REPORT
Incident Handler's Log

v.1.9.4

Author:

Eldon Gabriel

August 12th 2025

TABLE OF CONTENTS

REVISION HISTORY

Version	Date	Author	Description of Changes
v1.0.0	02/16/2025	Eldon G.	Initial draft.
v1.1.1	02/16/2025	Eldon G.	Recorded new incident: Healthcare clinic security breach.
v1.1.2	02/20/2025	Eldon G.	Updated the incident Handler's log with the function incident report tables.
v1.1.3	02/20/2025	Eldon G.	Added new reports to the incident handler's log.
v1.1.4	02/22/2025	Eldon G.	Incorporated the likelihood of threat event rating.
v1.1.5	02/23/2025	Eldon G.	Updated reports with the latest Python for cybersecurity activity.
v1.1.6	02/24/2025	Eldon G.	Updated reports with the latest Python for cybersecurity activity.
v1.1.7	02/27/2025	Eldon G.	Updated reports with the latest Python module on strings, lists, and regular expressions.
v1.1.8	03/01/2025	Eldon G.	Added new Python automation for cybersecurity tasks.
v1.1.9	03/02/2025	Eldon G.	Added Cyber Kill Chain & MITRE ATT&CK research report.
v1.2.0	03/03/2025	Eldon G.	Added Enterprise Security Software Types report.
v1.2.1	03/13/2025	Eldon G.	Logged covert social media account creation for OSINT operations.
v1.2.2	03/14/2025	Eldon G.	Documented search for sensitive information leaks on code repositories.
v1.2.3	03/15/2025	Eldon G.	Added passive asset mapping report using dnsdumpster.com.
v1.2.4	03/21/2025	Eldon G.	Logged phishing/spear-phishing site identification using urlscan.io.
v1.2.5	03/24/2025	Eldon G.	Logged activity using Google search techniques for threat intel.
v1.2.6	03/27/2025	Eldon G.	Logged SSL assessment activity.

REVISION HISTORY

Version	Date	Author	Description of Changes
v1.2.7	03/28/2025	Eldon G.	Logged activity on TCP port scanning using Nmap.
v1.2.8	03/31/2025	Eldon G.	Logged activity on UCP port scanning using Nmap.
v1.2.9	05/20/2025	Eldon G.	Logged VM setup delay and books read.
v1.3.0	05/20/2025	Eldon G.	Added YARA threat-hunting lab setup.
v1.3.1	05/22/2025	Eldon G.	Completed a professionally documented YARA rule.
v1.3.2	05/23/2025	Eldon G.	Wrote a YARA rule that can find itself.
v1.3.3	05/24/2025	Eldon G.	Submitted YARA rule for small portable executables.
v1.3.4	05/26/2025	Eldon G.	Created a YARA rule searching for specific strings.
v1.3.5	06/01/2025	Eldon G.	Logged virtual machine lab setup
v1.3.6	06/03/2025	Eldon G.	Logged virtual machine lab setup
v1.3.7	06/04/2025	Eldon G.	Fixed Docker daemon via reinstallation.
v1.3.8	06/06/2025	Eldon G.	Pull and run the hello-world Docker container
v1.3.9	06/09/2025	Eldon G.	Attempted OpenVAS setup; hit ARM64 issue.
v1.4.0	06/10/2025	Eldon G.	Tried pulling Greenbone images; access denied.
v1.4.1	06/11/2025	Eldon G.	Standardized structure in legacy reports.
v1.4.2	06/12/2025	Eldon G.	Retested OpenVAS; explored remote scanner setup.
v1.4.3	06/13/2025	Eldon G.	Cleaned legacy OpenVAS; started GVM build.
v1.4.4	06/14/2025	Eldon G.	Resolved GVM setup issues; GUI is live.
v1.4.5	06/15/2025	Eldon G.	Manual GVM install; Docker fails ARM64.
v1.4.6	06/16/2025	Eldon G.	Fixed gvmd lockfile; service started.
v1.4.7	06/17/2025	Eldon G.	Built and installed GVM libraries from source.
v1.4.8	06/18/2025	Eldon G.	Deployed Greenbone Docker stack on ARM64.
v1.4.9	06/19/2025	Eldon G.	Recovered GVM; prepared for scans.

REVISION HISTORY

Version	Date	Author	Description of Changes
v1.5.0	06/26/2025	Eldon G.	Configured Burp Spider for DVWA crawl.
v1.5.1	06/27/2025	Eldon G.	Brute-force login using Burp Intruder module.
v1.5.2	06/28/2025	Eldon G.	Used Dumpzilla for browser log extraction.
v1.5.3	06/29/2025	Eldon G.	Malware Lab Isolation Setup.
v1.5.4	07/01/2025	Eldon G.	PEStudio Static Analysis.
v1.5.5	07/02/2025	Eldon G.	DNS Query Analysis.
v1.5.6	07/03/2025	Eldon G.	MSAF Enrollment & Blog Draft.
v1.5.7	07/04/2025	Eldon G.	Virtual Network Modes Report.
v1.5.8	07/05/2025	Eldon G.	Virtualization and Hypervisors Report.
v1.5.9	07/06/2025	Eldon G.	WSL Installation.
v1.6.0	07/08/2025	Eldon G.	Deployed Ubuntu VM on GCP.
v1.6.1	07/09/2025	Eldon G.	Revised reports & submitted AWS lab.
v.1.6.2	07/10/2025	Eldon G.	Planned VMware lab & finalized report structure.
v1.6.3	07/11/2025	Eldon G.	Executed Fusion lab. Set up ARM64 VMs, fixed ICMP issues, and created a snapshot.
v1.6.4	07/12/2025	Eldon G.	Flagged ESXi/macOS M2 issue. Asked the instructor for an alternative method.
v1.6.5	07/13/2025	Eldon G.	Grammarly edits and section updates
v1.6.6	07/14/2025	Eldon G.	Report formatting polished
v1.6.7	07/15/2025	Eldon G.	ESXi VM connectivity test submitted
v1.6.8	07/16/2025	Eldon G.	ESXi VM test resubmitted with fixes.
v1.6.9	07/17/2025	Eldon G.	OSI vs TCP/IP report drafted.
v.1.7.0	07/18/2025	Eldon G.	Finalized the OSI vs TCP/IP report PDF.
v1.7.1	07/19/2025	Eldon G	Added router section, minor edits to report draft.

REVISION HISTORY

Version	Date	Author	Description of Changes
v1.7.2	07/20/2025	Eldon G.	Added device-OSI mapping
v1.7.3	07/21/2025	Eldon G.	Began network diagram recon
v1.7.3	07/22/2025	Eldon G.	Created static diagram with segmentation and security zones
v1.7.4	07/23/2025	Eldon G.	Attempted IPSec tunnel config, hit CLI limitations in Packet Tracer
v1.7.5	07/24/2025	Eldon G.	Diagnosed VPN tunnel issues; fixed ISAKMP key and static routes
v1.7.6	07/25/2025	Eldon G.	Debugged IPSec tunnel & built core VLAN network infrastructure
v1.7.7	07/26/2025	Eldon G.	Traced PC packet drop issue in multi-router NAT setup
v1.7.8	07/27/2025	Eldon G.	Solved NAT failure by removing no ip cef on firewall
v1.7.9	07/28/2025	Eldon G.	Repaired NAT in 3-router chain after topology & config alignment
v1.8.0	07/29/2025	Eldon G.	Fixed NAT/routing in remote branch; power-cycled routers for NAT
v1.8.1	07/30/2025	Eldon G.	Diagnosed IPSec VPN tunnel Phase 1/2 failures; fixed Layer 2 ARP issues blocking public IP connectivity.
v1.8.2	07/31/2025	Eldon G.	Restored guest VLAN internet access by fixing recursive static route; prepared for VPN tunnel setup
v1.8.3	08/01/2025	Eldon G.	Validated IPSec tunnel functionality; resolved physical and IP addressing issues; refined troubleshooting report
v1.8.4	08/02/2025	Eldon G.	Advanced VPN troubleshooting report progress; confirmed working Phase 1 & 2 tunnel with encryption verification
v1.8.5	08/03/2025	Eldon G.	Finalized and formatted VPN troubleshooting report with professional documentation and clean formatting

REVISION HISTORY

Version	Date	Author	Description of Changes
v1.8.6	08/04/2025	Eldon G.	Updated LinkedIn profile and portfolio with refined technical projects and strategic branding
v1.8.7	08/05/2025	Eldon G.	Troubleshot VLAN mismatch blocking local connectivity; confirmed IPSec VPN tunnel active despite traceroute timeouts
v1.8.8	08/06/2025	Eldon G.	Polished VPN troubleshooting documentation; expanded troubleshooting log and finalized version history
v1.8.9	08/07/2025	Eldon G.	Finalized website branding, navigation, and blog draft; updated Linktree bio for professional consistency
v1.9.0	08/08/2025	Eldon G.	Finalized blog post content and enhanced online branding; created a dynamic featured image and optimized Linktree structure for user engagement.
v1.9.1	08/09/2025	Eldon G.	Completed foundational CompTIA Network+ training on networking fundamentals and physical networks with strong assessment results.
v1.9.2	08/10/2025	Eldon G.	Shifted focus to University of Colorado's Computer Security & Systems Management course; completed virtualization and security modules with high grades.
v1.9.3	08/11/2025	Eldon G.	Refined BYOD security report and finalized a comprehensive BYOD contract template; developed targeted promotional content for Linktree.
v1.9.4	08/12/2025	Eldon G.	Promoted BYOD report and contract template via Linktree; optimized user experience and mobile accessibility; completed University of Colorado security course with 95.5%.

SECTION 1.0 INCIDENT REPORTS

Ransomware Attack: Encrypted Medical Records & Business Disruption

Date: 02/16/2025

Entry #: 1

Likelihood: Low

Severity: Low

Status: Escalated: The incident requires further attention or higher-level supp…

Description: A small clinic faced a ransomware attack on Tuesday around 9 a.m. Workers couldn't reach key files like patient records. A message popped up asking for money to unlock the files. The attack started with phishing emails carrying malware. This malware locked the clinic's files. This stopped them from doing business. The clinic shut down its computers. They then called the authorities for help.

Tools/System Involved:

The 5 W's:

- **Who:** An organized group of unethical hackers
- **What:** Hackers used a phishing attack to get into the company's system.
- **When:** On Tuesday at 9:00 am.
- **Where:** At a U.S. healthcare clinic
- **Why:** The hackers used a phishing attack to get into the company's system. They then installed ransomware. This software locked all the company's files. The hackers want money. They left a ransom note. It demands a large payment for the key to unlock the files.

Additional Notes:

- What steps can prevent similar problems later?

Ransomware Attack: Encrypted Medical Records & Business Disruption

Date: 02/16/2025

- Should the company pay the ransom money?
- Is the decryption key worth its price?
- What security is now in place at the clinic?
- Does the company offer security training each quarter?

Failed Login Attempt Detected Incident Report

Date: 02/24/2025

Entry #: 2

Likelihood: High

Severity: Moderate

Status: Escalated: The incident requires further attention or higher-level supp…

Description: A security alert was triggered by several failed login tries on the ejones account. These attempts came fast from an outside IP address. The IP address was marked as risky. User login info was checked for any problems.

Tools/System Involved: Python Script (Failed Login Detection)

The 5 W's:

- **Who:** User **ejones**, external attacker
- **What:** Multiple failed login attempts from an external IP address
- **Where:** Internal network, targeting user account **ejones**
- **When:** Detected at 8:50 AM
- **Why:** Attempt to gain unauthorized access via brute-force attack

Phishing Email Attempt Detected Incident Report

Date: 02/24/2025

Entry #: 3

Likelihood: Moderate

Severity: High

Status: Escalated: The incident requires further attention or higher-level supp…

Description: An employee, jsmith@company.com, got a phishing email. The email looked like a real system alert. It tried to grab login details. The email had a bad link. The link asked for private data.

Tools/System Involved: Python Script (Phishing Detection and Alerting)

The 5 W's:

- **Who:** Employee **jsmith**, external attacker
- **What:** Phishing email disguised as a system notification
- **Where:** Sent to **jsmith@company.com**
- **When:** Received at 10:00 AM
- **Why:** The attacker attempted to collect sensitive credentials using a fake login page

Malware Infection Detected on Workstation Incident Report

Date: 02/24/2025

Entry #: 4

Likelihood: Low

Severity: High

Status: Escalated: The incident requires further attention or higher-level supp…

Description: Endpoint security software found malware on workstation WS-004. A system scan caught it during a check. The malware then tried to contact a server outside the network.

Tools/System Involved: Python Script (Malware Detection and Isolation)

The 5 W's:

- **Who:** User **WS-004**, external attacker
- **What:** Malware infection detected
- **Where:** On **WS-004**, affecting internal systems
- **When:** Detected at 11:10 AM
- **Why:** Attempt to infect the system for remote control and data theft

Unusual Outbound Traffic from Database Server Incident Report

Date: 02/24/2025

Entry #: 5

Likelihood: Moderate

Severity: Moderate

Status: Escalated: The incident requires further attention or higher-level supp…

Description: DB-01 showed strange outgoing traffic; this could mean someone tried to steal data. The network traffic watch found lots of data sent to an outside IP address.

Tools/System Involved: Python Script (Network Traffic Monitoring and Data Flow Analysis)

The 5 W's:

- **Who:** Database Server **DB-01**, external attacker
- **What:** Abnormal outbound traffic detected, potential data exfiltration
- **Where:** Server **DB-01**, outbound to external IP
- **When:** Detected at 1:05 PM
- **Why:** Attempt to extract sensitive data through a misconfigured firewall

SECTION 2.0 LOG ANALYSIS

Network Traffic Analysis Report: Packet Analysis Using Wireshark

Date: 02/16/2025

Entry #: 1
Tools/System Involved: Wireshark
Likelihood: Low
Severity: Low
Status: Resolved: The issue has been fixed or addressed.
Description: I'm using Wireshark to check network traffic. Wireshark looks at data sent between users and websites. I find IP addresses to see where data comes from and goes. I check protocols and data packets for security problems. I open files in Wireshark to inspect them. I use filters to focus on certain IPs. I also look at DNS and TCP packets. The work means I must know packet layers. I filter traffic to find key network data.
Conclusion: I looked at network traffic to find important details. I found IP addresses, protocols like TCP and DNS, and payload data. Hands-on practice boosted my grasp of packet analysis. I built on skills I learned from Cybrary. I also mastered Wireshark filters. Now, I can find and study key network data better. This makes my security work stronger and more focused.
Follow-Up Actions: Keep using packet analysis for security checks to find weak spots and risks. Make filters better to speed up analysis. This helps find security problems faster. Check and improve filters often. Target things like odd traffic or suspect IP addresses. Better filters mean finding system flaws more easily. We can then respond to security issues faster and better.

Network Traffic Analysis Report: Network Traffic Analysis Using Wireshark

Date: 02/16/2025

Entry #: 2

Tools/System Involved: Wireshark

Likelihood: Low

Severity: Low

Status: Resolved: The issue has been fixed or addressed.

Description: This report covers analyzing website network traffic. We used Wireshark to check the traffic. The goal was to study packet data from a user's request. We looked at protocols, IP addresses, and packet content. Filters helped us focus on key traffic for closer inspection.

Conclusion: I analyzed network traffic using Wireshark. I checked the packet capture file. This helped me grasp web traffic and different protocols. I also learned about DNS lookups. I used filters to find certain IP addresses. I isolated DNS, TCP, and HTTP traffic. I got better at using Wireshark for network checks.

My Cybrary training gave me Wireshark basics. This experience boosted my network analysis skills. I can now spot network issues better. I improved my use of filters and protocol analysis. This strengthens network security skills.

Follow-Up Actions: Keep a close watch on the network for strange things. Look for unusual activity that seems out of place. Use what you find to make the filters better. Add more filters to focus on key areas. Watch for odd DNS queries or unexpected IP addresses.

Look for traffic that doesn't seem right. This helps find security problems faster. It also helps the network run better. You can spot bottlenecks and fix slow spots. Update Wireshark filters often. This helps you deal with new threats. Regular checks of packet data boost my ability to find weak spots. You'll get a clearer view of the network's health and security.

Malware Analysis Report: File Hash Investigation Assessment

Date: 02/20/2025

Entry #: 3

Tools/System Involved: VirusTotal

Likelihood: High

Severity: High

Status: Escalated: Malicious file identified, investigation ongoing

Description: On February 20, 2025, an employee opened a dangerous spreadsheet. The file was password-protected. I checked the file with VirusTotal. Over 50 security firms said it was malware. It was even labeled as Flagpro malware. The file had bad stuff inside.

For example, it used a strange website: org.misecure.com. It also used a weird IP address: 207.148.109.242. The file's MD5 hash is ***287d612e29b71c90aa54947313810a25***. I saw odd network activity. The attack used tools to steal data. BlackTech likely did this. They are known for using complex malware.

Conclusion: A VirusTotal report showed the file was bad. Over 50 security companies called it Flagpro malware. We found clues about this malware, too. This includes a bad website (org.misecure.com) and an IP address (207.148.109.242).

The file's MD5 hash is **287d612e29b71c90aa54947313810a25**. We also saw network activity and tools used to steal data. The malware seemed to be controlled remotely.

Follow-Up Actions: Watch the network traffic. Look for strange activity linked to the malware IP and domain. Add filters to network tools. This helps find suspicious connections tied to the malware.

Make sure the security software flags files like *bfsvc.exe*. Do this before users open them. Team up with the IT team to check things out. They can also take needed actions. After fixing the problem, check the security. Doing so helps improve protection later.

Phishing Incident Report: Malicious File Hash Investigation

Date: 02/20/2025

Entry #: 4

Tools/System Involved: VirusTotal

Likelihood: Moderate

Severity: Moderate

Status: **Escalated: Forwarded to SOC Level 2 Analyst**

Description: On Thursday, February 20, 2025, at approximately 09:30 a.m. EST. An employee opened a bad file from a phishing email. The email came from a strange address: 76tguyhh6tgftrt7tg.su. It said it was from Clyde West but showed the name Def Communications. The email had a password-protected file named bfsvc.exe. This file is known to be harmful. This could mean a backdoor or ransomware attack. The alert ticket is documented below under the section titled "Phishing Alert Ticket".

Conclusion: The file is malicious. The threat level is medium. The email had weird details like the email address and poor grammar. This makes the phishing attempt obvious. The incident is now with a SOC Level 2 analyst.

