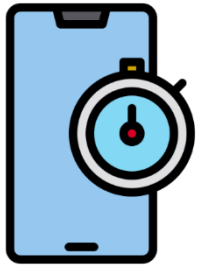
Network Security Fundamentals

Dmytro Zubov, PhD
dmytro.zubov@ucentralasia.org

Naryn, 5:36pm, December 6, 2022

Lessons learnt last time



- Application, Presentation, and Session: Explain how the functions of the application layer, presentation layer, and session layer work together to provide network services to end user applications
- Peer-to-Peer: Explain how end user applications operate in a peer-to-peer network
- Web and Email Protocols: Explain how web and email protocols operate
- IP Addressing Services: Explain how DNS and DHCP operate
- File Sharing Services: Explain how file transfer protocols operate

What we gonna discuss today?

- Security Threats and Vulnerabilities: Explain why basic security measure are necessary on network devices
- Network Attacks: Identify security vulnerabilities
- Network Attack Mitigation: Identify general mitigation techniques
- Device Security: Configure network devices with device hardening features to mitigate security threats

Security Threats and Vulnerabilities

- Security Threats and Vulnerabilities

Security Threats and Vulnerabilities

- Types of Threats

  - Attacks on a network can be devastating and can result in a loss of time and money due to damage, or theft of important information or assets. Intruders can gain access to a network through software vulnerabilities, hardware attacks, or through guessing someone's username and password. Intruders who gain access by modifying software or exploiting software vulnerabilities are called threat actors.

  - After the threat actor gains access to the network, four types of threats may arise:
    - Information Theft
    - Data Loss and manipulation
    - Identity Theft
    - Disruption of Service

Security Threats and Vulnerabilities

- Types of Vulnerabilities

  - Vulnerability is the degree of weakness in a network or a device. Some degree of vulnerability is inherent in routers, switches, desktops, servers, and even security devices. Typically, the network devices under attack are the endpoints, such as servers and desktop computers.

  - There are three primary vulnerabilities or weaknesses:

    ° **Technological Vulnerabilities** might include TCP/IP Protocol weaknesses, Operating System Weaknesses, and Network Equipment weaknesses

    ° **Configuration Vulnerabilities** might include unsecured user accounts, system accounts with easily guessed passwords, misconfigured internet services, unsecure default settings, and misconfigured network equipment

    ° **Security Policy Vulnerabilities** might include lack of a written security policy, politics, lack of authentication continuity, logical access controls not applied, software and hardware installation and changes not following policy, and a nonexistent disaster recovery plan

  - All three of these sources of vulnerabilities can leave a network or device open to various attacks, including malicious code attacks and network attacks

Network Attacks

- Network Attacks

Network Attacks

- Types of Malware

  - Malware is short for malicious software. It is code or software specifically designed to damage, disrupt, steal, or inflict “bad” or illegitimate action on data, hosts, or networks. The following are types of malware:

    ° **Viruses** - A computer virus is a type of malware that propagates by inserting a copy of itself into, and becoming part of, another program. It spreads from one computer to another, leaving infections as it travels.

    ° **Worms** - Computer worms are similar to viruses in that they replicate functional copies of themselves and can cause the same type of damage. In contrast to viruses, which require the spreading of an infected host file, worms are standalone software and do not require a host program or human help to propagate.

    ° **Trojan Horses** - It is a harmful piece of software that looks legitimate. Unlike viruses and worms, Trojan horses do not reproduce by infecting other files. They self-replicate. Trojan horses must spread through user interaction such as opening an email attachment or downloading and running a file from the internet.

Network Attacks

- Types of Malware (cont.)

Network Attacks

- Reconnaissance Attacks

  - In addition to malicious code attacks, it is also possible for networks to fall prey to various network attacks. Network attacks can be classified into three major categories:

    ° **Reconnaissance attacks** - The discovery and mapping of systems, services, or vulnerabilities

    ° **Access attacks** - The unauthorized manipulation of data, system access, or user privileges

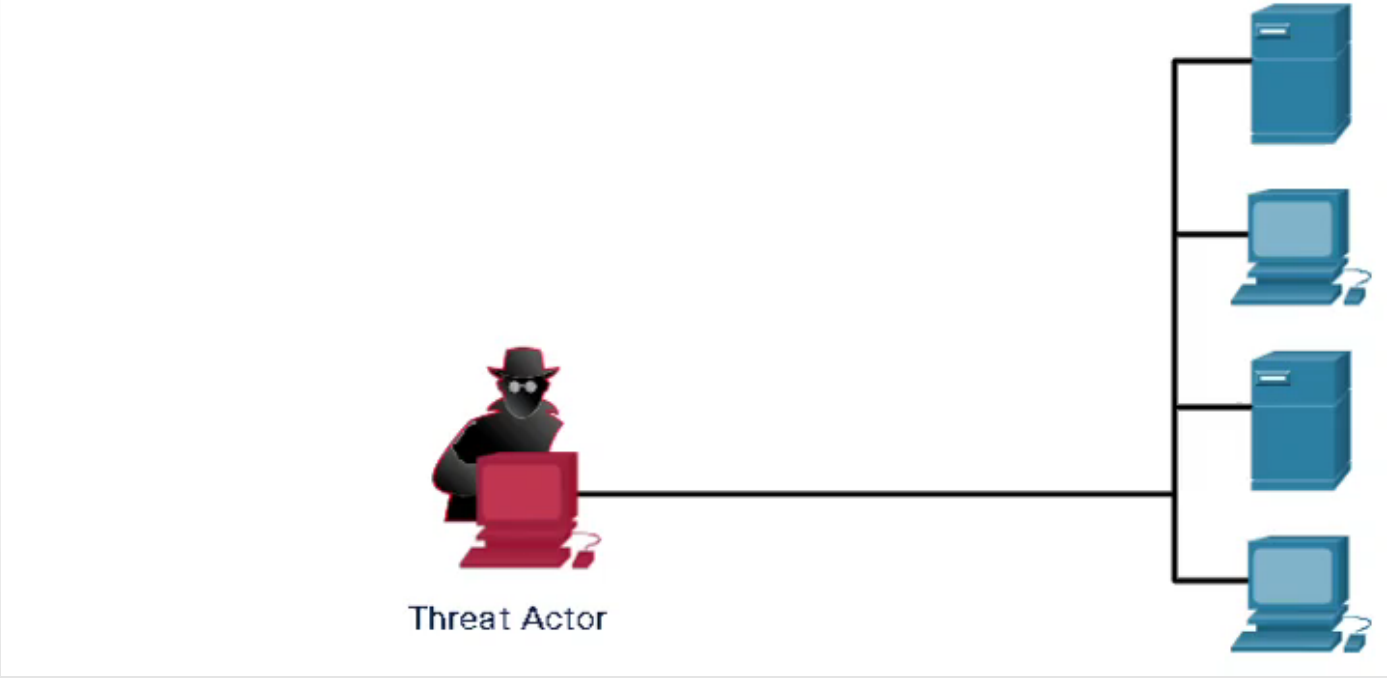
    ° **Denial of service** - The disabling or corruption of networks, systems, or services

