CISCO

Principles of Cyber Security

Attackers and Their Tools

Who is Attacking Our Network?

In this presentation we will investigate Threat, Vulnerability, and Risk

- Threat
  - Is a potential danger to an asset such as data or the network.
- Vulnerability and Attack Surface
  - A vulnerability is a weakness in a system or its design that could be exploited by a threat.
  - Attack surface describes different points where an attacker could get into a system and could get to the data (Example – operating system without security patches)
- Exploit
  - Is a mechanism used to leverage a vulnerability to compromise an asset.
  - A Remote exploit works over the network.
  - A Local exploit is when a threat actor has user or administrative access to the end system.
- Risk
  - Likelihood that a threat will exploit a vulnerability of an asset and result in an undesirable consequence.

What exactly are Hackers? Hacker vs. Threat Actor

- White Hat Hackers
  - Ethical hackers who use their programming skills for good, ethical, and legal purposes.
  - Perform penetration tests to discover vulnerabilities and work with developers to address cyber issues
- Grey Hat Hackers
  - Commit crimes and do unethical things but not for personal gain or to cause damage.
- Black Hat Hackers
  - Unethical criminals who violate security for personal gain, or for malicious reasons, such as attacking networks.

It is important to note: **Threat actors** is a term used to describe grey and black hat hackers.

Evolution of Threat Actors

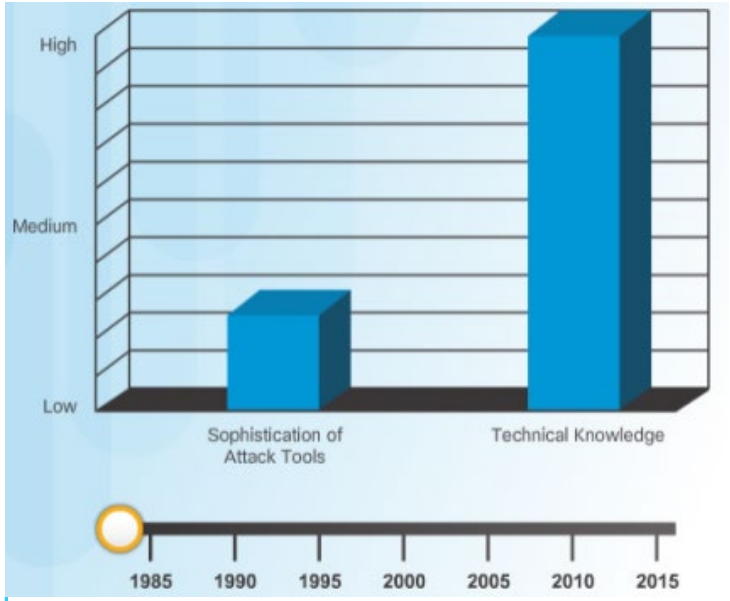
- Script Kiddies (began around the 1980s)
  - Inexperienced hackers running existing tools and exploits to cause harm, but typically not for profit.
- State-Sponsored
  - White or black hats who steal government secrets, gather intelligence, and sabotage networks.
  - Targets are typically foreign governments, terrorist groups, and corporations.
- Cybercriminals
  - Black hat threat actors that steal billions of dollars from consumers and businesses.
- Hacktivists
  - Grey hats who rally and protest against political and social ideas.
  - Post articles and videos to leak sensitive information. Sometimes they deface websites
- Vulnerability Broker
  - Discover exploits and report them to vendors, sometimes for prizes or rewards.

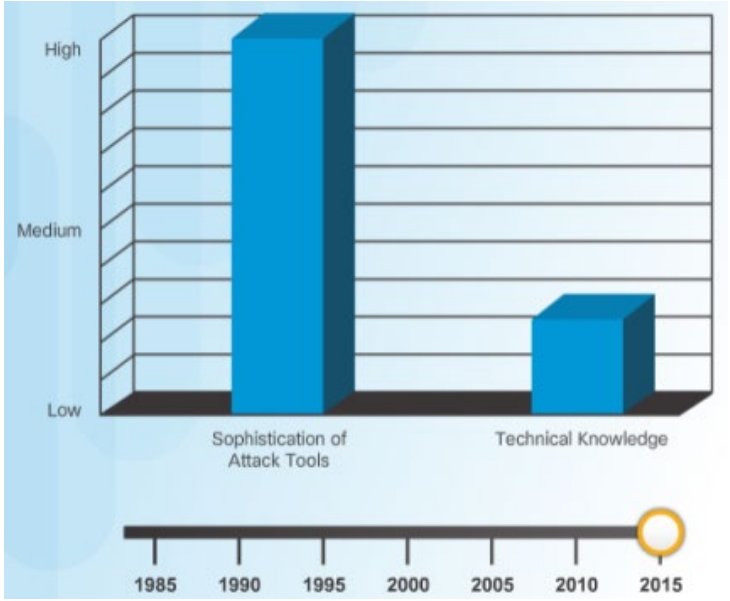
Cybersecurity Tasks – How do we protect against attacks

- Develop good cybersecurity awareness.
- Report cybercrime to authorities.
- We must aware of potential threats in email and web
- Guard important information from theft.
- Organizations must take action and protect their assets, users, and customers.
- Develop cybersecurity tasks and implement those tasks on a reoccurring basis.

Introduction of Attack Tools

- Attackers use tools to exploit a vulnerability.
- Sophistication of attack tools and technical knowledge to conduct attacks has changed since 1985.





Categories of Attacks

Common Categories of Network Attacks

- **Eavesdropping** – essentially captures and listen to network traffic.
- **Data modification** - alters the captured data in a *packet* in the data stream without the knowledge of the sender or receiver. (FYI- A network packet is a formatted unit of data carried by a packet-switched network)
- **IP address spoofing** – this constructs an IP packet that appears to originate from a valid address inside the corporate intranet.
- **Password-based** - uses the stolen valid accounts to obtain lists of other users and network information.
- **Denial-of-Service** - prevents normal use of a computer or network by valid users.
- **Man-in-the-Middle** - hackers position themselves between a source and destination to monitor, capture and control communication.
- **Compromised-Key** – essentially gaining access to a secured communication by obtaining the secret encryption key.
- **Sniffer** - an application or device that can read, monitor, and capture network data.

Common Threats and Attacks

What are the types of Malware?

- The term Malware is short for malicious software or malicious code.
  - Specifically designed to damage, disrupt, steal or inflict illegitimate action on data hosts or networks.

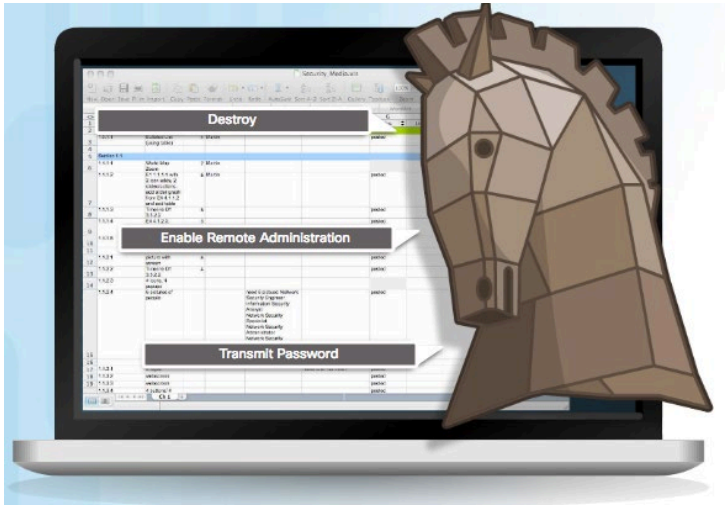
What are Viruses?

