ELYSIUM ACADEMY
Milestone of Cognizance

CYBER SECURITY

ELYSIUM ACADEMY SPARK NOTES

VERSION 2.1

ELYSIUM ACADEMY
Milestone of Cognizance

01. Basics of Cybersecurity

- **Cybersecurity -** The practice of protecting systems, networks, and programs from digital attacks.
- **Goals (CIA Triad) -**
  - o Confidentiality: Ensuring that information is accessible only to those authorized to access it.
  - o Integrity: Maintaining the accuracy and completeness of data.
  - o Availability: Ensuring that information and resources are available to those who need them.

02. Types of Cyber Attacks

- **Malware -** Malicious software designed to harm or exploit devices.
  - o Examples: Viruses, Worms, Trojans, Ransomware, Spyware.
  by Google for building
- **Phishing -** Attempt to trick users into revealing personal information by pretending to be a trustworthy entity.n.
- **Denial of Service (DoS): -** An attack meant to shut down a machine or network, making it inaccessible to users.
- **Man-in-the-Middle (MitM) -** Attack where the attacker intercepts communication between two parties.
- **SQL Injection -** malicious SQL queries to manipulate a database.
- **Zero-Day Exploit -** An attack that occurs on the same day a weakness is discovered in software.

03. Security Measures

- **Firewalls -** Network security systems that monitor and control incoming and outgoing network traffic.
- **Encryption -** Programs designed to detect and remove malware.
- **Antivirus Software -** The process of converting data into a code to prevent unauthorized access.

- **Multi-Factor Authentication (MFA) -** Security system that requires more than one method of authentication.
- **Intrusion Detection Systems (IDS) -** Monitors network traffic for suspicious activity and issues alerts.
- **Patch Management -** : Regularly updating software to protect against vulnerabilities.

04.Cryptography

- **Symmetric Encryption -** The same key is used for both encryption and decryption (e.g., AES).
- **Asymmetric Encryption -** Uses a pair of keys (public and private); one encrypts, the other decrypts (e.g., RSA).
- **Hashing -** Converts data into a fixed-size string of characters, which is typically a hash code (e.g., SHA-256).
- **Digital Signatures -** A digital code (encrypted hash) attached to a message or document to verify its authenticity..

05.Cybersecurity Frameworks

- **NIST Cybersecurity Framework -** Provides a policy framework of computer security guidance for how private sector organizations can assess and improve their ability to prevent, detect, and respond to cyberattacks.
- **ISO/IEC 27001 -** A standard for information security management systems (ISMS).
- **CIS Controls -** A set of best practices for securing IT systems and data against the most pervasive cyber-attacks.

06.Network Security

- **VPN (Virtual Private Network) -** Encrypts internet connections to secure data sent and received.
- **Proxy Server -** Acts as an intermediary for requests from clients seeking resources from other servers.

- **Network Segmentation-** Dividing a network into segments to improve security and performance.
- **Secure Sockets Layer (SSL) / Transport Layer Security (TLS) -** Protocols for securing internet communications.

07. Security Policies

- **Access Control Policy -** Defines who can access and use company information and resources.
- **Incident Response Plan -** A predefined strategy for identifying, responding to, and recovering from cyber incidents.
- **Data Protection Policy -** Guidelines for how to protect and manage sensitive data.
- **Acceptable Use Policy -** Defines what constitutes appropriate use of company resources.

08.Cybersecurity Best Practices

- **Regular Backups -** Frequently back up critical data to prevent loss during an attack.
- **Employee Training -** Regularly train employees on cybersecurity awareness and safe practices..
- **Strong Passwords -** Use complex passwords and change them regularly
- **Least Privilege -** Grant users only the access they need to perform their job functions.
- **Monitor Logs -** Regularly review logs to detect and respond to suspicious activity.

09. Compliance and Regulations

- **GDPR (General Data Protection Regulation -** European Union regulation on data protection and privacy.
- **HIPAA (Health Insurance Portability and Accountability Act) -** US law designed to protect patient health information.
- **PCI DSS (Payment Card Industry Data Security Standard) -** Standards for securing credit card information.

10. Emerging Threats

- **Ransomware -** Malware that encrypts data and demands payment for the decryption key.
- **Advanced Persistent Threats (APTs) -** Prolonged and targeted cyberattacks where an intruder remains undetected for an extended period.
- **IoT Vulnerabilities -** Security risks associated with the increasing number of connected devices.
- **AI-Powered Attacks -** Cyberattacks that leverage artificial intelligence to evade detection.

This spark notes provides a quick overview of key concepts, practices, and tools in cybersecurity, covering various types of cyber attacks, security measures, cryptography, frameworks, and best practices.

ELYSIUM ACADEMY
Milestone of Cognizance

Thank you

For Your Learning Today

elysiumacademy.org | info@elysiumacademy.org

Scan Here for More
Spark Notes