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 The target system was found to be running outdated and vulnerable services, which allowed remote code execution (RCE) through two distinct attack vectors: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 Outdated Samba Service – Vulnerable to a known buffer overflow (trans2open).

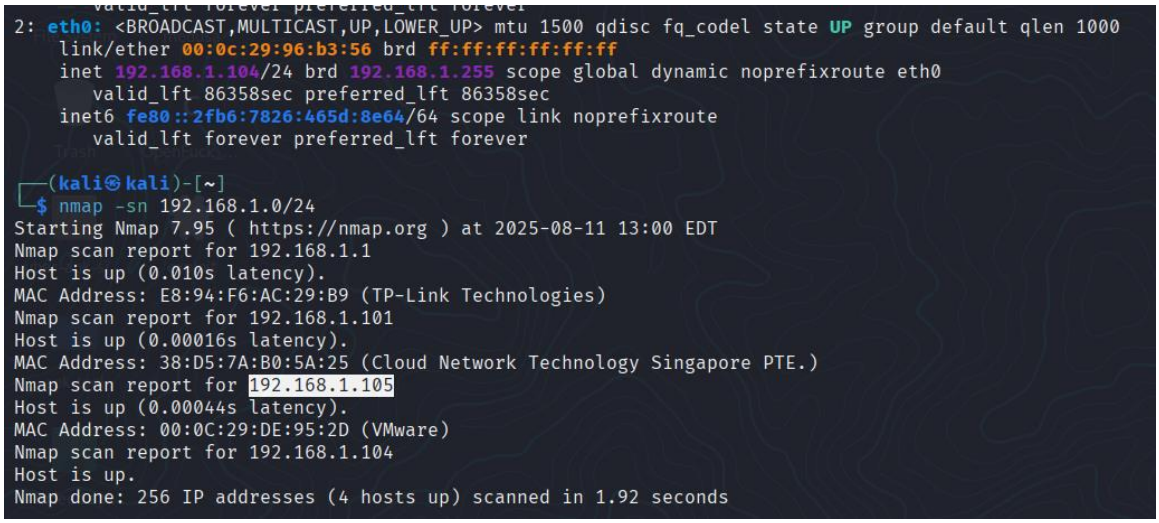
Both vulnerabilities were successfully exploited, granting full root-level compromise. Persistence mechanisms were also established to ensure continued access.

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.



