

Hacking Using Armitage & the Metasploit Framework

A. Introduction

A.1. Armitage:

Armitage is software that is included with Backtrack 5 version R3. It incorporates the several key hacking frameworks such as Metasploit and utilizes built-in tools like NMAP to automate the process of hacking.

A.2. In this lab:

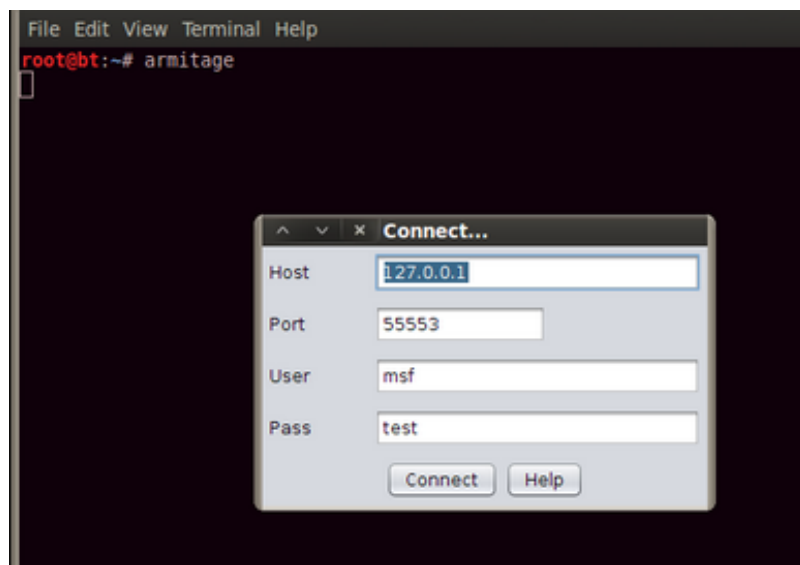
In this lab your focus will be a full-circle attempt at hacking a windows XP machine on a network, starting with enumeration and ending with full-admin access to the target machine.

You have been given the following information:

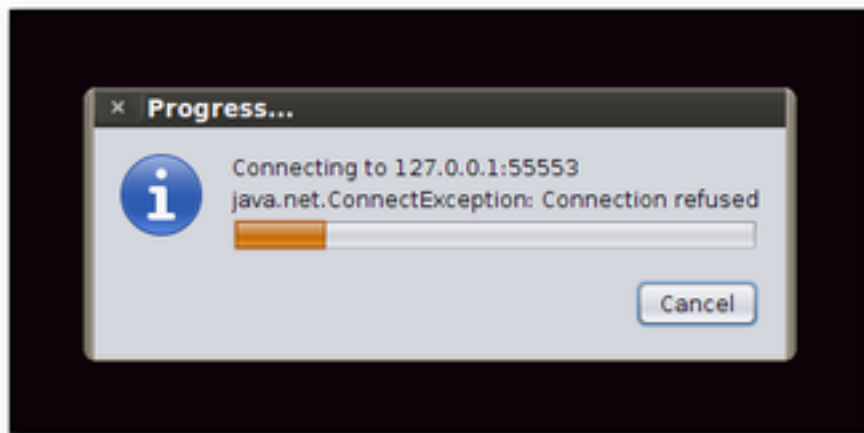
“There is a vulnerable machine located on the 10.0.0.255 network. Use your resources to hack it and leave something behind to show that you have infiltrated the machine.”

B. Armitage Start-Up

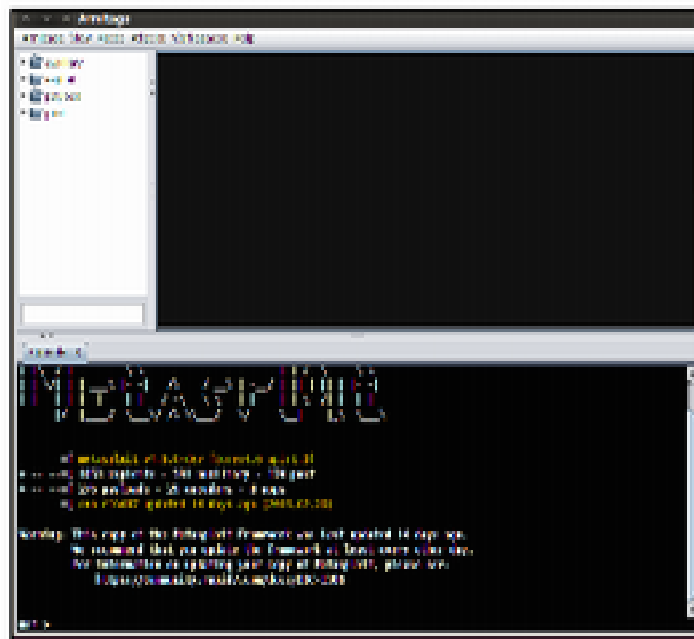
1. Begin by opening up a terminal on your backtrack machine and typing the following;
 - a. **armitage**
 - b. Upon doing so, you will be prompted with the following options:



- c. From here click “**connect**” since you are not connected to the internet.
- d. You will then be prompted with a screen, asking if you want to let Armitage start up a Metasploit RPC server. Since we are using Metasploit, click “**YES.**”
- e. You should now see a connection screen (Give it a second as we are on a virtual server and computing power takes time at 256mb of ram).



