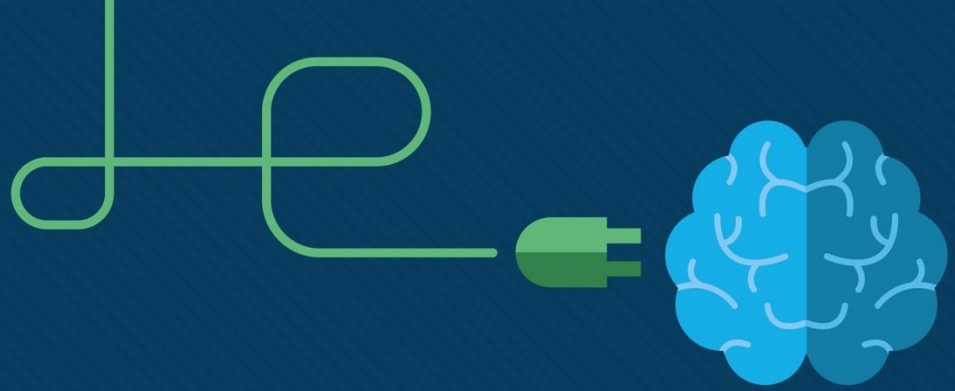


Module 3: Network Security Concepts

Enterprise Networking, Security, and Automation v7.0 (ENSA)

Module Objectives

Module Title: Network Security Concepts

Module Objective: Explain how vulnerabilities, threats, and exploits can be mitigated to enhance network security.

Topic Title	Topic Objective
Current State of Cybersecurity:	Describe the current state of cybersecurity and vectors of data loss.
Threat Actors	Describe tools used by threat actors to exploit networks.
Malware	Describe malware types.
Common Network Attacks	Describe common network attacks.
IP Vulnerabilities and Threats	Explain how IP vulnerabilities are exploited by threat actors.
TCP and UDP Vulnerabilities	Explain how TCP and UDP vulnerabilities are exploited by threat actors.
IP Services	Explain how IP services are exploited by threat actors.
Network Security Best Practices	Describe best practices for protecting a network.
Cryptography	Describe common cryptographic processes used to protect data in transit.

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

3.1 Current State of Cybersecurity

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Current State of Affairs

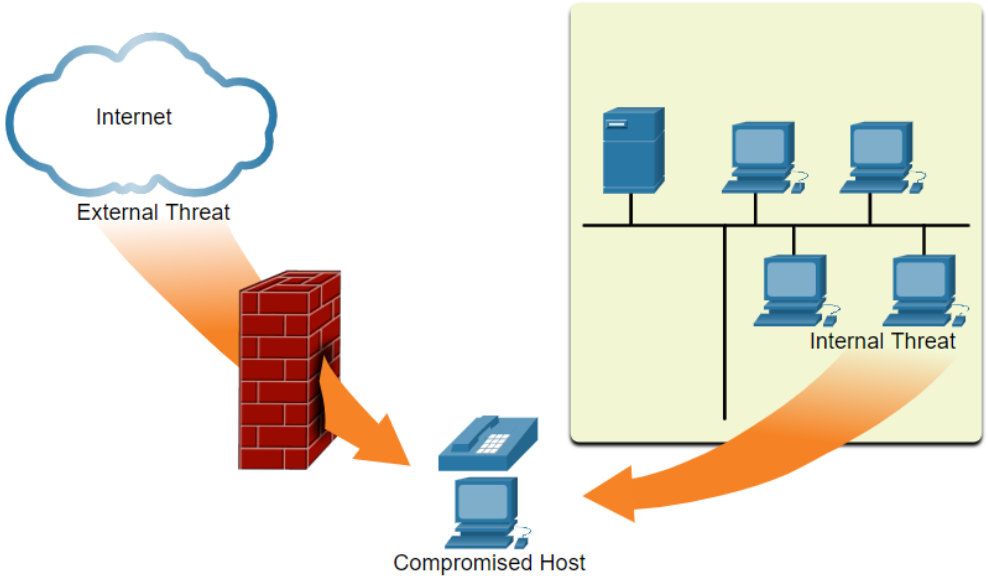
- Cyber criminals now have the expertise and tools necessary to take down critical infrastructure and systems. Their tools and techniques continue to evolve.
- Maintaining a secure network ensures the safety of network users and protects commercial interests. All users should be aware of security terms in the table.

Security Terms	Description
Assets	An asset is anything of value to the organization. It includes people, equipment, resources, and data.
Vulnerability	A vulnerability is a weakness in a system, or its design, that could be exploited by a threat.
Threat	A threat is a potential danger to a company's assets, data, or network functionality.
Exploit	An exploit is a mechanism that takes advantage of a vulnerability.
Mitigation	Mitigation is the counter-measure that reduces the likelihood or severity of a potential threat or risk. Network security involves multiple mitigation techniques.
Risk	Risk is the likelihood of a threat to exploit the vulnerability of an asset, with the aim of negatively affecting an organization. Risk is measured using the probability of the occurrence of an event and its consequences.

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Vectors of Network Attacks

- An attack vector is a path by which a threat actor can gain access to a server, host, or network. Attack vectors originate from inside or outside the corporate network, as shown in the figure.
- **Internal threats** have the potential to cause greater damage than **external threats** because internal users have direct access to the building and its infrastructure devices.



© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Data Loss

Data loss or data exfiltration is when data is intentionally or unintentionally lost, stolen, or leaked to the outside world. The data loss can result in:

- Brand damage and loss of reputation
- Loss of competitive advantage
- Loss of customers
- Loss of revenue
- Litigation/legal action resulting in fines and civil penalties
- Significant cost and effort to notify affected parties and recover from the breach

Network security professionals must protect the organization's data. Various Data Loss Prevention (DLP) controls must be implemented which combine strategic, operational and tactical measures.

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Data Loss (Cont.)

Data Loss Vectors	Description
Email/Social Networking	Intercepted email or IM messages could be captured and reveal confidential information.
Unencrypted Devices	If the data is not stored using an encryption algorithm, then the thief can retrieve valuable confidential data.
Cloud Storage Devices	Sensitive data can be lost if access to the cloud is compromised due to weak security settings.
Removable Media	One risk is that an employee could perform an unauthorized transfer of data to a USB drive. Another risk is that a USB drive containing valuable corporate data could be lost.
Hard Copy	Confidential data should be shredded when no longer required.
Improper Access Control	Passwords or weak passwords which have been compromised can provide a threat actor with easy access to corporate data.

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

3.2 Threat Actors

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

The Hacker

Hacker is a common term used to describe a threat actor

Hacker Type	Description
White Hat Hackers	These are ethical hackers who use their programming skills for good, ethical, and legal purposes. Security vulnerabilities are reported to developers for them to fix before the vulnerabilities can be exploited.
Gray Hat Hackers	These are individuals who commit crimes and do arguably unethical things, but not for personal gain or to cause damage. Gray hat hackers may disclose a vulnerability to the affected organization after having compromised their network.
Black Hat Hackers	These are unethical criminals who compromise computer and network security for personal gain, or for malicious reasons, such as attacking networks.

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

The Evolution of Hackers

The table displays modern hacking terms and a brief description of each.

Hacking Term	Description
Script Kiddies	These are teenagers or inexperienced hackers running existing scripts, tools, and exploits, to cause harm, but typically not for profit.
Vulnerability Broker	These are usually gray hat hackers who attempt to discover exploits and report them to vendors, sometimes for prizes or rewards.
Hacktivists	These are gray hat hackers who publicly protest organizations or governments by posting articles, videos, leaking sensitive information, and performing network attacks.
Cyber criminals	These are black hat hackers who are either self-employed or working for large cybercrime organizations.
State-Sponsored	These are either white hat or black hat hackers who steal government secrets, gather intelligence, and sabotage networks. Their targets are foreign governments, terrorist groups, and corporations. Most countries in the world participate to some degree in state-sponsored hacking

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Cyber Criminals

It is estimated that cyber criminals steal billions of dollars from consumers and businesses. Cyber criminals operate in an underground economy where they buy, sell, and trade attack toolkits, zero day exploit code, botnet services, banking Trojans, keyloggers, and much more. They also buy and sell the private information and intellectual property they steal. Cyber criminals target small businesses and consumers, as well as large enterprises and entire industries.

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Hacktivists

Two examples of hacktivist groups are Anonymous and the Syrian Electronic Army. Although most hacktivist groups are not well organized, they can cause significant problems for governments and businesses. Hacktivists tend to rely on fairly basic, freely available tools.

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

State-Sponsored Hackers

State-sponsored hackers create advanced, customized attack code, often using previously undiscovered software vulnerabilities called zero-day vulnerabilities. An example of a state-sponsored attack involves the Stuxnet malware that was created to damage Iran's nuclear enrichment capabilities.

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

3.3 Threat Types

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Attack Types

Attack Type	Description
Eavesdropping Attack	This is when a threat actor captures and “listens” to network traffic. This attack is also referred to as sniffing or snooping.
Data Modification Attack	If threat actors have captured enterprise traffic, they can alter the data in the packet without the knowledge of the sender or receiver.
IP Address Spoofing Attack	A threat actor constructs an IP packet that appears to originate from a valid address inside the corporate intranet.
Password-Based Attacks	If threat actors discover a valid user account, the threat actors have the same rights as the real user. Threat actors could use that valid account to obtain lists of other users, network information, change server and network configurations, and modify, reroute, or delete data.
Denial of Service Attack	A DoS attack prevents normal use of a computer or network by valid users. A DoS attack can flood a computer or the entire network with traffic until a shutdown occurs because of the overload. A DoS attack can also block traffic, which results in a loss of access to network resources by authorized users.
Man-in-the-Middle Attack	This attack occurs when threat actors have positioned themselves between a source and destination. They can now actively monitor, capture, and control the communication transparently.
Compromised-Key Attack	If a threat actor obtains a secret key, that key is referred to as a compromised key. A compromised key can be used to gain access to a secured communication without the sender or receiver being aware of the attack.
Sniffer Attack	A sniffer is an application or device that can read, monitor, and capture network data exchanges and read network packets. If the packets are not encrypted, a sniffer provides a full view of the data inside the packet

