FUNDAMETALS OF CYBERSECURITY

BY - MANAS PANCHWAGH

Index

- Social Engineering Principles

10. Data Loss Prevention (DLP)
    - Objective and Examples
11. Security Domains (CISSP)
    - Security and Risk Management
    - Asset Security
    - Security Architecture and Engineering
    - Communication and Network Security
    - Identity and Access Management (IAM)
    - Security Assessment and Testing
    - Security Operations
    - Software Development Security
12. Attack Types
    - Password Attacks
      - Brute Force
      - Rainbow Table
    - Social Engineering Attack
      - Phishing
      - Smishing
      - Vishing
      - Spear Phishing
      - Whaling
      - Social Media Phishing
      - Business Email Compromise (BEC)
      - Watering Hole Attack
      - USB Baiting
      - Physical Social Engineering
    - Physical Attacks
      - Malicious USB Cable
      - Malicious Flash Drive
      - Card Cloning/Skimming
    - Adversarial Artificial Intelligence
    - Supply Chain Attacks
    - Cryptographic Attacks
      - Birthday Attack
      - Collision Attack

- Downgrade Attack

13. Attackers and Threat Actors

- Threat Actor
- Advanced Persistent Threat (APT)
- Insider Threats
- Hacktivists
- Hackers
  - Authorized Hackers (Ethical Hackers)
  - Semi-authorized Hackers (Researchers)
  - Unauthorized Hackers (Unethical Hackers)

14. Security Frameworks

- Overview and Purpose
- Key Components of a Security Framework
  - Security Controls
  - CIA Triad
  - NIST Cybersecurity Framework (CSF)
  - FERL-NERC

15. Security Standards and Regulations

- FedRAMP (Federal Risk and Authorization Management Program)
- Center for Internet Security (CIS)
- General Data Protection Regulation (GDPR)
- Payment Card Industry Data Security Standard (PCI DSS)
- HIPAA (Health Insurance Portability and Accountability Act)
- SOC Type 1 and SOC Type 2

16. Security Ethics

- Ethical Principles in Security
- Guidelines for Security Professionals
- HIPAA as an Example

17. Security Tools and Concepts

- Logs
- SIEM (Security Information and Event Management) Tools
- Playbooks
- Network Protocol Analyzers
- Programming for Automation
- Web Vulnerabilities
- Antivirus Software
- Intrusion Detection Systems (IDS)
- Encryption
- Plaintext
- Ciphertext

18. Penetration Testing

- Definition and Purpose
- Process

Benefits of Cybersecurity

1. Protection Against Threats
Internal threats & External threats

2. Regulatory Compliance - Ensures adherence to industry standards and regulations

3. Business Improvement - Enhances overall business operations and trust

4. Expense Reduction - Lowers costs associated with security breaches and threats

5. Board/Technical Support- Maintains confidence and backing from the board and technical teams

Role of a Security Analyst

- Monitoring & Protection: Responsible for safeguarding the network. Analyzes internal security issues.

- Operations & Projects:
Operations focus: Detection of threats and vulnerabilities.
Projects focus: Building and implementing security solutions

- Compliance and Framework:
Compliance: Adherence to both internal and external regulations. Ensures that security measures align with regulatory standards
Framework: Guidelines for developing security plans. Implement controls to minimize and manage risks

Transferable and Technical Skills

1. Communication: Effective use of language in a cybersecurity context.
2. Collaboration: Working with teams to address security challenges.
3. Analysis: Evaluating security data and identifying risks.
4. Problem Solving: Addressing and mitigating security issues.
5. SIEM Tools: Use of Security Information and Event Management (SIEM) tools.
Critical during security audits and for intrusion detection

Data Privacy

1. PII (Personally Identifiable Information)
2. SPII (Sensitive Personally Identifiable Information)

Early Attacks

1. Computer Virus: A malicious code designed to interfere with computer operations.
Primary goal: Cause damage to the system.

2. Malware: Malware spreads through the Internet and is software designed to harm devices and networks.

   Notable Examples:
   1. Brain Virus: Created by the Alvi brothers. One of the first computer viruses
   2. Morris Worm: Created by Robert Morris Known for being one of the first worms to spread widely on the Internet.

   Effects of Malware:
   Infection: Infects computers and any disk inserted into the infected computer. Spreads to other computers through the infected disks.

   Operational Impact: Attempts to assess the size of the Internet. Reinstalls itself and can lose track of operations, leading to memory overflow and eventual computer crashes.

Response to Early Attacks

CERTs (Computer Emergency Response Teams):
Introduced as a response to increasing cybersecurity threats.
Role: Manage and respond to computer security incidents and threats.

Digital Attacks

1. Love Letter (Conel de Cruzmann)

- Description: A malware disguised as a love letter email. It spread through email systems, exploiting human curiosity and trust.

