Association For Cyber Security

Understanding Vulnerabilities and Threats

Agenda

- Introduction to Cybersecurity Threats
- Basic Terminology
- Viruses and Worms
- Malware Overview
- Viruses
- Worms
- Trojans
- Introduction to Vulnerabilities
- Types of Vulnerabilities
- Types of Threat Actors
- Common Attack Techniques
- Case Studies, Q&A, and Wrap-up

Introduction to Cybersecurity Threats

- Definition: Cybersecurity threats are potential dangers that can exploit vulnerabilities to breach security and cause harm.

Importance: Protecting data in confidentiality, integrity and availability.

Basic Terminology

- Cybersecurity: Measures to protect computer systems from cyber attacks.
- Threats vs Vulnerabilities: Threats are potential malicious actions, while vulnerabilities are weaknesses that can be exploited.
- Malware
- Exploits
- Attack Vectors
- Threat Actors

Viruses and Worms

- Viruses
- Worms

- Differences: Viruses need a host file to spread, worms do not.

Historical Context: The Morris Worm (1988), one of the first major worms.

Malware Overview

□ Definition: Malware encompasses various forms of harmful software.

□ Types:

□ - Viruses

□ - Worms

□ - Trojans

□ - Ransomware

□ - Spyware

□ - Adware

□ Spread Mechanisms: Email attachments, malicious downloads, infected advertisements.

□ Impacts: Data theft, financial loss, system damage.

Viruses

- Function: Attach to files and execute when the file is opened.
- Common Types:
- - File Infector: Infects executable files.
- - Macro Virus: Targets macro-enabled documents.
- - Boot Sector Virus: Infects the boot sector of storage devices.
- - Polymorphic Virus: Changes its code to avoid detection.

Prevention: Use antivirus software, keep systems updated, exercise caution with email attachments.

Worms

□ Function: Spread autonomously across networks.

□ Notable Worms:

□ - ILOVEYOU (2000): Caused widespread damage.

□ - Conficker (2008): Infected millions of computers.

□ - WannaCry (2017): A ransomware worm causing global disruption.

Prevention: Use firewalls, keep software updated, monitor network traffic.

Trojans

- Definition: Malicious software disguised as legitimate.
- Spread: Users unknowingly download and install them.
- Common Types:
- - Backdoor Trojans: Provide unauthorized access.
- - Rootkits: Hide other malicious activities.
- - Banker Trojans: Steal financial information.

Prevention: Download software from trusted sources, use security software.

Introduction to Vulnerabilities

- Definition: Vulnerabilities are weaknesses or flaws in software, hardware, or organizational processes.
- Common Sources:
  - Software Bugs: Mistakes in code.
  - Configuration Issues: Incorrect settings.
  - Human Error: Mistakes like weak passwords.

Importance: Finding and fixing vulnerabilities is crucial for security.

Types of Vulnerabilities

□ Software Vulnerabilities:

□ - Buffer Overflow: Too much data causes issues. (infinite loops)

□ - SQL Injection: Malicious commands to databases. (1 = 1)

□ - Cross-Site Scripting (XSS): Malicious scripts on websites.

□ Human Vulnerabilities: Social engineering tactics like phishing.

Statistics: Many breaches result from unpatched vulnerabilities.

Types of Threat Actors

- Hackers:
- - Black Hat: Malicious hackers.
- - White Hat: Ethical hackers.
- - Gray Hat: Hackers who are sometimes good, sometimes bad.
- Organized Crime Groups: Cybercriminal gangs.
- Nation-State Actors: Government-backed hackers .
- Insider Threats: Employees causing harm.
- Hacktivists: Hackers with political or social motives.

Common Attack Techniques

- Phishing: Deceptive emails to steal information.
- Denial-of-Service (DoS) Attacks: Overloading systems to crash them.
- Man-in-the-Middle (MitM) Attacks: Intercepting communications.
- SQL Injection: Manipulating databases.
- Zero-Day Exploits: Attacks exploiting unknown vulnerabilities.

Statistics: Phishing is a major cause of security breaches.

Q&A and Wrap-up

- Conclusion : In today's digital age, understanding vulnerabilities and threats is crucial for safeguarding personal and organizational data. By familiarizing ourselves with basic cybersecurity terminology, the nature of various malware types, and the techniques used by threat actors, we can better protect our systems from potential attacks. Recognizing the importance of identifying and mitigating vulnerabilities helps in maintaining robust security. Stay informed, stay vigilant, and always prioritize cybersecurity to protect your digital assets.

- Q&A Session.

In 2017, Equifax experienced a data breach that exposed the personal information of 147 million people, including names, Social Security numbers, birth dates, and addresses.

Case Study: The 2017 Equifax Data Breach

❑ March 2017 : A critical security vulnerability in Apache Struts was disclosed and patched.

❑ May 2017 : Hackers exploited the unpatched vulnerability in Equifax’s web application.-

❑ July 2017 : Equifax detected suspicious activity and began an investigation.

❑ September 2017: Equifax publicly announced the breach.

Impact

- Financial: Significant costs related to legal fees, consumer restitution, and cybersecurity

- Reputational: Severe damage to Equifax’s reputation and consumer trust.

- Regulatory: Investigations by regulatory bodies; a settlement agreement of up to $425 million for consumer restitution.

Association For
Cyber Security

Thank You