu	e c	- x
banboard 40 Liano 40 Pataward 40 Laguat 10 Laguat 10 Laguat 10 Laguat 10 Final 10 0 brenzes ∮ Final 10 0 brenzes ∮ Power 10 0 brenzes	System Information Name Versions Updates C7U type C3U usage Load average	CPTearms.Acadiomam CPTearms.Acadiomam CPTearms.Acadiomam CPTearms.Pt2.1-am046 Prost8D 113.781L048 p1 Crick to relack for applates. AND Syncis SSSXI 15-Care Processor (4 cross, 4 liberath)	Service Service configd cron dhcpd login ntpd	Description System Configurati Cron DHCPv4 Server Users and Groups Network Time Dae	ion Daemon	<ul> <li>Add wid</li> </ul>	get 2 colu	c c	- ×
Litand D Pataward Q Litand Q Litanda Q File System A Interfaces A Firewall Q Firewall Q Firewa	System Information Name Versions Updates O'U type O'U usage Load average	V     ×       OPNerms-Accalionam     OPNerms233-amd04       Proteids 01.13.RBLANE p1     Opners31.11.10.100 kg/2013       Officience of the opdates.     AM0 0g/and 95/80(1)6-Opne Processor (4 cores, 4 lineads)       100	Services Service configd cron dhcpd login nipd	Description System Configurati Cron DHCPv4 Server Users and Groups Network Time Dae	lon Daemon		0	c	- *
Passeed 4 Passeed 4 Lagat 4 A Reputing 1 4 Reputing 4 4 Reputies 4 5 Convert 4 6 Convert	System Information Name Versions Updatus C/U system C/U usage Load average	CPHorms.Acadoman     CPHorms.Acadoman     CPHorms.22.7-am064     ProcedDo L33.RELEXE p.1     OpenedS.11.1.0.1.00 My 2020     Click to check for applaces.     AND 3grest SSR01.15-Care Processor (4 cores, 4 librash)     To	Services Service configd cron dhcpd login nipd	Description System Configurati Cron DHCPv4 Server Users and Groups Network Time Dae	ion Daamon		0	c	- *
Patendol 44 Laguet 14 El Separting 14 El System Storettoors Storettoors Storettoors Storettoors Storettoors Storettoors Storettoors Storettoors Storettoors Storettoors Storettoors Storettoors	Name Versions Updates CPU type CPU toope Load average	CPTNerms-Rockloman CPTNerms-ZX-rund64 ProteSD-L12-RRAUER at CpretSD-L12-RRAUER at CpretSD-L12-RRAUER at CpretSD-Complexe. AND System S-SNOX15-Come Processor (if come, 4 threads)	Service contigd cron dhcpd login nipel	Description System Configurati Cron DHCPv4 Server Users and Groups Network Time Dae	ion Daemon		0	c	
Lagoot () k Beparting T System L Interfaces B Freenell O myt O myt O myt O myt D mytem D myt	Versions Updates CPU type CPU usage Load average	C (1986) ILL RELATED AND A CONTRACT OF A CON	cron dhcpd ntpd	System Configuration Cron DHCPv4 Server Users and Groups Network Time Date	ion Daemon			c	
k Roparting E System 9 Freewall 9 Dervices 9 Dervices 9 Help	Versions Updates CPU type CPU usege Load average	CTYNeme 23.7-and04 prot05011.3.14.00.04 pi Cynet05011.3.14.00.04 pi Cynet05010.3.14.00.04 pi Citch Corden Arto Ingelacu. AND Synet S-NOX115-Case Processor (Ecose, 4 Uneach)	configd cron dhcpd login ntpd	System Configurati Cron DHCPV4 Server Users and Groups Network Time Dae	ion Daemon			c	
E Syaram A Interfaces 9 Facewall 9 Facewall 9 Facewall 9 Facewall 9 Help	Updates CPU type CPU usage Load average	preside La La Rectarde pro Ganetia La La Sol May 2003 Clark to check for updates. AND Rysen S 4550X 15-Case Processor (4 cores, 4 Dreads) 100 0	cron dhcpd login ntpd	Cron DHCPv4 Server Users and Groups Network Time Dae				C	
gunna 6 Frewall 9 Interfaces 9 Inter 9 Interfaces 6 Power 2 Help	Updates CPU type CPU usage Load average	Click to check for updates. AND Rysen 9 58503 (B-Case Processor (4 cones, 4 threads) 100 0	dhopd login ntpd	DHCPv4 Server Users and Groups Network Time Dae					
A Interfaces 9 YPN 9 YPN 9 Enroken 9 Proce 9 Help	CPU type CPU type Load average	AND Byten 9 5550X 15-Core Processor (4 cores, 4 threads)	login ntpd	Users and Groups Network Time Dae				0	
9 (Forwell 2 Univer 2 Dervices 6 Prover 2 Help	CPU type CPU usage Load average	AND Ryzer 9-58508 18-Care Processor (4 cares, 4 threads)	ntpd	Users and Groups Network Time Dae			_		-
9 vra 9 Services ∮ Ivaer 9 Help	CPU usage	0	ntpd	Network Time Dae			•	C	
9 Bervikes Prover ⊉ Helo	Load average	0			mon		•	C	
k Power B Help	Load average		01	Packet Filter				le'	
roner B Help		0.14, 0.14, 0.16	-						
₿ Helo	Uptime	04:01:43	routing	System routing				C	
	Comment data Mana	Print and the second seco	syscti	System tunables				C	
	current cate/unie	Ph 3ah 20 20 4731 010 2024	sustances	Susloning Daemon				0	
	Last config change	Fri Jan 26 20:47:45 UTC 2024							-
	CPU usage	0%	unbound	Unbound DNS			•	C	•
	State table size	0%(50/405000)	webgul	Web GUI				C	
	MBHEUKANA	0.567(1524/2509281)							
	weare mage	n in ( rond ronnin )	Gateways					1.	- ×
	Memory usage	11 % (450/4052 MB) (ARC size 159 MB)	Name	RTT	RTTd	Loss	Status		
	SWAP usage	0.95 (0/8192 MB)					-		
	Disk usage	5%/ (zfc) (1.2G/23G)	-	-	-	-	Ordere		
		1% /boot/efi [msdosfs] (1.8M/260M)	where party						
		0% /var/mail [zfs] (96K/22G)	192.168.2.1				<b>United</b>		
		0% /zroot [zfs] (96K/22G)							
		0% /use/home (zfs) (%K/22G)	Interfaces						
		0% /tmp [2%] (320K/22G)	International Action of the In						
		0% /usr/ports [zts] (06K/22G)	= LAN	↑ 106base-T <tul< p=""></tul<>	II-duplet>	10.13.37.1			
		0%6/var/log [zts] (1.1M/226)	= WAN	↑ 100base-T <ful< p=""></ful<>	II-duplex>	192.168.2.170			
	0% /var/audit [zfs] (96K/226)								
	0% /var/crash [zfs] (90K/22G)								
		0% /usr/arc [zfs] (96%/22G)							

Figure 51 – OPNsense Dashboard

Image: Control Contro Control Control Control Control Control Control Control Control C		Withold prop           board           n           OPPErsense.localdomain           OPERsense.localdomain           OPERsense.localdomain           OPERsense.localdomain           OPERsense	readiy	Service Service contigo cron dhcad legin ntpd pf routing systi	COPNeerce-localdomail Description System Configurat Crom DHCP-v4 Server Users and Groups Network Time Dae Packet Filter System routing System tunables	n a a	C Add and	iget Z colu		- *
Internet         Control         Contro         Control         Control <t< th=""><th></th><th>board         •           •         OPTisense Jacaidomain           •         OPTisense Jacaidom</th><th>raeg</th><th>Service Service contigd cron dhapd iogin ntpd pf routing systl</th><th>OPNsense-localdonnee Description System Configurat Cron DHCPv4 Server User and Groups Network Time Dae Network Time Dae System runables</th><th>n e Q</th><th>O Add wed</th><th>iget 2 colu</th><th></th><th>- ×</th></t<>		board         •           •         OPTisense Jacaidomain           •         OPTisense Jacaidom	raeg	Service Service contigd cron dhapd iogin ntpd pf routing systl	OPNsense-localdonnee Description System Configurat Cron DHCPv4 Server User and Groups Network Time Dae Network Time Dae System runables	n e Q	O Add wed	iget 2 colu		- ×
integer     Biology (2)     Biology	Li Linky  A Roardig  Spatem Spatem  Spatem  A trachos  Cotegories  Cotegories  Alores  Cotegories  Cot	board	P - x	Service Service configd cron dhapd login ntpd pf routing systl	Description System Configurat Cron DHCP-V4 Server Users and Groups Network: Time Das Packet: Filer System routing System tunables	ion Daemon mon	O Add wrd	iget Z colu		- *
Biguing System Instructions         Second System Instructions         Second System Instructions <t< td=""><td>Anoreman in the interface interface in the interface int</td><td>OPTiverse.lecaldomain     OPTiverse.lecaldomain     OPTiverse.lec</td><td>P - x</td><td>Services Service confligs cron dhcpd login ntpd pf routing systil</td><td>Description System Configurat Crun DHCP-v4 Server Users and Groups Network Time Dae Packet Filter System routing System tunables</td><td>Ion Daemon</td><td>C Add wid</td><td>E E E E E E E E E E E E E E E E E E E</td><td></td><td>- x</td></t<>	Anoreman in the interface interface in the interface int	OPTiverse.lecaldomain     OPTiverse.lec	P - x	Services Service confligs cron dhcpd login ntpd pf routing systil	Description System Configurat Crun DHCP-v4 Server Users and Groups Network Time Dae Packet Filter System routing System tunables	Ion Daemon	C Add wid	E E E E E E E E E E E E E E E E E E E		- x
System         System Information         Image: Control (Control (Contro) (Control (Contro) (Control (Control (Control (Co	<ul> <li>System indexeads</li> <li>Tetrafaces</li> <li>Aranes</li> <li>Critograd</li> <li>Aranes</li> <li>Critograd</li> <li>Mara</li> <li>Critograd</li> <li>Mara</li> <li>Critograd</li> <li>Mara</li> <li>Critograd</li> <l< td=""><td>n OPTecesso-localdomain OPTecesso-localdomain Control 21 / and04 Ferendo 23 / and04 Ferendo 23 / and04 Citek to check for update. Add byses 6 5500t In-Core Processor (4 cetes, 4 the 100 0.22, 0.23, 0.27 0.420,43 Fr. Junit 2004937 UTC2024 Fr. Junit 2004937 UTC2024 Fr. Junit 2004937 UTC2024</td><td>reads)</td><td>Services Service contigs dhupd login ntpd pf routing systi</td><td>Description System Configurat Cron DHCPv4 Server Uters and Groups Network Time Dae Packet Filter System routing System tunables</td><td>ion Daemon</td><td></td><td></td><td>, c c c c c c c c c c c c c c c c c c c</td><td>- ×</td></l<></ul>	n OPTecesso-localdomain OPTecesso-localdomain Control 21 / and04 Ferendo 23 / and04 Ferendo 23 / and04 Citek to check for update. Add byses 6 5500t In-Core Processor (4 cetes, 4 the 100 0.22, 0.23, 0.27 0.420,43 Fr. Junit 2004937 UTC2024 Fr. Junit 2004937 UTC2024 Fr. Junit 2004937 UTC2024	reads)	Services Service contigs dhupd login ntpd pf routing systi	Description System Configurat Cron DHCPv4 Server Uters and Groups Network Time Dae Packet Filter System routing System tunables	ion Daemon			, c c c c c c c c c c c c c c c c c c c	- ×
system kolonanie         system kolonanie         social	A Interfaces     Autors     Alaces     Autors     Contegrates     Autors     Contegrates     Autors     Contegrates     Autors     Contegrates     Autors     Contegrates     Autors     Contegrates     Contegrate	n OPFIscene.localdomain OPFIscene.localdomai	/ - x	Service Service confligd cron dhqud legin ntpd pf routing systet	Description System Configurat Cron DHCPv4 Server Uters and Groups Network Time Dae Packet Filter System routing System tunables	ion Daemon				- ×
Name         OP/Restrict/advance         Service         Berkrighter           Alores         Verson         Op/Restrict/advance	Hervall     Alase	07F0cores_localdomain 07F0cores_localdomain FreetidD 312.45(L456);01 07end63(L114);03 Mory 2020 Click to check for update. Add hysion 65502(L56.Cox Processor (4 cores, 4 the 100 0.22, 0.23, 0.27 0.420,43 Fr. Jan 29 20:4537 UTC 2024 Fr. Jan 29 20:4537 UTC 2024	read(5)	Service confligd uron dhupd login ntpd pf routing systi	Description System Configurat Cron DHCPV4 Server Users and Groups Network Time Dae Packet Filter System routing System tunables	ion Daemon mon				•
Alarss         Prisone 21 ArRUNA         Prisone 22 Aradid         Pris	Alacea Alacea Cregories Alacea Cregories MAT E Chi type Chi type C	079Nexms 22.1-3m084 Freed(50.32.84.154:0-0 Open551.1.1.3x-10 Mey 2023 Click to shock for cyclates. Add to pays to 5502 1.6-Care Processor (4 cares, 4 the 100 0.22, 0.23, 0.27 0.422, 0.23, 0.27 0.422,42 Fr. Jan 29 204957 UIC 2024 Fr. Jan 29 204957 UIC 2024	readis)	confligd cron dhupd login ntpd pf routing sysci	System Configurat Cron DHCPv4 Server Users and Groups Network Time Dae Packet Filter System routing System tunables	mon				•
Auder     0     Invest00 123 AULAKU-93       Colorgenie     0     0       Outgenie     Updata     Chi für der Kungdata.       Nation     0     0       Nation     0	Autors under an and an	Investigo 13.2.48.LL46/c-11 OpenSEI.1.1.1.100 May 2023 Click to share fir update. AMD hysin 0 55502 L6-Care Processor (4 cores, 4 the 100 0.12, 0.20, 0.17 0.402.94 In Jan 20 20-0857 UIC 2024 Fir Jan 20 20-0857 UIC 2024	readisj	cron dhupd login ntpd pf routing sysci	Cron DHCPv4 Server Users and Groups Network Time Dae Packet Filter System routing System tunables	mon			0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	•
Lingting       Updates       Updat	Linguisti     Linguistic       NAT     Chill Index       Rules     Chill Index       Rules     Chill Index       Loghuk     Chill Index       Shaper     Chill Index       Loginiki     Chill Index       Dugorotica     Batter State State State       Viril     Batter State       Services     State       Viril     State       Batter     State	Capitol, Licka and Strong and Strong Annual Click to device the regulation. Add Topson 0 5500X 156-Cane Processor (4 canes, 4 the 0 52, 0 20, 0 1, 127 0 452, 0 20, 0 10, 0 10, 0 10, 0 10, 0 10, 0 10, 0 10, 0 10, 0 10, 0 10, 0 10, 0 10, 0 10, 0 10, 0 10, 0 10, 0 10	readisj	dhepd login ntpd pf routing sysctl	DHCPv4 Server Users and Groups Network Time Dae Packet Filter System routing System tunables	mon			0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	•
Cooge         L         Updates         Cock to frace frace frace frace         Updates	Groups     L.     Updates       NAT     C/U Ippa       Rudat     C/U Ippa       Rudat     C/U Ippa       Longhouck     Concreage       Statings     QL       Log Strings     QL       Stations     Statistical solution       Nown     Statistical solution       Nonory usage     Statistical solution       Services     Statistical solution       Power     Disk install	Click to direct for updates. Aith Dyno II 55021 I-6-Care Processor (4 cases, 4 the 0 0.12, 0.23, 0.27 0450244 Fr. Jan 29 204957 UIC 2024 Tr. Jan 29 204759 UIC 2024	reads)	login ntpd pf routing sysctl	Users and Groups Network Time Dae Packet Filter System routing System tunables	mon			0 0 0 0	•
htt     Chi type     Abit hyper 558000 (L-Core Processor) (cross, 4 transar)     leigh     Materian Glocopia     C	MT     III     Chi ti pia       Russ     Chi ti pia     Chi ti pia       Loading     Chi ti pia     Loading       Log     Loading     Loading       Shaper     Chi ti nage     Chi ti nage       Log Filo     Stating     Chi ti nage       Log Filo     Stating     Stating       Log Filo     Minory utage     Nonory utage       Serves     Stating stating stating     Stating stating stating       Nower     Stating stating stating stating     Stating stating stating stating	AMD Byzen 9 35500 16 Core Processor (4 cores, 4 the 90 0.32, 0.20, 0.17 0.423243 Fri Jan 26 20:49:57 UTC 2024 Fri Jan 26 20:61:55 UTC 2024	readisj	login ntpd pf routing sysctl	Users and Groups Network Time Dae Packet Filter System routing System tunables	mon			c c c	-
Intering         CPU Large         100	Buse         CPU usage           Floating         Lod anneage           Lot         Second           Logkub         Second           Next         Concreted databins           Second         State           Log Pilos         State blas blas           Orgonotics         Maluf: Loggin           Vivi         Saverage           Vivi         State blas blas           Vivi         Saverage           New         Saverage           Holp         Saverage	100 0.32, 0.20, 0.17 0400548 Fri Jan 28 2049:57 UTC 2024 Fri Jan 28 2049:55 UTC 2024		ntpd pf routing syscti	Network Time Dae Packet Filter System routing System tunables	mon			0 0 0	•
Floring         0           1.43         Lod average         0.22, 20, 20, 12. T         ending         5 gitter modified         ending         5 gitter modified         ending         5 gitter modified         5 gitter modifi	Finding     Local average       Levi     Local average       Lopanik     Description       With     Description       Bituper     Control disfloying       Log Fills     State table and Desprotte       Von     Monory valge       Services     Station and Description       New     Station and Description       New     Station and Description	0 0.32, 0.20, 0.17 0450343 Fri Jan 26 2049:57 UTC 2024 Fri Jan 26 2047:55 UTC 2024		pf routing sysctl	Packet Filter System routing System tunables				c	
Lod average         0.22, 2.21, 0.17         method         system recently         System recently         C         C           Logback         6000         600, 0.22, 0.21, 0.17         9000         9000         9000         9000         9000         9000         9000         9000         9000         9000         9000         9000         0         1.0         20, 0.0000         0         90000         0         9000         0         9000         0         9000         0         9000         0         9000         0         9000         0         9000         9000         9000         9000         9000         9000         9000         9000         9000         9000         9000 <td>LAY Lod average Logauk. Optime Way Correct data/any Statuper Y Lod config chang Statuper C C/U usage Disprostica C C/U usage Disprostica C C/U usage Disprostica C C U usage Disprostica C C C U usage Disprostica C C C C C C C C C C C C C C C C C C C</td> <td>0.32, 0.20, 0.17 04:03:43 Fri Jan 28 20:49:57 UTC 2024 Fri Jan 28 20:47:45 UTC 2024</td> <td></td> <td>routing sysctl</td> <td>System routing System tunables</td> <td></td> <td></td> <td></td> <td>c</td> <td></td>	LAY Lod average Logauk. Optime Way Correct data/any Statuper Y Lod config chang Statuper C C/U usage Disprostica C C/U usage Disprostica C C/U usage Disprostica C C U usage Disprostica C C C U usage Disprostica C C C C C C C C C C C C C C C C C C C	0.32, 0.20, 0.17 04:03:43 Fri Jan 28 20:49:57 UTC 2024 Fri Jan 28 20:47:45 UTC 2024		routing sysctl	System routing System tunables				c	
Logekå         Ottom         045545         International Statement         Internatistatestatement         International Statement </td <td>Logeback Direct databan Nov Direct databan Stanper Y Lisc crift databan Log Filos S State table sole Disportion S State table sole Nov M Monory usage Ser Vices S State Park and Park Nover S State Park and Park Ser Vices S State Park and Park Ser Vices S State Park and Park Ser Vices S State Park and Park Nover S State Park and Park State Park State Park State Park and Park State Park State</td> <td>04:03:x83 Fri Jan 26 20:49:57 UTC 2024 Fri Jan 26 20:47:45 UTC 2024</td> <td></td> <td>systel</td> <td>System tunables</td> <td></td> <td></td> <td></td> <td>C</td> <td></td>	Logeback Direct databan Nov Direct databan Stanper Y Lisc crift databan Log Filos S State table sole Disportion S State table sole Nov M Monory usage Ser Vices S State Park and Park Nover S State Park and Park Ser Vices S State Park and Park Ser Vices S State Park and Park Ser Vices S State Park and Park Nover S State Park and Park State Park State Park State Park and Park State Park State	04:03:x83 Fri Jan 26 20:49:57 UTC 2024 Fri Jan 26 20:47:45 UTC 2024		systel	System tunables				C	
With         Derest data/une         In Jan 28 20x832 VUI (2024)         System thabits         Sys	With         Durrent data/unit           Shaper         Y         Laccortig charac           Log Files         Chu wage         Log Files         Bata shale she           Dagnostics         M         Multir usage         NN           Services         Services         Services         Noir wage           Now         Now         Monory usage         Now wage           Holp         Doix wage         Now         Now	Fri Jan 26 20:49:57 UTC 2024 Fri Jan 26 20:47:45 UTC 2024		syscti	System tunables					
Statistic         Statistic <t< td=""><td>Samayer         Y         Lext curling change           Samayer         C         Chu wage           Log Filos         State table site           Disprotito         Mature tables           Vini         Mature tables           Vini         State tables           Vini         State tables site           Vini         State tables           Vini         State tables</td></t<> <td>Fri Jan 26 20:47:45 UTC 2024</td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td>U.</td> <td></td>	Samayer         Y         Lext curling change           Samayer         C         Chu wage           Log Filos         State table site           Disprotito         Mature tables           Vini         Mature tables           Vini         State tables           Vini         State tables site           Vini         State tables	Fri Jan 26 20:47:45 UTC 2024							U.	
Satering:         CPU mage         2%           Log Rink:         Bate table size         6% ((48500))           Dogroom:         Bate table size         6% ((48500))           Win/         MEMF scoge         0% ((48500))           Memory carge         116 (448)(4502 M8) ((A67 carb L4 M8))           Services         State table size           Dok mage         0% ((1822 M8))           Memory carge         10% (0482 M8) ((MR Carb L4 M8))           Memory carge         0% (0182 M8)           Services         Disk mage           Disk mage         5% (NR (11, 10070))           0% house (Left) Rescale 114 (MR Carb)	Setting C C/U usage Log Filos C Musey Dogorottos C Multi rosoge Von Munory usage Serves S Sub/P usage Nower Sub/P usage Nower S Sub/P usage			syslog-ng	Syslog-ng Daemon				C	
Lating         Table Isable actor         Bitle Isable actor<	Log Filss and Log Fils and	2%		unbound	Unbound DNS			Þ	c	
Lóg had         and         Christian         Christreinter in the ford for the ford ford for the for the	Log Pilos on Mall Pilos Netrono (Log Pilos Netrono) (Log Pilos Net	0.55 (8/405000)		webgul	Web GUI				c	
Dogoniza         Main Hodge         Unit (1,14/2004)         Calensing	Disprostics Mester Logge VerN Memory Usage Services SNUP usage Power Disk usage Help									
NMINON VUNY         MUNON VUNGE         1156 (423/2023/18) [/MC 2021 /88].         NMINON VUNGE         RTT	VPN Mcmory usage Services SWAP usage Power Disk usage Help	0%(1524/250898)		Gateways					1	- ,
Services	Services SWAP usage Power Disk usage Help	11 % ( 463/4052 MB ) ( ARC size 158 MB	s)	Name	PTT	RTTA	Loss	Status		
Pose         Disk (usage         9% (2%) (23(2/26) 10% (beschell 9% (auchnell (ph) (9%2/26) 0% (auchnell (ph) (ph) (ph) (ph) (ph) (ph) (ph) (ph)	Power Disk usage Help	0 % (0/8192 MB)								
Bits/p         139 (hotodi (finusidadi) (Lank/2000)         MAX 2002         MAX 2002           0% (sourd) (fin) (MV202)         121481.3         121481.3           0% (sourd) (fin) (MV202)         121481.3         121481.3           0% (sourd) (fin) (MV202)         121481.3         121481.3           0% (sourd) (fin) (MV202)         141474568         1216828         121481.3           0% (sourd) (fin) (MV202)         141474568         1216828         12131.3         1           0% (sourd) (fin) (MV202)         1414         1216828         12131.3         1         1           0% (sourd) (fin) (MV202)         1414         1216828         1216828         12131.3         1         1         1         12141.3         1	Help	5% / [zts] (1.26/236]		WAN_DHCP6	-	-	-	Coline		
Image         Other, January (Left) (1997) (2017)         Interfaces         Interfaces           Off, Interfaces (Left) (1997) (2017)         Interfaces         Interfaces         Interfaces         Interfaces           Off, Interfaces (Left) (1997) (2017)         Interfaces         Interfaces         Interfaces         Interfaces         Interfaces           Off, Interfaces (Left) (1997) (2017)         Interfaces         Interfaces         Interfaces         Interfaces         Interfaces           Off, Interfaces (Left) (1997) (2017)         Interfaces         Interfaces         Interfaces         Interfaces           Off, Interfaces (Left) (1997) (2017)         Interfaces         Interfaces         Interfaces	Help	1% /boot/efi [msdosfs] (1.8M/260M)						-		
		0% /var/mail (zfs) (96K/22G)		192.165.2.1				College		
		0% /zroot [zfs] (98K/22G)								
の参加         (MIRITARIA         MIRITARIA           の参し、Ample (MIRITARIA         第二人工業         第二人工業         第二人工業           の参し、Ample (MIRITARIA         第二人工業         第二人工業         第二人工業         1.050ase 1.461         <		0% /usr/home [zfs] (96K/22G)		Interference						
이하, Anziperts (16) (1997/220) 이하, Anziperts (16) (1997/220)		0% /tmp [2fs] (320K/22G)		Interfaces					1	
ゆか、Anacleg (JN) (11,142730) の切()-valuet (JAG) 1994/2020) のか、Anacrona (Jn4) (964/2020) のかい、Anacrona (Jn4) (964/2020) のから、Anacrona (Jn4) (964/2020) のから、Anacrona (Jn4) (964/2020)		0% /usr/ports [zfs] (96K/22G)		= LAN	10Gbase T Kful	ll-duplec>	10.13.37.1			
0%/wijkel/Edi/09/2200         Adda		0% /var/log [zts] (1.1M/22G)		TT WAN	A 100hore.1 (fr)	Lehenhach	192 168 2 128			
6% /vatices) (Http://doc.200) 0% /vatices (Http://doc.200) 0% /vatices (Http://doc.200)		which is an element of the Particle States of the second s		- 1053	Tradasen Ha	in ouplex.	192.100.2.170			
0% /met/trow (cds) 0042220) 0% /met/sec (zds) (004/220)		vits /var/audit [zts] (96K/22G)								
0%/tantarc(tht)(00K/226)		0% /var/audit [zts] (9%/226) 0% /var/crash [zts] (96K/226)								
		0% /var/audit (zts) (90K/220) 0% /var/crash (zts) (96K/220) 0% /var/tmp (zfs) (96K/220)								
AMPL		0% /var/studik (zts) (96K/226) 0% /var/crash (zts) (96K/226) 0% /var/trup [zfs) (96K/226) 0% /var/trup [zfs) (96K/226)								
	Officience in 2014-20	0% /var/audit [zts] (96K/226) 0% /var/crash [zts] (96K/226) 0% /var/tmp [zts] (96K/226) 0% /var/src [zts] (96K/226)								

26. Now, let us look at the firewall rule creation. Navigate to **Firewall** | **Rules**:

### Figure 52 – Dashboard Firewall Rule

- <u>ک</u> ۵۲۵ Firewall: Rules: WAN System Edit Firewall rule renaces O Action Block Alizes O Disable ъ 4 Cates 0 Quick O Interface O TCP/IP Vers Protocol O ICMP type Uno this O Source anv Рожи Open O Destinatio an 0 Dext Log packets Olor
- 27. Add new firewall rules to control inbound and outbound traffic:

Figure 53 – WAN Firewall Rule

28. In this example, create a WAN firewall rule to BLOCK inbound ICMP. Click the Log Packets that are handled by this rule option and provide Categories and a description. Then click Save:

Services		any
∯ Power (1) Help	OLog	Log packets that are handled by this rule
	Category	WAN × DENY × KMP × N ×
	Description	WAN - Deny ICMP IN
	O No XMLRPC Sync	
	0 Schedule	none
	() Gabeway	default •
	Advanced features	Show/Hide
		Save Cancel
	CPNsense (c) 2054-2023 Deciso B.V.	