  - For *reconnaissance attacks*, external threat actors can use internet tools, such as the **nslookup** and **whois** utilities, to easily determine the IP address space assigned to a given corporation or entity. After the IP address space is determined, a threat actor can then ping the publicly available IP addresses to identify the addresses that are active

Network Attacks

- Reconnaissance Attacks (cont.)

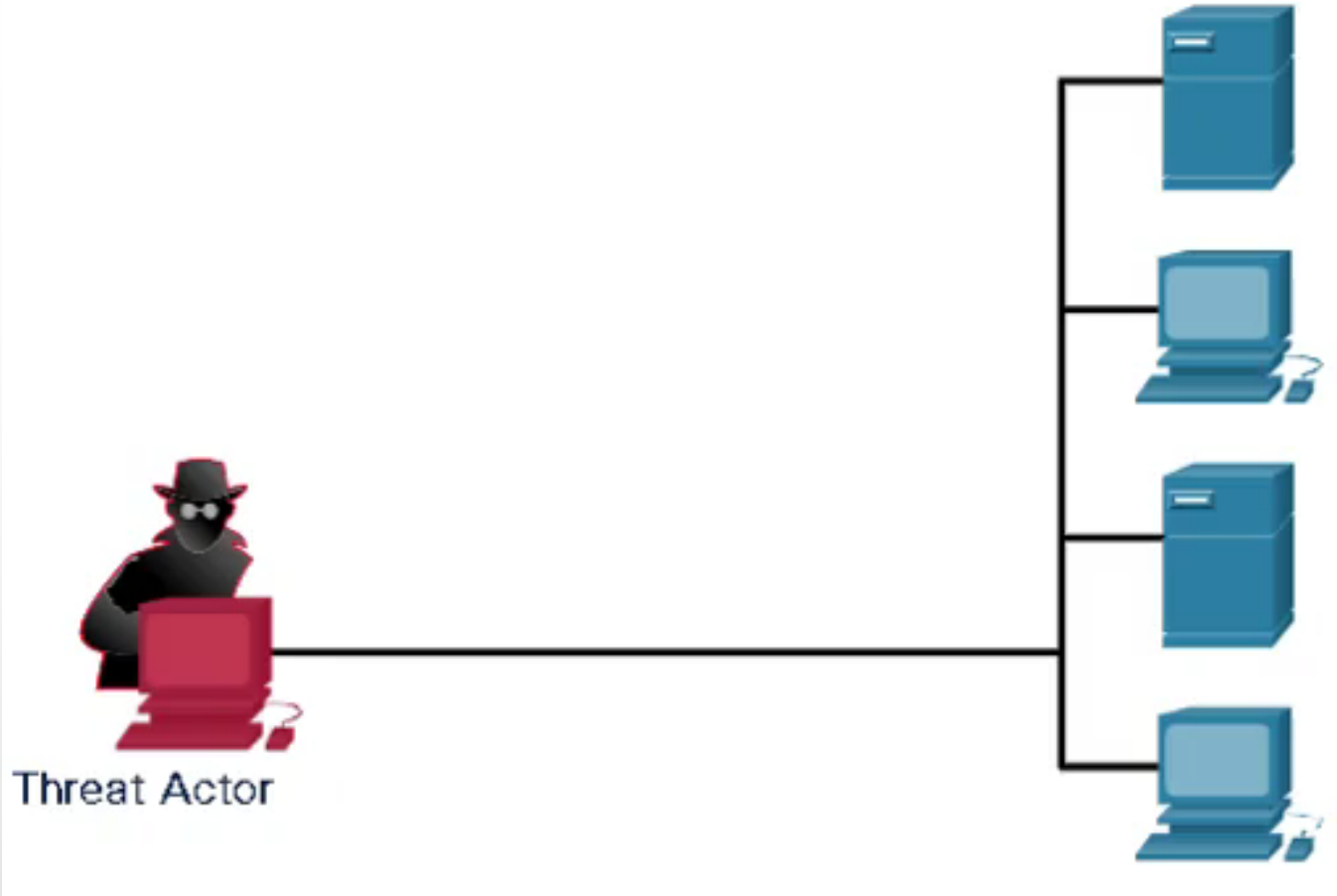
  - The threat actor is looking for initial information about a target. Various tools can be used, including Google search, the websites of organizations, whois, and more.