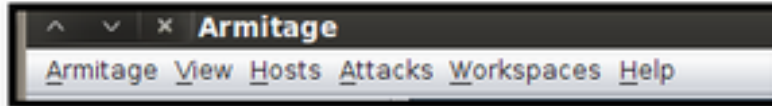
- f. After the connection module is finished, if all was done successfully, you should now see the Armitage GUI. Congrats and get ready to have some fun!



C. Getting around in Armitage

The Menu Bar:

Lets start with an overview of the GUI and a quick synopsis of how things work.



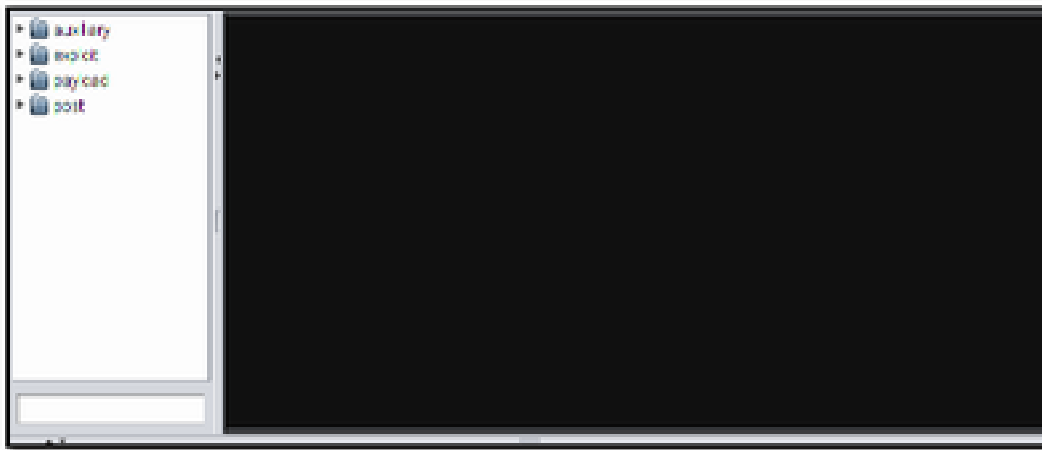
Armitage has the following options available for users in the menu bar:

1. **Armitage:** This is used much like a normal file section. Users can set preferences and connections (i.e. VPN) along with various options such as their exploit rank which will adjust the sensitivity of certain exploits (This is very useful for network testing).
2. **View:** The view option controls items and processes listed at the bottom of the screen (i.e. Where you currently see the Metasploit Logo). The “**View**” option lets you control the way information is formatted as it is processed through Metasploit.
3. **Hosts:** The “**Hosts**” option lets you discover and manage hosts on a myriad of different networks. You can either choose to add hosts manually or discover new hosts using tools like NMAP or even DNS enumeration.
4. **Attacks:** This option is used to do one of two things. First, it can find attacks for a specific host and let you choose which one you wish to attempt. Alternately, it has an attack automation process known as “Hail Mary” that will find and execute **all** known attacks in the metasploit frameworks database against a given target. This option should only be used if a hacker is very lazy or very desperate as it leaves a large network footprint.
5. **Workspaces:** This enables you to manage the Current Hosts selected, and if you desire, it allows you to create multiple views and attack spectrums (e.g. as is used for migrating through several levels of network defense).
6. **Help:** Links to helpful websites about Armitage.

The Exploit and Workspace Windows:

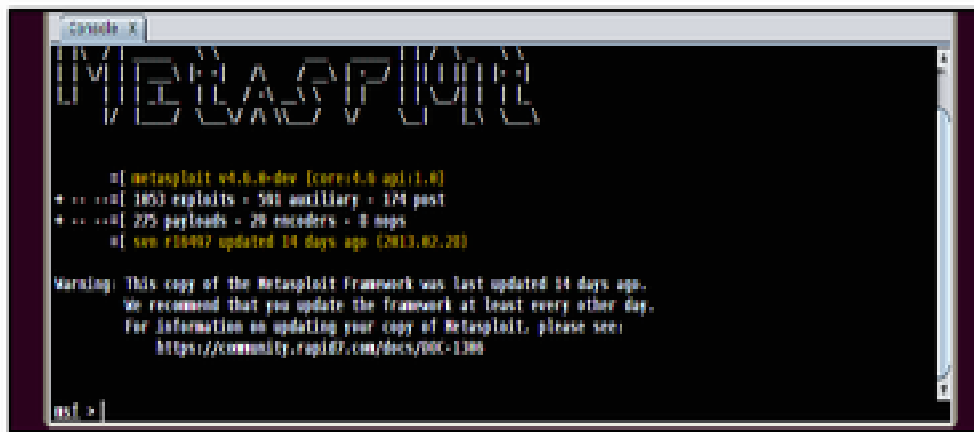
The Exploit Window (i.e. the smaller window to the left) is used to list all the available exploits that are currently available to you via the Metasploit network. These exploits can either be searched through manually or a search for a specific exploit or operating system can be conducted using the small search box beneath the window.