Figure 54 – Saving Firewall Rule

29. Once you save the rule click **Apply Changes**:

			sen X 📫 New Tab															
			A https://10.13.37.1/fre										<b>\$</b>			9 6		
۶OF	⊃∏ <mark>sensei</mark> <										root@0P	Nsens	se.localdomain 🌒 🔍					
😐 Lobby	u		Firewall: Rules:	WAN									Select category			• [	® Inspi	et
ah Interface	5	_	The firewall rule config You must apply the cha	uration has bee nges in order fo	n changed. r them to take el	fect.										'apiy (	hanges	
Catego	, ntes	*		Protocol	Source	Port	Destination	Port	Gateway	Schedi	ule	4	Description 😡		•	e a	8 0	1
Groups		4	<u>۵</u>										Automatically generated rules		0	•		
NAT		=	□ × → † 0	IPv4 ICNP			•						WAN - Deny ICMP IN		+	10		
Rules	ing	~	<ul> <li>pass</li> <li>pass (disabled)</li> </ul>	××	block block (disabled)		O reject O reject (d	isabled)		D log D log (di	isabled)		→ in ← out	* *	first match last match			
LUN			📫 🛗 Active/Inactive Sc	hedule (click to	view/edit)													
Loopi	back		Alias (click to view/ed	(1)														
WAN			WAN rules are evaluated	on a first-match	basis by default	(i.e. the ad	tion of the first ru	ie to matcl	h a packet will	be execute	ed). This m	ioans 1	that If you use block rules, you will	l have t	o pay attentio	in to th	e rule	
Shaper		τ	order. Everyoning diacis i	for explicitly pa	sseo is blocked t	y detaut.												
Setting	p	0																
Log Fil	8	÷.																
Diagno	istics	1ČI																
O VPN																		
O Services																		
∭er Power																		
O Help																		

# Figure 55 – Applying Changes

30. Next, test the firewall rules by attempting to access resources from various network locations:

	sectoc@maul: -	ж	seco	loc@pihole-debia	n 12-kvm-svr: ~	×	sectoo@maul: -	× •
sectorimaul:=\$ pirg 102. PING 192.168.2.175 (102. C							Select sategory	
26 packets transmitter,	e vecsiver, 1100							
sectoripaul :=\$								

# (a) Testing Rule





## Figure 56 – Live Firewall Logs

31. Monitor traffic and manage firewall rules regularly.

One particular note, like pfSense, OPNsense supports various plug-ins or modules such as Snort and Surricata. OPNsense, supports other plug-ins not available within pfSense such as Zenarmor (<u>https://www.zenarmor.com/</u>) which you can install and extend the capabilities of the firewall to include Layer-7 inspection and proxy capabilities.

Following is a sample screenshot of the dashboard and visibility associated with Zenarmor:



Figure 57 – OPNsense Zenarmor Plugin Dashboard

Let's move on to the next lab.

# Lab 3: SIEM Solution Using Graylog Open in a Virtual Environment

Graylog is an open-source, centralized log management and analysis platform that helps organizations collect, store, and analyze log data from various sources, such as servers, applications, and network devices. Built on top of Elasticsearch, MongoDB, and other open-source technologies, Graylog provides a scalable and flexible solution for managing large volumes of log data in real-time. Its user-friendly web interface allows users to easily search, filter, and visualize log data, enabling them to quickly identify and investigate potential security incidents, performance issues, and other important events. Graylog also offers a powerful alerting system that can notify administrators when specific conditions are met, such as when a critical error occurs or when suspicious activity is detected. With its extensive plugin ecosystem and APIs, Graylog can integrate with a wide range of tools and services, making it a versatile and valuable addition to any organization's monitoring and logging infrastructure. Whether used for security, compliance, or troubleshooting purposes, Graylog empowers organizations to gain valuable insights from their log data and make informed decisions to improve their overall IT operations.



Figure 58 – Graylog Website

The prerequisites are:

- A VM capable of running Graylog (in this lab/example the VM is Ubuntu 22.04 Server with 4-cores and 16GB of RAM and 100GB Harddrive).
- Administrative privileges for software installation
- Java 8 or higher

Let us look at the steps:

- 1. Create a new VM to host the Graylog server.
- 2. Allocate sufficient resources based on the expected volume of log data.
- 3. Set up network adapters to communicate with other VMs (for log sources) and potentially the host machine.
- 4. For the Graylog installation, install MongoDB and Elasticsearch as Graylog dependencies.

- Download and install Graylog repository configuration with the package manager or go to <u>https://qo2docs.gravlog.org/5-</u>
   <u>2/downloading\_and\_installing\_gravlog/ubuntu\_installation.html</u>. The lab shows the step-by-step instructions associated with installing Graylog Server 5.2 running Opensearch as referenced on the Graylog Website.
- 6. Now, let's move to the installation of Graylog. To configure the Graylog server to use a particular time zone, run the following command:

sudo timedatectl set-timezone UTC

#### Note

The mongodb package included with Ubuntu distributions is not maintained by MongoDB Inc and conflicts with the official mongodb-org package. If the mongodb package is already installed, you must uninstall it first before proceeding.

7. To install MongoDB Community Edition, import the public key for the package management system, if gnupg and curl are not already installed, run:

```
sudo apt-get install gnupg curl
```

Import the MongoDB public GPG key from <a href="https://pgp.mongodb.com/server-7">https://pgp.mongodb.com/server-7</a>
 7.0.asc using this command:

```
curl -fsSL https://pgp.mongodb.com/server-7.0.asc | \
   sudo gpg -o /usr/share/keyrings/mongodb-server-7.0.gpg \
   --dearmor
```

9. For Ubuntu 22.04 (Jammy), create the repository file at /etc/apt/sources.list.d/mongodb-org-7.0.list:

```
echo "deb [ arch=amd64,arm64 signed-
by=/usr/share/keyrings/mongodb-server-7.0.gpg ]
https://repo.mongodb.org/apt/ubuntu jammy/mongodb-
org/7.0 multiverse" | sudo tee
/etc/apt/sources.list.d/mongodb-org-7.0.list
```

10. Reload the local package database - run this command to refresh the local package index:

# sudo apt-get update

11. To install the latest stable version, issue the following:

```
sudo apt-get install -y mongodb-org
```

12. If you need to incorporate proxies or other restricted environments, you can implement a keyserver solution using a widget.

```
wget -q0-
'http://keyserver.ubuntu.com/pks/lookup?op=get&search=0xf56
79a222c647c87527c2f8cb00a0bd1e2c63c11' | sudo apt-key add -
```

13. Configure MongoDB to start automatically when the operating system boots up, and check that the MongoDB service is active and running:

sudo	systemctl	daemon-reload
sudo	systemctl	enable mongod.service
sudo	systemctl	restart mongod.service
sudo	systemctl	type=servicestate=active   grep mongod

- 14. The OpenSearch documentation recommends following their user guides for installation at the following URL: <u>https://opensearch.org/docs/latest/install-</u> and-configure/install-opensearch/debian/.
- 15. To integrate OpenSearch with Graylog, you can take these steps. This example demonstrates installing OpenSearch using the DEB package. Import the public GPG key to verify that the APT repository is signed:



16. Create an APT repository for OpenSearch:

```
echo "deb [signed-by=/usr/share/keyrings/opensearch-
keyring]
https://artifacts.opensearch.org/releases/bundle/opensearch
/2.x/apt stable main" | sudo tee
/etc/apt/sources.list.d/opensearch-2.x.list
```

17. Check that the repository was added correctly:

# sudo apt-get update

18. After adding the repository information, display all OpenSearch versions available for installation:

```
sudo apt list -a opensearch
```

19. Select the OpenSearch version to install (the latest version will be installed if a specific version is not specified):

## sudo apt-get install opensearch

20. To configure Graylog for OpenSearch, start by opening the Graylog configuration file in YAML format:

## sudo nano /etc/opensearch/opensearch.yml

21. At minimum, update these configuration fields (for an unsecured single-node setup) to integrate OpenSearch with Graylog:

```
cluster.name: graylog
node.name: ${HOSTNAME}
path.data: /var/lib/opensearch
path.logs: /var/log/opensearch
```

You can see these in the following image:



Figure 59 – Opensearch YAML Configuration – Parameters Part 1

Updating the OpenSearch YAML file is crucial when setting up Graylog to ensure seamless integration and optimal performance. The YAML file contains essential configuration settings that define how OpenSearch, a powerful open-source search and analytics engine, interacts with Graylog. By modifying this file, you can customize various aspects of OpenSearch's behavior, such as cluster settings, node roles, and memory allocation. Proper configuration of the OpenSearch YAML file is necessary to ensure that Graylog can efficiently index, store, and retrieve log data, enabling fast and accurate search results. Additionally, updating the YAML file allows you to enable important features like authentication, encryption, and data replication, which are critical for securing your log data and ensuring high availability. Failing to update the OpenSearch YAML file correctly can lead to suboptimal performance, compatibility issues, and even data loss. Therefore, taking the time to carefully review and modify the YAML file is an essential step in setting up a robust and reliable Graylog implementation:

```
discovery.type: single-node
network.host: 0.0.0.0
Http.port: 9200
```

These are visible in the following image:



Figure 60 – Opensearch YAML Configuration – Parameters Part 2

By setting action.auto\_create\_index: false in the OpenSearch YAML configuration, you enhance security, optimize performance, ensure compatibility with Graylog's index management strategies, and promote better governance over your log data indices:

```
action.auto_create_index: false
plugins.security.disabled: true
```

It's important to note that disabling the OpenSearch security plugin does not mean that your log data is unprotected. Graylog's built-in security features, combined with proper network isolation and access controls, can still provide a robust security framework for your log management system.

However, if your organization has specific security requirements or compliance regulations that mandate the use of the OpenSearch security plugin, you may need to keep it enabled and configure it accordingly. In such cases, you should refer to the Graylog documentation and OpenSearch security plugin documentation to ensure proper integration and configuration:



Figure 61 – Opensearch YAML Configuration – Parameters Part 3

22. Once all updates are made to the opensearch.yaml file, press CTRL+O and press Enter and then exit by pressing CTRL+X:

plugins.security.cneck_snapsnot_restore_write_privit	Leges: true		
plugins.security.restapi.roles_enabled: [*all_access			
plugins.security.system_indices.enabled: true			
plugins.security.system_indices.indices: [*.plugins-			".plugins-ml-conversation-meta", ".plugins-ml-conversation
node.max_local_storage_modes: 3			
######### End OpenSearch Security Demo Configuration			
action.auto_create_index: false			
plugins.security.disabled: true			
File Name to Write: /etc/opensearch/opensearch.yml			
°G Help	N-E DOS Format	M-A Append	N-B Backup File
Cancel	N-N Mac Format	M-P Prepend	T Browse

Figure 62 – Saving Configuration

23. Use these commands to add the Graylog package repository and install Graylog:

```
wget https://packages.graylog2.org/repo/packages/graylog-
5.2-repository_latest.deb
sudo dpkg -i graylog-5.2-repository_latest.deb
sudo apt-get update && sudo apt-get install graylog-server
```

Adding the Graylog package repository and installing Graylog from it is crucial to ensure a smooth and secure setup of your log management system. By using the official Graylog package repository, you gain access to the latest stable version of Graylog, which is thoroughly tested and optimized for production environments. The package repository also simplifies the installation process by handling dependencies and providing automatic updates, ensuring that your Graylog instance remains up-to-date with the latest features, bug fixes, and security patches. This streamlined approach reduces the risk of compatibility issues and vulnerabilities that may arise from manual installations or using outdated packages. Moreover, the Graylog package repository provides a consistent and reliable way to deploy Graylog across multiple systems or environments, making it easier to maintain and scale your log management infrastructure. By leveraging the package repository, you can focus on configuring and using Graylog to gain valuable insights from your log data, rather than worrying about the intricacies of the installation process. Overall, adding the Graylog package repository and installing Graylog from it is a best practice that ensures a robust, secure, and maintainable log management solution:



Figure 63 – Installing Graylog

24. Review the instructions in the Graylog server configuration file at /etc/graylog/server/server.conf and modify as necessary. You must also add values for password\_secret and root\_password\_sha2 in this file, as Graylog will fail to start if these parameters are missing.

Generate a password\_secret value by running this command:

#### //dev/urandom tr -dc A-Z-a-z-0-9 | head -c\${1:-96};echo;

Reviewing and modifying the Graylog server configuration file (/etc/graylog/server/server.conf) is essential to ensure that your Graylog instance is set up correctly and securely. The configuration file contains various settings that control the behavior and performance of your Graylog server, such as network interfaces, authentication mechanisms, and data retention policies. By carefully reviewing and adjusting these settings, you can tailor Graylog to your specific requirements and optimize its performance for your environment.

One of the most critical aspects of configuring Graylog is setting the password\_secret and root\_password\_sha2 parameters. These parameters are essential for securing your Graylog installation and protecting sensitive data:

- A. password\_secret: This is a randomly generated secret string used for securely encrypting and decrypting sensitive data, such as user passwords and access tokens. Without a valid password\_secret, Graylog will not be able to start, as it cannot ensure the security of stored data. Generating a strong, random password\_secret is crucial to prevent unauthorized access and protect your log data from potential breaches.
- B. root\_password\_sha2: This parameter sets the SHA-2 hash of the root user's password. The root user is a built-in administrative account with full access to the Graylog system. By setting a strong, hashed password for the root user, you prevent unauthorized access to your Graylog instance and ensure that only authorized personnel can manage the system.

To generate a secure password secret value, you can use the command:

## < /dev/urandom tr -dc A-Z-a-z-0-9 | head -c\${1:-96};echo;</pre>

This command reads random data from the /dev/urandom device, filters out only alphanumeric characters, and generates a 96-character random string. Using a randomly generated secret helps ensure the strength and uniqueness of the password\_secret, making it much harder for attackers to guess or crack.

In summary, reviewing and modifying the Graylog server configuration file, particularly setting the password\_secret and root\_password\_sha2 parameters, is critical for securing your Graylog installation. By generating a strong, random password\_secret and setting a hashed password for the root user, you protect your log data, prevent unauthorized access, and ensure the overall integrity of your log management system. Neglecting to set these parameters or using weak values can leave your Graylog instance vulnerable to security risks and compromise the confidentiality and reliability of your log data:



#### Figure 64 – Graylog Password Secret

25. Then generate the **root password sha2** hash using this command:



26. Once both hash values are generated, save these to a text file so they can be placed within the <a href="https://www.etw.conf">/etc/graylog/server/server.conf</a> file.

Update and uncomment the file for the following configuration items:

password\_secret

#### root\_password\_sha2

Saving the generated hash values for password\_secret and root\_password\_sha2 to a text file before placing them in the /etc/graylog/server/server.conf file is important for several reasons:

- A. Secure Storage: Storing the hash values in a separate text file allows you to keep them in a secure location, such as an encrypted disk or a password manager. This is particularly important for the password\_secret, as it is used to encrypt sensitive data in your Graylog instance. By storing the hash values separately, you reduce the risk of accidentally exposing them to unauthorized users or committing them to version control systems.
- B. Backup and Recovery: Having a separate text file with the hash values serves as a backup in case the /etc/graylog/server/server.conf file becomes corrupted, accidentally modified, or lost. If you need to restore your Graylog configuration or migrate to a new server, having the hash values readily available in a text file will make the process faster and easier.
- C. Auditing and Documentation: Storing the hash values in a text file creates a record of the values used for your Graylog installation. This can be useful for auditing purposes, as you can verify that the correct hash values were used and that they haven't been changed unexpectedly. It also serves as documentation for future reference, making it easier for you or other administrators to understand and maintain the Graylog setup.

After saving the hash values to a text file, you need to update and uncomment the corresponding configuration items in the /etc/graylog/server/server.conf file:

A. password\_secret: Locate the password\_secret setting in the configuration file and uncomment it by removing the # symbol at the beginning of the line. Paste the generated password\_secret hash value

from your text file after the = sign. This setting is critical for Graylog to securely encrypt and decrypt sensitive data.

B. root\_password\_sha2: Find the root\_password\_sha2 setting in the configuration file and uncomment it by removing the # symbol at the beginning of the line. Paste the generated root\_password\_sha2 hash value from your text file after the = sign. This setting ensures that the root user's password is securely stored and validated.

By updating and uncommenting these configuration items with the hash values from your text file, you are enabling the security features essential for protecting your Graylog installation. Failure to set these values correctly may result in Graylog failing to start or leaving your system vulnerable to unauthorized access.

In summary, saving the generated hash values to a text file before placing them in the Graylog server configuration file is a best practice that promotes secure storage, backup and recovery, and auditing. Updating and uncommenting the password\_secret and root\_password\_sha2 settings with the correct hash values is crucial for ensuring the security and proper functioning of your Graylog instance:



Figure 65 – Update Graylog Server Configuration with Secret

The http\_bind\_address setting in the Graylog server configuration file (/etc/graylog/server/server.conf) is used to specify the IP address and port on which the Graylog web interface will listen for incoming HTTP connections. This setting determines how users and other systems can access the Graylog web interface.

It's important to carefully consider the <a href="http\_bind\_address">http\_bind\_address</a> setting and configure it according to your specific requirements. Setting it incorrectly or exposing the Graylog web interface to untrusted networks can pose security risks and allow unauthorized access to your log management system:

#### http bind address

The <a href="http\_bind\_address">http\_bind\_address</a> setting in the Graylog server configuration determines the IP address and port on which the Graylog web interface listens for incoming HTTP connections. It plays a critical role in controlling access to the web interface and should be configured in alignment with your network setup and security requirements. By properly setting the <a href="http\_bind\_address">http\_bind\_address</a>, you can ensure that the Graylog web interface is accessible to authorized users and systems while minimizing the risk of unauthorized access:



Figure 66 – Update Graylog Server Configuration – Binding IP Address

The configuration file for Graylog still references Elasticsearch settings like elasticsearch\_hosts, elasticsearch\_index\_prefix, elasticsearch\_analyzer, elasticsearch\_shards, and elasticsearch\_replicas because Graylog was originally designed to work with Elasticsearch as its backend storage and search engine. However, OpenSearch has emerged as a popular alternative to Elasticsearch, and Graylog now supports using OpenSearch as well:

```
rotation_strategy
```

elasticsearch max docs per index

Together, the rotation strategy and

elasticsearch\_max\_docs\_per\_index settings help you manage the lifecycle of Elasticsearch indices in Graylog. They allow you to control how data is organized, rotated, and retained over time, ensuring optimal performance and storage efficiency:



Figure 67 – Update Graylog Server Configuration – Index and Rotation

The elasticsearch\_hosts setting in the Graylog server configuration file (/etc/graylog/server/server.conf) is used to specify the connection details for one or more Elasticsearch nodes that Graylog will use for storing and searching log data. Elasticsearch is a distributed search and analytics engine that serves as the backend storage for Graylog:

# elasticsearch hosts

It's crucial to ensure that the elasticsearch\_hosts setting is properly configured to point to the correct Elasticsearch (opensearch) node(s) and that the specified nodes are accessible from the Graylog server. Misconfiguration or connectivity issues between Graylog and Elasticsearch can prevent Graylog from storing and searching log data effectively:





The elasticsearch\_index\_prefix, elasticsearch\_analyzer,
elasticsearch\_shards, and elasticsearch\_replicas settings in
the Graylog server configuration file

(/etc/graylog/server/server.conf) are used to control various aspects of how Graylog interacts with Elasticsearch and manages the indexing and storage of log data:

```
elasticsearch_index_prefix
elasticsearch_analyzer
elasticsearch_shards
elasticsearch_replicas
```

When configuring these settings, consider your specific requirements, data volume, performance needs, and Elasticsearch cluster setup. It's recommended to consult the Elasticsearch documentation and best practices to make informed decisions based on your deployment scenario.

By properly tuning the elasticsearch\_index\_prefix,
elasticsearch\_analyzer, elasticsearch\_shards, and
elasticsearch\_replicas settings, you can optimize how Graylog
interacts with Elasticsearch, ensuring efficient indexing, searching, and storage
of log data while meeting your performance and availability goals:



Figure 69 – Update Graylog Server Configuration – Elasticserach (opensearch) configuration

The retention\_strategy and retention\_strategy settings in the Graylog server configuration file (/etc/graylog/server/server.conf) are used to define how Graylog handles the retention and deletion of old log data. These settings allow you to control the lifecycle of your log data, ensuring that your storage space is efficiently utilized and that you retain log data for the desired duration:

```
retention_strategy retention_period
```

By carefully configuring the retention\_strategy and elasticsearch\_retention\_period settings, you can effectively manage the lifecycle of your log data in Graylog, ensuring that you retain data for the necessary duration while optimizing storage utilization and performance:



Figure 70 – Update Graylog Server Configuration – Elasticserach (opensearch) Retention Configuration

Running the command sudo systemctl daemon-reload after making updates to the Graylog server configuration is important because it ensures that the systemd manager is aware of the changes made to the configuration files:

```
sudo systemctl daemon-reload
```

Note that Graylog does not start automatically after installation.

27. To configure Graylog to start on system boot, run these commands:

	sudo	systemctl	enable	e gray	ylog-se	erver.ser	rvi	ce		
	sudo	systemctl	start	gray]	og-ser	ver.ser	∕ic€			
sudo	o syst	temctlty	ype=sei	rvice	stat	e=active	)	grep	graylo	g

Let's go through each command and explain its importance:

A. sudo systemctl enable graylog-server.service: This command enables the Graylog server service to start automatically at system boot.

- B. sudo systemctl start graylog-server.service: This command starts the Graylog server service immediately.
- C. sudo systemctl --type=service --state=active | grep graylog: This command is used to verify the status of the Graylog server service. It lists all the active systemd services and filters the output to include only the lines containing the word "graylog".

The combination of these commands ensures that the Graylog server service is properly enabled, started, and verified:

If there are any issues with the installation or configuration, starting the service may result in errors or failures, which would need to be addressed separately:



Figure 71 – Restart Graylog Service

28. Now, onto accessing web interface. Open the Graylog web interface by



navigating to http://lyour\_graylog\_ip]:9000:

Figure 72 – Graylog Web Login Screen

Once your Graylog instance or cluster is running, you can access the web interface for searching and analyzing indexed data and managing your Graylog

configuration. By default, the interface is available at <a href="https://<graylog-server>:9000/">https://<graylog-server>:9000/</a>.

29. If you run into the issue where the web interface is not loading, run the command netstat -nl within the terminal on the Ubuntu server to make sure that the system is listening on port 9000:



**Figure 73 – Netstat System Listening Ports** 

- 30. To log into the web interface, open a browser and navigate to <u>https://<io-</u> address>:9000, substituting your Graylog server's IP address.
- 31. Sign in as an admin user and enter the password secret set during Graylog installation:



Figure 74 – Login to Graylog

32. After logging in, you will be brought to the initial welcome screen:



#### Figure 75 – Graylog Welcome Screen

Now that the hard part is over, you can get started with other aspects of getting data into Graylog:

- Input configuration: Set up an input in Graylog to receive data. For example, create a Syslog UDP input to listen for incoming logs.
- System integration: Configure systems to send logs to Graylog. For Snort, you may set up Barnyard2 to forward Snort logs to Graylog or syslog from OPNsense.
- **Creating dashboards**: Within the Graylog interface, create dashboards to visualize the incoming log data and analyze events.
- Alert configuration: Set up alerts in Graylog to notify you of potential security incidents based on the logs.

I have placed sample content packs for Graylog in my Github page which can be found at <u>https://github.com/secdoc</u>, which can be a starting point and enable you further in getting Graylog configured. This includes dashboards, inputs and pipelines. Here is the example of pipeline JSON:

{

```
"v": "1",
      "type": {
        "name": "pipeline rule",
        "version": "1"
      },
      "id": "d983c394-563a-4d22-b52b-f77f8553ea56",
      "data": {
        "title": {
          "@type": "string",
          "@value": "src-ip threat intel"
        },
        "description": {
          "@type": "string",
          "@value": "src-ip threat intel"
        },
        "source": {
          "@type": "string",
          "@value": "rule \"src-ip threat intel\"\nwhen\n
has field(\"nf src address\") && !
in private net(to string($message.src ip)) \nthen\nlet
src addr intel =
threat_intel_lookup_ip(to_string($message.nf_src_address),
\"nf_src_address\");\nset_fields(src_addr_intel);\n\nlet
dns question intel =
threat intel lookup domain(to string($message.dns question)
\"dns question\");\nset fields(dns question intel);\n\nlet
whois intel =
whois lookup ip(to string($message.nf src address),
\"nf src addressr\");\nset fields(whois intel);\nend"
```



Each lab session should be followed by a cleanup procedure to reset the environment if needed. Additionally, by running these labs in virtual environments, you not only ensure a controlled and replicable setup for each lab iteration but also provide an opportunity to simulate a more realistic network environment with multiple interacting systems. This approach offers a safer and more scalable method for cybersecurity training and experimentation.

By combining controls for prevention, detection, analysis, and alerting, network security tools provide pervasive visibility and protection across environments. Architects must carefully evaluate options to balance risk coverage and TCO.

# **Endpoint protection tools**

Let us look at the labs.

# Lab 1: Antivirus Software Implementation Using ClamAV

ClamAV is a popular open-source antivirus software designed to detect and prevent malware infections on various operating systems, including Linux, Windows, and macOS. Developed by Cisco Talos, ClamAV provides a comprehensive toolkit for scanning files, email attachments, and web traffic for viruses, trojans, malware, and other security threats. Its versatility and reliability have made it a go-to solution for system administrators, security professionals, and individuals seeking to protect their systems from malicious software. ClamAV offers both command-line and graphical user interfaces, making it accessible to users with different levels of technical expertise. It features regular database updates to ensure protection against the latest threats, and its modular architecture allows for integration with other security tools and platforms. Whether used as a standalone antivirus solution or as part of a larger security infrastructure, ClamAV plays a crucial role in maintaining the integrity and security of computer systems in today's threat landscape.



Figure 76 – ClamAV Website

You can access this site at https://www.clamav.net/.

ClamAV is an open-source antivirus engine for detecting trojans, viruses, malware, and other malicious threats.

The prerequisites include:

- A virtual machine (VM) running a Linux distribution (e.g., Ubuntu Desktop for a GUI).
- Internet access for downloading software.
- Administrative privileges within the VM.

If you have followed the lab in Chapter 2 for the installation of ClamAV, this lab can be skipped, but if you bypassed the lab, go back to Chapter 2 and follow the instructions.

# Lab 2: Endpoint Detection and Response (EDR) Solution Implementation Using Wazuh

Wazuh is a powerful and open-source security monitoring solution that provides threat detection, integrity monitoring, and incident response capabilities for a wide range of operating systems and platforms. It is designed to help organizations protect their infrastructure from security threats, detect intrusions, and ensure compliance with security policies and regulations. Wazuh combines the benefits of a **host-based** intrusion detection system (HIDS) and a security information and event management (SIEM) solution, offering a comprehensive and centralized approach to security monitoring. With its agent-based architecture, Wazuh collects and analyzes security data from multiple sources, including log files, system events, and network traffic, to identify potential security issues and anomalies. It utilizes a rule-based approach and machine learning algorithms to detect threats in real-time and generate alerts for further investigation. Wazuh also provides a web-based user interface for managing and monitoring the security status of the entire infrastructure, making it easier for security teams to respond to incidents and maintain a strong security posture. Its open-source nature and active community support make Wazuh a cost-effective and flexible solution for organizations of all sizes looking to enhance their security monitoring capabilities.



Figure 77 – Wazuh Website

Wazuh is a free, open-source EDR solution that provides host-based intrusion detection, system monitoring, and incident response.

The prerequisites are:

• Based on the Wazuh website

(https://documentation.wazuh.com/current/quickstart.html), following is the requirements based on the number of agents that will be deployed:

Agents	CPU	RAM	Storage (90 days)
1-25	4 vCPU	8 GiB	50 GB
25-50	8 vCPU	8 GiB	100 GB
50-100	8 vCPU	8 GiB	200 GB

 Table 1 – Wazuh System Requirements

- A VM with a Linux distribution.
- Internet access for downloading software, <a href="https://wazuh.com/">https://wazuh.com/</a>.
- Administrative privileges within the VM.

Let us look at the steps:

- Create a new VM to serve as the Wazuh server, indexer and dashboard. Optionally, create additional VMs to act as Wazuh agents.
- 2. Download and run the Wazuh installation assistant:

curl	-s0	https://packages.wazuh.com/4.7/wazuh-install.sh	& &
sudo	basł	./wazuh-install.sh -a	

By following these steps, you create a dedicated VM to host the Wazuh server components and optionally set up additional VMs as Wazuh agents. The installation assistant simplifies the installation process by automating the necessary tasks and configurations.

After completing these steps, you will have a functional Wazuh security monitoring system in place. The Wazuh server will be ready to receive and analyze security data from the agents, and you can access the web-based dashboard to monitor and investigate security events in your infrastructure.

Remember to configure the Wazuh agents on the systems you want to monitor and ensure proper network connectivity between the agents and the Wazuh server for seamless data collection and analysis:



Figure 78 – Wazuh Installation

After the assistant completes the installation, it prints the access credentials and a confirmation message indicating the installation succeeded.

3. Access the Wazuh web interface at <a href="https://wazuh-dashboard-ip">https://wazuh-dashboard-ip</a> using these credentials:

Username: admin

**Password**: <ADMIN\_PASSWORD> (the password provided in the terminal after a successful login)

On first login, the browser may display a warning that the certificate is untrusted since it was not issued by a known authority. You can accept the certificate as an exception or replace it with a trusted certificate.