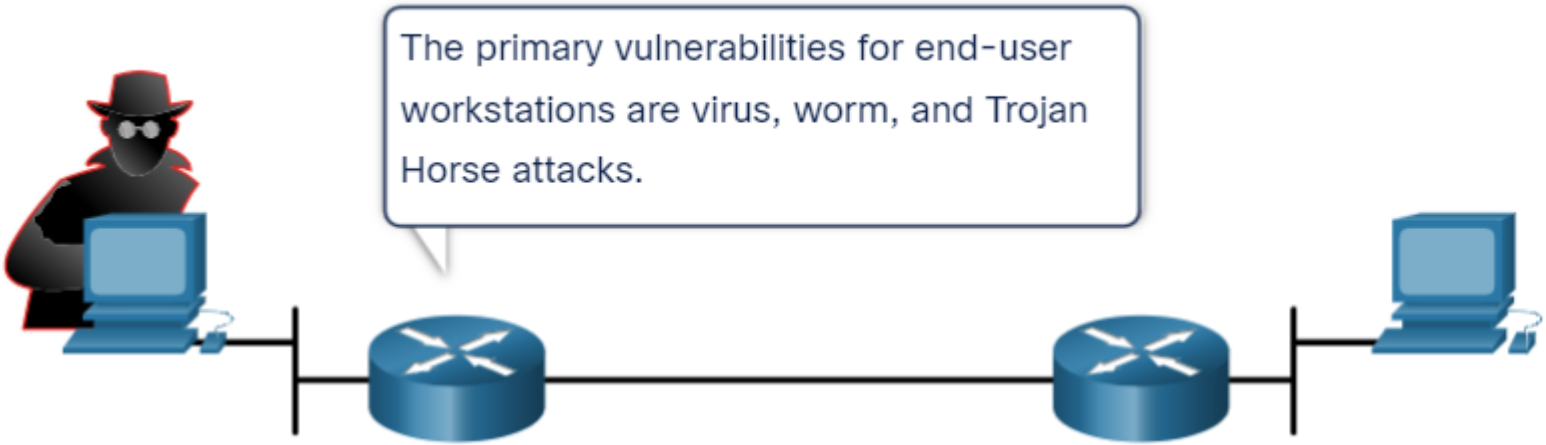
© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

3.4 Malware

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Overview of Malware

- Now that you know about the tools that hacker use, this topic introduces you to different types of malware that hackers use to gain access to end devices.
- End devices are particularly prone to malware attacks. It is important to know about malware because threat actors rely on users to install malware to help exploit the security gaps.



© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Viruses and Trojan Horses

- The first and most common type of computer malware is a virus. Viruses require human action to propagate and infect other computers.
- The virus hides by attaching itself to computer code, software, or documents on the computer. When opened, the virus executes and infects the computer.
- Viruses can:
  - Alter, corrupt, delete files, or erase entire drives.
  - Cause computer booting issues, and corrupt applications.
  - Capture and send sensitive information to threat actors.
  - Access and use email accounts to spread.
  - Lay dormant until summoned by the threat actor.

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Viruses and Trojan Horses (Cont.)

Modern viruses are developed for specific intent such as those listed in the table.

Types of Viruses	Description
Boot sector virus	Virus attacks the boot sector, file partition table, or file system.
Firmware viruses	Virus attacks the device firmware.
Macro virus	Virus uses the MS Office macro feature maliciously.
Program viruses	Virus inserts itself in another executable program.
Script viruses	Virus attacks the OS interpreter which is used to execute scripts.

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Viruses and Trojan Horses (Cont.)

Threat actors use Trojan horses to compromise hosts. A Trojan horse is a program that looks useful but also carries malicious code. Trojan horses are often provided with free online programs such as computer games. There are several types of Trojan horses as described in the table.

Type of Trojan Horse	Description
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 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 functioning.
Denial of Service (DoS)	Trojan horse slows or halts network activity.
Keylogger	Trojan horse actively attempts to steal confidential information, such as credit card numbers, by recording key strokes entered into a web form.

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Other Types of Malware

Malware	Description
Adware	•Adware is usually distributed by downloading online software. •Adware can display unsolicited advertising using pop-up web browser windows, new toolbars, or unexpectedly redirect a webpage to a different website. •Pop-up windows may be difficult to control as new windows can pop-up faster than the user can close them.
Ransomware	•Ransomware typically denies a user access to their files by encrypting the files and then displaying a message demanding a ransom for the decryption key. •Users without up-to-date backups must pay the ransom to decrypt their files. •Payment is usually made using wire transfer or crypto currencies such as Bitcoin.
Rootkit	•Rootkits are used by threat actors to gain administrator account-level access to a computer. •They are very difficult to detect because they can alter firewall, antivirus protection, system files, and even OS commands to conceal their presence. •They can provide a backdoor to threat actors giving them access to the PC, and allowing them to upload files, and install new software to be used in a DDoS attack. •Special rootkit removal tools must be used to remove them, or a complete OS re-install may be required.
Spyware	•Like adware but, used to gather information about the user and send to threat actors without the user's consent. •Spyware can be a low threat, gathering browsing data, or it can be a high threat capturing personal and financial information.
Worm	•A worm is a self-replicating program that propagates automatically without user actions by exploiting vulnerabilities in legitimate software. •It uses the network to search for other victims with the same vulnerability. •The intent of a worm is usually to slow or disrupt network operations

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

3.5 Common Network Attacks

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Overview of Common Network Attacks

- When malware is delivered and installed, the payload can be used to cause a variety of network related attacks.
- To mitigate attacks, it is useful to understand the types of attacks. By categorizing network attacks, it is possible to address types of attacks rather than individual attacks.
- Networks are susceptible to the following types of attacks:
  - Reconnaissance Attacks
  - Access Attacks
  - DoS Attacks

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Reconnaissance Attacks

- Reconnaissance is information gathering.
- Threat actors use reconnaissance (or recon) attacks to do unauthorized discovery and mapping of systems, services, or vulnerabilities. Recon attacks precede access attacks or DoS attacks.