Follow-Up Actions: The SOC Level 2 analyst will investigate the incident further and take necessary actions based on their findings.

Phishing Alert Ticket

Ticket ID	Alert Message	Severity	Details	Ticket status
A-2703	SERVER-MAIL Phishing attempts possible download of malware	Medium	The user may have opened a malicious email and opened attachments or clicked links.	Escalated

Ticket Comments
An alert showed that an employee got a malicious file. They downloaded it from a phishing email and opened it. The email had odd details. The sender's email was "76tguyhh6tgftrt7tg.su." The email called the sender "Clyde West." But the sender's name was "Def Communications." The email had bad grammar. It also had a password-protected file named "bfsvc.exe." The employee downloaded and opened it. I checked this file before. It is a known malicious file. The alert is a medium threat. I sent this to a SOC Level 2 analyst. They will take the next steps.

Additional Information

Known Malicious File Hash:

54e6ea47eb04634d3e87fd7787e2136ccfbcc80ade34f246a12cf93bab527f6b

Subject Email:

From: Def Communications <76tguyhh6tgftrt7tg.su> <114.114.114.114>
Sent: Thursday, February 20, 2025 09:30:14 AM
To: <hr@inergy.com> <176.157.125.93>
Subject: Re: Infrastructure Egnieer role

Dear HR at Ingergy,

I am writing for to express my interest in the engineer role posted from the website.

There is attached my resume and cover letter. For privacy, the file is password protected. Use the password paradise10789 to open.

Thank you,

Clyde West
Attachment: filename="bfsvc.exe"

Phishing Incident Report: File Hash Investigation

Date: 02/20/2025

Entry #: 5

Tools/System Involved: VirusTotal

Likelihood: High

Severity: High

Status: **Escalated: Malicious file identified, investigation ongoing**

Description: On February 20, 2025, at approximately 09:30 a.m. EST, an employee opened a file. It was a spreadsheet with a password. The file came from a phishing email. The email had the password in it. Opening the file started a harmful program. I found the file and the SHA256 hash. I checked it on VirusTotal. This helped me learn more about the threat. The analysis ticket is documented below under the section titled "Malicious File Hash Analysis".

Conclusion: VirusTotal found the file to be harmful. Over 50 security programs labeled it as Flagpro malware. This malware is used by skilled attackers. Several clues showed the file was dangerous.

- The domain org.misecure.com was contacted by the malware.
- The IP address 207.148.109.242 is tied to this bad domain.
- The file's MD5 hash is **287d612e29b71c90aa54947313810a25**.

The malware made HTTP requests to org.misecure.com. It also used input capture to steal data. The malware sets up command and control communications.

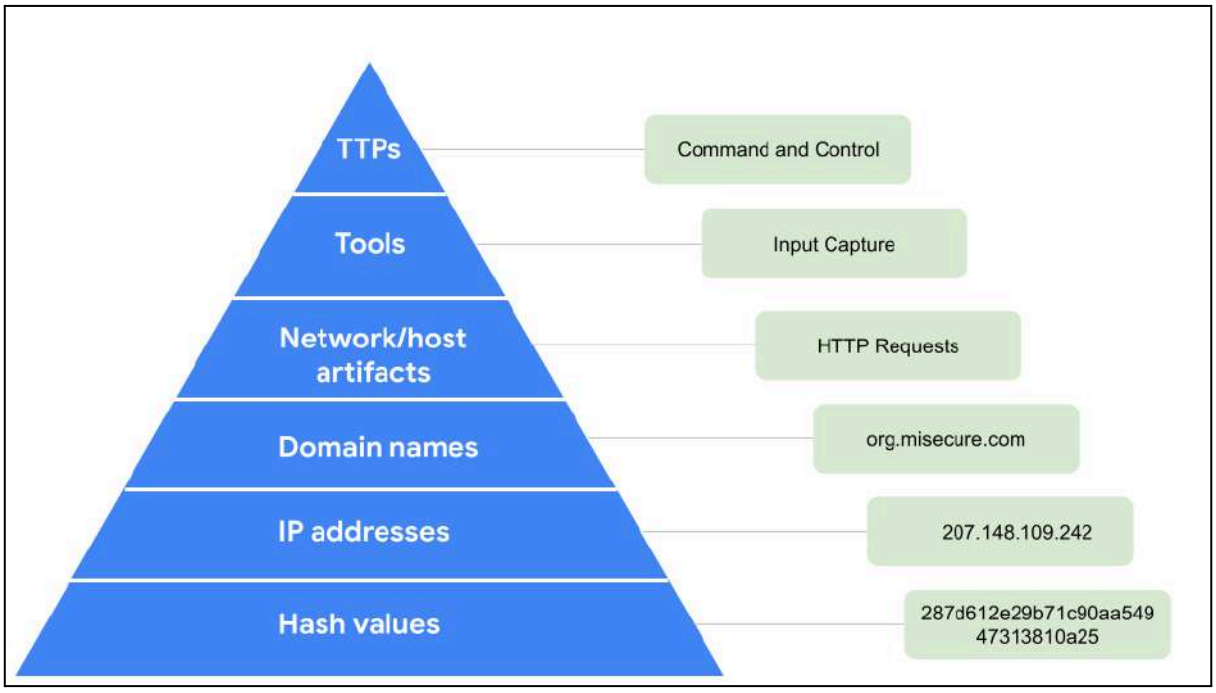
Follow-Up Actions: Watch network traffic closely. Look for strange activity linked to org.misecure.com and IP 207.148.109.242. Improve email security. Block similar phishing attempts using stronger filters. Update antivirus software on all devices.

Make sure it blocks known malware. Keep studying the malware. See if the data was stolen or if there's more damage. Tell the security team what you find. They can investigate further and stop the threat. After fixing this problem, check the security rules. Update them to stop future issues. Teach employees about phishing and improve password rules.

Malicious File Hash Analysis

Has this file hash been reported as malicious? Explain why or why not.

Security firms say the file is bad. Over 50 vendors flagged its hash. The file links to Flagpro malware. BlackTech uses this threat. Flagpro can launch remote attacks. It also steals important data.



Automation and Scripting Report: Python Programming

Date: 02/23/2025

Entry #: 6

Tools/System Involved: Python Programming, Google Cybersecurity Course

Likelihood: Low

Severity: Low

Status: New: Incident has just been reported and is awaiting review.

Description: I studied Python's use in cybersecurity and learned to automate security tasks. I wrote scripts for quick incident response and for log analysis. These scripts also helped to find weak spots in systems. I learned about data types and variables. I also learned about conditional statements and loops. Using these concepts helped me build scripts. The scripts made the cybersecurity workflow better.

Conclusion: I learned basic Python and how it helps with security. I can now use it to automate tasks. For example, Python can help with incident response. It also helps find weak spots. This progress shows promise for more security automation.

Follow-Up Actions: Keep coding in Python to create complex security tools. Use these tools for real tasks. Check how well my automation scripts work and make them better. Add my Python scripts to the current security work. This will make things faster and more efficient.

SECTION 3.0 ACTIVITY REPORTS

Activity Report: Review of Data Breach Final Report

Date: 02/21/2025

Entry #: 1

Activity Name: Review of Final Report: Data Breach Incident

Tools/System Involved: None

Priority: High

Description:
A retail company had a large security problem. Over one million users were affected by a data breach. The final report covers this major incident. Hackers got into the system without permission. They stole personal data from about 50,000 customers. This included names and financial information.

Summary of Findings: On December 28, 2022, at approximately 3:13 p.m. PT, a hacker broke into our online store. They used a flaw in the website to see private information. The hacker changed order numbers on purchase pages. This lets them see customer details and grab data. Then, the hacker asked for $50,000 in crypto. They wanted to be paid to keep the stolen data secret.

Our security team started looking into the hack that day. The hacker sent an email with some stolen data as proof. We found the break-in in the website's logs. The logs showed how the hackers got in and what data they stole.

Key Takeaways: A data breach (*forced browsing attack*) occurred due to a flaw in the company's online store. Attackers used this flaw to access private customer information. The hackers then demanded $50,000 in crypto. They threatened to release the stolen data if they didn't get paid. The company worked with its PR team to announce the breach. They also provided free identity theft protection to those affected.

Next Steps: Regularly scan for weaknesses and test the system's security. Control access to my data. Allowlisting limits URL access. Authentication protects sensitive info.

Activity Report: Suricata Rule Exploration and Alert Analysis Report

Date: 02/21/2025

Entry #: 2

Activity Name: Suricata Rule Exploration and Alert Analysis

Tools/System Involved: Suricata IDS/IPS, Network Traffic Logs, Rule Sets

Priority: Low

Description:
I studied Suricata rule sets. I looked at alerts triggered by specific rules. This helped me analyze network alerts. I dug deep into Suricata alerts to find threats. I checked how bad the problems were. I focused on the rules about network traffic. These rules looked for bad stuff like port scans. They also spotted denial of service attacks (DoS). I checked for people trying to sneak into the network.

Summary of Findings: We saw strange traffic coming in. It looked like someone was scanning our ports. Traffic to our web server spiked. This could mean a denial-of-service attack. Many failed logins hit a key service. The logins came from different places, so it looks like a brute-force attack.

Our system flagged some bad IP addresses. These IPs were talking to our network. We also saw some false alarms. This happened because some rules were too wide. Network setup mistakes also caused false alarms.

Key Takeaways: Adjusting rules helps lower false alarms and highlight real threats. Sorting and ranking alerts let you spot true dangers fast. Keep Suricata rules updated for the newest threat data. Check failed logins and odd traffic often for ongoing security.

Next Steps: Tweak Suricata rules to find more real threats. Lessen the number of false alarms, too. Make the rule logic better to cut down on alert noise. Check out shady IP addresses and the traffic they send. Look for trends linked to these threats. Update signature databases often. This helps spot new attack methods faster.

Activity Report: Python Programming for Cybersecurity

Date: 02/23/2025

Entry #: 3

Activity Name: Learning & Practicing Python for Cybersecurity

Tools/System Involved: Python Programming Environment, Jupyter Lab

Priority: Low

Description: Module 1 of the Google Cybersecurity Course focused on Python programming for cybersecurity. Activities included:

- Watching instructional videos on Python and its applications in cybersecurity.
- Reading materials on Python environments and their use in security tasks.
- Practicing script creation, including using conditional statements and loops.
- Completing a lab that involved writing Python code for security tasks.
- Testing knowledge through quizzes and practice assignments, and achieving a perfect score.

Summary of Findings: Hands-on practice reinforced Python skills, especially for security automation. The Python lab deepened my understanding of loops and conditions. Quizzes and homework showed a strong grasp of these key ideas.

Key Takeaways: Gained hands-on experience in Python for security automation. Mastered the creation of Python scripts with loops and conditional statements. Achieved a 100% score on practice assignments, demonstrating proficiency in core Python concepts.

Next Steps: Apply Python scripting skills to real-world cybersecurity scenarios. Continue refining scripts for automating tasks like incident response and log analysis. Explore more advanced Python features and their application in cybersecurity tasks.

Activity Report: Completed Python Functions and Code Readability Module

Date: 02/25/2025

Entry #: 4

Activity Name: Completed Module 2, Python Functions and Code Readability Module

Tools/System Involved: Python Programming Environment, Jupyter Lab

Priority: Low

Description: This activity focused on Python functions, modules, and code clarity. The module had videos, readings, quizzes, and labs. I learned to define and call functions using parameters. I also learned about return statements. Python functions are useful in cybersecurity. Modules and libraries help build reusable code, ensuring that code readability is important.

Summary of Findings: I gained proficiency in defining and calling Python functions. I understand various parameters and return statements. Python's built-in functions simplify coding. I explored the use of Python's built-in functions and how they can simplify coding. I learned code readability by adhering to proper syntax and structure. Labs and quizzes reinforced what I learned. Videos and readings reinforced the concepts learned.

Key Takeaways: Python functions break down tasks and enhance the reusability of code. Python modules and libraries make development easier. They give access to pre-built functionalities. Readable code is critical in cybersecurity and software development, ensuring maintainability and collaboration.

Next Steps: Next, I will continue to apply Python functions in practical cybersecurity scenarios. I will improve code readability in all future projects. This will enhance efficiency. It will also help with teamwork. I plan to explore Python topics to build expertise in coding for cybersecurity tools.

Activity Report: String Operations, Lists,... with Python

Date: 02/27/2025

Entry #: 5

Activity Name: Completed Module 3 on String Operations, Lists, and Regular Expressions

Tools/System Involved: Python Programming Environment, Jupyter Lab

Priority: Low

Description: This module covered Python strings and lists. Topics included operations, list manipulation, and using regular expressions to extract patterns. Skills were used to make a basic algorithm and use regex for pattern matching in text.

Summary of Findings: I improved my skills in Python string and list handling. I did exercises using string indices, slices, and list operations. I also built a simple algorithm and used regular expressions to find string patterns.

Key Takeaways: Strings and list manipulations are key tools for handling data in Python. This is especially true for cybersecurity. Regular expressions help extract and analyze data patterns. This skill is relevant to security analysis.

Next Steps: Next, I will continue practicing string and list operations. This will help with harder algorithm tasks. I will also learn more applications of regular expressions in cybersecurity contexts. Log file analysis is one example.

Activity Report: Automating Cybersecurity with Python

Date: 03/01/2025

Entry #: 6
Activity Name: Course Completion - Automate Cybersecurity Tasks with Python
Tools/System Involved: Python Programming Environment, Jupyter Lab
Priority: Low
Description: Completed the "Automate Cybersecurity Tasks with Python" course from the Google Cybersecurity program. The course taught Python basics for security automation. It covered file handling and data parsing. I also learned to apply regular expressions and Python debugging. The course offered hands-on practice. I automated tasks and tackled real-world cybersecurity challenges.
Summary of Findings: Key findings include a better grasp of Python and its use in cybersecurity. I now know how to import and read files. This helps with automating log analysis and monitoring. I got better at working with regular expressions for pattern matching. This is key for identifying security risks. Also, I learned debugging techniques. This helps optimize and boost Python scripts.
Key Takeaways: Python helps automate cybersecurity tasks, which simplifies log reviews and finds incidents. It also makes data parsing easier. Regular expressions help find patterns in large datasets quickly. Debugging skills are vital. They ensure the accuracy and efficiency of scripts in production environments.
Next Steps: Apply Python automation to enhance current cybersecurity workflows. Build a script to parse and analyze security logs, identifying potential threats. Continue developing Python skills. Use it for advanced cybersecurity tasks. These could include vulnerability scanning and incident response automation.

Activity Report: Cyber Kill Chain & MITRE ATT&CK Research

Date: 03/02/2025

Entry #: 7
Activity Name: Research – Cyber Kill Chain Model & MITRE ATT&CK Framework
Tools/System Involved: Documentation, PDF creation tools
Priority: Low
Description: Created a versioned report exploring the Cyber Kill Chain model and the MITRE ATT&CK framework. Focused on mapping attacker tactics and identifying gaps in defenses.
Summary of Findings: Both frameworks offer structured insight into attacker behavior. Understanding them supports stronger detection and response capabilities.
Key Takeaways: These models enhance threat analysis and can guide defensive strategy.
Next Steps: Apply both frameworks to future incident investigations and threat modeling exercises.

Activity Report: Enterprise Security Software Research

Date: 03/03/2025

Entry #: 8
Activity Name: Report – Enterprise Security Software Types – v1.0.0
Tools/System Involved: Documentation, PDF Creation Tools
Priority: Low
Description: Completed a research report on key types of enterprise security software. Covered functions, use cases, and general limitations of major categories.
Summary of Findings: Each tool plays a role in protecting systems, but no single solution is comprehensive.
Key Takeaways: Understanding software categories supports informed decision-making for security planning.
Next Steps: Use this knowledge in future recommendations or assessments of enterprise environments.

Activity Report: Covert Social Media Account Creation

Date: 03/12/2025

Entry #: 9
Activity Name: Covert Social Media Account Creation
Tools/System Involved: Social Media Platforms, Privacy Settings
Priority: Moderate
Description: Created Covert social media profiles for OSINT work. Set up strong privacy measures to stay anonymous. Recorded a clear-screen video to show how I configured everything.
Summary of Findings: Covert accounts are crucial for viewing private data during OSINT investigations. Proper configuration helps lower the risk of exposure.
Key Takeaways: Maintaining anonymity and strong security is vital in investigative work. Managing covert accounts enhances data access while keeping identities safe.
Next Steps: Maintain operational discipline with these accounts. Make sure to include them in future OSINT workflows.

Activity Report: Searching for Information Leaks on Code Repositories

Date: 03/14/2025

Entry #: 10
Activity Name: Code Repository Leak Detection
Tools/System Involved: GitHub, GitLab, Bitbucket, Code Search Tools
Priority: High
Description: Specialized tools helped find leaks of sensitive information in public code repositories. The focus was on uncovering exposed credentials, API keys, and other private data. Often
Summary of Findings: Often, Information leaks happen because of accidental commits. Running regular scans can stop unauthorized access and data breaches before they happen.
Key Takeaways: Security hygiene in code repositories is critical. Developers must avoid committing sensitive data.
Next Steps: Moving forward, automation should be added to the CI/CD pipeline for continuous scanning. It’s also important to keep practicing good habits for secure code management.

Activity Report: Passive Asset Mapping with dnsdumpster.com

Date: 03/15/2025

Entry #: 11
Activity Name: Passive Mapping of External Assets
Tools/System Involved: dnsdumpster.com
Priority: High
Description: Used dnsdumpster.com to gather information about an organization without alerting its systems. Mapped out related domains, subdomains, and IP addresses to understand its external setup.
Summary of Findings: The findings revealed key assets that showed the company's online presence. These insights highlighted possible weak points without causing any alarms.
Key Takeaways: Passive asset mapping proves to be a simple way to check a company's digital setup and potential risks. It allows for safe assessment without direct contact with the target’s systems.
Next Steps: Incorporate passive mapping as part of regular OSINT research and threat assessment workflows.

Activity Report: Phishing Site Detection with urlscan.io

Date: 03/21/2025

Entry #: 12

Activity Name: Phishing Site Detection with urlscan.io

Tools/System Involved: urlscan.io

Priority: Moderate

Description: Performed a practical test with URLScan.io to find phishing and spear-phishing websites. The platform offers detailed analysis by mimicking a browser's activity. It captures screenshots, DOM data, network requests, and JavaScript behavior. The investigation focused on identifying malicious domains mimicking legitimate services.

