



## **CYBERPATRIOT SEMIFINALS** **PLATINUM VULNERABILITY CATEGORIES**



### **Windows 10**

• Account Policy	2
• Application Security	12
• Application Updates	3
• Defensive Countermeasures	1
• Forensics Questions	4
• Local Policy	5
• Malware	2
• Operating System Updates	1
• Prohibited Files	2
• Service Auditing	2
• Uncategorized Operating System Settings	4
• Unwanted Software	3
• User Auditing	5

### **Server 2019**

• Account Policy	2
• Application Security	10
• Application Updates	1
• Forensics Questions	3
• Local Policy	6
• Malware	2
• Operating System Updates	1
• Prohibited Files	1
• Service Auditing	3
• Uncategorized Operating System Settings	4
• Unwanted Software	5
• User Auditing	7

## **Ubuntu 22**

• Account Policy	2
• Application Security	9
• Application Updates	2
• Defensive Countermeasures	1
• Forensics Questions	3
• Local Policy	5
• Malware	2
• Operating System Updates	2
• Prohibited Files	7
• Service Auditing	2
• Uncategorized Operating System Settings	3
• User Auditing	3

## **Fedora 36**

• Account Policy	2
• Application Security	11
• Application Updates	2
• Defensive Countermeasures	2
• Forensics Questions	4
• Local Policy	7
• Malware	3
• Operating System Updates	2
• Prohibited Files	2
• Service Auditing	2
• Uncategorized Operating System Settings	2
• Unwanted Software	3
• User Auditing	4



## **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.