Network Attacks

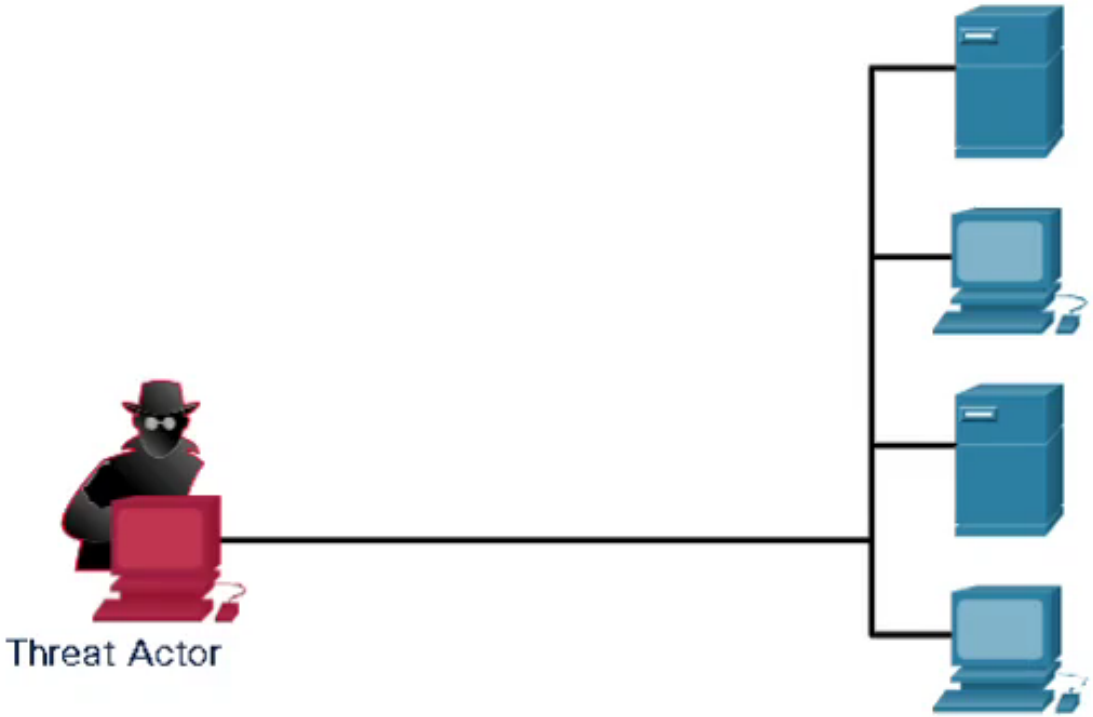
- Reconnaissance Attacks (cont.)

  - The threat actor initiates a ping sweep to determine which IP addresses are active.



Network Attacks

- Reconnaissance Attacks (cont.)
  - Threat actor performs a port scan on the discovered active IP addresses.



Network Attacks

- Access Attacks

  - Access attacks exploit known vulnerabilities in authentication services, FTP services, and web services to gain entry to web accounts, confidential databases, and other sensitive information

  - Access attacks can be classified into four types:

    ◦ **Password attacks** - Implemented using brute force, trojan horse, and packet sniffers

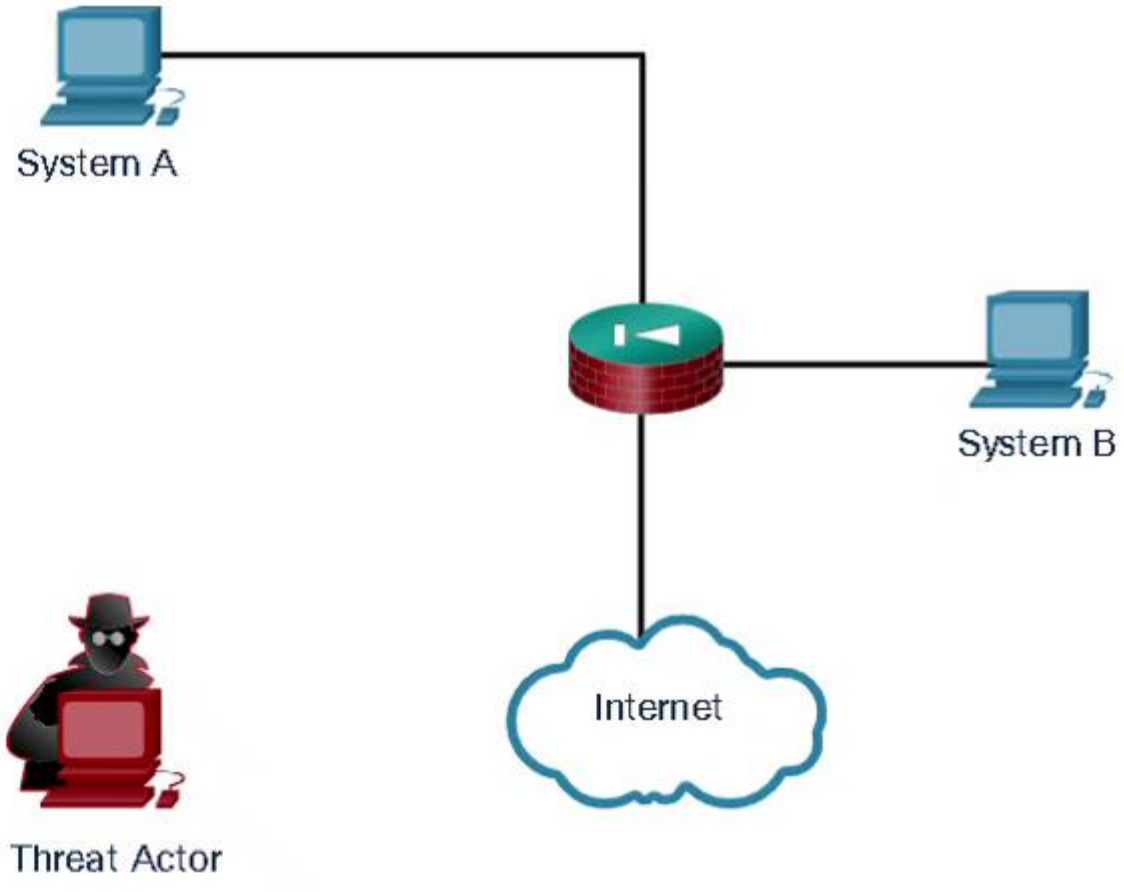
    ◦ **Trust exploitation** - A threat actor uses unauthorized privileges to gain access to a system, possibly compromising the target

