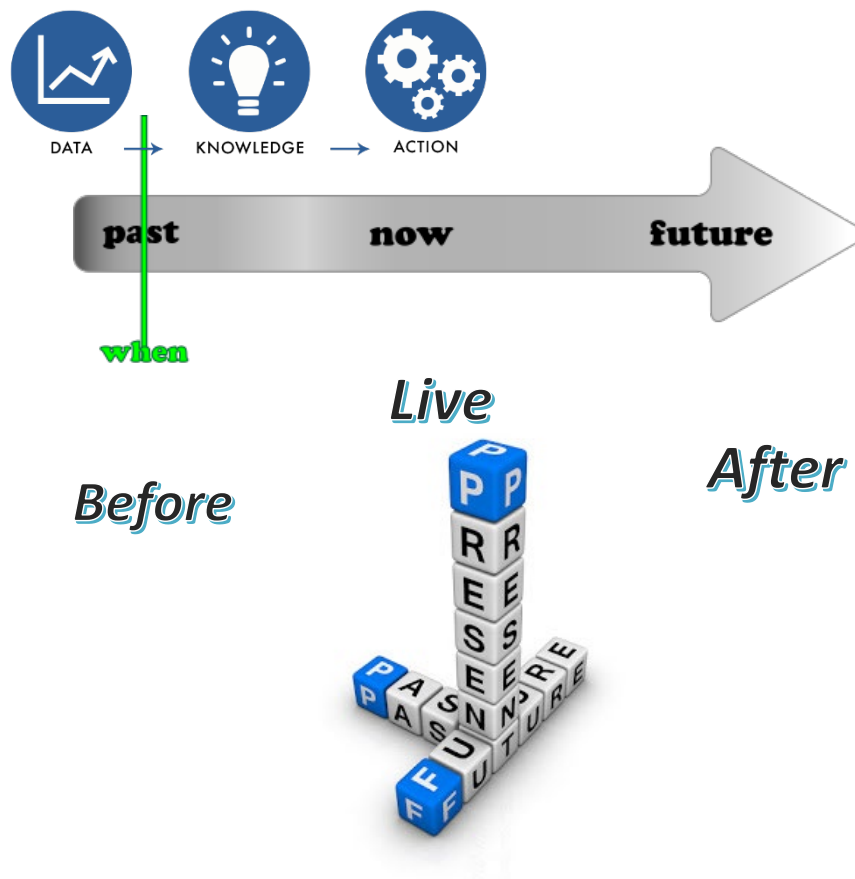




Advanced Cybersecurity (ACCB6000)

Hardening Network



Objectives

Note 1: To proceed with Activity8 completion of Activity 1, 2, 3, 4, 6 and 7 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*
- *Exploiting the Network*

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 9.*

Using Metasploit to Gain Access

1. **Hide Files using NTFS Streams**
2. **Covering Tracks**

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. Hide Files using NTFS Streams

1. Login into your Windows Server 2022. Check your drive's file system.

What is your File System Format?

2. Create a folder in C Drive. In my case, I have created HideMyFiles.
3. Copy any exe application file to the created Folder. I have taken two files for this activity.

 npp	22/01/2018 12:31	Application	4,070 KB
 PwDump7	01/07/2007 02:35	Application	76 KB

4. List the Directory to check if the files are present.

```
C:\HideMyFiles>dir
Volume in drive C has no label.
Volume Serial Number is 6A66-BCF5

Directory of C:\HideMyFiles

20/03/2022  16:31    <DIR>          .
20/03/2022  16:31    <DIR>          ..
22/01/2018  12:31         4,167,312  npp.exe
01/07/2007  01:35         77,824  PwDump7.exe
```

5. Create a notepad with a name readme.txt using command prompt.

```
C:\HideMyFiles>notepad readme.txt
```

Write a basic read me note on the text file and save the file.

6. Check the size of the exe files and the notepad files.

What is the file sizes?

Notepad:

Exe: NPP.exe

Exe: PwDump7.exe

7. Hide the exe file in the txt file.

```
type c:\HideMyFiles\npp.exe > c:\HideMyFiles\readme.txt:npp.exe
```

8. Check the file size again.

What is the file sizes?

Notepad:

Exe: NPP.exe

Exe: PwDump7.exe

Any Changes? Yes or No. Why?

9. Delete the npp.exe file from C drive HideMyFiles folder. (This action means, we have literally deleted the npp.exe file from our machine)

10. Execute the Hidden exe file now.

```
mklink backdoor_npp.exe readme.txt:npp.exe
```

symbolic link created for backdoor_npp.exe <====>
readme.txt:npp.exe

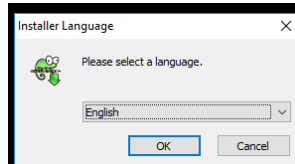
11. Execute backdoor_npp.exe

What happened when executing the above command?

Did the file execute?

If Yes, go to next step.

