CS3018 - NETWORK SECURITY

Assignment 1

> Name: M K Lokesh Kumar

> Registration No.: 22011103026

> Class: Cyber Security

Evolution of Network Security

Over the course of the past two decades, network security has undergone significant transformation driven by increasingly complex cyber threats and several advancements in defensive technologies. Some developments with respect to technologies like firewalls, IDP/IPS, and encryption are discussed below:

- Firewalls
  - Early
    - Traditional firewalls employed static rule sets to control network traffic based on IP addresses and port numbers
    - Effective for basic threat mitigation
    - Struggled against sophisticated attacks
  - Modern
    - Integrate deep packet inspection and application-layer controls for greater security
    - They are equipped with the ability to inspect encrypted network traffic and identify threats at the application level
- Intrusion Detection System/Intrusion Prevention System(IDS/IPS)
  - Early
    - Relied on signature-based detection mechanisms, matching traffic patterns
    - Effective against known threats at the time
    - Failed to detect zero-day attacks
  - Modern
    - Incorporate behaviour-based detection, anomaly analysis, and machine learning models to detect both known and unknown threats
- Encryption
  - Early
    - Early encryption methods and algorithms like DES and RSA offered limited key lengthd
    - They were suspectible to brute force attacks
  - Modern
    - Advanced encryption algorithms such as AES-256 and TLS(for web application security) are quite secure for modern applications
    - Qantum-resistant cryptographic research is gaining relevance to counter future quantum computing threats

Security Models

Security models are formal frameworks used to define and endore security policies within computer systems and networks. The nature of traditional and modern security models are discussed below:

- Traditional Models
    - Bell-LaPadula Model
        - Follows a "no read up, no write down" principle, focusing on data confidentiality
    - Biba Model
        - Follows a "no write up, no read down" principle, focusing on data integrity
- Modern Models
    - NIST Cybersecurity Framework
        - Includes the core functions of Identify, Protect, Detect, Respond, and Recover
        - It is useful for critical infrastructure protection
    - ISO 27001
        - It is an international standard primarily emphasizing risk management and information security policies

Modern frameworks focus not only on access control but also on incident response and continuous improvement.

Evolution of Risk Management Strategies

Risk management involves systematic assessment and mitigation of threats, of both active and passive nature. Organisations adopt appropriate frameworks to identify, evaluate, and respond to risks effectively.

- Techniques

    - Asset Identification - Involves the process of cataloging critical digital assets
    - Threat Modeling - Using models ot understand potential attack vectors; examples include STRIDE(spoofing, tampering, repudation, information disclosure, denial of service, elevation of privileges)
    - Vulnerability Analysis
    - Risk Evaluation - Risk matrices are employed to assess likelihood versus impact guide prioritization of mitigation strategies

- Strategies

    - For Passive Attacks - Use of strong encryption standards such as TLS
    - For Active Attacks - By rate limiting, using IDS/IPS, and more

- Application

    - ISO 27005
        - Focuses on continuous identification, evaluation, and treatment of risks
    - NIST
        - Offers detailed security controls for federal agencies adn enterprises
        - Focuses on continuous monitoring, identity management, and incident response

Conclusion

The evolution of network security technologiess and risk managmenet frameworks has been instrumental in addressing the increasing complexity of cyber threats. Modern approaches emphasize proactive threat detection, continous risk assessment, and dynamic defense technologies. As cyberattacks grow more sophisticated, the adoption of security frameworks like NIST remain critcial for maintaining reobust security postures in both public and private sectors.