**Forensic Approach – Credential Compromise (Not Ransomware)**

1. Isolate the server

* Connect an Ethernet cable directly from the laptop to the ESXi server.
* On the laptop, go to Network Settings > Ethernet Adapter, Set a manual IP address> IP: 10.0.0.10
* Open a web browser and go to:<https://10.0.0.3>
* Make sure it's not connected to any corporate network ,
* Plug in the Wireless USB Adapter , Install drivers if required and then connect to Hotspot for Internet
* Install Autopsy from USB on the DC and run it and analyze the results .
* Install Cisco CSE & Scan for Malware with Cisco EDR

1. **Look for suspicious activity based on the outcome of Autopsy**

* Run the [Domain Controller Compromise Assessment PS script](https://github.com/ec-sd-itsecops/ecpub/blob/main/Containment/Domain%20Controller%20Compromise%20chek.ps)

*Open Power Shell /CMD*

* netstat -ano
* netstat -ano | findstr ESTABLISHED
* net group "Domain Admins" /domain
* taskschd.msc
* Get-Process
* Get-Service | Where-Object { $\_.StartType -eq 'Auto' -and $\_.Status -eq 'Running' }
* Resource Monitor>Network
* Go to Programs and Features> Look for remote access tools like AnyDesk, TeamViewer,Ultra viewer etc.
* Start>Run> shell:startup
* Start>Run>%TEMP% folder for unknown scripts

Check For Unusual Persistence (Run without “”)

* Open Powershell > “reg query HKLM\Software\Microsoft\Windows\CurrentVersion\Run”
* Open Powershell > “reg query HKCU\Software\Microsoft\Windows\CurrentVersion\Run”

1. **Review logs collected from the site , and run it in Autopsy**

**Security Log:**  
 4624 – Successful logons  
 4625 – Failed logons

4648 – Logons with explicit credentials  
 4672 – Special privilege logons  
 4720 – New user account created  
 4722 – User account enabled  
 4728 – User added to privileged group  
 1102 – Audit logs cleared

Export Logs If Needed

* Create directory C:\Forensics
* Open PowerShell
* wevtutil epl Security "C:\Forensics\Security.evtx"
* wevtutil epl System "C:\Forensics\System.evtx"
* wevtutil epl Application "C:\Forensics\Application.evtx"

1. **Decide on risk & Make the Call: If the following are true, close the case:**
   * No Malware or C2 traffic
   * No unauthorized software’s installed
   * No unauthorized accounts
   * No persistence mechanisms
   * No suspicious logins post-reset
   * No lateral movement

**Next Steps for Strengthening Security Posture:**

* Integrate DNS with Cloudflare
* Integrate into Mimecast
* Harden Azure Entra Conditional Access Policies
* Apply geo-blocking rules to only allow logins from approved countries
* Block or restrict legacy authentication protocols and untrusted devices.
* Enforce MFA Using Authenticator App for All Employees