    ◦ **Port redirection** - A threat actor 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.

    ◦ **Man-in-the middle** - The threat actor is positioned in between two legitimate entities in order to read or modify the data that passes between the two parties

Network Attacks

- Trust exploitation



Network Attacks

- Denial of Service Attacks

  - Denial of service (DoS) attacks are the most publicized form of attack and among the most difficult to eliminate. However, because of their ease of implementation and potentially significant damage, DoS attacks deserve special attention from security administrators.

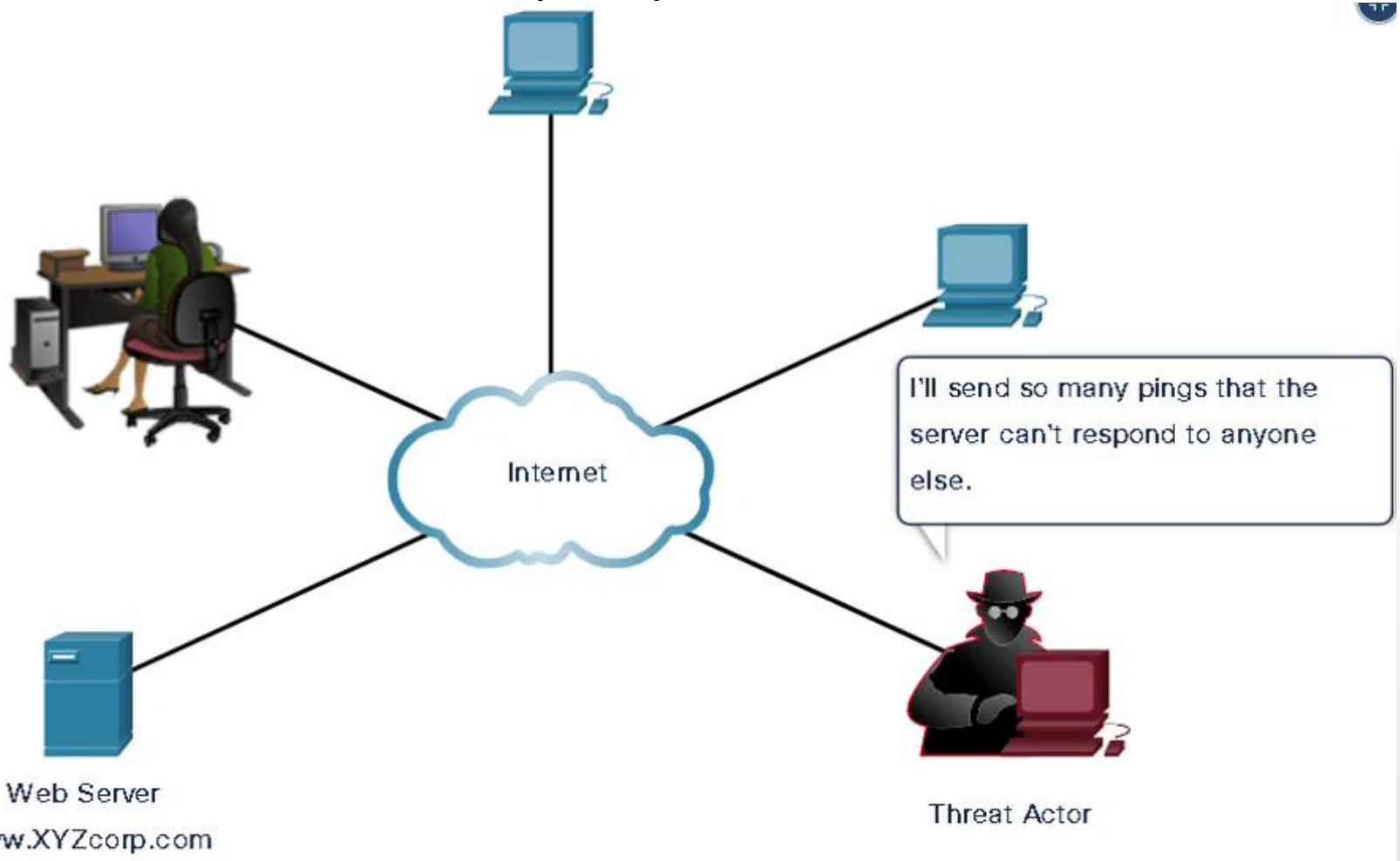
    ° DoS attacks take many forms. Ultimately, they prevent authorized people from using a service by consuming system resources. To help prevent DoS attacks it is important to stay up to date with the latest security updates for operating systems and applications.