Summary of Findings: Multiple malicious scans uncovered fake login pages that looked like official email and cloud service sites. These fake portals were tied to suspicious providers and used self-signed or invalid SSL certificates. They also showed strange redirect behavior that stood out.

Key Takeaways:

- Urlscan.io is useful for spotting phishing setups and suspicious activities
- It helps uncover ongoing threats by checking scan history and domain variations.
- Detecting spear-phishing requires context-aware analysis (e.g., brand spoofing, domain similarity).

Next Steps: Use urlscan.io as part of my everyday OSINT tasks for tracking brands and spotting phishing attempts. Share domains that seem suspicious with threat intelligence teams or reporting systems. Practice setting up alert rules to catch phishing signs, like login pages that match my logo or domains that seem out of place.

Activity Report: Using Google Dorks to Identify Open Malware Sandboxes

Date: 03/024/2025

Entry #: 13

Activity Name: Research and Demonstration of Google Search Queries for Malware Sandbox Discovery

Tools/System Involved: Google Search Engine, Various Google Dork Queries

Priority: Moderate

Description: I explored different Google search queries, known as Google Dorks. I aimed to find publicly available malware sandboxes online. These searches used specific words to locate websites that host sandbox environments for testing and analyzing malware.

Summary of Findings: The exercise showed how well-made search queries can find exposed malware sandbox environments. Spotting these sandboxes helps improve threat intelligence and makes malware testing safer. The study revealed that even publicly available sandboxes can accidentally reveal sensitive malware information.

Key Takeaways:

1. Google Dorks remains a powerful tool for threat intelligence and OSINT investigations.
2. Combining search terms effectively helps uncover hidden or poorly secured online resources.
3. Finding open malware sandboxes allows analysts to study malware safely without risking infection.

Next Steps: By Using these search techniques in controlled setups is key to improving malware research. Regularly update my search methods on Google to keep up with changing patterns. Then, add the results to a larger threat intelligence work.

Activity Report: SSL Configuration Assessment using sslscan

Date: 03/27/2025

Entry #: 14

Activity Name: Use `sslscan` to Assess SSL Configuration Settings

Tools/System Involved: sslscan, Linux Terminal

Priority: Moderate

Description: Completed an activity to check secure communication setups on public-facing services. I followed a set of clear steps and recorded all observations internally.

Summary of Findings: Confirmed exposure to various configurations. Completed all required documentation and deliverables in alignment with the exercise objectives.

Key Takeaways:

1. Reinforced skills related to secure communications assessment.
2. Gained experience in using specialized tools in a structured, privacy-compliant workflow.

Next Steps: Keep using these methods in future exercises. Doing so will help improve my understanding of how to set up secure protocols properly.

Activity Report: TCP Port Scan Using Nmap

Date: 03/28/2025

Entry #: 15
Activity Name: TCP Port Scanning with Nmap
Tools/System Involved: Nmap
Priority: Moderate
Description: Conducted a TCP port scan on a remote target system using Nmap. Performed a scan to identify open ports and running services to assess potential security risks.
Summary of Findings: Identified open ports and associated services on the target system, providing insight into potential vulnerabilities.
Key Takeaways: Knowing which ports and services are open helps assess how secure a system is. It's essential for planning steps to fix vulnerabilities and stay safe.
Next Steps: Use scan results to guide further security assessments and improve system defenses.

Activity Report: UDP Port Scan Using Nmap

Date: 03/31/2025

Entry #: 16
Activity Name: UDP Port Scan Using Nmap
Tools/System Involved: Nmap
Priority: Moderate
Description: Performed a UDP port scan on a remote target system using Nmap. The goal was to find open UDP ports and running services.
Summary of Findings: The scan revealed open UDP ports and the related services they hosted. This information is useful for checking the security of the system.
Key Takeaways: Identifying open UDP ports is crucial in a thorough network security assessment. It helps spot potential vulnerabilities that could be exploited by attackers. Knowing this data can guide better security measures to protect the network.
Next Steps: Analyze scan results to support further security evaluations and remediation efforts.

Activity Report: Continuous Learning and VM Setup

Date: 03/31/2025 – 05/20/2025

Entry #: 17

Activity Name: Virtual Machine Configuration and Cybersecurity Reading

Priority: Moderate

Description: I spent a long time setting up a virtual machine environment using UTM on macOS for practical YARA Rule exercises. At the same time, I focused on self-study by reading important cybersecurity books.

This helped me learn more about ethics, upcoming trends, the basics of InfoSec, and key tools for system administration. Combining hands-on work with reading improved my overall skills in cybersecurity.

Books Read:

- *The Ethics of Cybersecurity*
- *Cybersecurity: Navigating the Future Landscape*
- *Beginner's Guide to InfoSec*
- *20 Windows Tools Every SysAdmin Should Know*

Activity Report: Lab Setup – Threat Hunting with YARA

Date: 05/20/2025

Entry #: 18
Activity Name: Lab Setup – Threat Hunting with YARA
Tools/System Involved: UTM (macOS), YARA
Priority: High
Description: Set up a virtual machine lab for threat hunting with YARA.
Summary of Findings: The lab is ready for YARA-based threat-hunting activities.
Key Takeaways: Established a controlled environment for future exercises.
Next Steps: Begin YARA rule testing.

Activity Report: Write a YARA Rule That Is Professional Documented

Date: 05/22/2025

Entry #: 19
Activity Name: Write a Professionally Documented YARA Rule
Tools/System Involved: UTM (macOS), YARA
Priority: Moderate
Description: I created a YARA rule that is easy to understand and clearly explains what it does. I added helpful notes and important information so others could quickly know how the rule works and why it was made.
Summary of Findings: Adding good notes and clear names made the rule easier to use and helped the team work better together.
Key Takeaways: Writing clear and detailed notes is important for finding threats and sharing information with others. Good rule names and comments make it easier for everyone to understand.
Next Steps: Keep using these good writing habits for future YARA rules and teach the team how to do it too.

Activity Report: Write a YARA Rule That Can Find Itself

Date: 05/23/2025

Entry #: 20
Activity Name: Write a YARA Rule That Can Find Itself
Tools/System Involved: UTM (macOS), YARA
Priority: Moderate
Description: Completed a video submission exercise demonstrating how to write a YARA rule capable of matching itself.
Summary of Findings: Confirmed that the rule syntax and structure were understood and that YARA could successfully detect its rule definition in a scan.
Key Takeaways: This exercise strengthened foundational YARA rule-writing skills and deepened my understanding of how rules match specific byte and string patterns.
Next Steps: Advance to more complex rule creation using hex patterns and conditions.

Activity Report: Write a YARA rule that can find small portable executables

Date: 05/24/2025

Entry #: 21
Activity Name: Write a YARA rule that can find small portable executables
Tools/System Involved: YARA, YARA PE Module
Priority: Moderate
Description: Completed a video submission and script demonstrating a YARA rule designed to detect small Windows Portable Executable (PE) files.
Summary of Findings: The rule successfully identifies key PE characteristics and file size constraints, aiding in the detection of small PE files that may be malicious.
Key Takeaways: Gained hands-on experience writing YARA rules focused on PE file attributes, improving the ability to detect potentially harmful executables.
Next Steps: Expand rule complexity to cover additional PE metadata and anomaly detection.

Activity Report: Write a YARA Rule to Search for Files with Specific Strings

Date: 05/26/2025

Entry #: 22
Activity Name: Write a YARA Rule to Search for Files with Specific Strings
Tools/System Involved: YARA
Priority: Moderate
Description: Completed an exercise focused on developing a YARA rule to identify files based on specific internal patterns.
Summary of Findings: The exercise helped reinforce the ability to create targeted YARA rules for improved threat detection.
Key Takeaways: Practicing rule creation enhances skills for identifying potential threats efficiently.
Next Steps: Continue refining rule-writing techniques to support threat-hunting efforts.

Activity Report: YARA Rule – Search for Files with Given Strings

Date: 05/29/2025

Entry #: 23
Activity Name: Write a YARA Rule to Search for Files with Specific Strings
Tools/System Involved: YARA, Text Editor
Priority: Moderate
Description: I practiced writing a YARA rule to find files with specific strings. My first version didn't work, so I fixed the rule and submitted it again.
Summary of Findings: Writing accurate rules takes practice. The rule must match both strings correctly to be useful.
Key Takeaways: Failing the first time helped me understand how to test and fix my mistakes. Now I can write better YARA rules.
Next Steps: Keep practicing YARA by writing more complex rules that match real malware behaviors.

Activity Report: Lab Setup – Deploy Virtual Machines

Date: 06/01/2025

Entry #: 24
Activity Name: Lab Setup – Deploy Virtual Machines
Tools/System Involved: UTM, Windows
Priority: Moderate
Description: I installed virtual machines and connected them to a private network. This setup will be used for learning and practicing safely.
Summary of Findings: Using virtual machines helps keep the main system safe while doing hands-on training.
Key Takeaways: Virtual machines are important for learning cybersecurity skills in a safe space.
Next Steps: Use these machines for future labs and testing.

Activity Report: Lab Setup – Software Development

Date: 06/03/2025

Entry #: 25
Activity Name: Lab Setup – Software Development
Tools/System Involved: ARM64 platform, UTM, Linux, Folder Structure
Priority: Moderate
Description: I set up a software development lab on my computer. I made folders for different programming languages so I could keep things organized.
Summary of Findings: Having a clean setup helps me work on code faster and learn more easily.
Key Takeaways: A good setup saves time and helps with learning multiple languages.
Next Steps: Start using it to practice coding and complete exercises.

Activity Report: Docker Daemon Troubleshooting and Reinstallation

Date: 06/04/2025

Entry #: 26
Activity Name: Docker Daemon Troubleshooting and Reinstallation
Tools/System Involved: ARM64 platform, UTM, Kali Linux, Docker, Systemd, journalctl
Priority: Moderate
Description: Began debugging a Docker installation that failed to start. Reviewed systemd service status and logs via `sudo systemctl status docker.service` and `sudo journalctl -xeu docker.service`. Based on the findings, I completely purged Docker and reinstalled it, including support packages like `containerd.io`.
Summary of Findings: Docker was installed, but unable to start due to service misconfiguration or missing dependencies. Reinstallation and service re-enabling fixed the issue.
Key Takeaways: Knowing how to read `journalctl` logs is essential in diagnosing Docker startup issues.
Next Steps: Confirm Docker stability and proceed with image pulls.

Activity Report: Pull and Run Hello-World Docker Container

Date: 06/06/2025

Entry #: 27
Activity Name: Pull and Run Hello-World Docker Container
Tools/System Involved: ARM64 platform, UTM, Kali Linux, Docker Hub
Priority: Low
Description: Successfully pulled and ran the `hello-world` container after rebooting Kali and enabling VPN to overcome time-out issues.
Summary of Findings: The VPN connection resolved Docker Hub access issues, which caused time-outs during image pulls.
Key Takeaways: Docker Hub connectivity issues can stem from network restrictions or slow DNS resolution; VPN is a simple workaround.
Next Steps: Proceed with pulling larger, more complex containers like OpenVAS.

Activity Report: OpenVAS Container Setup

Date: 06/09/2025

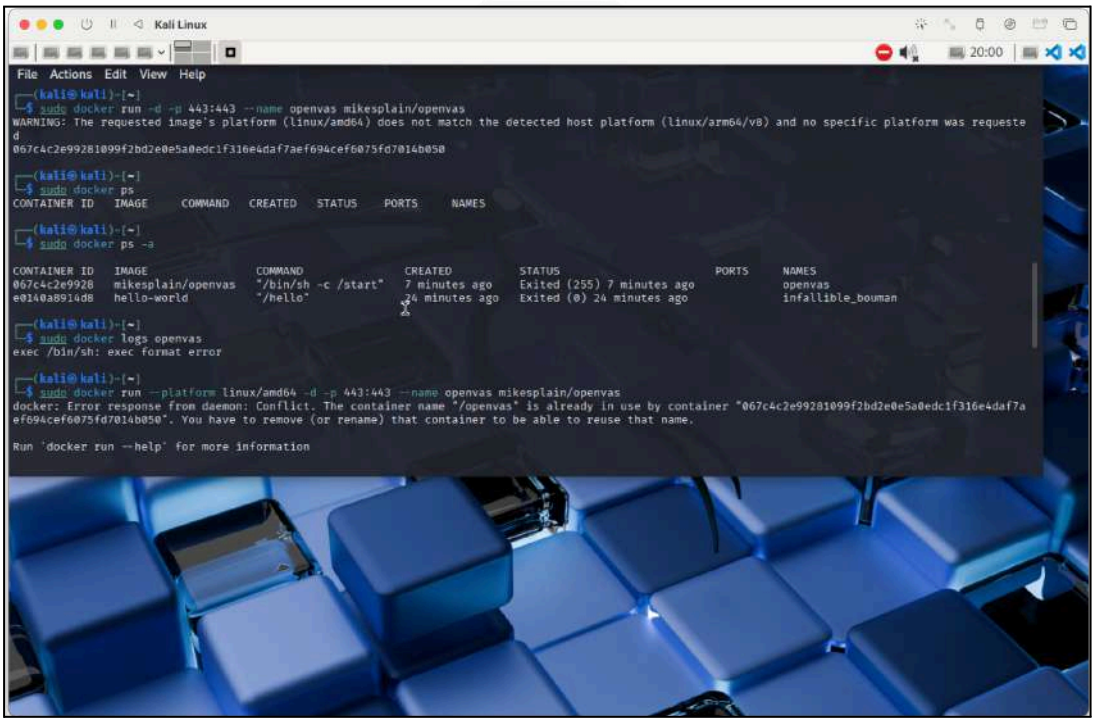
Entry #: 28

Activity Name: OpenVAS Container Setup (mikesplain/openvas)

Tools/System Involved: Docker, Kali Linux, ARM64 platform

Priority: Moderate

Description: Pulled `mikesplain/openvas` image. Encountered `exec format error` due to a mismatch between the container's amd64 build and the host's ARM64 architecture. Attempted to run with `--platform linux/amd64`, but container exited with code 255.



Summary of Findings: `mikesplain/openvas` is not compatible with ARM64 natively. Emulation with `--platform` fails or is unstable.

Key Takeaways: Platform architecture compatibility is critical when selecting Docker images.

Next Steps: Explore building from source using Greenbone's `docker-gvm` repo

Activity Report: OpenVAS Container Setup

Date: 06/09/2025

or use an amd64-compatible host.

Activity Report: Attempted Pull of Official Greenbone GVM Images

Date: 06/10/2025

Entry #: 29

Activity Name: Attempted Pull of Official Greenbone GVM Images

Tools/System Involved: Docker, Kali Linux, Docker Hub

Priority: Low

Description: I tried pulling `greenbone/community-edition` and `greenbone/gvm`. Both failed with access errors, indicating that the images are private or require a login.

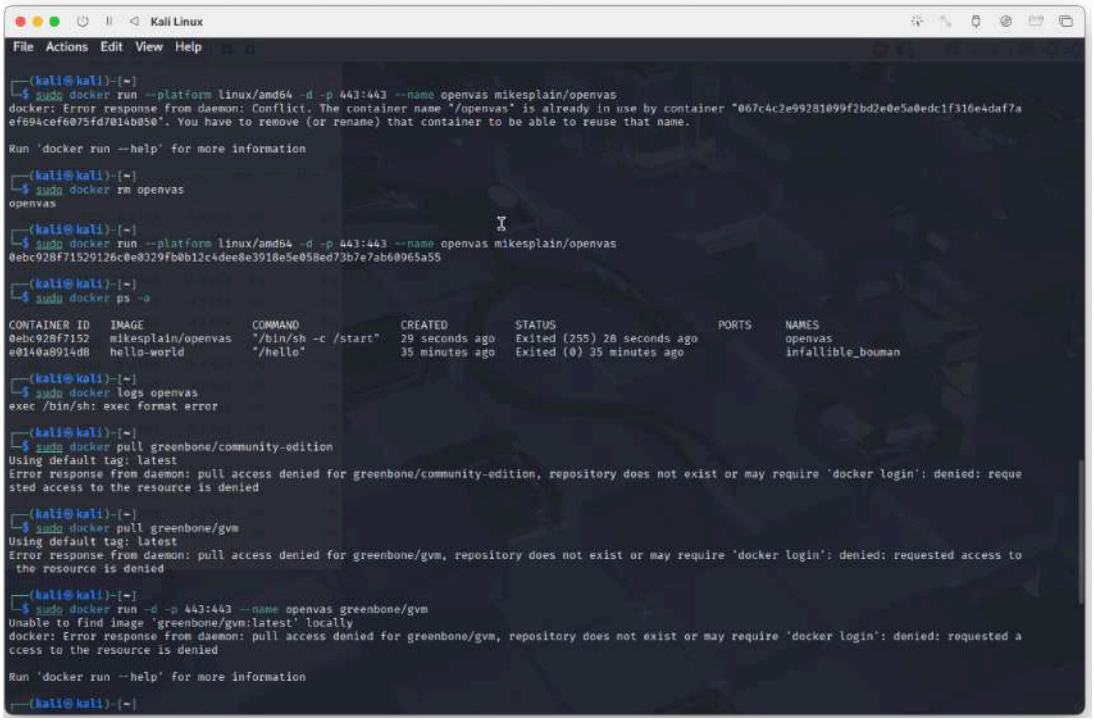


Figure 1: Kali Linux VM screenshot, June 10, 2025

Summary of Findings: Official Greenbone Docker images are either not publicly available or restricted.

Key Takeaways: Not all Docker images advertised in the documentation are publicly accessible; fallback options or manual builds are sometimes necessary

Next Steps: Clone and build Greenbone's official GVM image from the source to

Activity Report: Attempted Pull of Official Greenbone GVM Images

Date: 06/10/2025

ensure ARM64 support and compatibility.

Activity Report: Updating Legacy Cybersecurity Projects

Date: 06/11/2025

Entry #: 30

Activity Name: Updating Legacy Cybersecurity Projects

Tools/System Involved: Google Docs, Markdown, Version Control (Semantic Versioning), GRC Reporting Templates

Priority: Low

Description: Reviewed and updated multiple previously completed cybersecurity reports to improve formatting and structure using a standardized GRC template. This included applying hierarchical section numbering, inserting formal conclusions, and revising revision history tables to reflect version control best practices.