If no, Troubleshoot



12. Similarly do the same for PwDump7.exe file.

What happened when executing the backdoor?

Did the file execute? No, it wont execute the exe file.

A error message pops out stating required DLL File was not found or missing.

Do research to find out steps to execute the exe file along with the required DLL File.

Document the step with adequate screenshot and description. You shall use these identified steps in your demonstration.

By hiding files using NTFS File Streams, what could you achieve?

Two Dimensions: As an attacker, based on your activities so far, where you have created different exe files/ backdoors that you used to gain and maintain access. Those files could be hidden using NTFS streams (like this method), so that the users could not see your malicious file. So, you could execute them remotely whenever you need it. **If you are a security personal (doing a penetration testing) keep in mind that the malicious files could be hidden in this format which needs your attention.**

13. Reflection

- a. Do research to find out steps to execute the exe file along with the required DLL File. *Document the step with adequate screenshot and description. You shall use these identified steps in your demonstration.*

2. Clearing Tracks

1. Login into your Windows Server 2022.
2. Use Auditpol.
3. Login to your Windows 2022 Server.
4. Command Prompt
 - a. Auditpol /get/category:* ↵
(It would list all the categories)
 - b. Enable the Audit Policies
 - c. auditpol /set /category:"system", "account logon" /success:enable
/failure:enable ↵
 - d. Auditpol /get/category:* ↵
(You could see the settings)
 - e. To clear them: Auditpol /clear /y Auditpol /get/category:* ↵

What is Auditpol? How is it helpful in covering tracks?

Set various Auditpol policies and document with screenshots

List out similar tools that are used for covering tracks.

5. Reflection
 - a. What is Auditpol?
 - b. Setting various policies using Auditpol.
 - c. List out other tools used for auditing purpose/ covering tracks
 - d. Document with adequate screenshots and necessary description

Record your Reflection:



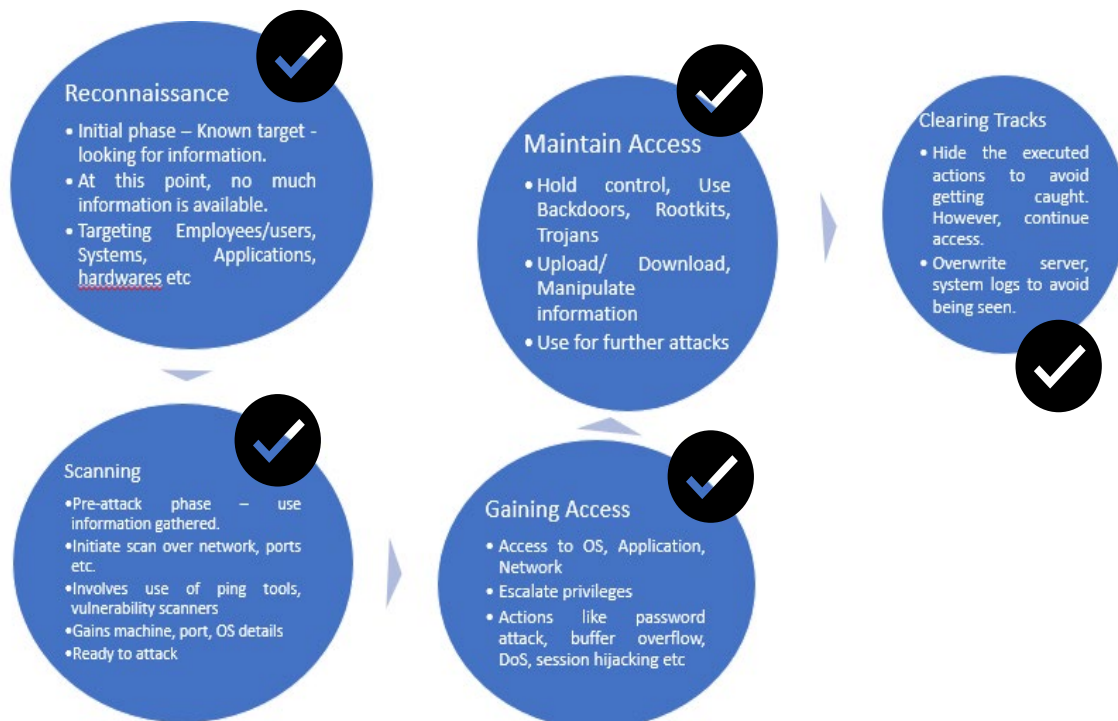
1. Understanding on all the activities
2. Understanding about various tools used
3. New/ Similar tools you identified and used
4. Compare and Contrast the tutorial tools with your identified tools
5. Rate yourself: How confident are you to do footprinting, reconnaissance, vulnerability assessment, social engineering, gaining access activity ethically?
6. Any other Troubleshooting Steps, you need to share?

End of All Activities. Our activities have completed.

Checkpoint:

Complete all the activities

All the very best for your future!!!!



Reference:

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