Mini Threat Model Security Project

1. Incident Response Plan

Detection:
The first step in responding to an incident is identifying it. For my project, one effective method is continuous log monitoring combined with intrusion detection systems (IDS). These tools flag suspicious behaviors, such as:

- Multiple failed login attempts within a short period.
- Unusual traffic spikes that could signal a Denial-of-Service attempt.
- Login attempts from unrecognized devices or locations.

This early detection ensures we can respond quickly before the threat escalates.

Containment:
Once suspicious activity is confirmed, the immediate priority is to limit the damage. Containment steps in our project would include:

- Temporarily disabling compromised accounts to prevent attackers from moving further.
- Disconnecting infected devices from the network to stop malware from spreading.
- Blocking malicious IP addresses at the firewall.

This “stop the bleeding” stage ensures the attack does not expand.

Eradication and Recovery:

- Eradication: We completely remove the root cause of the issue. This means deleting malware files, applying patches to vulnerable software, and resetting credentials that may have been stolen.
- Recovery: Once the system is clean, we restore functionality. This includes reloading clean data from backups, re-enabling accounts after verification, and closely monitoring the environment for any signs of reinfection.

Attack Type – Phishing (Example):
Phishing is when attackers impersonate trusted sources (e.g., fake login emails) to steal user credentials. In our mini threat model project, a phishing attempt could compromise user accounts. By detecting unusual login behavior, isolating compromised accounts, and forcing resets, we can block the attack path and protect users.

---

2. Comprehensive Security Policy

Key Security Rules/Guidelines:

1. Strong Authentication and MFA: All users must use complex passwords and two-factor authentication to reduce the risk of credential theft.
2. Access Control and Least Privilege: Users are given only the permissions they need. Admin rights are tightly restricted and reviewed regularly.
3. Data Encryption and Secure Transfer: Sensitive files and communications must always be encrypted, whether stored on disk or sent across the network.

Incident Response Steps (Policy Connection):
If a breach occurs, staff must follow the defined response steps: detection, containment, eradication, and recovery. These are clearly documented and practiced to minimize confusion during a real incident.

Maintaining the CIA Triad:

- Confidentiality: Password rules, MFA, and encryption prevent unauthorized access to sensitive user credentials.
- Integrity: Regular updates, patching, and verifying backup files ensure data cannot be maliciously altered without detection.
- Availability: Backup recovery procedures and incident response steps ensure users can still access their data and services quickly after a breach.

Application to Mini Threat Model:
These policies keep user credentials safe (confidentiality), ensure the data inside our system remains accurate and unchanged (integrity), and guarantee that even if something goes wrong, our service is restored promptly (availability).

---

3. Encryption & Hashing Demonstration

AES Encryption:

- Plaintext (before encryption): `User credentials must be protected.`
- Encrypted (AES ciphertext): Appears as random unreadable data, e.g. `b'\xa7\xcdn\x9d…'`.
- Decrypted (after AES): `User credentials must be protected.`

SHA-256 Hashing:

- Hashed Value: `d3d2f94927ffde7d3…` (fixed-length hash output).

How This Applies to Our Threat Model:

- AES Encryption: Protects sensitive files or data being transmitted so that even if attackers intercept it, they cannot read the contents.
- SHA-256 Hashing: Passwords in our system are stored as hashes, not plaintext. Even if an attacker steals the database, they won't immediately have access to the actual passwords.

---

4. Legal and Ethical Compliance

Relevant Laws/Regulations:

- HIPAA: Requires organizations handling health-related data to secure and report breaches. If our project stored healthcare records, this would directly apply.
- GDPR: Governs how personal data of EU citizens is collected, processed, and protected. Requires breach notifications within strict timelines.

Ethical Considerations:
Beyond the law, we have an ethical duty to protect users' data, respect their privacy, and be transparent about any breach. Even if the law does not apply, ethically we must not hide incidents from users who may be impacted.

How Our Plan Upholds Compliance:

- Detection & Reporting: Quick identification of breaches ensures compliance with laws requiring timely notification.
- Encryption & Hashing: Meets legal standards for data protection (e.g., GDPR requires "appropriate technical measures").
- Policies: Access control and authentication align with both legal requirements and ethical responsibility to minimize unnecessary exposure of user data.

Application to Mini Threat Model:
If our project stores user credentials, applying HIPAA/GDPR-level standards shows that we are treating data as if it's legally protected. This not only keeps us compliant but also builds trust with users, which is ethically important.

Final Wrap-Up

This mini threat model project demonstrates:

- A clear incident response plan (detect, contain, eradicate, recover).

- A comprehensive security policy with rules tied to the CIA triad.
- Real use of encryption and hashing to protect user credentials.
- Strong awareness of legal and ethical compliance to guide our practices.

Together, these show a complete approach to cybersecurity: protecting user data, ensuring system reliability, and upholding both professional and legal standards.