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Reconnaissance Attacks (Cont.)

Some of the techniques used by malicious threat actors to conduct reconnaissance attacks are described in the table.

Technique	Description
Perform an information query of a target	The threat actor is looking for initial information about a target. Various tools can be used, including the Google search, organizations website, whois, and more.
Initiate a ping sweep of the target network	The information query usually reveals the target's network address. The threat actor can now initiate a ping sweep to determine which IP addresses are active.
Initiate a port scan of active IP addresses	This is used to determine which ports or services are available. Examples of port scanners include Nmap, SuperScan, Angry IP Scanner, and NetScanTools.
Run vulnerability scanners	This is to query the identified ports to determine the type and version of the application and operating system that is running on the host. Examples of tools include Nipper, Core Impact, Nessus, SAINT, and Open VAS.
Run exploitation tools	The threat actor now attempts to discover vulnerable services that can be exploited. A variety of vulnerability exploitation tools exist including Metasploit, Core Impact, Sqlmap, Social Engineer Toolkit, and Netsparker.

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Access Attacks

- Access attacks exploit known vulnerabilities in authentication services, FTP services, and web services. The purpose of these types of attacks is to gain entry to web accounts, confidential databases, and other sensitive information.
- Threat actors use access attacks on network devices and computers to retrieve data, gain access, or to escalate access privileges to administrator status.
- **Password Attacks:** In a password attack, the threat actor attempts to discover critical system passwords using various methods. Password attacks are very common and can be launched using a variety of password cracking tools.
- **Spoofing Attacks:** In spoofing attacks, the threat actor device attempts to pose as another device by falsifying data. Common spoofing attacks include IP spoofing, MAC spoofing, and DHCP spoofing. These spoofing attacks will be discussed in more detail later in this module
- Other Access attacks include:
    - Trust exploitations
    - Port redirections
    - Man-in-the-middle attacks
    - Buffer overflow attacks

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Social Engineering Attacks

- Social engineering is an access attack that attempts to manipulate individuals into performing actions or divulging confidential information. Some social engineering techniques are performed in-person while others may use the telephone or internet.
- Social engineers often rely on people's willingness to be helpful. They also prey on people's weaknesses.

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Social Engineering Attacks (Cont.)

Social Engineering Attack	Description
Pretexting	A threat actor pretends to need personal or financial data to confirm the identity of the recipient.
Phishing	A threat actor sends fraudulent email which is disguised as being from a legitimate, trusted source to trick the recipient into installing malware on their device, or to share personal or financial information.
Spear phishing	A threat actor creates a targeted phishing attack tailored for a specific individual or organization.
Spam	Also known as junk mail, this is unsolicited email which often contains harmful links, malware, or deceptive content.
Something for Something	Sometimes called “Quid pro quo”, this is when a threat actor requests personal information from a party in exchange for something such as a gift.
Baiting	A threat actor leaves a malware infected flash drive in a public location. A victim finds the drive and unsuspectingly inserts it into their laptop, unintentionally installing malware.
Impersonation	This type of attack is where a threat actor pretends to be someone they are not to gain the trust of a victim.
Tailgating	This is where a threat actor quickly follows an authorized person into a secure location to gain access to a secure area.
Shoulder surfing	This is where a threat actor inconspicuously looks over someone’s shoulder to steal their passwords or other information.
Dumpster diving	This is where a threat actor rummages through trash bins to discover confidential documents

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Social Engineering Attacks (Cont.)

- The Social Engineering Toolkit (SET) was designed to help white hat hackers and other network security professionals create social engineering attacks to test their own networks.
- Enterprises must educate their users about the risks of social engineering, and develop strategies to validate identities over the phone, via email, or in person.
- The figure shows recommended practices that should be followed by all users.

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

DoS and DDoS Attacks

- A Denial of Service (DoS) attack creates some sort of interruption of network services to users, devices, or applications. There are two major types of DoS attacks:
  - **Overwhelming Quantity of Traffic** - The threat actor sends an enormous quantity of data at a rate that the network, host, or application cannot handle. This causes transmission and response times to slow down. It can also crash a device or service.
  - **Maliciously Formatted Packets** - The threat actor sends a maliciously formatted packet to a host or application and the receiver is unable to handle it. This causes the receiving device to run very slowly or crash.
- 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 Distributed DoS Attack (DDoS) is similar to a DoS attack, but it originates from multiple, coordinated sources.

