SunsetNoontide Writeup – Proving Grounds

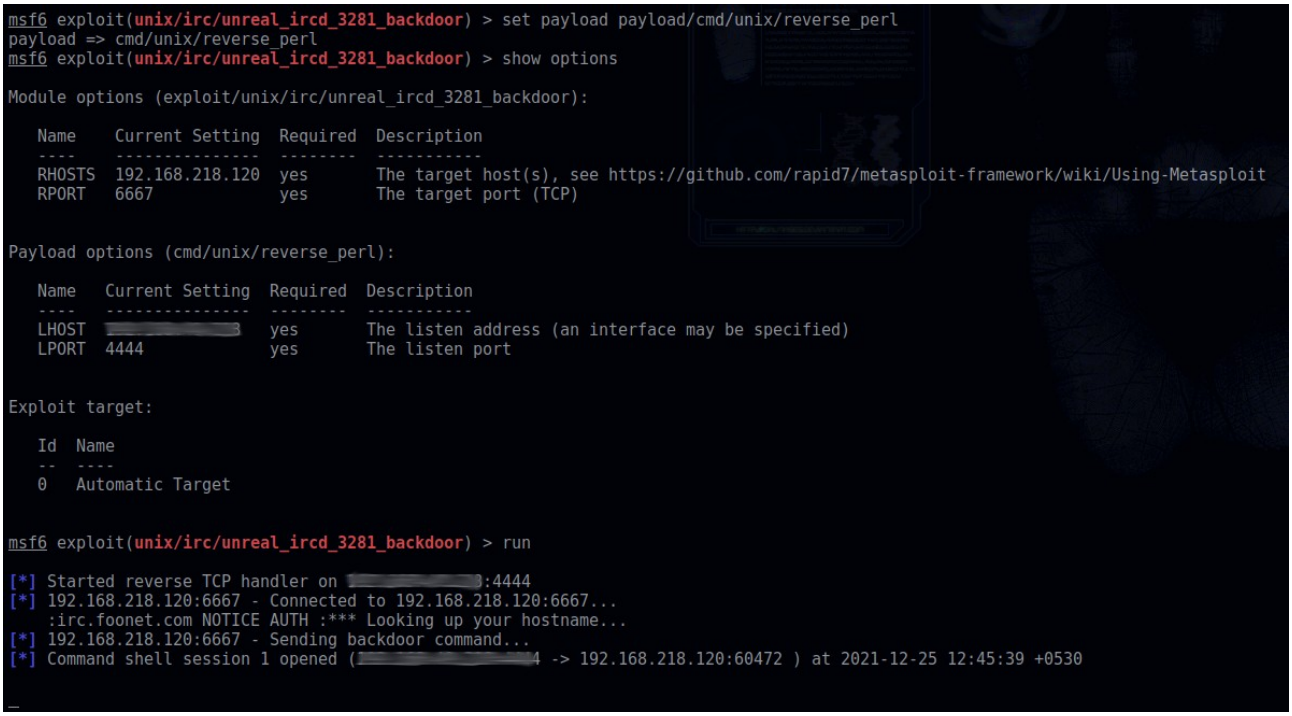
Scanning :-

```
~
➜ sudo nmap sunsetnoon.tide -v -p- -T 5 --script=vuln
[sudo] password for maskman:
Starting Nmap 7.92 ( https://nmap.org ) at 2021-12-25 12:17 IST
Nmap wishes you a merry Christmas! Specify -sX for Xmas Scan
(https://nmap.org/book/man-port-scanning-techniques.html).

Scanning sunsetnoon.tide (192.168.218.120) [65535 ports]
Discovered open port 6667/tcp on 192.168.218.120
Discovered open port 8067/tcp on 192.168.218.120
Discovered open port 6697/tcp on 192.168.218.120

PORT     STATE SERVICE
6667/tcp open  irc
|_irc-unrealircd-backdoor: Server closed connection, possibly due to too
many reconnects. Try again with argument irc-unrealircd-backdoor.wait
set to 100 (or higher if you get this message again).
| irc-botnet-channels:
|_  ERROR: Closing Link: [192.168.49.218] (Too many unknown connections
from your IP)

6697/tcp open  ircs-u
|_ssl-ccs-injection: No reply from server (TIMEOUT)
| irc-botnet-channels:
|_  ERROR: Closing Link: [192.168.49.218] (Too many unknown connections
from your IP)

8067/tcp open  infi-async
|_irc-unrealircd-backdoor: Looks like trojaned version of unrealircd.
See http://seclists.org/fulldisclosure/2010/Jun/277
| irc-botnet-channels:
```

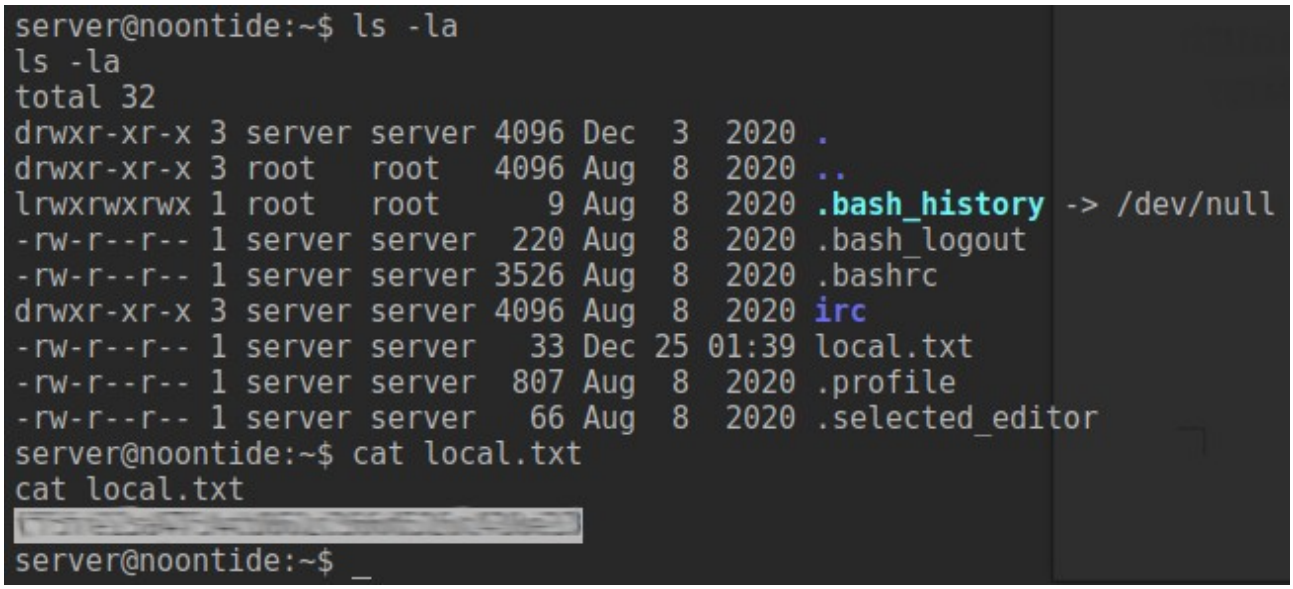
Foothold :-

I searched in searchsploit and found few exploits for UnrealIRCd. To make things easier I used metasploit to gain foothold.

unix/irc/unreal_ircd_3281_backdoor is the exploit in Metasploit Framework.



Here’s the user flag :



Privilege Escalation :-

Privilege escalation is a piece of cake in this machine. Root account’s password is root itself. That was totally unexpected.
Here’s the Root flag :