CyberPatriot 18 Round 2
Image Answers and Vulnerabilities

Windows 11

Forensics Question 1 Answer: C:\Users\litt\Documents\Personal

Forensics Question 2 Answer: benjamin
Answer: jpearson
Answer: kbennett
Answer: jquelling
Answer: dscott

- Removed unauthorized user aholt
- Removed unauthorized user jquelling
- User dscott is not an administrator
- User shuntley is not an administrator
- Changed insecure password for user llitt
- User sbandaru has a password
- Passwords are not stored using reversible encryption
- A secure account lockout duration exists
- Do not require CTRL+ALT+DEL [disabled]
- Firewall protection has been enabled
- Remote desktop sharing is turned off
- World Wide Web Publishing service has been stopped and disabled
- 7-Zip has been updated
- LibreOffice has been updated
- Removed prohibited MP3 files
- Removed TicTacToe
- Removed Cursor
- Removed Tini backdoor

Mint 21

Forensics Question 1 Answer: 220 Welcome to AFA

Forensics Question 2 Answer: rzane
Answer: shuntley

- Guest account is disabled
- Removed unauthorized user tgianopolous
- Removed unauthorized user jquelling
- User dscott is not an administrator
- Changed insecure password for user llitt
- Created new administrator account for edarby
- User edarby must change password at next login
- A minimum password length is required
- IPv4 TCP SYN cookies have been enabled
- Uncomplicated Firewall (UFW) protection has been enabled
- Insecure permissions on FTP root directory fixed
- OpenSSH service is disabled or removed
- The system refreshes the list of updates automatically
- The update manager installs updates automatically
- Install updates from important security updates
- Systemd has been updated
- Chromium has been updated
- Vsftpd has been updated
- Prohibited MP3 files are removed
- Prohibited software aMule removed
- Prohibited software Wireshark removed
- Prohibited software Zangband removed
- FTP users may log in with SSL

Server 2022

Forensics Question 1 Answer: T00GooD4Harvard!

Forensics Question 2 Answer: jpearson

Forensics Question 3 Answer: dscott
Answer: harvey123

- Removed unauthorized user ttanner
- Removed unauthorized user tgianopolous
- User kbennett is not an administrator
- User rzane is not an administrator
- Changed insecure password for user dscott
- Created group Exec SMB Users
- Added users to group Exec SMB Users
- A secure minimum password length is required
- A secure lockout threshold exists
- Audit File Share [Success]
- Everyone may not access this computer from the network
- Limit local use of blank passwords to console only [enabled]
- Microsoft network server: Digitally sign communications (always) [enabled]
- File sharing disabled for hidden share Private$
- Created Executive SMB Share
- Windows automatically checks for updates
- Notepad++ has been updated
- Wireshark has been updated
- Removed plain text file with passwords in it
- Removed TightVNC Server
- Removed netcat backdoor
- Exec SMB share permissions have been correctly configured
- SMB 1.x removed or disabled

CYBERPATRIOT ROUND 2
VULNERABILITY CATEGORIES

Windows 11

- Account Policy 2
- Application Updates 2
- Defensive Countermeasures 1
- Forensics Questions 2
- Local Policy 1
- Malware 1
- Prohibited Files 1
- Service Auditing 1
- Uncategorized Operating System Settings 1
- Unwanted Software 2
- User Auditing 6

Mint 21

- Account Policy 1
- Application Security 1
- Application Updates 2
- Defensive Countermeasures 1
- Forensics Questions 2
- Local Policy 1
- Operating System Updates 4
- Prohibited Files 1
- Service Auditing 1
- Uncategorized Operating System Settings 1
- Unwanted Software 3
- User Auditing 7

Server 2022

- Account Policy 2
- Application Security 2
- Application Updates 2
- Forensics Questions 3
- Local Policy 4
- Malware 1
- Operating System Updates 1
- Prohibited Files 1
- Uncategorized Operating System Settings 2
- Unwanted Software 1
- User Auditing 7

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.