The Workspace Window to the right is our main attack listing area. In this area machines will be listed and these can be selected for further exploitation. We will cover the Workspace window further through the course of this lab.



The Console Log:

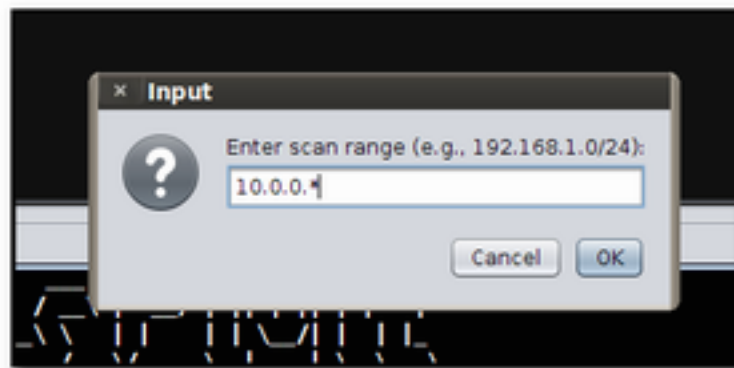
The console log is for all operations that the Armitage framework is committing from your actions. From this screen you will be able to view many useful items such as, for example, scanning information to attack progress or even password keylogging. The possibilities are only limited to the current script you are using. This window will be covered further in our examples.



D. Enumeration in Armitage

We will start our attack by scanning the **10.0.0.0** network using NMAP (i.e. Network Mapper). This is a built in Armitage security scanner used for host discovery and services identification on a network, as well as port scanning and operating system detection.

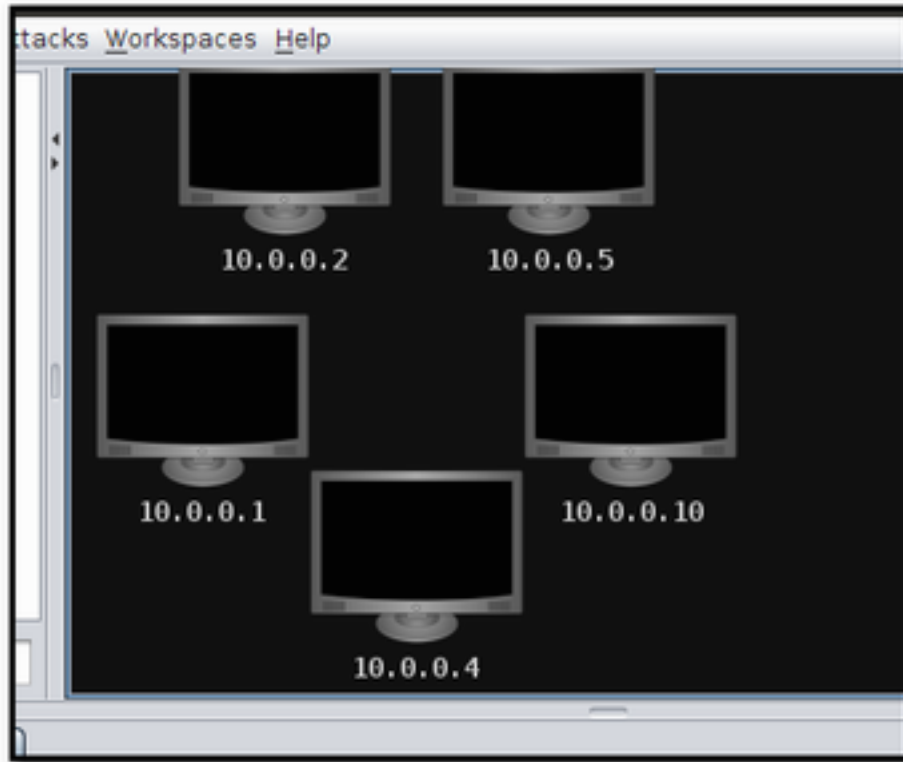
1. Begin by selecting the “**Hosts**” option and choosing the following:
 - a. **Nmap Scan -> Intense Scan**
 - b. You will then be greeted with an input box. This will be the address of the network we want to scan. Enter the following information:
 - i. **10.0.0.*** (the star is a wildcard that denotes all 255 machines) & click **OK**.



- c. You should now see that the console window has opened up a new window called “**nmap.**” Further, you will see the following information being to scroll on the screen:

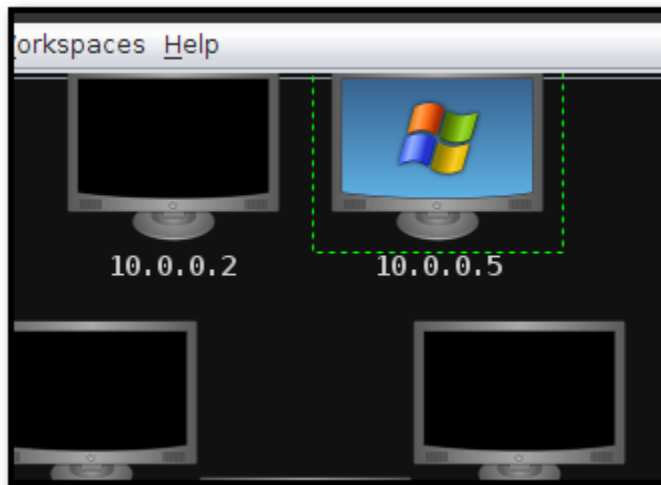
```
[*] Nmap: 80/tcp open  http
[*] Nmap: 135/tcp open  msrpc
[*] Nmap: 139/tcp open  netbios-ssn
[*] Nmap: 443/tcp open  https
[*] Nmap: 445/tcp open  microsoft-ds
[*] Nmap: 1025/tcp open  NFS-ar-IIIS
[*] Nmap: Nmap scan report for 10.0.0.10
[*] Nmap: Host is up (0.0002% latency).
[*] Nmap: Not shown: 94 closed ports
[*] Nmap: PORT      STATE SERVICE
[*] Nmap: 22/tcp    open  ssh
[*] Nmap: 80/tcp    open  http
[*] Nmap: 443/tcp  open  https
[*] Nmap: 3306/tcp  open  mysql
[*] Nmap: 3389/tcp  open  ms-term-serv
[*] Nmap: 5900/tcp  open  vnc
[*] Nmap: Nmap done: 256 IP addresses (5 hosts up) scanned in 13.19 seconds
nmap >
```

d. Allow the scan to run completely (this should take a minute or two) and ultimately, you will notice the “discovered” machines depicted in the “**Workspace**” window.

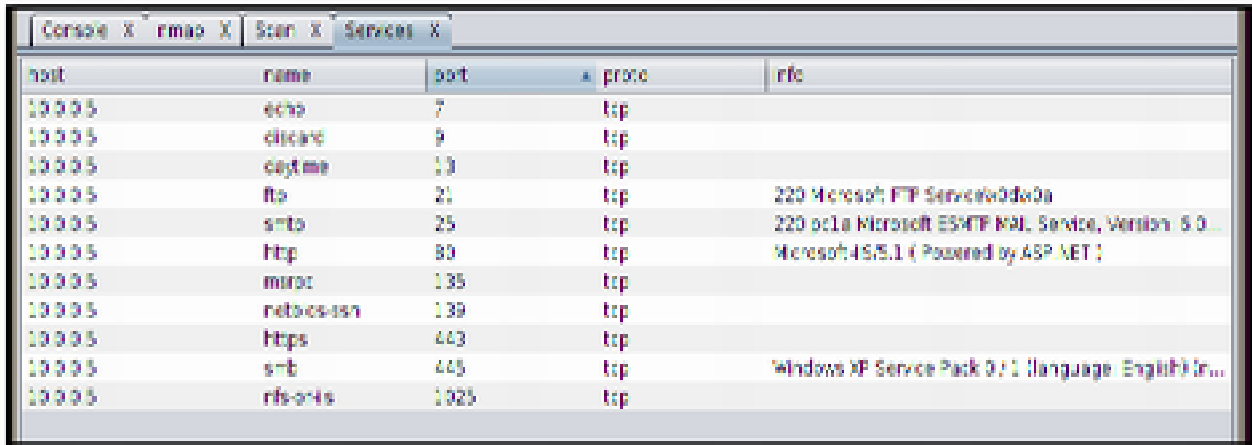


e. These are machines that have been found on the **10.0.0.*** network. Lets dig deeper.

- i. You should see that the icon in the workspace view has changed to a Windows logo as seen below:



- ii. To find out more about this machine:
 1. Right click the **10.0.0.5** machine and then click “**services.**”
 2. You should now see a new console log window called “**Services**” which gives a listing of all the current services that are running on this machine along with information about each service, such as port number, the protocol it operates on, etc.



host	name	port	proto	info
10.0.0.5	echo	7	tcp	
10.0.0.5	discard	9	tcp	
10.0.0.5	daytime	19	tcp	
10.0.0.5	ftp	21	tcp	220 Microsoft FTP Service[00d00a]
10.0.0.5	smtp	25	tcp	220 001a Microsoft SMTP MAIL Service, Version 6.0.
10.0.0.5	http	80	tcp	Microsoft IIS/5.1 (Powered by ASP.NET)
10.0.0.5	mysql	135	tcp	
10.0.0.5	netbios-ssn	139	tcp	
10.0.0.5	https	443	tcp	
10.0.0.5	smb	445	tcp	Windows XP Service Pack 0 / 1 (language English) (n...
10.0.0.5	rpc-ssls	1025	tcp	

You have now successfully fingerprinted the operating system and the services running the victim machine and have enough information to formulate an attack.

