CYBERSECURITY TERMINOLOGY

INTRODUCTION

Welcome to the presentation on Cybersecurity Terminology. Understanding these terms is essential for navigating the intricate landscape of cybersecurity, regardless of whether you're a novice or a seasoned professional. Throughout this session, we will delve into fundamental concepts, prevalent attacks, protective measures, and pivotal technologies in the realm of cybersecurity.

1.FOUNDATIONAL CONCEPTS

1.1. Threat

A threat encompasses any potential danger to information or systems. It could be intentional, such as a cyberattack, or unintentional, like a natural disaster. Threats take advantage of vulnerabilities to cause harm or unauthorized actions.
Examples: Malware, hackers, natural disasters

1.2. Vulnerability

A vulnerability represents a weakness in a system, application, or network that can be exploited by threats. Vulnerabilities may stem from software bugs, misconfigurations, or weak security practices.
Examples: Unpatched software, open ports, default passwords.

1.3. Risk

Risk denotes the potential for loss or damage when a threat exploits a vulnerability. It is typically calculated as Risk = Threat x Vulnerability x Impact.
Examples: Data breaches, financial loss, reputation damage.

1.4 Attack Vector

An attack vector is the method or pathway used by a threat actor to gain unauthorized access to a system or network.

Examples: Phishing emails, compromised websites, infected USB drives.

1.5 Exploit

An exploit refers to a tool or technique used to take advantage of a vulnerability in a system to cause unintended behavior.

Examples: Buffer overflow, SQL injection, ransomware payloads.

2.COMMON CYBER ATTACKS

2.1.Phishing

Phishing is a social engineering attack where perpetrators pose as trustworthy entities to dupe individuals into providing sensitive information, such as passwords or credit card numbers.
Examples: Deceptive emails, fake websites, fraudulent messages.

2.2.Malware

Malware (malicious software) is code designed to disrupt, damage, or gain unauthorized access to a system.
Types: Viruses, worms, Trojans, ransomware, spyware.

2.3.Denial of Service (DoS)

A DoS attack aims to render a system or network resource unavailable by overwhelming it with a flood of illegitimate requests.
Examples: Flood attacks, Ping of Death, SYN flood.

2.4.Man-in-theMiddle (MitM)

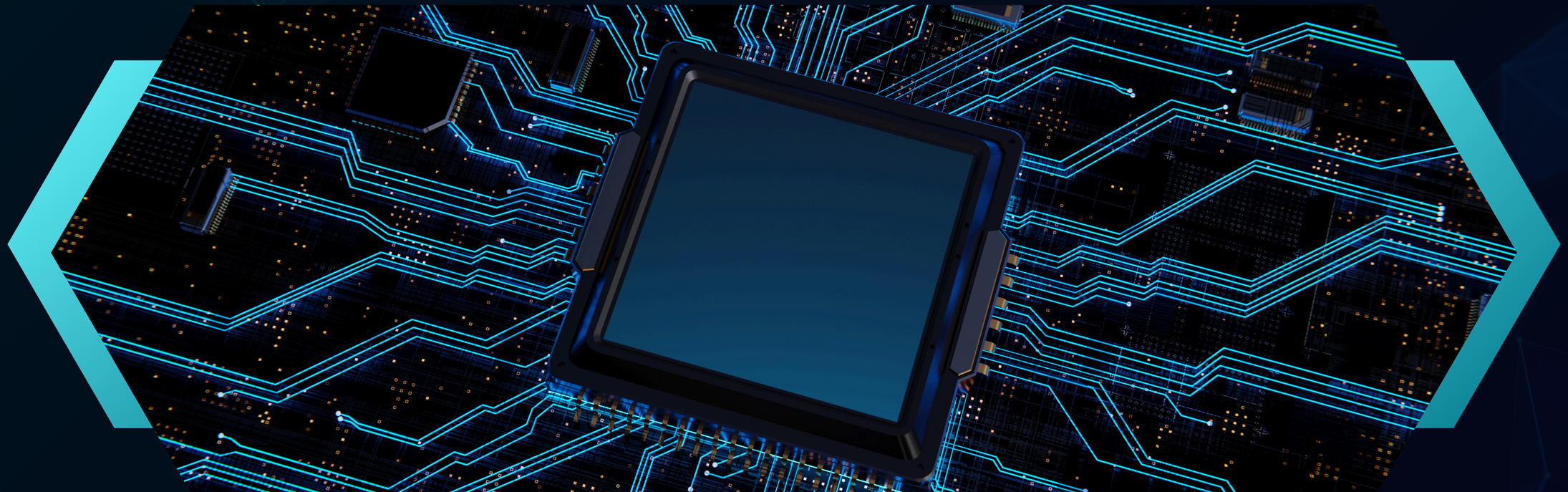
In a MitM attack, the attacker covertly intercepts and relays messages between two parties who believe they are communicating directly with each other.
Examples: Eavesdropping, session hijacking, SSL stripping.