Summary of Findings:

- Older reports were missing standardized numbering (e.g., 1.0, 1.1) and clear conclusions.
- Some reports had repeated section titles or inconsistent titles and formats.
- Versioning history needed updates to track formatting-related changes.

Key Takeaways:

- Consistent structure and semantic versioning significantly improve report professionalism.
- Formal conclusions add analytical value and reinforce actionable outcomes.
- Hierarchical formatting enhances readability and aligns with audit documentation standards.

Next Steps: Continue updating the remaining legacy reports with the new structure.

Activity Report: Continued Testing & Validation of OpenVAS on ARM64 Kali

Date: 06/12/2025

Entry #: 31
Activity Name: Continued Testing and Validation of OpenVAS on ARM64 Kali
Tools/System Involved: Docker, Kali Linux (ARM64), Docker Hub
Priority: Moderate
Description: Reattempted running `mikesplain/openvas` with `--platform linux/amd64` on ARM64 Kali, but the container exited with `exec format error`. Checked for existing containers, removed conflicting names, and retried without success. Attempts to pull `greenbone/gvm` and `greenbone/community-edition` failed due to access denial. Revisited the use of previously working `netizensoc/openvas-scanner` for a possible remote scanner setup with `Docker Compose`.
Summary of Findings: `mikesplain/openvas` still fails due to architecture mismatch. Official Greenbone images remain inaccessible. Reliable scanner setup may require remote container deployment with proper master configuration.
Key Takeaways: Docker images must be architecture-compatible or run under effective emulation. Container naming conflicts must be resolved before reuse.
Next Steps: Finalize scanner container setup using `netizensoc/openvas-scanner` and ensure communication with GVM master using keys and scanner ID.

Activity Report: Cleanup and Preparation for Greenbone GVM Build

Date: 06/13/2025

Entry #: 32

Activity Name: Cleanup and Preparation for Greenbone GVM Build

Tools/System Involved: Docker, Kali Linux (ARM64)

Priority: Low

Description: Identified and removed legacy `mikesplain/openvas` containers, which caused repeated compatibility issues due to AMD64-only support. Verified that prior GVM crashes were caused by insufficient memory rather than container corruption.

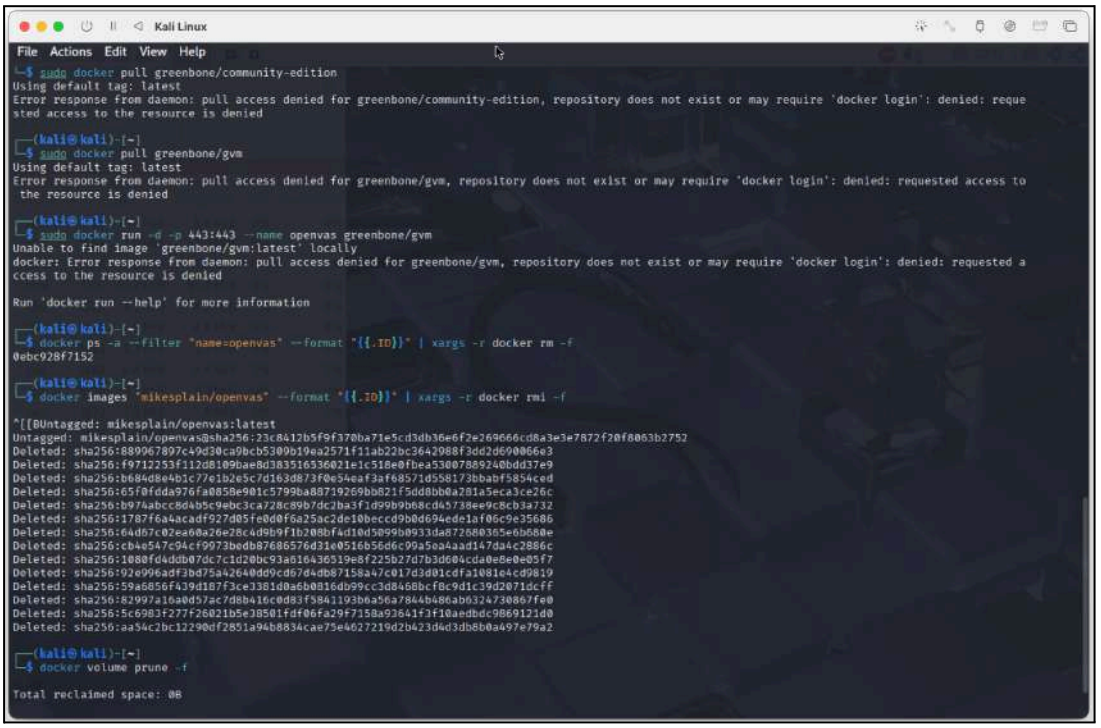


Figure 2: Removed Legacy `mikesplain/openvas` Containers Screenshot, June 13, 2025

Activity Report: Cleanup and Preparation for Greenbone GVM Build

Date: 06/13/2025

Initiated a fresh GVM build from source using Greenbone's official repositories on a Kali Linux ARM64 VM. Progressed through multiple missing dependency errors, resolving the following:

- `libhiredis-dev`
- `libgpgme-dev`
- `libgcrypt20-dev`
- `uuid-dev`
- `libnet1-dev`, `libpcap-dev`, `libgnutls28-dev`, `libglib2.0-dev`

The build process is currently **blocked** due to the missing **`libpaho-mqtt3c`** package, required for MQTTv5 support in GVM. This library is **not available in Kali's default repositories** and must be built from source or installed from a compatible Debian package.

Activity Report: Cleanup and Preparation for Greenbone GVM Build

Date: 06/13/2025

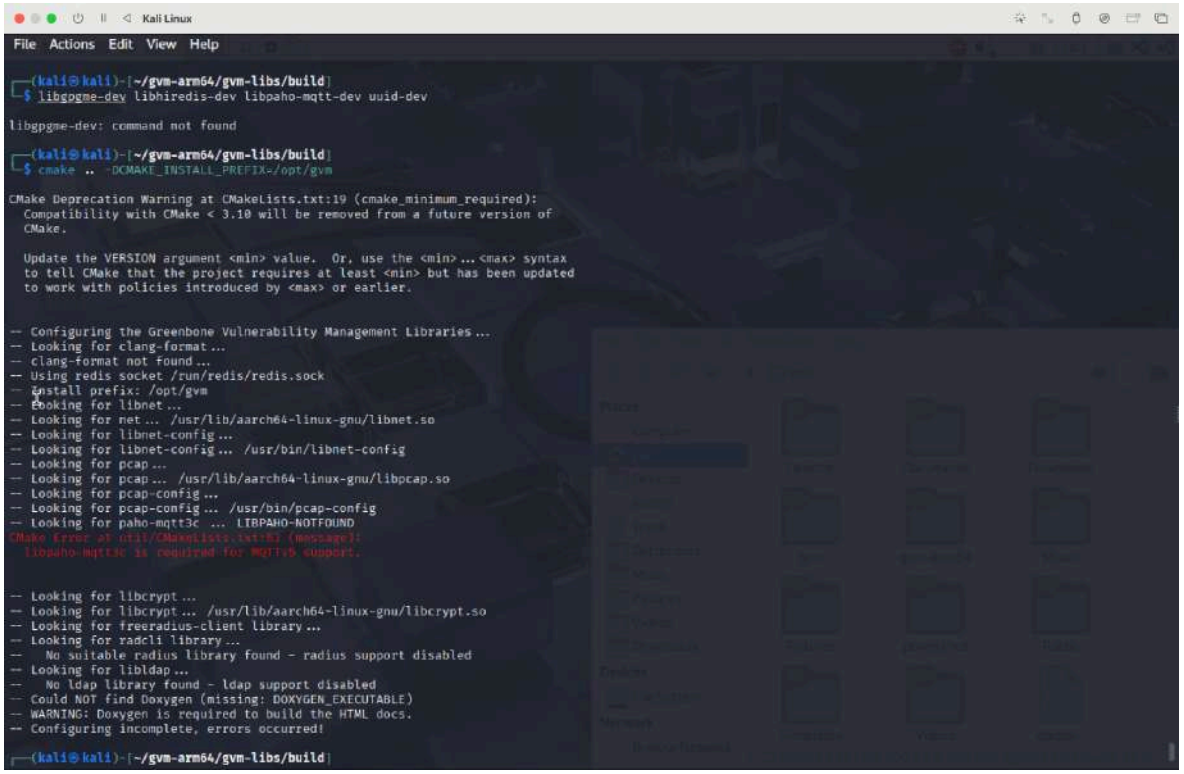


Figure 3: Missing `libpaho-mqtt3c` Package Screenshot., June 13, 2025

Summary of Findings:

- The legacy OpenVAS container is deprecated and incompatible with ARM64.
- The GVM build process on ARM64 is complex and incomplete, with dependencies not fully resolved out of the box.
- The missing `libpaho-mqtt3c` is a showstopper that requires a manual workaround or alternate package source.

Activity Report: Cleanup and Preparation for Greenbone GVM Build

Date: 06/13/2025

Key Takeaways:

- GVM builds on ARM64 and requires extensive manual dependency resolution.
- Compatibility with ARM64 systems depends on the availability of upstream packages or source-based workarounds.
- The current blocker (`libpaho-mqtt3c`) highlights the need for better ARM64 build documentation in the Greenbone ecosystem.

Next Steps: Locate and install `libpaho-mqtt3c` for ARM64:

  - **Option 1:** Build from source from the Eclipse Paho GitHub repo.
  - **Option 2:** Find a prebuilt `.deb` compatible with ARM64.

- Resume the `CMake` build process once the MQTT dependency is resolved.
- Proceed to build `gvmd`, `openvas`, and `gsa` components after a successful library build.

Activity Report: OpenVAS/GVM Operational Setup on Kali

Date: 06/14/2025

Entry #: 33

Activity Name: OpenVAS/GVM Operational Setup on Kali

Tools/System Involved: Greenbone Vulnerability Manager (GVM) 26.0.0, OpenVAS Scanner, Kali Linux (running on ARM64), Docker (initial attempt, pivoted to manual install), `Systemctl`, `journalctl`, `runuser`, GSA Web UI (Greenbone Security Assistant)

Priority: Moderate

Description: This task involved resolving multiple installation, configuration, and service-level issues to get Greenbone Vulnerability Manager (GVM) with OpenVAS running and fully functional on Kali Linux. It included feed synchronization, permission issues, memory troubleshooting, and successful GUI access.

Terminal Transcript Highlights:

Figure 4: Verifying GVM installation version. Screenshot, June 14, 2025

Figure 5: Starting `gvmd` as the `_gvm` user. Screenshot, June 14, 2025

Figure 6: Launching `gsad` on port 9392. Screenshot, June 14, 2025

Activity Report: OpenVAS/GVM Operational Setup on Kali

Date: 06/14/2025

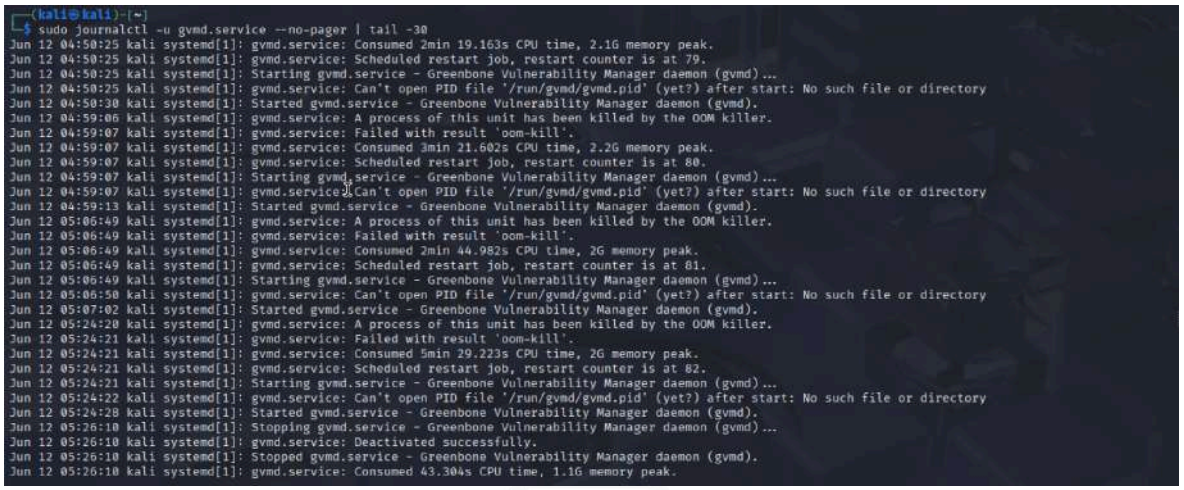


Figure 7: Memory Crash (OOM Killer) Screenshot, June 14, 2025

Figure 8: Checking RAM availability (3.8GB total, no swap). Screenshot, June 14, 2025

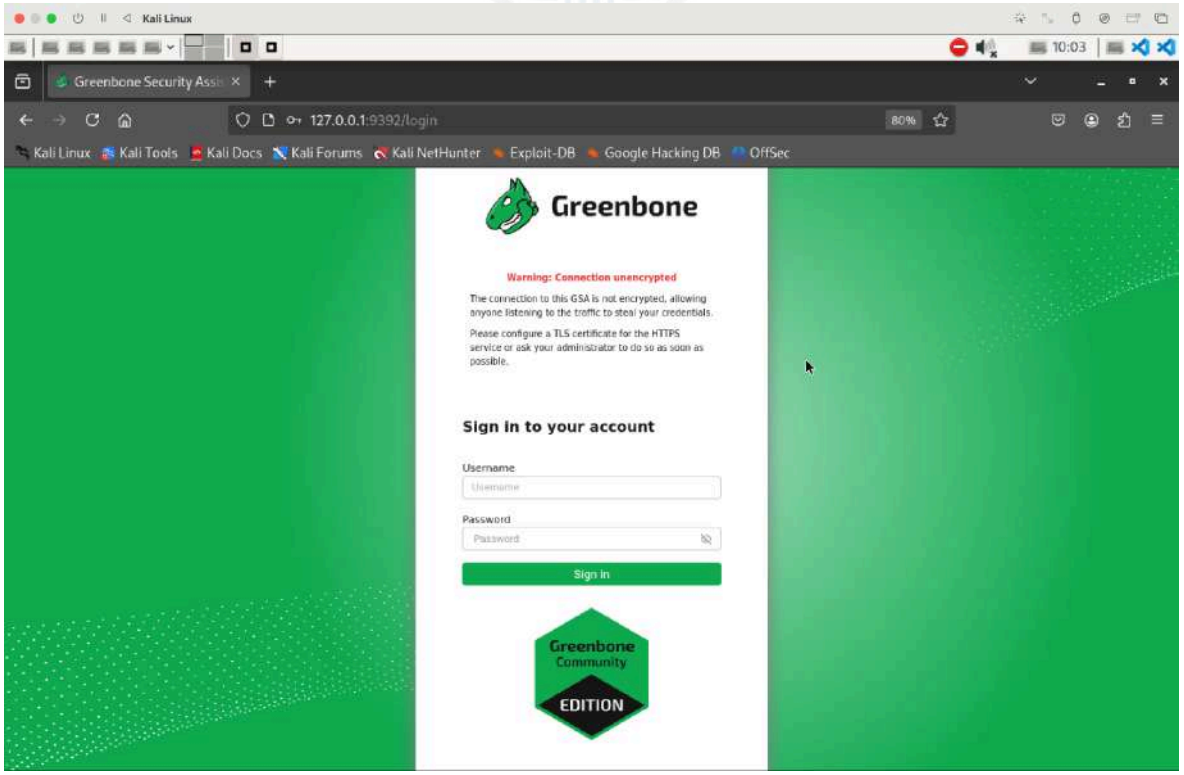


Figure 9: GSAD Web GUI Up (Unencrypted Warning Shown) Screenshot, June 14, 2025

Activity Report: OpenVAS/GVM Operational Setup on Kali

Date: 06/14/2025

Figure 10: Manual Feed Owner Fix Screenshot, June 14, 2025

Summary of Findings: GVM services (`gvmd`, `gsad`) failed to start initially due to:

- Missing PID directory permissions
- Memory overcommit (OOM killer)
- Feed not fully imported due to unset `feed_owner`

Successfully bypassed service start errors by:

- Manually creating a user (`admin`)
- Assigning `feed_owner` using `gvmd --modify-setting`
- Feed sync completed with 297,701 CVEs and 1.4 million+ CPEs.
- The GUI is accessible via *`http://localhost:9392`*, offering full scanning functionality.

Key Takeaways: OpenVAS setup on Kali running on ARM64 requires manual service invocation under the correct user context (`_gvm`).

- Build-from-source setups on Kali require extra care around pathing and persistent permissions.
- Limited RAM and no swap can trigger feed sync issues via OOM kills; 4GB+ RAM is preferred.
- Final confirmation of sync and scanner registration is crucial for scan readiness.

Activity Report: OpenVAS/GVM Operational Setup on Kali

Date: 06/14/2025

Next Steps:

- Run first authenticated scan on internal test target (Windows 7/XP VM)
- Export and analyze scan reports as part of the vulnerability management workflow
- Optionally, automate GVM and GSAD startup via `systemd`.

Activity Report: Manual GVM Deployment & Docker Troubleshooting

Date: 06/15/2025

Entry #: 34

Activity Name: Manual GVM Deployment & Docker Troubleshooting

Tools/System Involved:

- Kali Linux ARM64 (via UTM)
- Docker (multiple image attempts)
- Terminal (strace, journalctl, ps)
- `apt`, `netstat`, `ss`, `gvmd`, `ospd-openvas`

Priority: Moderate

Description: Attempted multiple Docker-based GVM deployments. All failed due to incompatibility with ARM64 architecture. Switched to manual installation. Documented failures, reviewed system calls via `strace`, and confirmed that containers (including Greenbone community Docker) either failed to start or terminated during init due to missing x86 dependencies. Began manual build route for GVM stack.

Terminal Highlights:

- `Docker run greenbone/community-edition` → segmentation fault (unsupported arch)
- **Manual install:** `/usr/sbin/gvmd: command not found` → resolved via package path discovery
- `Strace gvmd` is used to step through startup failures.

