Security Threats and Vulnerabilities --- Objective: explain why basic security measures are necessary

Threats

- Definition: Intruders (অনুপ্রবেশকারী) who gain access by modifying software or exploiting software vulnerabilities are called threat actors.
- Cause:
  Access to network through
  1) software vulnerabilities
  2) hardware attacks
  3) someone's username and password
- Result: theft or damage of important information, time, or money
- 4 types:
  1) Information theft
  2) Data loss and manipulation
  3) Identity theft
  4) Disruption of service

Vulnerabilities

- Definition: Vulnerability is the degree of weakness in a network or device
- 3 types:

1) Technological	2) Configuration:	3) Security Policy
- TCP/IP protocol - OS - Network equipment	- Unsecured account - Unsecured default settings - Easily guessed password - Misconfigured internet service - Misconfigured network equipment	Lack of - Written security policy - Authentication - Disaster recovery plan

TCP- Transmission control protocol

IP - internet protocol

Physical Threats

4 types
1) Hardware
2) Environmental
3) Electrical
4) Maintenance

Def: If network resources can be physically compromised, a threat actor can deny the use of network resources

Network Attacks ---- Objective: Identify security vulnerabilities

Malware/Malicious Software

• Definition: is code or software specifically designed to damage, disrupt, steal, or inflict "bad" or illegitimate action on data, hosts, or networks.

• 3 types

1) Viruses	2) Worms	3) Trojan Horses
- inserts a copy of itself into program - becomes part of another program. - spreads from one computer to another - leaves infections as it travels. - need infected host program to spread - reproduce by infecting other files.	- replicate functional copies of themselves and can cause the same type of damage. Doesn't need infected host program to spread reproduce by infecting other files.	Looks legitimate (safe) Doesn't reproduce by infecting other files. Can self-replicate (copy) spread through user interaction 1) opening an email attachment 2) downloading and running a file from the internet

Comparison

Network attacks: 3 types

1) Reconnaissance attacks — The discovery and mapping of systems, services, or vulnerabilities.

2) Access attacks: 4 types — The unauthorized manipulation of data, system access, or user privileges

Password attacks	Trust exploitation	Port redirection	Man-in-the middle
uses brute force trojan horse packet sniffers	uses unauthorized privileges to gain access to a system	uses a compromised system as a base for attacks against other targets. For example, a threat actor using SSH (port 22) to connect to a compromised host A. Host A is trusted by host B and, therefore, the threat actor can use Telnet (port 23) to access it.	The threat actor is positioned in between two legitimate entities to read or modify the data that passes between the two parties

3) Denial of service attacks (DoS) — Def: The disabling or corruption of networks, systems, or services.
Need handle specially cause
- Easily can be implemented
- Cause significant damage
- most publicized form of attack
- most difficult to eliminate.

Network Attack Mitigation (making less severe)

Name of Approach: defense-in-depth approach (or layered approach)

Definition: combination of networking devices and services working in tandem to mitigate network attacks by securing devices including routers, switches, servers, and hosts. (5 general mitigation techniques)

<table>
<tr>
<td colspan="4">Keep backups
Data backups are usually stored offsite to protect the backup media if anything happens to the main facility

Should be performed regularly to avoid data loss

Consider 4 things</td>
<td colspan="3">Upgrade, Update, and Patch

3 tasks

Upgrade Patch Update</td>
<td colspan="3">Authentication, Authorization, and Accounting (AAA)

way to control 3 tasks

• The concept of AAA is similar to the use of a credit card.</td>
<td colspan="4">Firewalls
reside between two or more networks
control the traffic between them
help prevent unauthorized access

allow outside users controlled access to specific services --- DMZ (demilitarized zone)

4 methods of firewalls (to prevent/allow access)</td>
<td>Endpoint Security
An endpoint /host is an individual computer system/device that acts as a network client</td>
</tr>
<tr>
<td>Frequency
•Perform backups on a regular basis</td>
<td>Storage

Full backups: time-consuming

perform monthly/weekly backups with frequent partial backups of changed files.</td>
<td>Security

