CP-XIV ROUND 1 MIDDLE SCHOOL VULNERABILITY CATEGORIES

Server 2019
- Account Policies   2
- Application Updates   2
- Forensic Questions   2
- Local Policies   1
- Operating System Updates   1
- Prohibited Files   1
- Service Auditing   1
- Uncategorized Operating System Settings   1
- Unwanted Software   4
- User Auditing   6

Windows 10
- Account Policies   2
- Application Security Settings   1
- Application Updates   1
- Defensive Countermeasures   1
- Forensic Questions   2
- Local Policies   1
- Operating System Updates   1
- Prohibited Files   1
- Service Auditing   1
- Uncategorized Operating System Settings   1
- Unwanted Software   3
- User Auditing   6

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.