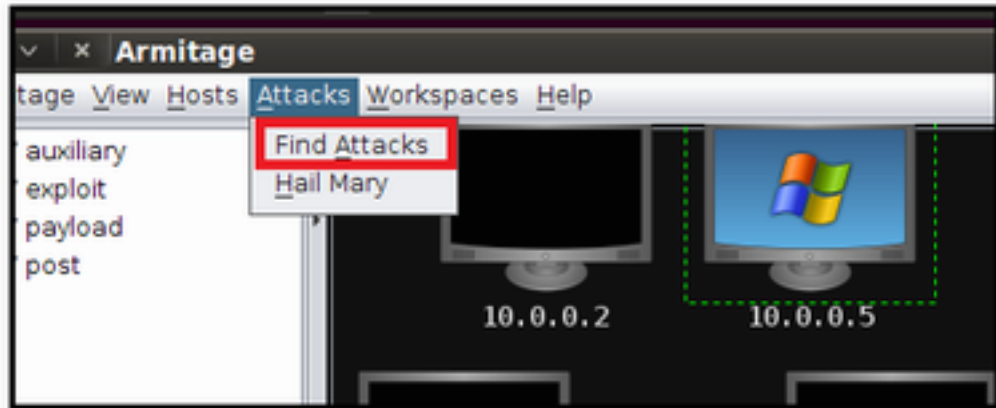
E. The Attack

Gaining Access:

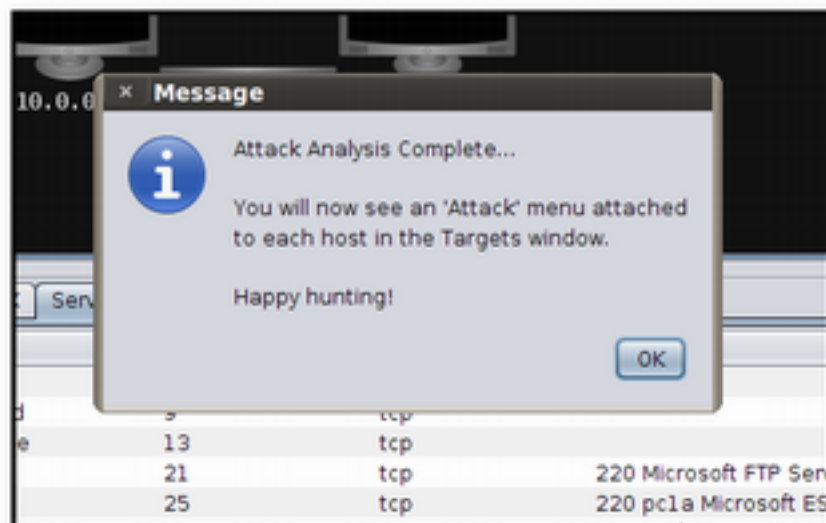
Armitage has several options available to exploit a Windows XP machine. With XP machines being used in over **30 percent** of the worlds networks this is highly advantageous to hackers.

1. To start the attack, highlight the **10.0.0.5** machine and choose the following:

Attacks -> Find Attacks



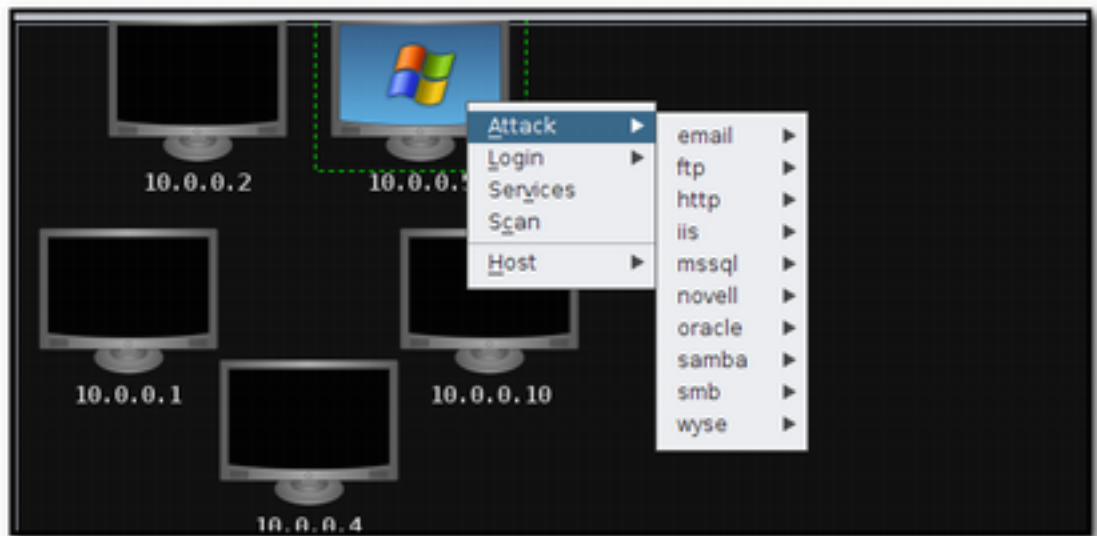
- a. After choosing this option you should be greeted with the following



