CyberPatriot 18
Round 1 Image Answers and Vulnerabilities

Windows 11

Forensics Question 1 Answer: I know you are a fraud!

Forensics Question 2 Answer: dhardman, hgunderson, rzane, cdennis

- Removed unauthorized user dhardman
- Removed unauthorized user cdennis
- Removed unauthorized user twolf
- User jkirkwood is not an administrator
- User dpaulsen is not an administrator
- Created user account edarby
- Updated Remote Desktop Users group
- A secure minimum password age exists
- A secure lockout threshold exists
- Limit local use of blank passwords to console only [enabled]
- Do not allow anonymous enumeration of SAM accounts [enabled]
- Firewall protection has been enabled
- Remote Assistance connections have been disabled
- FTP service has been stopped and disabled
- The majority of Windows updates are installed
- Notepad++ has been updated
- Google Chrome has been updated
- Removed Wireshark
- Removed CCleaner
- RDP network level authentication enabled

Mint 21

Forensics Question 1 Answer: 7bd6478ecf2641bebc989892f835cf85

Forensics Question 2 Answer: /home/benjamin/Music/

- Removed unauthorized user ttanner
- Removed unauthorized user cdennis
- User kbennett is not an administrator
- Created user account mross
- User mross must change password at next login
- A default minimum password age is set
- Uncomplicated Firewall (UFW) protection has been enabled
- Apache2 service has been disabled or removed
- The system refreshes the list of updates automatically
- Install updates from important security updates
- Chromium has been updated
- OpenSSH has been updated
- Prohibited MP3 files are removed
- Prohibited software aisleriot removed
- Prohibited software ophcrack removed
- SSH root login has been disabled

CYBERPATRIOT ROUND 1
VULNERABILITY CATEGORIES

Windows 11

- Account Policy 2
- Application Security 1
- Application Updates 2
- Defensive Countermeasures 1
- Forensics Questions 2
- Local Policy 2
- Operating System Updates 1
- Service Auditing 1
- Uncategorized Operating System Settings 1
- Unwanted Software 2
- User Auditing 7

Mint 21

- Account Policy 1
- Application Security 1
- Application Updates 2
- Defensive Countermeasures 1
- Forensics Questions 2
- Operating System Updates 2
- Prohibited Files 1
- Service Auditing 1
- Unwanted Software 2
- User Auditing 5

CYBERPATRIOT VULNERABILITY CATEGORY SUMMARY

Account Policies
Password Policy, Lockout Policy, etc.

Application Security Settings
Critical Service Settings, Required Application Settings, Application Permission, etc.

Application Updates
Application Updates, Application Automatic Update Settings, etc.

Defensive Countermeasures
Firewall, Anti-virus, Encryption, etc.

Forensic Questions

Local Policies
Audit Policy, User Rights Assignment, Security Options --
Security Options include Network Security Options and Privilege Elevation Authorization, etc.

Operating System Updates
Windows Updates, Service Packs, Windows Automatic Update Settings, etc.

Policy Violation: Malware
Backdoors, Remote Administration Tools, Keyloggers, Password Sniffers, etc.

Policy Violation: Prohibited Files
Individual Files, Software Archives, Confidential In Forensic Questions, etc.

Policy Violation: Unwanted Software
Games, Servers, Scareware, Adware, PUP, "Hacking" Tools, etc.

Service Auditing
Enable and Disable Services, etc.

Uncategorized Operating System Settings
Remote Access, File Sharing, Screen Locking, Group Policy Settings, Operating System Permissions, etc.

User Auditing
Authorized Users, Groups, and other settings unique to users, etc.