4. The passwords for the Wazuh indexer and API users are stored in the wazuhpasswords.txt file inside the wazuh-install-files.tar archive. To display them, extract and print the file:

```
tar xvf wazuh-install-files.tar wazuh-passwords.txt
cat wazuh-passwords.txt
```

5. To uninstall the Wazuh central components, run the Wazuh installation assistant again with the <u>-u</u> or <u>--uninstall</u> option:



Figure 79 – Wazuh Login Screen

Now that your Wazuh installation is ready, you can start deploying the Wazuh agent. This can be used to protect laptops, desktops, servers, cloud instances, containers, or virtual machines. The agent is lightweight and multi-purpose, providing a variety of security capabilities.

Instructions on how to deploy the Wazuh agent can be found in the Wazuh web user interface:
= 🛆 wazuh, 🗸 Modales				ە 🔕
tenerapore O	Autora agente O		Denating agains O	
A Na sports were added to this manager. And agent				
ысилту втоти	STION NASADEMENT		ALOTTHO AN	D FOLICY MONITORINS
Security overes traver through your society of ets, identifying somes and through in sour overeamore.	Integrity mentioning Anto-related to the damps, including permissions, concert, concepto and 200 bits.	LAL Policy veriging	maninoing Int par systems are configured according to your security Elaborat	System cultifies A dit core behavior, manifolising command resistant and electing or 20050 to 20052 Mer.
			ity configuration assessment In Fasets as part of a configuration assessment audit.	
THREAT BETECTS	OH AND RESPONSE			DRY COMPLIANCE
Vulnerabilities     Excerce white applications is your continuenant arc should by well     income white addition.	MATRELATTACK     Security service memory to its window loss of adversary tools: a me techniques based or nul-work observations	PCI D: Geodi	125 Sourby standord for ontblos that process, stars or transmit et cantholder data	NGT 800-53 Yassad initatio of Stimbards and Technology Social Publication 644-53 MET 884-521 with galifiling the fielders information systems.
		TISC Text of Content	arvicas Critaris în: Socarite, Availability, Processing Integrity, eta-dig-artif Mixecy	COPR Deviced Data Protocolar Regulation (2014) and qualitatives for proveniting of period af Eres.
		HIRAA Huatti prode enterra	l Insurance Penals Re and Accountab Re Act of 1996 (1994) In de a place president in y provision for odequesting medical netw.	

Figure 80 – Wazuh Dashboard

6. On a different VM, install the Wazuh agent by following similar steps or using a pre-built package for the specific OS:

≡ 🗅 wozuh, ∨ Agens		<u>ه</u>
	o reteat Deploy new agent	
	Select the peckage to download and install on your system:	
	LINUX MINDOWS mscOS	
	2 Sarver address:	
	This is the address the agent uses to communicate with the server. Enter an IP oddress or a fully qualified domain name (+ 2014).	
	3 Optional settings:	
	Dy default, the objectivenent cannot the housenene as the agent manne. Optionally, you cannot an different agent mannels The field feature	
	Anlign en egent name: 💿	

Figure 81 – Deploy Wazuh Agent

- 7. In this lab deploy the agent on a Windows 10 system.
- 8. Now, let us look at agent registration. Select the desired target agent operating system:

≡ ∩ wozuh ∨ Aconts				
	Dep	olov new agent		
	Select the package to downloar	d and install on your system:		
	🛆 LINUX	WINDOWS	📹 macOS	
	DEBand64 C 555 aerohd4			
				E.

Figure 82 – Wazuh Windows Agent

 Provide the Wazuh server address the agent uses to communicate with the server. Enter an IP address or a <u>fully qualified domain name</u> (FDQN):

≡   û   wazuh. ∨ Agun				ه   💽 ا
		WINDOWS	macOS	
	O BPM an 654 O BPM avec 154 O DEB an 154 O DEB aon 154		⊂ INH _ Apple silicon	
	Server address:			
	This is the address the agent uses to name (FDGN).	o communicate with the server. Enter an IP	address or a fully qualified domain	
	Annige a surver address: 🚯			

Figure 83 – Wazuh Agent Configuration – Server Address

10. By default, the deployment uses the hostname as the agent name. Optionally, you can use a different agent name in the field:

≡ △ Wazuh, ✓ Açonts		<ul> <li>Image: Second sec</li></ul>
	Addgas some addrese: (f) 192368 2:160	
	Optional setting: By official, the designant use the hotowere as the agent name. Optionally, yes can use a different agent name in the relation. Agent name:	
	feket one anner sonling groupe:	

Figure 84 – Wazuh Agent Configuration – Assign Agent Name

11. To download and install the Wazuh agent on Windows:



This will download the agent installer, save it to the temp folder, and silently install the agent by specifying the Wazuh manager and registration server:



Figure 85 – Wazuh Agent Installation

12. Once the script has completed the download and installation, you can start the agent by running the following command:

NET START WazuhSvc

It's important to note that you may need administrator privileges to run the NET\_START command and start the Wazuh agent service. If you encounter any permission-related issues, make sure you are running the command with the necessary privileges.

After starting the Wazuh agent service, it will continue to run in the background, performing its security monitoring tasks until it is manually stopped or the system is shut down:



Figure 86 – Wazuh Agent Creation Final Details

By running the NET START WazuhSvc command, you are essentially activating the Wazuh agent on the Windows system, enabling it to perform its security monitoring functions and contribute to the overall security visibility provided by the Wazuh system:



Figure 87 – Run Wazuh Agent

13. Then verify the installation within the Wazuh dashboard:

	wazuh. 🗸 🔤								
	STATUS Active (1)			DETAILS					
(	Osconrector()()     Perding #0     Never cossecter()()	Active 1 Lost registered spent DESKTOP-OR6U96L	Date that bat	0 Most actin DESKT	Never connected 0 0P-0R6U96L	agarith constaige 100.00%			
Agents									
		IP address		Operating system					
				🔲 Nicrosoft Windows I					



- 14. Now, let us move to testing and validation. Generate security events on the agent VM (e.g., create and delete files in critical directories).
- 15. Validate that the events are detected by the agent and reported to the manager.

16. Monitor alerts and analyze the data collected by Wazuh:

= C waruh y	Comment Cosstor Carues												
Security sector Integrity monitor													
n.	Materia B active (2)	th a firms, the rescure	Merian Merian vel 23	Droops Official		Demaing tydare Microsoft Withdows ID Pro 16 (23)	Civilies receiv recard)		ngistrationi data av 22. oktor gy 19130	0/289	t ort torop after Jan 22, 2024 (p. 1	125.08.000	
MITRE													
Tep Teolioi			<ul> <li>22563)</li> <li>22563</li></ul>										
Events count evolution					SCA Lastes	A Scans L Windows 10 Enterprise Dem		12,075,000204					
-													
1- 													
t na n													

Figure 89 – Wazuh Agent Monitor Dashboard

17. Configure active response in Wazuh to automatically take action in response to certain triggers:

= 🛆 wazuh. 🗸 Mate	DESITOPONE.	ATRE ATTACK (S						
Intelligence Framework Dashboard								
<b>R</b> I ≪ - Seven								
naragerrane wasin-sturb/204-ivm interview.id								
wassh-alerte-* ~								
R Search Reld Names								
The by type     Submetant     If note the function     If note the function     If note the function     If note the function     If note the function								
Available failing	time -	atoritai		rate and the baseline	a de description	10.00	rum in	
it agentid								
It agent / a me	JUE 27, 2024 0	10.04129.000 11.042.001		seronas evacaan	augus agoit ctoppos.			
<ol> <li>data estra data</li> </ol>								
t dendernere								
(f) decodes parent	table pon							
it fulling								
(1) M		ecent.td #						
(K) input type								
( location		agent mare 11						
t managername								
👔 rule, fracheren		dender om						
it ningip								
r rule.gog13								
i urjerštorba			ees: Agent stapped: "BibKTOP-0					
<ol> <li>role higher</li> </ol>								
2 nie nal			06430548.1337					
<ol> <li>Receive a factorization</li> </ol>								
<ul> <li>Nucleist, 500, 55</li> <li>nucleist, 500, 55</li> </ul>		Institut at	m its constant					
Contractory of the second								
L Harves	1	monager.nomo	zuh-sbuntszztk-kon					

Figure 90 – Wazuh Event Triggers

18. Generate and review reports through the Wazuh:



Figure 91 – Wazuh Event Report Creation

Both labs emphasize the importance of performing operations within a controlled environment, understanding configuration and output, and ensuring that the system's detection and response capabilities are functioning as expected. Additionally, these labs facilitate familiarity with real-time incident response scenarios and threat hunting practices.

By combining malware prevention, advanced threat analytics, and unified visibility, endpoint protection delivers in-depth security for devices that often represent a prime attack vector for infiltrating enterprise networks.

# Identity and access management (IAM) tools

Let us look at the exercise.

## Exercise: Setting Up and Configuring Keycloak for IAM

IAM encompasses tools and processes for ensuring that the right individuals have access to the appropriate resources for the right reasons. Here, I will outline an exercise that utilizes Keycloak, a popular open-source IAM solution. Packt has a book detailing Keycloak in detail called *Keycloak - Identity and Access Management for Modern Applications*, consider picking it up and turning the exercise into a lab and if you want to work more with Keycloak.

Keycloak is an open-source **identity and access management** (**IAM**) solution that provides authentication, authorization, and **single sign-on** (**SSO**) capabilities for modern applications and services. Developed by Red Hat, Keycloak offers a comprehensive and flexible platform for securing and managing user identities across diverse environments, including on-premises, cloud, and hybrid infrastructures. With its rich set of features, such as user federation, RBAC, and support for various identity protocols (OAuth 2.0, OpenID Connect, SAML), Keycloak simplifies the implementation of secure and scalable authentication and authorization mechanisms. It provides a centralized user management system, allowing administrators to create, manage, and authenticate users across multiple applications and services. Keycloak's extensible architecture and customization options make it adaptable to different security requirements and integration scenarios. Whether you are building a single application or a complex microservices architecture, Keycloak empowers developers and administrators to focus on their core business logic while relying on a robust and secure identity management solution.



Figure 92 – Keycloak Website

The prerequisites are:

- A virtualization platform such as VMware, VirtualBox, or a cloud service capable of hosting VMs.
- A VM with at least 2 GB RAM and 2 CPU cores.
- A supported operating system installed on the VM, such as Ubuntu Server.
- Internet access for downloading software packages.

Let us look at the steps:

- 1. Prepare a VM with the chosen operating system, following best practices for setting up a secure VM environment.
- 2. Ensure the VM is connected to the network with proper firewall rules to allow HTTP/HTTPS traffic.
- 3. Download and install Java JDK which is a prerequisite for Keycloak. For Ubuntu, use:

### sudo apt install default-jdk

- Download Keycloak from the official website, <u>https://www.keycloak.org/</u>, using wget or curl.
- Unzip the Keycloak archive to an appropriate location, for example, /opt/keycloak.
- 6. Navigate to the Keycloak bin directory and run the standalone script with ./standalone.sh to start the server.
- Access the Keycloak admin console via a web browser at http://[VM\_IP]:8080/auth/.
- 8. Complete the initial setup by creating an admin account.
- Once logged in, create a new realm by clicking on Add realm. Give it a meaningful name that represents your organization or project.

- 10. Within the realm, configure necessary tokens, session settings, and other realmspecific settings.
- Navigate to the Users section and add users manually or by importing a user list.
- 12. Assign credentials to users and manage their roles and group memberships.
- 13. In the **Clients** section, register a new client (application) that will be secured by Keycloak.
- 14. Configure the client with correct protocol (e.g., OpenID Connect), access type, and valid redirect URIs.
- 15. Define roles under the **Roles** section that will be used to grant access to resources.
- 16. Create groups under the **Groups** section and map them to the roles.
- 17. Under the **Authorization** section within clients, set up resource-based policies, permission scopes, and access policies.
- 18. Use Keycloak's built-in tools to test user authentication and token generation.
- 19. Verify that users can log in and are granted access according to their roles and group memberships.
- 20. Configure Keycloak to act as an **identity provider** (**IdP**) by setting up identity brokering with external providers (if needed).
- 21. Configure Keycloak to act as a **service provider** (**SP**) by integrating with external IdP services (if needed).
- 22. Install Keycloak adapters on applications that should be secured by Keycloak for **single sign-on** (**SSO**) capability.
- 23. Examine the logs for any authentication or authorization issues.
- 24. Set up audit logging to track user sessions and operations.

- 25. Create a backup of the Keycloak database and the configuration files.
- 26. Document a recovery process in case of failure.
- 27. Monitor Keycloak's performance and make necessary adjustments to **Java** Virtual Machine (JVM) settings or database configurations.
- 28. Document the entire setup process, configurations made, and policies implemented.
- 29. Include diagrams and flowcharts that visualize the authentication and authorization flows.

By following these steps, you will set up a working IAM environment using Keycloak that can manage users, authenticate and authorize client applications, and integrate with other IdP services if necessary. The lab's ultimate goal is to provide hands-on experience with IAM best practices, tools, and configurations in a controlled, virtualized setting.

By centralizing identity, access, and privileges, IAM limits the attack surface and enforces least privilege, providing accountability and auditability for access.

# Data protection tools

Let us look at the lab.

For the purpose of this lab, we will focus on encryption using VeraCrypt, an open-source disk encryption software.

## Lab: Data Encryption with VeraCrypt

VeraCrypt is a powerful open-source disk encryption software that provides a high level of security for protecting sensitive data on your computer. It is a fork of the discontinued TrueCrypt project and builds upon its strong foundation while adding enhanced security features and addressing known vulnerabilities. VeraCrypt allows you to create encrypted volumes or containers, which can be mounted as virtual disks, and encrypt entire partitions or storage devices, such as hard drives or USB drives. With VeraCrypt, you can safeguard your confidential files, documents, and personal information from unauthorized access, theft, or data breaches. It supports various encryption algorithms, including AES, Twofish, and Serpent, and offers multiple cascading encryption modes for added security. VeraCrypt also provides plausible deniability through hidden volumes, allowing you to create a decoy system within an encrypted volume to further protect your sensitive data. Whether you are an individual, business, or organization dealing with confidential information, VeraCrypt is a reliable and user-friendly solution for ensuring the privacy and integrity of your digital assets.

e Source Code Downlo	ads Documentation Donate Forums			
anch	Commit message	Author	Age	
wSysEncWizard	Windows: fix buffer overrun caused by wrong use of wmemset	Mounir IDRASSI		
EncWizardPR957	New sys enc wizard (#957)			
	Documentation: Remove Flattr as donation platform since it is shutting down			
	Download	Author	Age	
aCrypt_1.26.7	VeraCrypt_1.26.7.tar.gz_VeraCrypt_1.26.7.zip			
aCrypt_1.26.6	VeraCrypt_1.26.6.tar.gz_VeraCrypt_1.26.6.zip			
aCrypt_1.25.9	VeraCrypt_1.25.9.tar.gz_VeraCrypt_1.25.9.zip			
aCrypt_1.25.7	VeraCrypt_1.25.7.tar.gz_VeraCrypt_1.25.7.zip	Mounir IDPASSI		
aCrypt_1.25.4	VeraCrypt_1.25.4.tar.gz_VeraCrypt_1.25.4.2lp	Mounir IDRASSI		
aCrypt_1.24 Update8_MatO5X	VeraCrypt_1.24-Update8_MacOSX.tar.gz_VeraCrypt_1.24-Update8_MacOSX.zip	Mounir IDRASSI		
acrypt_1.24-Update7	VeraCrypt_1.24-Update7.tar.gz_VeraCrypt_1.24-Update7.zip	Mounir IDRASSI		
aCrypt_1.24-Update6	VeraCrypt 1.24-Update6.tar.gz VeraCrypt 1.24-Update6.zip	Mounir IDRASSI		
aCrypt_1.24-Update5	VeraCrypt 1.24-Update5.tar.gz VeraCrypt 1.24-Update5.zip	Mounir IDRASSI		
acrypt_1.24-update4	veracrypt_1.24-update4.tar.gz_veracrypt_1.24-update4.zip	Mounir IDRASSI		
	Commit message	Author	Files	lines
tours	Documentation: Remove Flattr as donation platform since it is shutting down HEAD [master]	Mounir IDRASSI		
	Documentation: Mention that TRIM is not supported on macOS	Mounir IDRASSI		
	Documentation: Add more information about TRIM behavior in VeraCrypt	Mounir IDRASSI		
945	Documentation: Update bank account details for USD donations	Mounir IDRASSI		
av5	02Nov23-Update Language.es.xml (#1241)			
iys	Documentation: Mention default PIM values when no PIM is specified	Mounir IDRASSI		
	Linux: Focus PIM field when selected (#1239)			
ays	Update Language.ro.xml (#1237)			
	Documentation: Update supported macOSX versions to remove Big Sur and add Sonoma			
	Update Language.7h-cn.xml (#1233)			
ne				
s://github.com/veracrypt/VeraCryp	tgit			
neithalt code of notice burger anticed				

Figure 93 – Veracrypt Website

The prerequisites are:

- A virtualization platform like VirtualBox, VMware, or similar, where VMs can be created.
- A VM with a Windows or Linux operating system installed.
- Internet access for downloading VeraCrypt.
- Basic knowledge of disk encryption and file systems.

Let us look at the steps:

- 1. Create a new VM using your virtualization software.
- 2. Install your chosen operating system on the VM.
- 3. Within the VM, download VeraCrypt from the official website, https://www.veracrypt.fr/code/VeraCrypt/.

4. On Windows, run the installer and follow the on-screen instructions:



Figure 94 – Veracrypt Download

5. On Linux, extract the downloaded package and run the installation script.

This lab provides instructions for creating, mounting, and using a VeraCrypt volume stored in a file container. It is recommended to read other sections of the VeraCrypt manual for important additional information.

 Download and install VeraCrypt if you have not already. Launch VeraCrypt by double-clicking VeraCrypt.exe or the Start menu shortcut.

Open File	- Security War	ning	×
Do you	want to run tl	nis file?	
-	Name:	rs\secdoc\Downloads\VeraCrypt_Setup_x64_1.26.7.ms	i
	Publisher:	IDRIX SARL	
	Туре:	Windows Installer Package	
	From:	C:\Users\secdoc\Downloads\VeraCrypt_Setup_x64_1.26	
		Run Cancel	
🗹 Alwa	iys ask before o	pening this file	
1	While files fr harm your co <u>What's the ri</u>	om the Internet can be useful, this file type can potential omputer. Only run software from publishers you trust. <u>sk?</u>	У

## (a)



Figure 95 – Installing Veracrypt Windows Installer

7. In the main VeraCrypt window, click **Create Volume** to open the Volume Creation Wizard:

vç	VeraCr	vpt						_		Х
Vo	lumes	System	Favorites	Tools	Settings	Help			Homepa	ge
	Drive A: B: F: G: H: I: J: K: L: M:	Volume				Size	Encryption Algorithm	Туре		*
	C	reate Volun	ne		Volume	Propert	ies	Wipe (	ache	
	Volume VeraCry	pt ☑ Ne	ver save his	tory		V	✓	Select Select De	File	
	м	lount	A	uto-Moun	t Devices		Dismount All		Exit	

Figure 96 – Veracrypt Dialog Window

8. In the Wizard, choose **Create an encrypted file container** as the volume type. Click **Next**:



Figure 97 – Veracrypt Volume Creation Wizard

9. Select Standard VeraCrypt volume as the volume format and click Next:



Figure 98 – Veracrypt Volume Type

10. Click **Select File** to choose where to create the VeraCrypt container file:



Figure 99 – Veracrypt Volume Location

11. Browse to the desired folder (e.g. F:\Data) and enter a filename for the container (e.g. MyVolume.hc). Click **Save** to return to the Wizard:

veracrypt volume creation	1 Wizard	_	~		
Specify Path and File Na	ime				
← → • ↑ 🗄 → 11	his PC > Documents >				
Organize 👻 New fold	ler				E 🕶 😮
<u>^</u>	Name	Date modified	Туре	Size	
📌 Quick access	PsGetsid.exe	3/30/2023 5:57 PM	Application	404 KB	
💻 Desktop 🛛 🖈	PsGetsid64.exe	3/30/2023 5:57 PM	Application	495 KB	
🕂 Downloads 🖈	Psinfo.exe	3/30/2023 5:57 PM	Application	433 KB	
🔮 Documents 🖈	PsInfo64.exe	3/30/2023 5:57 PM	Application	524 KB	
Networks 🖉	💶 pskill.exe	3/30/2023 5:57 PM	Application	382 KB	
DFIR-06-L3	skill64.exe	3/30/2023 5:57 PM	Application	466 KB	
Log Parser 2.2	💶 pslist.exe	3/30/2023 5:58 PM	Application	213 KB	
NIS02	💶 pslist64.exe	3/30/2023 5:58 PM	Application	261 KB	
	PsLoggedon.exe	6/28/2016 12:51 PM	Application	149 KB	
NS-04-L3	PsLoggedon64.exe	6/28/2016 12:49 PM	Application	167 KB	
💻 This PC	psloglist.exe	3/30/2023 5:58 PM	Application	306 KB	
a 3D Objects	📧 psloglist64.exe	3/30/2023 5:58 PM	Application	370 KB	
Desktop	📧 pspasswd.exe	3/30/2023 5:58 PM	Application		
Documente	📧 pspasswd64.exe	3/30/2023 5:58 PM	Application	265 KB	
Developed	📧 psping.exe	3/30/2023 5:57 PM	Application	281 KB	
Downloads	📧 psping64.exe	3/30/2023 5:57 PM	Application	339 KB	
J Music	PsService.exe	3/30/2023 5:58 PM	Application	262 KB	
Pictures	PsService64.exe	3/30/2023 5:58 PM	Application	315 KB	
Videos	psshutdown.exe	3/30/2023 5:57 PM	Application	675 KB	
🏪 Local Disk (C:) 🛛 🗸	psshutdown64.exe	3/30/2023 5:57 PM	Application	791 KB	
File name: Supe	r secret encrypted container				
Save at type: All E	ler (* *)				
Save as type: All FI	ies(,)				

#### Figure 100 – Veracrypt Volume Location Selection

12. Click **Next** to continue in the Wizard:



Figure 101 – Veracrypt Volume Location Wizard

13. Keep the default encryption and hash algorithms or choose your own preferences. Click **Next**:



Figure 102 – Veracrypt Wizard Encryption Options

14. Enter the desired size of the container (e.g. 250 MB). Click Next:



Figure 103 – Veracrypt Volume Size

15. Choose a secure password and enter it twice to continue:



Figure 104 – Veracrypt Volume Password

- 16. Move your mouse randomly within the Wizard for 30+ seconds to generate encryption keys.
- 17. Click **Format** to create the container file. Click **OK** when done and **Exit** to exit:

🐱 VeraCrypt	×	
VeraCrypt Volume Creation Wizard	_	
	Volume Format	
	Options Filesystem NTFS  Cluster Default  Full Format Dynamic	~
• <mark>//</mark> •	Random Pool: .*-,/,*+*+*,-/,*-//*-*-++,+/+ Header Key: ************************************	
	Abort	t
A LONG TO THE ATTACK	Done Speed Left	
VeraCrypt	IMPORTANT: Move your mouse as randomly as possible within this window longer you move it, the better. This significantly increases the cryptograph of the encryption keys. Then click Format to create the volume. Randomness Collected From Mouse Movements	. The nic strength
	Help < Back Format	Cancel

Figure 105 – Veracrypt Volume Format

- 18. In the main VeraCrypt window, choose a drive letter to mount the container.
- 19. Click **Select File** and browse to the container file created earlier. Click **Open**.
- 20. Click **Mount** and enter the container password. Click **OK**:

2	VeraC	rypt						_		×
٧	olumes	System	Favorites	Tools	Setting	s Help			Homep	oage
	Drive	Volume				Size	Encryption Algorithm	Туре		^
	A:	\super_s	ecret_encry	oted_con	itainer	499 MiB	AES(Twofish(Serpent)	) Normal		
	<u>В</u> :									
	E:									
	- G:									
	H:									
	):									
	K:									
	M:									
										•
		<u>C</u> reate Volun	ne		<u>V</u> olun	ne Propert	es	<u>W</u> ipe (	Cache	
	Volume	·								
		<b>C:/</b> U	sers\secdoc\	Documer	nts\super	_secret_e	ncrypted_contai ~	Select	<u>F</u> ile	
T	VeraC	ypt <u>N</u> e	ver save his	tory		N	olume <u>T</u> ools	Select D	evice	
		<u>D</u> ismount	A	uto-Mour	nt Device:	s	Di <u>s</u> mount All		E <u>x</u> it	

Figure 106 – Veracrypt Volume Status Window

- 21. The container is now mounted as an encrypted virtual disk. To close, click **Dismount** in VeraCrypt.
- 22. Now, let's move ahead to understanding VeraCrypt. Open VeraCrypt and familiarize yourself with the user interface.
- 23. Review the documentation to understand concepts like volumes, mount points, and encryption algorithms.
- 24. Now, onto creating an encrypted volume. Once mounted, the encrypted volume behaves like any other drive. Store sensitive files inside this volume. When unmounted, the files are secured with the chosen encryption.

- 25. To secure the data, dismount the volume in VeraCrypt. Verify that the volume is inaccessible without mounting it again with the correct password.
- 26. Copy the encrypted volume file to another secure location as a backup. Document the volume details, password, and keyfile locations for recovery purposes.
- 27. Understand the importance of strong passwords, backup strategies, and the implications of encryption on system performance.
- 28. Explore other VeraCrypt features such as hidden volumes, system encryption, and creating a VeraCrypt Rescue Disk.
- 29. Test the performance of your system with the encrypted volume mounted.
- 30. Practice recovery scenarios, including mounting the volume on a different system or VM.
- 31. Document the process, configuration choices, and any issues encountered.
- 32. Prepare a guide for end-users on how to access and use the encrypted volume.

Through this lab, participants will acquire practical skills in using encryption as a data protection tool, understanding the balance between security and usability, and the importance of comprehensive documentation and user education. This hands-on experience is vital for cybersecurity professionals tasked with safeguarding sensitive information.

Given growing data volumes and increasingly sophisticated threats, architects must integrate robust controls for data discovery, access, transmission, encryption, and analytics. Doing so limits exposure while enabling data utility across infrastructure.

# Vulnerability management tools

Vulnerability management is a critical component in the cybersecurity domain, focusing on the identification, classification, remediation, and mitigation of various software vulnerabilities. One of the prominent open-source tools in this arena is OpenVAS (Open Vulnerability Assessment System). This lab will guide you through setting up and using OpenVAS within a virtual environment.

### Lab: Vulnerability Scanning with OpenVAS

**OpenVAS** (**Open Vulnerability Assessment System**) is a powerful open-source vulnerability scanning and management framework that helps organizations identify and assess security vulnerabilities in their networks, systems, and applications. It is a widely used tool for performing comprehensive vulnerability scans and generating detailed reports to aid in the remediation process. OpenVAS consists of a scanner, a manager, and a web-based user interface, providing a centralized platform for managing and executing vulnerability scans. With its extensive database of **network vulnerability tests** (**NVTs**), OpenVAS can detect a wide range of security issues, including missing patches, misconfigurations, and known vulnerabilities. It supports various scan types, such as authenticated and unauthenticated scans, and can be customized to fit specific security requirements. OpenVAS integrates with other security tools and frameworks, allowing for seamless integration into existing security workflows. Its regular updates and active community support ensure that OpenVAS stays up-to-date with the latest vulnerability information, making it an essential tool for proactively identifying and mitigating security risks in today's dynamic threat landscape.

Greenbone OpenVA	s		Ŏ						
Gr	eenhone Open\/AS								
51	eenbolie openvA3								
Open level in type o The s	OpenVAS in a full-featured whereability scanner. Its capabilities include unaufterificated and authenticated leasing, various high level and pow- level intermet and hidustrial protocols, performance turing for large-scale scans and a powerful internal programming language to implement any type of varianzability text. The scanner dottains the tots for detecting varianzabilities from a feed that has a long history and daily updates.								
Open produ	OpenVAS has been developed and driven forward by the company Greenbore since 2006. As part of the commercial vulnesability management product family Greenborne Enleryrise Appliance, the scanner forms the Greenborne Community Edition together with other open-source modules.								
Road									
Re	lated Links								
	Products	Test Now	Product Documentation						
		<b>٦</b> :ً٢ <>>							
	Security Response Team	Source Code	Community Forum						
Co	ntact								
• We	sbsite Greenbone:								



You can access this here: https://openvas.org/.

The prerequisites include:

- A virtualization solution such as VirtualBox, VMware, or a cloud-based platform capable of deploying virtual machines.
- A VM with at least 4 GB RAM and 2 CPU cores.
- A supported Linux distribution installed on the VM, such as Kali Linux, which comes with OpenVAS pre-installed. Understand the while Kali comes with OpenVAS installed it is not the version maintained by OpenVAS and there are known issues with the installation in Kali.
- Internet access for updates and downloading plugins.