    ° DoS attacks are a major risk because they interrupt communication and cause significant loss of time and money. These attacks are relatively simple to conduct, even by an unskilled threat actor.

    ° A DDoS is similar to a DoS attack, but it originates from multiple, coordinated sources. For example, a threat actor builds a network of infected hosts, known as zombies. A network of zombies is called a botnet. The threat actor uses a command and control (CnC) program to instruct the botnet of zombies to carry out a DDoS attack.

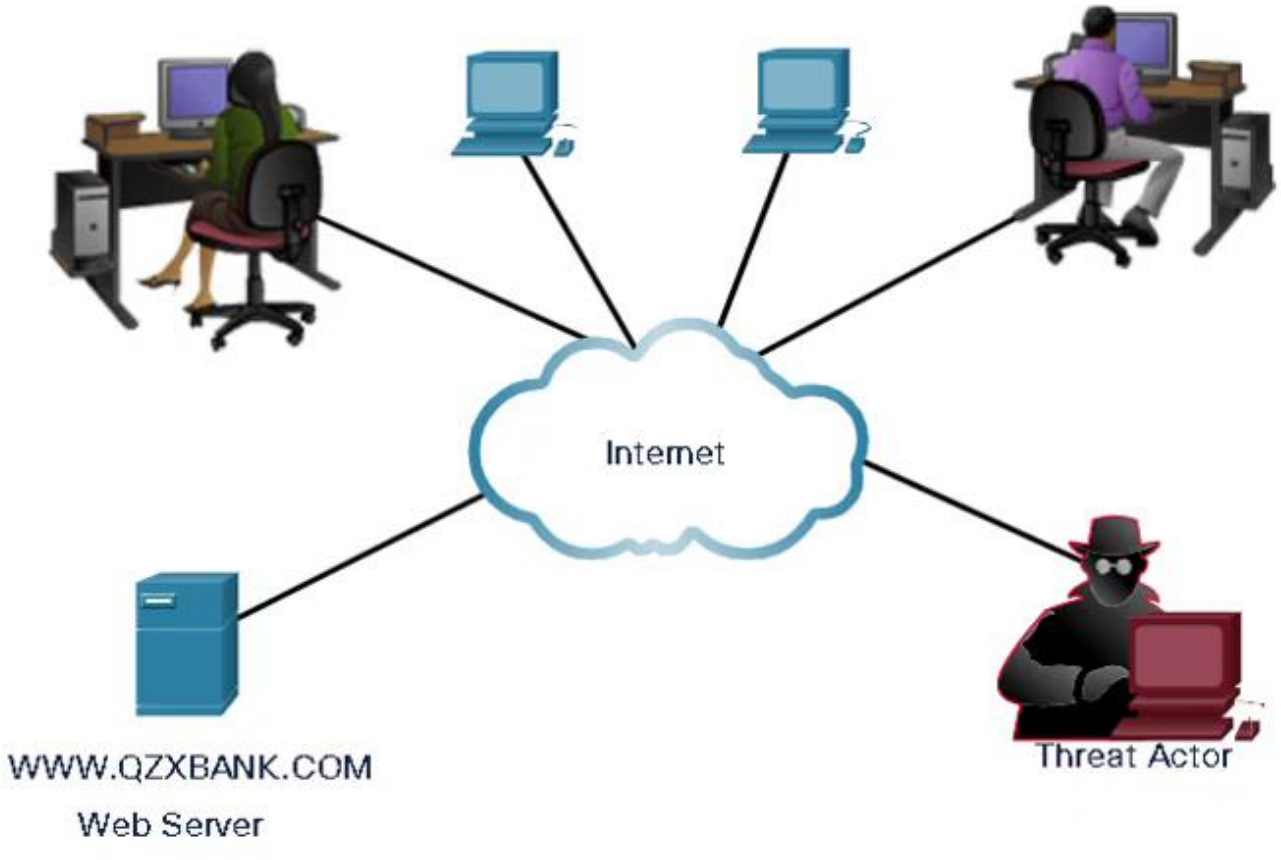
Network Attacks

- Denial of Service Attacks (DoS)



Network Attacks

- Distributed Denial of Service Attacks (DDoS)