- Viruses are a type of malware that propagates by inserting a copy of itself into another program.
- Spread from one computer to another, infecting multiple computers.
- Spread by USB memory drives, CDs, DVDs, network shares and email.
- Viruses can lay dormant and activate at a specific time and date.
- Viruses require human action to insert malicious code into another program.
- Execute a specific often harmful function on a computer.
- **This is why we run anti-virus software on our computers to avoid these viral infections**

Trojan Horses

- This is malicious code that's designed to look legitimate.
- Its often found attached to online games.
- It is a non-replicating type of malware.
- Exploits the privileges of the user that runs the malware.
- Can cause immediate damage, provide remote access to the system, or access to a system through a back door.

Trojan Horse Classification

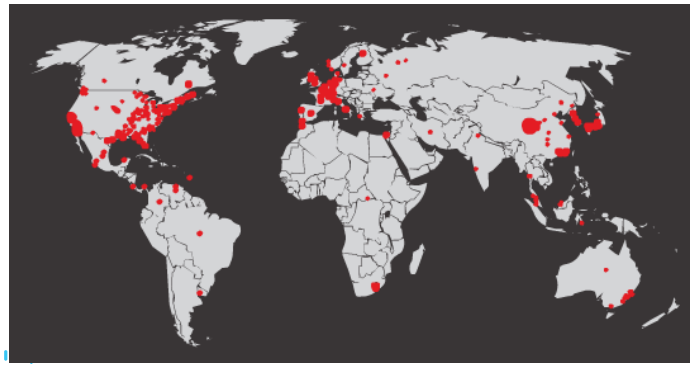


- **Remote-access Trojan horse** - Enables unauthorized remote access.
- **Data-sending Trojan horse** - Provides the threat actor with sensitive data, such as passwords.
- **Destructive Trojan horse** - Corrupts or deletes files.
- **Proxy Trojan horse** - This will use the victim's computer as the source device to launch attacks and perform other illegal activities.
- **FTP Trojan horse** - Enables unauthorized file transfer services on end devices.
- **Security software disabler Trojan horse** - Stops antivirus programs or firewalls from even functioning.
- **DoS Trojan horse** - Slows or halts network activity.

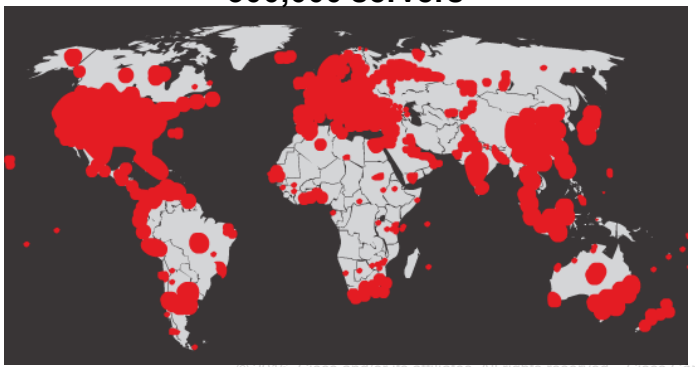
Worms

- A worm executes arbitrary code and installs itself in the memory of the infected device.
- Automatically replicates itself and spreads across the network from system to system.
- Components of a worm attack include an exploiting vulnerability, delivering a malicious payload, and self-propagation.
- Unlike viruses, however, worms can run by themselves without any human intervention

As an example in 2001, the Code Red Worm was launched against 658 servers

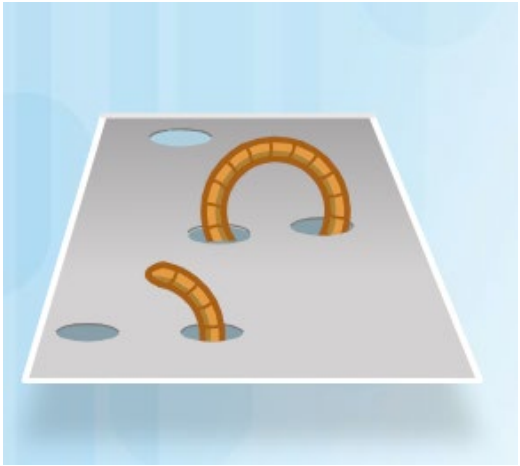


Code Red Worm Infection– 19 Hours Later 300,000 servers



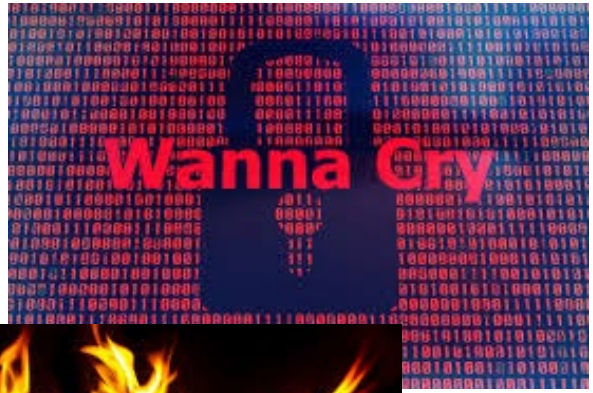
Worm Components

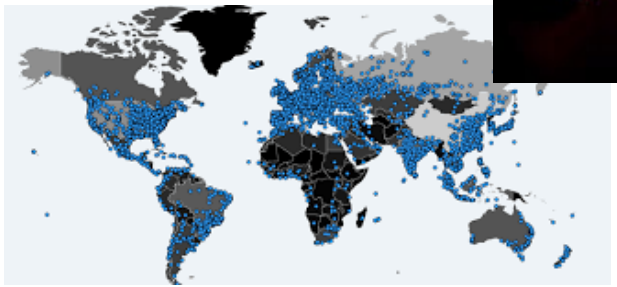
- A worm attack consists of three components:
  - **Enabling vulnerability** - A worm installs itself using an exploit mechanism, such as an email attachment, an executable file, or a Trojan horse, on a vulnerable system.
  - **Propagation mechanism** - After gaining access to a device, the worm replicates itself and locates new targets..
  - **Payload** - Any malicious code that results in some action is a payload which is used to create a backdoor that allows a threat actor access to the infected host, or to create a DoS attack.



As an example of a worm

The **WannaCry** ransomware attack was a May 2017 worldwide cyberattack by the WannaCry ransomware cryptoworm. It targeted computers running the Microsoft Windows operating system by encrypting data and demanding ransom payments in Bitcoin cryptocurrency.





Ransomware

- Malware that denies access to the infected computer system or its data.
- Cybercriminals demand payment to release the computer system.
- Frequently, ransomware uses an encryption algorithm to encrypt system files and data and cannot be decrypted.
- Email and malicious advertising are vectors for ransomware campaigns.
- Social engineering is also used. As an example, would be cybercriminals who identify themselves as security technicians call homes and persuade users to connect to a website that downloads the ransomware to the user's computer.

This is an example screen capture of a computer that has been encrypted with Ransomware. The next step would be to send the threat actors money in the form of Bitcoin to unlock your files.

Other Malware

- Other Modern Malware includes:
  - **Spyware** - Used to gather information about a user and send the information to another entity without the user's consent. Can be a system monitor, Trojan horse, Adware, tracking cookies, or key loggers.
  - **Adware** - Typically displays annoying pop-ups to generate revenue for its author. It may analyze user interests by tracking the websites visited and send pop-up advertising pertinent to those sites.
  - **Scareware** - Includes scam software which uses social engineering to shock or induce anxiety by creating the perception of a threat. It attempts to persuade the user to infect their computer by taking action to address that threat. An example may include a pop-up that notifies the user they are being monitored by the FBI and have visited illegal websites and must pay an online fine, or be arrested.
  - **Phishing** - Attempts to convince people to divulge sensitive information. Examples include receiving an email from their bank asking users to divulge their account and PIN numbers.
  - **Rootkits** - Installed on a compromised system. After its installed, it continues to hide its intrusion and provide privileged access to the threat actor.