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

3.6 IP Vulnerabilities and Threats

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

IPv4 and IPv6

- IP does not validate whether the source IP address contained in a packet actually came from that source. For this reason, threat actors can send packets using a spoofed source IP address. Security analysts must understand the different fields in both the IPv4 and IPv6 headers.
- Some of the more common IP related attacks are shown in the table

IP Attack Techniques	Description
ICMP attacks	Threat actors use Internet Control Message Protocol (ICMP) echo packets (pings) to discover subnets and hosts on a protected network, to generate DoS flood attacks, and to alter host routing tables.
Amplification and reflection attacks	Threat actors attempt to prevent legitimate users from accessing information or services using DoS and DDoS attacks.
Address spoofing attacks	Threat actors spoof the source IP address in an IP packet to perform blind spoofing or non-blind spoofing.
Man-in-the-middle attack (MITM)	Threat actors position themselves between a source and destination to transparently monitor, capture, and control the communication. They could eavesdrop by inspecting captured packets, or alter packets and forward them to their original destination.
Session hijacking	Threat actors gain access to the physical network, and then use an MITM attack to hijack a session

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

ICMP Attacks

- Threat actors use ICMP for reconnaissance and scanning attacks. They can launch information-gathering attacks to map out a network topology, discover which hosts are active (reachable), identify the host operating system (OS fingerprinting), and determine the state of a firewall. Threat actors also use ICMP for DoS attacks.
- **Note**: ICMP for IPv4 (ICMPv4) and ICMP for IPv6 (ICMPv6) are susceptible to similar types of attacks.
- Networks should have strict ICMP access control list (ACL) filtering on the network edge to avoid ICMP probing from the internet. In the case of large networks, security devices such as firewalls and intrusion detection systems (IDS) detect such attacks and generate alerts to the security analysts.

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

ICMP Attacks (Cont.)

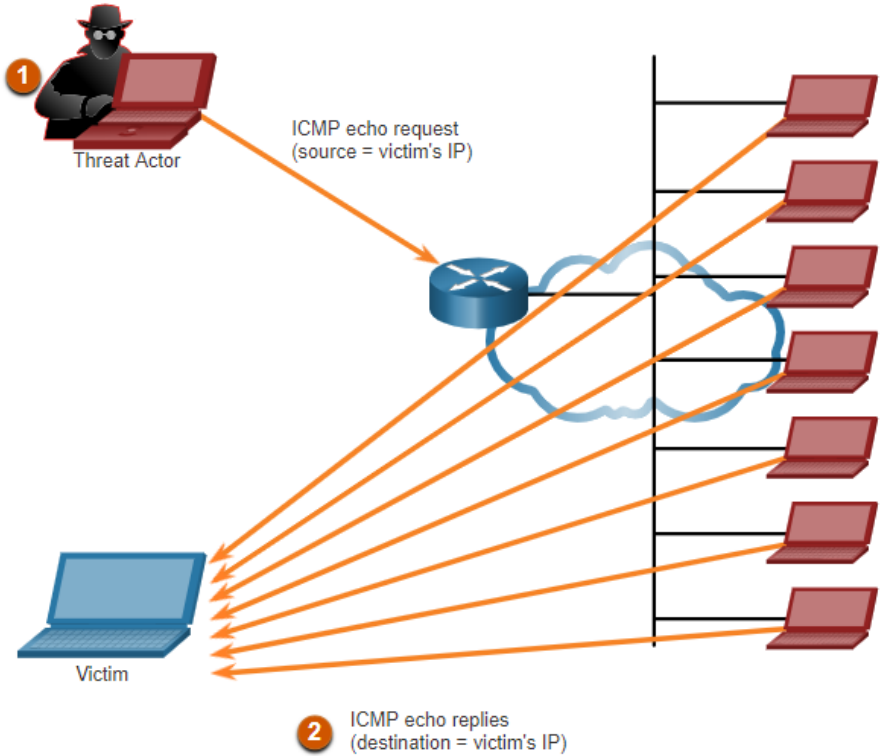
Common ICMP messages of interest to threat actors are listed in the table.

ICMP Messages used by Hackers	Description
ICMP echo request and echo reply	This is used to perform host verification and DoS attacks.
ICMP unreachable	This is used to perform network reconnaissance and scanning attacks.
ICMP mask reply	This is used to map an internal IP network.
ICMP redirects	This is used to lure a target host into sending all traffic through a compromised device and create a MITM attack.
ICMP router discovery	This is used to inject bogus route entries into the routing table of a target host.

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Amplification and Reflection Attacks

- Threat actors often use amplification and reflection techniques to create DoS attacks. The example in the figure illustrates a Smurf attack is used to overwhelm a target host.
  - **Note**: Newer forms of amplification and reflection attacks such as DNS-based reflection and amplification attacks and Network Time Protocol (NTP) amplification attacks are now being used.
- Threat actors also use resource exhaustion attacks to either to crash a target host or to consume the resources of a network.



© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Address Spoofing Attacks

- IP address spoofing attacks occur when a threat actor creates packets with false source IP address information to either hide the identity of the sender, or to pose as another legitimate user. Spoofing is usually incorporated into another attack such as a Smurf attack.
- Spoofing attacks can be non-blind or blind:
  - **Non-blind spoofing** - The threat actor can see the traffic that is being sent between the host and the target. Non-blind spoofing determines the state of a firewall and sequence-number prediction. It can also hijack an authorized session.
  - **Blind spoofing** - The threat actor cannot see the traffic that is being sent between the host and the target. Blind spoofing is used in DoS attacks.
- MAC address spoofing attacks are used when threat actors have access to the internal network. Threat actors alter the MAC address of their host to match another known MAC address of a target host.

