Install Rekall on your OS  <http://www.rekall-forensic.com/>  and try to perform a memory analysis of your system, Don't worry as this lab will be covered later in more detail in the windows forensic course in sha Allah.

**🛡️ Affected Parties, Write Blockers, Short & Long Term IM Goals, and Rekall**

**1. 🧍 Affected Parties – Who Gets Impacted in a Cyber Incident?**

**🔍 Who Are "Affected Parties"?**

Any individual, system, team, or third-party **impacted by the incident**, including:

| **Affected Party** | **Examples** |
| --- | --- |
| 👤 **Users/Employees** | Lose access, data stolen |
| 🏢 **Organization** | Financial loss, downtime, brand damage |
| 🤝 **Customers/Clients** | Personal data breached |
| 🔗 **Vendors/Partners** | Their systems may be at risk too |
| ⚖️ **Regulators** | Must be informed (e.g. data protection agencies) |
| 📰 **Public/Media** | May be informed, especially if it’s a big breach |

📌 Understanding affected parties helps with **communication, legal compliance, and response coordination**.

**2. 🔒 What Are Write Blockers?**

**🧰 Definition:**

A **write blocker** is a **hardware or software tool** used in **digital forensics** to prevent any changes to a storage device (e.g., hard drive) while reading or copying its data.

**🧠 Why Use It?**

When collecting evidence after a cyberattack:

* You want to **read but not alter** the data
* Prevent **tampering**, even accidentally
* Ensure data is **legally admissible in court**

✅ It’s a must-have in forensic investigations to maintain **evidence integrity**.

**3. 🎯 Incident Management Goals (Short & Long Term)**

**📍 Short-Term Goals (During or Right After the Incident)**

| **Goal** | **Why It Matters** |
| --- | --- |
| 🔍 Identify the threat | Know what you’re dealing with |
| 🧯 Contain the damage | Stop the spread of attack |
| 🚫 Isolate affected systems | Prevent further infection |
| 📢 Communicate internally | Keep staff informed and organized |
| 📄 Preserve evidence | For investigation and legal use |

**🚀 Long-Term Goals (After Recovery)**

| **Goal** | **Why It Matters** |
| --- | --- |
| 🛠️ Patch weaknesses | Fix the issue that caused the breach |
| 📚 Update policies | Improve your playbooks, plans, training |
| 🧪 Train staff | Reduce human error and phishing risk |
| 📊 Report findings | For management, stakeholders, regulators |
| 🔁 Review and rehearse | Run simulations to prepare better next time |

📌 Together, short and long-term goals help **respond effectively and build stronger security** over time.

**4. 🧠 Rekall – Memory Forensics Tool**

**🔧 What is Rekall?**

* A **free open-source memory analysis tool** used in **incident response and digital forensics**.
* Can **analyze RAM dumps** to detect malware, rootkits, or suspicious behavior.

**📌 Use Cases:**

| **Use** | **Example** |
| --- | --- |
| 🔍 Detect Malware | Even if it runs only in memory (no files) |
| 🧠 Analyze Processes | What was running when the system was hacked? |
| 🛑 Catch Stealthy Attacks | Find hidden or injected code |
| 📂 Investigate Exploits | Look at what loaded into memory and when |

Rekall helps you “look inside the brain” of a compromised system.

**📝 Summary Table**

| **Topic** | **Description** |
| --- | --- |
| 🧍 Affected Parties | Anyone who suffers from the incident |
| 🔒 Write Blockers | Tools to read drives without modifying them (forensics) |
| 📍 Short-Term IM Goals | Immediate response: contain, preserve, inform |
| 🚀 Long-Term IM Goals | Learn, improve, secure, and train |
| 🧠 Rekall | Memory forensics tool to detect malware in RAM |