Network Attack Mitigations

- Network Attack Mitigations

Network Attack Mitigations

- The Defense-in-Depth Approach

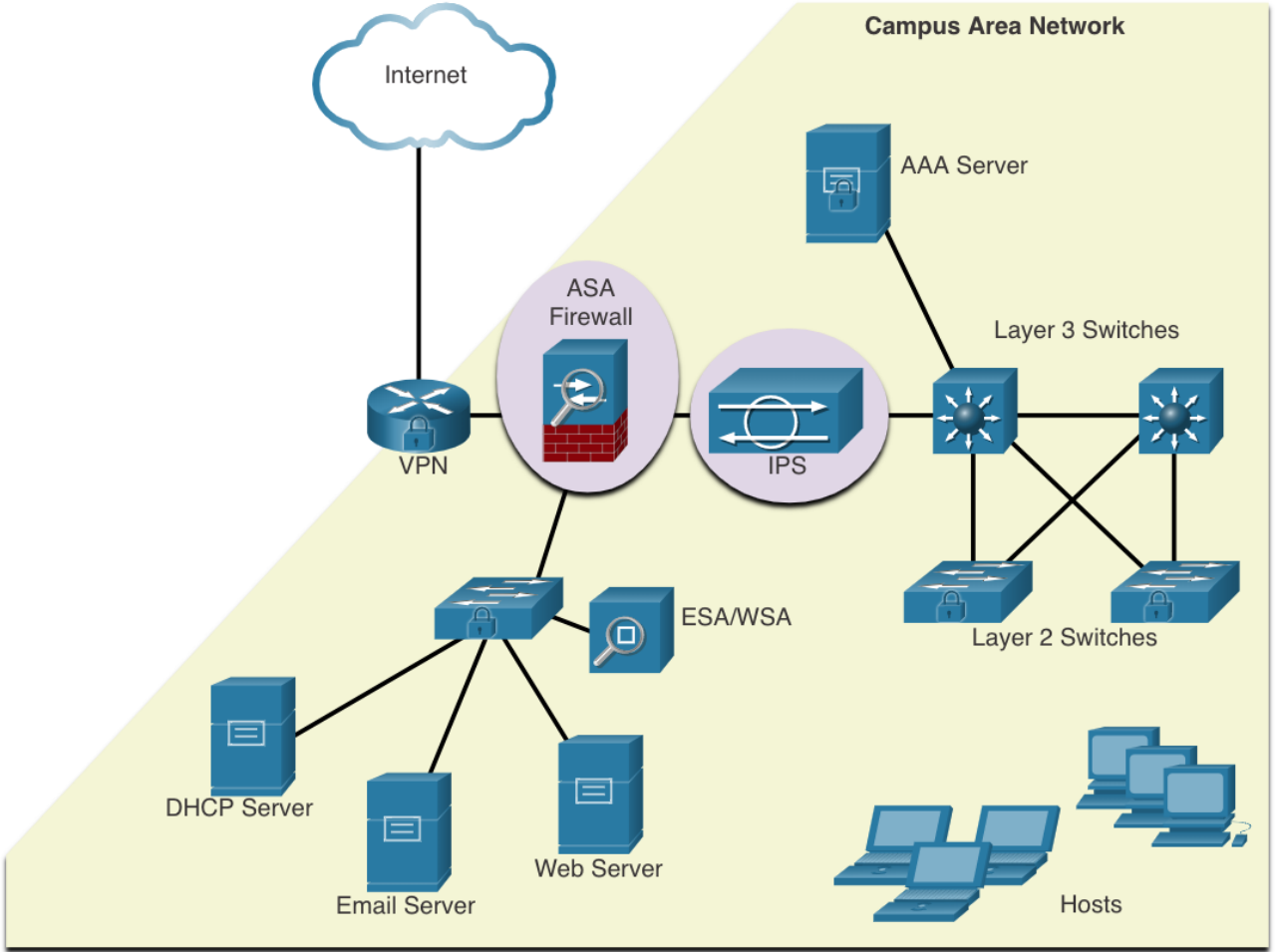
  - To mitigate network attacks, you must first secure devices including routers, switches, servers, and hosts. Most organizations employ a defense-in-depth approach (also known as a layered approach) to security. This requires a combination of networking devices and services working in tandem.

  - Several security devices and services are implemented to protect an organization's users and assets against TCP/IP threats:
    - VPN
    - ASA (Adaptive Security Appliance) Firewall
    - IPS (Intrusion Prevention Systems)
    - ESA/WSA (Email Security Appliance / Web Security Appliance)
    - AAA Server*

*AAA is a set of services for controlling access to computer resources, enforcing policies, assessing usage, and providing the information necessary to bill for services.

Network Attack Mitigations

- The Defense-in-Depth Approach (cont.)



Network Attack Mitigations

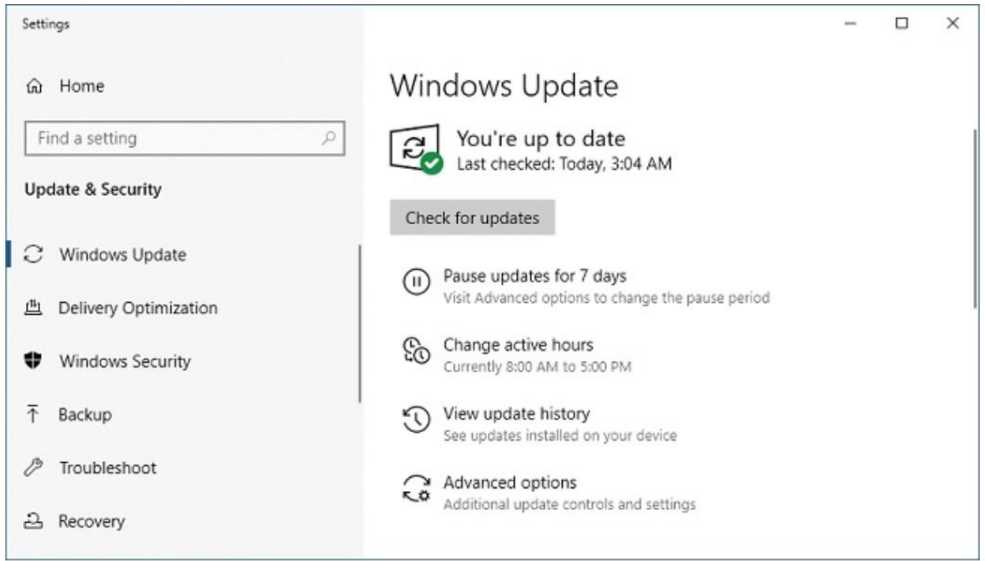
- Keep Backups

  - Backing up device configurations and data is one of the most effective ways of protecting against data loss. Backups should be performed on a regular basis as identified in the security policy. Data backups are usually stored offsite to protect the backup media if anything happens to the main facility.
  - The table shows backup considerations and their descriptions:

Consideration	Description
Frequency	•Perform backups on a regular basis as identified in the security policy •Full backups can be time-consuming, therefore perform monthly or weekly backups with frequent partial backups of changed files
Storage	•Always validate backups to ensure the integrity of the data and validate the file restoration procedures
Security	•Backups should be transported to an approved offsite storage location on a daily, weekly, or monthly rotation, as required by the security policy
Validation	•Backups should be protected using strong passwords. The password is required to restore the data

Network Attack Mitigations

- Upgrade, Update, and Patch
  - As new malware is released, enterprises need to keep current with the latest versions of antivirus software
    - The most effective way to mitigate a worm attack is to download security updates from the operating system vendor and patch all vulnerable systems
    - One solution to the management of critical security patches is to make sure all end systems automatically download updates



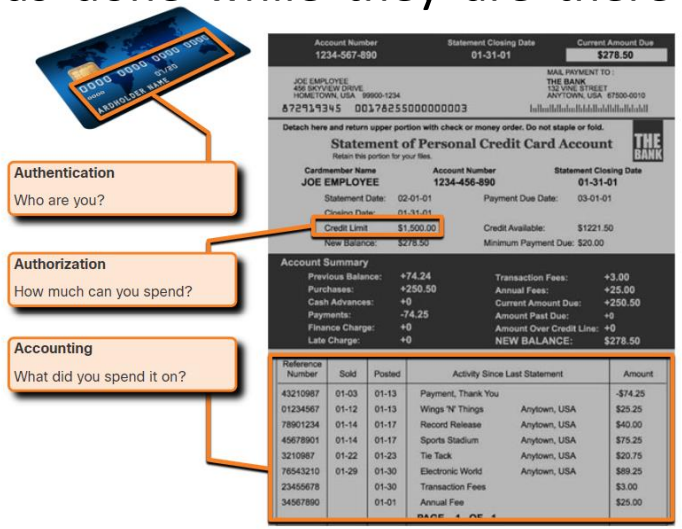
Network Attack Mitigations

- Authentication, Authorization, and Accounting

  - Authentication, authorization, and accounting (AAA, or “triple A”) network security services provide the primary framework to set up access control on network devices

    - AAA is a way to control who is permitted to access a network (authenticate), what actions they perform while accessing the network (authorize), and making a record of what was done while they are there (accounting)

    - The concept of AAA is similar to the use of a credit card. The credit card identifies who can use it, how much that user can spend, and keeps account of what items the user spent money on



Network Attack Mitigations

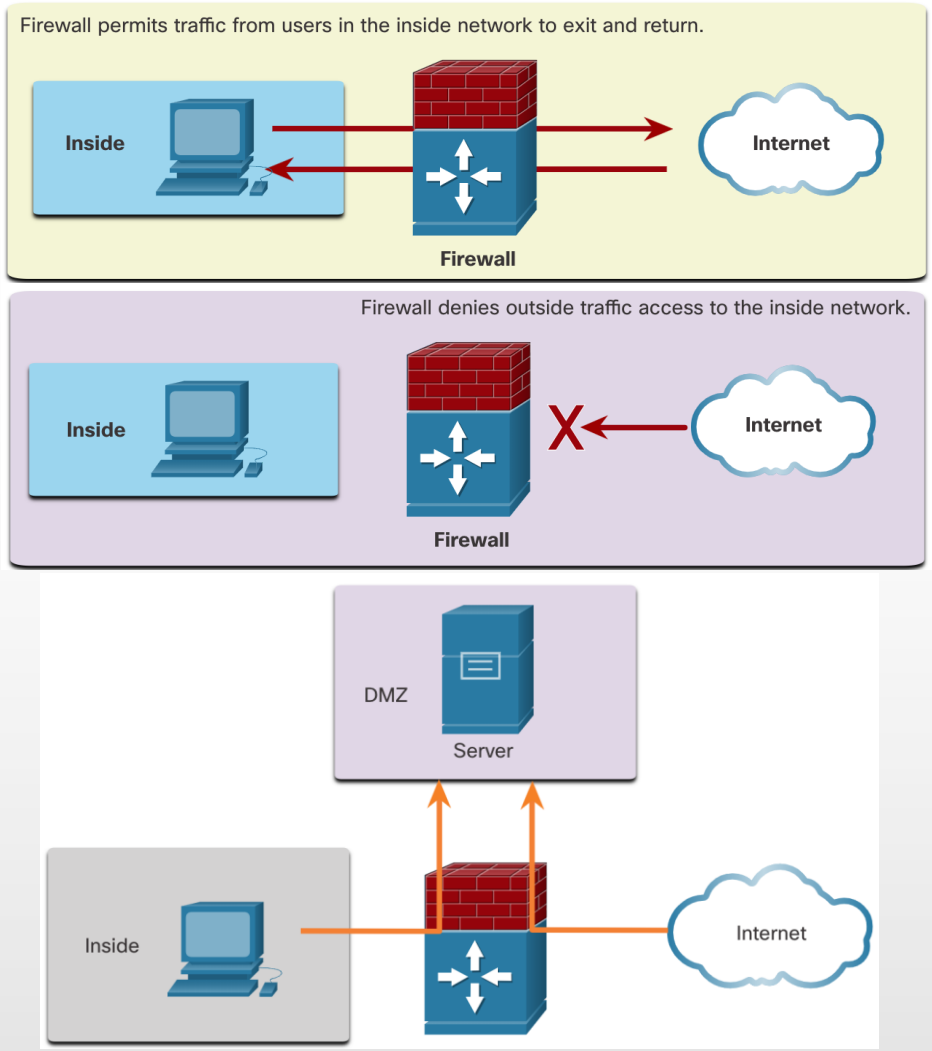
- Firewalls

  - Network firewalls reside between two or more networks, control the traffic between them, and help prevent unauthorized access

  - A firewall could allow outside users controlled access to specific services. For example, servers accessible to outside users are usually located on a special network referred to as the demilitarized zone (DMZ). The DMZ enables a network administrator to apply specific policies for hosts connected to that network.