Common Malware Behaviors, how do I know if my computer is infected:

- Computers infected with malware often exhibit one or more of the following:
  - Appearance of strange files, programs, or desktop icons.
  - Antivirus and firewall programs are turning off or reconfiguring settings.
  - Computer screen is freezing or system crashing.
  - Emails are spontaneously being sent without your knowledge to your contact list.
  - Files that have been modified or deleted.
  - Increased CPU and/or memory usage. An example includes threat actors using your computer to mine cryptocurrency without your knowledge
  - Problems connecting to networks.
  - Slow computer or web browser speeds.
  - Unknown processes or services running.
  - Connections are made to hosts on the Internet without user action.
  - Strange computer behavior.

Tips on Securing Your Computer

- Use a firewall
- Install antivirus software
- Install an anti-spyware package
- Use complex passwords
- Keep your OS, apps and browser up to date
- Ignore spam
- Back up your computer
- Shut your device down if not in use
- Use virtualization (If needed)
- Use two-factor authentication
- Use encryption

What are the Types of Network Attacks?

- Attacks are typically classified in three major categories:

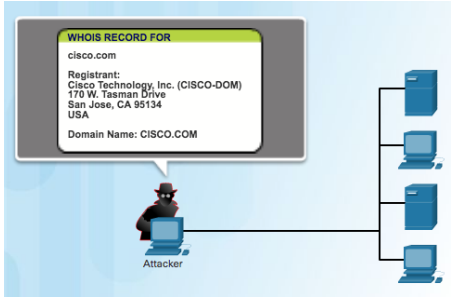
- By categorizing network attacks, it is possible to address types of attacks rather than individual attacks.

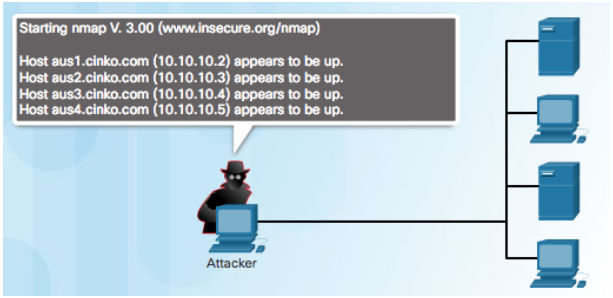
Reconnaissance Attacks

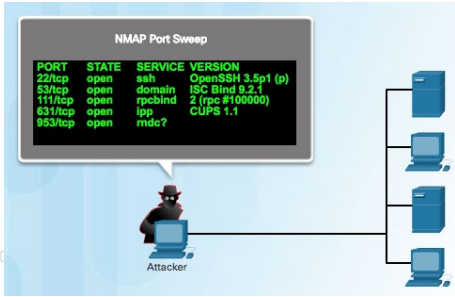
- They are also known as information gathering, reconnaissance attacks that perform unauthorized discovery and mapping of systems, services, or vulnerabilities.
- They are similar to a thief surveying a neighborhood by going door-to-door pretending to sell something.
- These Recon attacks precede intrusive access attacks, or DoS attacks and employ the use of widely available malware tools.

As an Example of a Reconnaissance Attack

- **First, the attacker performs an information query of a target.** The threat actor is looking for initial information about a target. Tools: Google search, public information from DNS registries using various opensource tools. (dig, nslookup, and whois)
- **The threat actor then initiates a ping sweep** of the target networks and identifies which IP addresses are active.
- **The threat actor also initiates port scans** on hosts identified by the ping sweep, to determine which ports or services are available.



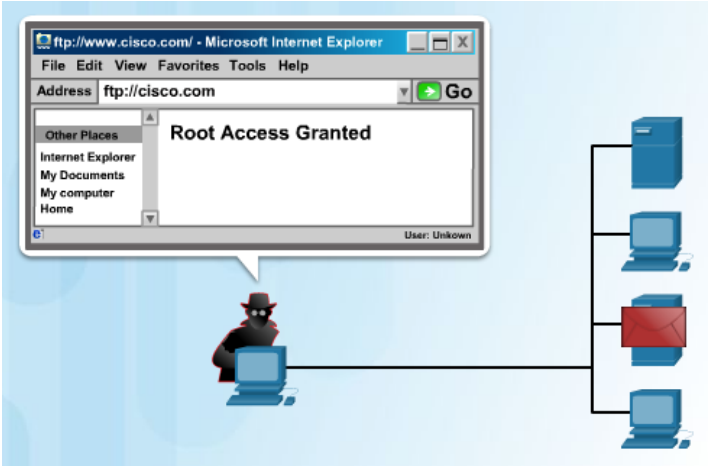




Access Attacks

- Access attacks exploit vulnerabilities in authentication services, FTP services, and web services to retrieve data, gain access to systems, or to escalate access privileges.

- There are at least three reasons that threat actors would use access attacks on networks or systems:
  - To retrieve data
  - To gain access to systems
  - To escalate access privileges



Types of Access Attacks

- **Password attack** - Threat actors attempt to discover critical system passwords using phishing attacks, dictionary attacks, brute-force attacks, network sniffing, or using social engineering techniques.
- **Hash Attacks** - Attackers gain access to the user's machine and uses malware to access the stored password hashes. In a Windows OS the passwords are stored in a hash value (output of a hashing algorithm like MD5, or SHA).
- **Trust exploitation** - Hackers use a trusted host to gain access to network resources.
- **Port redirection** - Uses a compromised system as a base for attacks against other targets.
- **Man-in-the-middle attack** - Threat actors are positioned in between two legitimate entities in order to read, modify, or redirect the data that passes between the two parties.
- **IP, MAC, DHCP Spoofing** - One device attempts to pose as another by falsifying address data.

Social Engineering Attacks

- This is an attack that attempts to manipulate individuals into performing actions or divulging confidential information needed to access a network.
  - Examples of social engineering attacks include:
    - **Pretexting** - An attacker calls an individual and lies to them in an attempt to gain access to privileged data.
    - **Spam** - The attacker uses spam email to trick a user into clicking an infected link, or downloading an infected file.
    - **Phishing** - The threat actor sends enticing custom-targeted spam email to individuals with malicious links.
    - **Something for Something (Quid pro quo)** - The attacker requests personal information from a party in exchange for something, like a free gift.
    - **Tailgating** - The attackers follows an authorized person with a corporate badge into secure location.
    - **Visual hacking** – The attacker physically observes the victim entering credentials such as a workstation login, or an ATM PIN. Also known as “shoulder surfing”.
    - **Baiting** - Threat actor leaves a malware-infected physical device, such as a CD disk in a public location such as a corporate breakroom. Example: An individual walks in and sees a CD lying on a counter with the words, pictures from Vegas trip, written on it. They drop it into their disk drive to see who in the office went to Vegas, and bam their computer is infected.

Phishing Attacks

- Phishing
  - This is a common social engineering technique that threat actors use to send emails that appear to be from a legitimate organization (such as a bank)
  - Variations include:
    - **Spear phishing** - Targeted phishing attack tailored for a specific individual or organization.
    - **Whaling** – Similar to spear phishing but is focused on big targets such as top executives of an organization.
    - **Watering hole** – The attacker determines websites that a target group visits regularly and attempts to compromise those websites by infecting them with malware
    - **Vishing** – Phishing attack using voice and the phone system instead of email.
    - **Smishing** – Phishing attack using SMS texting instead of email.

An Example of a Spear-Phishing Attack:

In March 2016, the personal Gmail account of John Podesta, a former White House chief of staff was compromised in a data breach via a spear-phishing attack. Experts believe the Russian cyber group named Fancy Bear, which is a unit of the Russian military intelligence agency launched the attack.

Mr. Podesta used a Gmail account to handle all of his email, this email account had approximately 10 years of business and personal messages in it.

This is a screen shot of the actual spear-phishing email that John Podesta received. It says, someone just used your password to try to sign into a Google account and Google was able to stop this sign in attempt. You should change your password immediately, and it gave him a malicious change password link. It was not a Google link, but a shortened bit.ly link.

John Podesta's administrative assistant sent the email to the IT department because it was suspected of being fake. An IT employee send a response that the Google email was "legitimate" but later said he meant to write "illegitimate. Mr. Podesta was told he needed to change his password immediately and initiate two-factor authentication at Google.com.