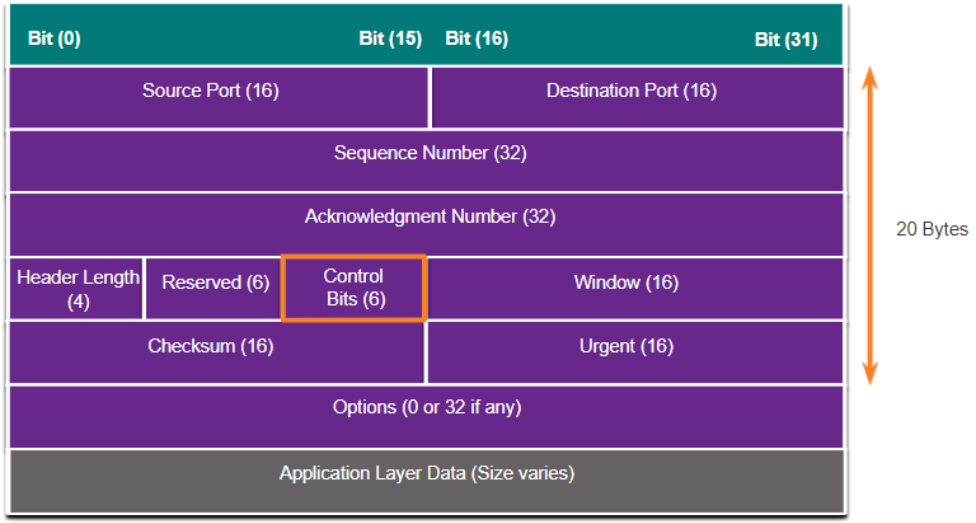
© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

3.7 TCP and UDP Vulnerabilities

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

TCP Segment Header

- TCP segment information appears immediately after the IP header. The fields of the TCP segment and the flags for the Control Bits field are displayed in the figure.
- The following are the six control bits of the TCP segment:
  - **URG** - Urgent pointer field significant
  - **ACK** - Acknowledgment field significant
  - **PSH** - Push function
  - **RST**- Reset the connection
  - **SYN** - Synchronize sequence numbers
  - **FIN** - No more data from sender



© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

TCP Services

TCP provides these services:

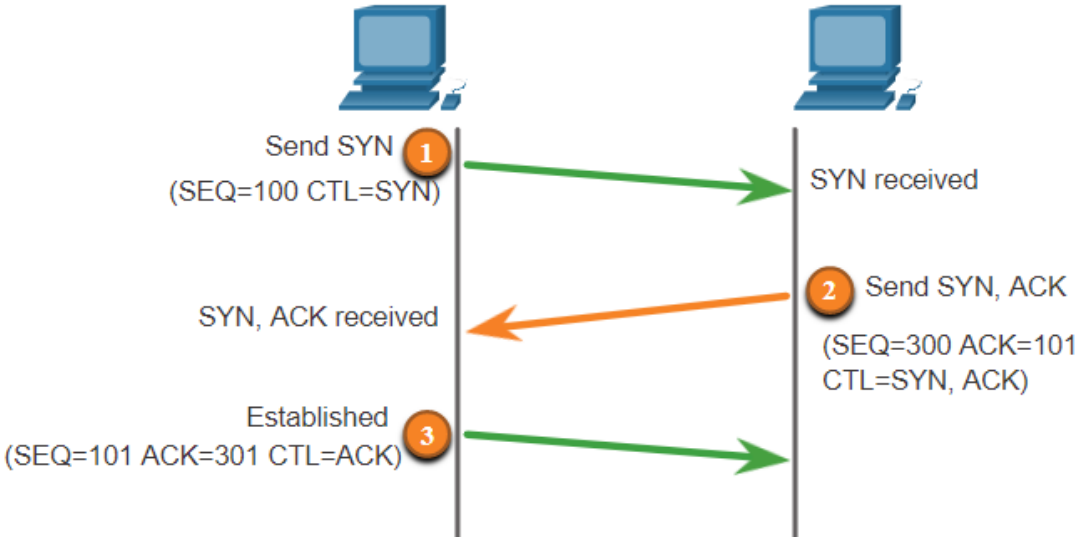
- **Reliable delivery** - TCP incorporates acknowledgments to guarantee delivery. If a timely acknowledgment is not received, the sender retransmits the data. Requiring acknowledgments of received data can cause substantial delays. Examples of application layer protocols that make use of TCP reliability include HTTP, SSL/TLS, FTP, DNS zone transfers, and others.
- **Flow control** - TCP implements flow control to address this issue. Rather than acknowledge one segment at a time, multiple segments can be acknowledged with a single acknowledgment segment.
- **Stateful communication** - TCP stateful communication between two parties occurs during the TCP three-way handshake.

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

TCP Services (Cont.)

A TCP connection is established in three steps:

1. The initiating client requests a client-to-server communication session with the server.
2. The server acknowledges the client-to-server communication session and requests a server-to-client communication session.
3. The initiating client acknowledges the server-to-client communication session.