Activity Report: Manual GVM Deployment & Docker Troubleshooting

Date: 06/15/2025

Key Takeaways:

- Most prebuilt GVM Docker images are x86-only — ARM64 requires manual compilation or native ARM packages.
- GVM on ARM64 is doable but non-trivial
- You need to babysit every service layer (scanner daemon, PostgreSQL, gvmd) manually

Next Steps:

- Finish the manual GVM build
- Begin persistent systemd or background service setup for gvmd and ospd
- Test port bindings and socket creation for GMP and OSP

Activity Report: GVM Initialization, Lock/Socket Debugging, and Service Recovery

Date: 06/16/2025

Entry #: 35

Activity Name: GVM Initialization, Lock/Socket Debugging, and Service Recovery

Tools/System Involved:

- `strace`, `ps aux`, `killall`, `runuser`
- File system debugging (lockfiles, sockets)
- `tail`, `chmod`, `useradd`, `groupmod`

Priority: Moderate

Description: Tracked down `gvmd` failures to a persistent lockfile (`gvm-serving`) blocking startup. Used `strace` to confirm the process exited with `EAGAIN` when failing to acquire a lock. Killed zombie processes, deleted lockfiles, and restarted `gvmd` successfully. The system now reports “ready to accept GMP connections.” Still missing scanner socket connection due to `ospd-openvas` not running yet.

Terminal Highlights:

`flock(15, LOCK_EX|LOCK_NB) = -1 EAGAIN` → gvmd refusing to start
`sudo killall gvmd && rm /var/lib/openvas/gvm-serving` → successful unlock
`runuser -u _gvm -- gvmd` → finally starts clean
`gvmd is ready to accept GMP connections`
Log tailing permission error fixed via `sudo` use

Key Takeaways:

- GVM startup is fragile and dependent on manual cleanup during misconfiguration
- Lockfiles are not automatically purged; they must be deleted manually after crashes
- `gvmd` now working — progress checkpoint achieved

Activity Report: GVM Initialization, Lock/Socket Debugging, and Service Recovery

Date: 06/16/2025

Next Steps:

- Start and verify `ospd-openvas` scanner daemon
- Ensure `/run/ospd/ospd-openvas.sock` is created and readable
- Finish full-stack GVM validation (scanner + manager + web interface)

Activity Report: Build and Install GVM Libraries from Source

Date: 06/17/2025

Entry #: 36

Activity Name: Build and Install GVM Libraries from Source

Tools/System Involved: `apt`, `cmake`, `make`, `gcc/g++`, Linux terminal (Kali ARM64)

Priority: Moderate

Description: Installed all necessary dependencies for GVM libraries on Kali Linux ARM64, configured the build environment with `cmake`, compiled the source with make using all available cores, and installed the compiled libraries with sudo make install. Addressed CMake deprecation warnings, but no blocking errors occurred. Verified libraries and header files are installed correctly under `/usr/local`.

Terminal Highlights:

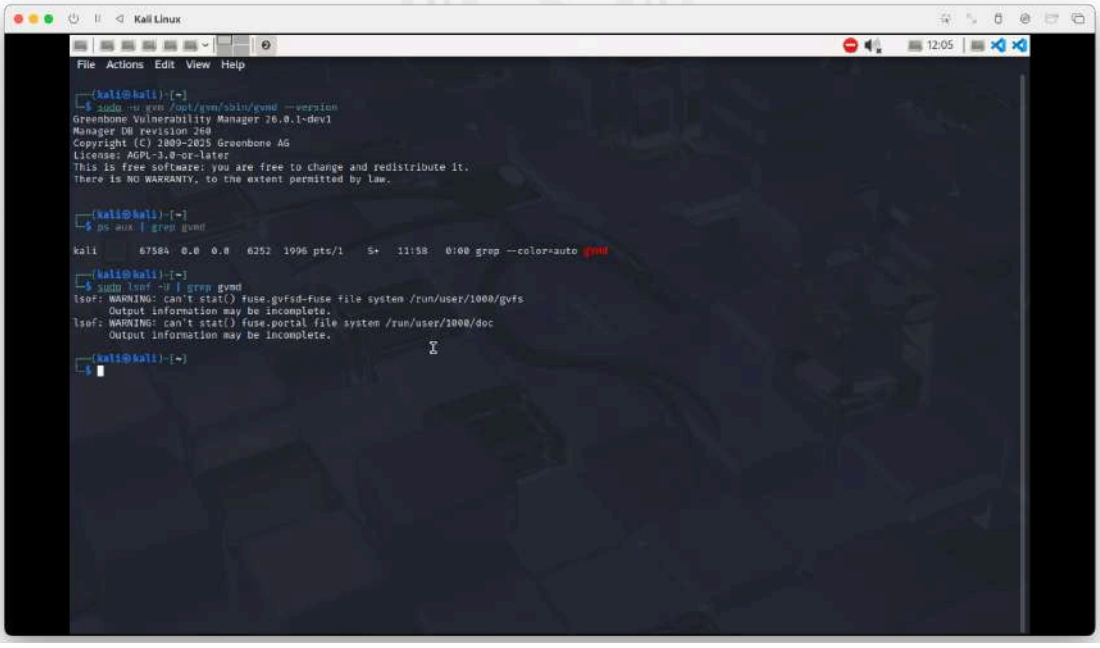


Figure 11: Showing `gvmd --version` output and process check results. Screenshot, June 17, 2025

Activity Report: Build and Install GVM Libraries from Source

Date: 06/17/2025

- Dependencies confirmed up-to-date via `apt install`
- Successful `CMake` configuration without critical errors
- Parallel build completed at 100% progress
- Installation placed libraries and headers in the expected system paths

Key Takeaways:

- ARM64 build for GVM libraries is straightforward when dependencies are satisfied.
- Pay attention to deprecation warnings for future-proofing builds.
- Installing with `sudo` ensures system-wide availability.

Next Steps:

- Proceed to build the other GVM components (like gvmd, gsa, openvas-scanner) in a similar fashion.
- Document any build or runtime issues for ARM64-specific quirks.
- Start integrating components and testing GVM functionality on the ARM64 environment.

Activity Report: GVM Docker Build

Date: 06/18/2025

Entry #: 37

Activity Name: GVM Docker Build

Tools/System Involved: Docker, GVM, Kali (UTM)

Priority: High

Description: Successfully deployed the Greenbone Community Edition stack using Docker on Kali ARM64 (via UTM). Created and validated all GVM volumes. Confirmed all containers are running.

Terminal Highlights:

- `Docker ps`: All services running
- **Volume inspection:** Confirmed ~13 volumes created
- Resized disk from 50GB to 100GB using `growpart` and `resize2fs`
- Verified free space increased (`df -h`)

Key Takeaways:

- Docker GVM can run on ARM64 with sufficient resources
- Disk space is critical—volume data sits in `/var/lib/docker`
- Volume inspection is key for data persistence validation

Next Steps:

- Run and validate the Windows VM scan
- Document vulnerabilities and severity
- Export scan report

Activity Report: GVM Recovery & Scan Prep

Date: 06/19/2025

Entry #: 38

Activity Name: GVM Recovery & Scan Prep

Tools/System Involved: Kali Linux (UTM ARM64), Docker / Docker Compose, Greenbone Community Edition (OpenVAS)

Priority: High

Description: Restored and reconfigured GVM after persistent socket failures and incomplete scans. Resized Kali's disk and extended the ext4 partition to free space for scan data. Pulled the latest containers, verified volume mounts, checked for the presence of the scanner socket, and validated the OSPD service. A stalled vulnerability scan was detected, and containers were redeployed. Explored fallback options via manual repository cloning.

Summary of Findings:

- Verified: `ospd-openvas.sock` present after full service reload
- Resolved container volume persistence issues
- Investigated git failures and repo fallbacks

Key Takeaways:

- ARM64 Docker deployments require aggressive manual verification (especially with persistent volumes and sockets).
- GVM feed load time is significant; scanning cannot start until VTs load (~70k+ signatures).
- Resetting Docker Compose brings stability but may require checking all layers (OS, volume space, runtime logs).
- GitHub repo issues and redirects may necessitate alternate cloning methods (`wget` failed, `git clone` with depth fixed).

Activity Report: GVM Recovery & Scan Prep

Date: 06/19/2025

Next Steps:

- Retest scan targeting after confirming `ospd-openvas.sock` is stable.
- Finalize the detailed MRCI lab submission once the scan completes.

Activity Report: DVWA Spider Crawl Setup

Date: 06/26/2025

Entry #: 39

Activity Name: DVWA Spider Crawl Setup

Tools/System Involved: Burp Suite Community Edition v1.7.36, Firefox, Apache2, MariaDB, PHP 8.4, DVWA, Terminal (Kali Linux ARM64)

Priority: High

Description: Today's session focused on configuring and launching Burp Suite's Spider against Damn Vulnerable Web Application (DVWA) for authenticated crawling. Key goals included setting up DVWA locally, proxying traffic through Burp, handling HTTPS trust errors, and confirming authenticated form submissions to enable deep site crawling.

Terminal Highlights:

```
sudo apt install apache2 php mariadb-server php-mysqli git
sudo mysql_secure_installation
sudo mariadb -u root -p
CREATE DATABASE dvwa;
CREATE USER 'dvwa'@'localhost' IDENTIFIED BY 'p@ssw0rd';
GRANT ALL PRIVILEGES ON dvwa.* TO 'dvwa'@'localhost';
FLUSH PRIVILEGES;
git clone https://github.com/digininja/DVWA.git
sudo nano /var/www/html/DVWA/config/config.inc.php
java -jar burpsuite_community_v1.7.36.jar
```

Activity Report: DVWA Spider Crawl Setup

Date: 06/26/2025

Key Takeaways:

- DVWA must be served using the exact directory name (`dvwa` lowercase) for Burp to track it correctly.
- Firefox must be explicitly configured to proxy local traffic by enabling `network.proxy.allow_hijacking_localhost`.
- Capturing login cookies is critical for authenticated crawling. Manual login followed by right-clicking "Spider from here" is the right workflow.
- Burp Spider prompts for form field values if a login is detected, enabling authenticated crawl automation.

Next Steps:

- Review results under Spider → Control to ensure 200+ requests.
- Capture screen recording showing:
  - Proxy intercept of `/login.php`
  - Spider auto-submitting login
  - Expanded site tree under Target → Site map
- Submit a video per MCSI requirements.

Activity Report: Use Burp Suite's Intruder Feature To Brute Force A Login Page

Date: 06/27/2025

Entry #: 40

Activity Name: Use Burp Suite's Intruder Feature To Brute Force A Login Page

Tools/System Involved: Burp Suite (Intruder), Firefox, DVWA (local instance)

Priority: Moderate

Description: Completed an exercise focused on brute-forcing a web login page using Burp Suite's Intruder feature. The objective was to simulate an attack scenario where weak credentials might allow unauthorized access to a system.

After intercepting the login request through Burp Proxy, it was transferred to Intruder, where payload positions were defined for credential fields. Custom payload lists were loaded to systematically test combinations. Response behaviors were analyzed to identify successful login attempts based on redirect patterns.

Summary of Findings:

- Intercepted POST request through Burp Proxy
- Configured Intruder payload positions using Cluster Bomb
- Loaded simplified credential wordlists
- Launched an attack and analyzed HTTP status codes and headers
- Verified successful login through manual browser test

Key Takeaways:

- Identical status codes can obscure brute force success — redirect destinations provide the true signal
- A successful brute-force attempt doesn't always change the response length or code
- Low-security settings in vulnerable applications are ideal for practicing tool workflows

Activity Report: Use Burp Suite's Intruder Feature To Brute Force A Login Page

Date: 06/27/2025

- Community Edition limits are manageable with scoped payloads

Next Steps: Submit video per MCSI requirements, then perform DNS scans using Fierce.

Activity Report: Use Dumpzilla To Extract Forensics Browser Logs

Date: 06/28/2025

Entry #: 41

Activity Name: Use Dumpzilla To Extract Forensics Browser Logs

Tools/System Involved: Dumpzilla, Firefox, Kali Linux Terminal

Priority: High

Description: Performed structured forensic data extraction from a browser profile using terminal-based tools. Handled issues related to file access, profile duplication, and output verification. Validated artifact collection integrity via command-line inspection.

Terminal Highlights:

- File and directory operations (`cp`, `rm`, `ls`, `cat`)
- Redirected tool outputs to named files
- Validated presence and content of extracted data

Key Takeaways:

- Importance of working from a clean and isolated workspace
- Profile data can easily be lost if directory paths are misused
- Tool-specific quirks (e.g., JSON parsing errors) must be handled gracefully

Next Steps:

- Record final demo video for submission
- Use PE Studio to analyze 5 files on my computer

Activity Report: Malware Lab Isolation Setup

Date: 06/29/2025

Entry #: 42

Activity Name: Malware Lab Isolation Setup

Tools/System Involved: UTM, Windows 10, PEStudio, Windows CMD, PowerShell

Priority: High

Description: Prepared a dedicated Windows 10 virtual machine for isolated malware analysis using PEStudio. Transferred malware and analysis tools into the VM, confirmed local storage, and removed all network interfaces and shared folder access to ensure air-gapping. Windows Defender was disabled, and tests confirmed 100% packet loss to external IPs (e.g., 8.8.8.8), validating full isolation. Snapshot planned post-verification.

Terminal Highlights:

```bash
ipconfig           → no IPv4 address assigned
ping 8.8.8.8       → 100% packet loss
net use Z: /delete → shared folder was mounted
```

Key Takeaways:

- Air-gapping requires more than removing internet — shared folders, and Defender also poses risks
- 192.168.x.x doesn't guarantee isolation — 100% ping loss is the real indicator
- Isolation-first is the safest workflow for handling malware, even during static analysis

Activity Report: Malware Lab Isolation Setup

Date: 06/29/2025

Next Steps:

- Re-copy and extract PEStudio properly
- Extract malware sample and begin PEStudio analysis
- Begin drafting answers for report questions
- Take a clean snapshot of the fully isolated and tool-ready VM

Activity Report: PEStudio Static Analysis

Date: 07/01/2025

Entry #: 43

Activity Name: PEStudio Static Analysis

Tools/System Involved: PEStudio, certutil, pefile (Python)

Priority: High

Description: Performed static analysis on five Windows PE files, including system binaries and a provided malware sample. Tasks included hash generation, signature verification, import/export analysis, and header inspection. One sample was replaced due to missing string data in PEStudio.

Summary of Findings:

- Used certutil to manually generate and verify SHA256 and MD5 hashes
- Used PE header fields (*Magic*, *Characteristics*) to confirm PE type
- Analyzed signature data and expiration using PEStudio's Signature tab

Key Takeaways:

- File extensions are unreliable, PE headers provide accurate classification
- Some signed files had expired certificates; unsigned files were also common
- PEStudio may show string counts but fail to render them; sample substitution resolved the issue

Next Steps:

- Finalize and submit the formatted PDF report
- Upon successful submission and certificate issuance, this will mark the completion of the *Introduction to Cybersecurity* course.

Activity Report: DNS Query Analysis

Date: 07/02/2025

Entry #: 44

Activity Name: DNS Query Analysis

Tools/System Involved: `dig`, Terminal, DNS protocol documentation, *Computer Networking: Principles, Protocols, and Practice* by Olivier Bonaventure

Priority: High

Description: Performed a technical deep dive into how DNS functions under different conditions by issuing real-time queries using the `dig` tool. Followed recursive queries from root to authoritative servers, identified IP addresses of all 13 root DNS servers, and analyzed DNS behavior when subjected to spoofing conditions.

Summary of Findings:

- Queried root servers using `dig . NS`
- Retrieved IPv4/IPv6 addresses of root servers
- Examined TTL values and MX records for multiple domains
- Observed response behavior to modified Query IDs (spoofing simulation)

Key Takeaways:

- DNS root servers are reachable via both IPv4 and IPv6
- Query ID randomization helps mitigate spoofing attacks
- TTL values are critical in caching behavior and resolution speed
- MX records reveal the mail handling setup of a domain, useful in recon

Next Steps:

- Document results and screenshots in my DNS analysis report
- Compare behavior across different resolver configurations

Activity Report: DNS Query Analysis

Date: 07/02/2025

- Explore DNSSEC to understand further protections

Activity Report: MSAF Enrollment & Blog Draft

Date: 07/03/2025

Entry #: 45

Activity Name: MSAF Enrollment & Blog Draft

Tools/System Involved: Mossé Cyber Security Institute (OLP), MICS Certificate Dashboard, Confirmation of Enrolment Letter, Portfolio Website, Hemingway App

Priority: High

Description: Documented my transition from completing MICS to enrolling in the MSAF - System Administration Fundamentals course. Verified and reviewed my Cybersecurity Learner Level 1, 2, and 3 certificates from MICS.

Drafted a full-length blog post that outlines key takeaways from MICS, reasons for choosing MSAF, and what practical system administration skills I'll gain.

Terminal Highlights: *N/A – research and documentation day*

Key Takeaways:

- MICS course completion gave me 3 stackable certifications tied to practical labs
- MSAF will build deeper system-level skills across Windows, Linux, and virtual environments
- Publicly documenting transitions boosts credibility and portfolio visibility

Next Steps:

- Publish a blog on my site or LinkedIn
- Add MSAF to the LinkedIn Education section with trimmed 500- and 1000-character bios
- Begin working through MSAF virtualization exercises

Activity Report: Virtual Network Modes Report

Date: 07/04/2025

Entry #: 46

Activity Name: Virtual Network Modes Report

Tools/System Involved: VirtualBox Manual, Google Sheets, UTM (ARM), Kali Linux ARM, Grammarly, Quillbot

Priority: High

Description: Finished a detailed report on virtual network modes in virtualization platforms. It explains different adapter types, when to use them, and what they mean for system admins. The report points out compatibility issues with Apple Silicon. Clear tables and diagrams are included to make the information easy to follow.