Instead of going to Google.com, Mr. Podesta went back to his original email and clicked the link that was provided by the hackers which immediately unlocked 10 years of his emails.

All of those emails were later made available on Wikileaks.

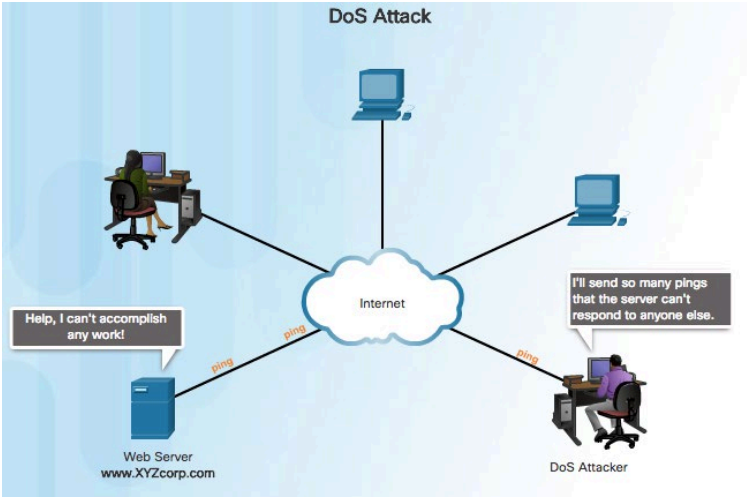
Source: Wikipedia

Strengthening the Weakest Link

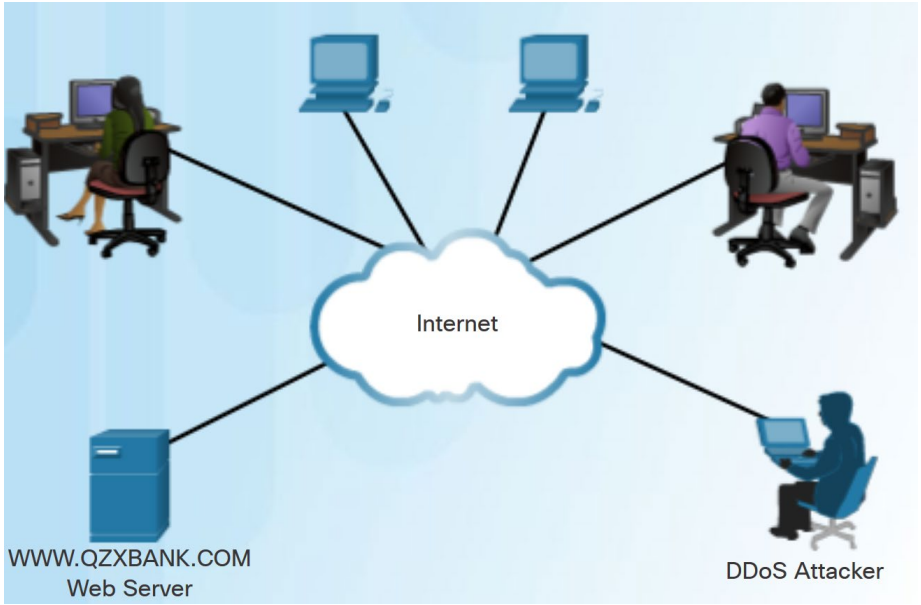
- People are typically the weakest link in cybersecurity. This is why social engineering attacks are so successful.
- Organizations must actively train their personnel and create a “security-aware culture.”

Denial of Service Attacks (DoS attack or DDoS attack)

- Typically result in some sort of interruption of service to users, devices, or applications.
- Can be caused by overwhelming a target device with a large quantity of traffic or by using incorrectly formatted packets.
- A threat actor forwards packets containing errors that cannot be identified by the application, or forwards improperly formatted packets.



Example Distributed DoS Attack



1. The threat actor builds or purchases a botnet of zombie hosts.

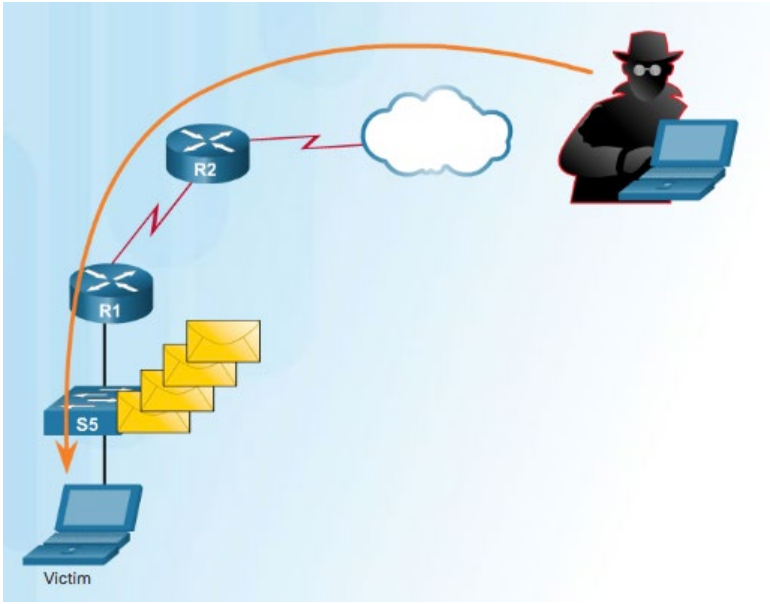
2. Zombie computers continue to scan and infect more targets to create more zombies.

3. When ready, the botmaster uses the handler systems to make the botnet of zombies carry out the DDoS attack on the chosen target.

4. The targets systems are overwhelmed causing an interruption in service

Buffer Overflow Attack

- The goal is to find a system memory-related flaw on a server and exploit it.
- Exploiting the buffer memory by overwhelming it with unexpected values usually renders the system inoperable.
- For example:
  - A threat actor enters input into a data field that is larger than expected by the application running on a server.
  - The application accepts the large amount of input and stores it in memory.
  - It consumes the memory buffer and potentially overwrites adjacent memory, eventually corrupting the system and causing it to crash.

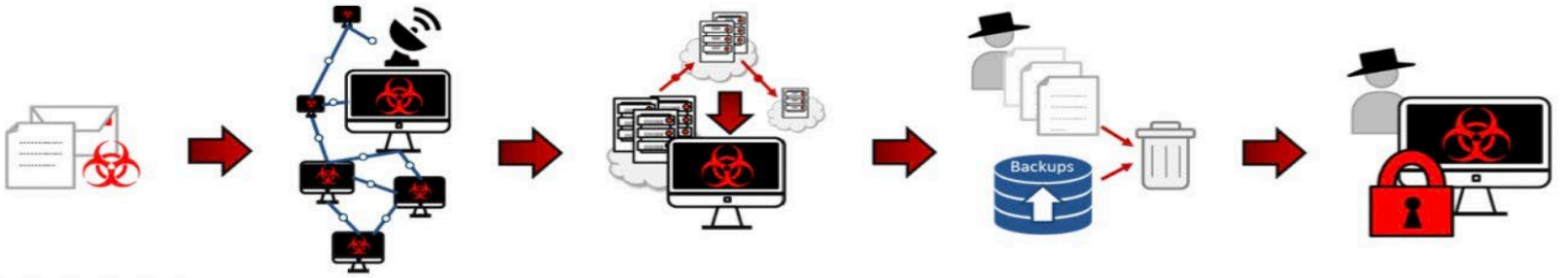


Evasion Methods

- Threat actors learned long ago that malware and attack methods are most effective when they are undetected.
- New attack and evasion methods are constantly being developed; therefore, network security personnel must be aware of the latest attack methods in order to detect them.