Let us look at the steps:

 Set up a new VM on your virtualization platform with your chosen Linux distribution. The documentation at the end of this bullet provides instructions for installing Greenbone Community Edition from the native Kali Linux repository. The Greenbone install packages are maintained by Offensive Security. Any issues found during installation or usage should be reported through the Kali Linux Bug Tracker, following the guidelines for submitting Kali bugs. If you would like to install OpenVAS on another Linux Distro, you can follow the guide at the following OPenVAS link:

https://greenbone.github.io/docs/latest/22.4/container/index.html.

2. Configure the network settings for the VM to ensure it can reach the internet and the internal network for scanning purposes. Before installing Greenbone Community Edition, first update the local package lists for all configured repositories and **personal package archives** (**PPAs**) on your Kali Linux system. As a rolling release distribution, Kali continuously updates system software to the latest versions without requiring OS reinstallation. Rolling releases typically provide new software soon after release. It is highly recommended to also perform a full package upgrade beforehand since Greenbone requires the newest PostgreSQL version. Upgrading proactively avoids potential issues configuring PostgreSQL later in the installation process.

See the troubleshooting section if having problems with the PostgreSQL upgrade or configuration while installing Greenbone.

For distros that do not come with OpenVAS, install it via the package manager.
 For example, on Debian-based systems: sudo apt-get install
 openvas:



Figure 108 – OpenVAS Installation on Kali

On Kali Linux, OpenVAS (now known as GVM) can be set up by running sudo gvm-setup.

4. Run the setup script if necessary, which will download the latest vulnerability feeds and configure the various components of OpenVAS:



Figure 109 – OpenVAS Setup

## Note

There is a known error with some of the installation modules and separate installation of those modules may be required. Such as the installation of the pg-gvm module. To correct run the following commands: sudo apt install postgresql-16-pg-gvm and sudo runuser -u postgres -- /user/share/gvm/create-postgresql-database.

5. After running the setup script run sudo gvm-check-setup for validation of the installation and default configuration:



Figure 110 – OpenVAS Setup Validation and initial password

### Note

Take note of the admin user generated password on completion of a successful setup. This is a randomly generated key at first installation.

6. The Kali Linux installation of Greenbone uses the same components and configuration options as compiling the source code directly. Here are some common customizations:

First, let us look at enabling remote web interface access.

By default, Greenbone is configured for local-only access to the web interface on 127.0.0.1. To allow external access, edit /usr/lib/systemd/system/gsad.service and update the -listen argument:

```
-ExecStart=/usr/local/sbin/gsad --foreground --
listen=127.0.0.1 --port=9392
```

```
+ExecStart=/usr/local/sbin/gsad --foreground --
listen=0.0.0.0 --port=443
```

This opens the web interface on all interfaces. Optionally change the port to 443 for default HTTPS:



Figure 111 – OpenVAS Listening IP and Port Configuration

7. On Kali, ensure all services related to GVM are started with sudo gvmstart:



Figure 112 – Starting OpenVAS

- 8. By default, OpenVAS serves its web interface on port <u>9392</u>. Access this via a web browser by navigating to <u>https://[VM\_IP]:9392</u>.
- 9. Now, let us look at customizing your Greenbone Community Edition installation. The Kali Linux installation of Greenbone uses the same components and configuration options as compiling the source code directly. Here are some common customizations:

Let us enable remote web interface access.

By default, Greenbone is configured for local-only access to the web interface on 127.0.0.1. To allow external access, edit /usr/lib/systemd/service/gsad.service and update the -listen argument:

```
-ExecStart=/usr/local/sbin/gsad --foreground --
listen=127.0.0.1 --port=9392
+ExecStart=/usr/local/sbin/gsad --foreground --
listen=0.0.0.0 --port=443
```

10. This opens the web interface on all interfaces. Optionally change the port to 443 for default HTTPS:



Figure 113 – OpenVAS Dashboard using LAN Interface

11. Login using the credentials set up during the installation or the default provided by the system:

۲	-		Greenbone Security Assistant — Mozilla Firefox			8
۲						
÷	⇒ c ≙ ⊂	🗛 🕶 https://12	7.0.0.1:9392/login	습		
-91	nport bookmarks 🛸 Kali Linux	👩 Kali Tools 🛛 💆 K	ali Docs 🚿 Kali Forums 🛷 Kali NetHunter 🛸 Exploit-DB 🛸 Google H			
			Cusanhana			1
			S ureenbone			
			-			
			Sign in to your account			
			Usemame			
			admin			
			Password			
			Sign In			
			•			
			Community			
14						
			EDITION			
			And the second			

Figure 114 – OpenVAS Login

12. Prior to running initial scans, Greenbone parses vulnerability feed data into the gvmd PostgreSQL database. Without populated vulnerability data, scans cannot initialize or complete without errors. The feed population process begins during Greenbone setup but commonly requires a few minutes to multiple hours to finish based on system resources. The feed status can be monitored on the **Feed Status** page which is located under the **Configuration** menu section. Scanning should not be started until the feeds show as synchronized and finished updating:



Figure 115 – OpenVAS Dashboard

13. In the web interface, go to the **Scanners** section to ensure your scanner is properly set up:



Figure 116 – Selecting Scanner Configuration

14. Navigate to **Configuration** and then **Targets** to define the IP range or specific hosts you wish to scan:

٠		Greenbone	Security Assistant - Targets	— Mozilla Firefox				(	
i 🍪 Greenbone Security Assis									
$\leftarrow$ $\rightarrow$ C $\textcircled{a}$	○ 🖧 https://127.0	<b>).0.1</b> :9392/targets				☆		ර (	> ≡
🕣 Import bookmarks 🔌 Kali Lir	nux p Kali Tools 🧧	Kali Docs 🥆 Kali Foi	rums 🛛 🤜 Kali NetHunte	r 🔌 Exploit-DB	📤 Google Hacking DB  🦚	OffSec			
Greenbone Security Assistant									8
@[*			Filter			\$X00Z			T
Targets 0 of 0	New Target					×			
	Name	Network							
No targets available	Comment								
(Applied filter: sort=name first=1 rows=10)	Hosts	<ul> <li>Manual</li> <li>From file Browse</li> </ul>							
	Exclude Hosts	Clude Hosts     From file Browse No file selected.							
	Allow simultaneous scanning via multiple IPs	💿 Yes 🔘 No							
	Port List	All IANA assigned TCF	▼ [*						
	Alive Test	Scan Config Default	¥						
	Credentials for aut	henticated checks							
	SSH		▼ on port 22	C*					
	CMR		<b>↓</b> □ <b>★</b>						
	Cancel					Save			
				Gree	nbone Security Assistant (GSA) Cop	pyright (C) 2009-2023 by Gree	nbone AG	, www.gre	enbone.net

## Figure 117 – Defining Targets

- 15. Go to **Scans** and then **Tasks** to create a new task.
- 16. Assign a name, select the target previously created, and select the scanning configuration (there are several default configurations available):

单 📣 Greenbone Security Assis 🔅	× 🤞 Greenbone S	ecurity Assist ×	÷						~
< → C ŵ	🔿 🔒 https://192.1	168.2.173/tasks				☆		ම එ	🧈 =
🕣 Import bookmarks 🛸 Kali Linu	ix 🚓 Kali Tools 🧧	Kali Docs 👘 Kali F	orums 🛛 🕂 Kali Netl	lunter 🔌 Exploit-DB	🔦 Google Hacking DB				
Greenbone Security Assistant									گ
Dashboards Scan									
@≮₫			Filter			( )	KOØE -		Ŧ
Tasks 0 of 0	New Task					×			Ŀю
Tasks by Severity Cla	Name Comment	Unnamed					atus (Total: 0)		×
	Scan Targets Alerts		•	]C  C					
	Schedule Add results to		V 🗌 Ono	• 🗆 *					
	Assets Apply Overrides Min Coll	Yes O No							
No Tasks available	Alterable Task	Ves O No	ally delete concrts						
(Applied filter: apply_overrides=0 min_god=7)	Reports	<ul> <li>Automatically de</li> </ul>	lete oldest reports but a	always keep newest 5	reports	1			
	Scanner	OpenVAS Default	•						
	Scan Config	Full and fast	•						
	Cancel					Save			
				Gree	enbone Security Assistant (GSA)	Copyright (C) 200	9-2023 by Greenbo	te AG, www	k greenbone net

Figure 118 – Defining Tasks

17. Start the scan task and monitor its progress:
| ← → ♂ @ ○ A https://192.168.2   | 173/tasks              |                          |                               | ជ                              | ල එ 🚽 ≡                      |
|---|------------------------|--------------------------|-------------------------------|--------------------------------|------------------------------|
| 🕣 Import bookmarks 🏷 Kali Linux  🏫 Kali Tools 🛚 🚊 Kali E                | ocs 🔨 Kali Forums  Kal | i NetHunter 🔺 Exploit-DB | 🖕 Google Hacking DB           |                                |                              |
| Security Assistant  |                        |                          |                               |                                | සි                           |
| Dashboards Scans Assets   | Resilience             | SecInfo                  | Configuration                 | Administration                 | Help                         |
| @*C   | Filter                 |                          |                               | ¢X୦0ľ                          | •                            |
| Tasks 1 of 1  |                        |                          |                               |                                | Lt Q                         |
|   | - 1 - 51               |                          |                               |                                | 0.0                          |
| Tasks by Severity Class (Total: 1) ×                                    | Tasks with mos         | t High Results per Host  | ×                             | Tasks by Status (Total:        | 1) ×                         |
| N/A   |                        |                          |                               |                                | New                          |
|   | +                      | Results per Host         | _                             |                                |                              |
|   |                        | _                        |                               |                                |                              |
|   |                        |                          |                               |                                | <  <  1 - 1 of 1  >  >       |
| Name  wireless scan   | Status                 | Reports Last Report      |                               | Severity Trend                 | Actions                      |
|   |                        |                          |                               | Apply to page of               | ontents V Silline            |
| (Applied filter.apply_overrides=0 min_qod=70 sort=name first=1 rows=10) |                        |                          |                               |                                | <  <  1 - 1 of 1  >  >       |
|   |                        |                          |                               |                                |                              |
|   |                        |                          |                               |                                |                              |
|   |                        |                          |                               |                                |                              |
|   |                        |                          |                               |                                |                              |
|   |                        |                          |                               |                                |                              |
|   |                        | Gree                     | mbone Security Assistant (GSA | Copyright (C) 2009-2023 by Gre | enbone AG, www.greenbone.net |



Once the scan is complete, review the results for any identified vulnerabilities.

18. Analyze the reported vulnerabilities, reviewing the severity, description, and recommended actions:

< → C @	O 🔒 http	s:// <b>192.168.2.173</b> /res	ults			ជ	🛛 එ 🍦 =
Import bookmarks	🛰 Kali Linux 📪 Kali To	ools 🧧 Kali Docs 🔨	Kali Forums 🛛 🧟 Kali Net	Hunter 🛸 Exploit-DB 🔺 Go			
Greenbone Security Assiste	ant						සි
Dashboards	Scans	Assets	Resilience	Secinfo	Configuration	Administration	Help
0			Filter			¢X٥٥	
Results 71	of 72						Цэ
	Results by Severity (	Class (Total: 71)	×		Results by CVSS	(Total: 71)	×
			Log Low Medium	45- 50- 45- 45- 45- 45- 10- 10- 10- NIA Log 0.1	1 1 1 1 1 2 3 4 Seve	1 1 1 5 6 7 Ry	
Vulnerability			🛔 Severity 🗸	QoD Host	Name	Location	Created
DNS Cache Snooping Vuln	erability (UDP) - Active Ch	eck	5.0 (Medium)	70 % 192.168.40.116		53/udp	Sun, Jan 28, 2024 5:25 PM UTC
Cleartext Transmission of	Sensitive Information via F	HTTP	4.8 (Medium)	80 % 192.168.40.114		9123/tcp	Sun, Jan 28, 2024 5:21 PM UTC
TCP Timestamps Informati	ion Disclosure		2.6 (Low)	80 % 192.168.40.115		general/tcp	Sun, Jan 28, 2024 5:22 PM UTC
TCP Timestamps Informati	ion Disclosure		2.6 (Low)	80 % 192.168.40.116		general/tcp	Sun, Jan 28, 2024 5:25 PM UTC
Services			0.0 (Log)	80 % 192.168.40.116		5000/tcp	Sun, Jan 28, 2024 5:18 PM UTC
Services			0.0 (Log)	80 % 192.168.40.116		7000/tcp	Sun, Jan 28, 2024 5:18 PM UTC
				Greenbone Se	curity Assistant (GSA) Co	pyright (C) 2009-2023 b	50n/tan/28/2024/5/27/PM-ret

Figure 120 – Scan Results

19. Use the filtering tools to sort and prioritize the vulnerabilities.

20. Generate a report by going to **Reports** in the web interface:

🤞 🧳 Greenbone Security Assis × 🧳 Greenbone Security Ass	sis × 🤌 Greenbone Securi	ty Assist× +			~
← → C @ ○ A https://192.168.2.173/				ជ	ල රු 🍚 =
-Ə Import bookmarks 🤏 Kali Linux p Kali Tools 💆 Kali Docs	🔨 Kali Forums 🛛 🧟 Kali Netl	Hunter 🔺 Exploit-DB			
Security Assistant					පි
Dashboards Scans Assets	Resilience	SecInfo	Configuration	Administration	Help
◈▤⁺≡`≡₿®★®⋧ Ł⊳	Filter			¢X٥	?⊈▼
Repor Sun, Jan 28, 2024 5:16 PM t: UTC	Done ID: 59748554-ee15- a0d5-0e29d45b0	49b7- Cre 0e0 Cre	eated: Sun, Jan 28, 2024 5:16 PM	Modified: Sun, Jan J	28, 2024 7:25 PM Owner: admin
Information Results (29 of 262) (6 of 11) (5 of 17) (3 of 3)	Operating Systems C( (3 of 4) (5	/Es Closed CVEs	TLS Certificates Err	or Messages	User Tags
					1 - 29 of 29
Vulnerability	🛓 Severity 🔻	QoD Host	Namo	Location	Created
SSL/TLS: Report Vulnerable Cipher Suites for HTTPS		98 % 192.168.40.2	Hante	15000/tcp	Sun, Jan 28, 2024 7:07 PM UTC
SSL/TLS: Report Weak Cipher Suites	5.9 (Medium)	98 % 192.168.40.2		15000/tcp	Sun, Jan 28, 2024 7:07 PM UTC
SSL/TLS: Server Certificate / Certificate in Chain with RSA keys less than 2048 bits	5.3 (Medium)	80 % 192.168.40.2		15000/tcp	Sun, Jan 28, 2024 7:07 PM UTC
Missing 'HttpOnly' Cookie Attribute (HTTP)	5.0 (M <mark>edium)</mark>	70 % 192.168.40.2		443/tcp	Sun, Jan 28, 2024 7:09 PM UTC
Missing 'HttpOnly' Cookie Attribute (HTTP)	5.0 (Medium)	70 % 192.168.40.3		443/tcp	Sun, Jan 28, 2024 7:03 PM UTC
Missing 'Secure' Cookie Attribute (HTTP)	5.0 (Medium)	70 % 192.168.40.3		443/tcp	Sun, Jan 28, 2024 7:03 PM UTC
Missing 'HttpOnly' Cookie Attribute (HTTP)	5.0 (Medium)	70 % 192.168.40.4		443/tcp	Sun, Jan 28, 2024 7:05 PM UTC
Missing 'Secure' Cookie Attribute (HTTP)	5.0 (Medium)	70 % 192.168.40.4		443/tcp	Sun, Jan 28, 2024 7:05 PM UTC
Missing 'Secure' Cookie Attribute (HTTP)	5.0 (Medium)	70 % 192.168.40.2		443/tcp	Sun, Jan 28, 2024 7:09 PM UTC
DNS Cache Snooping Vulnerability (UDP) - Active Check	5.0 (Medium)	70 % 192.168.40.11	6	53/udp	Sun, Jan 28, 2024 5:25 PM UTC
Cleartext Transmission of Sensitive Information via HTTP	(2) 4.8 (Medium)	80 % 192.168.40.11	4	9123/tcp	Sun, Jan 28, 2024 5:21 PM UTC
Cleartext Transmission of Sensitive Information via HTTP	A 2 (Marlium)	80 % 192 168 40 <sup>Gree</sup>	enbone Security Assistant (GSA) Co	pyright (C) 2009-2023	by (Sunsijan: 28, 2024)7512-PM.net



- 21. Select the desired format (HTML, XML, CSV, etc.) and download the report for offline analysis or for sharing with stakeholders.
- 22. Address the reported vulnerabilities by applying patches, changing configurations, or implementing compensating controls.
- 23. Document the remediation steps and update your security posture documentation accordingly.
- 24. After remediation, re-run the scan to verify that the vulnerabilities have been resolved.
- 25. Set up a recurring scan schedule to regularly assess the security state of your targets.
- 26. Regularly update the OpenVAS vulnerability feed with sudo greenbonefeed-sync.

- 27. Keep the OpenVAS software updated via your Linux distribution's package manager.
- 28. Document your findings and the steps taken during the scan.
- 29. Refine your scanning process, target definitions, and remediation procedures based on lessons learned.
- 30. Some optional advanced configurations include exploring advanced configurations such as setting up multiple scanners or segmenting scan targets.
- 31. Ensure that the OpenVAS VM is secured with appropriate firewall rules, strong passwords, and access controls.
- 32. Consider the impact of scanning on network and host performance, scheduling scans during low-usage periods if necessary.

Through this lab, you will gain comprehensive hands-on experience with OpenVAS for vulnerability scanning, from installation and configuration to scanning, reporting, and remediation. This experience is crucial for cybersecurity professionals responsible for maintaining an organization's defensive posture against the ever-evolving threat landscape. By thoroughly scanning for vulnerabilities across the attack surface, architects gain visibility to proactively address risks before exploitation.

# Security configuration and patch management tools

Security configuration and patch management are vital practices within cybersecurity management to ensure systems are up-to-date and configured according to the best security policies. For the purpose of this lab, we will focus on using Ansible for Security Configuration Management and **Windows Server Update Services** (**WSUS**) for Patch Management within a virtual environment.

### Lab 1: Security Configuration Management using Ansible

Ansible is an open-source automation tool that simplifies the process of configuring, managing, and deploying systems and applications across various environments. It is an agentless platform that uses SSH or WinRM to communicate with target machines, making it lightweight and easy to set up. Ansible uses a simple, human-readable

language called YAML to define automation tasks, known as playbooks. These playbooks describe the desired state of the systems and the steps required to achieve that state, enabling consistent and repeatable deployments. With Ansible, you can automate a wide range of tasks, including configuration management, application deployment, orchestration, and provisioning. It provides a vast library of pre-built modules and plugins that allow you to interact with different systems, services, and tools, making it highly extensible and adaptable to diverse environments. Ansible's idempotent nature ensures that tasks are executed only when necessary, minimizing the risk of unintended changes. Its push-based architecture and parallel execution capabilities enable efficient management of large-scale infrastructures. Whether you are managing a handful of servers or a complex multi-tier application stack, Ansible empowers you to streamline your IT operations, reduce manual efforts, and improve the reliability and scalability of your systems.



Figure 122 – Ansible Website

You can access this at https://www.ansible.com/.

The prerequisites include:

• A virtualization platform like VirtualBox or VMware.

- A Control VM (Ansible Control Node) running a Linux distribution with Ansible installed.
- One or more Target VMs (managed nodes) that you wish to configure.
- Network connectivity between the control node and the managed nodes.

Let us look at the steps.

- Set up a Linux VM as the Ansible Control Node. Ansible is a powerful automation tool for managing multiple servers. Using Python and SSH, it can configure servers, routers, switches, and more from a central control node. This lab covers installing Ansible on Debian 12 **Bookworm** from the official repositories. First, update the system with the latest packages to enable installing Ansible. As a Debian stable release, Bookworm receives ongoing security updates but limited feature updates. Updating packages now ensures compatibility with the Ansible version available in the repos. With the system updated, we are ready to install Ansible and configure the control node. From this central management server, Ansible can then automate tasks across servers in the infrastructure through SSH.
- 2. Set up one or more Target VMs (Linux or Windows) that will be managed by Ansible.
- 3. Install Ansible on the Control Node using the package manager (for Ubuntu/Debian systems). After updating packages, install the Ansible package to set up the control node. This will install Ansible and all required dependencies on Debian 12. Additional packages may be needed in some use cases, but this covers the Ansible basics. With Ansible installed, the central management server can now automate tasks and configure infrastructure components including servers, routers, switches etc. through SSH connectivity:

```
sudo apt update && sudo apt upgrade -y
sudo apt install ansible
```

4. To verify Ansible installed correctly on Debian 12, check the version. This will print the Ansible version number along with Python and OpenSSL dependency versions. Reviewing the output confirms Ansible is present and accessible on the command line after installation completes:

#### ansible -version

5. To enable Ansible to connect to managed hosts, generate SSH keys on the Ansible control node and distribute the public key to each host. This creates public and private ssh key files on the Ansible server. Copy the public key to each managed host that Ansible will need to access, allowing passwordless SSH authentication between Ansible and managed nodes:

#### ssh-keygen

The server that will be managed through Ansible is:



#### Figure 123 – ifconfig for Target System

6. Copy the public key to the Target Nodes using (in the lab, I am using an Ubuntu 22.04 server as the managed client):

ssh-copy-id

7. To allow Ansible to run sudo commands on managed hosts without prompting for a password, configure passwordless sudo access for the sysops user (or whichever admin user Ansible utilizes) on each host:



## NOTE

Make sure to replace secdoc with the user you created or are using on the ansible system.

8. Create a project directory for Ansible automation called **ansible** and change into it:





### Figure 124 – Defining core settings

Here are the settings:

```
[defaults]
inventory = ./inventory
host_key_checking = false
remote_user = sysops
ask_pass = False
[privilege_escalation]
become=true
become_method=sudo
become_user=root
become_ask_pass=False
```

10. Then press CTRL+O to save the file and then CTRL+X to exit.

This specifies the inventory file location, disables host key checking, sets the default remote user, disables password prompting, and configures sudo privileges.

11. Finally, create an empty inventory file to define groups of managed hosts:

```
[prod]
[dev]
192.168.1.184
```

- 12. Then press CTRL+O to save the file and then CTRL+X to exit.
- 13. The ansible directory now contains ansible.cfg and inventory files to automate managed nodes.

- 14. To test connectivity from the Ansible control node to managed hosts, run the following ad-hoc ansible ping command, ansible all -m ping.
- 15. This performs a basic ping test to each defined host. Getting a successful ping response confirms Ansible can reach the managed nodes. With basic connectivity verified, we can create a sample playbook to install an Nginx server on a dev node.
- 16. To create the installation config, enter the following by editing in Nano using nano nginx.yml:

```
---
- name: Install NGINX Web Server
hosts: dev
tasks:
- name: install nginx package
ansible.builtin.apt:
    name: nginx
    state: prese
- name: Start nginx service
    service:
    name: nginx
    state: started
```

- 17. Then press CTRL+O to save the file and then CTRL+X to exit.
- 18. To execute the sample playbook:

ansible-playbook nginx.yml

- 19. This will install Nginx on the dev node based on the playbook instructions.
- 20. To verify Nginx was installed and started successfully:

ansible	dev	-m	shell	-a	'dpkg -l  d	grep -i	nginx'
ansible	dev	-m	shell	-a	'systemctl	status	nginx'

Getting the expected output confirms the playbook achieved the desired state configuration on the target managed host.

Ansible is now fully operational for patch management, deployment automation, and orchestrating infrastructure from this central control server. Playbooks can automate regular sysadmin tasks across many machines in just minutes!

- 21. Document the configurations applied, any issues encountered, and remediation steps.
- 22. Update the playbooks as security policies evolve.

Let us move on to the next lab.

### Lab 2: Patch Management with WSUS

WSUS (Windows Server Update Services) is a Microsoft tool that enables centralized management and distribution of updates and patches for Microsoft products, including Windows operating systems, Office applications, and other Microsoft software. It is designed to simplify the process of keeping systems up to date and secure within an organization's network. With WSUS, administrators can create a local repository of updates on a Windows server, which acts as a central point for managing and deploying updates to client computers. Instead of each client independently downloading updates from Microsoft's servers, they can retrieve them from the local WSUS server, reducing internet bandwidth usage and providing better control over the update process. Administrators can use WSUS to approve or decline specific updates, schedule update installations, and monitor the update status of client computers. WSUS integrates with Active Directory, allowing for the creation of computer groups and the application of different update policies based on organizational requirements. By using WSUS, organizations can ensure that their Microsoft systems are consistently patched, reducing the risk of vulnerabilities and maintaining a secure and stable computing environment.



Figure 125 – WSUS Website

You can access this at <a href="https://learn.microsoft.com/en-us/windows-server/administration/windows-server-update-services/get-started/windows-server-server-server-services/get-started/windows-server-server-server-server-server-services/get-started/windows-server-se

Because of the nature of WSUS and the need for explicit Windows infrastructure, this is an exercise to help you understand the steps needed to deploy patching services within a Windows-based infrastructure. As part of this, it is recommended to read and understand the first step in the deployment of WSUS and to make important decisions regarding the deployment. As such I have provided the Microsoft link to assist in the planning: <a href="https://leam.microsoft.com/en-us/windows-server/administration/windows-server-update-services/plan/plan-your-wsus-server/administration/windows-server-update-services/plan/plan-your-wsus-server/administration/windows-server-update-services/plan/plan-your-wsus-server/server-update-services/plan/plan-your-wsus-server/server-update-services/plan/plan-your-wsus-server-update-services/plan/plan-your-wsus-server/server-update-services/plan/plan-your-wsus-server-server-update-services/plan/plan-your-wsus-server-server-update-services/plan/plan-your-wsus-server-server-update-services/plan/plan-your-wsus-server

deployment.

The prerequisites include:

- A virtualization platform like VirtualBox or VMware.
- Windows infrastructure and a Windows Server VM to act as the WSUS server.
- Windows Client VM(s) to manage patches for.

Let us look at the steps:

1. Install Windows Server on a VM and configure it with a static IP address.

- 2. Add the WSUS role through the Server Manager interface.
- 3. Configure the WSUS according to your organizational requirements, such as choosing which updates to download, when to download them, and which machines to apply them to.
- 4. On the Windows Client VMs, set the Group Policy or registry settings to point to the WSUS server for updates.
- 5. In the WSUS Administration Console, approve updates for the relevant computer groups.
- 6. Ensure that client VMs are checking in with the WSUS server and downloading the approved updates.
- 7. Use the WSUS Administration Console to monitor update deployment and client status.
- 8. Generate reports to track update coverage and identify any issues with deployment.
- 9. If updates fail to install, use logs from both the WSUS server and client machines to troubleshoot the issue.
- 10. Regularly clean up the WSUS database and declined updates to maintain WSUS server performance.
- 11. Ensure communication between the WSUS server and clients is secured.
- 12. Regularly update the WSUS server itself to protect against vulnerabilities.
- 13. Document the WSUS configuration settings, update policies, and any troubleshooting steps.

Through this lab and exercise, participants will gain hands-on experience with automating security configurations using Ansible and managing patches in a Windows environment using WSUS. These processes help ensure consistent application of security policies and timely deployment of important security updates. Proactively hardening configurations and installing the latest patches blocks exploitation of known vulnerabilities. Architects must balance security with availability when planning change windows.

# Incident response and forensics tools

Incident response and digital forensics are pivotal components of cybersecurity, focusing on addressing and managing the aftermath of security breaches or attacks and performing detailed investigations to understand the breach and recover from it. For the purpose of this lab, we will use **The Sleuth Kit** (**TSK**) and Autopsy for digital forensics analysis, and Security Onion as an incident response platform, within a virtualized environment.

## Lab 1: Digital Forensics with The Sleuth Kit and Autopsy

Digital forensics is a critical field in today's digital age, and The Sleuth Kit (TSK) and Autopsy are two powerful open-source tools that have become essential in the forensic investigation of digital devices. The Sleuth Kit is a collection of command-line tools and libraries that allow investigators to analyze disk images and recover deleted files, while Autopsy is a graphical interface that sits on top of TSK, providing a user-friendly environment for conducting forensic investigations. Together, these tools enable forensic examiners to perform a wide range of tasks, including data recovery, file system analysis, timeline creation, and artifact examination. With support for various file systems and the ability to handle large volumes of data, TSK and Autopsy have become the go-to tools for digital forensics in law enforcement, corporate investigations, and incident response. Whether investigating a computer intrusion, analyzing digital evidence in a criminal case, or conducting internal investigations, TSK and Autopsy provide the necessary capabilities to uncover digital traces, reconstruct events, and gather crucial evidence to support the investigation process.



Figure 126 – The Sleuth Kit (TSK) and Autopsy Website

The prerequisites are:

- A virtualization platform like VirtualBox or VMware.
- A forensic workstation VM with a Linux OS or Security Onion which includes TSK and Autopsy.
- A disk image or a VM snapshot to investigate, simulating a suspect system.
- Network connectivity between your forensic workstation VM and other devices if remote analysis is required.