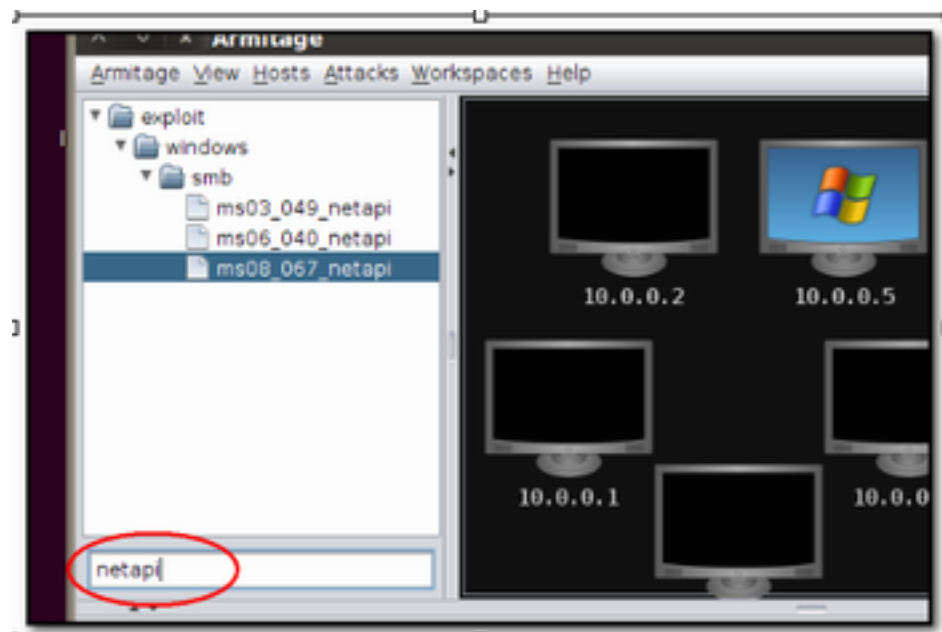
screen:

- b. Click "**OK**" and navigate back to the **10.0.0.5** machine. Right-Click on this machine and you should now see an option labeled "**attacks**". As you can see

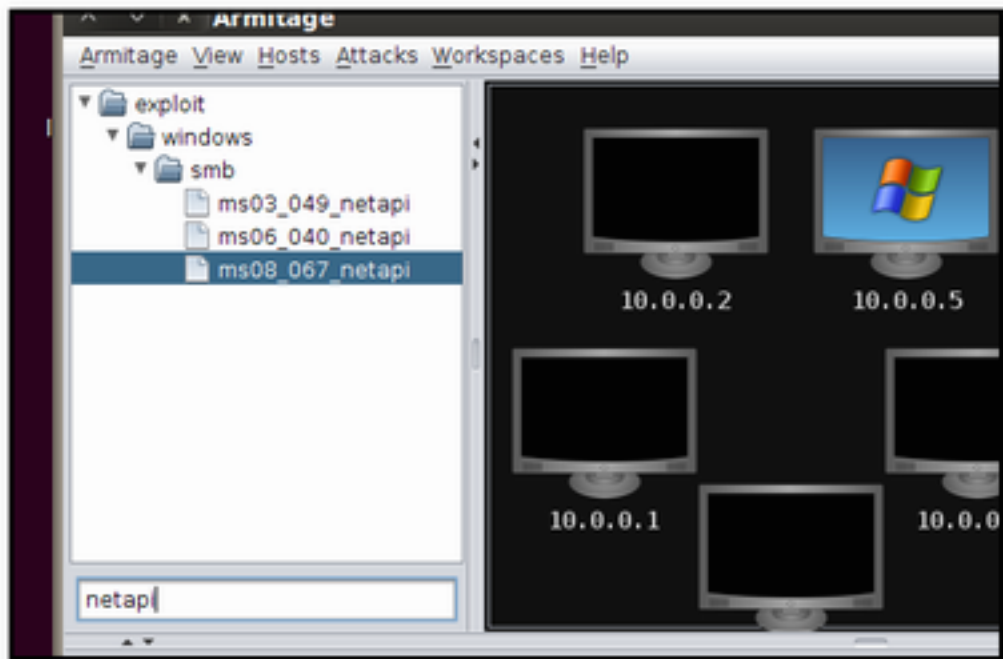
that there are several options to choose, but how do you know which one works?



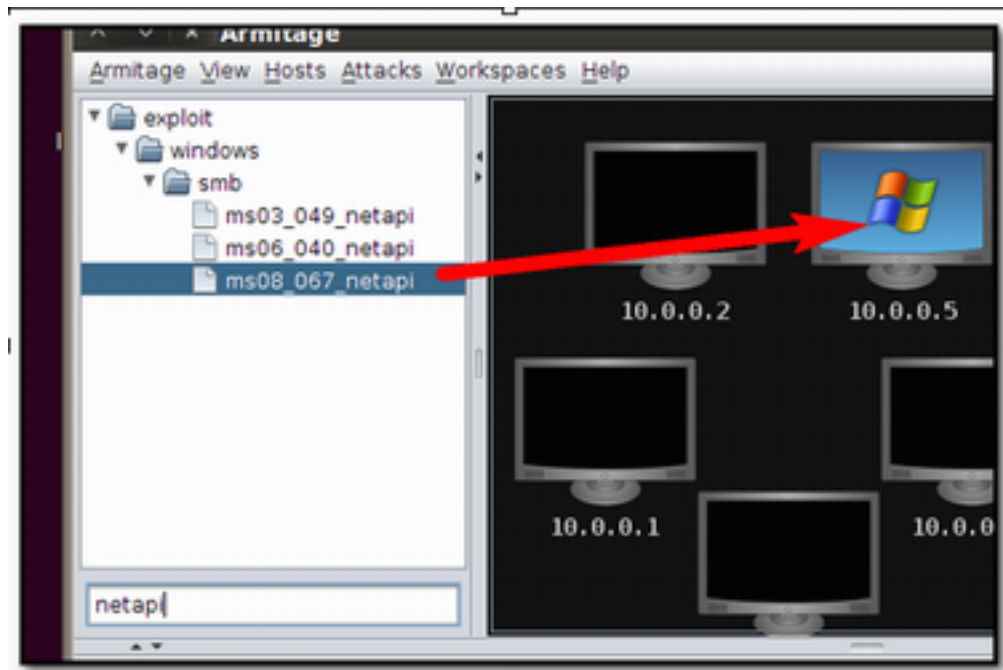
- c. Instead of using one of these options we are going to do our homework and use a well known exploit entitled **ms08_067_netapi**. Enter the word **“netapi”** into the exploit browser’s search box on the left, as seen below:



