Threats, Vulnerabilities, and Attacks

Website & Web application

- **A web site** are typically informational in nature with a limited amount of advanced functionality.
- Simple websites consist primarily of static content where the data displayed is the same for every visitor and content changes are infrequent
- **Web applications**, or Rich Internet Applications (RIA), are presented as either a web site or as part of a web site, but not all web sites are web applications.
- **A web application** is a web site that DOES something other than display content to the masses.
- It's intended for user interactions and transactions, performing actual business functions, and not simply displaying information to a user.

Website & Web application

- Ebay is a web application. So are Paypal, Twitter, Facebook, YouTube, Flickr, eHarmony, eTrade, GMail, and Wikipedia.
- Your bank, assuming it offers online banking, has a web application component on its site.
- If you can think of a site where you create an account, log in, and conduct some actual business, it's probably a web application

Definitions

- When discussing network security, the three common terms used are as follows:
- **A threat** is any potential occurrence, malicious or otherwise, that could harm an asset. In other words, a threat is any bad thing that can happen to your assets.
- **A vulnerability** is a weakness that makes a threat possible. This may be because of poor design, configuration mistakes, or inappropriate and insecure coding techniques.
- **An attack** is an action that exploits a vulnerability or enacts a threat. Examples of attacks include sending malicious input to an application or flooding a network in an attempt to deny service.
- **What are the differences between attack and Threat?**

What are the differences between attack and Threat?

- **The main difference** between threat and attack is a threat can be either intentional or unintentional where as an attack is intentional.
- **Threat** is a circumstance that has potential to cause loss or damage whereas **attack** is attempted to cause damage.
- Threat to the information system doesn't mean information was altered or damaged but attack on the information system means there might be chance to alter, damage, or obtain information when attack was successful.
- A security threat is the expressed potential for the occurrence of an attack.
- A security attack is an action taken against a target with the intention of doing harm.

Vulnerability

- Intentional attacks on computing resources and networks persist for a number of reasons
- The vulnerabilities could be weaknesses in the technology, configuration, or security policy.
- Any discovered vulnerability must be addressed to mitigate any threat that could take advantage of the vulnerability.
- It is difficult to thoroughly test an application for all possible intrusions

Vulnerability

- **In summary, vulnerability**—A weakness that is inherent in every network and device. This includes:
- routers, switches, desktops, servers, and even security devices themselves.

❑ Networks are typically plagued by one or all of three primary vulnerabilities or weaknesses:

- Technology weaknesses
- Configuration weaknesses
- Security policy weaknesses

Vulnerability

- **Technology weaknesses**
- Computer and network technologies have intrinsic security weaknesses.
  - These include **TCP/IP** protocol weaknesses,

HTTP, FTP, and ICMP are inherently insecure

The UNIX, Linux, Macintosh, Windows NT, 9x, 2K, XP

  - operating system weaknesses,
  - and network **equipment** weaknesses.

such as routers, firewalls, and switches, have security weaknesses

Password protection
Lack of authentication
Routing protocols
Firewall holes

Go to slid 10

Vulnerability

- Transmission Control Protocol (TCP) and Internet Protocol (IP) are two distinct network protocols.
- TCP/IP is arguably the single most important computer networking technology. The Internet and most home networks support TCP/IP as the "language" computers use to find and connect with each other.

Back

Vulnerability

- Configuration Weaknesses
- Network administrators or network engineers need to learn what the configuration weaknesses are and correctly configure their computing and network devices to compensate.

Unsecured user accounts

System accounts with easily guessed passwords

Misconfigured Internet services

Unsecured default settings within products

Misconfigured network equipment

For example:

A common problem is to turn on JavaScript in web browsers, enabling attacks by way of hostile JavaScript when accessing untrusted sites

For example:

Misconfigured access lists, routing protocols
Misconfigured or lack of encryption and remote-access controls

Vulnerability

- Security Policy Weaknesses
- Security policy weaknesses can create unforeseen security threats.
- The network can pose security risks to the network if users do not follow the security policy.

Lack of written security policy

Politics

Lack of continuity.

Logical access controls. not applied.

