Port Forwarding for Security Test

Port forwarding is a pivoting technique that is used to relay packets through a man in the middle from an attacker to a target. There are port forwarding techniques that can be used in both Microsoft and Linux/Unix environments.

Figure 1 – The Network

So, in this example, both the Attacker and Bob are running the Linux operating systems, and we have compromised Alice. Our goal is to use Alice as a pivot point to allow for the Attacker to attack the Webb server running on TCP/8888 on Bob via port forwarding on Alice.

Microsoft Windows

If Alice is running the Microsoft Windows Operating System, and we have a command shell on Alice, then using **fpipe.exe** we can forward **TCP/80** on **Alice** to **TCP//8888** on **Bob** using the following commands:

```
C:\> fpipe.exe -i 192.168.2.99 -l 8080 -r 80 172.16.2.201
```

Unix/Linux

If **Alice** is running the Unix/Linux Operating System, and we have a command shell on **Alice**, then using **netcat(nc)** we can forward **TCP/8080** on Alice to **TCP//80** on **Bob** using the following commands. The first thing that we need to do is to create a pipe. We do this as follows:

```
$ mknod pivot p
```

How we can use the following commands on **Alice** to function as port forwarder. In the following we are listening on **TCP/8080** on **Alice** and forwarding a TCP connection from the **Attacker** to **TCP/80** on **Bob**.

```
$ nc -l -p 8080 0<pivot | nc 172.16.2.201 80 1>pivot
```

Metasploit

If we have a meterpreter shell on **Alice**, we can forward **TCP/8080** on **Alice** to **TCP/80** on **Bob** using the following commands. This uses the **portfwd** component of Metasploit to create, list and delete port forwarding within the **meterpreter** payload.

```
meterpreter > portfwd add -l 8080 -p 80 -r 172.16.2.201
[*] Local TCP relay created: 0.0.0.0:8080 >-> 172.16.194.191:80
meterpreter >
```

Using **meterpreter** we can list all of the port forwarding functions that we are performing, and we can delete a port forwarding function as follows:

```
meterpreter > portfwd list
0: 0.0.0.0:8080 -> 172.16.2.201:80
1: 0.0.0.0:139 -> 172.16.2.201:139
1: 0.0.0.0:22 -> 172.16.2.201:22

3 total local port forwards.
meterpreter > portfwd delete -l 8080 -p 80 -r 172.16.2.201
[*] Successfully stopped TCP relay on 0.0.0.0:8080
meterpreter >
```