



CP-XII STATE ROUND
VULNERABILITY CATEGORIES
GOLD TIER



Windows 10

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

Server 2016

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

Ubuntu 14

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



CP-XII 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.