- Historical Example: The Love Letter worm, also known as the "ILOVEYOU" virus, was one of the first instances of widespread social engineering attacks via email.

2. Equifax Breach

- Description: A major data breach that exposed the personal information of millions of people.

- Impact: Sensitive data was collected and potentially used for identity theft.

Social Engineering

Definition: A manipulation technique that exploits human error to gain private information or access.

Example:
Love Letter: Sending a malware disguised as a love letter email.

Phishing

Definition: The use of digital communication to trick individuals into revealing sensitive data or deploying malicious software.

Types:

1. Business Email Compromise (BEC): Targets businesses by sending emails that appear to be from a trusted source.
2. Spear Phishing: Targets specific individuals with emails that appear to originate from a trusted source.
3. Whaling: A form of spear phishing that targets high-profile individuals, such as executives.
4. Vishing: Exploitation of electronic voice communication to deceive individuals.
5. Smishing: Phishing through SMS text messages.

Malware

- Definition: Malware spreads through the Internet and is software designed to harm devices and networks.

- Types:

1. Worms: Malware that duplicates itself and spreads across systems, often without user interaction.
2. Viruses: Requires user action to initiate, but can spread to other systems.
3. Ransomware: Encrypts an organization's data and demands payment for decryption.
4. Spyware: Collects and sells information without the user's consent.

Social Engineering

Types of Social Engineering Attacks:

1. Social Media Phishing
   Description: Deceptive tactics used on social media platforms to trick users into revealing personal information or clicking malicious links.

2. Watering Hole Attack
   Description: An attack where hackers target a specific group of users by infecting websites that they frequently visit.
   Example: Placing malware on a popular website frequented by a particular community.

3. Baiting
   Description: Enticing a victim to engage with something enticing, such as a free download or USB drive, which then installs malware.

4. Physical Social Engineering
   Description: Exploiting physical access to steal data or install malicious software, such as leaving a compromised USB stick in a public place.

Social Engineering Principles:

1. Authority: Exploiting a person's tendency to obey authority figures.

2. Intimidation: Using fear or threats to coerce someone into providing information or access.

3. Consensus/Social Proof:
   Leveraging the tendency of people to follow the actions of a larger group.

4. Scarcity: Creating a sense of urgency by making something seem rare or limited.

5. Familiarity: Building trust by pretending to be someone known or familiar.

6. Trust: Exploiting a pre-existing relationship or creating a false sense of security.

7. Urgency: Pressuring someone to act quickly, without thinking through the consequences.

Data Loss Prevention (DLP)

Objective: Preventing data breaches by protecting sensitive data from being accessed, leaked, or stolen.
Example: Implementing strict access controls and monitoring to prevent unauthorized access.

Security Domains (As per CISSP)

1. Security and Risk Management
   Role: Overseeing security policies, procedures, and controls to manage and mitigate risks.
   Key Components: Asset management, risk assessment, and compliance.

2. Asset Security
   Role: Protecting data and information assets through proper classification and handling.
   Focus: Ensuring data integrity, confidentiality, and availability.

3. Security Architecture and Engineering
   Role: Designing and maintaining secure infrastructure and systems.
   Focus: Implementing robust security measures in the architecture of IT systems.

4. Communication and Network Security
   Role: Securing networks and communication channels from unauthorized access and threats.
   Focus: Ensuring secure data transmission and network integrity.

5. Identity and Access Management (IAM)
   Role: Controlling and validating

access to systems and data.
Focus: Managing user identities, authentication, and authorization processes.

6. Security Assessment and Testing
   Role: Regularly evaluating the effectiveness of security measures through audits and testing.
   Focus: Identifying vulnerabilities and ensuring compliance with security policies.

7. Security Operations
   Role: Monitoring and managing security incidents and ensuring the ongoing protection of systems.
   Focus: Implementing incident response strategies and maintaining operational security.

8. Software Development Security
   Role: Ensuring that software development practices incorporate security measures.
   Focus: Secure coding practices, vulnerability management, and testing for security flaws.

Attack Types

1. Password Attacks

   Description: Attempts to access password-secured devices, systems, networks, or data.

   Techniques:

   Brute Force: Repeatedly trying different combinations of passwords until the correct one is found.

   Rainbow Table: Using a precomputed table of hash values to reverse-engineer passwords.

2. Social Engineering Attack

   Domain: Security and Risk Management

   Description: Exploiting human error to gain unauthorized access or information.
   Examples:
   Phishing: Sending fraudulent emails to trick users into revealing sensitive information.

   Smishing: Phishing attacks conducted via SMS.

   Vishing: Voice phishing, where attackers use phone calls to extract information.

   Spear Phishing: Targeting specific individuals with personalized phishing attacks.

   Whaling: Spear phishing attacks targeting high-profile individuals like executives.