Let us look at the steps:

 Set up a VM to serve as your forensic workstation. This could be a Linux distribution with digital forensics tools installed or a specialized distro like Security Onion. In this lab I will be using the SANS SIFT Workstation as the system to install the tools. The SIFT Workstation is available as an OVA download or with specific installation instruction at the following SANS URL: https://www.sans.org/tools/sift-workstation/.

- 2. Obtain a disk image (e.g., E01, dd, aff) or VM snapshot for analysis. Ensure legal permission for analysis if required. In this example I will be using a Windows Server image (WinServer.dd).
- 3. On a Linux VM, install The Sleuth Kit using the package manager with sudo apt-get install sleuthkit:

	Terminal	Q = - 0 😣
	secdoc@slftworkstation	
	05: Ubuntu 20.04.0 LTS x80.04 Host: KVN/DENU (Standard PC (Q35 + ICH9, 2009) Kernel: 5.15.0-92-generic Uptime: secs Packapes: 2915 (dpkg), 11 (snap) shell: bask 5.0.17 Resolutions: 1920x1080 DE: CNOME Territani: gnome-territai CPU: AND Myren 9 S950X (4) 0 3.399GHz GPU: AND Myren 9	IN
secdocasiftworkstation: - S sudo apt install sleuthkit [sudo] password for secdoc: heading package lists Done suitaing dependency tree Reading state information Done iteuthkit is already the newest version (4 aleuthkit is already the newest version (4 aleuthkit is already the newest version (4 aleuthkit set to manually installed. The following packages were automatically girl.2-gaal.d librarint.2-todi libraugh linux-image-5.15.0-87-generic linux-modu Juse 'sudo apt autorenove' to renove then. D uggraded, 0 newly installed, 0 to renove secdocasiftworkstation: -	ORKSTATION .7.0-2ppa3=focal). Installed and are no longer required: plugini libamibi linux-headers-5.15.0-87-generic les-5.15.0-87-generic linux-nodules-extro-5.15.0- and 62 not upgraded.	linux-hwe-5.15-headers-5.15.0-87 d7-generic

### Figure 127 – Sleuthkit Install

Note that Sleuthkit is a cli/terminal only application.

 Install Autopsy by downloading the latest version from the official website, <u>https://www.sleuthkit.org/</u>, and following the installation instructions. Autopsy is installed on Windows:

C → C	Alexand X + O A https://www.auv/spery.ecom/dournico.ad/		0 \$	e 🧿 e
	DOWNLOAD ADD-ON	AUTOPSY	setemp-421.02-668.emi A four-sectored ket = 1.1 of 1.1 GB (133 MB/car) Show all downloads	×
	4.21.0 RELEASE FASTER SEARCH AND N	MALWARE SCANNING		
	Download Autopsy VERSION 4.21.0 FOR WINDOWS	Download	and Register	
	DOWNLOAD 64-BIT >	First Name	Last Name	
	DOWNLOAD FOR LINUX AND OS X Autopsy 4 will run on Linux and OS X. To do so:	Job Title		
	Download the Autopsy ZIP file	Organization		
	Follow the instructions to install other dependencies	Business Email*		
	3 <sup>rd</sup> Party Modules	Autopsy Download		
	3rd party add-on modules can be found in the Module github repository.	Please Select	~	
	From this repository, you can download all modules or just the ones that you want.	Country		
	Older Versions	Submit		
	You can find other versions of Autopsy at:			
	Autopsy 4.3.0 and earlier: Source Forge			
	Advanced			
	Six files are made available with each release:			
	<ul> <li>autopsy-X.X.X-32bit.msi: A 32-bit Windows installer.</li> </ul>			
	<ul> <li>autopsy-X.X. 64bit.msi: A 64-bit Windows installer.</li> <li>autopsy-X.X. debit.msi: A 64-bit Windows installer.</li> </ul>			

(a) Autopsy Download



(b) Autopsy Installation Wizard

No Autopsy Secup		$\times$
Ready to Install		
The Setup Wizard is ready to begin the Au	utopsy installation	2
Click "Install" to begin the installation. If y installation settings, click "Back". Click "Ca	you want to review or change any o ncel" to exit the wizard.	fyour
Advanced Installer	< Back	Cancel

(c) Autopsy Installation



Figure 128 – Autopsy Installation Completion

5. Open Autopsy and create a new case, providing all the necessary case details. It is important to note that you should run Autopsy as Administrator:

Do you want to allow this app from an unknown publisher to make changes to your device? autopsy64.exe Publisher: Unknown File origin: Hard drive on this computer Show more details Yes No	User Account Control		×
autopsy64.exe Publisher: Unknown File origin: Hard drive on this computer Show more details Yes No	Do you want to allow tl unknown publisher to r device?	his app from an make changes to your	
Publisher: Unknown File origin: Hard drive on this computer Show more details Yes No	autopsy64.exe		
Show more details Yes No	Publisher: Unknown File origin: Hard drive on this cor	nputer	
Yes No			
	Yes	No	

(a) UAC Initial Autopsy Start



Figure 129 – Autopsy Default Dashboard

6. Add a new host to the case and select the disk image or local drive to investigate. Follow the prompts to complete case creation:



# (a) Selecting New Case

😹 Autopry 421.0				— 🗆 🗙
Case View Tools Window Help				
Att Did Serve 🜆 Ingel Video 📓 Connurration 🦞 Beloaden	Timeline 📕 Bezoway	Generalis Report 📴 Cines Care	📾 🛛 🗢 - Expectition	Re Keyword Search
	3 New Case Information	×		
	Steps	Case Information		
	Certeinmen     Gytendintenden	Car Name Super Land Smoothy Justimet		

(b) Autopsy Case Default Location

eps	Optional Information
Case Information Optional Information	Case
	Number: 1337
	Examiner
	Name: Super Secret
	Phone: 123-456-7890
	Email: ss@supersecret.local
	Notes:
	Corganization
	Organization analysis is being done for: Not Specified V Manage Organizations
17/1	

# (c) Case Information

Steps	Select Host
Select Host     Select Data Source Type     Select Data Source     Configure Ingest     Add Data Source	Hosts are used to organize data sources and other data.

# Figure 130 – Selecting Host

7. If working with a live system, use TSK or another acquisition tool to create an image of the suspect system's disk:

Steps	Select Data Source Type	
Select Host     Select Data Source Type     Select Data Source     Configure Ingest	Disk Image or VM File	
5. Add Data Source	Local Disk	
	Logical Files	
	Unallocated Space Image File	
	Autopsy Logical Imager Results	
	XRY Text Export	

(a) Selecting Data Source

	₩ Super_Secret_Security_Incident - Autopsy-4.21.0							
Ø gen         inter interim         Ø gen         Ø gen </th <th>🕂 Add Data Source 📠 Images/Videos 📓 Communications 💡 Geolocation</th> <th>🛃 Timeline 🚑</th> <th>Discovery 🛓</th> <th>Generate</th> <th>Report 🍙 Close Case</th> <th></th> <th>1</th> <th>S · Keywo</th>	🕂 Add Data Source 📠 Images/Videos 📓 Communications 💡 Geolocation	🛃 Timeline 🚑	Discovery 🛓	Generate	Report 🍙 Close Case		1	S · Keywo
Image: Section for the section of t		😹 Open Lookin	hostfiles		v <b>3</b> ⊅≣-	×		
Image: State of type     Image: State of type       Image: State of type     Ima		Recent Horns	CIT DFIR NetSec	i da				
if is store     Waterstaft       Neteriki     Her of type       Al Supported Types     Cancel		Documents Documents This PC					Browne	
Notivetik     Piles of type     Alf Supported Types     Cancel       Hash Yakas (soptional)     MDS		٠	Lie name:	WinServ	rdd	Open	~	
Hah Valac (optionul)       M05:       944-1:       944-1:       944-1:       950-20       NOTE These values will not be validated when the data searce is in salidad.		Network	Files of types	All Supp	orted Types 🗸 🗸	Cancal	×	
( Bark Nexts Finish Court Help					Hah Valva (optionut) MD5	ed.		
Value interior and interior					< Eeck	Next > Finish	Cancel Help	

# (b) Selecting Drive Image

😹 Add Data Source		×			
Steps	Select Data Source				
1. Select Host	Path:				
Select Data Source Type     Select Data Source	C:\Users\secdoc\Documents\hostfiles\WinServer.dd	Browse			
<ol> <li>Configure Ingest</li> <li>Add Data Source</li> </ol>	Ignore orphan files in FAT file systems				
	Time zone: (GMT-6:00) America/Chicago				
	Sector size: Auto Detect $\checkmark$				
	Hash Values (optional):				
	MD5:				
	SHA-1:				
	SHA-256:				
	NOTE: These values will not be validated when the data source is added.				
	< Back Next > Finish Cancel	Help			

## (c) Data Source Validation

teps	Configure Ingest
Select Host Select Data Source Type Select Data Source • Configure Ingest Add Data Source	Run ingest modules on:         All Files, Directories, and Unallocated Space <ul> <li>Interesting Files Identifier</li> <li>Central Repository</li> <li>PhotoRec Carver</li> <li>Vitual Machine Extractor</li> <li>Data Source Integrity</li> <li>Android Analyzer (IEAPP)</li> <li>Cyber Triage Malvare Scanner</li> <li>Dil Drone Analyzer</li> <li>Plaso</li> <li>YARA Analyzer</li> <li>GOS Analyzer (IEAPP)</li> <li>GPX Parser</li> <li>Android Analyzer</li> <li>Select All</li> <li>Deselect All</li> </ul> History
	Rack Nets Einich Carrel Halo

(d) Data Ingestion Configuration

Super Servet Security, Incident - Justepsy 421.0				- 0
e View Tools Window Help				
P Add Data Source 🚛 Iwages/Welses 🔀 Communications 💡 Geelocation	🏹 Tiveeline ቭ Discovery 🚡 Gener	ito Report 🍵 Close Case	S 10	Enverd Lists     Gr Keyword Sear
6 3	O Using			
Data Selarces	Table Threader Commence			
File Views     File Turser				Sec. Table as
B x Deleted Files				Sere have a
E MB File Size	Nerse			
Recent Documents (2)	writeweide_i rees			
Analysis Results				
CS Accounts				
Tapi				
Reports				
	Add Data Source		×	
	Steps	Add Data Source		
	<ol> <li>Select Host</li> <li>Select Data Source Type</li> </ol>			
	5. Select Data Source	The second		
	S. Add Data Source	una source has been abbed to the local basebase. Hies are being analyses.		
	17/1			
		(Dec) Dec)	Data Canada Distric	
		* DBCK NUT	Hindan Cances Hisp	
			Analyzing files from WinServer.dd	IN II G more-

Figure 131 – Add Data Source

- 8. Navigate through the file system using Autopsy's interface to look for any obvious signs of compromise or artifacts of interest.
- 9. Use the keyword search and timeline analysis features to locate files or system activity relevant to the time frame of the incident:



Figure 132 – Timeline Analysis

10. Now, let's do a deep dive with TSK. When a forensic investigator arrives at an incident scene, they first seize all relevant evidence and capture volatile data at risk of loss when power is removed. The evidence is then transported to a forensics lab, taking care not to alter the original data.

At the lab, an identical copy of the evidence is created to prevent tampering of the original. Changes are documented and chain of custody is recorded detailing all personnel who handled evidence. This log is included in the final report to demonstrate integrity.

11. Use command-line tools from TSK such as fls, istat, icat, and mmls to analyze the file system structure, recover deleted files, and examine file metadata. To create a bit-for-bit forensic duplicate of a hard drive and generate an MD5 checksum,

run this command on Kali Linux: dcfldd if=/dev/sdb1 hash=md5
of=/media/[filename].dd bs=512 noerror.

Here:

- if=/dev/sdb1 specifies the source drive to image
- hash=md5 calculates an MD5 hash of the image for verification
- o of=/media/[filename].dd is the output image file saved externally
- o bs=512 transfers 512 bytes of data at a time
- o noerror continues reading on errors by writing zeros

This command images the entire disk bit-for-bit to an external drive, saving it as a .dd file while hashing the image. The external drive must have greater capacity than the source drive. The noerror option can be omitted if preferred. As I already have an image to analyze, this step will not be necessary.

- 12. To create a hash execute md5sum [filename].dd.
- Use the mmls command to get details of the image file including the partition layout information:

#### mmls [filename].dd

14. After obtaining a verified image, the next step is analyzing the evidence to investigate the incident. This typically involves recovering data, extracting hidden files, and accessing protected content if technically possible and legally permitted. The fsstat tool provides extensive file system details. An offset of 2048 is used to skip either unallocated space or the partition table area. Other regions can also be examined. Hard disks often contain hidden host protected areas with vendor utilities that could conceal data if aware of their existence. The disk stat Sleuth Kit tool detects if a HPA is present on the disk:

fsstat -o 2048 [filename].dd

15. Use the fls tool to view files and directories in the file system. Deleted files are denoted with a \* prefix, like \* eula.2052.txt. To examine a specific directory, reference it by its inode number from the fls output:

#### fls -o 2048 [filename].dd

16. You can use icat to read files as part of the investigation. In addition, if there are multiple files associated with the same inode, you can pipe the command to less to read them in a more manageable way:

#### icat -o 2048 [filename].dd [inode number] | less

The command icat -o 2048 [filename].dd [inode number] |

**less** is used in digital forensics to read the contents of a specific file associated with a given inode number from a disk image, and display the output in a more manageable way using the **less** command.

This command is particularly useful when dealing with multiple files associated with the same inode number. In some cases, a single inode may have multiple file names or entries pointing to it, such as in the case of hard links. By using **icat** with the inode number, you can read all the files associated with that inode.

Using **less** to view the output makes it easier to examine the file contents, especially if the file is large or contains a lot of information. You can scroll up and down, search for specific text, and navigate through the content more efficiently.

It's important to note that the specific options and parameters used with *icat* may vary depending on the version of TSK you are using and the specifics of your investigation. Always refer to the documentation and guidelines provided by TSK for the most accurate and up-to-date information on using *icat* and other TSK tools in your forensic investigations:



Figure 133 – inode View of Drive dd Image

- 17. Additional Sleuth Kit tools for metadata analysis include ifind and ffind, which locate files by searching for text string matches. Beyond keyword searches, file signature analysis is another common approach to identify files pertinent to the case by their headers rather than extensions. Focusing on relevant file types aids the investigation.
- 18. Document findings and extract evidence using icat to retrieve file contents based on inode numbers.
- 19. Document every step taken during the forensic investigation, noting how evidence was preserved and analyzed. The forensic report is the concluding

deliverable presented to the party who initiated the investigation. It contains only objective facts pertinent to the case, including at minimum:

- An executive summary outlining the case background and key findings.
- An analysis summary fully detailing evidence gathering and examination methodology. This comprehensively covers all analysis steps taken by the investigator to prove or disprove foundational allegations.
- A final summary that recapitulates closing statements and ultimate conclusions.
- 20. The report relays pure evidence-based conclusions, free of subjective interpretations. The process transparency provided by an exhaustive analysis summary ensures integrity that stands up to legal scrutiny.
- 21. Generate reports using Autopsy, including file lists, timelines, and hashes of relevant files.
- 22. Secure the evidence and ensure any copies of disk images are stored securely or deleted if no longer needed.
- 23. Reset the forensic workstation to a clean state if it will be used for future investigations.

Let us look at the next lab.

## Lab 2: Incident Response with Security Onion

Security Onion is a powerful open-source intrusion detection, enterprise security monitoring, and log management solution that provides a comprehensive platform for detecting, investigating, and responding to security threats. Built on a foundation of industry-leading open-source tools, such as Zeek (formerly Bro), Suricata, Wazuh, and Elastic Stack, Security Onion offers a unified and scalable approach to network security monitoring. It combines **network intrusion detection systems** (**NIDS**), HIDS, full packet capture, and advanced analytics to give security professionals deep visibility into their network traffic and system activities. With its intuitive web-based interface, Security Onion allows users to monitor alerts, investigate suspicious activities, and

perform forensic analysis, empowering them to quickly identify and respond to potential security incidents. Whether deployed in a single server or distributed across multiple nodes, Security Onion provides a robust and flexible solution for organizations of all sizes looking to enhance their security posture and defend against evolving cyber threats.



Figure 134 – Security Onion Website

The prerequisites are:

- A virtualization platform like VirtualBox or VMware.
- A VM to serve as the Security Onion monitoring server. If your only goal is to import pcaps using so-import-pcap, you can set up Security Onion 2 as an Import Node with these minimum specifications:
  - o 4GB RAM
  - o 2 CPU cores
  - 200GB storage

- For any other deployment beyond a basic import node, Security Onion 2 requires at minimum:
  - o 12GB RAM
  - o 4 CPU cores
  - o 200GB storage
- Additional VMs or physical machines to serve as clients/network devices to be monitored.

Let us look at the steps:

24. Install Security Onion on a VM, following the official installation guide (Security Onion Uses Oracle Linux 9 as the standard Linux Distro used when installing via the ISO):



Figure 135 – Security Onion installation dialog box

### Note

The installation and configuration of Security Onion can take a considerable amount of time as it installs and sets up all the various modules/packages, so do not be discouraged if it is taking a long time.

Here's a look at Security Onion's login screen:

Seci	urity ônion	
	Login to Security Onion	
	Email Address	
	Required.	
	Password	

Figure 136 – Security Onion Login

≡ Security (	Dnion	
Overview	Overview	
Averts		Reported to sole the
C Deshboards	Getting Started	prought to you up.
• Hunt	New to Security Onion 2? Click the menu in the upper-right corner and you'll find links for <u>their</u> and a <u>Circuit/unior</u> that will help you best utilize Security Onion to hunt for evil! In addition, check out our free	
Cases	Security Onion 2 Essentials online course, available on our training website.	Security(a) nion
	If you're ready to drive in, take a look at the <u>Alerth</u> interface to see what Security Onion has detected so far. Then go to the <u>Destroyed</u> interface for a general overview of all logs collected or go to the <u>many</u> interface	Security Shion
🛃 Grid	for more focused threat hunting. Once you've found something of interest, escalate it to <u>Callers</u> to then collect evidence and analyze observables as you work towards closing the case.	SOLUTIONS
<ul> <li>Downloads</li> </ul>	What's New	
<ul> <li>Administration</li> </ul>	To see all the interflections and lines in this contine of Castello Daiot, slick the owner daily many and then	
	to see an the sales restares and takes in this version or security union, cack the upper-right menu and then click the <u>Whot's home</u> link	
🛃 Kibana	Customize This Space	
🛃 Grafana	Make this area your own by customizing the content. The content is stored in the setd at file, which uses the common Markdown i midi format. To learn more about the format, clease see markdownaudia.	
CyberChef	To contrasting this content, basic to the measure of \$50 and source to the following command.	
Playbook	in casoninze one content, regin to one manager via asin and execute the rokowing commania.	
E FleetDM	sude cp /opt/be/sattstach/defwit/satt/soc/files/soc/ Then edit the new file as desired using your favorite text editor	
C Nevigetor	Finally, restart SOC to make the changes take effect:	

Figure 137 – Security Onion home screen
- 25. Configure network settings to allow the Security Onion VM to monitor traffic (e.g., in promiscuous mode or connected to a span/mirror port).
- 26. Deploy **network intrusion detection systems** (**NIDS**) like Snort or Suricata on Security Onion to monitor network traffic:



### Figure 138 – Security Onion Hunt Dashboard

27. Configure log management and SIEM tools like Squert, Kibana, and TheHive for alert management and analysis. It is important that you review and use the Security Onion documentation at <a href="https://docs.securitvonion.net/en/2.4/first-lime-users.html">https://docs.securitvonion.net/en/2.4/first-lime-users.html</a> through the rest of this lab. The complexity of setting up the initial Security Onion configuration can vary from environment to environment and as such, being able to walk through the documentation versus the verbatim steps in this lab will be helpful for you for a successful installation:

≡ Security	(@nicn								
Discus	Dashboards	DOM:NO							Total Found: 2
NOT									
C Destituents	G were and to united a south surface	event data sel servico como der memoria	TRACKS -Sandara within	a computer conversion		1 Last 242		-	-
0.04	n Fleg computer_name   groupby event.d	statet   groupely user ramo   groupey dr	st.q.eryname   graup	by process a vec. table (	groupby				
	n ming event, data SurgetObject   groupby	tie target   proupby notation   group by	elexabilitation.ip.) grosep	dy destration,part					
. unes									
	and a second by second and a second s								
	Basic Metrics								
At some last and									
	100								and the second
f Kome									
e comont									
	Capito Menta				• 🔻 filter Levels				
				and shall be		fore data to a	man daman 🔳	and dial to a	
	and the second second second second						process, receiver		HISTOREWADDIRS.
	1000		110				registry relation		@Wik7(8.her
	and all all all all all all all all all al		ACCOMPTING.		(G) complexity				
	THE REFE STREET	1							an annotaniaca, seare
	- And - Contraction of the Contr	el les anno 1980	- THE OWNER WATER		and the second se				
			COLUMN STREET,						MT AUTHORITINA PTWONE SERVICE
	A CONTRACTOR OF		Non Coloma and Street of		DCL Prant article local				AT AUTOMOTIVATIONS SERVICE LAPTOP (LAPING TIMAS
	and the second s	Charles Provent	TANK STREET		DCLESS and address for all		highling period (cell in percent, break-steel		MEANTHERTMETINGS SERVER LATTER ANTIGETINGS NTHEREAS
		Parameter of	PANA		DCL Provine Bank Sout DCL Provine Bank Sout DCL Provine Bank South South South DCL Bank South South South South		proving transferred to proving transferred proving the specifier		STATISHTVATURE SPACE LATER ARTIGETORS Machine Francosterborthioner

Figure 139 – Threat Dashboard

- 28. Generate or simulate suspicious network traffic that could indicate a security incident (e.g., using Metasploit or other penetration testing tools).
- 29. Review the alerts generated by the NIDS on Security Onion.
- 30. Use Security Onion's tools to analyze the data and determine the nature of the incident.
- 31. Practice containment strategies to limit the impact of the incident.
- 32. Follow an eradication process to remove the threat from the environment.
- 33. Document the incident response process, noting all alerts, actions taken, and lessons learned.
- 34. Generate reports detailing the incident and response actions for future reference.
- 35. Use lessons learned to improve the incident response plan and security posture.
- 36. Ensure that all monitoring tools are reset and ready for future incident detection.

Through these labs, participants will gain valuable experience in both the technical and procedural aspects of digital forensics and incident response. The iterative process of collection, examination, analysis, and reporting is essential for effective cyber investigation and response.

By combining investigative tools and platforms, security teams can rapidly analyze incidents, determine impact, and drive recovery while preserving evidence.

# **Application security tools**

Application security tools are essential in identifying and mitigating security vulnerabilities within software applications. The exercise will look at SonarQube and will focus on **static application security testing** (**SAST**). In this lab, **dynamic application security testing** (**DAST**) using OWASP ZAP as well. Another popular tool similar to ZAP is Burp Suite. Packt has a great book on Burp Suite called *Hands-on Application Penetration Testing with Burp Suite* by Carlos A. Lozano, Dhruv Shah, and Riyaz Ahemed Walikar.

## **Exercise: SAST with SonarQube**

SAST (Static Application Security Testing) with SonarQube is a powerful approach to identifying and mitigating security vulnerabilities and code quality issues early in the software development lifecycle. SonarQube is an open-source platform that performs static code analysis, which means it examines the source code without executing it, to detect potential security flaws, bugs, and code smells. By integrating SonarQube into the development process, teams can continuously scan their codebase, receive immediate feedback on code quality and security, and track the progress of issue resolution. SonarQube supports a wide range of programming languages and integrates seamlessly with popular development tools and CI/CD pipelines. It provides an intuitive web interface that displays code metrics, highlights issues, and offers detailed insights into the health and security of the codebase. With its extensive rule sets and customizable quality profiles, SonarQube helps organizations enforce coding standards, adhere to best practices, and maintain a high level of code quality. By leveraging SAST with SonarQube, development teams can proactively identify and address security vulnerabilities, reduce technical debt, and deliver more secure and reliable software.



### Figure 140 – SonarQube Website

The prerequisites are:

- A virtualization platform like VirtualBox or VMware.
- A virtual machine (VM) or a physical machine to serve as the analysis environment.
- The source code of the application to be analyzed.

Let us now look at the steps:

- 1. Set up a Linux VM which will be used to host the SonarQube server.
- 2. Ensure the VM has enough resources (CPU, memory, and storage) to perform analysis.
- 3. Install SonarQube on the VM following the official documentation, https://www.sonarsource.com/products/sonarqube/.

- 4. Make sure to install the required database (e.g., PostgreSQL) and connect it with SonarQube.
- 5. Access the SonarQube web interface through the browser on the host machine using the VM's IP address and port 9000.
- 6. Configure the quality profiles and rules according to the application's technology stack.
- 7. Install SonarScanner on the development machine where the application's source code resides.
- 8. Run SonarScanner against the source code repository to start the analysis.
- 9. Monitor the progress via the SonarQube dashboard.
- 10. Once the analysis is complete, review the issues flagged by SonarQube.
- 11. Use the detailed descriptions provided to understand the context and potential impact of each issue.
- 12. Address the reported issues in the application's source code.
- 13. Rerun SonarScanner to ensure the fixes were effective and did not introduce new issues.
- This is optional: Integrate SonarQube with a <u>continuous integration</u> (<u>CI</u>)/<u>continuous deployment</u> (<u>CD</u>) pipeline for automated scanning on code commits.
- 15. Document the SAST process, findings, and remediation actions for compliance and audit purposes.

### Lab: DAST with OWASP ZAP

**DAST** (**Dynamic Application Security Testing**) with OWASP ZAP is a powerful technique for identifying security vulnerabilities in web applications by actively interacting with them in a runtime environment. OWASP **ZAP** (**Zed Attack Proxy**) is a popular open-source web application security scanner that helps developers and

security professionals find and fix security issues in their applications. With OWASP ZAP, you can perform automated and manual security testing, mimicking the actions of a potential attacker to uncover vulnerabilities such as SQL injection, **cross-site scripting** (**XSS**), and broken authentication. By sending carefully crafted requests to the application and analyzing the responses, OWASP ZAP can detect security flaws that may not be apparent through static code analysis alone. It provides a user-friendly interface, allowing users to configure and customize the scanning process, set up authentication, and define the scope of the testing. OWASP ZAP generates detailed reports highlighting the discovered vulnerabilities, their severity, and recommendations for remediation. With its extensive community support, regular updates, and a wide range of plugins and add-ons, OWASP ZAP is a versatile and essential tool for conducting DAST and ensuring the security of web applications.



Figure 141 – OWASP ZAP

The prerequisites include:

- A virtualization platform like VirtualBox or VMware.
- A VM to serve as the testing environment with OWASP ZAP installed.

• An instance of a web application to test, which could be hosted within a VM or accessible over the network.

Let us look at the steps:

- Set up a VM with a suitable operating system (e.g., Kali Linux which includes OWASP ZAP). You can also step through the **Getting Started** documentation at the OWASP ZAP site using the following link: <u>https://www.zaproxy.org/getting-</u> started.
- 2. If not pre-installed, download and install OWASP ZAP from the official website, https://www.zaproxy.org/.
- 3. Ensure the target web application is running and accessible from the ZAP VM.
- 4. On initial startup, ZAP asks if you want to persist sessions. By default, ZAP saves testing sessions into HSQLDB database files locally without persistence enabled. Selecting this option preserves your session data for later access instead of deleting it upon exiting ZAP. Enabling persistence allows providing custom names and file paths to control where databases are saved. Without persistence, default unnamed database files generated at default locations are removed when closing ZAP:



Figure 142 – OWASP ZAP Dashboard

- 5. Open OWASP ZAP and set up the local proxy settings.
- 6. Configure your web browser to use the ZAP proxy.
  - A. You will need to set your browser to use ZAP as a proxy for scanning web traffic. By default, ZAP runs on localhost Address with Port 8080, changeable in **Options** | **Network** | **Local Servers/Proxies**. Here are browser-specific instructions for proxy configuration for Chrome (Windows):
    - i. Click the icon in top right and select Options
    - ii. Go to Change proxy settings
    - iii. In LAN Settings, enable proxy server and enter ZAP's Address and Port
  - B. Here are browser-specific instructions for proxy configuration for Firefox (Windows):

- i. Go to Tools | Options | General | Network Settings
- ii. Choose Manual proxy configuration
- iii. Enter ZAP's Address and Port for HTTP Proxy and SSL Proxy
- C. Here are browser-specific instructions for proxy configuration for Firefox (Linux):
  - i. Go to Edit | Preferences:

		Settings — Mazilla Firefox		
٠	Kali Linux ×	(		
		Firefax about:preferences	\$	
	nport beekmarks 🦄 Kali Linu	ar 👩 Kali Toots 🚊 Kali Docs 🥆 Kali Forums 💸 Kali NetHunter 🍺 Exploit-DB 🍺 Google Hacking DB 🦚 OffSec		
		O that between a being managed be your neuroscience.		
	Home Home	Use recommended performance settings Learn more		
	Q Search			
	Privacy & Security			
	Sync			
	More from Mozilla	Use gutoscrolling		
		Ose smooth scrolling     Always show scrolling		
		Always use the cursor keys to navigate within pages		
		Search for text when you start typing		
		Cable picture in picture video controls Learn more		
		Control media <u>v</u> ia keyboard, headset, or virtual interface <u>Learn more</u>		
		Recommend extensions as you browse Learn more		
		S Recommend features as you browse Learn more		
		Network Settings		
	2 Extensions & Themes	Configure how Firefox connects to the internet. Learn more Settings		
	③ Firefox Support			



ii. Follow Windows instructions from General section:

Connection Settings	×
Configure Proxy Access to the Internet <ul> <li>No proxy</li> <li>Auto-detect proxy settings for this network</li> <li>Use system proxy settings</li> </ul>	
<u>Manual proxy configuration</u>	
HTTP Proxy 127.0.0.1	Port 8080
HTTPS Proxy 127.0.0.1	P <u>o</u> rt 8080
SO <u>C</u> KS Host	Por <u>t</u> 0
<u>A</u> utomatic proxy configuration URL	
No proxy for	
Example: .mozilla.org, .net.nz, 192.168.1.0/24 Connections to localhost, 127.0.0.1/8, and ::1 are never proxied.	
Do not prompt for authentication if password is saved	
$\Box$ Proxy <u>D</u> NS when using SOCKS v5	Cancel OK

Figure 144 – Browser Proxy Settings

- D. Here are browser-specific instructions for proxy configuration for Firefox (OS X):
  - i. Go to Firefox | Preferences
  - ii. Follow Windows instructions from General section

- E. Here are browser-specific instructions for proxy configuration for Safari (OS X):
  - i. Click Safari settings icon in top right
  - ii. Go to Preferences | Advanced | Proxies
  - iii. Click Change Settings and configure as system proxy

With browsers routing traffic through ZAP, you can now scan web applications.