Example of a TrickBot / Ryuk Cyber Attack

There is currently an increase in TrickBot infections that lead to a Ryuk infection. For example, TrickBot disables the organizations endpoint antivirus application and spreads throughout the network, infecting hundreds of endpoints. Since **TrickBot is a banking trojan**, it likely harvested and exfiltrated financial and other sensitive information prior to deploying **Ryuk ransomware**.



TrickBot malware arrives via email. Often with malicious macro-enabled documents and is downloaded onto the system.

TrickBot malware uses various modules to saturate the network. Sensitive data is funneled out of the network to the attacker's servers.

TrickBot drops Ryuk onto the network. The CTAs deploy Ryuk network wide using PowerShell, PSEXEC, and Group Policy.

The CTAs establish persistence and manually delete backups and shadow copies.

Ryuk encrypts all systems on the network and creates a ransom note.

*Cyber Threat Actors (CTAs)

Typically, an employee clicks on an attachment in an email that unleashes the malware into their network

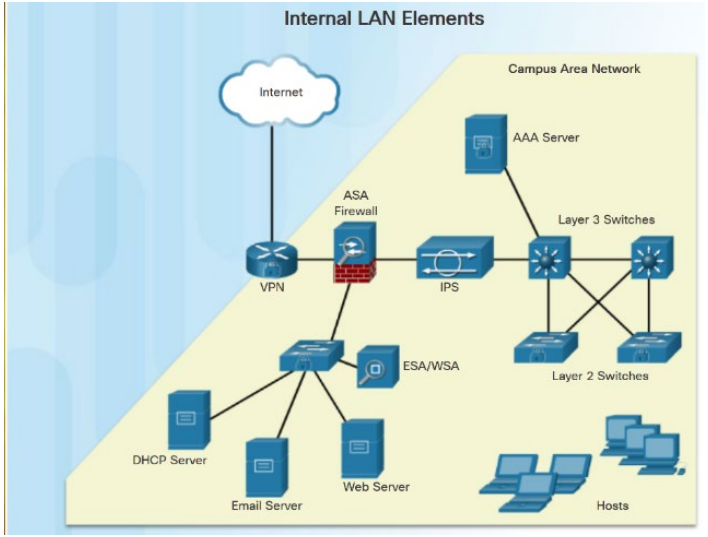
Image source: cisecurity.org

So how do we protect our systems?

Endpoint Security and Analysis

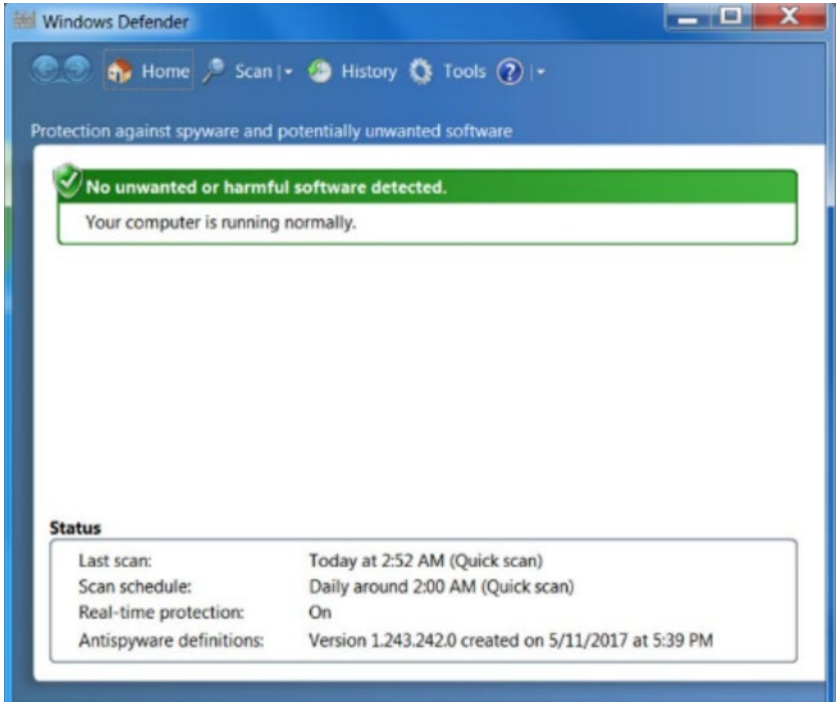
Endpoint Security

- We have two internal LAN elements to secure:
  - Endpoints - Hosts commonly consist of laptops, desktops, printers, servers, and IP phones.
  - Network infrastructure - LAN infrastructure devices interconnect endpoints and typically include switches, wireless devices, and IP devices.



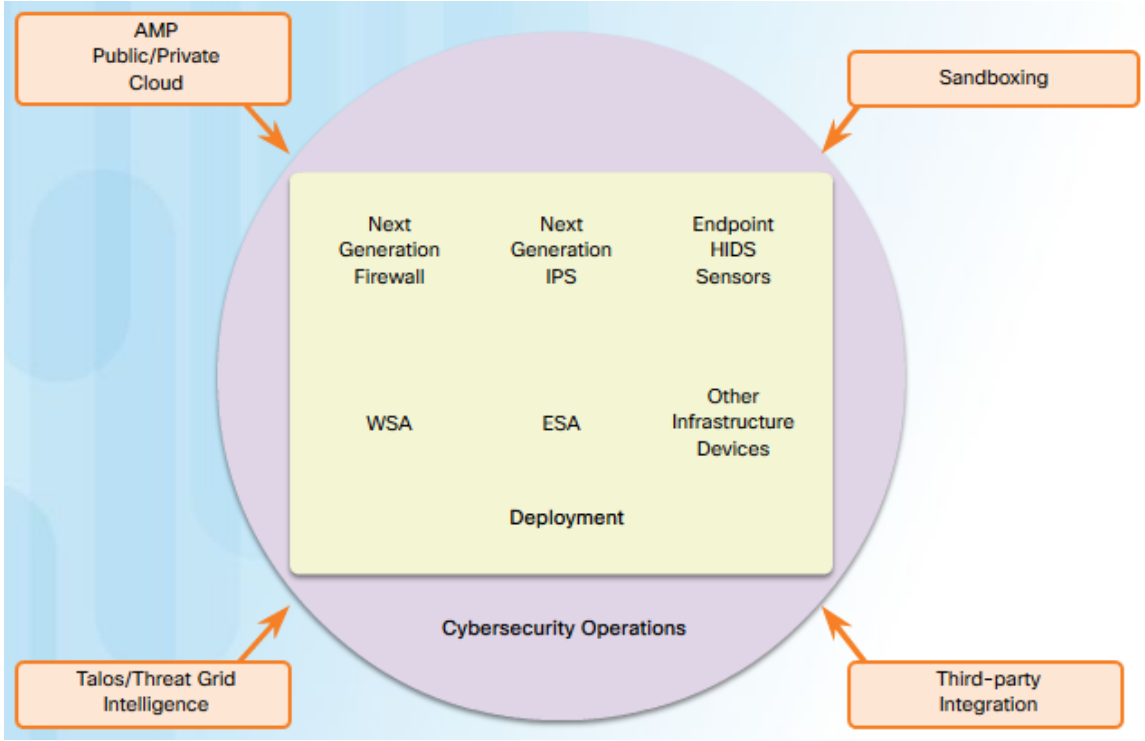
Host-Based Malware Protection

- Antimalware/antivirus software.
  - Signature-based – Recognizes various characteristics of known malware files.
  - Heuristics-based – Recognizes general features shared by various types of malware.
  - Behavior-based – Employs analysis of suspicious behavior.
- Host-based Firewall - restricts incoming and outgoing connections.
- Host-based Security Suites - include antivirus, anti-phishing, safe browsing, Host-based intrusion prevention system, firewall capabilities and robust logging functionality.