Summary of Findings:

- Verified hardware limitations on Apple M2
- Used `UTM` for ARM-based network simulation
- Referenced VirtualBox official documentation
- A diagram comparing virtualization architectures

Key Takeaways:

- Networking modes differ significantly in isolation, reachability, and lab safety
- Visual aids and comparison tables support comprehension
- Apple Silicon hardware introduces real-world testing constraints

Next Steps: Finalize the second exercise, Research and explain the role of virtualization and its benefits for cybersecurity

Activity Report: Virtualization and Hypervisors

Date: 07/05/2025

Entry #: 47

Activity Name: Virtualization and Hypervisors

Tools/System Involved: Windows Documentation, Microsoft Learn, UTM, Diagram Generator, Grammarly, Quillbot

Priority: High

Description: Completed a detailed report on virtualization and hypervisor technology. Explained Windows virtualization features and BIOS/UEFI settings. Comparing Type-1 and Type-2 hypervisors. Added original diagrams and screenshots to highlight platform limits and options for macOS M2 systems

Summary of Findings:

- Described steps to enable virtualization in the BIOS
- Compared to Hyper-V, Sandbox, WSL2, and VMP
- Generated Type-1 vs Type-2 hypervisor diagram
- Used UTM screenshots to supplement hardware limitations

Key Takeaways:

- Virtualization enables safe, isolated cybersecurity testing.
- Hypervisor selection depends on performance, compatibility, and use case
- Apple M2 requires ARM-compatible tools like UTM and Parallels

Next Steps: Begin next system administration exercise (Lab Setup: Install Windows Subsystem for Linux.

Activity Report: WSL Installation

Date: 07/06/2025

Entry #: 48

Activity Name: WSL Installation

Tools/System Involved: PowerShell, Microsoft Store, Ubuntu WSL

Priority: Moderate

Description: Turned on Windows Subsystem for Linux and Virtual Machine Platform on Windows 10 using PowerShell. Installed Ubuntu from the Microsoft Store and finished the setup. Opened the Ubuntu shell and created a test file in the home folder.

Summary Findings:

- Successfully enabled WSL and required platform features on Windows 10.
- Installed and launched a Linux distribution from the Microsoft Store without issues.
- Confirmed ability to navigate the Linux shell and create files in the home directory.
- The environment is ready for further system administration and scripting tasks.

Key Takeaways:

- Enabled WSL features quickly via the command line with minimal issues.
- The Ubuntu installation from the Microsoft Store was straightforward.
- Demonstrated ability to access and manage a Linux environment inside Windows 10 through WSL.

Next Steps: Lab Setup: Deploy a Virtual Machine in GCP

Activity Report: Deploy GCP VM

Date: 07/08/2025

Entry #: 49

Activity Name: Deploy GCP VM

Tools/System Involved: Google Cloud Console, SSH, Kali Terminal

Priority: High

Description: Deployed an Ubuntu virtual machine on Google Cloud Platform from start to finish. Created a new SSH key pair on Kali, configured firewall rules, attached the public key to the VM, and connected via SSH successfully. Recorded all steps in a quiet 3-minute demo video for the lab submission.

Summary Findings:

- Successfully generated an RSA SSH key pair with a custom comment.
- Configured firewall rules to allow SSH access (TCP port 22) to the VM.
- Deployed an Ubuntu VM instance on Google Cloud Platform.
- Verified SSH connectivity from Kali Linux host using private key authentication.
- Demonstrated secure remote access with a minimal Linux environment.

Key Takeaways:

- The correct username and public key format are critical for successful SSH access.
- GCP firewall rules must allow TCP port 22.
- A clean SSH connection confirms proper configuration from the local to the cloud environment.

Next Steps: Lab Setup: Deploy a Virtual Machine in AWS

Activity Report: Report Structuring & AWS Lab Submission

Date: 07/09/2025

Entry #: 50

Activity Name: Report Structuring & AWS Lab Submission

Tools/System Involved: Google Docs, Hemingway App, Semantic Versioning, NIST SP 800-30 Rev. 1, AWS Console, DreamCreator 8 Screen Recording Software

Priority: High

Description: Completed structural revisions and formatting for three cybersecurity assessment reports:

- Access Control Incident
- Server Security Evaluation
- USB Security Risk Assessment

Each report was updated with clear section headers, numbering, and conclusions following professional standards and NIST guidelines. Also submitted a **video lab submission** for **Lab Setup: Deploy a Virtual Machine in AWS**, demonstrating secure provisioning in a cloud environment.

Terminal Highlights: N/A – Work focused on report writing and cloud lab setup through web interface.

Key Takeaways:

- Consistency in report formatting boosts clarity and professional credibility.
- Learned to apply semantic versioning appropriately based on the scope of report changes.
- Reinforced understanding of AWS instance deployment and cloud infrastructure basics.

Activity Report: Report Structuring & AWS Lab Submission

Date: 07/09/2025

Next Steps:

- Finalize export of each report as a polished PDF for portfolio inclusion.
- Begin outlining the next lab report: Create a Virtual Machine in VMware.
- Optionally create stylized social media posts for AWS VM deployment.

Activity Report: VMware Lab Planning & Report Workflow Continuation

Date: 07/10/2025

Entry #: 51

Activity Name: VMware Lab Planning & Report Workflow Continuation

Tools/System Involved: VMware Fusion (Mac), Google Docs, Markdown, NIST SP 800-53, Hemingway App

Priority: Moderate

Description: Initiated planning for the next lab exercise: **Create a Virtual Machine in VMware**. Looked at compatibility issues and how to set up the ISO for Apple Silicon. Continued updating the reports by finishing structural changes in the USB Security Risk Assessment and Server Security Evaluation. I ensured the access control documents match NIST SP 800-53 (AC-6) standards. Changed the titles and conclusions for better clarity.

Summary of Findings:

- Explored VMware Fusion ISO configuration paths
- Reviewed system settings for ARM64 compatibility

Key Takeaways:

- Apple Silicon requires alternate VM setup workflows compared to traditional x86 architecture
- Finalizing report structure across multiple assessments strengthens consistency and version control discipline
- Proactive planning ensures smoother execution for the upcoming VMware lab

Next Steps:

- Finalize export of all completed reports as polished PDFs
- Begin VMware lab execution and produce a clean screen recording

Activity Report: VM Networking + Snapshot Recovery

Date: 07/11/2025

Entry #: 52

Activity Name: VM Networking + Snapshot Recovery

Tools/System Involved: VMware Fusion, Kali Linux ARM, Windows 11 ARM, VirtIO Drivers, Windows Firewall

Priority: Low

Description:

Completed two core system administration tasks in VMware Fusion on macOS (M2):

1. Set up and configured Kali Linux and Windows 11 ARM virtual machines
2. Turned on NAT networking and fixed Windows firewall issues to allow ICMP/ping from Kali to Windows
3. Took a snapshot of the Windows VM to preserve a clean, configured state for future use

Terminal Highlights:

bash

```
ip a          # Checked Kali IP address

ping <win-ip>    # Validated network connectivity from Kali to Windows

# Windows CMD:

ipconfig

ping <kali-ip>
```

Activity Report: VM Networking + Snapshot Recovery

Date: 07/11/2025

Key Takeaways:

- Windows 11 ARM needs VirtIO drivers and firewall rule adjustments for proper networking in VMware Fusion on Apple Silicon.
- Snapshots help keep a safe system backup before testing, tool deployment, or major configuration changes.

Next Steps: Install and configure VMware ESXi with vSphere on both Windows and Linux VMs for advanced virtualization and enterprise lab environments.

Activity Report: ESXi Compatibility Check

Date: 07/12/2025

Entry #: 53

Activity Name: ESXi Compatibility Check

Tools/System Involved: VMware ESXi, macOS (M2), VMware Fusion, OVH (researched)

Priority: High

Description: Reviewed the new exercise requiring VMware ESXi installation. Identified that ESXi is not compatible with macOS running on Apple Silicon (M2). ESXi requires bare-metal or nested x86 virtualization, which is not supported in Fusion on ARM architecture. Prepared a brief inquiry to the instructor seeking alternative options without suggesting workarounds.

Summary of Findings:

- ESXi is a Type 1 hypervisor and not supported on Apple Silicon (ARM).
- VMware Fusion does not allow nested ESXi on M1/M2 hardware.
- A bare-metal environment is required for full functionality.
- Cloud providers (e.g., OVH) offer possible solutions if approved.

Key Takeaways:

- ESXi does not support macOS ARM setups.
- Nested virtualization is not viable with Fusion on Apple Silicon.
- Instructor guidance is needed before proceeding.

Next Steps:

- Await the instructor's response on the acceptable alternative.
- Prepare to pivot to OVH bare metal if approved.
- Document findings in the final report to show the technical evaluation effort.

Activity Report: Grammarly Writing Enhancement

Date: 07/13/2025

Entry #: 54

Activity Name: Grammarly Writing Enhancement

Tools/System Involved: Grammarly, Hemingway App, Word Processor (Google Docs)

Priority: Moderate

Description: Completed an editing task to improve the spelling and grammar of a technical report using Grammarly. The original content focused on front-running in DeFi vs. CeFi. The exercise required demonstrating clear improvements between the unedited (MISTAKE) and edited (FINAL) versions. The final version showed corrected grammar, better sentence flow, and improved formatting with section numbers.

Summary of Findings:

- Grammarly successfully detected and suggested fixes for sentence structure, passive voice, article usage, and punctuation errors.
- Section headers and numbering were added for a clearer structure.
- A descriptive introduction was written to explain the purpose of the exercise.
- Revision History was updated to reflect changes and submission ID.

Key Takeaways:

- Grammarly is a powerful tool for refining both technical and business writing.
  Well-structured writing is just as important as technical accuracy in cybersecurity reporting.
- Version control and documentation (e.g., revision history) improve professionalism.

Next Steps: May take a couple of days off to complete a 7-day fasting schedule.

Activity Report: Grammarly Writing Enhancement

Date: 07/13/2025

Will resume coursework after adequate refeeding and recovery time.

Activity Report: Report Polish & Format Revisions

Date: 07/14/2025

Entry #: 55

Activity Name: Report Polish & Format Revisions

Tools/System Involved: Grammarly, Hemingway App, Google Docs

Priority: Moderate

Description: Finalized formatting on multiple cybersecurity reports, including the Server Security Evaluation and USB Risk Assessment. Edits included improved section numbering, clearer headings, and alignment with portfolio standards.

Summary of Findings: Enhanced consistency, improved clarity, added NIST references.

Key Takeaways: Structure and visual layout matter as much as technical accuracy.

Next Steps: Waiting for instructor response on my question about a compatibility issue for the exercise "*Install and configure VMware ESXi with Vsphere in Windows and Linux VMs*".

Activity Report: ESXi VM Connectivity Test Submission

Date: 07/15/2025

Entry #: 56
Activity Name: ESXi VM Connectivity Test Submission
Tools/System Involved: VMware vSphere Hands-on Labs, ping, ifconfig
Priority: High
Description: Tested basic network connectivity between Linux and Windows VMs in VMware's Hands-on Lab. Captured and submitted screen recording as part of lab requirements..
Summary of Findings: Successful ping from Linux → Windows
Key Takeaways: Connectivity worked inside the VM Network.
Next Steps: Await instructor feedback.

Activity Report: ESXi VM Connectivity Test Resubmission

Date: 07/16/2025

Entry #: 57
Activity Name: ESXi VM Connectivity Test Resubmission
Tools/System Involved: VMware vSphere Hands-on Labs, ping, ifconfig
Priority: High
Description: Corrected IP address entry and re-tested VM connectivity. Captured and resubmitted screen recording as part of lab requirements..
Summary of Findings: Successful ping from Linux to Windows
Key Takeaways: The Wrong IP address caused the previous failure.
Next Steps: Rerecord the final clip and resubmit.

Activity Report: OSI vs TCP/IP Report Drafting

Date: 07/17/2025

Entry #: 58
Activity Name: OSI vs TCP/IP Report Drafting
Tools/System Involved: Grammarly, Hemingway App, Google Docs
Priority: Moderate
Description: Drafted professional report comparing OSI and TCP/IP models, with emphasis on cybersecurity implications like segmentation, defense in depth, and protocol isolation.
Summary of Findings: Highlighted how OSI layers guide security architecture and packet inspection.
Key Takeaways: The OSI model isn't just theory—it helps guide practical cybersecurity architecture.
Next Steps: Finalize with comparison tables and visual aids.

Activity Report: OSI vs TCP/IP Security Analysis Report

Date: 07/18/2025

Entry #: 59

Activity Name: OSI vs TCP/IP Security Analysis Report

Tools/System Involved: Grammarly, Hemingway App, Google Docs, Google IT Support Course Study Notes

Priority: Low

Description: Worked on a cybersecurity report comparing the OSI and TCP/IP models. Changed section headers to make them clearer and easier to follow. Used Grammarly and Hemingway to keep the language simple, around a Grade 9 level. Added study notes to match protocols with their behaviors and vulnerabilities. Updated diagrams to show which threats affect a specific layer.

Summary of Findings:

- Each model shows different views of network-layer threats.
- OSI separates layers more clearly in theory, while TCP/IP matches how systems work in real life.
- Both need layers of defense, but TCP/IP's simpler design can hide some risks.
- Diagrams and clear labels help link threats to the right layers.

Key Takeaways:

- Clear words and pictures make technical ideas easier to understand.
- Matching cyber risks to layers helps make reports more exact.
- Leveraging different writing tools improves tone and meets client-friendly standards.

Activity Report: OSI vs TCP/IP Security Analysis Report

Date: 07/18/2025

Next Steps:

- Finish examples of common attacks for each layer.
- Do one last check of grammar and formatting.
- Save the PDF version for submission to the instructor and wait for a response.

Activity Report: Router Documentation & Equipment Analysis

Date: 07/19/2025

Entry #: 60

Activity Name: Router Documentation & Equipment Analysis

Tools/System Involved: Grammerly, Hemingway App, Google Docs, Google IT Support Course Study Notes, PlagiarismDetector.net

Priority: Moderate

Description: Wrote and finalized the router section for the hardware analysis report. Covered core functions, enterprise usage, pros, and cons—maintaining a clear, Grade 9 reading level. Ensured content was fully original, non-plagiarized, and aligned with portfolio-quality standards. Cross-referenced with earlier entries (hub, switch) to ensure consistent formatting and tone.

Summary of Findings:

- Routers interconnect separate networks using IP-based routing.
- Enterprise routers often bundle in firewalls and ACLs.
- Misconfiguration can pose serious security risks.
- Regular updates and monitoring are essential for router security.

Key Takeaways:

- Routers are important for linking local networks to the internet.
- Most business routers come with built-in security features like firewalls and access control lists.
- When writing about technical equipment for others to read, it's important to keep things clear and consistent.
- All the content I wrote was in my own words, not copied from AI or any other source.

Next Steps: Put all the completed parts together into a nicely formatted report to

Activity Report: Router Documentation & Equipment Analysis

Date: 07/19/2025

submit.

Activity Report: Enterprise Networking Devices

Date: 07/20/2025

Entry #: 61

Activity Name: Enterprise Networking Devices

Tools/System Involved: Google Sheets & Docs, Hemingway App, Wikimedia Commons OSI Model Reference, Google IT Support Course Study Notes, PlagiarismDetector.net

Priority: High

Description: Researched the most common types of networking equipment used in enterprise networks. Mapped each device to the appropriate OSI layer and documented their primary roles, typical use cases, pros/cons, and security implications.

Summary of Findings:

Identified 10 key devices and aligned them with OSI layers and enterprise use cases. Developed a cleaned-up table format optimized for technical clarity and space constraints (Google Sheets version).

Key Takeaways:

- Reinforced OSI model layer functions
- Recognized how each device fits into secure enterprise architecture
- Practiced clean technical documentation for real-world reporting

Next Steps:

Activity Report: Network Diagram Recon & Planning

Date: 07/21/2025

Entry #: 62

Activity Name: Network Diagram Recon & Planning

Tools/System Involved: Draw.io (sketch planning)

Priority: High

Description:

Began reconnaissance and planning for a static network diagram for a small business with 100 employees. Reviewed lab requirements and identified key components to include—such as web, file, DNS, and SQL servers, as well as workstations, printers, routers, switches, firewalls, VPN, and a DMZ.

Summary of Findings:

Sketched initial layout concepts based on standard enterprise segmentation practices. Mapped out device categories and researched secure placement strategies based on function and access level.

Key Takeaways:

- Strengthened understanding of secure network layout principles
- Reviewed best practices for server placement and network segmentati
- Prepared a foundation for translating conceptual plans into a visual diagram

Next Steps:

Start building the full diagram in Draw.io with labeled segments, enforce logical flow paths, and apply cybersecurity best practices (firewalls, isolation, access control).

Activity Report: Static Network Diagram

Date: 07/22/2025

Entry #: 63

Activity Name: Static Network Diagram

Tools/System Involved: Draw.io

Priority: High

Description: I built and labeled a static network diagram for a small business with 100 users. I segmented the network into three zones: Perimeter, DMZ, and Internal. The diagram shows a simple, functional enterprise design aligned with cybersecurity best practices. I placed switches, firewalls, servers, and user groups in the right zones and added security controls. The diagram follows basic cybersecurity rules, with firewalls between zones and a VPN ready.

Summary of Findings:

- Final design includes perimeter, DMZ, and internal LAN segmentation.
- All key devices and departments labeled clearly (e.g., Support Dept, SQL Server).
- Traffic flow indicated with arrows and strategic switch placements for clarity.

Key Takeaways:

- Network diagrams should be easy to read and follow a clear structure.
- Segmenting zones helps control access and reduce risks.
- Simple layouts still need to meet technical needs.

Next Steps:

- Download and install Cisco Packet Tracer
- Start dynamic 1,000-user network design with best practices

Activity Report: IPSec Tunnel Attempt

Date: 07/23/2025

Entry #: 64

Activity Name: IPSec Tunnel Attempt

Tools/System Involved: Cisco Packet Tracer v.8.2.2, Google Docs, Hemingway App, PlagiarismDetector.net

Priority: High

Description: Tried setting up a secure tunnel between two networks. Used the command line interface (CLI) to apply interface and security commands. Hit repeated command line errors when assigning commands. Packet Tracer didn't support key command line inputs needed to move forward.

Summary of Findings: Couldn't finish the configuration. CLI commands failed. Packet tracer didn't allow the current network configuration setup for a working tunnel.

Key Takeaways:

- Cisco Packet Tracers limitations and system bugs blocked progress
- Logged CLI errors for later review
- Need a clean topology environment to test advanced configurations

Next Steps:

- Check how Packet Tracer supports the IPSEC tunnel
- Check know bugs and bugs within Packet Tracer
- Start fresh with just the basic router configuration

Activity Report: VPN Tunnel Diagnostics

Date: 07/24/2025

Entry #: 65

Activity Name: VPN Tunnel Diagnostics

Tools/System Involved: Cisco Packet Tracer v.8.2.2, Google Docs, Hemingway App, PlagiarismDetector.net

Priority: Low

Description: Worked on resolving the VPN tunnel failure between VLAN2 and VLAN3 routers. Verified Layer 3 connectivity by testing public IP reachability between both peers. Found and removed a misconfigured ISAKMP key on VLAN3 that referenced its own address.

