TRAINING DAY 5 REPORT

Understand advantages, limitations of cyber security and cyber defense and vulnerability research

Today, I learned some important concepts

- ## Advantages of Cyber Security

1. Protection Against Cyber Threats

- Safeguards systems from viruses, malware, ransom ware, phishing, and other cyber attacks.
- Prevents unauthorized access to sensitive data.

2. Business Continuity

- Minimizes downtime from cyber incidents.
- Ensures operations run smoothly without major disruptions.

3. Data Protection

- Secures personal, financial, and confidential business data.
- Helps comply with data privacy laws like GDPR, HIPAA, or CCPA.

4. Cost Savings

- Reduces financial losses from data breaches and recovery costs.
- Avoids legal penalties due to non-compliance or data leaks.

5. Improved Risk Management

- Identifies vulnerabilities early through audits and monitoring.
- Enables proactive responses to potential threats.

6. Employee and User Safety

- Protects staff and users from identity theft, fraud, and scams.
- Encourages safe digital behavior through cyber security awareness.

- # Limitations of Cyber Security

1. Human Error

- People are often the weakest link (e.g., falling for phishing emails or using weak passwords).
- Even with strong systems, one mistake can cause a breach.

2. High Cost

- Implementing strong cyber security measures can be expensive.
- Small businesses may struggle to afford advanced tools and professional support.

3. Constantly Evolving Threats

- Cyber threats evolve rapidly (e.g., new viruses, AI-driven attacks).
- Security systems must be updated frequently, which can be challenging.

4. Skill Shortages

- There is a global shortage of skilled cyber security professionals.
- Many organizations can't find or afford qualified experts.

5. Complexity of Integration

- Implementing cyber security into legacy systems or across complex networks can be difficult.
- Poor integration can leave gaps in protection.

- # Cyber Defense

  Cyber defense refers to the strategies, technologies, and practices used to protect digital systems**,** networks, and data from cyber attacks. It focuses on preventing**,** detecting**,** responding to, and recovering from threats.

- **Key Goals of Cyber Defense**

1. **Prevent Attacks** – Stop threats before they cause harm.

2. **Detect Intrusions** – Identify attacks in real time.
3. **Respond Quickly** – Limit damage through rapid action.
4. **Recover Systems** – Restore data and services after an incident.

- ## Skills of an Ethical Hacker

1. Knows the art of Googling!!

2. At least one professional certification(OSCP, CEH, Sec+)

3. Strong cryptography skills

4. Strong Social Engineering skills

5. Patience and out-of-the-box thinking

6. Always updated and optimistic

- ## Information Security Policies

1. Rules and regulations issued by an organization to ensure CIA of it's IT infrastructure

2. Objectives: Security of digital assets comply with the rules and guidelines

3. Scope: Varies, sometimes hierarchical

4. Implementation: Workers sign an agreement and apply the necessary changes

5. Trainings and evaluations may be organized

6. If database needs to be encrypted, every person responsible should be made aware and make changes accordingly.

7. People are the weakest part of defense!

8. Streamlined with company's primary goals and strategies

9. Only applicable within an organizations boundaries of authority

- # Vulnerability Research

  Vulnerability research is the process of discovering, analyzing, and documenting weaknesses in software, hardware, or systems that can be exploited by attackers. It plays a crucial role in improving security by identifying flaws before they are exploited.