Network Attack Mitigations

- Firewalls



Network Attack Mitigations

- Types of Firewalls

  - Firewall products come packaged in various forms. These products use different techniques for determining what will be permitted or denied access to a network. They include the following:

    - **Packet filtering** - Prevents or allows access based on IP or MAC addresses
    - **Application filtering** - Prevents or allows access by specific application types based on port numbers
    - **URL filtering** - Prevents or allows access to websites based on specific URLs or keywords
    - **Stateful packet inspection (SPI)** - Incoming packets must be legitimate responses to requests from internal hosts. Unsolicited packets are blocked unless permitted specifically. SPI can also include the capability to recognize and filter out specific types of attacks, such as denial of service (DoS).

Network Attack Mitigations

- Endpoint Security

  - An endpoint, or host, is an individual computer system or device that acts as a network client. Common endpoints are laptops, desktops, servers, smartphones, and tablets.

  - Securing endpoint devices is one of the most challenging jobs of a network administrator because it involves human nature. A company must have well-documented policies in place and employees must be aware of these rules.

  - Employees need to be trained on proper use of the network. Policies often include the use of antivirus software and host intrusion prevention. More comprehensive endpoint security solutions rely on network access control.

Device Security

- Device Security

Device Security

- Cisco AutoSecure

  - The security settings are set to the default values when a new operating system is installed on a device. In most cases, this level of security is inadequate. For Cisco routers, the Cisco AutoSecure feature can be used to assist securing the system.
  - In addition, there are some simple steps that should be taken that apply to most operating systems:
    - ° Default usernames and passwords should be changed immediately
    - ° Access to system resources should be restricted to only the individuals that are authorized to use those resources
    - ° Any unnecessary services and applications should be turned off and uninstalled when possible
    - ° Often, devices shipped from the manufacturer have been sitting in a warehouse for a period of time and do not have the most up-to-date patches installed. It is important to update any software and install any security patches prior to implementation.

Device Security

- Passwords

- To protect network devices, it is important to use strong passwords. Here are standard guidelines to follow:
  - Use a password length of at least eight characters, preferably 10 or more characters
  - Make passwords complex. Include a mix of uppercase and lowercase letters, numbers, symbols, and spaces, if allowed
  - Avoid passwords based on repetition, common dictionary words, letter or number sequences, usernames, relative or pet names, biographical information, such as birthdates, ID numbers, ancestor names, or other easily identifiable pieces of information
  - Deliberately misspell a password. For example, Smith = Smyth = 5mYth or Security = 5ecur1ty.
  - Change passwords often. If a password is unknowingly compromised, the window of opportunity for the threat actor to use the password is limited.
  - Do not write passwords down and leave them in obvious places such as on the desk or monitor
- 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. A passphrase is often easier to remember than a simple password. It is also longer and harder to guess.

Device Security

- Additional Password Security

  - There are several steps that can be taken to help ensure that passwords remain secret on a Cisco router and switch including these:

    - Encrypt all plaintext passwords with the **service password-encryption** command
    - Set a minimum acceptable password length with the **security passwords min-length** command
    - Deter brute-force password guessing attacks with the **login block-for # attempts # within #** command
    - Disable an inactive privileged EXEC mode access after a specified amount of time with the **exec-timeout** command

Device Security

- Additional Password Security (cont.)

```
Router(config)# service password-encryption
Router(config)# security password min-length 8
Router(config)# login block-for 120 attempts 3 within 60
Router(config)# line vty 0 4
Router(config-line)# password cisco
Router(config-line)# exec-timeout 5 30
Router(config-line)# transport input ssh
Router(config-line)# end
Router#
Router# show running-config | section line vty
line vty 0 4
 password 7 03095A0F034F
 exec-timeout 5 30
 login
Router#
```

Device Security

- Enable SSH

  - It is possible to configure a Cisco device to support SSH using the following steps:

    1. **Configure a unique device hostname**. A device must have a unique hostname other than the default.
    2. **Configure the IP domain name.** Configure the IP domain name of the network by using the global configuration mode command **ip-domain name**.
    3. **Generate a key to encrypt SSH traffic.** SSH encrypts traffic between source and destination. However, to do so, a unique authentication key must be generated by using the global configuration command **crypto key generate rsa general-keys modulus** bits. The modulus bits determines the size of the key and can be configured from 360 bits to 2048 bits. The larger the bit value, the more secure the key. However, larger bit values also take longer to encrypt and decrypt information. The minimum recommended modulus length is 1024 bits.
    4. **Verify or create a local database entry**. Create a local database username entry using the **username** global configuration command.
    5. **Authenticate against the local database.** Use the **login local** line configuration command to authenticate the vty line against the local database.
    6. **Enable vty inbound SSH sessions.** By default, no input session is allowed on vty lines. You can specify multiple input protocols including Telnet and SSH using the **transport input [ssh | telnet]** command.

Device Security

- Disable Unused Services

  - Cisco routers and switches start with a list of active services that may or may not be required in your network. Disable any unused services to preserve system resources, such as CPU cycles and RAM, and prevent threat actors from exploiting these services.

    ° The type of services that are on by default will vary depending on the IOS version. For example, IOS-XE typically will have only HTTPS and DHCP ports open. You can verify this with the **show ip ports all** command.

    ° IOS versions prior to IOS-XE use the **show control-plane host open-ports** command

Do you have any questions or comments?

Thank you
for your attention !

In this presentation:

- Some icons were downloaded from flaticon.com and iconscout.com