- 7. Navigate through the application in your browser while OWASP ZAP passively analyzes the traffic.
- 8. Use the **Attack** feature in ZAP to actively scan the application for vulnerabilities:



(a) Automated Scanning

	untited Session - ZAP 234.0	<b>k</b>
File Edit View Analyse Report Tools Import Export O	Online Help	
Standard Mode 🗸 🗋 🖴 🖬 📾 📾 📾 📾 📰 📟		
😂 Stes 🛨	🤆 🖗 Quick Start 🖈 👄 Request 👄 Response 🔗 Requester 🛨	
0		
✓ ➡ Contexts	Automated Scan	ර 🔶
Stes	This screen allows you to launch an automated scan against an application - just enter its URL below and press	
~ 🔁 🎮 http://192.168.2.10.3100	'Attack'.	
GET:/	Please be aware that you should only attack applications that you have been specifically been given permission to text	
) 🛄 👹 favicons		
> 🛄 🗰 fonts	URL to attack: http://192.168.2.10:3100 🗸 🔮 Select	
> 🛄 🗰 img	Use traditional spider: 🗵	
리(李 <b>四</b> ) (()	Use alax spider:	
]] 糊 GET:manifest.json	# Attack Stop	
> 🔜 🗰 svg	Progress: Actively scanning (attacking) the LIBLs discovered by the spider(s)	
🔄 🖓 🗰 GET:a		
<ul> <li>BOST graphel/U// incertion/incerting/incert</li></ul>		
POST:graphql//[{ operationName .nut, variable		
		$\mathbf{\gamma}$
📲 History 🔍 Search 🏴 Alerts 📄 Output 🕷 Spider	₩AJAX Spider 👌 Active Scan 🖉 🕱 🔸	
New Scan, Progress: 0: http://192.168.2.10:3100	0 26% Qurrent Scans: 1 Num Requests: 1226 New Alerts: 0 7 Export	$ \prec $
Sent Messages Eltered Messages		
ID Reg. Timestamp Resp. Timestamp Meth	od URL. Code Reason RTT Size Resp. Header Size Resp. Body R	
1,396 1/30/24, 10:46:11 AM 1/30/24, 10:46:11 AM GET	http://192.106.2.10/3100/assets/ions 301 Moved Pe 3 ms 419 bytes 193 bytes 220 bytes 270 bytes 270 bytes	
1,399 1/30/24, 10:48:11 AM 1/30/24, 10:48:11 AM POST 1,400 1/30/24, 10:48:11 AM 1/30/24, 10:48:11 AM POST	http://192.158.2.10/310/graphql 200 0K 5 ms 382 bytes 370 bytes	Y
1,401 1/30/24, 10:48:11 AM 1/30/24, 10:48:11 AM POST	http://192.168.2.10.3100/graphgl 200 0K 1 nms 382 bytes 370 bytes	
1,402 1/30/24, 10:48:11 AM 1/30/24, 10:48:11 AM GET	http://192.168.2.10:3100/_assets/img 301 Moved Pe 1 ms 417 bytes 189 bytes	
1,403 1/30/24, 10:48:11 AM 1/30/24, 10:48:11 AM GET	http://192.168.2.10:3100/_assets/img/splash 301 Moved Pe 1 ms 424 bytes 203 bytes	
1,404 1/30/24, 10:48:11 AM 1/30/24, 10:48:11 AM POST	http://192.168.2.10:3100/graphql 200 OK 2 ms 382 bytes 370 bytes	
1,405 1/30/24, 10:48:11 AM 1/30/24, 10:48:11 AM POST	http://192.168.2.10/3100/graphql 200 OK 2 ms 383 bytes 1,154 bytes	
1,400 1/30/24, 10:48:11 AM 1/30/24, 10:48:11 AM POST 1,407 1/30/24, 10:48:11 AM 1/30/24, 10:48:11 AM POST	http://192.168.2.10/310/graphq/ 200 0K 1 ms 382 bytes 3/0 bytes	
1.408 1/30/24, 10:48:11 AM 1/30/24, 10:48:11 AM CFT	http://192.168.2.10:3100/ assets/is 301 Moved Pe 2 ms 416 bytes 197 bytes	
1,409 1/30/24, 10:48:11 AM 1/30/24, 10:48:11 AM POST	http://192.168.2.10:3100/graphql 200 OK 1 ms 381 bytes 205 bytes	- 7
1,410 1/30/24, 10:48:11 AM 1/30/24, 10:48:11 AM POST	http://192.168.2.10:3100/graphql 200 OK 3 ms 382 bytes 370 bytes	
Alerts 월 0 🔑 1 🔑 1 科 2 Main Proxy: localhost:8080	Current Scans 🤤 0 🕸 0 🕸 4 🧯 1 🔘 0 🎢 0 🗰 0	-

Figure 145 – Scan Progress

- 9. Monitor the results and identify any security issues detected.
- Review the vulnerabilities found by OWASP ZAP, which can include issues like SQL injection, cross-site scripting (XSS), and more:

	Use ajax spider: v with Firefox Headless v v Attack Stop Progress: Attack complete - see the Alerts tab for details of any issues found
History Search Pickets Dupt Output O	Spider
Alerte 20 0 21 121 2 Main Proving Incohert 20	liert Reference: 10038-1 hput Vector: Description: Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including Cross Site Scripting (XSS) and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare Character Server 00.0 #0.0 #0.0 #0.0 #0.0 #0.0 #0.0 #0.

### Figure 146 – Content Security Policy (CSP) Header Information

- 11. Analyze the risk and potential impact of each finding.
- 12. Explore manual testing features such as forced browsing, manual request editing, and breakpoint debugging to further investigate potential vulnerabilities. While passive scanning and automated attacks provide an initial vulnerability assessment, they have some key limitations:
- 13. Login-protected pages are not discoverable without configuring authentication in ZAP. There is little control over passive scan exploration or the sequence/types of automated attacks. ZAP does offer more advanced options beyond these basics. Spiders enter limited test data which may not expose complex forms. Manual exploration with real inputs reveals more of the application. Obscure pages sometimes go live without notice, so exhaustive manual site exploration is important even if pages don't link elsewhere. Obscurity is not security.
- 14. To thoroughly explore the application:
  - Launch a browser configured to proxy through ZAP via the Quick Start tab.
     This automatically handles certificates.
  - Or manually configure your browser to proxy via ZAP and import/trust the ZAP root CA certificate for sites with errors.
  - Be sure to manually visit every page, submit realistic form data, and execute all site functionality. ZAP will passively scan traffic for weaknesses.
- 15. Combining automated scanning with comprehensive manual exploration and real-world testing generates more accurate findings by fully exercising complex application logic and surfaces obscured pages:

∫ Quick Start 🖉 🔿 Request	Response⇔ +
<	Manual Explore 💫
This screen allows you to launce ZAP.	h the browser of your choice so that you can explore your application while proxying through
The ZAP Heads Up Display (HU	D) brings all of the essential ZAP functionality into your browser.
URL to explore:	http://
Enable HUD:	
Explore your application:	Launch Browser Firefox 💌
You can also use browsers that import the ZAP root CA certifica	you don't launch from ZAP, but will need to configure them to proxy through ZAP and to ite.

(a) Manual Scan



Figure 147 – Scan Target Site

- 16. Address the vulnerabilities in the application's code or configuration.
- 17. Retest the application to ensure that the remediations are effective.
- 18. Generate a report within OWASP ZAP detailing the vulnerabilities found and the steps taken to remediate them:



Figure 148 – San Report

19. Document the DAST process, findings, remediation actions, and any additional manual testing steps taken.

Through these labs, participants will gain practical skills in both static and dynamic analysis, covering a comprehensive approach to application security testing. Proper documentation and regular analysis are crucial for maintaining application security over time.

Layered application testing provides code level through runtime assurance of software security throughout the development lifecycle. Architects combine results to prioritize remediation efforts.

# **Cloud security tools**

Lab exercises for cloud security tools often involve services provided by cloud service providers such as AWS, Azure, or GCP. For this example, we will focus on using AWS native tools to ensure security within the AWS cloud environment. The lab will cover AWS **Identity and Access Management** (**IAM**), AWS Security Groups, AWS Inspector, and AWS CloudTrail.

### Lab: Setting up and securing an AWS environment

AWS (Amazon Web Services) is a comprehensive cloud computing platform provided by Amazon, offering a wide range of services and tools for building, deploying, and managing applications and infrastructure in the cloud. With AWS, organizations can leverage a global network of data centers and a robust set of cloud services to scale their applications, store and process data, and deliver content to users worldwide. AWS provides a flexible and cost-effective environment that allows businesses to focus on their core competencies while offloading the complexity of managing underlying infrastructure. From compute power and storage to databases, networking, and security, AWS offers a vast array of services that cater to different application requirements and workload patterns. With its pay-as-you-go pricing model, extensive documentation, and strong community support, AWS has become a popular choice for startups, enterprises, and government agencies looking to embrace the benefits of cloud computing and drive innovation in their respective domains. Setting up and securing an AWS environment is crucial to ensure the integrity, confidentiality, and availability of your applications and data. AWS provides a shared responsibility model, where AWS is responsible for the security of the cloud infrastructure, while customers are responsible for securing their applications and data within the cloud.

By implementing these security best practices and leveraging AWS security services, organizations can establish a robust and secure AWS environment. It's important to continuously monitor, assess, and improve the security posture of your AWS environment to stay ahead of evolving threats and maintain the confidentiality, integrity, and availability of your applications and data.

AWS offers extensive documentation, whitepapers, and resources to guide customers in setting up and securing their environments. Additionally, AWS provides professional services and support to assist customers in their cloud security journey.



Figure 149 – AWS Website

The prerequisites include:

- An AWS account with administrative access.
- A virtual machine or local development environment to run AWS CLI and SDKs if not using AWS CloudShell.

Let us look at the steps:

1. Create or log into your AWS Management Console:



# Figure 150 – AWS Login

2. Familiarize yourself with the AWS services that will be used in this lab, specifically IAM, EC2, Inspector, and CloudTrail:



(a) AWS Console



#### Figure 151 – AWS Service Listing

3. Create a new IAM user with programmatic access. In the left navigation pane, click **Users** and then click the **Add user** button:



Figure 152 – Adding User

4. Enter a user name and select the type of access as **Programmatic access** for access with Access Key ID and Secret Access Key:



Figure 153 – User Creation dialog box

- 5. Click Next: Permissions.
- 6. Select **Attach existing policies directly** to assign desired managed policies to the user based on intended access level. You may need multiple policies:



### Figure 154 – Setting User Permissions

- 7. Click **Next: Tags**. Add any resource tags if applicable.
- 8. Click **Next: Review** to review all user details and permissions before continuing.
- 9. Click **Create user** once you have verified the configuration is correct:

$\leftarrow \rightarrow$	C @ (	) 👌 ≓ https://us-east-1	1.console.aws. <b>amazon.com</b> /iamv2/l	nome?region=us-east-2#/users/create			⊚	ඩ 🍦
	t bookmarks 🐂 Kali Linux	🕵 Kali Tools 🚊 Kali Docs	🔨 Kali Forums 💦 Kali NetHunter					
aws	Services Q Search		[Alt+	s] 🛛	) 🔶	0 0	Global 🔻	secdoc_lat
=	Step 2 Set permissions	User det	noices. After you create the user, you t	an view and download the autogenerated	i password,	If enabled.		
	Step 3 Review and create	User name secdoc	Co	insole password type one	Require p No	assword reset		
		Permissi	ions summary				< 1	>
		Name 🛃	•	Type $ abla$	Used as			
				No resources				
		Tags - opt Tags are key- user.	tional value pairs you can add to AWS resources to	help identify, organize, or search for resources.	Choose any ta	ags you want to a	associate with ti	his
		Кеу		Value - optional				
		Q secdo	ic-lab X	Q lab	×	Remove	]	
		Q, Enter	key	Q Enter value		Remove	]	
		Add net You can add	t specify a tag key w tag up to 48 more tags.					
				Ca	ncel	Previous	Create u	ser

Figure 155 – Create User

10. The user Access key ID and Secret access key will display only once, be sure to copy or download the keys before continuing as they cannot be retrieved later:

•	secdoc   IAM   Global — Mozilia Firefox	
🧅 🥔 Greenbone Security Assia 🛛 🧃		
<⇒ c a l O A	🔒 😅 https://us-east-1.console.av/s. <b>amazon.com</b> /lamv2/home?region=us-east-2#/users/details/secdoc?sec 🕁	ම ඩ 🖑 ≡
🐵 Import bookmarks 🐘 Kali Linux 👩 K	Kali Tools 🧕 Kali Docs 🚿 Kali Forums 😴 Kali NetHunter 🛸 Exploit-DB 🛸 Google Hacking DB 🌔 OffSec	
aws III Services Q. Search	[Alt+5] [Alt+5] [Alt+5]	• sector_tab •
Identity and Access ×	Device type Identifier Certifications Created on	U
Management (IAM)	No MFA devices. Assign an MFA device to improve the security of your AWS environment	9
	Assign MFA device	
Q. Search IAM		
Dashboard	Access keys (0) Create access	bey
▼ Access management	Use access keys to send programmatic calls to AWS from the AWS CU, AWS Tools for PowerShell, AWS SDKs, or direct AWS API calls. You can have a maxim two access keys (archer or inactive) at a time. Learn more 20	num of
User groups		
Users	No access keys. As a best practice, avoid using long-term credentials like access keys. Instead, use tools which provide short term	n
Roles	credentials. Learn more 🙋	
Policies	Create access key	
Identity providers		
Account settings		
▼ Access reports	SSH public keys for AWS CodeCommit (0) Actions V Upload SSH public	oey
Access Analyzer	User SSH public keys to authenticabe access to AWS CodeCommit repositories. You can have a maximum of five SSH public keys (active or inactive) at a Dime. Learn more C	
External access		
Unused access	SSH Key ID Uploaded Status	
Analyzer settings	No 55H aublic keys	
Credential report	Upload SSH public key	
Organization activity	- the second sec	
Service control policies (SCPs)		
	HTTPS Git credentials for AWS CodeCommit (0)	ala
Related consoles	Generate a user name and pateword you can use to sucherticate HTTPS connections to NWS CodeCommit repositories. You can have a maximum of 2 sets	at
IAM Identity Center 🛃	credentiala (active or inactive) at a time. Learn more 🖸	
AWS Organizations 2	A MAN A survey like Function for an in Allebra. Belance Survey	Contra and an and
A) CISLOSTICU FEEDBACK	6/2024, Amazon Web Service, Inc. or Its amazers. Privacy Terms	Cookie presences



- 11. Click **Close** once you have the keys saved externally.
- 12. The new user is now created and can access AWS programmatically using the Access Key ID and Secret Access Key.
- 13. Assign the IAM user to groups with policies granting the necessary permissions for EC2, Inspector, and CloudTrail. In the left navigation pane, select **Groups**:



Figure 157 – User Groups

14. Click the **Create new group** button:



Figure 158 – Create User Group

15. Give the group a name like **EC2-Inspector-Access** and click **Create Group**:

•	Create user group   IAM   Global — Mozilla Firefox	
🧅 🧳 Greenbone Security Assis 🔿	Create user group   AM   × +	
< → C @	O A ≓ https://us-east-1.console.aws. <b>amazon.com</b> /iarrv2/home?region=us-east-2#/groups/create area of G	=
Kali Linu	ax 🔉 Kali Tools 🖉 Kali Docs 🔪 Kali Forums 💐 Kali NetHunter 🛸 Exploit-DB 🌑 Gopole Hacking DB 🌗 OffSec	
aws III services Q. Scarch		v 10. •
Identity and Access × Management (IAM)	IAM > User groups > Create user group	
	Create user group	9
Q. Search MM		
	Name the group	
Dashboard	User group name	
▼ Access management	Enter a meaningful name to identify this group.	
User groups	E.L.P.Inspector Access Madmum 128 duracters. Use alphanumeric and 're, @' duracters.	
Users		
Policies	Add users to the aroun - Optional (1/1) in	
Identity providers	An IAM user is an writig that you creater in AWS to represent the person or application that uses it to interact with AWS.	
Account settings	Q, savch < 1 > ∅	
▼ Access reports		
Access Analyzer	User name 🕜 🔺 Groups Last activity V Creation time V	
External access	Sector 0 None 12 minutes ago	
Analyzer settings		
Credential report	Attach permissions policies - Optional (1/910) tota	
Organization activity	You can ettach up to 10 policies to this user group. All the users in this group will have permissions that are defined in the selected policies.	
Service control policies (SCPs)	All brans  V (123456746)	
Related consoles	Policy name A Type V Used as V Description	
AWS Organizations	AdministratorAccess AWS managed - job None Provides full access to AWS services and resources.	
	🗌 🗈 🔒 AdministratorAcce AWS managed None Grants account administrative permissions while explicitly allowing direct access to	
	🗌 🗈 🛈 AdministratorAcce AWS managed None Grants account administrative permissions. Explicitly allows developers and admini	
	E      E      AlexaForBusinessD AWS managed None Provide device setup access to AlexaForBusiness services	
	Grants full access to AlexaForDusinessE AWS managed None Grants full access to AlexaForDusiness resources and access to related AWS Services	
	AlexaForBusinessG_ AWS managed None Provide gateway execution access to AlexaForBusiness services	
	Alexalizedisciperal     AVS managed     Hone     Provide access to Lifesize AVS devices	
🔁 Claud Shell Feedback	© 2024, Annaton Web Services. Inc. or 83 affiliates. Privacy: Terms: Coskie pr	ferences

Figure 159 – Access Group Name

16. Select the newly created group in the list:



Figure 160 – Select Group

17. On the **Permissions** tab, click **Attach Policy**:

单 🥔 Greenbone Security Assist X		
< → C @	🛇 🔒 ≓ https://us-east-1.console.aws. <b>amazon.com</b> /iamv2/home?region=us-east-2#/groups/details/E 🛛 🚳 🆙	ල ඩ 🗳 ≡
-🗉 Import bookmarks 🛸 Kali Linu	🛪 🔉 Kali Tools 💆 Kali Docs 🚿 Kali Forums 💦 Kali NetHunter 🛸 Exploit-DB 🛸 Goople Hacking DB 🌗 OffSec	
WS III Services Q. Search		🕐 🙆 Global 🔻 seccior_lab 1
Identity and Access × Management (IAM)	EC2-Inspector-Access	Delete
Q, Search UAM	Summary	Edit
Dashboard Access management User groups	User group name Creation time ARN EC2-Impector Access January 30, 2024, 12:44 (JTC-06:00) Creation Simularity 30, 2024, 12:44 (JTC-06:00) Access	19451:group/EC2-Inspector-
Users Roles Policies Identity providers Account settings	Users (1) Permissions Access Advisor	Add permittion:
Access reports     Access Analyzer     External access     Unused access	Consistency products (1) market     Consistency products (1)	Attach policies Create Inline policy < 1 >
Analyzer settings Credential report Organization activity Service control policies (SCPs)	Pelicy name (2	Ψ
Related consider UAM identity Center 2 AWS Organizations 2		

## Figure 161 – Attaching Policy

- 18. Search for and select the following managed policies:
  - A. AmazonEC2FullAccess:



Figure 162 – EC2 Inspector Policy

B. AmazonInspectorFullAccess

۲		Add permissions   I	AM   Global — Mozilla Firefox		0 0 8
۲	I Greenbone Security Assis × 📑 Add permissions				
	→ C @ O A ≓ https://us-	east-1.console.aws.amazon.c		groups/details/EC 80% 🏠	ල රු 🌛 =
-91	import bookmarks 🛸 Kali Linux 👩 Kali Tools 💆 Kal	i Docs 📃 Kali Forums 🥳 Kal	li NetHunter 🐁 Exploit-DB 🔺 Google	Hacking DB () OffSec	
aws	Services Q. Scorch	[Alt+5]		-	🕽 Global 🕈 secdor_jab 🕈
=	IAM > User groups > DC2-inspector-Access > Add permission	15			©
	Attach permission policies to EC2	Inspector-Access			9
	Attach permission policies to Ecz-	inspector-Access			
	<ul> <li>Current permissions policies (1)</li> </ul>				
	Other permission policies (3/909)				G
	Tou can attach up to 10 managed pances to the user group. At at the user	s in this group intent the attached pennission	Filter by Type		
	Q, Amazonimspect	×	All types 🔻	5 matches	< 1 > @
		Туре	▼ Used as		
	🛛 🕒 📫 Amazoninspector2FuliAccess	AWS managed	None	Provides full access to	Amazon inspect
	Amazoninspector2ManagedCisPolicy	AWS managed	None	This is a managed poli	icy that custome
	Amazoninspector2ReadOnlyAccess	/WS managed	None	Provides read only acc	ess to the Amaz
	AmazoninspectorFullAccess	AWS managed	None	Provides full access to	Amazon inspect
	AmazoninspectorReadOnlyAccess	AWS managed	None	Provides read only acc	ess to Amazon I
				Cancel	Attach policies
R	IoudShell Feedback			0 2024, Amazon Web Services, Inc. or its affliates. Prov	acy Terms Ceckie protoronces

Figure 163 – Permissions

C. AWSCloudTrailFullAccess



Figure 164 – CloudTrail Policy

19. Click **Attach policy** to attach all three policies to the group:

	ess   IAM   Global — Mozilla Firefox		
8 EC2-Inspector-Access   IA × +			
O A # https://us-east-1.console.aws.amazor	n.com/iamv2/home?region=us-east-2#/g	groups/details/EC 80% 🏠	ම රු 🍣 :
🐢 Kali Tools 🚊 Kali Docs 🚿 Kali Forums 🔿 K	Kali NetHunter 🐞 Exploit-DB 💧 Google	Hacking DB 🌔 OffSec	
[Nt+5]		S 4 0	🙆 Babal 🔹 andar Jab
slicy removed.			×
M X thereases X #72 investor from			
or / on going / compromotion			
EC2-Inspector-Access 🛶			Delete
Summary			
Summery			- Cart
User group name	Creation time	ARN	
EC2-Impector-Azern	January 30, 2024, 12:44 (UTC-06:00)	Atxess	p/EC2-impector-
Users (1) Permissions Access Advisor			
Permissions policies (4) teta		C Simulate 🛛 Remove Add	d permissions 🔻
na tak atau up ta konsanges patans.	Either Inc Turus		
Q. Sesroh	All types	*	<1>0
Petroy name 2	• Туре	V Actioned entities	
Amazone 2 Juniores	ANS managed	1	
Amazonims pector 27 ut Access	All'S managed	1	
AmazonimspectorFullAccess	AWS managed	1	
AMAGE IN ANTICASE ENERGY AND	AWS managed	1	
	Second Control of Con	See Kall Tools & Kall Doos & Kall Perrums & Kall NetHanner & Exploit DB & Coogle  (74+5)  stoy resource.  Semmary User programe E2-Ampeter-Access see  Semmary User programe E2-Ampeter-Access see  Semmary User programe E2-Ampeter-Access Filter by 50, 2024, 12-4 (UTC-00.02)  User (1) Permission policies (4) tas  Filter by Type  Second Filter by Type  Filter by Type	Sommary User program Cretion for the product of the second of the secon

Figure 165 – Permission Policies

20. In the left navigation pane, select **Users**:



Figure 166 – Selecting Users

21. Select the target user you want to grant access permissions to:



Figure 167 – User for Permissions

22. On the **Permissions** tab, click **Add user to groups**:

•	secdoc   IAM   Global — Mozilla Firefox	0	- <b>8</b>
单 🥔 Greenbone Security Assi			
< → C @	🛇 🛔 ≢ https://us-east-1.console.aws.amazon.com/liarw2/home?region=us-east-2#/users/details/sec 🛛 🔐 🏠	ල රු 🍦	
🕀 Import bookmarks 🛸 Kali Li	inux 🔉 Kali Tools 🧧 Kali Docs 🔪 Kali Forums 💦 Kali NetHunter 🛸 Exploit-DB 🛸 Google Hacking DB 🌗 OffSec		
aws III Services Q. Search	(AII+5) D 4 0 0		
Identity and Access X	WM > Users > secoloc		0
Management (IAM)	secdor ht	Delete	G
Q. Search MM			
	Summary		
Dashboard	ADH Console access Access feet 1		
▼ Access management	Consider diversion     Consider diversio		
User groups	Created Last console sign-in		
Users	January 30, 2024, 12:29 (UTC-06:00) -		
Policies			
Identity providers	Permissions Groups [1] Tags [1] Security credentials Access Advisor		
Account settings			
▼ Access reports	User groups membership (1) Remove Add use	r to groups	
Access Analyzer	A war group is a collection of UM users. Use groups to specify permissions for a collection of users. A user can be a member of up to 10 groups at a time.		
External access	□ Group name ▲ Attached policies [2]	~	
Unused access	EC2-Inspector-Access Amazonhispectorful/Access, AmazonEC2/ful/Access and 2 more		
Credential report			
Organization activity			
Service control policies (SCPs)			
			2
Related canables			
IAM Identity Center			
Arra Giganzatoris 🖻			
🕅 CloudShell Feedback	di 2024, Annoon Web Services, Inc. or Rs etMilistes. Privacy	Terms Coskie pref	erences

Figure 168 – Adding User to Group

- 23. Select the **EC2-Inspector-Access** group and click **Add to Groups**.
- 24. The user is now an IAM group member with the necessary EC2, Inspector, and CloudTrail permissions to perform actions allowed by those service-specific policies.
- 25. Create an IAM role with security auditing permissions and assign it to an EC2 instance for Inspector scanning. Launch an EC2 instance that will be the target for security assessment:


Figure 169 – Selecting EC2

26. Now, let's look at an EC2 instance setup. Launch an EC2 instance that will be the target for security assessment:



Figure 170 – Launching EC2 Instance

- 27. Ensure that the security group associated with the EC2 instance allows traffic only on the necessary ports (e.g., 80 for HTTP, 443 for HTTPS).
- 28. In the EC2 console, click **Instances** and select the newly launched instance:



Figure 171 – EC2 Instance Details

29. Under the **Details** tab, copy or note down the instance ID:



Figure 172 – EC2 Instance ID

30. Open the IAM service in the AWS console:



Figure 173 – IAM Console

31. Click **Roles** and then **Create role**:



Figure 174 – IAM Roles

32. Under Select type of trusted entity, choose EC2:

		Sector and the	and a second second				
	Consistence permitiy where a	Crute nee ( 459) Cartail 9 +					
		2 🗄 🗮 Manufation Contraction and and a 🗧	amiantinnihugses	en-ant-Maintalanna 💵	수 문 눈	ຍ 🖉 🗉	
	l importacionarias	🔉 Keli Toris, 💆 Kali Doon 📃 Kali Foroms 💰 Kel					
	12 III + Q	(1944)			D 4 3 8 mm	· · · · · · · · · · · · · · · · · · ·	
=	MIT > Real > Granterinte	Q. Titler works or you see				0	
	big t	Internetly shell writes				0	
	Select twoled outry	82	1				
	144	Star				10	
S	Add permittalization	Tilker services					
	100	Amagins EMIE Senseniests		() minimum			
	North, include, and anothe	Assesses Open laws & Second	Windowe .	Altern case bolocited by the americal			
		Ariantelization	Access)	saludna Bita nati Lapartinte acheraria Bita artisetti		1 mm	
		Anglity					
		hard and				1 9, 90, 91	
		Application Auto Scaling	Star Bright				
		Application Discovery Service					
		appearers impress service					
No.		4003718910					
100 B. C. B. C.		Applaya					
		-AVS Beckup			-		
		AVS Oxford (Neine Conference on Con-					

