**🧯 Incident Response Management – Part 1**

**(What to do after you’ve been hacked)**

**🛠️ 1. Restoring from Backups**

* **Why?** Backups are clean copies of your data before the hack.
* **Goal:** Bring systems back to a safe state.
* ✅ Use only **verified**, **recent**, and **clean** backups.
* 🔁 Always test backups **before** restoring.

**🧼 2. Remove Malicious Software**

* Use antivirus, EDR tools, and manual inspection.
* Look for:
  + Malware
  + Backdoors
  + Rogue user accounts
* Delete or quarantine all suspicious files.

**🛡️ 3. Improve Defenses**

* Fix what allowed the hack.
* Examples:
  + Update firewall rules
  + Disable unused ports/services
  + Add MFA (Multi-Factor Auth)
  + Patch vulnerable software

**🔍 4. Vulnerability Analysis**

* Scan systems to find **weak points**.
* Use tools like:
  + Nessus
  + OpenVAS
  + Nmap
* Check:
  + Outdated software
  + Misconfigurations
  + Exposed services

**✅ 5. Recovering from Incident (Validation)**

* After cleanup and patching, **test everything**:
  + Does the system behave normally?
  + Any suspicious traffic left?
  + Any new user accounts or services?

✅ Think of it like checking the house before you move back in after a robbery.

**🏭 6. Restore Operations**

* Gradually bring systems and services back online.
* Monitor closely after restoration.
* Inform users and reset passwords.

**🔁 7. What If Hackers Come Back?**

* They often try! Why?
  + You didn’t fix the backdoor
  + They planted scheduled tasks/malware to return
* So:
  + Check logs regularly
  + Use **EDR/SIEM** tools
  + Monitor **new users**, **scripts**, **connections**

**📚 8. Lessons Learned (MOST IMPORTANT PART)**

Ask your team:

* What worked?
* What failed?
* Were alerts ignored?
* Did we follow the playbook?
* How can we do better next time?

💡 Every attack teaches you something. Don't waste the lesson.

**🌐 9. Monitor Ingress/Egress Traffic**

* **Ingress:** What’s coming *into* your network (e.g., downloads, emails)
* **Egress:** What’s going *out* (e.g., stolen data)

Use:

* IDS/IPS (like Snort)
* Firewalls
* SIEM (Security Info and Event Mgmt)

**🧠 10. Use DNS Data Effectively**

**Tools:**

* **Malware Domain List** (ethen.robins DNS blacklist)
* **Cisco Umbrella** or **Google SafeBrowsing**

Check:

* Suspicious domain names
* Beaconing behavior (repeating connections to weird domains)
* DNS tunneling

**🌐 11. Web Proxy Data**

Web proxies log:

* Which websites were visited
* By which users/devices
* When and how

Use this to:

* Track malware downloads
* Spot phishing sites
* Trace suspicious traffic

**📊 12. Incident Response Data Sources**

| **Data Source** | **What It Tells You** |
| --- | --- |
| 🔎 DNS Logs | Suspicious lookups |
| 📑 Proxy Logs | Websites visited |
| 📁 File Logs | What was opened/downloaded |
| 👥 Login Logs | Who logged in, when |
| 🛜 Network Logs | IPs, ports, protocols used |

**💻 13. Using WMIC to Pull Data (Windows)**

**WMIC = Windows Management Instrumentation Command**

Examples:

wmic process list brief

wmic startup get caption,command

wmic useraccount list

📌 Helps you gather data **quickly** from remote or infected systems.

**🖥️ 14. SCCM (System Center Configuration Manager)**

* Tool used by companies to:
  + Push updates
  + Monitor systems
  + Deploy software

During incident response:

* Use SCCM to **push security patches**
* Remove bad software remotely
* Track **which machines** are affected

**📝 Final Summary Table**

| **Task** | **Purpose** |
| --- | --- |
| 🔁 Restore from Backups | Return to clean system state |
| ❌ Remove Malware | Clean up infected systems |
| 🔐 Improve Defenses | Block future attacks |
| 🔍 Vulnerability Scan | Find weak points |
| ✅ Validate Recovery | Confirm cleanup success |
| 📈 Restore Ops | Gradually bring systems back |
| 🧠 Lessons Learned | Improve response next time |
| 📊 Monitor Traffic | Spot signs of future attacks |
| 🌐 Use DNS/Proxy Logs | Detect suspicious domains |
| 💻 WMIC & SCCM | Collect data + manage systems |