Set default static routes on both routers, pointing to the ISP router to enable external traffic flow. Generated interesting traffic from VLAN2 to VLAN3 internal hosts to trigger Phase 1 tunnel negotiation. Used `show crypto isakmp sa` and `show crypto ipsec sa` to monitor tunnel status. I may use debug commands if the tunnel remains down.

Summary of Findings:

- Verified that VLAN3 can reach VLAN2's public IP, confirming Layer 3 connectivity
- Removed an incorrect ISAKMP key on VLAN3 that pointed to its own address
- Static default routes configured correctly on both routers toward the ISP
- Initiated internal traffic between VLAN2 and VLAN3 to prompt VPN negotiation

Key Takeaways:

- Successful VPN setup depends on confirmed Layer 3 reachability between peers
- ISAKMP key configuration must be accurate and reciprocal on both sides

Activity Report: VPN Tunnel Diagnostics

Date: 07/24/2025

- Crypto ACLs must match the traffic — otherwise the tunnel won't initiate
- Debugging is essential for isolating handshake issues during Phase 1 & Phase 2

Next Steps:

- Confirm consistent bidirectional public IP ping results
- Monitor tunnel state using show commands after triggering traffic
- If the tunnel remains inactive, activate debug logging to trace negotiation
- Adjust VPN settings or ACLs based on debug output

Activity Report: IPSec Tunnel Debug & Core Network Build

Date: 07/25/2025

Entry #: 66

Activity Name: IPSec Tunnel Debug & Core Network Build

Tools/System Involved: Cisco Packet Tracer v8.2.2, Google Docs, Hemingway App, plagiarismdetector.net

Priority: High

Description: Description:

Today's focus was on fixing an IPSec VPN tunnel between the main and remote offices in Cisco Packet Tracer. The tunnel was partially working, traffic was being decrypted, but key pings from the 192.168.20.0 network to the 192.168.30.0 network weren't being decapsulated. This either pointed to a send error, policy mismatch, or ACL problem.

At the same time, I built the core network infrastructure. I created VLANs and configured a Multilayer Switch (MLS) using a routed port and Switch Virtual Interfaces (SVIs) to handle inter-VLAN routing. I also confirmed that both VPN routers could ping each other over their public IPs, proving the WAN connection works.

On the head office's firewall, I cleared up command-line confusion and designed out a plan to use the packet-tracer command to simulate how traffic is handled, if the tunnel still fails after retesting.

Summary of Findings:

- `show crypto ipsec sa` showed decryption but **no decapsulation**
- Created VLANs 10, 20, and 30 with port assignments
- Set up SVIs and a routed uplink on the MLS
- Verified WAN connectivity with successful pings: `203.0.113.5 ↔ 203.0.113.1`

Activity Report: IPSec Tunnel Debug & Core Network Build

Date: 07/25/2025

Key Takeaways:

- IPSec tunnels can fail if crypto ACLs or routing paths are misaligned
- A clean Layer 2/3 core simplifies VPN problem-solving
- Verifying public IP reachability confirms the base tunnel path
- Cisco's packet tracer tool will help simulate and diagnose traffic issues

Next Steps:

- Retest tunnel using internal PC ping
- Review ISAKMP and IPSec SA status on both routers
- Double-check NAT, ACLs, and crypto maps for accuracy

Activity Report: Multi-Router NAT Debug & PC Packet Drop

Date: 07/26/2025

Entry #: 67

Activity Name: Multi-Router NAT Debug & PC Packet Drop

Tools/System Involved: Cisco Packet Tracer v8.2.2, Google Docs, Hemingway App, plagiarismdetector.net

Priority: High

Description: I conducted an intensive troubleshooting of a enterprise network on Packet Tracer involving multi-router NAT commands. I began by verifying topology clarity, confirming router interface configurations, and validating NAT functionality. A key finding was that while the network infrastructure (Layer 3) and NAT were working, the PC remained unreachable despite correct IP settings.

Packet simulation logs pointed to a local host issue where packets were being dropped due to no service listening—most likely caused by the simulated firewall behavior or software glitch.

Summary of Findings:

- `show ip interface brief` output confirmed all router interfaces were *up/up*
- `debug ip nat` revealed successful translation and de-translation on ISP Router
- Manual reconfiguration of PC IP to 10.0.20.2 / Gateway 10.0.20.1
- Packet Trace message: *"The device does not have a service that accepts this frame."*

Key Takeaways:

- NAT on all routers was operational and confirmed via live packet inspection.
- Simulation issues may stem from firewall emulation or Packet Tracer instability.

Activity Report: Multi-Router NAT Debug & PC Packet Drop

Date: 07/26/2025

- Even when networking fundamentals are correct, endpoint configuration errors (firewall, service listeners) can block successful communication.

Next Steps:

- Reboot all virtual devices and restart Packet Tracer to clear simulation bugs.
- Temporarily disable simulated firewall settings if available.
- Confirm basic services (e.g., ICMP or web) are active on the PC node.
- If unresolved, rebuild PC node or topology segment from scratch.

Activity Report: Internet Connectivity & NAT Debugging

Date: 07/27/2025

Entry #: 68

Activity Name: Internet Connectivity & NAT Debugging

Tools/System Involved: Cisco Packet Tracer v8.2.2, Google Docs, Hemingway App, plagiarismdetector.net

Priority: High

Description: Focused on securing full internet connectivity through the remote office's firewall and diagnosing NAT issues on the router remote office's edge firewall/router. Key configurations on the "ISP Server" and ISP-Router were validated. Successfully enabled ICMP traffic from the firewall (remote office's firewall) to external IPs (8.8.8.8). Investigated NAT translation issues and discovered a critical misconfiguration: no ip cef was unintentionally disabling NAT processing.

Summary of Findings:

- `ping 8.8.8.8` successful from NY-FW
- `show ip nat statistics` revealed *misses*, confirming translation not occurring
- `no ip cef` removed, allowing NAT to function properly
- `debug ip packet` returned no output, indicating possible Packet Tracer quirk or traffic misdirection

Key Takeaways:

- Removing `no ip cef` was essential—CEF is a prerequisite for NAT operations.

Activity Report: Internet Connectivity & NAT Debugging

Date: 07/27/2025

- Packet Tracer’s simulation limits can obscure actual packet behavior.
- NAT troubleshooting often requires confirming both translation stats *and* packet flow visibility.

Next Steps:

- Restart Packet Tracer and reinitiate NAT tests fromremote office’s edge firewall/router
- Use `debug ip packet` during controlled pings to verify data path integrity
- Confirm if the issue lies in traffic not reaching NY-FW or in simulation artifacts

Activity Report: Network NAT Troubleshooting

Date: 07/28/2025

Entry #: 69

Activity Name: Network NAT Troubleshooting

Tools/System Involved: Cisco Packet Tracer v8.2.2, Google Docs, Hemingway App, plagiarismdetector.net

Priority: High

Description:

Today I focused on identifying and resolving persistent ping failures from remote office's pc to the ISP-Router and the wider internet. The root issue stemmed from an incomplete understanding of the routing path and NAT configurations on a multi-router setup within the B segment of the network.

Summary of Findings:

- Discovered a key network topology detail: a three-step router path from remote office's pc →remote office's edge firewall/router → remote office's firewall → ISP-Router.
- Adjusted IP configurations on remote office's firewall to align with the correct routing path.
- Verified link states and IP bindings via show ip interface.
- Implemented static routes onremote office's edge firewall/router and remote office's firewall to ensure upstream connectivity.
- Applied NAT configurations toremote office's edge firewall/router, but encountered NAT status issues on both routers.
- Identified likely emulation-related bug in Packet Tracer requiring a power cycle to activate NAT features.

Activity Report: Network NAT Troubleshooting

Date: 07/28/2025

Key Takeaways:

- Accurate topology understanding is essential before applying routing or NAT solutions.
- Multi-router setups require coordinated IP schemes and static routes for successful packet forwarding.
- Packet Tracer’s emulation quirks can delay NAT activation even when configurations appear correct

Next Steps:

- Power cycleremote office’s edge firewall/router and remote office's firewall to trigger NAT functionality.
- Confirm NAT configuration is applied and functional on remote office's firewall.
- Re-test end-to-end connectivity from remote office’s pc to internet endpoints (e.g., 8.8.8.8).
- Proceed to VPN configuration once basic internet access is validated.

Activity Report: NAT & Routing Fixes – Remote Office Segment

Date: 07/29/2025

Entry #: 70

Activity Name: NAT & Routing Fixes – Remote Office Segment

Tools/System Involved: Cisco Packet Tracer v8.2.2, Google Docs, Hemingway App, plagiarismdetector.net

Priority: High

Description: Today's session focused on fixing persistent network issues between remote office's pc and the simulated Internet in a complex, multi-router environment. The network involved a two router chain in the remote branch: remote office's pc → remote office's edge firewall/router → ISP-Router. Initial symptoms showed failed pings and unreachable networks, despite correct-looking configs.

I identified that incomplete static routes and NAT configuration gaps were blocking outbound traffic. After correcting the IP addressing on remote office's firewall and reapplying static routes, I ran into NAT activation issues. These issues didn't respond to proper syntax and required a full power cycle of the devices—pointing to simulation limitations in Packet Tracer.

Summary of Findings:

- `show ip interface brief` verified all interface states were up/up.
- Applied static routes on remote office's edge firewall/router for proper next-hop reachability.
- Configured NAT rules on remote office's edge firewall/router, but `show ip nat translations` returned empty—until power cycling.
- NAT ACLs defined for outbound Internet traffic (`permit ip 10.10.30.0 0.0.0.255 any`).

Activity Report: NAT & Routing Fixes – Remote Office Segment

Date: 07/29/2025

Key Takeaways:

- You must understand the full router chain before applying NAT or routing.
- Static routes must be paired with proper NAT rules for Internet access.
- Packet Tracer sometimes delays NAT activation—device reboots may be needed.
- Even when the config is correct, emulation bugs can cause misleading failures.

Next Steps:

- Confirm NAT is fully working on **remote office's firewall/router**.
- Re-test ping from **remote office's pc** to **8.8.8.8** to verify external reachability.
- Once Internet is confirmed, move to setting up and verifying the VPN tunnel

Activity Report: IPSec VPN Tunnel Debug

Date: 07/30/2025

Entry #: 71

Activity Name: IPSec VPN Tunnel Debug

Tools/System Involved: Cisco Packet Tracer v8.2.2, Google Docs, Hemingway App, plagiarismdetector.net

Priority: High

Description: Today's focus was on diagnosing and resolving a persistent issue preventing Phase 1 and Phase 2 of an IPSec VPN tunnel from establishing between two network endpoints: home office's firewall and remote office's firewall.

Initial configurations had been completed on both devices, including ISAKMP policy creation, crypto map application, and ACL definitions for interesting traffic. Despite this, no Security Associations (SAs) were forming.

After extensive troubleshooting, a critical issue was identified: neither endpoint could ping the other's public IP. Investigation revealed Layer 2 ARP resolution problems on the ISP link, confirmed by `debug` output from the ISP-Router showing encapsulation failures.

Summary of Findings:

Breakthrough Achieved: The public IP connectivity between remote office's firewall and home office's firewall is now fully operational. Both routers and connected PCs can reach external addresses (e.g., 8.8.8.2).

Configuration Mismatches Persist:

- remote office's firewall and home office's firewall are still missing key ISAKMP parameters: `hash sha`, `lifetime 86400`, and `mode tunnel`.

Activity Report: IPSec VPN Tunnel Debug

Date: 07/30/2025

- home office's firewall has a mismatched pre-shared key and group number.
- Direct command changes to crypto maps and transform-sets failed due to dependency locks, prompting a new reconfiguration strategy.

Key Takeaways:

- **Connectivity Comes First:** IPSec tunnels cannot form without successful Layer 3 connectivity. Diagnosing routing and ARP failures early prevents wasted effort on higher-layer configs.
- **Precise Matching is Essential:** VPNs require exact parameter matching for ISAKMP Phase 1 and IPSec Phase 2 to succeed.
- **Dependency Awareness:** In-use crypto maps block edits to transform-sets and policies. A correct workflow involves temporarily removing the crypto map from the interface.

Next Steps:

1. Apply the consolidated configuration fixes to both remote office's firewall and home office's firewall, ensuring group, key, hash, lifetime, and mode settings align.
2. Re-attach crypto maps after modification.
3. Trigger interesting traffic from LAN to LAN to initiate the tunnel. Verify establishment with `show crypto isakmp sa` and `show crypto ipsec sa`.

Activity Report: IPSec VPN Tunnel Debug

Date: 07/30/2025

4. Document successful tunnel establishment with updated configurations.

Activity Report: Guest Network Internet Access & VPN Tunnel Prep

Date: 07/31/2025

Entry #: 72

Activity Name: Guest Network Internet Access & VPN Tunnel Prep

Tools/System Involved: Cisco Packet Tracer v8.2.2, Google Docs, Hemingway App, plagiarismdetector.net

Priority: High

Description: Today marked a major breakthrough in completing the internet access path for the guest VLAN (192.168.50.0/24). I checked the full path. I confirmed that guest PC traffic is routed through head office's guest services router, multi-layer switch, edge firewall, and then out to the simulated internet.

The main issue blocking traffic was a **recursive static route misconfiguration** on multi-layer switch. Which sent the guest network route back to itself (10.0.0.1). Guest traffic now goes through guest services router's 192.168.41.2 interface. This resolved the return path and restored full connectivity.

I also looked at nuanced behaviors in Packet Tracer. Particularly around **ARP cache behavior and command inconsistencies**. I used `debug ip packet` on Guest Services router. This confirmed that the device was handling traffic. It helped me pinpoint troubleshooting problems.

The second half of the session I moved toward VPN setup. I prepared for IPSec tunnel deployment. Initial checks revealed **Phase 1 (ISAKMP) is not coming up**. `show crypto isakmp sa` was empty on the company's firewall. This sets the stage for tomorrow's focus on ISAKMP policy verification and deeper tunnel

Activity Report: Guest Network Internet Access & VPN Tunnel Prep

Date: 07/31/2025

diagnostics.

Summary of Findings:

- Corrected recursive static route on causing packet loops.
- Verified successful outbound traffic flow for guest network.
- Identified early indicators of VPN tunnel misconfig (Phase 1 ISAKMP not forming).
- Utilized `debug ip packet` for real-time path tracing.
- Gained insight into how Packet Tracer handles ARP behavior and crypto output.

Key Takeaways:

- Always verify the **next-hop IP in static routes** to avoid recursive routing loops.
- Debugging from the **inside-out remains a reliable network troubleshooting method**.
- Simulator behavior may deviate from real hardware — expect edge cases.
- VPN tunnel issues often begin at **Phase 1 misalignments or IP reachability problems**.
- Granular command output (`debug ip packet`, `show crypto`) is invaluable for confirmation.

Activity Report: Guest Network Internet Access & VPN Tunnel Prep

Date: 07/31/2025

Next Steps:

- Confirm **public IP reachability** between home office's firewall and remote office's firewall.
- Review and align **ISAKMP policies** on both endpoints.
- Use `debug crypto isakmp` and `show access-lists` to trace Phase 1 behavior.
- Begin **Phase 2 config prep** once Phase 1 is successfully established

Activity Report: VPN Tunnel Validation & Report Cleanup

Date: 08/01/2025

Entry #: 73

Activity Name: Final Troubleshooting and Report Refinement

Tools/System Involved: Cisco Packet Tracer v8.2.2, Google Docs, Hemingway App, plagiarismdetector.net

Priority: High

Description: Today's work focused on validating the IPSec tunnel functionality. Also resolving final connectivity issues, and refining the associated documentation.

First, I identified and resolved physical connection problems in my Packet Tracer topology. A major issue was the guest router not linking to the network. I used a systematic inside-out troubleshooting approach to track down and fix these misconfigurations.

Next, I investigated a deeper issue with IP addressing on the Multilayer Switch (MLS). This required rethinking part of the network design. This pushed me into critical decision-making, aligning with the Advanced Beginner skill level.

To confirm the IPSec was working I used `tracert`. This shows that traffic was moving through the tunnel as intended. I then used `show crypto isakmp sa` and `show crypto ipsec sa` to confirm the security associations were active and the data's encrypted.

Finally, I revised my report. I removed overly detailed and redundant sections. This made the final version more concise and focused on the real troubleshooting path I followed.

Summary of Findings:

- Physical connectivity issues prevented initial tunnel success.
- Misconfigured IP addressing on L3 switch disrupted routing logic.
- VPN validated via tracert and show crypto output.
- Report restructured to emphasize real technical decisions.

Activity Report: VPN Tunnel Validation & Report Cleanup

Date: 08/01/2025

Key Takeaways:

- Logical design flaws can break functionality even when configs look correct.
- Visualizing packet flow (`tracert`) helps confirm end-to-end VPN function.
- Reporting should prioritize technical clarity over verbosity.

Next Steps:

- Submit finalized topology: `DIAGRAM - Adapted VPN Configuration Topology – v1.0.0`
- Archive project files using version-controlled names.
- Continiunig viewing CCNA documentation.

Activity Report: IPSec Tunnel Troubleshooting Report Progress

Date: 08/02/2025

Entry #: 74

Activity Name: IPSec Tunnel Troubleshooting Report Progress

Tools/System Involved: Cisco Packet Tracer v8.2.2, Google Docs, Hemingway App, plagiarismdetector.net

Priority: High

Description: Made major progress on the VPN Troubleshooting Guide and refined key sections of the report. This includes router configuration, license activation, and VPN command blocks using professional formatting. Drafted the full troubleshooting and lessons learned section. It breaks down real issues and resolutions. Verified working tunnel with Phase 1 and Phase 2 settings. I analyzed encryption/encapsulation via `show crypto` outputs. Clarified nuanced details such as tunnel mode verification and ACL symmetry across both routers.

The VPN troubleshooting guide saw big progress. Key parts of the report got refined. This included router setup details. License activation steps were clarified. VPN command blocks were improved. I wrote the troubleshooting section. It covers real problems and fixes. Lessons learned were also added. The VPN tunnel now works well. We checked its Phase 1 settings. Phase 2 settings were verified. Encryption and data flow were analyzed. This used 'show crypto' outputs. Key nuances were made clear. Tunnel mode was fully verified. Network rules matched on both routers.