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Identified outdated HTTP daemon vulnerable to RCE.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

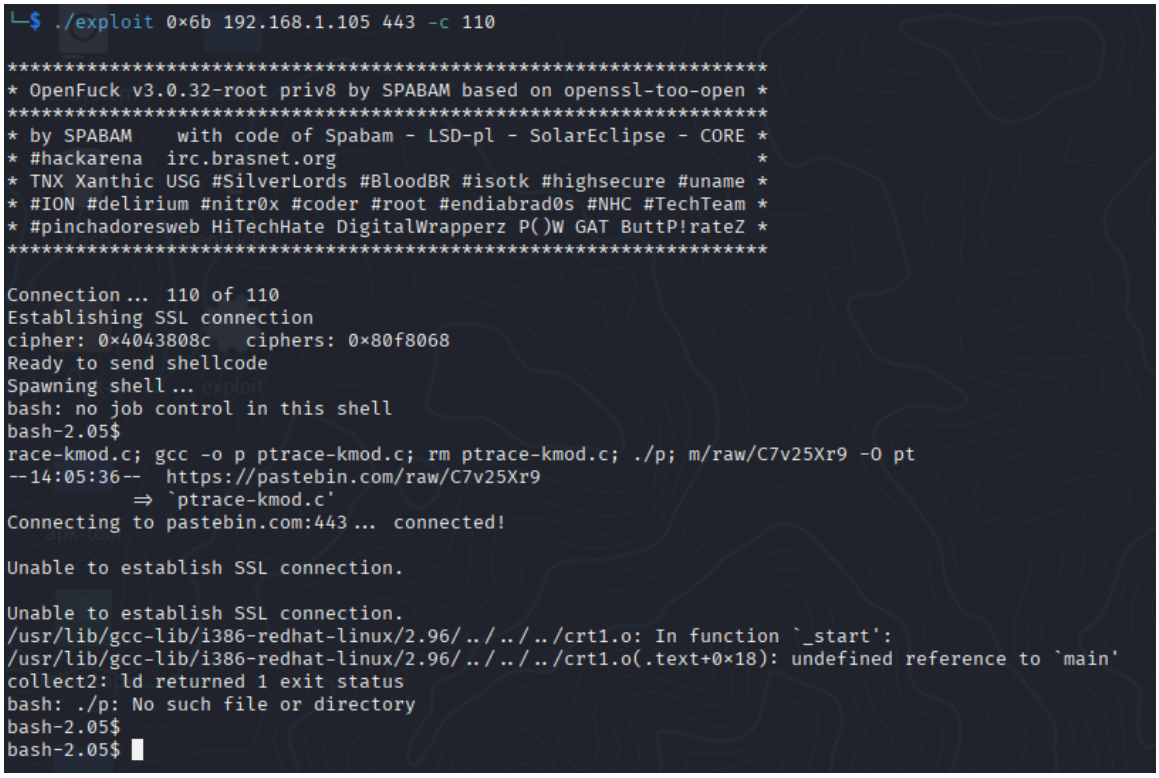
Searched for relevant exploits using searchsploit.
Original exploit script failed due to compatibility issues.
Located a modified version on GitHub named OpenLuck.
Compiled and prepared exploit.

```
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.



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

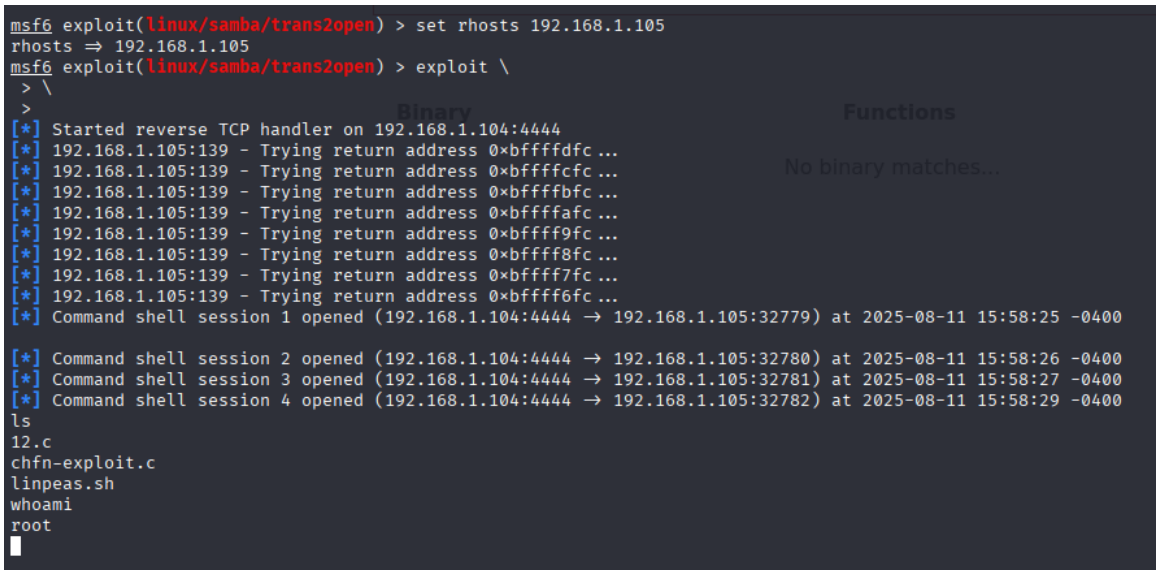
```
   #  Name                                                  Disclosure Date  Rank     Check  Description
   -  ----                                                  ---------------  ----     -----  -----------
