CP-XIII ROUND 3
SILVER AND MIDDLE SCHOOL
VULNERABILITY CATEGORIES

Windows 10

- Account Policies – 2
- Application Security Settings – 6
- Application Updates – 2
- Defensive Countermeasures – 1
- Forensics Questions – 3
- Local Policies – 5
- Operating System Updates – 1
- Policy Violation: Malware – 2
- Policy Violation: Prohibited Files – 1
- Policy Violation: Unwanted Software – 3
- Service Auditing – 3
- Uncategorized Operating System Settings – 4
- User Auditing – 5

Server 2019

- Account Policies – 1
- Application Security Settings – 5
- Application Updates – 1
- Defensive Countermeasures – 1
- Forensics Questions – 4
- Local Policies – 8
- Operating System Updates – 1
- Policy Violation: Malware – 2
- Policy Violation: Prohibited Files – 2
- Policy Violation: Unwanted Software – 2
- Service Auditing – 1
- Uncategorized Operating System Settings – 3
- User Auditing – 6

Ubuntu 18

- Account Policies – 4
- Application Security Settings – 6
- Application Updates – 2
- Defensive Countermeasures – 1
- Forensics Questions – 3
- Local Policies – 4
- Operating System Updates – 3
- Policy Violation: Prohibited Files – 1
- Policy Violation: Malware – 1
- Policy Violation: Unwanted Software – 4
- Service Auditing – 2
- Uncategorized Operating System Settings – 1
- 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.

Forensics 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
Media Files, Software Archives, Confidential Information, 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.