# Cyber Security Internship Report

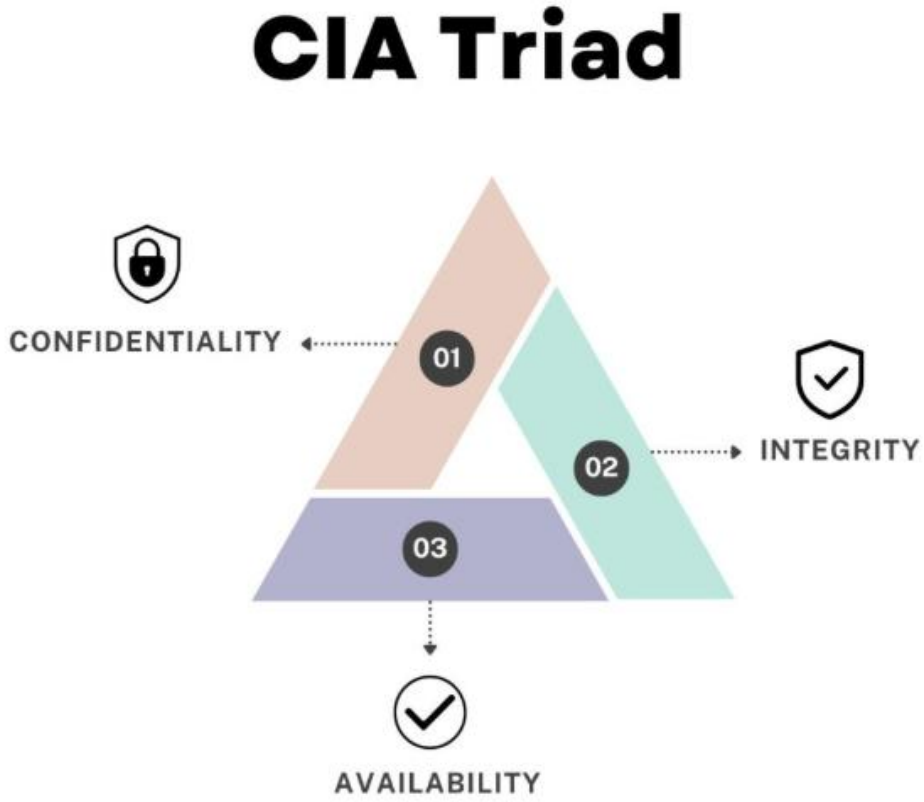
## Cyber Security Internship – Task 1

## Cyber Security Basics & Attack Surface Analysis

**Submitted by: Hetal Antala**

**Date : 15 / 01 / 2026**

1) CIA Triad :




⇒ The CIA Triad is a foundational cybersecurity model defining three core principles for information security:

1.Confidentiality (keeping data private from unauthorized access)

2. Integrity (ensuring data is accurate and unaltered), 3. Availability (ensuring timely access for authorized users)

## Confidentiality :

Confidentiality ensures that sensitive data is accessible only to authorized individuals or systems. Its purpose is to prevent unauthorized viewing, access, or misuse of private information.

### Examples

In banking, confidentiality prevents unauthorized access to account details via encryption and multi-factor authentication; the 2017 Equifax breach exposed 147 million users' sensitive data, enabling identity theft. On social media like Facebook, it protects private messages and profiles from phishing or data leaks, as seen in the 2018 Cambridge Analytica scandal where harvested user data influenced elections without consent.

## Integrity :

Integrity ensures that data remains accurate, authentic, and unaltered during storage or transmission. Any unauthorized modification or corruption compromises the reliability of data.

### Examples

Banking relies on integrity for unaltered transaction records, using checksums and digital signatures; a manipulated SWIFT message in the 2016 Bangladesh Bank heist transferred $81 million due to compromised integrity controls. Social media platforms like Twitter (now X) maintain post authenticity via hashing to detect tampering, preventing fake news spread as in coordinated disinformation campaigns during elections.

## Availability :

Availability ensures that systems, networks, and data are accessible to authorized users whenever needed. Disruptions can halt operations and cause major losses.

### Examples

Banks ensure 24/7 ATM and app access through redundant servers and DDoS protection; the 2020 Twitter outage from a DDoS attack halted services for hours, mirroring banking disruptions like the 2016 Dyn attack affecting financial sites. Social media uptime supports real-time sharing, with Instagram using load balancers to counter high-traffic spikes or attacks that could block user access during viral events.

## 2) Types of Cyber Attackers :

Script Kiddies

**Chief Goal:** Attack, vandalize, and inflict as much damage as possible.

**Typical Targets:** Easy-to-penetrate systems and networks, which are vulnerable to widely-known threats.

**Mitigation Tactics**: While script kiddies may lack advanced skills, they often succeed by exploiting basic security gaps:

- **Disable unused ports and services:** Minimize your attack surface by closing common entry points often targeted by automated tools.

- **Use security configurations and hardening guides:** Apply best practices for system setup to block default vulnerabilities.

- **Implement basic intrusion detection systems (IDS):** Detect and alert on known attack signatures these threat actor types tend to reuse.

- **Keep antivirus and firewalls active and updated:** Foundational defenses still matter—especially against low-effort attacks.

- **Enforce secure password policies:** Weak or reused credentials are easy wins for script-based attacks.

- **Stay current with patching:** Even amateur actors can exploit unpatched software using freely available exploits.