Summary of Findings:

- `show crypto isakmp sa` → **QM_IDLE**
- `show crypto ipsec sa` → **Encaps/Decaps incrementing**

Key Takeaways:

- Built a working site-to-site IPSec VPN tunnel from scratch
- Structured and documented a complex technical report

Activity Report: IPSec Tunnel Troubleshooting Report Progress

Date: 08/02/2025

- Troubleshot real-world networking issues
- Verified best practices like ACL symmetry and tunnel integrity

Next Steps: Finalize and polish troubleshooting report, prep for PDF export.

Activity Report: Update & Format VPN Troubleshooting Report

Date: 08/03/2025

Entry #: 75

Activity Name: Update & Format VPN Troubleshooting Report

Tools/System Involved: Cisco Packet Tracer v8.2.2, Google Docs, Hemingway App, plagiarismdetector.net

Priority: High

Description: Today I finalized and polished my Enterprise IPsec VPN report. I converted technical notes and raw outputs into a professional, well-structured document. This aligns with MSAF standards. The focus was on formatting, troubleshooting documentation. Also, confirming that the VPN tunnel was operational with verifiable outputs.

Summary of Findings:

- Completed and reviewed all report sections from initial network build to tunnel verification.
- Used proper Markdown formatting and code blocks for configurations and terminal commands.
- Documented key troubleshooting steps, including fixing syntax errors and reapplying lost configs.
- Provided working `show crypto` command outputs showing tunnel status as QM_IDLE and verified encapsulation.
- Explained the difference between ACLs for NAT exemption and VPN traffic.
- Clarified the roles of the Multi-Layer Switch vs. routers in routing and gateway behavior.
- Marked the project as an independent portfolio build to reflect skill growth beyond structured labs.

Activity Report: Update & Format VPN Troubleshooting Report

Date: 08/03/2025

Key Takeaways:

- Turning raw CLI data into readable, reference-quality content builds reporting skills.
- Troubleshooting logs help show depth of understanding, not just successful results.
- Clean formatting improves communication and can serve as a reusable guide for future projects.
- This marks a key milestone in applying both technical and documentation skills at an advanced beginner level.

Next Steps:

- Submit report as part of independent project documentation.
- Share highlights in a professional LinkedIn post.
- Review more CCNA topics related to networking for further depth.

Activity Report: LinkedIn Profile & Portfolio Update

Date: 08/04/2025

Entry #: 76

Activity Name: LinkedIn Profile & Portfolio Update

Tools/System Involved: Linkedin, Google Docs, Hemingway App, plagiarismdetector.net

Priority: Low

Description: Today I focused on sharpening my professional brand. I updated both my portfolio and LinkedIn profile to better reflect my current skill set. I revised multiple hands-on cybersecurity projects. This includes Nmap scanning exercises, sslscan assessments, and OSINT investigations using platforms like Shodan.io, DNSDumpster, and Urlscan.io. I also refreshed a project centered on webpage change detection to demonstrate my interest in digital forensics.

On the strategic side, I rewrote my LinkedIn headline and summary to be clearer and more recruiter-friendly. I started tailoring my resume for Threat Intelligence roles. I especially highlighting transferable skills from my land investing background. I included risk analysis and incident response. I added a new "Cybersecurity Projects & Labs" section that features practical experience with tools such as YARA, OpenVAS, and Google Dorking.

Summary of Findings:

- Updated LinkedIn headline and summary with a sharper professional tone.
- Added refined descriptions of hands-on technical labs and OSINT projects.
- Revised resume experience sections to emphasize threat intel relevance.

Key Takeaways:

- Clear, targeted language is essential for standing out to recruiters.
- Showcasing hands-on labs directly improves the strength of my portfolio.
- My background in entrepreneurship supports my transition through skills like decision-making under risk, planning, and investigation.

Activity Report: LinkedIn Profile & Portfolio Update

Date: 08/04/2025

Next Steps:

- Finalize revised resume and upload to portfolio site.
- Continue updating technical lab writeups with clearer summaries and skills tags.
- Reach out to more industry connections and continue refining my professional story.

Activity Report: IPSec Tunnel Troubleshooting

Date: 08/05/2025

Entry #: 77

Activity Name: IPSec Tunnel Troubleshooting

Tools/System Involved: Cisco Packet Tracer v8.2.2, Google Docs, Hemingway App, plagiarismdetector.net

Priority: Moderate

Description:

Today, I focused on diagnosing and fixing network connectivity issues. This time between a head office PC and router across a VLAN-enabled multilayered switch and an IPSec VPN tunnel. I began by checking VLAN settings on the switch. I found and corrected a VLAN mismatch that was preventing local Layer 2 communication. After I fixed the VLAN setting on the PC's switch port, I confirmed successful local connectivity via ping.

Next, I looked at traceroute failures over the IPSec VPN tunnel between home office and a remote site. I checked the VPN tunnel status using Cisco commands (`show crypto isakmp sa`, `show crypto ipsec sa`) on both firewalls. Some intermediate hops timed out during traceroute. This is normal due to security filtering—the connection still reached its goal. This showed the IPSec tunnel was active and handling data traffic.

Summary of Findings:

- VLAN mismatch caused initial local connectivity failure; corrected by assigning PC port to correct VLAN.
- Local ping tests confirmed restored connectivity.
- Traceroute over IPSec VPN succeeded despite ICMP timeouts.
- `show crypto` command outputs showed active IPSec tunnel with encryption and decryption packet counts, verifying VPN operation.

Activity Report: IPSec Tunnel Troubleshooting

Date: 08/05/2025

Key Takeaways:

- Accurate VLAN port assignments are critical for Layer 2 communication.
- Intermediate traceroute timeouts can be normal in secure networks.
- Cisco crypto commands provide valuable insight into VPN tunnel health and traffic.
- Systematic troubleshooting from local LAN to VPN layer ensures end-to-end connectivity verification.

Next Steps:

- Document the troubleshooting process and findings for my portfolio.
- Continue practicing VPN configuration and advanced troubleshooting.
- Explore CCNA documentation to deeper my understanding of networking.

Activity Report: Report Finalization & Structure Update

Date: 08/06/2025

Entry #: 78

Activity Name: Report Refinement & Troubleshooting Log Update

Tools/System Involved: Cisco Packet Tracer v8.2.2, Google Docs, Hemingway App, plagiarismdetector.net

Priority: Low

Description: Today, I worked through several collaborative and technical updates to finalize my IPSec VPN documentation. I focused on polishing the troubleshooting section, refining structural clarity, and ensuring the document reflected all technical actions taken throughout the project.

Summary of Findings:

- Corrected and expanded the "VPN Deployment Challenges and Troubleshooting Log" with specific error conditions like the **ISAKMP lifetime mismatch** and the missing `mode tunnel` command.
- Reorganized the troubleshooting narrative into **two clear subsections**: "Flawed Troubleshooting Efforts" and "Root Cause Discovery and Final Resolution."
- Added **SECTION 0.0 Portfolio Overview** to frame the project in a professional, portfolio-ready format.
- Included **new configuration blocks** for interfaces, static routes, NAT rules, and crypto maps to demonstrate practical skills.
- Replaced a malfunctioning router in the topology to resolve incomplete traceroutes and confirm tunnel traffic flow.
- Finalized the **version history**, promoting the report from draft v1.0.9 to final release v1.1.0.
- Clarified internal vs. external versioning practices to align future drafts with portfolio documentation expectations.

Activity Report: Report Finalization & Structure Update

Date: 08/06/2025

Key Takeaways:

- Clean documentation and clear sectioning greatly improve readability, especially during technical reviews.
- Small misconfigurations like an omitted mode tunnel can cause tunnel failures that are hard to trace without structured diagnostics.
- Maintaining a detailed version history helps track progress and establish a clear publication timeline.

Next Steps:

- Begin the internal draft for **v2.0.0**, which will include extended lessons learned, packet captures (if feasible), and references to Cisco documentation.
- Prepare a visual summary of the troubleshooting timeline for future presentation or teaching purposes.

Activity Report: Website Finalization, Branding Polish & Blog

Date: 08/07/2025

Entry #: 79

Activity Name: Website Finalization, Branding Polish & Blog

Tools/System Involved: Wordpress, Google Docs, Hemingway App, Youtube, Linktree

Priority: Low

Description: Today was focused on strengthening my digital presence through a full pass on branding, layout structure. Createed content clarity across my website and supporting platforms. I finalized the homepage with a “Risk-Aware Technologist” lead-in. This is built for recruiter scanability and SEO value. I rewrittend My About page to reflect my mission-driven journey. I blended MCSI training, GRC curiosity, and entrepreneurial lessons under a unified tone.

I refactored the Experience page to split out certifications and labs with proper summaries. I included download options, and ethical disclaimers. Lab walkthroughs (IT setup, Linux, SQL) were also embedded from YouTube giving visual proof-of-work.

Beyond content, I upgraded navigation labels to better align with the voice of the brand. Menu items like "About Me" and "Contact" were revised to feel more intentional and purpose-driven.Also refined my Linktree bio to better reflect my evolving professional identity. Its offering a tight summary that introduces my labs, skills, and why it all matters.On the blog side, I collaborated on outlining and revising a new post about my journey through the MSAF Network Fundamentals course. This included structural edits, style adjustments, and voice consistency aligned with my brand.

Summary of Findings:

- Homepage rewritten with focused, recruiter-friendly messaging
- About page deployed with clear narrative arc and personal touches
- Experience page restructured to separate labs and certs, with embedded content

Activity Report: Website Finalization, Branding Polish & Blog

Date: 08/07/2025

- Navigation improved for clarity and UX flow
- Blog draft refined with feedback loop and tone alignment
- Linktree updated to reflect current brand and portfolio goals

Key Takeaways:

- Consistency between platform tone and layout boosts credibility and impact
- Telling a mission-driven story is more powerful than listing achievements
- Real-world lab content benefits from structured presentation and ethical framing
- Voice, layout, and SEO must work together to support visibility

Next Steps:

- Final proofread of all site pages
- Embed missing YouTube walkthroughs and add download links to select labs
- Publish the MSAF blog post after final style review
- Begin outlining next blog entry: Threat Detection in Layer 3 Environments

Activity Report: Blog & Online Presence Refinement

Date: 08/08/2025

Entry #: 80

Activity Name: Blog & Online Presence Refinement

Tools/System Involved: Google Docs, WordPress, Hemingway App, Google AI Studio Image Generation Tool, Linktree

Priority: Moderate

Description: Focused on finalizing my cybersecurity blog content and improving my professional online brand. I posted the final draft of a blog post along with an associated image. I enhanced the post's critical sections such as "Insights & Learnings" and "Mapping to Industry Frameworks." Consulted with AI on the best approach for a featured blog image; decided to create a fresh, dynamic image for better engagement while retaining the original graphic within the post.

Requested and received a professionally generated featured image tailored to the blog topic. Additionally, provided a Linktree template which was upgraded into a streamlined, attention-grabbing link funnel with mini headlines and one-liners to better guide visitors toward my portfolio, free resources, and contact info.

Summary of Findings: N/A

Key Takeaways:

- Fresh, eye-catching visuals improve blog post visibility and social shares.
- Curated Linktree structure strengthens professional branding and user navigation.
- Collaborating on content refinement helps clarify messaging and align with industry standards.

Next Steps:

- Implement the enhanced Linktree on professional profiles and social media.

Activity Report: Blog & Online Presence Refinement

Date: 08/08/2025

- Resume Windows security hardening research as planned for next session.

Activity Report: CompTIA Network+ Training – Networking Fundamentals & Physical Networks

Date: 08/09/2025

Entry #: 81

Activity Name: CompTIA Network+ Training – Networking Fundamentals & Physical Networks

Tools/System Involved: Coursea Online Platform, CompTIA Network+ (N10-008) – Packt Total Course

Priority: Moderate

Description: Today I dedicated time to structured study for the CompTIA Network+ Certification (N10-008): The Total Course, focusing on the Networking Fundamentals and Physical Networks section (Course 1 of 3). Covered foundational topics from the OSI Model through Ethernet basics. Reinforced understanding of network models, addressing, MAC addressing, frame structures, and physical cabling standards. Completed multiple graded assessments with high scores, demonstrating strong retention.

Summary of Findings:

- OSI Model and TCP/IP stack roles and layers clarified.
- Frame structure and MAC addressing thoroughly reviewed.
- Learned differences between broadcast and unicast traffic.
- Covered coaxial, twisted-pair, and fiber optic cabling types with use cases.
- Understood fire ratings and their role in cabling safety.
- Differentiated hubs vs switches, and proper methods for connecting switches.

Key Takeaways:

- The OSI Model is a universal reference for troubleshooting and designing networks.

Activity Report: CompTIA Network+ Training – Networking Fundamentals & Physical Networks

Date: 08/09/2025

- Physical cabling choice impacts performance, safety, and scalability.
- Ethernet fundamentals are the backbone of most LAN environments.
- Strong foundational knowledge will directly support future configuration and troubleshooting labs.

Next Steps:

- Start University of Colorado's Computer Security and Systems Management

Activity Report: Computer Security & Systems Management – Virtualization & Security

Date: 08/10/2025

Entry #: 82

Activity Name: Computer Security & Systems Management – Virtualization & Security

Tools/System Involved: Coursea Online Platform, University of Colorado – Enterprise System Management and Security (Course 1 of 4)

Priority: High

Description: Shifted focus from CompTIA Network+ study to the Computer Security and Systems Management course from the University of Colorado. Worked through core topics including Virtualization, Networking, and Information Security within enterprise contexts. Completed graded assignments on virtualization, networking fundamentals, and information security with high scores. Engaged in peer review for a BYOD (Bring Your Own Device) case study and gathered insights for a detailed BYOD security report.

Summary of Findings:

- Compared personal vs. enterprise computing environments and their security requirements.
- Mastered virtualization concepts, types, use cases, and limitations.
- Reinforced OSI model understanding in the context of system management.
- Reviewed security frameworks (FIPS 199) and CIA triad principles.
- Identified risks and policy considerations for BYOD adoption in organizations.

Key Takeaways:

- Virtualization is central to scalability, resource optimization, and disaster recovery in enterprise IT.
- Networking knowledge underpins all aspects of systems management.

Activity Report: Computer Security & Systems Management – Virtualization & Security

Date: 08/10/2025

- BYOD policies must balance flexibility with security enforcement to protect organizational assets.
- Risk assessment frameworks provide a structured approach to maintaining confidentiality, integrity, and availability.

Next Steps:

- Submit graded BYOD in Organizations assignment.
- Draft a detailed BYOD security report based on peer feedback and course materials.
- Progress toward completing Course 1 (91% done) to unlock Course 2 in the specialization.

Activity Report: BYOD Report Refinement and Contract Template Finalization

Date: 08/11/2025

Entry #: 83

Activity Name: BYOD Report Refinement and Contract Template Finalization

Tools/System Involved: Google Docs, Linktree, Research Articles, Writing Tools

Priority: Moderate

Description: Focused on refining the BYOD report for a professional yet accessible tone, targeting a 9th-grade reading level. Updated sections covering security challenges, organizational countermeasures, and future trends. Created a detailed BYOD contract template incorporating legal protections, technical requirements, and employee responsibilities. Finalized promotional copy for Linktree integration aimed at engaging small IT teams and SMB audiences.

Summary of Findings:

- Simplified complex sections without sacrificing technical detail.
- Incorporated recent cybersecurity incidents to improve report credibility.
- Produced a structured BYOD contract template addressing both compliance and operational needs.
- Crafted concise, targeted messaging for Linktree to drive engagement.

Key Takeaways:

- Simplicity in language ensures broader accessibility while maintaining authority.
- Timely, real-world examples increase the impact of technical reports.
- A well-balanced BYOD contract protects both the organization and its workforce.
- Strong promotional copy is essential for driving reader interest in technical resources.

Activity Report: BYOD Report Refinement and Contract Template Finalization

Date: 08/11/2025

Next Steps:

- Publish the BYOD report and contract template via Linktree and blog channels.
- Track engagement metrics and gather feedback for content refinement.
- Expand template library to support ongoing cybersecurity education efforts.

Activity Report: Content Distribution & Audience Engagement

Date: 08/12/2025

Entry #: 84

Activity Name: Content Distribution & Audience Engagement

Tools/System Involved: Linktree, Google Docs, Social Media Platforms, SEO Tools, Coursea Online Platform Online Platform

Priority: High

Description:

Focused on promoting the finalized BYOD report and contract template via Linktree. Optimized the page structure and messaging to boost clarity and engagement. Crafted targeted, concise copy aimed at small IT teams and SMB audiences to drive downloads and interaction. Addressed mobile display challenges with added user guidance. Explored alternate hosting platforms to diversify content accessibility.

Additionally, celebrated completion of the **University of Colorado's** *Computer Security and Systems Management* course with a **grade of 95.50%**, marking progress in formal cybersecurity education.

Summary of Findings:

- Streamlined Linktree links for better resource discoverability.
- Mitigated mobile viewing issues with clear instructions.
- Enhanced calls-to-action to boost template downloads.
- Explored alternative hosting for improved accessibility.
- Successfully completed a key cybersecurity course, reinforcing theoretical and practical knowledge.

Key Takeaways:

- Clear navigation and messaging improve user experience and engagement.
- Mobile-friendly content access is critical.
- Consistent branding and concise messaging build trust.
- Diversifying content platforms increases reach and redundancy.

Activity Report: Content Distribution & Audience Engagement

Date: 08/12/2025

- Formal coursework completion advances foundational cybersecurity skills.

Next Steps:

- Monitor engagement metrics to evaluate impact.
- Develop blog post on BYOD.
- Continue progressing through cybersecurity coursework and certifications.

SECTION 4.0 REPORT TEMPLATE

Incident Report
Date: 00/00/2025
Entry #:
Likelihood: Low
Severity: Low
Status: New: Incident has just been reported and is awaiting review.
Description:
Tools/System Involved:
The 5 W's:

Log Analysis Report

Date: 00/00/2025

Entry #: 0
Tools/System Involved:
Likelihood: Low
Severity: Low
Status: New: Incident has just been reported and is awaiting review.
Description:
Conclusion:
Follow-Up Actions:

Activity Report

Date: 00/00/2025

Entry #: 0
Activity Name:
Tools/System Involved:
Priority: Low
Description:
Summary of Findings:
Key Takeaways:
Next Steps: