SYLVARCON 2049
a cybersecurity adventure

Mission Name

The Backdoor

Historical Context

Ethan has identified unauthorized access on his computer, experiencing the irony of a hacker being hacked. His current objective is to locate the intruder and sever their connection.

Overview of Technical Strategy

Upon discovering unauthorized access to his computer, Ethan's priority is to uncover the concealed backdoor and eliminate it from his system.

Brief Mission Overview

Your computer has been compromised with a backdoor, putting you under surveillance. Your mission is to locate and eradicate this security threat. Best of luck!

Detailed Mission Brief

Ethan finds himself in a precarious situation with unauthorized access discovered on his computer—a hacker facing the brunt of hacking. He is now on a quest to identify the intruder and disrupt their communications.

Operational Venue

ANTUM | HAB BLOCK DISTRICT | ETHAN'S APARTMENT

Tools

- User: ethan
- Password: Myp4ssw0rd

Questions

What is the name of the artifact used as backdoor?

- Rootkit

What is the name of the artifact?

- Reptile

What is the port number of the backdoor configuration?

- 666

Hints

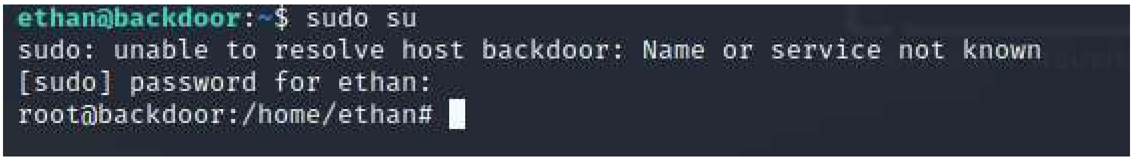
1. Sneaky, sneaky
2. Linux LKM
3. Mortal Kombat hidden character

Categories

- Enumeration
- Backdoor
- Rootkit

Write Up

Search for the rootkit. Once logged into the machine, it takes merely a minute to notice that the user Ethan has root privileges



```
ethan@backdoor:~$ sudo su
sudo: unable to resolve host backdoor: Name or service not known
[sudo] password for ethan:
root@backdoor:/home/ethan# 
```

Figure 1

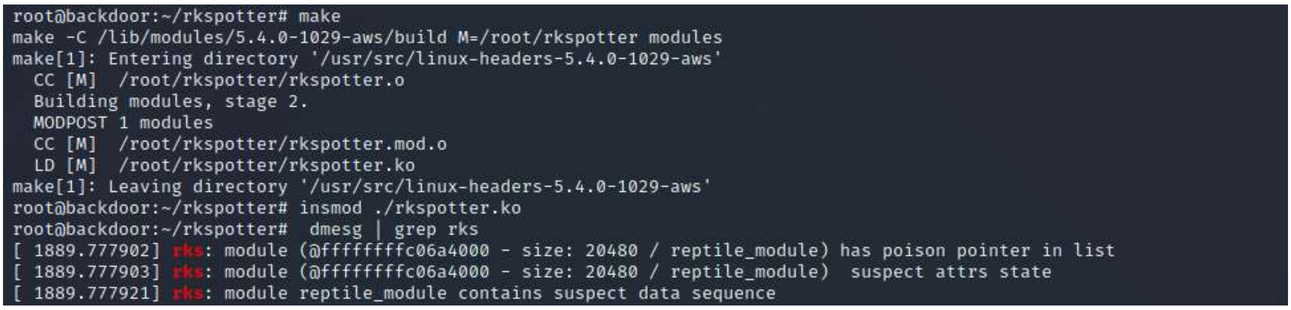
Regrettably, this doesn't significantly aid in locating the flag.

It's essential for the user to deduce that the only elements hidden from a root user could be a modified binary (identifiable, perhaps, by sorting files by modification date) or a rootkit, specifically an LKM in this scenario.

Standard rootkit detection tools like Rootkit Hunter or Chkrootkit might not yield results in this case.