   0  exploit/multi/samba/nttrans                           2003-04-07       average  No     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 SPAR
   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) >
```

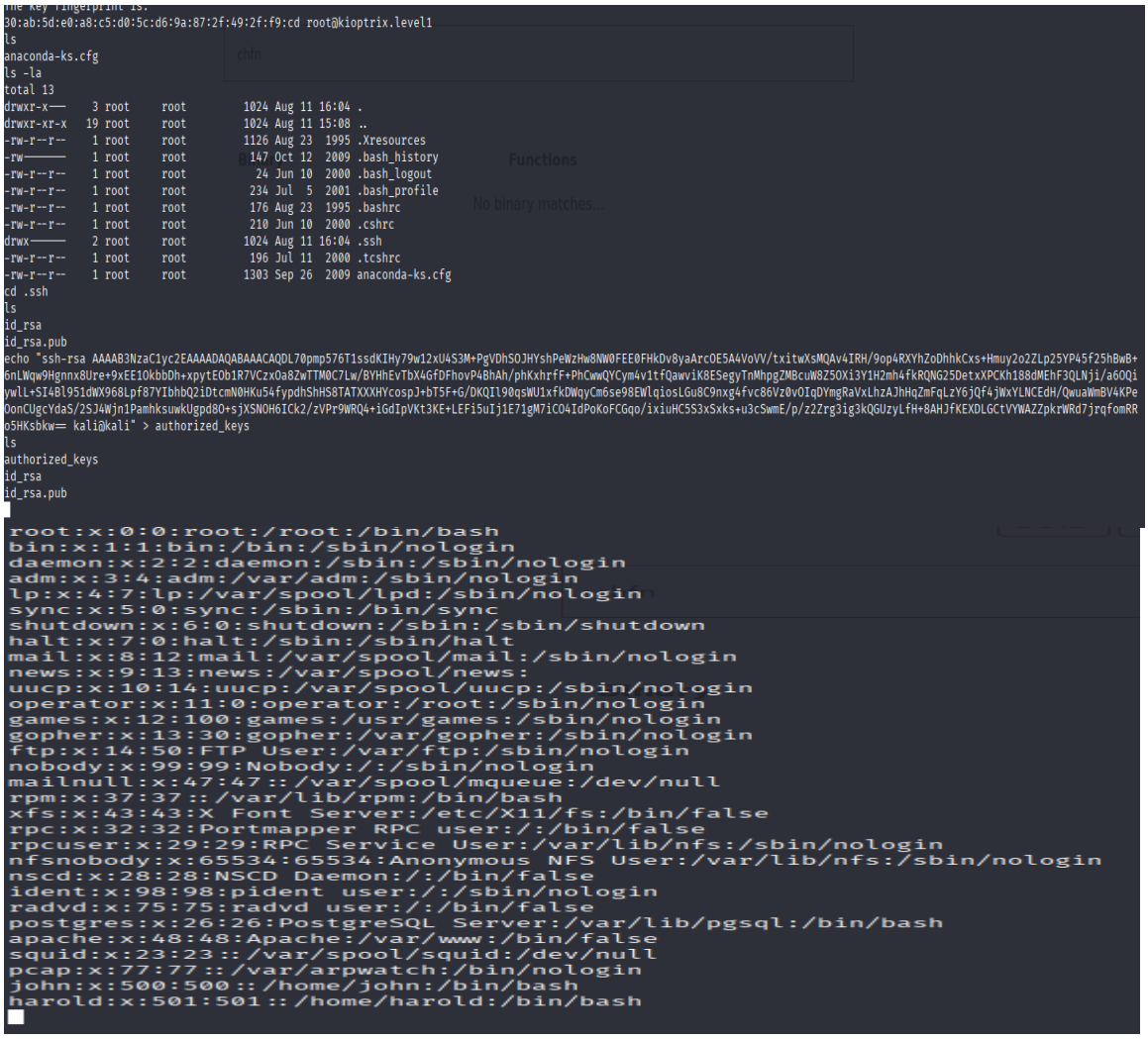
Exploitation

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



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.



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

1. Patch & Upgrade all services, including:
- Update HTTP daemon to the latest stable version.
- Upgrade Samba to a secure, supported release.
2. 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.