Insiders :

**Chief Goal:** Work from within an organization to get around its cybersecurity framework.

**Typical Targets:** Not limited to any specific type of organization.

**Mitigation Tactics**: Since insider threats operate from within the organization, detection and prevention require a mix of technology and trust management:

- **Implement user behavior analytics (UBA):** Track deviations from normal activity patterns to flag potential misuse of access.
- **Apply the principle of least privilege (PoLP):** Limit access to only what each role requires—nothing more.

- **Rotate credentials and disable dormant accounts:** Prevent former employees or unused accounts from becoming entry points.

- **Conduct regular audits and access reviews:** Routinely verify that current access levels align with job responsibilities.

- **Foster a culture of accountability:** Encourage reporting of suspicious behavior and provide clear policies on data handling.

- **Use data loss prevention (DLP) tools:** Monitor for unauthorized data transfers, downloads, or external email activity.

Hacktivists :

**Chief Goal:** Exposing secrets and disrupting organizations that are perceived as evil.

**Typical Targets:** Not limited to any specific type of organization or business.

**Mitigation Tactics:** Because hacktivists are driven by ideology rather than profit, their attacks are often public, disruptive, and aimed at damaging reputation:

- **Monitor digital presence**: Stay alert to chatter on forums, social platforms, and dark web channels where hacktivist activity may be planned.
- **Strengthen perimeter defenses**: Harden firewalls, secure APIs, and implement web application firewalls (WAFs) to block common exploit attempts.

- **Prepare a crisis communications plan**: A swift, coordinated public response can minimize reputational damage in the event of a breach.

- **Audit for weak points in public-facing systems**: These types of threat actors often target websites, customer portals, or email servers—make them harder to exploit.

- **Avoid unnecessary exposure**: Review content and messaging to reduce the chance of becoming a perceived adversary or target.

- **Conduct tabletop exercises**: Test incident response plans for politically or socially motivated attacks to strengthen organizational readiness.

Nation-State Actors :

**Chief Goal:** Espionage, theft, or other disruptive activity that furthers the interests of a particular nation/group of nations.

**Typical Targets:** Businesses and government-run organizations.

**Mitigation Tactics**: Defending against state-sponsored threat actors requires heightened vigilance and advanced security measures:

- **Adopt a zero-trust architecture:** Assume no implicit trust—validate every user, device, and connection inside and outside your network.

- **Implement threat intelligence feeds:** Stay ahead of known nation-state tactics by integrating up-to-date indicators of compromise (IOCs).

- **Conduct regular red team exercises:** Simulate advanced persistent threats to test and strengthen your detection and response capabilities.

- **Encrypt sensitive communications and data:** Limit the usefulness of any stolen information through strong encryption protocols.

- **Apply strict vulnerability management:** These types of threat actors often exploit zero-day or unpatched vulnerabilities—close gaps quickly.

- **Strengthen supply chain security:** Vet third-party vendors and monitor their security posture, as indirect entry points are common in state-sponsored campaigns.

## 3) Attack Surfaces :

### Web Applications

Web applications are accessible through browsers and are exposed to the internet.

**Common Attack Surfaces:**

- Login and registration pages
- Input forms (search, feedback, payment forms)
- File upload features
- URLs and parameters
- Cookies and session IDs

**Possible Attacks:**

- SQL Injection
- Cross-Site Scripting (XSS)
- Cross-Site Request Forgery (CSRF)
- Brute force attacks

## Mobile Applications

Mobile apps communicate with backend servers over the internet.

**Common Attack Surfaces:**

- Insecure API endpoints
- Local storage (saved passwords, tokens)
- App permissions
- Insecure communication (no encryption)

**Possible Attacks:**

- Reverse engineering
- API abuse
- Data leakage
- Man-in-the-Middle (MITM) attacks

## APIs (Application Programming Interfaces)

APIs allow applications to communicate with servers and other services.

**Common Attack Surfaces:**

- Unauthenticated or poorly secured APIs
- Excessive data exposure
- Improper access control
- Hard-coded API keys

**Possible Attacks:**

- API injection attacks
- Broken authentication
- Data scraping
- Unauthorized data access

## Network Infrastructure

Networks connect systems, servers, and devices.

**Common Attack Surfaces:**

- Open ports
- Weak firewall rules
- Unsecured Wi-Fi networks
- Routers and switches

**Possible Attacks:**

- Network sniffing
- Man-in-the-Middle attacks
- Denial of Service (DoS)
- Unauthorized network access

## Cloud Infrastructure

Cloud services host applications, databases, and storage.

**Common Attack Surfaces:**

- Misconfigured cloud storage (public buckets)
- Weak IAM policies
- Exposed admin consoles
- Insecure virtual machines

**Possible Attacks:**

- Data breaches
- Privilege escalation
- Account hijacking
- Service disruption

## 🔹 Mapping Daily-Used Applications to Attack Surfaces

### 📧 Email Applications (Gmail, Outlook)

**Attack Surfaces:**

- Login page
- Email attachments
- Links inside emails
- Backend mail servers

**Possible Attacks:**

- Phishing attacks
- Credential theft
- Malware through attachments
- Account takeover

## 💬 WhatsApp / Messaging Apps

**Attack Surfaces:**

- Mobile application
- APIs used for messaging
- Media file sharing
- Cloud backups

**Possible Attacks:**

- Malicious file sharing
- Account hijacking via OTP attacks
- Data leakage from backups
- MITM attacks on insecure networks

## 🏦 Banking Applications  Attack Surfaces:

- Mobile app login screen
- APIs for transactions
- Backend servers
- Network communication

**Possible Attacks:**

- Credential theft
- Session hijacking
- API abuse
- Fraudulent transactions