Exam Cram Notes: Threats, Vulnerabilities, and Mitigations – Threat Actors and Motivations

1. Types of Threat Actors

Threat actors are individuals or groups who exploit vulnerabilities for malicious purposes. Understanding who they are helps in determining appropriate defense strategies.

1. **Hackers**
    - **Motivation:** Intellectual challenge, curiosity, or gaining notoriety.
    - **Types:**
        - **White Hat Hackers:** Ethical hackers who help improve security (e.g., penetration testing).
        - **Black Hat Hackers:** Malicious hackers who exploit vulnerabilities for personal gain or damage.
        - **Gray Hat Hackers:** A mix of white and black hat; they may exploit vulnerabilities but disclose them later.
2. **Criminal Organizations**
    - **Motivation:** Financial gain through activities like **ransomware**, **fraud**, and **identity theft**.
    - **Methods:** Organized, sophisticated, and well-funded.
    - **Example:** Ransomware attacks, DDoS extortion attacks, and phishing campaigns targeting individuals or organizations.
3. **Nation-State Actors**
    - **Motivation:** Espionage, political influence, or disruption of another country's infrastructure.
    - **Methods:** Cyberwarfare, espionage, and politically motivated cyber attacks.
    - **Example:** Stuxnet (a cyber attack on Iran's nuclear facilities) or attacks on government websites.
4. **Insiders**
    - **Motivation:** Personal grievances, financial gain, espionage, or accidental negligence.
    - **Types:**
        - **Malicious Insiders:** Employees or contractors intentionally harming the organization.
        - **Negligent Insiders:** Employees who unintentionally expose sensitive information.
    - **Example:** A disgruntled employee leaking sensitive company data to competitors or hackers.
5. **Hacktivists**
    - **Motivation:** Political or social causes, disrupting organizations they see as unethical or unjust.
    - **Methods:** DDoS attacks, website defacements, or data breaches.
    - **Example:** Attacks on government websites or corporations involved in controversial issues (e.g., environmental issues).
6. **Script Kiddies**
    - **Motivation:** Gaining status or experience, not necessarily for financial gain.

    - **Methods:** Use pre-written scripts or tools to exploit vulnerabilities.
    - **Example:** Attacks targeting known vulnerabilities without understanding the underlying technology.
7. **Terrorists**
    - **Motivation:** Causing fear, disruption, and damage to critical infrastructure.
    - **Methods:** Cyber attacks against infrastructure, public services, or government systems to create chaos.
    - **Example:** Attacks on power grids or financial systems to create widespread disruption.

---

2. Threat Actor Motivations

Understanding the motivations behind attacks helps design more targeted defenses:

1. **Financial Gain**
    - **Common Tactics:** Phishing, ransomware, data theft, credit card fraud.
    - **Examples:** Ransomware targeting hospitals for payments, financial data breaches.
2. **Espionage/Intelligence Gathering**
    - **Common Tactics:** Malware, social engineering, spear phishing.
    - **Examples:** Nation-state actors stealing military or corporate secrets.
3. **Political or Ideological Causes**
    - **Common Tactics:** DDoS attacks, website defacement, leaking sensitive information.
    - **Examples:** Hacktivists attacking government websites to protest policies.
4. **Revenge or Personal Grudge**
    - **Common Tactics:** Sabotage, data leaks, insider threats.
    - **Examples:** Disgruntled employees sabotaging their company’s IT infrastructure or leaking data.
5. **Recognition and Fame**
    - **Common Tactics:** Hacking for public attention, exploiting new vulnerabilities.
    - **Examples:** Hackers who want to prove their skills or make a name for themselves in the hacking community.
6. **Destruction or Disruption**
    - **Common Tactics:** Denial-of-Service (DoS) attacks, spreading viruses, defacing websites.
    - **Examples:** Terrorist groups attempting to destroy critical infrastructure or public services.

---

3. Threat Actor Tactics, Techniques, and Procedures (TTPs)

Understanding TTPs helps in detecting and mitigating attacks:

- **Tactics**: The goals of the attack (e.g., data theft, disruption).

- **Techniques**: Methods used to achieve the goal (e.g., exploiting a vulnerability, social engineering).
- **Procedures**: Standardized methods and practices used by the threat actor.

Key Exam Tips

✅ Understand **who threat actors are** and **their motivations** to choose appropriate defensive strategies.

✅ Be prepared for **scenario-based questions** that require identifying the type of threat actor based on behavior or attack patterns.

✅ Know how to differentiate between **insider threats** (malicious vs. negligent) and **external actors**.

✅ Recognize **TTPs** and how they help in identifying and mitigating specific threats.