ADVANCED CYBER CAMP COMPETITION

Windows

1. **What is the run command to open the Local Users and Groups MMC snap-in?**
    - ○

2. **Which utility is used to monitor the security status of a Windows computer?**
    - ○

5. **Which command opens the Windows Security and Maintenance User Interface?**
    - ○

6. **Where can you find the option to add and remove programs in Windows 10?**
    - ○

7. **Which command is used to display the current settings of net accounts?**
    - ○

8. **What is the function of the 'net user' command?**
    - ○

9. **What is the primary use of the Process Explorer utility?**
    - ○

11. **What is the default security setting for loading and unloading device drivers in Local Security Policy?**
    - ○

12. **How can you start the Event Viewer in Windows 10?**
    - ○

13. **Which command is used to start the Local Group Policy Editor?**
    - ○

14. **What does the command 'net share' do?**
    - ○

15. **Which command is used to stop sharing a folder in Windows 10?**
    - ○

16. **Which tool in the Sysinternals Suite monitors the activity of all processes on a system?**
    - ○

17. **What is the abbreviation for the Windows Command Prompt executable?**
    - ○

18. **Which command is used to remove a user from the system in Windows 10?**
    - ○

19. **What is the purpose of the 'net localgroup' command?**

○

20. **Which command is used to view the status of services in Windows 10?**

○

21. **Which utility in the Sysinternals Suite helps analyze malware by monitoring system calls?**

○

22. **Which service manages Windows updates?**

○

23. **What is the default setting for Network access: Do not allow anonymous enumeration of SAM accounts?**

○

24. **Which command is used to change a user's password in Windows 10?**

○

25. **What is the run command to open the Programs and Features window?**

○

26. **Which utility helps in viewing and managing shared folders in Windows 10?**

○

27. **Which command is used to display information about network connections?**

○

28. **Which utility in Sysinternals Suite is used to explore the startup programs in Windows?**

○

29. **What does the 'net localgroup administrators' command do?**

○

30. **What is the function of the 'net accounts /minpwlen' command?**

○

31. **What does the 'net accounts /lockoutthreshold' command do?**

○

32. **What is the function of the 'net localgroup administrators /add' command?**

○

33. **Which command is used to open the Local Security Policy editor?**

○

34. **What is the default account lockout duration recommended by Microsoft?**

○

35. **Which command is used to find out which ports are being used by services in Windows 10?**

   ○

36. **What is the purpose of the 'icacls' command in Windows?**

   ○

37. **What is the purpose of the 'net accounts /maxpwage' command?**

   ○

38. **Which command is used to start the Task Manager in Windows 10?**

   ○

39. **What is the function of the 'net localgroup "Sys Admins"' command?**

   ○

System Hardening and CTF Questions

1. When it comes to Windows system hardening, it is always a good idea to set a password policy. Use the following parameters to configure the password policy settings:
    a. Password history: 6 passwords remembered.
    b. Minimum password age: 45 days
    c. Maximum password age: 75 days
    d. Minimum password length: 13 characters
    e. Password complexity requirements: Enable

2. Next, set the account lockout policy using the following:
    a. Account lockout duration: 30 minutes
    b. Account lockout reset duration: 30 minutes
    c. Account lockout threshold: 5 invalid logon attempts

3. Refer to the Windows Security Firewall & Network Protection settings and make sure all network firewalls have been enabled:
    a. Domain network
    b. Private network
    c. Public network

4. It is best practice to disable the Guest and Admin accounts. Check that both accounts are disabled. If not, be sure to disable them now.

5. You have been tasked to ensure that authorized user accounts have been configured correctly. Use the following to ensure that each user account is configured with the correct permissions and account types:
    a. Change the standard users, **epoe** and **rdale** to administrators.
    b. A new staff member with the username **hsimpson** was hired. The user should be an administrator with the password ***Mmmmmdonuts!***
    c. With the new CIS building's completion, some staff members are transferring to another department and need to be removed from the system. Delete the following user accounts:
        i.**tkane**

ii. **cdiaz**
iii. **hraj**

d. Now, add a new user with the username, **sgriffin** that is scheduled to start next week. Set the user's default password to ***Rupurt1234***. Set it so that the user must change his password at the next login.

e. Add new standard user named ***dvader***. Then add the user to the Sys Admin group.

f. Change the account type for the following two users to standard users:
i. **jterry**
ii. **CIS-Studen**t

g. Lastly, remove any users that were not mentioned, but NO NOT remove the users listed in the list of critical users. Critical Users:
i. **DefaultAccoun**t
ii. **Elang**
iii. **Guest**
iv. **RCC-Cyber-Defense**
v. **WDAGUtilityAccount**

6. Ensure the audit policy so that the security settings for all policies are set to Success, Failure.

7. We learned about gpedit and the settings in Administrative templates. Use your skills to find the enabled setting that is preventing the usage of OneDrive and then investigate further to find the **Flag**. __________________

8. It's come to your attention that an unauthorized user has accessed your event viewer logs using Custom Views. Search the system to find the Custom View that was created to uncover the **Flag.** ________________

9. User, Edgar has hidden a flag inside a hidden share, using either Windows MMC or the Command Prompt, find the share and see inside to capture the **Flag.** _____________

10. Being a network administrator can be challenging. Luckily, you've attended RCC's Cyber Camp and know how to use the Advanced Firewall. Hacker's love to find ways to extract data from your network, but you were able to narrow it down to Inbound port 999. Find the **Flag**. ________________

11. By now you're a pro in the Local GPO (Group Policy). Turn On Security Center to find your **Flag.** ___________________

12. Time to Run and take a shortcut to the cpl! We've explored some more Advanced Windows Settings, and now it's time to use what you've learned to get to System Properties. Look through the information in the System Properties to find the Flag! Get to this place and get the **Flag.** _________________