Interrogation Writeup

Description

In the latest case of Sherlock, a breach at the London Tower was executed with just a few lines of code. The perpetrator, the famous criminal consultant Moriarty, has been arrested. However, despite hours of interrogation, Moriarty has remained tight-lipped about both the software he used and the group he represents. As a result, our IT experts have turned their attention to his laptop. But Sherlock has warned us that Moriarty may have an anti-forensics laptop that adds an additional layer of complexity. By taking a look at his machine, Can you figure out the tool he used, the group he's affiliated with and the server used for coordination?
Flag format: shellmates{ToolName_GroupName_ServerName}
Username: ctf
Password: ctf

Solution

we were given this command to connect to ssh :

```
ssh ctf@interrogation.hackini24.shellmates.club -o ProxyCommand="openssl
s_client -quiet -connect interrogation.hackini24.shellmates.club:443 -
servername interrogation.hackini24.shellmates.club"
```

let's connect :

```
└─$ ssh ctf@interrogation.hackini24.shellmates.club -o ProxyCommand="openssl
s_client -quiet -connect interrogation.hackini24.shellmates.club:443 -
servername interrogation.hackini24.shellmates.club"
depth=2 C = US, O = Internet Security Research Group, CN = ISRG Root X1
verify return:1
depth=1 C = US, O = Let's Encrypt, CN = R3
verify return:1
depth=0 CN = *.hackini24.shellmates.club
verify return:1
ctf@interrogation.hackini24.shellmates.club's password:
Welcome to Ubuntu 22.04.3 LTS (GNU/Linux 5.15.120+ x86_64)

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

```
 * Support:        https://ubuntu.com/advantage

This system has been minimized by removing packages and content that are
not required on a system that users do not log into.

To restore this content, you can run the 'unminimize' command.
Last login: Sun Dec 17 18:32:20 2023 from 10.84.0.1
-bash: /usr/bin/groups: Permission denied
-bash: /usr/bin/locale-check: Permission denied
ctf@interrogation-9bd74c6b7-vdrcm:~$
```

so the flag name is in this form :

```
shellmates{ToolName_GroupName_ServerName}
```

we notice that we cannot run the majority of commands, we got a restricted shell.

the first part of the shell is a `ToolName`, we can check famous places where tools and binaries are placed, let's check the `PATH` env variable :

```
ctf@interrogation-9bd74c6b7-vdrcm:~$ echo $PATH
/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/usr/games:/usr
/local/games:/snap/bin
```

let's list those directories one by one, may be the tool will stand out.

but the `ls` command is restricted, we can list with `echo`, using `echo /DIR_PATH/*`, we can list the dir content, so we try those dirs in PATH one by one, and we notice an unusual tool in `/usr/bin/` :

```
ctf@interrogation-9bd74c6b7-vdrcm:~$ echo /usr/bin/*
/usr/bin/Cr1m3m4st3rm1ndK1t
...
```

that's gotta be the tool name.

the second part of the flag is the group name.

let's run `sudo -l` :

```
ctf@interrogation-9bd74c6b7-vdrcm:~$ sudo -l
[sudo] password for ctf:
Matching Defaults entries for ctf on interrogation-9bd74c6b7-vdrcm:
    env_reset, mail_badpass,
secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bi
n\:/snap/bin

User ctf may run the following commands on interrogation-9bd74c6b7-vdrcm:
    (Moriarty) /usr/bin/osqueryi
```

we can run `/usr/bin/osqueryi` as the user `Moriarty`, let's do that :

```
ctf@interrogation-9bd74c6b7-vdrcm:~$ sudo -u Moriarty /usr/bin/osqueryi
Thrift: Sun Dec 17 18:47:37 2023 TSocket::open() connect() <Path:
/home/Moriarty/.osquery/shell.em>: Connection refused
Using a virtual database. Need help, type '.help'
osquery>
```

the commands of osquery are similar to sqlite3, we can check the available tables with `.tables` :

```
osquery> .tables
  => acpi_tables
  => apparmor_events
  => apparmor_profiles
  => apt_sources
  => arp_cache
  => atom_packages
...
  => yara
  => yara_events
  => ycloud_instance_metadata
  => yum_sources
```

there is a table called `groups`, let's get the content of that table :