Figure 175 – EC2 Entity Selection

- 33. Under **Select your use case**, choose **EC2** then select **Next: Permissions**.
- 34. Search for and attach the AWS managed policies:
  - A. AmazonInspectorFullAccess:



Figure 176 – IAM Permissions

B. SecurityAudit:





35. Click **Next: Tags**, optionally add tags, then click **Next: Review**:

•			Create role   IAM   Global — Mozilla Firefox						
٠	Ø Greenbone Security Ass	s 🗶 🧧 Create role   IAM   Global. 🗶							
	→ C 🍙	O A ≓ https://us-east-1.conso	le.aws.amazon.com/iam/home?region=			☆		ර 🇳	
-Ð in	nport bookmarks 🛸 Kali L	inux 👩 Kali Tools 🧧 Kali Docs 🥆 Kal	li Forums  Kali NetHunter 🔺 Exploit-	DB 💊 Google Hacking DB	() Offs	Sec			
æs	E services. Q. Snarch					© 4	<b>0 8 4</b>		
=	MM > Rains > Create role								۵
	Select tracked writig	Name, review, and create							6
	they 2 Add permission	Role details							
	1117.1 Rama, enders, and creats	In the extended case to checkly the ode. Execute Auto-Entrol Preserve at Auto-Entrol Preserve at Auto-Entrol Biocycless Address and a sequence of the ode. Address and a sequence of the ode. Address at C2 instances to call AMS services on your behalt reserves 1000 Accesters. In Addresseeth and resp., Among Step 1: Select instand entities Trust policy	r r					Eex	
		1							
		Step 2: Add permissions						Edit .	
		Permissions policy summary							
		Policy name 🛛	▲ Type		*	Attached as		*	
		Amazenimpector27402com	ANS managed			Permissions policy			
		AmazanimpectorFallAccess	SWS managed			Permissions policy			
		Searly/off	/WS managed - job function			Permissions policy			
		Step 3: Add tags							
51.0	the numbers					on Web Sectors for our other	the Disc -	-	

Figure 178 – Adding Permission to Role

- 36. Enter a role name like **Inspector-Audit-Role** and create the role.
- **37**. Click on the newly created IAM role in the list:

•	Ri	oles   IAM   Global — Mozilla Firefox			$\odot$ $\odot$ $\otimes$
🔹 🧔 Greenbone Securit	Assis 🛪 🧧 Roles   IAM   Global 🛛 👋 🕂				
	O 🗛 ≓ https://us-east-1.console.aws.	amazon.com/iam/home?region=us-east-2#/roles	67% 🟠		<b>6</b>
- Import bookmarks	Kali Linux 👩 Kali Tools 🛛 💆 Kali Docs 🔨 Kali Forun	ns 🛭 💐 Kali NetHunter 🐞 Exploit-DB 🐞 Google Hacki	ng DB 🕠 OffSec		
🐸   🏭 Services 🔍 Scarch	[Alt+5]			0 8 cabel •	
Import Bookmarks.      An entry of Access Acce	Call Linux (a) Kall Tools (c) Kall Docs (c) Kall Perun         Call Linux (a) Kall Tools (c) Kall Docs (c) Kall Perun         Call Linux (a) Kall Tools (c) Kall Docs (c) Kall Docs (c) Kall Docs (c) Kall Docs (c) Kall Cocs (c) K	Kall NetHunder     Exploit-DB     Coogle Hacks      Market Hunder      Market extra a second by setter darpes on      Market extra a second by setter darpes      Market extra a seco	Ing DB Office Office C C C C C C C C C C C C C	Outer     Dester off       Outer     Cash off       Outer     Marga	
D cloudshell Predback			© 2024, Annacus Neb Services, Inc. or IS of	liates. Privacy Terros Co	okte preferences

Figure 179 – Inspector Roles

38. On the **Summary** page, click **Add inline policy** and select JSON:

۲	Inspector-Audit-Role   IAM   Global -	– Mozilla Firefox	•	. 8
👙 🥔 Greenbone Secu	ty Assis × 🧧 Inspector-Audit-Role   IAT × 🕂 +			
← → C @	A # https://us-east-1.console.aws.amazon.com/iam/hor Kali Linux A Kali Tools Kali Docs Kali Forums of Kali NetHunter	ne?region=us-east-2#/roles/details/	n හොද බොද වේ ේ B (1) OffSec	
205 III tervies Q. Search	[AH-5]		E 4 3 8 cant • and	
Identity and Access X Management (IAM)	Meth         > Impector-Audit-Role           Inspector-Audit-Role w/s         Adams Hot Internet to dial RMS services any your behalt.           Summary         Summary		Delete	0
Dashboard <b>v</b> Access management User groups Users Raise Policies Mentify considers	Creation date ARE Amazon (2014) ARE Creation date ARE Creation date Amazon (2014) ARE	inta 451 role/impector-Audit-Role Ø a	ner profile ADS emanstan: 98238319433 instance profile/Ingentor-Audit-Role	
Account settings * Account megarits Account Analgene External access Unused access Analgene settings Codestical report Organization settings Sarvice content plokies (SOPc)	Permissions         Total relationships         Tags (1)         Access Advisor         Reveks sessions           Permissions policies (3) win	Filter by Tope All types • •	(3) Simulate (2)         Review         Add particulation: ▼           <	
antinea consules UMM Monthly Context (2 AMIS Organizations (2)	Amazonivspector2FullAccess         Product bid access to focus when some to the whend across some some some some some some some s		(3) Copy 1500	
	C      C	nction	1	
E clouddell reallack			© 2024. Annual web servers, mc. or no offloers. Privacy terms cooke pr	elevenes

Figure 180 – Inspector Policy Permissions

- 39. Paste a JSON policy granting permissions to the S3 bucket where the AWS Inspector will store reports.
- 40. Click the **Review policy** button and then the **Save changes** button.
- 41. Return to the EC2 console and select the target instance again.
- 42. Click the **Actions** | **Instance Settings** | **Attach/Replace IAM Role** menus at the top:



**Figure 181 – Inspector Actions** 

43. Select the **Inspector-Audit-Role** role and click **Apply**:

٠	Modify IAM role   EC2   us-east-2 — Mozilia Firefox				000	3
٠	Ø Greenbone Security Assi: × 🗾 Modify IAM role (EC2 ) us × +					
	→ C A st https://us.aast.2.cosole.aws.amazon.com/ar2/homo?conion=us.aast.2#Mod	lifvtAMRoleciostan - 🕎			A 🖉 =	
-film	ort bookmarks 🔊 Kali Linux 🔿 Kali Tools 📮 Kali Doos 🥆 Kali Fooums 🔿 Kali NetHunter 🖕 Evoluit-DB 🔈 Google	Harking DB 0005ec			<b>· ·</b> -	
aws	iii Sendeze (Alt+C)		0 0	Obio T	sector lab T	
_	M Start (no. 2)		•••	0.00		
-	EC2 > Instances > I-02a91909d4f8be1b8 > Medify IAM role				G	1
	Modify IAM role Info Attach an IAM role to your instance.					
	Instance ID <b>Instance ID</b> <b>Instance ID</b> <b>Instanc</b>					
	currently attached to your instance.					
	No IAM Role E Instance will be removed. Are you					
	Choose Urs option to detach an IAM role Inspector-Audit-Role					
	arrcaws.lam:392382419451:instance-profile/Impector-Audit-Role					
	Cancel Update IAM role	•				
Þ.o	udShell Feedback 0 2024, Amazen Y	Web Services, Inc. or its affiliates.	Privacy 1	Terms C	ookie preferences	

Figure 182 – Complete Audit Role Update

The EC2 instance now has the necessary permissions through the attached IAM role for Inspector assessments.

44. Let us look at an AWS Security Groups review. Click **Launch VPC Wizard** and create a new VPC with subnets according to your requirements:



(a) VPC Console



Figure 183 – Create A VPC

45. Once the VPC is created, navigate to **Security Groups** in the left sidebar:



Figure 184 – Security Groups

46. Click the default security group that gets created with your VPC:

٠			SecurityGroups   VPC Console — Mozilla	Firefox		008
•	🤌 Greenbone Securi	ity Assis × 🥚 SecurityGroups   VPC Ce				
4-		O A ≠ https://us-east-7	console aws.amazon.com/voccoosole/h		ଅନ୍ତ ପ୍ର	<i>8</i> =
- 	enert benchmarker and	Kali Liever A Kali Tanie R Kali Dare	Kali Engang	ulai DR. • George Harber DR. • 000		
-2111		Kali Linux 👩 Kali Tools 👱 Kali Docs	Kau Porums 💦 Kau Nethunter 🔺 E	proit-DB Google Hacking DB 📢 Ons		
- 	G. Sam	A	[AII+5]		E  4 Ø Ø ∞••	nedocjab *
VPC	K breadriate	Security Groups (1/3) tota		C Actions V Expert security group	os to CSV • Create security pro	(C)
EC2	Global View 🛃	Q. Find responses by attribute or tag			(1)	@ 0
Div.	er he VEC	a, rearranter ay annual or reg				0
Se	lect a VPC V	■ Nome ♥ Security gro	up ID v Security group na	ne v VPCID	v Description	
* 1	Virtual private cloud	- 91-0800855	2435c33def launch-wizard-1	voc-015d86b1c86a0e022	launch-wizard-1 creater	8 2024-01
	Your VPCs	- se-Officities	dladbilfall default	ypc-05en31051562cf560	default VPC security ge	and
	Subnets	a - si-ttoafid	13344c400 refeut	vac-01505601(35600-022	default VPC security gr	00D
	Route tables					
	internet gateways					
	Egress only internet gateways					
	DHCP option sets					
	Einstic IPs					
	Managed prefix livits					
	Endpoints					
	Endpoint services					
	Persian concertions					
	Security		_			
	Network ACLs	sp-0b8dfbdf13344e4b6 - default				
	Security groups					
* 1	DNS firewall	Details Inboard rules Outboard	ules Taos			
	Rale groups					
	Domain lists					
	Network Firewall	Details				
	Frewalls					
	recent powers	Security group name	Security group ID	Description	VPC ID	
	groups	D ocfeat	g-068dfbdF13344e4b6	Cefault VPC security group	yac-015c86bic86a0e022	
	TLS impection	Owner	Inhound rules count	Outbound rules count		
	Network Firewall	Di AA5345418421	1 Merriession entry	1 Permission entry		
	resource groups					
* 1	/intual private network					
E] da				© 2124, Amazon Web Servic	en. Inc. or its attitudes. Privacy Terms Co	

Figure 185 – Select Security Group for VPC

47. On the **Inbound rules** tab, delete any overly permissive open inbound rules like SSH open to 0.0.0/0:



Figure 186 – Edit Inbound Rules

48. Click the outbound rules and delete any default allow all outbound rule:



Figure 187 – Edit Outbound Rules

49. Create a new custom security group, give it a name like **web-sg**:

•	CreateSecurityGroup   VPC	Console — Mozilla Firefox				0
单 😝 CreateSecurityGroup   VP × 🛛 +						
← → C @ O B #	https://us-east-2.console.aws.amazon.com		st-2#CreateSecuri 80% 🏠		- 🗳	
🗈 Import bookmarks 🛸 Kali Linux 👩 Kali	i Tools 🗧 Kali Docs 🥆 Kali Forums 💦 Kali Ne					
WS III Senices Q. Search	[Att+5]		5 4 Ø	🕲 0160 🕈	sector_lab •	
WPC > Security Groups > Create security group					0	
Create security group up					G	
A security group acts as a virtual firewall for your instan	ce to control inbound and outbound traffic. To create a new sec	urity group, complete the fields below.				
Basic details						
Security group name into						
web-sg Name connection edited after creation.						
ALLOW POLATS						
HEARING OFFICE						
VPC info						
vpc-015d86bfc86a0e022	¥					
Inbound rules toto						
This security arous has no inbound rules.						
Add rule						
Outbound rules Into						
Type Info Protocol Info	Port range Info Destination Info	De	escription - optional lefe			
All traffic 🔻 All	All Custom ¥	Q		Delete		
		0.0.0.0/0 ×				
Add rule						
					-	
CaudShell Feedback		/	© 2024, Amazon Web Services, Inc. or its affiliates. Print	acy Terra Co	akte preferences	1
			Long and the second second			

Figure 188 – Create Security Group

50. On the inbound rules tab, click **Edit rules**, **Add rule** and add the following:

- A. HTTP from your local workstation IP
- B. HTTPS from your local workstation IP:

				CreateSecuri	tyGroup   VPC	Console — Mozilla Firefox	_		_	_		
😑 Crea	ateSecurityGroup   VP											
→ C		08≈		.console.aws.ar	nazon.com			-east-2#CreateSecuri 80% 🏠			נ 🍦	2
	ıkmarks 🦄 Kali Lir		ols 🗧 Kali Docs	🔨 Kali Forums	Kali Ne	tHunter 🔸 Exploit-DB						
Sar	vices Q. Search			[Alt+S]				D 4	0 6	) Obio •	tecdo	к,
VPC Info												
vpc-015d	86bfc85a0e022			*								
Inbound	rules into											
Type Info		Protocol Info	Port range Info	s	purce Infe			Description - optional Info				
HTTP	•	TOP	80		My IP 🔻	Q		Allow 80	_	Delete		
						(32 ×						
HTTPS	•	TCP	443		My IP 🔻	9		Allow 643		Delete		
					.,	/32 ×						
Add rul	le.											
Outbour	nd rules into											
-								-				
Type Info	·	Protocol late	Port range Info	0	estination into			Description - optional lano				
All traffic	*	All	All		Custom 🔻	Q				Delete		
						0.0.0,00 X						
Add rul	le											
A Rules v	with source of 0.0.0.0/0 or ::	/0 allow all IP addr	esses to access your ins	tance. We recommen	d setting securi	ity group rules to allow access f	from know	wn IP addresses only.			×	
_												
Tags - or	ptional											
A tag is a lab	el that you assign to an AWS re-	source. Each tag consis	ts of a key and an optional	value. You can use tags	to search and filte	r your resources or track your AWS o	osts.					
No tegs ass	sociated with the resource.											
rudShell Fe	eedback							© 2024, Amazon Web Services, Inc. or its affiliates	. Privac	y Terms	Cookie pre	efe

Figure 189 – Inbound/Outbound Allow Rules

51. Click Save rules:

<⇒ ơ ŵ	🛇 👌 😅 https://us-east-2.console.aws.amazon.com/vpcconsole/home?region=us-east-2#SecurityGro. 🐲 🏠 😔 🖞	• =
- Import bookmarks	s Kali Linux 🎓 Kali Tools 👱 Kali Docs 🥆 Kali Forums 🐟 Kali NetHunter 🛸 Exploit-DB 💻 Google Hacking DB 🌗 OffSec	
aws I 🔛 services 🔍 Searc	ch [41-5] D A O O O One • mat	K,MD T
VPC dashbeard X	Security group (sg-553bd7208004eb(HC1.web-sg) was created successfully     Security group (sg-553bd7208004eb(HC1.web-sg) was created successfully     Security group (sg-553bd7208004eb(HC1.web-sg) was created successfully	< ©
Filter by VPC: Select or VPC •	VPC > Security Grage > sg-058bd7208009ebd90 - web-sg           sg-058bd7208009ebd90 - web-sg	
Your VPCs Subnets Boute tables	Details	
nouce cores Internet gateways Egress-only internet gateways DHCP option sets Elivitie (Es	Security group name         Security group ID         Description         VPC ID           ID         wtb sp         ID         sp 05tot7208009ebd90         ID         ALLOW 80/443         ID         sp 05tot7208009ebd90         ID         sp 05tot7208009ebd90         ID         Note: Cliption         VPC ID         ID         Sp 05tot7208009ebd90         ID         Note: Cliption         VPC ID         ID         Sp 05tot7208009ebd90         ID         Note: Cliption         Note: Cliption         ID         Note: Cliption         Note: Cliption         Note: Cliption         Note: Cliption         Note: Cliption         ID         Note: Cliption         Note: Clipt	
Managed prefix lists Endpoints Endpoint services	Inbound rules Outbound rules Tags	
Peering connections	Outbound rules (1)	
▼ Security		
Network ACLs	Q, Search < 1 > @	
Security groups	Name V Security group role. V IP version V Type V Protocol V Portrance V Data	
▼ DNS firewall		
Rule groups	- Sprusos tensuri com IENY AL DETIC ALL NU DULU	
Domain lists		
Network Firewall		
Firewalls		
Firewall policies		
groups		
TLS inspection		
configurations		
Network Firewall resource croups		
Virtual private network     GoudShelt Feedback	6 XXX4 Anneon Net Services Inc. or its officiales. Privacy: Terms: Cookie pr	eferences
the second s		

Figure 190 – Security Group Dashboard

- 52. Repeat to create additional locked down security groups for resources grouped logically, geographically etc.
- 53. Launch new EC2 instances, RDS databases etc. and assign appropriate regional, role-based security groups.
- 54. By leveraging VPC security groups that open just required minimum ports to authorized source IP ranges, you can drastically reduce your attack surface following least privilege access principles.
- 55. Now let us look at the AWS Inspector Setup. Open the Inspector service within the AWS console:



Figure 191 – Amazon Inspector Console

56. Click Get Started under Inspector Assessments:

۲	Amazon Inspector   us-east-2 — Mozilla Firefox	00	8
۲	4 Amazon Inspector   us-eo × +		
	→ C 📾 🗘 👌 🖛 https://us-east-2.console.aws. <b>amazon.com</b> /inspector/v2/home?region=us-east-2#/ 🛛 😂 🏚	<b>-</b>	
	mport bookmarks 🔌 Kall Unux 👩 Kall Tools 🙍 Kall Docs 🛝 Kall Forums 💰 Kall NetHunter 🛸 Exploit-DB 🛸 Google Hacking DB 🕧 OffSec		
aw.	:   # 5000 Q   Q   Q   Q   Q   Q   Q   Q   Q	sunds	••
=	© Impaction new supports deep Inspection of IC2 Instances.           Antivate deep Inspection         Antivate deep Inspection           Annamin Inspector not supports deep Impaction of IC2 Instances.         Antivate deep Inspection	×	Θ
	Annuen lagester edis additionel hui bete basel er sean onfryentien for ECR container image samring     Annuen lagester rezi allow you is manage tri automated resears of container image solding. AVX Baaks Container Registry (ECR basel or mage pathidae in addition to solding pachidae basel resear duration     contrained in State to Rev many the automated resears of container image is addition. Build data based "Be van bandle based "Be van duration" onling from the ECR writing page within the impects compare or APIs. Learn     uses E		
	O Amazon Inspector expands 60% Lumbds code scanning with generative All powered remediation Ancean Inspector code scanning for AIME Lumbds factions now includes assisted upper encluden song generative a tills. A intelligence (Al) and astemator reasoning. Ancean Inspector code remediation for Lumbda function provides in-context code partities for multiple scales of wavenabilities codected during security scales for XMS Lumbda function provides in-context code partities for multiple scales of wavenabilities codected during security scales for XMS Lumbda function provides in-context code partities for multiple scales of wavenabilities codected during security scales for XMS Lumbda function provides in-context code partities for multiple scales of wavenabilities codected during security scales for XMS Lumbda function provides in-context code partities for multiple scales of wavenabilities codected during security scales for XMS Lumbda function provides in-context code partities for multiple scales of wavenabilities codected during security scales for XMS Lumbda function provides in-context code partities for multiple scales of wavenabilities code context of the XMS Lumbda function provides in-context code partities for multiple scales of the XMS Lumbda function provides in-context code partities for multiple scales of the XMS Lumbda function provides in the XMS Lumbda function for Lumbda function provides function for Lumbda function for Lumbda function p	×	
	Anomal human technical contracts and the properties with developer test     Anomaly for contracts and the properties with developer test     Anomaly representation allows for a properties with a properties with a series and the properties with a properties of the properties of	×	
	C Anaron Inspector rate suggests Center of Internet Scenets (CIII) Sections 4 second rates and internet Scenets (CIII) Sections 4 second rates and internet in section rate and internets and inter		
	Amazon Inspector Get started with Inspector		
	automated and continual		
	vulnerability management at		
	scale		
	Annacton Impector is an automated will near all tymonogement service that continually scaro worklaads for software wheestablities and unificanted network opplaare.		
	Riden (2		
	Per meth-per figure		
	How It Works		
	About sur 15 day trial		
N	anNet in the sector of 2022 Automotive Services of a sector of the Secto	kie profeso	rus.

Figure 192 – Getting Started with Inspector

57. Specify an assessment target by choosing an existing resource group or creating a new resource group:

🔶 🖪 Settings > Account ma	max +	~
	🛇 🛔 🎫 https://us-east-2.console.aws.amazon.com/inspector/v2/home?region=us-east-2tt/settings/a- 🔤 🏠 🦃	
🕣 Import bookmarks 🔍 Kali	i Linux 👔 Kali Tools 🧕 Kali Docs 🔨 Kali Forums 🥳 Kali NetHunter 🛸 Exploit-DB 🔍 Google Hacking DB 🎵 OffSec	
🦥 🔛 Services 🔍 Service	xxxx ▼ ##0 Ø Ø ↓ A	Jab 🔻
Inspector ×	© Wilcome to Inspector Renage all accounts XX To get Identify Annual Multiple Control of Annual Annual Control	0 0
Deshboard Findings	© Welcame to Inspector. Your first scan is underway.	
By vulnerability By instance	🕲 Impactor new supports deep impactions of 622 Induces	
By container image By container repealory By Lambda function All findings	(a finishin longertar and is additional Pull Date Saved re-scan configeration for CDC contributer image scanning Annual longertar rate (longertar rate) files to be unauge the scanned or excansion (contrainer image) (CD) based on image pull date in addition to existing puph date based to exist an automot configuration. Statistic Roll and based "to exist and due con" configuration, you can now configure an additione Public and base fixed. The scan statistical "thirty fixed the ECR writing puph writin the torquester consist or ABNs. Learn more (2)	
Equori 1980Ms Suppression rules IV On demand scans ID5 scams	Amazan Ingector repinde XVIS Limited code controls with generative Al powered remediation     Annuan Ingector replication of the XVIS Limited infection was madele code of the module and power and float in tellspace [A] and animolations are power and float in tellspace [A] and animolations are power and float in tellspace [A] and animolations are power and float in tellspace [A] and animolations are power and float in tellspace [A] and animolations are power and float in tellspace [A] and animolations are power and float in tellspace [A] and animolations are power and float in tellspace [A] and animolations are power and float in tellspace [A] and animolations are power and float in tellspace [A] and animolations are power and float in tellspace [A] and animolations are power and float in tellspace [A] and animolations are power and float in tellspace [A] and animolations are power and float in tellspace [A] and animolations are power and float in tellspace [A] and animolations are power and float in tellspace [A] and animolations are power and float intermediation are power and animal and an animal and animal animal and animal animal animal and animal animal animal animal animal animal animal and animal anima	
Vulnerability database wareh Acceute management III Besonres coverage III Cansoni vettings EC2 scanning settings ECR scanning settings Unage	Ingerter y settion; > Animan management set  Account management set  Menage per extensity and reverse the covering of year meaners, repeatence, respect and further furthers.  Account in indexes: Container repeatencies Container images Lembids functions.  My Account [1] inte  C Account Account in an intervent of anyweb and maintain and a fill addea (2)  Account in an intervent of anyweb and maintain and a fill addea (2)	
Video tutorials What's New 10	C Example approximation and regions are regions and regions and regions are regions and regions and regions are regions a	
Switch to Inspector Clanak 🗹	Account number  V Account numb	
DaudShell Peadaatk	© 2224 Amazer Wild Sarvos, In: or to al Malao. Power Dooke per	

Figure 193 – Defining Inspector Targets

- 58. Select the EC2 instance(s) you want to scan by instance ID or tags.
- 59. Click Next:

•	Settings > Account management   Amazon Inspector   us-east-2 — Mozilla Firefox	
单 🧧 Settings > Account mar		
	🛇 👌 🕫 https://us-east-2.console.aws. <b>amazon.com</b> /inspector/v2/home?region=us-east-2#/settings/ar 🚳 🏠 😇 🖄	1 🖑 ≣
🕀 Import bookmarks 🦄 Kali	Linux 🎓 Kali Tools 🚊 Kali Docs 🥆 Kali Forums 💸 Kali NetHunter 🛸 Exploit-DB 🛸 Google Hacking DB 🥠 OffSec	
US III Services Q Statich		secclos_lab 🔻
Inspector ×	Insector > Settings > Account management	0
Deshboard V Findings	Account management ins Manage your accounts, and review the coverage of year instances, repositance, images and Lamitula functions.	9
By wulnerability By instance	Accessits Instances Container repositories Container insiges Lambde functions	_
By container repository By Lambda function	My Account (1) ans C Actions *	
All findings Export SDOMs	C Enable Impretor across all accounts and regions using CLI. <u>Soliton</u>	
Suppression rules TOn-demand scars	Q. terch < 1 > 0	Ð
CIS scans	Account number $\nabla$ Account name $\nabla$ Status $\nabla$ Amazon EC2 scanning $\nabla$ Amazon ECR scanning $\nabla$ AWIS Lambda scanning	v
Vuinerability database search	992382419451 - O Activated O Activated O Activated O Activated Standard scan	
Account management		
▼ General settings		
EC2 scanning settings ECR scanning settings		
Usage		
Video tutorials		
What's New 🚹		
Switch to Inspector Classic 🖾		
🔁 Cleard Proli	@ 2024, Ansaon Web Senders, Inc. or Int at Milates. Privacy Terms C	lookie proforances

Figure 194 – Account Management

60. Select an assessment template (e.g. **Common Vulnerabilities and Exposures**) and click **Next**:



Figure 195 – Scan Type

61. Configure any optional scope downs and advanced assessment settings (or leave as default) and click **Next**:

- → I Impo \$ II	CIS schedules > lab-scan × C a a b ttps://us-east-2.console.aws.ama rt bookmarks N Kall Linux & Kall Tools ▲ Kall Docs N Kall Forums of tarma a com	<b>zon.com</b> /inspector/v2/home?region=us-east-2#/on-deman	67% S7			
-) npo ∎	C C C C C C C C C C C C C C C C C C C	zon.com/inspector/v2/home?region=us-east-2#/on-deman	67% 公			
npo II	rt bookmarks 🛸 Kali Linux: 🌧 Kali Tools 💆 Kali Docs 🔪 Kali Forums 🤞				ப் 🍦	,
	terrore Q, Search [MErS]	🕈 Kali NetHunter 🔺 Exploit-DB 📥 Google Hacking DB 👩 Ö	ffSec			
	Scan configuration					
	Stan configuration name					
	lab-acan					
L	Target meaurce tage					
T	Key Vake					
L	FOLSY TRONGATION TO THE					
L	Specify another tanget resource tag					
н	TR Saving and a second second					
н	Io learn-more about CB-Bendmank lends explate the documentation. Learn more 🖉					
н	LEVEL_1 *					
н	Target accounts					
н	O Self (992382419451) O Specify accounts					
н						
н	Schedule Info					
L	One time scan     Son will sur ofter creation is complete.     Son will sur ofter creation is complete.					
н						
н	Reports Some will an stiane an schedule until concelled.					
	Horibly *					
	On day					
	Wednesday					
	Start time Time zone					
н	01:00 UTC *					
н	Use 24-hour format timestamp (Mcrew)					
	Scan configuration tags					
	Key 🖤 Value 🔻					
	Na scan comfiguration tass					
	No scan configuration tags to display.					
	Central Serve					

Figure 196 – Scan Configuration

- 62. Review the details on the final page, enter an Assessment name, and click **Start** assessment.
- 63. Now, let us look at the AWS CloudTrail setup. Open the CloudTrail service within the AWS console:



Figure 197 – CloudTrail Console

64. Click Create trail:



Figure 198 – Getting Started with CloudTrail

- 65. Enter a Trail name and optionally specify Tags.
- 66. For Storage location, create or choose an existing S3 bucket to store logs.
- 67. Click Next.
- 68. On the next page, click **Next** again to start logging using the default event selectors:

٠	CloudTrail   us-east-2	× SI Instance details   EC2   up × +												
		🙆 🔿 👌 🕫 https://us-east-2.console.aws.amazon.com/cloudtrail/home?region=us-east-2.tt/create 💵 🛱 👳 🖄												
	🕀 Import bookmarks 🕆 Kali Linux 💰 Kali Tools 🍷 Kali Dools 🍷 Kali Forums 🚓 Kali NetHunter 🍬 Exploit-DB i 👟 Google Hacking DB 👘 OffSec													
aws.	🖩 Services 🔍 Second	(Ar-s)	4	0	⊜   ono	• Indo	(Jah 🕈							
= 0	) Introducing CloudTrail Lake CloudTrail Lake lets you query multiple out						0							
	Cloudfink > Create trail													
	Choose log events													
	step 2 Choose log events	Connection was a second of the connect and the annex and the annex and the annex and the ord dwaps upply [2]												
	say a Review and create	Descrit type           Shares for year wants is by           Brancement worth         Interaction of the processor of the procesor of the procesor of the processor of the procesor of the proceso					l							
		Hanagement events wie Management to the America data memproval question performed in management and an exact in your Arth accurac.  (a) The additional charges apply to be memogement events on their local because this to your first capy of mengangement events.												
		All Activity Uncer on exceedences or under balage Theorem on exceedence or under balage Theorem on the operation of the operation the operati												
		Gaussi Previews												



69. Review the trail details and click **Create trail** to complete setup:

<ul> <li>♦</li> <li>●</li> <li>●</li> <li>Imp</li> <li>●</li> <li>●<th></th><th></th><th colspan="9">CloudTrail   us-east-2 — Mozilla Firefox</th><th></th><th></th><th>8</th></li></ul>			CloudTrail   us-east-2 — Mozilla Firefox											8
← ~ -Ð imp @vs	Cloud Frait   us-east-2	🛛 🖸 Instance details   I												
+Ə imp	→ ơ ŵ	OB a≅ https://us-e		e.aws.amazor				☆				÷		
eus = 0	oort bookmarks 🔌 Kali	Linux 🍙 Kali Tools 🚊 Kali I	DB 🐞 Google Hacking DB											
= 0	🔛 territors 🔍 Sesival		(Al+5)						Ø	- 4 - C	•	oliu •	ander,	140 <b>*</b>
	ntroducing Cloud Trail Lake DoudTrail Lake lets you query multiple ex	wet fields in your logs, across all regions, for i	auditing and analysis.	Learn more 🗹									×	@ 6
1	Journal > Counts tool													
	Step 1 Choose trail attributes	Review and create												
	Surp. 2	Step 1: Choose trail attributes				Edit								
	Step 2	General details												
	Beales and create	Tosi name Lub-trail Hult-region tosi Yes Apply-tosi to my organization Net availed	Tail log location ave-cloudtral- logs-9925024194 WSLogs/9925024 Log the SSE-HHS- Enabled AMS KMS log alla setise-lob-lone	151-3347ad05;M 119451 encryption	Log Me validation Drabled SVS notification delivery Disabled									
		CloudWatch Logs												
		Log group www.cloudtraiHoge-892302c19451-73	edoc_lab											
		Tags (1)												
			Value											
	sector-lab lab-trail													
		Step 2: Choose log events		Edit										
		Management events												
		No additional charges apply to management events.	se this is your first copy of											
5 - 0-	4 1000	API activity AU		Exclude AWS KIMS No Exclude Amazon P No	events 105 Data //H events			0.0014 (month)						

Figure 200 – Creating a Trail

70. The Inspector assessment will now run against the defined EC2 instance(s), while CloudTrail will begin recording management events for monitoring.