Backups should be transported to an approved offsite storage location</td>
<td>Validation

•Backups should be protected using strong passwords.
↓
required to restore data</td>
<td>As new malware is released, enterprises need to keep upgraded with the latest versions of antivirus software</td>
<td>download security updates from the operating system vendor and patch all vulnerable systems</td>
<td>make sure all end systems automatically download updates.</td>
<td>who is permitted to access a network (authenticate)

credit card identifies the user</td>
<td>what actions they perform while accessing the network (authorize)

how much the user can spend</td>
<td>making a record of what was done while they are there (accounting)

keeps account of what items the user spent money on.</td>
<td>Packet filtering

based on IP or MAC addresses</td>
<td>Application filtering

by specific application types based on port numbers</td>
<td>URL filtering
Uniform resource Locator

based on specific URLs or keywords</td>
<td>Stateful packet inspection (SPI)

Incoming packets remain blocked (not given access) unless permission given

recognize and filter out specific types of attacks (DoS).</td>
<td>Ex: devices, servers

Depends on network access control

most challenging jobs because it involves human nature.

A company must have
- well-documented policies
- employees must be aware of these rules.</td>
</tr>
</table>

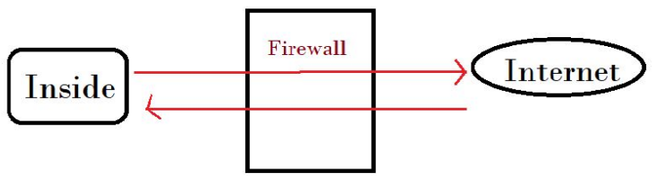

Fig 1: Allowing access

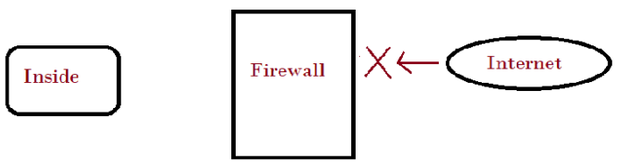

Fig 2: Denying outside access

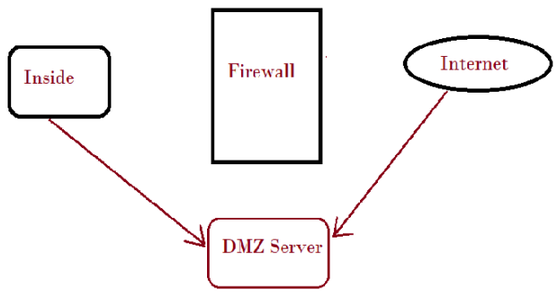

Fig 3: Specified access by DMZ

Device Security ---- Objective: Configure network devices with device hardening features to mitigate security threats

For security of Cisco routers - **Cisco Auto Secure feature**

Steps

Passwords	Additional password security (4 steps)	Enable SSH	Disable Unused Services
1) length – at least 8 characters 2) complex (mix uppercase and lowercase) 3) Avoid easily identifiable pieces of information 4) Use misspelling (For example, Smith = Smyth = 5mYth) 5) Change passwords often 6) Don't leave password written on public devices Extra tips: On Cisco routers, leading spaces are ignored for passwords, but spaces after the first character are not. Therefore, one method to create a strong password is to use the space bar and create a phrase made of many words. This is called a passphrase. - easier to remember - longer and harder to guess	1) Encrypt all plaintext passwords with the service password-encryption command. 2) Set a minimum acceptable password length with the security passwords min-length command. 3) Deter brute-force password guessing attacks with the login block-for # attempts # within # command. 4) Disable an inactive privileged EXEC mode access after a specified amount of time with the exec-timeout command.	1) Configure a unique device hostname 2) Configure the IP domain name 3) Generate a key to encrypt SSH traffic 4) Verify or create a local database entry using the username global configuration command 5) Authenticate against the local database 6) Enable vty inbound SSH sessions	Any unnecessary services and applications should be turned off and uninstalled when possible Packet Tracer Configure Secure Passwords and SSH