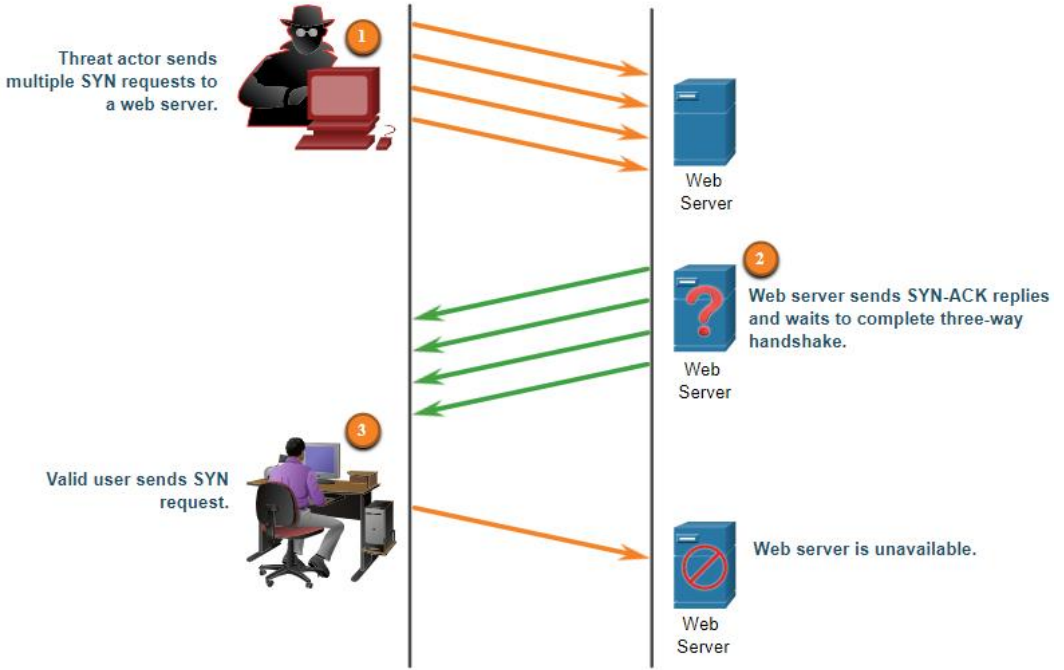


© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

TCP Attacks

TCP SYN Flood Attack

1. The threat actor sends multiple SYN requests to a webserver.
2. The web server replies with SYN-ACKs for each SYN request and waits to complete the three-way handshake. The threat actor does not respond to the SYN-ACKs.
3. A valid user cannot access the web server because the web server has too many half-opened TCP connections.



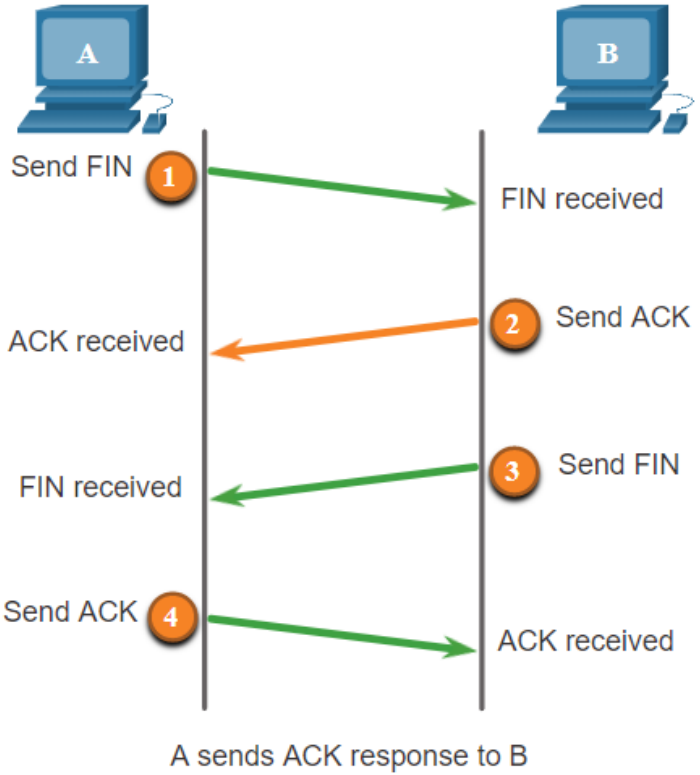
© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

TCP Attacks (Cont.)

Terminating a TCP session uses the following four-way exchange process:

1. When the client has no more data to send in the stream, it sends a segment with the FIN flag set.
2. The server sends an ACK to acknowledge the receipt of the FIN to terminate the session from client to server.
3. The server sends a FIN to the client to terminate the server-to-client session.
4. The client responds with an ACK to acknowledge the FIN from the server.

A threat actor could do a TCP reset attack and send a spoofed packet containing a TCP RST to one or both endpoints.



© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

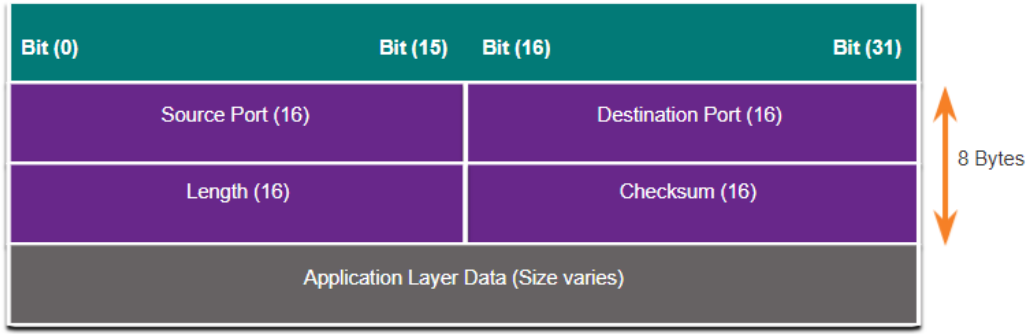
TCP Attacks (Cont.)