Network-Based Malware Protection

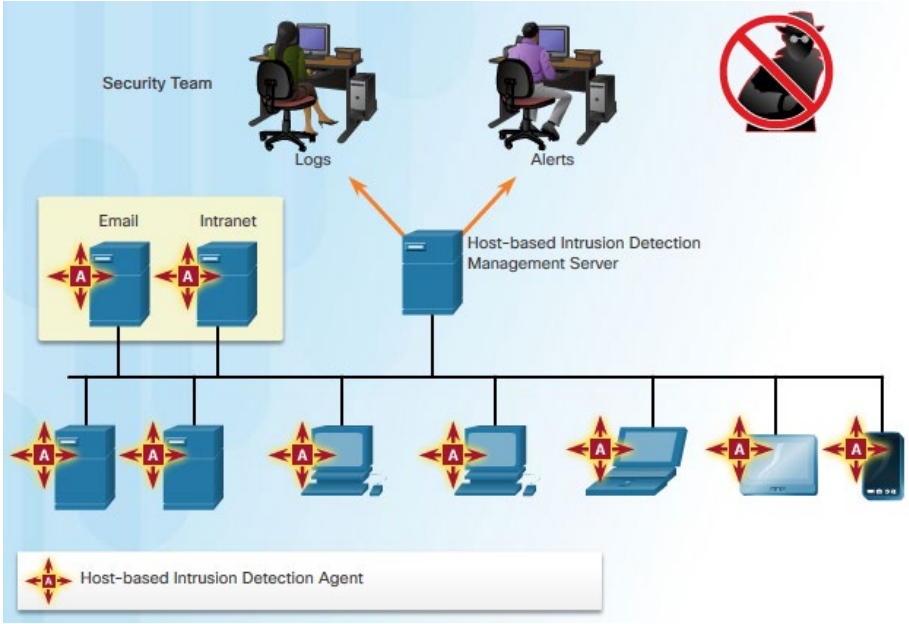
- Network-based malware protection
  - Advanced Malware Protection (AMP)
  - Email Security Appliance (ESA)
  - Web Security Appliance (WSA)
  - Network Admission Control (NAC)



Host-Based Firewalls

- Host-based personal firewalls are standalone software programs that control traffic entering or leaving a computer.
- Host-based firewalls include;
  - **Windows Firewall** - uses a profile-based approach to configuring firewall functionality.
  - **Iptables** - allows Linux system administrators to configure network access rules.
  - **Nftables** - successor to iptables, nftables is a Linux firewall application that uses a simple virtual machine in the Linux kernel.
  - **TCP Wrapper for Linux-based devices** - rule-based access control and logging system.

What is a Host-Based Intrusion Detection System



- Host-Based Intrusion Detection System (HIDS) protects hosts against malware and can perform:
  - monitoring and reporting
  - log analysis
  - event correlation
  - integrity checking
  - policy enforcement
  - rootkit detection
- HIDS software must run directly on the host, so it is considered an agent-based system.
- A HIDS not only detects malware but also can prevent it from executing if it should reach a host.

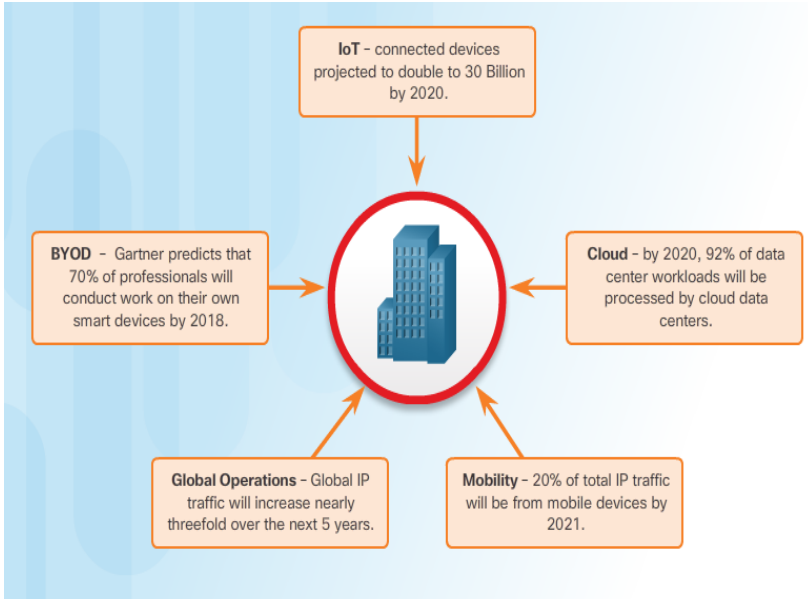
How does HIDS Operate?

- An additional set of strategies are used to detect malware that evades signature detection:
  - **Anomaly-based** - host behavior is compared to a learned baseline model.
  - **Policy-based** – normal behavior is described by rules or by the violation of rules.

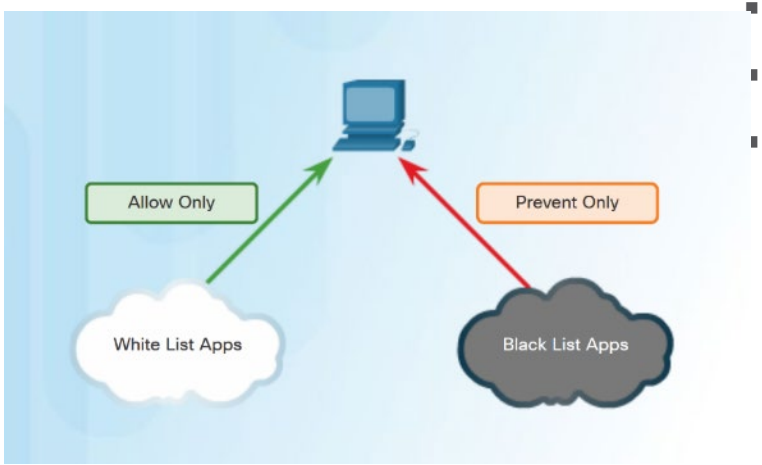
In addition, some malware families exhibit polymorphism. This means the malware has the ability to change its signature just enough to not be detected.

What is an Attack Surface?

- An attack surface is the total sum of the vulnerabilities.
  - Include open ports, applications, wireless connections, and users.
- Attack surfaces are currently expanding due to cloud-based systems, mobile devices, BYOD and the IoT.
- The SANS Institute describes three components of the attack surface:
  - *Network Attack Surface*
  - *Software Attack Surface*
  - *Human Attack Surface*



Systems also use Application Blacklisting and Whitelisting



- Application blacklist – which apps are not permitted.
- Application whitelist – which apps are allowed to run.
- Websites can also be whitelisted and blacklisted.
  - Cisco's FireSIGHT security management system is an example of a device that can access the Cisco Talos security intelligence service to obtain blacklists.

System-Based Sandboxing

- Sandboxing is a technique that allows suspicious files to be analyzed and run in a safe environment.
- A number of online public sandboxes exist. These services allow malware samples to be uploaded for analysis. An example of these services are VirusTotal and Hybrid Analysis.

