CyberPatriot Windows 11
Training 2 Image Answer Key

Welcome to the CyberPatriot Training Round 2!

The vulnerabilities in this image are some of the most basic ones found during a CyberPatriot competition. Even if you do very well with these vulnerabilities, you will experience greater difficulty as the season progresses. The README file on the desktop in this image may be more detailed than those you see during the competition. You will have to use your own knowledge, not just the hints in this file, to achieve a high score during the actual competition.

Below are the answers to the problems that are being scored in this image.

It is also possible to lose points during the competition. Simple penalties that may arise are noted below the answers. There are many ways to solve some of the problems below. This answer key just shows one method in each case.

Coaches will be sent categories of vulnerabilities following each online round.

Answers

1. Forensics Question 1

   Answer: 192.168.202.138

   Open **attack.pcap** shortcut on Desktop > go to lines 5, 6, and 9 > host IP address is under the **Source** column

2. Forensics Question 2

   Answer: There are always ticking clocks

   Open a ciphertext decrption tool such as https://www.mobilefish.com/services/one_time_pad/one_time_pad.php > set conversion method to **Decrypt** > enter e302a1b9e317659052c83f56033d4a85c74b12e85ef63b628b82fb02b10ab1 as the **one-time pad ciphertext** > enter b76ac4cb863704e237e85e3a745c33f6e73f7b8b359f5505abe1976dd261c2 as the **message/cipher** > select **Convert**

3. The Guest account is not enabled

   In the search bar, search **Computer Management** > **Local Users and Groups** > **Users** > double-click on **Guest** > Select **Account is disabled** > Click **Apply**

4. Remove unauthorized user darkarmy

   In the search bar, search **Computer Management** > **Local Users and Groups** > **Users** > Right-click on **darkarmy** > **Delete** > **Yes** > **OK**

5. Remove unauthorized user fsociety

   In the search bar, search **Computer Management** > **Local Users and Groups** > **Users** > Right-click on **fsociety** > **Delete** > **Yes** > **OK**

6. Create user account for user penguru

   In the search bar, search **Computer Management** > **Local Users and Groups** > **Users** > **More Actions** > **New User** > in the User name: field, enter **penguru** > **Create**

7. Change unauthorized administrator jchutney to standard user

   Click on the search bar > **Settings** > **System** > **Accounts** > **Other users** > **jchutney** > **Change account type >** Click on the dropdown arrow, select **Standard User** > **OK**

8. Change unauthorized administrator sjacobs to standard user

   Click on the search bar > **Settings** > **System** > **Accounts** > **Other users** > **sjacobs** > **Change account type >** Click on the dropdown arrow, select **Standard User** > **OK**

9. User sswailem password expires

   In the search bar, search **Computer Management** > **Local Users and Groups** > **Users** > Double-click on user **sswailem** > uncheck the box **Password never expires** > **Apply** > **OK**

10. A secure minimum password length is required

    Press the **Windows button + R** and search **secpol.msc** > **Account Policies** > **Password Policy** > **Minimum password length** > Use the arrow to set the length to 10 characters > **Apply**

11. Passwords are not stored using reversible encryption

    Press the **Windows button + R** and search **secpol.msc** > **Account Policies** > **Password Policy** > **Store passwords using reversible encryption** > **Disabled** > **Apply**

12. Passwords must meet complexity requirements

    Press the **Windows button + R** and search **secpol.msc** > **Account Policies** > **Password Policy** > **Password must meet complexity requirements**

13. Microsoft network client: Digitally sign communications (always) [enabled]

    Press the **Windows button + R** and search **secpol.msc** > **Local Policies** > **Security Options** > **Microsoft network client: Digitally sign communications always (always)** > **Enabled** > **Apply** > **OK**

14. Do not require CTRL+ALT+DEL [disabled]

    Press the **Windows button + R** and search **secpol.msc** > **Local Policies** > **Security Options** > **Do not require CTRL+ALT+DEL** > **Disabled** > **Apply**

15. Windows Remote Management service does not send or receive unencrypted traffic

    Press the **Windows button + R** and search **gpedit.msc** > **Computer Configuration** > **Administrative Templates** > **Windows Components** > **Windows Remote Management Service (WinRM)** > **Allow unencrypted traffic** > **Disabled** > **Apply** > **OK**

16. Firewall protection has been enabled

In the search bar, search **Windows Security** > **Firewall & network protection** > Under **Domain network**, select **Turn On** > **Yes** > Under **Private network**, select **Turn On** > **Yes** > Under **Public network**, select **Turn On** > **Yes**

17. Remote desktop sharing is turned off

    Press the **Windows button + R** and search **gpedit.msc** > **Computer Configuration** > **Administrative Templates** > **Windows Components** > **Remote Desktop Services** > **Remote Desktop Session Host** > **Connections** > **Allow users to connect remotely by using Remote Desktop Services** > **Disabled** > **Apply** > **OK**

18. Notepad++ has been updated

    Open Notepad++ > ? > **Update Notepad++** > **Yes** > **Yes** > **Yes** > **OK** > **Next** > **I Agree** > **Next** > **Next** > **Install** > **Finish**

19. Google Chrome has been updated

    Open Google Chrome > On the top-right, select **Reinstall Chrome** > **Download Chrome** > On the bottom task bar of the browser, the file **ChromeSetup.exe** will appear. Select the up arrow next to the file. Then select Show in folder. Double-click on **ChromeSetup** > **Yes** > Open Google Chrome > **About Chrome** > **Relaunch**

20. Removed shellshock exploit script

    Open File Explorer > **Local Disk (C:)** > **Users** > **ealderson** > **Downloads** > Right-click on **shellshock-exploit.py** > **Delete**

21. Remove Jellyfin Media Player

    Open File Explorer > **Local Disk (C:)** > **Program Files** > Right-click **Jellyfin** folder > **Delete**

22. Remove Burp Suite Community Edition

    On the desktop, right-click on **Burp-Suite Community Edition** > **Delete**

23. Remove Python3

    On the desktop, right-click on **Python 313 (64-bit)** > **Delete**

24. Remove Nmap

    Open File Explorer > **Local Disk (C:)** > **Program Files (x86)** > Right-click **Nmap** folder > **Delete**

25. Disable Apache server signature

    Open File Explorer > **Local Disk (C:)** > Apache24 > conf > httpd.conf > Select open with Notepad++ > Just once > On like 61, change the test Server Signature On to Server Signature Off > File > Save

Penalties

- Account lockout threshold less than 5 is deprecated
- Google Chrome is not installed at the default location
- Notepad++ is not installed at the default location
- 7-Zip is not installed at the default location
- Wireshark is not installed at the default location