**1. Incident Response Lifecycle Reference (Cheat Sheet)**

* Quick overview of **NIST SP 800-61** or **SANS IR Phases**
* Helps guide your decisions during the simulation
* Example format:
* 1. Preparation → 2. Detection & Analysis → 3. Containment →

4. Eradication → 5. Recovery → 6. Lessons Learned

**2. MITRE ATT&CK Mapping Table**

* A simplified table or chart showing common attacker tactics (e.g. phishing, PowerShell abuse) mapped to **MITRE techniques**
* Example:
  + Phishing → T1566
  + PowerShell Execution → T1059.001
* Helps justify your response choices and improves your simulation score

**3. Pre-Defined Toolkits / Commands Reference**

Make a list of:

* Key tools: e.g. Wireshark, Sysmon, Splunk, EDR
* Common investigative commands:
  + netstat -an
  + Get-ScheduledTask (PowerShell)
  + whoami /groups
  + SIEM search queries
* Useful for “Response Cards” to argue that you’re using a solid method = bonus on dice roll!

**4. Roles Cheat Sheet**

If your group has roles (e.g., SOC Analyst, IR Lead, Comms Officer), a quick breakdown helps:

* Who leads containment?
* Who takes notes?
* Who reports to upper management?

📌 Bonus: Use this to divide responsibility and avoid confusion during the timeboxed rounds.

**5. Observation/Notes Template**

Even if Moodle provides one, you may want:

* A **personal scratchpad** for quick notes
* Mark which phase you’re in
* Write what card was revealed, your team's response, and what you said/did

**6. List of Well-Known Response Procedures**

Prepare 4–5 responses you can confidently use and name-drop frameworks for:

* **Log Analysis** → Detects C2 activity, maps to MITRE T1071
* **User Behavior Review** → Useful for insider threats
* **Endpoint Triage** → SANS Phase 2/3, MITRE T1059
* **Network Isolation** → Containment, best practice per NIST
* **Restoring from Backup** → Recovery phase

This gets you the **+3 bonus on dice rolls**!

**7. Time Tracker / Phase Timer**

(Optional but helpful)

* Use your phone stopwatch or a simple timer app to **track how long you're spending on each phase**.
* It keeps your group focused — important since it’s **timeboxed**.

**8. Summary Slide or Diagram (for reporting)**

Post-exercise, having a simple diagram showing:

* Attack path (Initial compromise → Persistence → C2 → Lateral movement)
* Your detection/response points Makes your evaluation **visually strong** if submitting a Word doc or presenting findings.

**9. Mock Questions to Practice**

Prepare answers to questions like:

* “How did you detect the attacker’s movement?”
* “Why did you choose that response action?”
* “What gaps did you identify?”
* “What framework/procedure supported your action?”

**🚀 Optional (Advanced But Impressive)**

* **SIEM Playbook or SOC Dashboard Screenshot (mock)**  
  Even a simple flow diagram helps visualize your toolset and decision-making process.
* **A shared team document** (e.g., Google Doc or shared Excel if allowed) for collaborative notes.