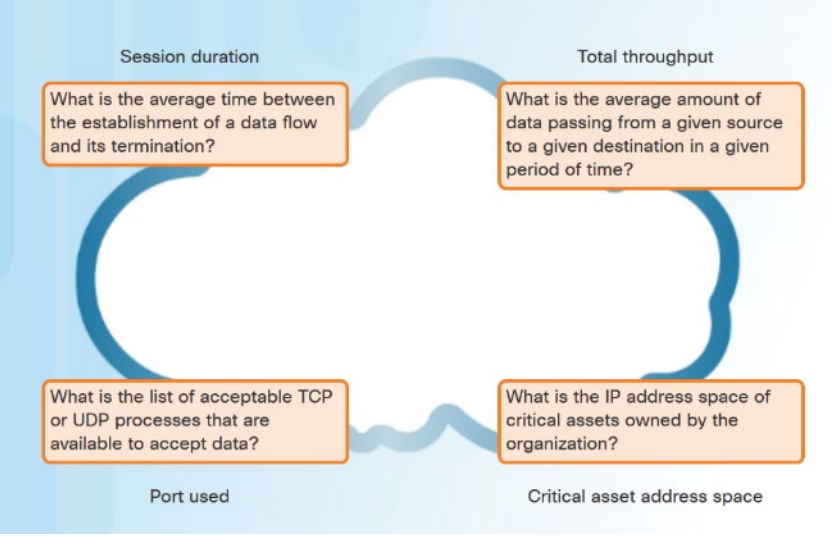
CISCO

Endpoint Vulnerability Assessment

Network Profiling

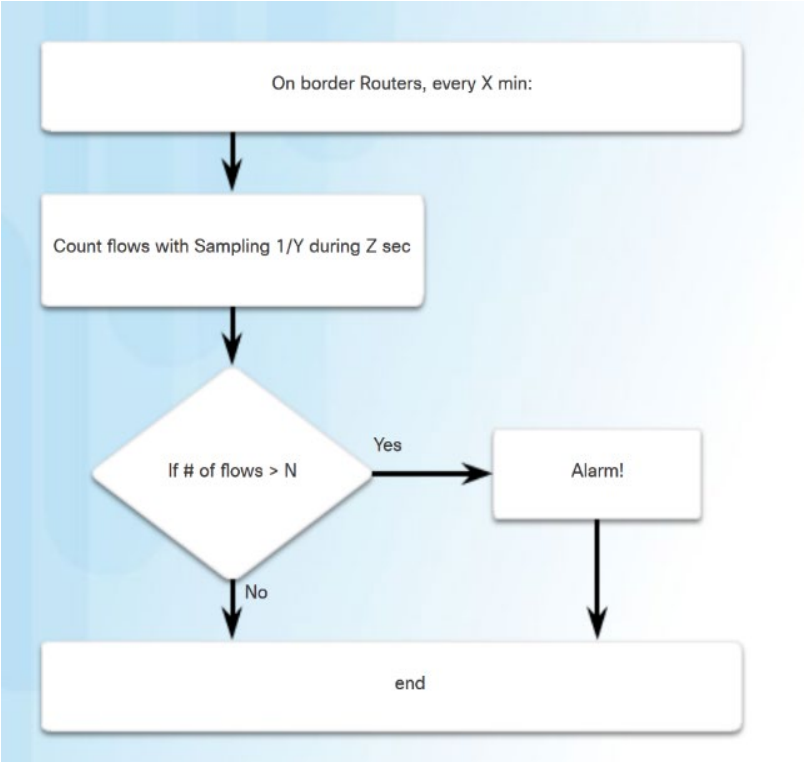
- Network profiling – create a baseline to compare against when an attack occurs.
- Elements of a network baseline should include:
  - Session duration
  - Total throughput
  - Critical asset address space
  - Typical traffic type

Remember: Networks have a rhythm (behavior), anything outside of that rhythm may be suspicious



Network Anomaly Detection

- Network behavior is described by a large amount of diverse data such as the features of **packet flow**, features of the packets themselves, and telemetry from multiple sources.
- Big Data analytics techniques can be used to analyze this data and detect variations from the baseline.
- Anomaly detection can recognize network congestion caused by worm traffic and also identify infected hosts on the network.



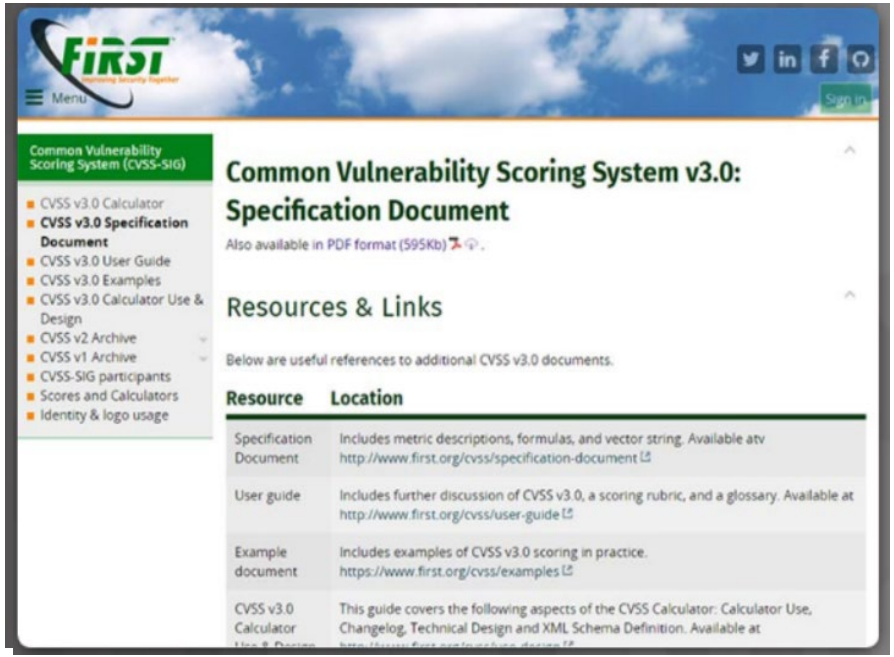
*__Traffic flow definition:__ Packet **flow,** or network flow, is a sequence of packets from a source computer to a destination, which may be another host, a multicast group, or a broadcast domain. RFC 2722 defines traffic flow as "an artificial logical equivalent to a call or connection."

Network Vulnerability Testing

- Network vulnerability testing can include risk analysis, vulnerability assessment, and penetration testing.

Activity	Examples	Tools
Risk Analysis	individuals conduct comprehensive analysis of impacts of attacks on core company assets and functioning	internal or external consultants, risk management frameworks
Vulnerability Assessment	patch management, host scans, port scanning, other vulnerability scans and services	OpenVas, Microsoft Baseline Analyzer, Nessus, Qualys, Nmap
Penetration Testing	use of hacking techniques and tools to penetrate network defenses and identify depth of potential penetration.	Metasploit, CORE Impact, ethical hackers