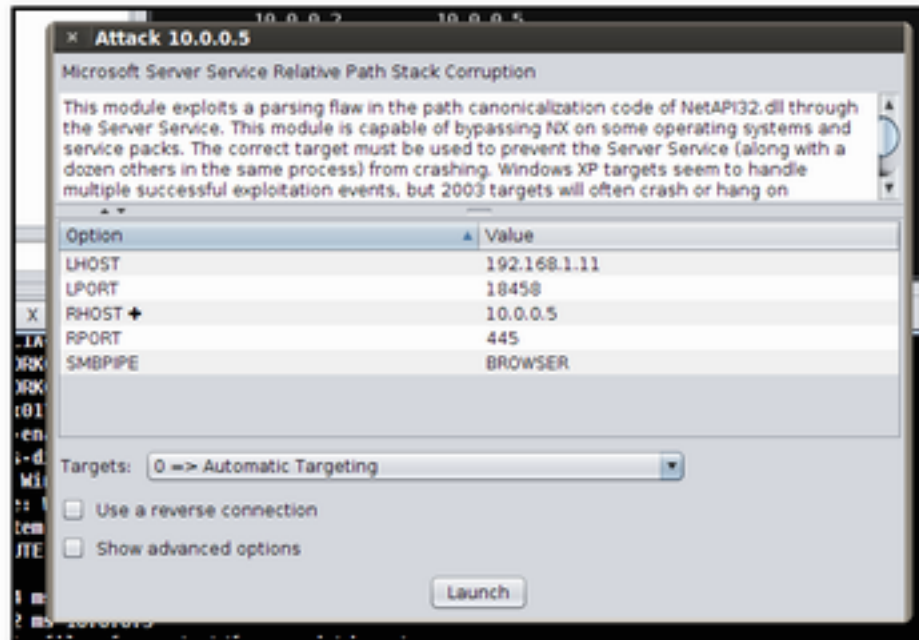
- d. You should then see the following:



- e. Drag-and-drop the option entitled **ms08_067_netapi** onto the **10.0.0.5** machine.

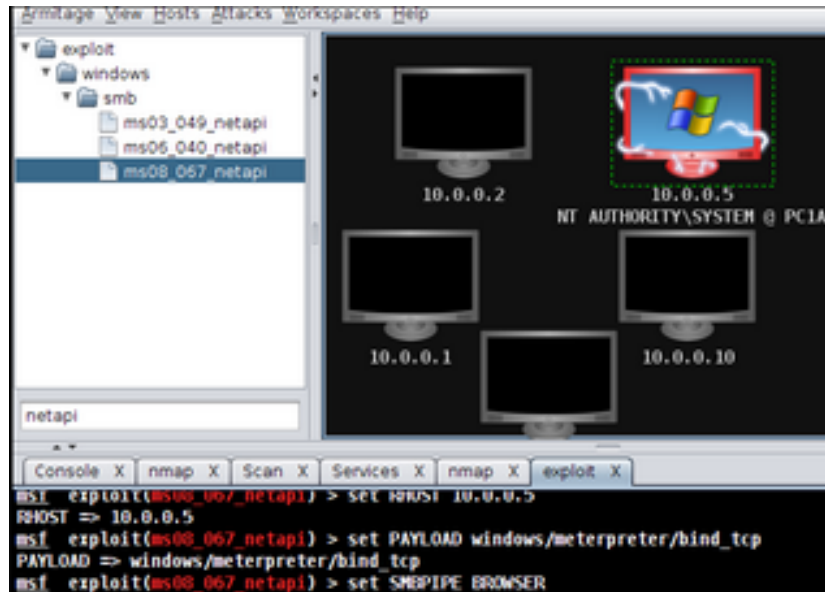


- f. After doing so you will be given the screen seen below. This screen contains several options and a brief synopsis about what the exploit does. We are going to leave everything as its default setting for now and click on the “Launch” icon.



- g. At this point, a new console log window will be created entitled “exploit” which shows how the exploit is communicating with the victim machine. Additionally, a lightning graphical effect appears on the icon for machine **10.0.0.5** to indicate that it has been compromised. You have successfully hacked the victim machine!

