*A structured preparation guide to help Windows team members think clearly, act confidently, and defend effectively under pressure.*

## ***1. Credential & Access Control Hygiene***

***Objective:*** *Validate that only authorized accounts exist and that privilege is properly scoped.*

* *Enumerate local accounts:  
   Get-LocalUser, net user*
* *Audit administrative groups:  
   net localgroup Administrators*
* *Identify excessive group memberships (e.g., RDP, Power Users)*
* *Check for enabled Guest or default accounts*
* *Examine recent account changes in logs (IDs 4720, 4722)*

***Ask yourself:*** *What accounts shouldn’t exist—and how would you find them without relying on your memory?*

## **2. Firewall & Port Visibility**

**Objective:** Ensure critical services are reachable—but only by those who should access them.

* List listening ports and owning processes:  
   netstat -ano, then tasklist /FI "PID eq <PID>"

Review firewall profiles and rules:  
Get-NetFirewallProfile

Get-NetFirewallRule | ? { $\_.Enabled -eq $true }

* Validate that ports like 389, 53, 80/443, 3389 are **limited to required source IPs**
* Disable or scope RDP and SMB to internal ranges if possible

**Mental Model:** Every port is a decision. If it’s open, you should know why—and to whom.

## **3. Event Log Familiarity**

**Objective:** Recognize key security-relevant system events, and build habits for regular review.

* Key Event IDs to remember:  
  + 4624 – Successful logon
  + 4625 – Failed logon
  + 4720 – New user created
  + 7045 – New service installed
  + 1102 – Audit log cleared
  + 4688 – New process created *(requires audit policy enabled)*

Efficient triage with PowerShell:  
  
 Get-WinEvent -LogName Security | Where-Object { $\_.Id -eq 4720 }

**Ask yourself:** Can you spot an attacker’s presence in the logs before the service is taken down?

## **4. Threat Hunting & Artifact Discovery**

**Objective:** Proactively search for signs of compromise or unauthorized persistence.

* Inspect persistence mechanisms:  
  + **Startup entries**: Autoruns, reg query HKLM\...\Run
  + **Scheduled tasks**: schtasks /query /fo LIST /v
  + **Unusual services**: Get-Service | Where { $\_.StartType -eq 'Auto' }
* Check known drop zones:  
  + C:\Windows\Temp
  + C:\Users\Public
  + %TEMP%

Review running processes for anomalies:  
  
   
Get-Process | Sort-Object CPU -Descending

## **5. Scripting & Automation Familiarity**

**Objective:** Use PowerShell confidently for diagnostics, auditing, and response.

* Useful scripting capabilities:  
  + Enumerate and disable non-admin users

Extract recent login failures:  
Get-EventLog -LogName Security -InstanceId 4625 -Newest 10

* + Audit firewall status and changes

List running services and their statuses:  
Get-Service | Sort-Object Status

**Goal:** You’re not just memorizing commands—you’re building muscle memory to ask and answer the right questions faster.

## **6. Incident Response Preparedness**

**Objective:** Detect, respond to, and document intrusions with clarity and accountability.

* Build timelines of attacker behavior:  
  + Who
  + What
  + When
  + Where
  + How

**Expectations:** Your IR writeups should prove situational awareness, technical accuracy, and root cause analysis—not just “we found a bad thing.”