However, the following tool proves useful: https://github.com/linuxthor/rkspotter

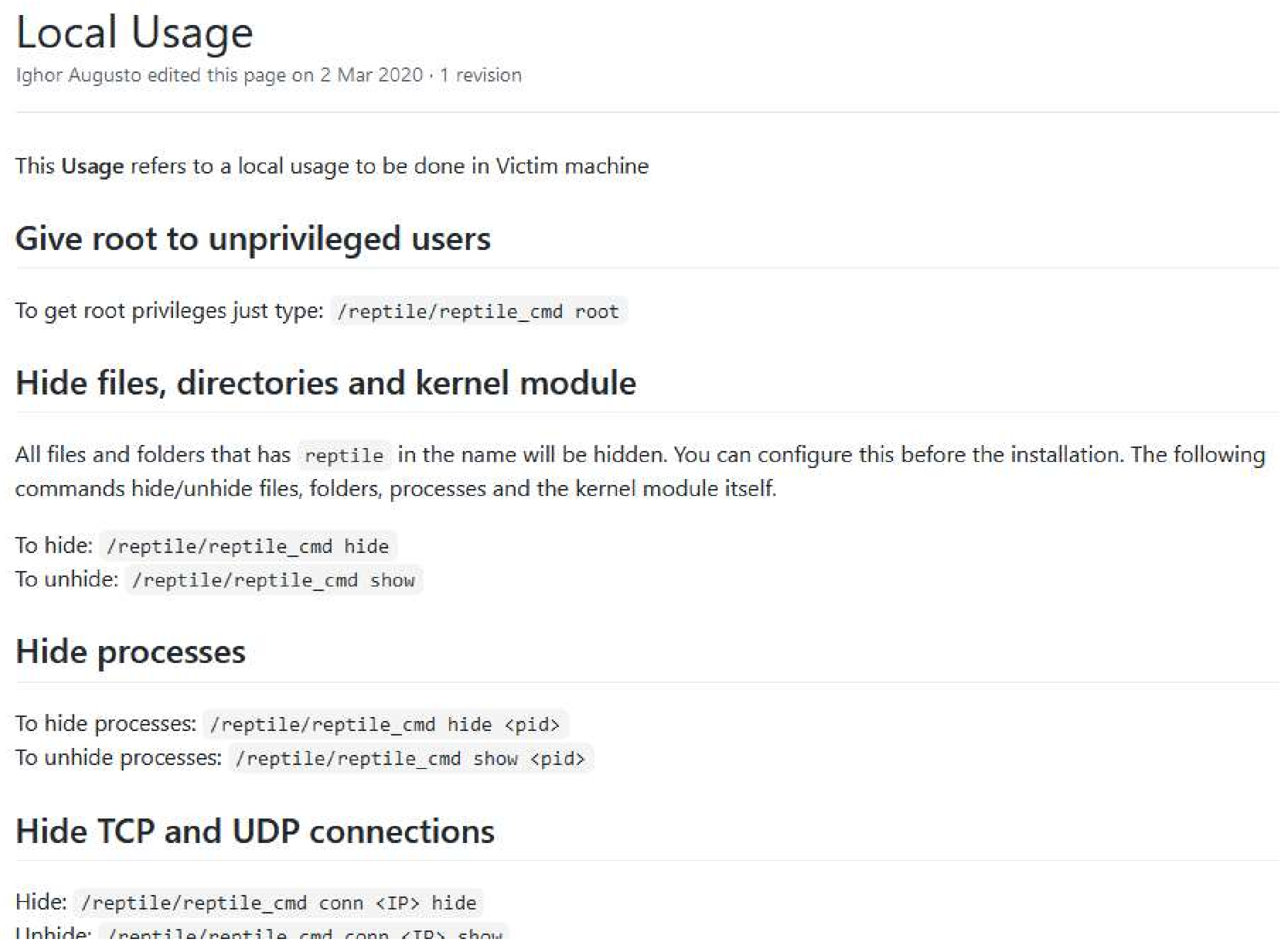
Download it to the machine, compile, and run it to examine the findings.



```
root@backdoor:~/rkspotter# make
make -C /lib/modules/5.4.0-1029-aws/build M=/root/rkspotter modules
make[1]: Entering directory '/usr/src/linux-headers-5.4.0-1029-aws'
  CC [M]  /root/rkspotter/rkspotter.o
  Building modules, stage 2.
  MODPOST 1 modules
  CC [M]  /root/rkspotter/rkspotter.mod.o
  LD [M]  /root/rkspotter/rkspotter.ko
make[1]: Leaving directory '/usr/src/linux-headers-5.4.0-1029-aws'
root@backdoor:~/rkspotter# insmod ./rkspotter.ko
root@backdoor:~/rkspotter#  dmesg | grep rks
[ 1889.777902] rks: module (@ffffffffc06a4000 - size: 20480 / reptile_module) has poison pointer in list
[ 1889.777903] rks: module (@ffffffffc06a4000 - size: 20480 / reptile_module)  suspect attrs state
[ 1889.777921] rks: module reptile_module contains suspect data sequence
```

Figure 2

Success! It identifies the Reptile LKM rootkit. Proceed to its repository and consult the wiki section for local usage instructions: https://github.com/f0rb1dd3n/Reptile/wiki/Local-Usage



Local Usage

Ighor Augusto edited this page on 2 Mar 2020 · 1 revision

This **Usage** refers to a local usage to be done in Victim machine

Give root to unprivileged users

To get root privileges just type: `/reptile/reptile_cmd root`

Hide files, directories and kernel module

All files and folders that has `reptile` in the name will be hidden. You can configure this before the installation. The following commands hide/unhide files, folders, processes and the kernel module itself.