This lab provides a foundational understanding of how to utilize AWS tools for ensuring cloud security. It covers the deployment of resources and the configuration of native AWS security services. Adapting this lab to another cloud provider would involve similar concepts but would use the specific tools and services provided by the respective cloud platform (e.g., Azure Security Center, Google Security Command Center).

Layered cloud-native tools extend security visibility, data protection, and threat prevention to reduce risk introduced by cloud adoption.

## Cybersecurity governance and compliance tools

Cybersecurity governance and compliance are critical components of an organization's overall security posture, ensuring that security practices align with business objectives

and regulatory requirements. The lab below focuses on the implementation and usage of **governance, risk management, and compliance** (**GRC**) tools.

## Lab: Implementing and configuring a GRC tool (using an open-source GRC tool like Eramba)

Eramba is a comprehensive and intuitive integrated risk management platform designed to help organizations streamline and automate their GRC processes. It provides a centralized framework for managing risks, controls, audits, incidents, and compliance requirements across various domains, including IT, finance, operations, and security. With Eramba, organizations can gain a holistic view of their risk landscape, assess and prioritize risks, implement effective controls, and monitor compliance with internal policies and external regulations. The platform offers a user-friendly interface, customizable workflows, and robust reporting capabilities, enabling teams to collaborate effectively, make informed decisions, and demonstrate compliance to stakeholders and auditors. Eramba's modular architecture allows organizations to tailor the solution to their specific needs, integrating with existing tools and systems to create a seamless GRC ecosystem. Whether you are a small business or a large enterprise, Eramba empowers you to proactively manage risks, optimize controls, and drive a culture of continuous improvement in your governance and compliance efforts.



Figure 201 – Eramba

The prerequisites are:

- A virtualization platform (e.g., VirtualBox, VMware) to host the GRC tool.
- A virtual machine (VM) or container with a supported operating system (e.g., Ubuntu, CentOS). In this lab I will be installing on Debian 12.
- Installation of Docker
- Download the installation package for an open-source GRC tool like Eramba. The community edition and install instructions can be found at https://www.eramba.org/get-community.

Let us look at the steps.

- 1. Prepare a VM or a container within your virtualization platform.
- 2. Allocate sufficient resources (CPU, memory, storage) based on the requirements of the GRC tool and intended usage.
- 3. Configuring the Docker APT Repository https://docs.docker.com/engine/install/debian/.
- 4. On a new host system, the Docker Engine apt repository must be initialized before installing Docker for the first time. This involves setting up the repository configuration to enable installing and updating Docker packages later on.
- 5. The process consists of adding Docker's GPG key to verify package integrity and then adding the stable apt repository definition from where Docker can be installed. With the repository configured, the Docker Engine can then be installed from the maintained repository instead of upstream sources. Subsequently, Docker can be kept up-to-date by upgrading packages from the same apt repo.
- 6. By setting up the optimized Docker apt repository on Debian-based systems before installation, it streamlines engine deployment and patching through a trusted and consistent package source going forward:

```
sudo apt-get update
sudo apt-get install ca-certificates curl
```



7. To install the latest version of the Docker Packages, run:



- 8. Once Docker Engine installation completes, verify it is working properly by running a simple test container.
- 9. Launch the standard Docker hello-world image to confirm the docker daemon starts correctly and can successfully pull images, run containers, etc:

## docker run hello-world

- 10. The output should show the test message and exit cleanly without errors.
- 11. Running this basic Docker image test provides a quick validation that the Engine was installed correctly and has connectivity to access images along with fundamental container runtime functionality. The ability to fetch and run this test hello-world image confirms that the Docker setup was successful.
- 12. Let us now look at Eramba's installation. Eramba provides a Docker deployment script that installs a container stack running the Eramba GRC platform and its dependencies:
  - MySQL (Database)
  - Redis (Caching)
  - Eramba (Web Application)
  - Cron (Batch Jobs)

It utilizes 3 persistent volumes:

- o data: Holds Eramba application data
- o app: Stores Eramba application files
- o db-data: Contains MySQL database files
- 13. To deploy Eramba with Docker, run:

## git clone https://github.com/eramba/docker

- 14. By leveraging Docker to containerize the application and its components, Eramba can be deployed consistently across environments without dependency hassles.
- 15. After cloning the Eramba Docker GitHub repository, navigate into the docker directory:

### cd docker

- 16. Update default database credentials
- 17. Edit .env file using Nano or Vi:

#### nano .env

- 18. Change DB PASSWORD and MYSQL ROOT PASSWORD variables
- 19. Validate external connectivity

- 20. Containers must reach Eramba servers for registration, updates etc.
- 21. Test connectivity with:

## curl https://support-v3.eramba.org/ping.html

Offline mode is unsupported.

- 22. By customizing credentials in .env and ensuring connectivity to Docker Hub and Eramba repositories, the containers can securely access private dependencies while checking for updates. Offline deployments are currently unavailable - external access is required.
- 23. You are now Ready to run the Docker Compose command:

## docker compose -f docker-compose.simple-install.yml up -d

- 24. Follow the installation guide provided by Eramba, <u>https://www.eramba.org/</u>, to set up the GRC platform.
- 25. Login screen: You should now be able to login to eramba using https://{IP ADDRESS}:8443
- 26. The default login credentials are:
  - Username: admin
  - Password: admin

Eramios	
🛓 admin 💧	
A 💳	
Delay by Control 1	
- Denaule (English)	
Login +	
Copyright 2011-2024 erambe Ltd	
Do schema version 20230918084154	
Community	

Figure 202 – Eramba Login

- 27. After login you will be asked to change the following:
  - o Default Password
  - Default Admin Email:

Change your credentials
Please enter your new email and password boltze
sector
THE PASSWORD MUST BE BIOLDAG, IT MUST CONEST OF ALTHANUMERIC CHARACTERS WITH
ALCIONE UNE NUMBER AND UPPERMIT. INCLUER INFORMATION (Syndrywar) OWAW/CERS
Company

Figure 203 – Eramba Initial User

28. Community users will be asked to insert their email for verification.

Token Validation We have sent a taken from our email no repuipermentation og to your email. Back Back	

29. A validation token will be sent to the email specified:

Figure 204 – Token Validation

30. With the installation of the system, you can begin building out your GRC process including report generation and more. Since the installation is the community addition, there is some limitation to what can be done but there is a lot of that can be learned and leveraged through Eramba. You can do a deep dive on the aspects of Eramba at <a href="https://www.eramba.org/learning">https://www.eramba.org/learning</a>:



Figure 205 – Eramba Dashboard

- 31. Let us now see the Compliance Management setup. Import compliance packages relevant to your organization (e.g., ISO 27001, GDPR, PCI-DSS) into Eramba.
- 32. Map the compliance requirements to your organization's processes and controls.
- 33. Let us look at risk assessment frameworks. Define a risk assessment methodology in Eramba (e.g., qualitative, quantitative).
- 34. Create risk assessment criteria, such as likelihood and impact scales.
- 35. Now, policy management. Use Eramba to draft, review, and approve security policies.
- 36. Set up a policy review schedule and reminders for periodic updates.
- 37. Create a catalog of security controls within Eramba.

- 38. Link the controls to applicable policies and compliance requirements.
- 39. Configure the incident management module in Eramba.
- 40. Set up incident reporting channels and response plans.
- 41. Schedule internal audits within Eramba to assess compliance with policies and standards.
- 42. Monitor compliance status through dashboards and automated alerts.
- 43. Generate reports for different stakeholders (e.g., IT, executives, auditors).
- 44. Customize dashboards to highlight key compliance metrics and risk status.
- 45. Document and assess third-party relationships and risks within Eramba.
- 46. Integrate third-party compliance information into the overall risk assessment.
- 47. Plan and track security awareness training sessions.
- 48. Record employee training status and schedule reminders for recurring training.
- 49. Use feedback and audit results to improve security practices.
- 50. Update risk assessments, controls, and policies accordingly.
- 51. If this was a test implementation, decommission the environment properly.
- 52. Document the configuration process, how the tool is used, and any issues encountered or insights gained during the lab.

This lab introduces the participant to the fundamental aspects of using a GRC tool for cybersecurity governance and compliance management. By importing compliance frameworks, creating policies, managing risks, and establishing auditing and reporting mechanisms, the participant gains hands-on experience that is crucial for managing cybersecurity governance and compliance in a real-world environment.

These tools provide centralized visibility and management of critical security program artifacts for consistency, accuracy, and compliance.

## Penetration testing and red team tools

A lab setup for penetration testing and Red Teaming involves configuring a controlled environment where security professionals can safely conduct attacks against systems, networks, and applications to identify vulnerabilities. This lab will demonstrate the use of Kali Linux, a popular penetration testing platform, alongside tools such as Metasploit for vulnerability exploitation and Nmap for network scanning.

## Lab: Penetration testing with Kali Linux and Metasploit Framework

Penetration testing, also known as pen testing or ethical hacking, is the practice of simulating real-world cyber attacks on computer systems, networks, and web applications to identify and exploit vulnerabilities before malicious actors can take advantage of them. Kali Linux, a powerful and widely used open-source operating system, is specifically designed for digital forensics and penetration testing. It comes pre-installed with a vast array of security tools, including the renowned Metasploit Framework, which is a powerful and versatile tool used for conducting penetration testing, exploit development, and vulnerability analysis. Together, Kali Linux and Metasploit Framework provide pen testers and security professionals with a comprehensive arsenal of tools and techniques to assess and strengthen the security posture of their systems, networks, and applications.



Figure 206 – Kali Website

The prerequisites are:

- A virtualization platform (e.g., VMware, VirtualBox) with a virtual network configured for the lab environment.
- Download the Kali Linux virtual machine image from the official website, https://www.kali.org/.
- Target VMs for penetration testing, like Metasploitable or OWASP Broken Web Applications, which are intentionally vulnerable.
- Permission and ethical guidelines established if not using provided vulnerable applications and in a real-world scenario.

Let us look at the steps beginning with the Kali Linux setup:

- 1. Import the Kali Linux VM into your virtualization platform.
- 2. Configure the network settings to ensure it is in the same virtual network as the target VMs but isolated from your production network.
- 3. Import the target VMs (like Metasploitable) into the virtualization platform:



Figure 207 – Metasploitable VM

4. Verify the network configuration for connectivity with the Kali Linux VM:

applicable law.
To access official Ubuntu documentation, please visit: http://beln.ubuntu.com/
No mail
nsfadmin@metasnloitable:~\$ ifconfig
etho Link encan: Ethernet Huaddr hc:24:11:e7:92:c7
inet addr: 192.168.2.192 Bcast:192.168.2.255 Mask:255.255.255.0 inet6 addr: fe80::be24:11ff:fee7:92c7/64 Scope:Link UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1 RX packets:2230 errors:0 dropped:0 overruns:0 frame:0 TX packets:1388 errors:0 dropped:0 overruns:0 carrier:0 collisions:0 txqueuelen:1000 RX bytes:127199 (124.2 KB) TX bytes:0 (0.0 B)
<pre>lo Link encap:Local Loopback inet addr:127.0.0.1 Mask:255.0.0.0 inet6 addr: ::1/128 Scope:Host UP LOOPBACK RUNNING MTU:16436 Metric:1 RX packets:135 errors:0 dropped:0 overruns:0 frame:0 TX packets:135 errors:0 dropped:0 overruns:0 carrier:0 collisions:0 txqueuelen:0 RX bytes:40109 (39.1 KB) TX bytes:40109 (39.1 KB)</pre>
nsfadmin@metasploitable:~\$

Figure 208 – ifconfig of Metasploitable VM

- 5. Start the Kali Linux VM and open the terminal.
- 6. Use Nmap to perform a network scan to discover active hosts and open ports:

```
sudo nmap -sV -T4 192.168.X.X/24
```

7. Analyze the output for potential targets:

Host is u	ip (0.	00012s laten	ty).
PORT	STATE	SERVICE	VERSION
21/tcp	open	ftp	vsftpd 2.3.4
22/tcp	open	ssh	OpenSSH 4.7p1 Debian Subuntu1 (protocol 2.0)
23/tcp	open	telnet	Linux telnetd
25/tcp	open	smtp	Postfix smtpd
53/tcp	open	domain	ISC BIND 9.4.2
B@/tcp	open	http	Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp	open	rpcbind	2 (RPC #100000)
139/tcp	open	netbios-ssn	Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp	open	netbios-ssn	Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp	open	exec?	
513/tcp	open	login?	
514/tcp	open	tcpwrapped	
1099/tcp	open	java-rmi	GNU Classpath grmiregistry
1524/tcp	open	bindshell	Metasploitable root shell
2049/tcp	open	nfs	2-4 (RPC #100003)
2121/tcp	open	ftp	ProFTPD 1.3.1
3306/tcp	open	mysql	MySQL 5.0.51a-3ubuntu5
5432/tcp	open	postgresql	PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp	open		VNC (protocol 3.3)
6000/tcp	open	X11	(access denied)
6667/tcp	open	irc	UnrealIRCd
8009/tcp	open	ajp13	Apache Jserv (Protocol v1.3)
8180/tcp	open	http	Apache Tomcat/Coyote JSP engine 1.1
And the second second second	cc. R	C:24:11:E7:9	2:C7 (Unknown)

Figure 209 – NMAP scan of Metasploitable VM

- Use a tool like OpenVAS on Kali Linux to scan the target VMs for known vulnerabilities. This can be a useful additional information gather step, but depending on the rules of engagement, may be something that could create too much noise for the engagement.
- 9. Review the vulnerability scan results, if appropriate, to prioritize targets for exploitation.
- 10. Open the Metasploit console on Kali Linux by typing msfconsole in the terminal:



Figure 210 – Metasploit Console on Kali

11. Search for appropriate exploits for the vulnerabilities found, for example, target vsftpd version 2.3.4:

search type:exploit platform:[platform] [vulnerability
details]

12. Configure and launch the exploit against a chosen target:

```
use exploit/[exploit name]
set RHOSTS [target IP]
set PAYLOAD [payload name] #This may not be necessary
as with the example shown
exploit
```

13. If successful, a shell or user session should be opened on the target system:



Figure 211 – Metasploitable VM Remote Reverse Shell via Metasploit

- 14. Document any sensitive information found or actions taken.
- 15. Document every step taken during the exploitation phase, including the output of each command.
- 16. Create a detailed report with the findings, including how each vulnerability was exploited and potential recommendations for remediation.
- 17. Reset the target VMs to their original state to repeat the lab or for other exercises.
- 18. Review and terminate any processes or sessions started on Kali Linux.
- 19. Always ensure that penetration testing is conducted within legal boundaries and with proper authorization.
- 20. Adhere to a code of ethics to respect privacy and avoid data damage.

This lab is a fundamental exercise for understanding the penetration testing process using tools commonly found in Kali Linux. It's crucial to conduct such labs in a controlled environment and to understand the potential impact of these tools and techniques in real-world scenarios. For advanced users, the lab can be expanded to include wireless network exploitation, web application attacks, and more sophisticated Red Team simulations.

Architects should leverage penetration testing toolkits judiciously based on scope and legal considerations to uncover security gaps without putting production systems at risk.

# Automation and orchestration tools

Automation and orchestration tools are essential for improving efficiency, consistency, and reliability in cybersecurity operations. They allow for the coordination of complex workflows across multiple systems and processes. In this lab, we'll set up a basic security automation and orchestration platform using StackStorm, an open-source automation engine that connects your apps, services, and workflows.

## Lab: Security automation with StackStorm

StackStorm is an open-source event-driven automation platform designed to simplify the automation of operational workflows and processes. It enables organizations to create and execute automated actions, known as **workflows**, in response to various events or triggers, such as monitoring alerts, system events, or user-defined conditions. StackStorm's architecture is built around three core components: sensors, rules, and actions. Sensors are responsible for monitoring and detecting events, rules define the logic and conditions for triggering actions, and actions are the automated tasks or operations performed in response to events. With its powerful rule engine, StackStorm allows for complex decision-making and conditional execution, making it a versatile solution for automating a wide range of IT operations, security operations, and business processes.



Figure 212 – StackStorm Website

You can access StackStorm here: https://stackstorm.com/.

The prerequisites include:

- A virtualization platform (e.g., VMware, VirtualBox) to host the virtual machines. StackStorm offers an OVA for a preinstalled VM but does require additional setup for use with Vagrant. You can see more at https://docs.stackstorm.com/install/vagrant.html.
- A virtual machine image with a compatible Linux distribution (e.g., Ubuntu 20.04 LTS). The screenshots will be based on Ubuntu 20.04.
- Internet access for downloading StackStorm and other necessary software components.
- Basic familiarity with Linux command-line operations and YAML syntax.

Let us look at the steps:

- 1. Set up a virtual machine within your virtualization platform and install a compatible Linux distribution.
- 2. Assign appropriate resources to the VM (e.g., at least 2 vCPUs, 4GB of RAM, and 20GB of disk space).
- 3. Access the VM via SSH or the console interface.
- Follow the official documentation to install StackStorm. This typically includes running a script that installs StackStorm and its dependencies called the Quickstart Script:

```
bash <(curl -sSL
https://stackstorm.com/packages/install.sh) --
user=st2admin --password=Ch@ngeMe
```



Figure 213 – Installation of StackStorm

5. Once the installation is complete, log into the StackStorm web interface using the credentials set during installation.



Head to https://YOUR HOST IP/ to access the WebUI:

#### Figure 214 – StackStorm Login

- 6. Script sets the default password for the st2admin user to Ch@ngeMe.
- 7. Familiarize yourself with the interface and the basic concepts of StackStorm, such as packs, actions, rules, and workflows:

		ckSto driven aut		 e) STORY								
~ 1												
	Ē TUE,							Installs or upg URL or a shor the actions, or rebool of som	racles a pack into local co thame matching an index moors and rules from the elst2 services.	entent repository, centry, Will down pack, Note that i	sither by load pac totall rec	
0			paeles.mstall cector(cf.27)									
•		19 44 28	consummote hosts="127.0.0.1".cmd+".uname=e"	5	tanual 4 st2adimin			REBUN				
•			core.local criss/ane-R*		tanual AstZodenin				Successfed			
h												
									) 2 2 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1			

Figure 215 – StackStorm Dashboard

8. StackStorm uses packs to group actions, sensors, and rules. Install a pack for a common integration (e.g., GitHub, Slack) from the StackStorm Exchange to use as a base for automation This can be installed from the WebUI or through the cli:

st2	pack	install	github
			-,



## (a) Install Github Module Pack

StackStorm Event-driven automation		U) ED EO EO EO Hefrem actions filles mados traduces	
~ Packs Her		github Githibur/Avgalian	
excel			
Read and White Excel spread sheets	1.0.0		
EXOS Actions for managing Extreme Networks EXOS devices			
freeye Finifye CM Series Integration			
foremen Interact with Foreman (P1 v2		Emeil info@esecksom.com Knywerst fothale forthebestarstrad fot form standaled	
fortinet Fortinet Firewall		RepolURL https://github.com/StackSterm-Exchange/Mackatorm-github	
fpm. fam package for building system packages (rpm, diab, python, gam, etc.)			
freeipa FreeiPA Integration Pack			
freight. Treight			
ghost2logger Sistikaj ercégoint for matchirule criteria			
pit Ge SCM	2.0.0		
griffrado Bidhiub intergrafices			
gittaŭ Galaŭ Rest API			
google 92 contant pack containing google integrations			
opo Peck for working with GPG.			
GreyNolae GreyNolae provides information on devices observed mass-sconning th			

#### Figure 216 – Install Module

9. Test an action from the installed pack to verify StackStorm is functioning properly. For example, if you installed the GitHub pack, you can list your repositories with an action:

st2 action list --pack=github

Certainly! After installing StackStorm and integrating it with various packs (collections of pre-built actions), it's essential to test and verify that the installed

packs and their actions are functioning correctly. One way to do this is by running a specific action from the installed pack.

10. In your example, you've mentioned installing the GitHub pack, which provides actions related to GitHub operations. To test if this pack is functioning properly, you can use the st2 action list command to list all the available actions within the GitHub pack.

#### st2 action list --pack=github

This command will display a list of all the actions available in the GitHub pack. You can then select a specific action from the list to test it. For instance, if you want to list your GitHub repositories, you can run the following command:

#### st2 action run github.repos list

This will execute the github.repos\_list action, which should retrieve and display a list of your GitHub repositories.

If the action runs successfully and outputs the expected result (e.g., a list of your GitHub repositories), it confirms that StackStorm is functioning correctly, and the GitHub pack is properly installed and integrated.

You can follow a similar approach for testing actions from other installed packs. Simply list the available actions using st2 action list -pack=<pack\_name>, select an action you want to test, and run it using st2 action run <action ref>.

By testing different actions from various packs, you can ensure that StackStorm is functioning as expected and can automate various tasks and workflows across different systems and services:

	\$ st2 act	ion listpack-github	
ref	pack	description	
github.add_comment	lgithub	Add a comment to the provided issue / pull request.	
github.add_status	github	Add a commit status for a provided ref.	
github.add_tean_membership	github	Add (and invite if not a member) a user to a team	
<pre>l github.check_deployment_env</pre>	github	Check if deployment event applies to this server.	
github.create_deployment	github	Create a new deployment for a GitHub repository	
github.create_ceployment_status	github	Create a new deployment Status for a GitHub repository	
github.create_file	github	Create a file in this repository.	
github.create_issue	github	Create a Github issue.	
github.create_pull	github	Creates a Github pull request. Example:	
		siz run github.create_putt user-user_or_org repo-nyreponame	
		base-master	
		i basemas ter	
github.create release	I github	Create a new velease for a GitHub venository D multible offerense	
github delete branch protection	github	Deletes branch protection	
github.deployment event	1 github	Process an github deployment event and install a pack if the	
		environment matches.	
github.get_branch_protection	github	Gets branch protection details for given repo and branch.	
github.get_clore_stats	l github	Retrieve clone statistics for a given repository	
github.get_contents	github	Gets the contents of a file or directory in a repository.	
github.get_deployment_statuses	github	Get the statuses of a deployment for a GitHub repository	
githüb.get_issue		Retrieve information about a particular Github issue.	
github.get_pull	github	Retrieve information about a particular Github pull request.	
github.get_traffic_stats	github	Retrieve traffic statistics for a given repository	
github.get_user	github	Get a user from the Github user database	
github.latest_release	github	List the latest release for a GitHub repository	
github.list_deployments	github	List deployments for a GitHub repository	
gichub.cist_issues	granup	r Retrieve a tist of issues (including pull requests) for a	
aithch list pulls	a ithur	Patricular representative. Patricular representative.	
greater cist_ports	L gathub	I list releases for a Gillub requests for a particular repository.	
github.list teams	Igithub	List teams in organization	
github.morge_pull	github	Morge a pull request.	
github.review pull	github	Review a Github pull request given its PR id.	
github.store pauth token	github	Store a users GitHub OAuth token.	
github.update_branch_protection	github	Updates branch protection.	
github.update_file	github	Update a file in this repository.	
	+		
secdocijstacikstom-ubuntu2004-kvn:-	\$		

### Figure 217 – Action List for Github Pack

More information can be found at https://docs.stackstorm.com/start.html.

- 11. Now, let us look at workflow design and sensors/triggers. Create a simple workflow using the Orquesta workflow engine built into StackStorm. Write a YAML file that defines the workflow. There are great examples provided by StackStorm to help you get started and learn the workflow process at <a href="https://docs.stackstorm.com/orquesta/start.html">https://docs.stackstorm.com/orquesta/start.html</a> and sensors/triggers at <a href="https://docs.stackstorm.com/sensors.html">https://docs.stackstorm.com/orquesta/start.html</a> and sensors/triggers at <a href="https://docs.stackstorm.com/sensors.html">https://docs.stackstorm.com/sensors.html</a>.
- 12. Monitor the StackStorm execution history in the web interface to see the results of your workflow.
- 13. Check the logs for any errors or issues:

```
tail -f /var/log/st2/st2*.log
```

14. Upon completion of the lab, remove any sensitive information from the StackStorm system if necessary.

15. Document the workflow creation process, action execution steps, rule definitions, and any troubleshooting steps taken during the lab.

This lab introduces the basic concepts of security automation using StackStorm. It covers the installation and initial configuration of the automation tool, the use of packs for integration, the design and execution of a simple workflow, and the creation of automation rules. Upon completion, participants will have a foundational understanding of how to leverage automation for cybersecurity tasks.

SOAR platforms enable architects to connect disparate tools into a unified security ecosystem while leveraging automation for improved efficiency, consistency, and response times.

The taxonomy and associated examples are not exhaustive, as the domain of cybersecurity is dynamic and continuously evolving. New categories or tools may emerge as technologies and threats progress. The integration and interoperability of these tools are also critical, as cybersecurity architects must ensure that disparate security systems can work together seamlessly to provide a comprehensive defense-indepth strategy.

# Summary

Based on the provided list of labs and exercises, it appears to cover a comprehensive range of topics and practical implementations related to cybersecurity and information assurance. The labs and exercises cover various aspects of security, including threat modeling, intrusion detection and prevention, firewalls, SIEM solutions, antivirus software, endpoint detection and response, identity and access management, data encryption, vulnerability scanning, security configuration management, patch management, digital forensics, incident response, application security testing, cloud security, GRC tools, penetration testing, and security automation.

These hands-on labs and exercises provide valuable opportunities to gain practical experience and develop skills in various security tools and technologies. Participants can learn about threat modeling using tools like Microsoft Threat Modeling Tool and OWASP Threat Dragon, configure and deploy intrusion detection/prevention systems with Snort, set up and configure firewalls using OPNsense, implement SIEM solutions with Graylog, and deploy antivirus software like ClamAV.

Additionally, participants can explore endpoint detection and response with Wazuh, configure IAM solutions like Keycloak, implement data encryption using VeraCrypt, perform vulnerability scanning with OpenVAS, and practice security configuration management with Ansible. The labs also cover patch management with WSUS, digital forensics using The Sleuth Kit and Autopsy, incident response with Security Onion, static and dynamic application security testing with SonarQube and OWASP ZAP, respectively.

Furthermore, participants can gain experience in securing cloud environments with AWS, implementing GRC tools, conducting penetration testing with Kali Linux and Metasploit, and automating security tasks with StackStorm.

Overall, these labs and exercises provide a comprehensive and practical learning experience, equipping participants with the knowledge and skills necessary to address various cybersecurity challenges and implement effective security measures across different domains.