*Use this to guide your preparation. Ask yourself how you would verify, defend, and monitor each of these.*

### **🧭 System Identification & Role Mapping**

* Can you identify the role of each Windows machine? (e.g., AD controller, DNS server, mail relay, web server)  
   → *Think: If you didn't label it, how would you prove what it does?*
* Do you understand which **services** must be up for scoring?  
   → *AD is worthless if DNS is broken. Know their dependencies.*

### **🔐 Account & Credential Hygiene**

* Do you know which accounts are present by default?  
   → *Can you detect and verify added/hidden users?*
* Are there default credentials anywhere on the system (services, IIS, SMB shares)?  
   → *Would you bet your scoring on that?*
* How do you validate that your team has full administrative control on Day 1?  
   → *Without assuming it's already true.*

### **🧱 Firewall & Network Awareness**

* Can you identify which ports must remain open for scoring?  
   → *Don't block RDP without knowing if it's needed for scoring or remote management.*
* Do you understand what the firewall is allowing inbound/outbound—**and why**?  
   → *Does DNS need to answer internal and external queries? Only from certain IPs?*
* Can you recognize unnecessary listening services or open ports?  
   → *What business need justifies this port being open?*

### **📄 Logging & Event Familiarity**

* Do you know the difference between “normal” and “anomalous” events in Windows logs?  
   → *What would a user creation or service installation look like?*
* Which Event IDs are worth knowing before competition day?  
   → Suggested: 4624, 4625, 4720, 7045, 1102
* Can you filter logs quickly to isolate critical changes?  
   → *Think: What filters will help you triage fast if something weird happens?*

### **🔍 Threat Detection & Artifact Hunting**

* Are you comfortable inspecting services, scheduled tasks, startup folders, and the registry for persistence?  
   → *How would a Red Team foothold look on this box?*
* Do you know where suspicious files are likely to show up?  
   → *Temp directories, Public folders, scripts in startup?*
* If you suspect compromise, how do you validate it **without guessing**?  
   → *Logs, process trees, network connections, file hashes...*

### **🛠 Tool Comfort & Mental Models**

* Can you confidently navigate Event Viewer, Services.msc, Task Scheduler, and Group Policy Editor?
* Are you comfortable using Process Explorer, TCPView, and Autoruns to investigate unknown behavior?
* Can you script basic PowerShell routines (e.g., to audit accounts, list recent logins, enumerate services)?  
   → *Tools should answer questions. Know which tool answers which question.*

### **🧾 Operational Discipline**

* Are you prepared to document every change you make to the system?  
   → *You’ll need this for injects, incident reports, and rollback.*
* If you find a breach, do you know how to write a clear incident report?  
   → *What happened, how you found it, what you did to stop it.*
* Can your team communicate what’s being hardened, what’s still vulnerable, and what’s in progress?  
   → *Team sync should drive defense, not chaos.*