**📚 Key Frameworks for Incident Response (for Lab 3)**

**1. NIST SP 800-61r2 – Computer Security Incident Handling Guide**

* Published by **NIST (National Institute of Standards and Technology)**.
* **Core document** for structuring incident response.
* Defines the **4 major phases**:
  1. **Preparation** – Set up IR plans, tools, training.
  2. **Detection & Analysis** – Identify and confirm incidents.
  3. **Containment, Eradication, and Recovery** – Control and remove threats.
  4. **Post-Incident Activity** – Lessons learned, improvement planning.

*Example*: After detecting lateral movement, following NIST you would first **contain** the spread before attempting to **eradicate** malware.

**2. NIST SP 800-171 – Protecting Controlled Unclassified Information (CUI)**

* Focuses on **best practices** for protecting sensitive but unclassified data.
* Covers **access control, incident response, and audit/monitoring**.

*Example*: If the simulated incident involved sensitive business data exfiltration, NIST 800-171 controls would become critical.

**3. MITRE ATT&CK Framework**

* **MITRE Corporation**'s massive knowledge base of:
  + Adversary **Tactics** (goals) and
  + **Techniques** (methods).
* Helps defenders **map attacker behaviors** to known patterns.
* Used for:
  + Detection strategy
  + Threat hunting
  + Gap analysis

*Example*: If the attacker uses PowerShell abuse, you can map it to MITRE **T1059.001** and know exactly what artifacts/logs to hunt.

**4. NIST Cybersecurity Framework (NIST CSF)**

* Organizes cybersecurity work into **5 Functions**:
  + **Identify** (assets, risks)
  + **Protect** (implement controls)
  + **Detect** (monitor events)
  + **Respond** (incident handling)
  + **Recover** (restore capabilities)

*Example*: Your tabletop decisions about isolating infected hosts are part of the **Respond** function of NIST CSF.

**5. SANS Incident Response Process**

* **SANS Institute** simplified view of NIST IR flow:
  1. **Preparation**
  2. **Identification**
  3. **Containment**
  4. **Eradication**
  5. **Recovery**
  6. **Lessons Learned**
* Emphasizes the **cyclical nature** of incident response.

*Example*: Even after recovering systems, you must still do a full post-mortem according to SANS.

**6. ISO/IEC 27035 – Information Security Incident Management**

* **International Standard** for incident response.
* Focuses heavily on:
  + Formal **reporting**
  + **Communication channels** during incidents
  + **Coordination** across teams and departments

*Example*: Reporting the incident clearly to executives and legal teams fits into ISO/IEC 27035 compliance.

**Summary Table: Frameworks vs Their Strengths**

| **Framework / Standard** | **Main Focus** | **Why Important for the Game & Lab** |
| --- | --- | --- |
| NIST SP 800-61r2 | Incident Response Lifecycle | Core playbook for handling incidents |
| NIST SP 800-171 | Data Protection and Access Control | Relevant if sensitive data is targeted |
| MITRE ATT&CK | Adversary Techniques and Behaviors | Guides threat hunting and detection strategies |
| NIST Cybersecurity Framework | Broad Cyber Risk Management | Context for decision-making |
| SANS IR Process | Simplified Incident Handling Flow | Easy to remember sequence |
| ISO/IEC 27035 | Incident Management and Communication | Best practice for formal reporting and coordination |