   Social Media Phishing: Using social media platforms to deceive users into revealing personal information.

   Business Email Compromise (BEC): Targeting businesses through emails that appear to be from trusted sources.

   Watering Hole Attack: Infecting websites frequently visited by a specific group to compromise their systems.

   USB Baiting: Leaving infected USB drives in public places, hoping someone will pick them up and use them.

   Physical Social Engineering: Exploiting physical access to gather information or install malicious software.

3. Physical Attacks

   Domain: Asset Security

   Examples:
   Malicious USB Cable: Cables that look normal but are designed to steal data or install malware.

4. Malicious Flash Drive: Infected USB drives that can compromise a system when plugged in.

   Card Cloning/Skimming: Duplicating payment cards by capturing their data using skimming devices.

5. Adversarial Artificial Intelligence

   Description: Manipulating AI and machine learning models to conduct attacks more efficiently.

   Impact: Can be used to bypass security measures, spread misinformation, or conduct cyber-attacks at scale.

6. Supply Chain Attacks

   Description: Targeting vulnerabilities within the supply chain to deploy malware or other malicious activities.

   Impact: Often costly and can affect various domains, as attackers exploit the interconnectedness of modern supply chains.

7. Cryptographic Attacks
   Domain: Communication and Network Security

   Description: Targeting secure forms of communication between a sender and recipient.

   Examples:
   Birthday Attack: Exploiting the mathematics of hash functions to find two different inputs that produce the same hash output.

   Collision Attack: Finding two different inputs that result in the same hash, thereby compromising the security of the hash function.

   Downgrade Attack: Forcing a communication channel to use a less secure version of a protocol, making it easier to compromise.

Attackers and Threat Actors

1. Threat Actor

   Definition: An individual or group that poses a security risk by attempting to compromise systems, networks, or data.

2. Advanced Persistent Threat (APT)

   Description: Highly skilled attackers who infiltrate networks without authorization, often remaining undetected for extended periods.

   Target: Large companies, government entities, critical infrastructure.

   Motives:
   Damaging critical infrastructure.
   Accessing and stealing intellectual property.
   Espionage and surveillance.

3. Insider Threats

   Description: Threats that originate from within an organization, often by employees, contractors, or trusted partners.

   Types:

   Sabotage: Deliberate damage or disruption to systems, data, or operations.

   Corruption: Unethical behavior leading to the misuse or compromise of data.

   Espionage: Unauthorized access to confidential information for the purpose of sharing it with external parties.

   Unauthorized Data Access/Leaks: Accessing or leaking sensitive information without permission.

4. Hacktivists

   Description: Individuals or groups driven by political or social

agendas who use hacking to further their cause.

Motives:

Demonstration: Protesting against organizations or governments.

Propaganda: Spreading their message to gain support.

Social Change Campaign: Advocating for specific social or political changes.

Fame: Seeking recognition or notoriety.

5. Hackers

   Description: Individuals who use computers to gain unauthorized access to systems, networks, or data.

   Types:

   Authorized Hackers (Ethical Hackers): Professionals who are permitted to test systems for vulnerabilities to improve security.

   Semi-authorized: Hackers (Researchers): Individuals who explore systems to find vulnerabilities, often for research purposes, but without explicit permission.

   Unauthorized Hackers (Unethical Hackers): Individuals who break into systems without permission for malicious purposes.

Security Frameworks

Overview

Security frameworks are structured guidelines used to build and implement plans that help mitigate risks and threats to data privacy.

Their purpose includes:

- Protecting Personally Identifiable Information (PII)
- Securing Financial Information
- Identifying Security Weaknesses
- Managing Organizational Risks
- Aligning Security with Business Goals

Key Components of a Security Framework

1. Security Controls

   Definition: Safeguards or countermeasures designed to reduce specific security risks.

   Examples: Firewalls, encryption, access controls, and intrusion detection systems.

2. CIA Triad

   Description: A foundational model in information security that helps organizations consider risk when setting up systems and security policies.
   It consists of three key components:

   Confidentiality: Ensuring that information is accessible only to those authorized to access it.

   Integrity: Ensuring that information is accurate and cannot be altered by unauthorized individuals.

   Availability: Ensuring that information and resources are available to those who need them when they need them.

3. NIST Cybersecurity Framework (CSF)

   Description: A voluntary framework consisting of standards, guidelines, and best practices to manage cybersecurity risks. It is widely used by organizations to strengthen their security posture.

   Purpose: Helps organizations identify, protect, detect, respond to, and recover from cybersecurity threats.

4. FERL-NERC

Definition: Refers to the Federal Energy Regulatory Commission (FERC)*and the North American Electric Reliability Corporation (NERC).

Purpose: These organizations establish standards and guidelines for the reliability and security of the electric grid in North America.