To hide: `/reptile/reptile_cmd hide`
To unhide: `/reptile/reptile_cmd show`

Hide processes

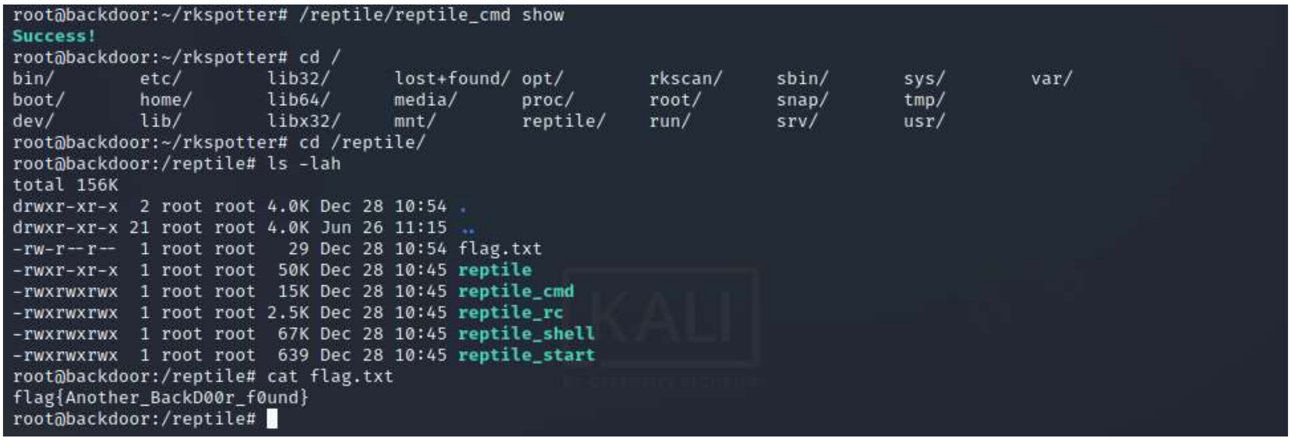
To hide processes: `/reptile/reptile_cmd hide <pid>`
To unhide processes: `/reptile/reptile_cmd show <pid>`

Hide TCP and UDP connections

Hide: `/reptile/reptile_cmd conn <IP> hide`
Unhide: `/reptile/reptile_cmd conn <IP> show`

Figure 3

After executing the command `/reptile/reptile_cmd show`, a new directory named "reptile" is discovered, containing the flag inside.



```
root@backdoor:~/rkspotter# /reptile/reptile_cmd show
Success!
root@backdoor:~/rkspotter# cd /
bin/        etc/        lib32/      lost+found/ opt/        rkscan/     sbin/       sys/        var/
boot/       home/       lib64/      media/      proc/       root/       snap/       tmp/
dev/        lib/        libx32/     mnt/        reptile/    run/        srv/        usr/
root@backdoor:~/rkspotter# cd /reptile/
root@backdoor:/reptile# ls -lah
total 156K
drwxr-xr-x  2 root root 4.0K Dec 28 10:54 .
drwxr-xr-x 21 root root 4.0K Jun 26 11:15 ..
-rw-r--r--  1 root root   29 Dec 28 10:54 flag.txt
-rwxr-xr-x  1 root root  50K Dec 28 10:45 reptile
-rwxrwxrwx  1 root root  15K Dec 28 10:45 reptile_cmd
-rwxrwxrwx  1 root root 2.5K Dec 28 10:45 reptile_rc
-rwxrwxrwx  1 root root  67K Dec 28 10:45 reptile_shell
-rwxrwxrwx  1 root root  639 Dec 28 10:45 reptile_start
root@backdoor:/reptile# cat flag.txt
flag{Another_BackD00r_f0und}
root@backdoor:/reptile# 
```

Figure 4

Flag Information

flag{Another_BackD00r_f0und}