2.5.SQL Injection

SQL Injection is an attack that allows perpetrators to execute arbitrary SQL code on a database by exploiting insecure input handling in applications.
Examples: Bypassing authentication, extracting data, modifying records.

2.6.Zero-Day Exploit

A zero-day exploit targets a vulnerability that is unknown to the vendor and has no existing patch or fix.
Examples: Exploiting new software vulnerabilities before they're patched.



3. PROTECTIVE MEASURES

3.1. Firewall

A firewall is a network security device or software that supervises and manages incoming and outgoing network traffic based on predetermined security rules.

Types: Network firewalls, application firewalls, next-generation firewalls.

3.2. Encryption

Encryption is the method involved with changing information into a coded design over completely to forestall unapproved access. Just approved parties with the decoding key can peruse the information.

Types: Symmetric encryption (AES), uneven encryption (RSA), hashing (SHA).

3.3. Multi-Factor Authentication (MFA)

MFA expects clients to check their personality through numerous strategies for verification, adding an additional layer of safety.

Models: Secret phrase + OTP, secret phrase + biometric check.

3.4.Intrusion Detection System (IDS)

An IDS screens network traffic for dubious exercises and issues alarms when potential dangers are identified.

Types: Organization based IDS (NIDS), have based IDS (HIDS).

3.5. Interruption Anticipation Framework (IPS)

An IPS recognizes dangers like an IDS asInterruption Anticipation Framework (IPS) well as makes preventive moves to impede or relieve them.

Models: Hindering traffic, resetting associations, reconfiguring firewalls.

3.6.Security Data and Occasion The board (SIEM)

SIEM frameworks give constant investigation of safety alarms produced by applications and organization equipment. They total and break down logs from different sources.

Models: Splunk, IBM QRadar, ArcSight.

3.7.Fix The board

Fix The board includes applying updates to programming and frameworks to fix weaknesses and further develop security.

Apparatuses: WSUS, SCCM, Ansible.

4. KEY ADVANCEMENTS AND PRACTICES

4.1.Virtual Confidential Organization (VPN)

A VPN scrambles web traffic and veils the client's IP address, giving a protected association over the web.

Types: Site-to-site VPN, remote access VPN.

4.2.Endpoint Discovery and Reaction (EDR)

EDR arrangements give nonstop observing and reaction to cutting edge dangers on endpoints, like PCs and cell phones.

Models: CrowdStrike Hawk, Carbon Dark, SentinelOne.

4.3.Public Key Framework (PKI)

PKI is a structure that oversees computerized testaments and encryption keys for getting correspondences and exchanges.

Parts: Authentication Specialists (CAs), computerized testaments, public/confidential keys.

4.4.Sandboxing

Sandboxing confines projects or cycles in a controlled climate to examine and recognize dubious way of behaving without gambling with the primary framework.

Models: Testing malware in virtual conditions, running untrusted code securely.

4.5.Danger Insight

Danger Insight implies gathering and examining data about expected dangers to more readily plan and answer assaults.

Sources: Danger takes care of, honeypots, OSINT (Open Source Insight).

4.6.Information Misfortune Anticipation (DLP)

DLP procedures and devices are intended to distinguish and forestall unapproved information transmission or access.

Models: Checking email for delicate information, obstructing USB moves.

5.EMERGING TRENDS

5.1. Zero Trust Design

Zero Trust is a security model where no client or gadget, inside or outside the organization, is trusted as a matter of course. Check is expected for each entrance demand.

Standards: Check expressly, utilize least honor, accept break.

5.2. Man-made brainpower (artificial intelligence) in Network protection

Artificial intelligence is utilized to break down enormous volumes of information for danger location, computerize reactions, and further develop security investigation.

Applications: Oddity identification, robotized episode reaction, prescient examination.

5.3. Blockchain Security

Blockchain innovation gives a decentralized and unchanging record for secure exchanges, helpful in regions like secure character the executives and information honesty.

Models: Cryptographic forms of money, savvy contracts, secure democratic frameworks.

5.4. Quantum Registering Dangers

Quantum registering presents possible dangers to current encryption techniques because of its capacity to tackle complex issues quicker than conventional PCs.

Countermeasures: Creating quantum-safe calculations.

CONCLUSION

Comprehending the terminology associated with network security is pivotal in grasping the challenges and innovations within the realm of network protection. This knowledge is instrumental in constructing robust security frameworks, implementing defensive strategies, and proactively addressing potential threats.

ADDITIONAL RECOMMENDATIONS:

For Books: Consider immersing yourself in "Network Security Basics" written by the esteemed author Charles J. Streams.

Regarding Websites: Explore the reputable SANS Institute and delve into the extensive NIST Network Security Framework.

In terms of Online Courses: Engage in the informative Network Security Seminars offered on platforms like Coursera and Udemy for a enriching educational opportunity.

CONTACT US

+91 9766695361

www.andintern.in

kushagrapitre2@gmail.com

14th A Cross Road, Sector 6,
HSR Layout, Bengaluru, Karnataka-560102

THANK YOU