Poorly chosen, easily cracked, or default passwords can allow unauthorized access to the network

Inadequate monitoring and auditing allow attacks and not applied unauthorized use to continue, wasting company resources

Threats

- A threat is an event that can take advantage of vulnerability and cause a negative impact on the network.

- Potential threats to the network need to be identified, and the related vulnerabilities need to be addressed to minimize the risk of the threat.

Threats

There are four primary classes of threats to network security:

- ***Unstructured threats***—Unstructured threats consist of mostly inexperienced individuals using easily available hacking tools such as shell scripts and password crackers.

- Even unstructured threats that are only executed with the intent of testing and challenging a hacker's skills can still do serious damage to a company.

- Unstructured threats—Threats that are random and usually the result of an attacker identifying the vulnerability by scanning the network looking for "targets of opportunity."

- This type of threat is by far the most common threat because it can be performed using automated tools (scripts) that are readily available on the Internet and can be performed by someone with very limited computer skills.

Threats

- **Structured threats : t**hreats that are preplanned and focus on a specific target.
- A structured threat is an organized effort to breach a specific network or organization

- These threats come from hackers who are more highly motivated and technically competent.
- These people know system vulnerabilities and can understand and develop exploit code and scripts.

Threats

- **External threats** can arise from individuals or organizations working outside of a company.
- They do not have authorized access to the computer systems or network.
- They work their way into a network mainly from the Internet or dialup access servers

Threats

- Internal threats occur when someone has authorized access to the network with either an account on a server or physical access to the network.
- According to the FBI, internal access and misuse account for 60 percent to 80 percent of reported incidents.

Attack

- **Attacks—**The threats use a variety of tools, scripts, and programs to launch attacks against networks and network devices.
- Typically, the network devices under attack are the endpoints, such as servers and desktops
- The home page of numerous organizations has been attacked and replaced by a new home page of the choosing crackers.
- Sites that **have been** cracked include **Yahoo,** the **U.S. Army, the CIA, NASA**, and the **New York Times**.
- In most cases, the crackers just put up some funny text and the sites were repaired within a few hours.

Attacks

- Numerous sites have been brought down by denial-of-service attacks, in which the cracker floods the site with traffic, rendering it unable to respond to legitimate queries.
- Often the attack is mounted from a large number of machines that the cracker has already broken into (**DoS atacks**).
- These attacks are so common.
- They can cost the attacked site thousands of dollars in lost business

Attacks

Four primary classes of attacks exist:

- Reconnaissance
- Access
- Denial of service
- Worms, viruses, and Trojan horses

Reconnaissance

- Reconnaissance attack is a kind of information gathering on network system and services. This enables the attacker to discover vulnerabilities or weaknesses on the network
- In most cases, it precedes an actual access or **denial-of-service** (DoS) attack.
- Reconnaissance is somewhat analogous to a thief casing a neighborhood for vulnerable homes to break into, such as an unoccupied residence, easy-to-open doors, or open windows.

Access

- System access is the ability for an unauthorized intruder to gain access to a device for which the intruder does not have an account or a password.
- Entering or accessing systems to which one does not have authority to access usually involves running a script, or tool that exploits a known vulnerability of the system or application being attacked.

Denial of service

- Denial of service implies that an attacker disables or corrupts networks, systems, or services with the intent to deny services to intended users.
- DoS attacks involve either crashing the system or slowing it down to the point that it is unusable.
- But DoS can also be as simple as deleting or corrupting information.
- In most cases, performing the attack simply involves running a script.
- The attacker does not need prior access to the target because a way to access it is all that is usually required.
- For these reasons, DoS attacks are the most feared.

Worms, Viruses, and Trojan Horses

- **Worms:** A malicious program that replicates itself until it fills all of the storage space on a drive or network.
- A Trojan horse is defined as a "malicious, security-breaking program that is disguised as something benign".
- For example, you download what appears to be a movie or music file, but when you click on it, you unleash a dangerous program that erases your disk, sends your credit card numbers and passwords to a stranger, or lets that stranger hijack your computer to commit illegal denial of service attacks.

Viruses

- **A computer program that is designed to replicate itself by copying itself into the other programs stored in a computer.**
- **It may be benign or have a negative effect, such as causing a program to operate incorrectly or corrupting a computer's memory**
- **What is the difference between worms and viruses?**