```
osquery> .all groups
+-------+-----------+-----------------+
| gid   | gid_signed | groupname        |
```

```
+-------+-----------+-----------------+
| 0     | 0         | root            |
| 1     | 1         | daemon          |
| 2     | 2         | bin             |
| 3     | 3         | sys             |
| 4     | 4         | adm             |
| 5     | 5         | tty             |
| 6     | 6         | disk            |
| 7     | 7         | lp              |
| 8     | 8         | mail            |
| 9     | 9         | news            |
| 10    | 10        | uucp            |
| 12    | 12        | man             |
| 13    | 13        | proxy           |
| 15    | 15        | kmem            |
| 20    | 20        | dialout         |
| 21    | 21        | fax             |
| 22    | 22        | voice           |
| 24    | 24        | cdrom           |
| 25    | 25        | floppy          |
| 26    | 26        | tape            |
| 27    | 27        | sudo            |
| 29    | 29        | audio           |
| 30    | 30        | dip             |
| 33    | 33        | www-data        |
| 34    | 34        | backup          |
| 37    | 37        | operator        |
| 38    | 38        | list            |
| 39    | 39        | irc             |
| 40    | 40        | src             |
| 41    | 41        | gnats           |
| 42    | 42        | shadow          |
| 43    | 43        | utmp            |
| 44    | 44        | video           |
| 45    | 45        | sasl            |
| 46    | 46        | plugdev         |
| 50    | 50        | staff           |
| 60    | 60        | games           |
| 100   | 100       | users           |
| 65534 | 65534     | nogroup         |
```

```
| 101   | 101        | systemd-journal  |
| 102   | 102        | systemd-network  |
| 103   | 103        | systemd-resolve  |
| 104   | 104        | crontab          |
| 105   | 105        | messagebus       |
| 106   | 106        | systemd-timesync |
| 107   | 107        | _ssh             |
| 999   | 999        | Moriarty         |
| 1010  | 1010       | APT221           |
| 998   | 998        | ctf              |
+-------+------------+------------------+
```

`APT221` looks interesting, that's gotta be the group name.

the last part of the flag is the server name, if we check the `crontab` table, we get this :

```
osquery> .all crontab
+-------+--------+------+--------------+-------+-------------+--------------
--------------------------------------------------------------------------
--------------+-------------------------+
| event | minute | hour | day_of_month | month | day_of_week | command
| path                     |
+-------+--------+------+--------------+-------+-------------+--------------
--------------------------------------------------------------------------
--------------+-------------------------+
|       | 17     | *    | *            | *     | *           | root cd / &&
run-parts --report /etc/cron.hourly
| /etc/crontab             |
|       | 25     | 6    | *            | *     | *           | root test -x
/usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.daily )
| /etc/crontab             |
|       | 47     | 6    | *            | *     | 7           | root test -x
/usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.weekly )
| /etc/crontab             |
|       | 52     | 6    | 1            | *     | *           | root test -x
/usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.monthly )
| /etc/crontab             |
|       | 0      | 0    | *            | *     | *           | ssh -R
*:1337:localhost:1337 Moriarty@Th3Sh3rl0ck3d
| /etc/crontab             |
```

```
|       | 30     | 3    | *            | *     | 0           | root test -e
/run/systemd/system || SERVICE_MODE=1 /usr/lib/x86_64-linux-
gnu/e2fsprogs/e2scrub_all_cron | /etc/cron.d/e2scrub_all |
|       | 10     | 3    | *            | *     | *           | root test -e
/run/systemd/system || SERVICE_MODE=1 /sbin/e2scrub_all -A -r
| /etc/cron.d/e2scrub_all |
+-------+--------+------+--------------+-------+-------------+--------------
-------------------------------------------------------------------------
--------------+-------------------------+
```

we notice this : `Moriarty@Th3Sh3rl0ck3d`, we found the server name `Th3Sh3rl0ck3d`.

combining all those, we can get the flag.

- flag: `shellmates{Cr1m3m4st3rm1ndK1t_APT221_Th3Sh3rl0ck3d}`