Relevance: Particularly important for entities involved in the energy sector, where securing critical infrastructure is paramount.

Security Standards and Regulations

1. FedRAMP (Federal Risk and Authorization Management Program)

   Description: A U.S. government program that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services.

2. Center for Internet Security (CIS)

   Description: A non-profit organization that provides best practices for securing IT systems and data against cyber threats. The CIS Controls and Benchmarks are widely used to improve cybersecurity measures.

3. General Data Protection Regulation (GDPR)

   Region: Europe-based

   Description: A legal framework that sets guidelines for the collection and processing of personal information from individuals who live in the European Union (EU).

   Purpose: To protect the privacy and personal data of EU citizens.

4. Payment Card Industry Data Security Standard (PCI DSS)

   Description: A set of security standards designed to ensure that all companies that process, store, or transmit credit card information maintain a secure environment.

5. HIPAA (Health Insurance Portability and Accountability Act)

   Region: U.S.-based

   Description: A U.S. law that sets standards for protecting sensitive patient health information.

   Key Components:

   Confidentiality: Ensuring patient information is not disclosed to unauthorized individuals.

   Integrity: Protecting patient data from being altered or tampered with.

   Privacy Protections: Safeguarding personal health information.

6. SOC Type 1 and SOC Type 2

   SOC Type 1: Evaluates the design of security controls at a specific point in time.

   SOC Type 2: Evaluates the effectiveness of security controls over a period of time.

Security Ethics

Ethical Principles in Security:

- Confidentiality: Respecting and protecting the privacy of information.
- Privacy Protections: Safeguarding individuals' personal information.
- Integrity: Ensuring accuracy and completeness of data and systems.
- Laws: Adhering to legal standards and regulations.

Guidelines for Security Professionals:

- Confidentiality: Protecting sensitive information from unauthorized access.
- Privacy: Upholding the privacy rights of individuals and organizations.
- Ethical Decision-Making: Making appropriate and ethical choices in professional security practices.

HIPAA as an Example

HIPAA*serves as an example of enforcing confidentiality, integrity, and privacy protections in the healthcare sector. It exemplifies the legal framework that governs the handling of sensitive information.

Security Tools and Concepts

1. Logs

- Definition: A record of events that occur within an organization's systems.
- Purpose: To track and review activities for security monitoring and incident investigation.

2. SIEM (Security Information and Event Management) Tools

- Description: Applications that collect, analyze, and manage log data to monitor and respond to critical activities within an organization.
- Features: Real-time monitoring and instant information.
- Examples:
  Splunk: Provides detailed log analysis and monitoring.
  Chronicle: Offers scalable security analytics and threat detection.

3. Playbooks

- Definition: Manuals that provide guidelines and procedures for responding to specific types of threats and incidents.
- Purpose: To offer structured responses and maintain a chain of custody for evidence.

4. Network Protocol Analyzers

- Definition: Tools designed to capture and analyze data traffic within a network.
- Examples:

  Wireshark: A widely used network protocol analyzer for capturing and examining network packets.

  tcpdump: A command-line packet analyzer for network troubleshooting.

5. Programming for Automation

- Description: Using programming to automate repetitive tasks in cybersecurity.
- Purpose: To enhance efficiency and consistency in security operations.

6. Web Vulnerabilities

- Definition: Unique flaws in web applications that can be exploited by threat actors using malicious code or behavior.
- Purpose: To gain unauthorized access or deploy malware.

7. Antivirus Software

- Definition: A program designed to prevent, detect, and remove malware and cyberattacks.

- Also Known As: Anti-malware software.
- Function: Monitors system activity to protect against various threats.

8. Intrusion Detection Systems (IDS)

- Definition: Systems that monitor network and system activities for suspicious or malicious behavior.
- Purpose: To detect and alert on potential threats.

9. Encryption

- Definition: The process of converting data from a readable format (plaintext) into a cryptographically encrypted format (ciphertext).
- Purpose: To protect data by making it unreadable to unauthorized individuals.
- Components:
  Plaintext: The original, readable data.
  Ciphertext: The encrypted data.

Penetration Testing

Definition

Penetration Testing: The act of conducting a simulated attack on a system, network, or application to identify vulnerabilities that could be exploited by attackers.

Purpose

- Identify Vulnerabilities: Discover weaknesses in systems or applications before malicious actors can exploit them.
- Evaluate Security Measures: Assess the effectiveness of existing security controls.
- Improve Security Posture: Provide recommendations to enhance security and reduce risks.

Process

1. Planning and Scoping: Define the scope, objectives, and rules of engagement for the test.
2. Information Gathering: Collect data about the target system or network.
3. Vulnerability Analysis: Identify potential security weaknesses.
4. Exploitation: Attempt to exploit identified vulnerabilities to assess their impact.
5. Reporting: Document findings, provide recommendations, and suggest improvements.