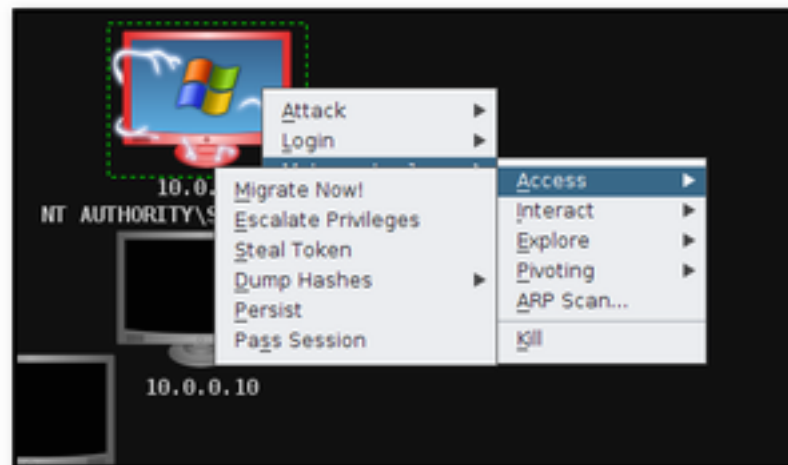
Collaborative Virtual Computer Lab (CVCLAB)
Penn State Berks



Maintaining Access:

Now that the machine has been compromised, what can we do with it? Begin by right-clicking on the newly infected machine and choose the following:

MeterPreter 1 -> Access -> Migrate Now!



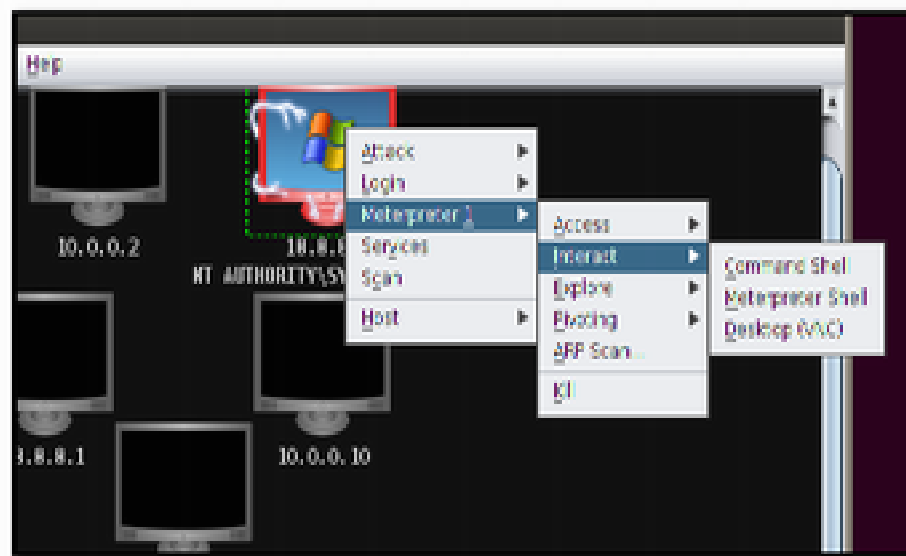
This is a very important step in the hacking process as it binds your newly created Meterpreter shell with a running process on the victim machine. It allows for full control of the shell so that it does not become blown out either by accident, or by the user OS terminating a service. This would cause you to have to repeat the entire process.

F. Leaving your mark


Since we are Pen-Testers and not malicious hackers we will leave our mark on this machine to let the victim know that we have hacked them while not doing any actual damage.

1. Start by right clicking the victim machine and choosing:

Meterpreter 1 -> Interact -> Command Shell



- a. By doing this you will receive a new console log window that should contain a very familiar command-line prompt:



```
C:\WINDOWS\system32>
C:\WINDOWS\system32>
C:\WINDOWS\system32>
C:\WINDOWS\system32>
C:\WINDOWS\system32>
C:\WINDOWS\system32>
C:\WINDOWS\system32> ipconfig
Windows IP Configuration

Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix  . :
    IP Address. . . . . : 10.0.0.5
    Subnet Mask . . . . . : 255.0.0.0
    IP Address. . . . . : fe80::250:56ff:fe87:85%4
C:\WINDOWS\system32>
```

- b. Use the following command to verify that you are in control of the victim machine:
 - i. **ipconfig**
 - ii. By doing this we can see that you IP address is now **10.0.0.5** and thus, you are operating on the victim machine.
 - iii. Browse to the the following directory using the commands you have previously mastered:

C:\wehackedyou

(Note: if your command-line skills are a little rusty, to access this directory, type: "**cd /wehackedyou**")

- iv. Once inside this folder create a folder with your the following format:
 - 1. **LastnameF** where F is equal to the first letter of your first name.
 - 2. This will let you instructor know that you have completed the lab.N
 - 3. Again, if you are uncertain the command is:: **mkdir** (i.e. make directory).
 - 4. So, for example, if your name was John Smith, type the following:
mkdir SmithJ
 - 5. To verify that it is there, type
dir \wehackedyou

- v. The final important step is to remove our current session so that we do not alarm system administrators or disrupt other hackers in your class.
 1. Right click the victim machine and choose the following:
 2. **Meterpreter 1 -> Kill**
 3. This will terminated your current Meterpreter Session.

Congratulations! You have sucessfully hacked a windows XP machine and can now be considered a fledgling script kiddie. Be sure to only use your newfound abilities to test suitable networks on which you have legal consent to do so.