GENCYBER – WEEK 1 – CYBER DEFENSE CHALLENGE

SY: Task must be performed by the system administrator
SA: Task must be performed by the security administrator
SE: Task must be performed by the server administrator
Multiple: Task can be performed by any of the listed roles.

Note: Tasks do not necessarily need to be completed sequentially, although many tasks build on previous tasks.

0. Write your role and your team number on the top of your sheet. A group with two students does not a system administrator; any tasks labeled SY can be completed by anyone. A group of four students will have two system administrators.

1. **SY or SA** Test connectivity to all floor computers by pinging each floor computer. You must have all pings completed to get a sign off. Write any host that cannot be pinged below.

2. **SY** Perform a tracert from any host on your floor to the IP address 8.8.8.8. What is the first hop the trace route goes through?

3. **SY** From any computer on your floor other than your Windows server, perform an nslookup to determine the IP address that the name of your active directory domain (metropolis-general.com) resolves to.

4. **SY** Carl Carlson has been reporting being unable to access the hospital webserver from Nurse Station B. Log into Nurse Station B as ccarlson and visit the hospital webserver. Verify that the ccarlson is able to access the web page.

5. **SY** The network administrator has asked that you verify the heartbeat server is functioning properly. Use netcat to connect to the heartbeat server three times and verify that, each time, that it sends you two two-digit numbers.

6. **SA** The chief security officer is concerned that the hospital FTP server is vulnerable. Use netcat to connect to the hospital FTP server (port 21) to get it's version number and search the Internet to determine if that server is vulnerable.

7. **SA** Using netcat, make an HTTP (GET /login.php HTTP/1.0) request to the hospital webserver to find the version number for Apache. Search the Internet to determine if the hospital webserver has known vulnerabilities.

8. **SE** Create a new group on your active server called *Management Users*.

9. **SY** Add the *Management Users* domain group to the local *Users* and *Remote Desktop Users* group of your floor management computer.

10. **SE** Create a user named *jjohnson* that is a member of the new *Management Users* group. Ensure that this user must change their password the next time they login.

11. **SE** Make sure that *jjohnson* is only allowed to log on to the floor management computer.

12. **SA** Using OSSIM, determine if any there have been any strange logins to systems at times you would not have expected. You may assume that there should have been no logins except those you performed.

13. **SE** The user *ddavidson* has moved from the nursing staff to the billing staff. Make the appropriate changes to the Windows server.

14. **SA or SE** Fran has reported to the security team that her password was compromised in a recent breach of a social media website. Make a change to the Windows server that would force Fran to reset her password the next time she logs in.

15. **SA** Using OSSIM, run a vulnerability scan on any one host to which you have OSSEC deployed. Verbally the results to the CEO, the training officer, or the security team lead. In your report, in your report, tell the person to whom you are reporting if you think the system is secure or not based on the vulnerability scan results.

16. **SA** Find and demonstrate three examples of actions that regular users (users who are not administrators on the computer) cannot perform.

17. **ANY** Alice has requested the ability to access to the billing computer so that she can work on a short-term project assigned to her that can be completed on any computer. Write down the two first principles this violates the most.

18. **ALL** The chief security officer has asked you to determine if any firewalls are active on any Windows hosts on your floor. Determine if any are active. Your group must have all accessible remote desktop connections open and showing the firewall status to get a sign off.

19. **ALL** The network administrator has reported seeing some strange traffic coming from your floor. Use the command *netstat -an* to determine if there are any suspicious network connections to or from any computers on your floor. You may need to research what ports are commonly used. You must show each the results from all five computers to get a sign off.

20. **SA** Determine the IP addresses of any suspicious network connections.

21. **SA** Research the primary Windows tool for implementing the first principle of *Data Hiding* and implement it on any one host in the environment.

22. **SY** The Chief Security Officer has determined that the billing and management computers need more restrictions. Modify user account control on these computers so that it as the maximum security level.

23. **SY or SE** Verify that no new user accounts have been created on any user host in the network. If you find a new user account, determine what groups the user account is a member account.

24. **SY or SE** Delete all suspicious user accounts from all hosts.

25. ***SA*** Using OSSIM and/or Windows logs, attempt to determine the time at which the suspicious user account was created.

26. **SA** Visit the web portal running on http://10.0.0.3/login.php in your web browser. View the source of the website and determine if there is any suspicious HTML in that code.

27. **ANY** Search the hard drives of your hosts to determine if there are any suspicious files located on those hard drives. Upload the suspicious files to virus total to determine if they are malicious.

28. **ANY** Research the file that you found to determine what kind of malware it is. Write down your answer.

29. **ANY** Research the specific exploit associated with the delivery of this malware. Your answer should begin with MS

RED ALERT, RED ALERT