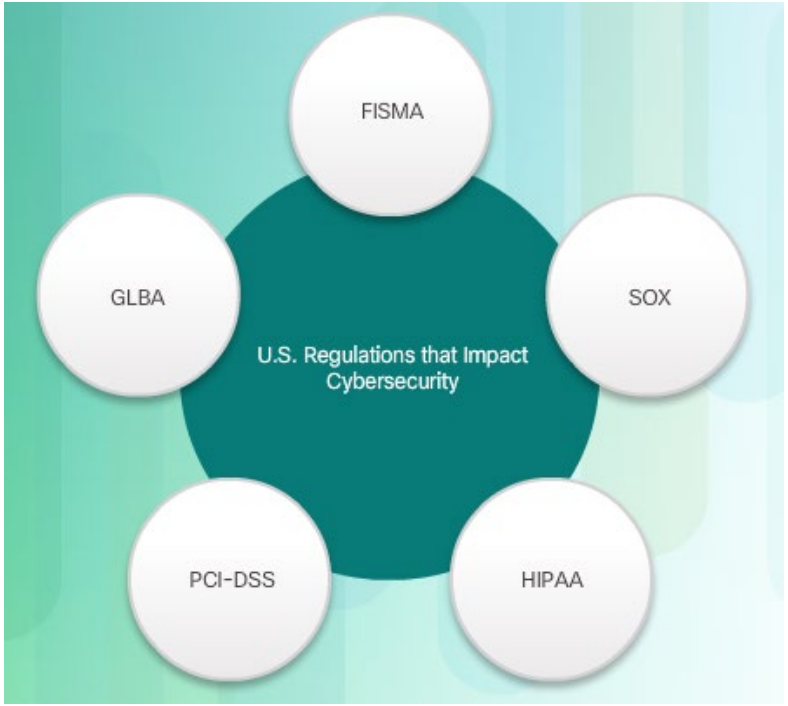
Vulnerability Information Sources



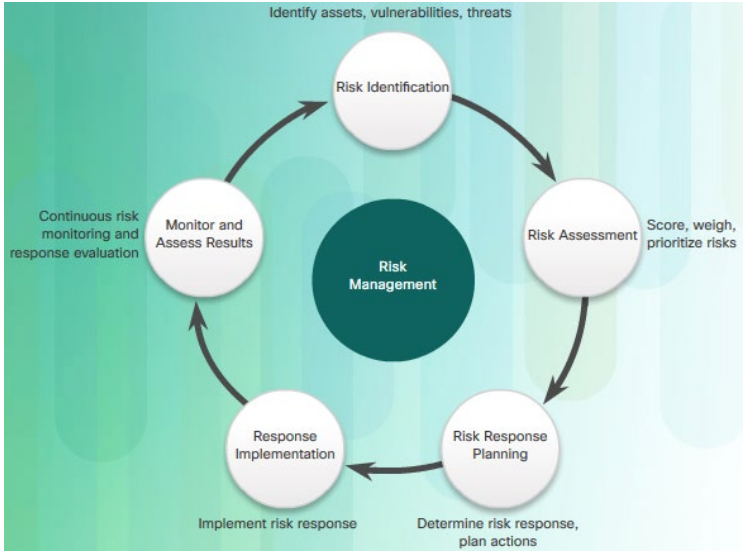
- **Common Vulnerability Scoring System (CVSS)** is a risk assessment designed to convey the common attributes and severity of vulnerabilities in computer hardware and software systems.
- **Common Vulnerabilities and Exposures (CVE)** - dictionary of common names, in the form of CVE identifiers, for known cybersecurity vulnerabilities.
- **National Vulnerability Database (NVD)** - utilizes CVE identifiers and supplies additional information such as CVSS threat scores

Compliance Regulations

- To prevent security breaches, a number of security compliance regulations have been developed.



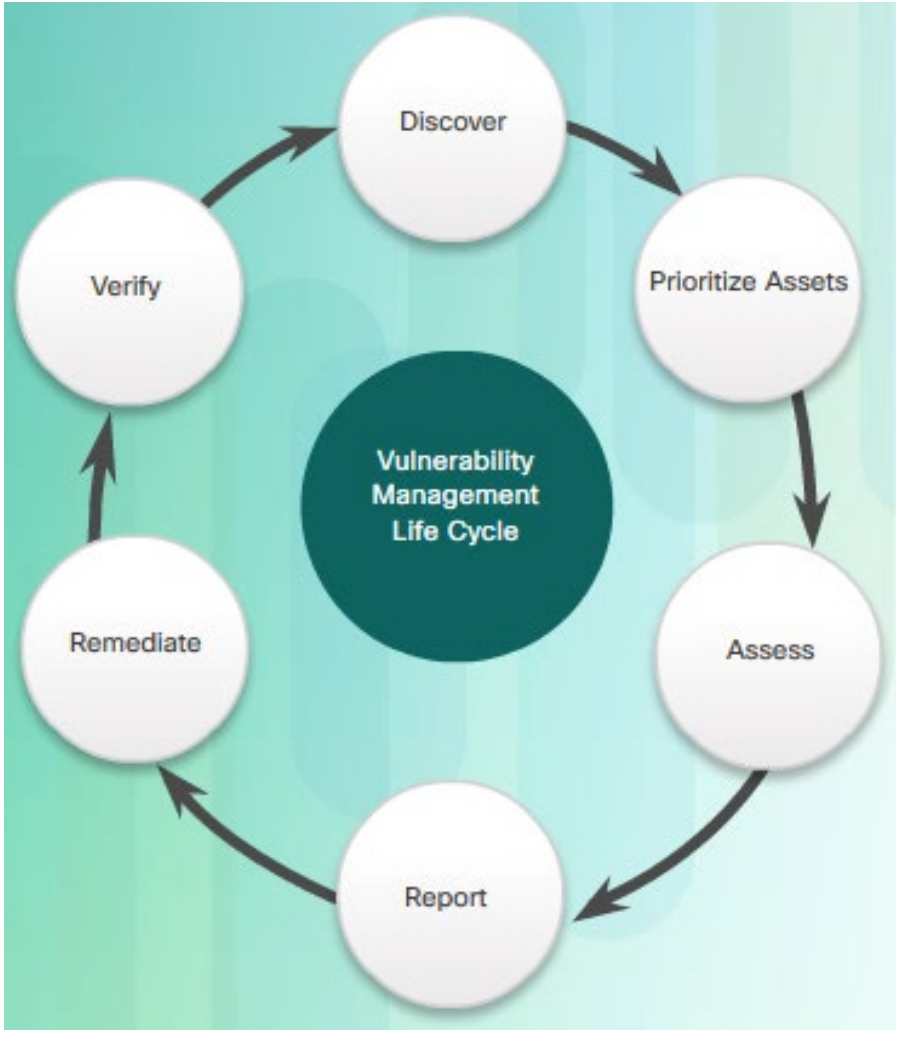
Risk Management



- Risk management involves the selection of security controls for an organization.
  - **Risk avoidance** - Stop performing the activities that create risk.
  - **Risk reduction** - Take measures to reduce vulnerability.
  - **Risk sharing** - Shift some of the risk to other parties.
  - **Risk retention** - Accept the risk and its consequences.

Vulnerability Management

Vulnerability management is a security practice designed to proactively prevent the exploitation of IT vulnerabilities.

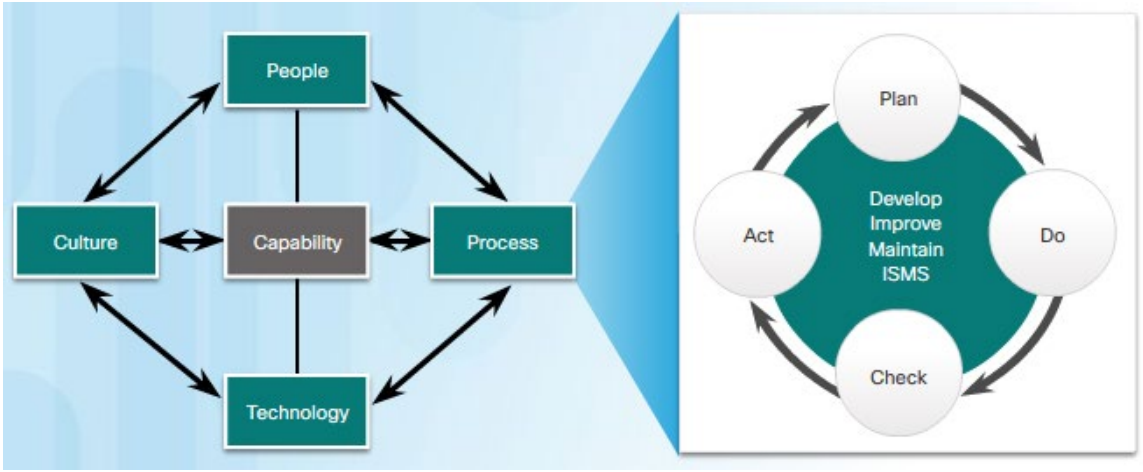


Enterprise Patch Management

- Patch management involves all aspects of software patching, including identifying required patches, acquiring, distributing, installing, and verifying that the patch is installed on all systems.

Security Management Systems

- Management framework to identify, analyze, and address information security risks



NIST Cybersecurity Framework

- **NIST Cybersecurity Framework** - a set of standards designed to integrate existing standards, guidelines, and practices to help better manage and reduce cybersecurity risk.

Core Function	Description
IDENTIFY	Develop the organizational understanding to manage cybersecurity risk to systems, assets, data, and capabilities.
PROTECT	Develop and implement the appropriate safeguards to ensure delivery of critical infrastructure services.
DETECT	Develop and implement the appropriate activities to identify the occurrence of a cybersecurity event.
RESPOND	Develop and implement the appropriate activities to take action regarding a detected cybersecurity event.
RECOVER	Develop and implement the appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity event.

If you enjoyed this presentation, you may want to take Cisco's Cyber Ops Security course, or CompTIA's Security + course

Questions?