TCP session hijacking is another TCP vulnerability. Although difficult to conduct, a threat actor takes over an already-authenticated host as it communicates with the target. The threat actor must spoof the IP address of one host, predict the next sequence number, and send an ACK to the other host. If successful, the threat actor could send, but not receive, data from the target device.

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

UDP Segment Header and Operation

- UDP is commonly used by DNS, TFTP, NFS, and SNMP. It is also used with real-time applications such as media streaming or VoIP. UDP is a connectionless transport layer protocol. It has much lower overhead than TCP because it is not connection-oriented and does not offer the sophisticated retransmission, sequencing, and flow control mechanisms that provide reliability.
- These reliability functions are not provided by the transport layer protocol and must be implemented elsewhere if required.
- The low overhead of UDP makes it very desirable for protocols that make simple request and reply transactions.



© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

UDP Attacks

- UDP is not protected by any encryption. You can add encryption to UDP, but it is not available by default. The lack of encryption means that anyone can see the traffic, change it, and send it on to its destination.
- **UDP Flood Attacks:** The threat actor uses a tool like UDP Unicorn or Low Orbit Ion Cannon. These tools send a flood of UDP packets, often from a spoofed host, to a server on the subnet. The program will sweep through all the known ports trying to find closed ports. This will cause the server to reply with an ICMP port unreachable message. Because there are many closed ports on the server, this creates a lot of traffic on the segment, which uses up most of the bandwidth. The result is very similar to a DoS attack.

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

3.8 IP Services

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

ARP Vulnerabilities

- Hosts broadcast an ARP Request to other hosts on the segment to determine the MAC address of a host with a particular IP address. The host with the matching IP address in the ARP Request sends an ARP Reply.
- Any client can send an unsolicited ARP Reply called a “gratuitous ARP.” When a host sends a gratuitous ARP, other hosts on the subnet store the MAC address and IP address contained in the gratuitous ARP in their ARP tables.
- This feature of ARP also means that any host can claim to be the owner of any IP or MAC. A threat actor can poison the ARP cache of devices on the local network, creating an MITM attack to redirect traffic.

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

ARP Cache Poisoning

ARP cache poisoning can be used to launch various man-in-the-middle attacks.

1. PC-A requires the MAC address of its default gateway (R1); therefore, it sends an ARP Request for the MAC address of 192.168.10.1.
2. R1 updates its ARP cache with the IP and MAC addresses of PC-A. R1 sends an ARP Reply to PC-A, which then updates its ARP cache with the IP and MAC addresses of R1.
3. The threat actor sends two spoofed gratuitous ARP Replies using its own MAC address for the indicated destination IP addresses. PC-A updates its ARP cache with its default gateway which is now pointing to the threat actor's host MAC address. R1 also updates its ARP cache with the IP address of PC-A pointing to the threat actor's MAC address.

The ARP poisoning attack can be passive or active. Passive ARP poisoning is where threat actors steal confidential information. Active ARP poisoning is where threat actors modify data in transit or inject malicious data.

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

DNS Attacks

- The Domain Name Service (DNS) protocol defines an automated service that matches resource names, such as www.cisco.com, with the required numeric network address, such as the IPv4 or IPv6 address. It includes the format for queries, responses, and data and uses resource records (RR) to identify the type of DNS response.
- Securing DNS is often overlooked. However, it is crucial to the operation of a network and should be secured accordingly.
- DNS attacks include the following:
  - DNS open resolver attacks
  - DNS stealth attacks
  - DNS domain shadowing attacks
  - DNS tunneling attacks

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

DNS Attacks (Cont.)

DNS Open Resolver Attacks: A DNS open resolver answers queries from clients outside of its administrative domain. DNS open resolvers are vulnerable to multiple malicious activities described in the table.

DNS Resolver Vulnerabilities	Description
DNS cache poisoning attacks	Threat actors send spoofed, falsified record resource (RR) information to a DNS resolver to redirect users from legitimate sites to malicious sites. DNS cache poisoning attacks can all be used to inform the DNS resolver to use a malicious name server that is providing RR information for malicious activities.
DNS amplification and reflection attacks	Threat actors use DoS or DDoS attacks on DNS open resolvers to increase the volume of attacks and to hide the true source of an attack. Threat actors send DNS messages to the open resolvers using the IP address of a target host. These attacks are possible because the open resolver will respond to queries from anyone asking a question.
DNS resource utilization attacks	A DoS attack that consumes the resources of the DNS open resolvers. This DoS attack consumes all the available resources to negatively affect the operations of the DNS open resolver. The impact of this DoS attack may require the DNS open resolver to be rebooted or services to be stopped and restarted.

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

DNS Attacks (Cont.)

DNS Stealth Attacks: To hide their identity, threat actors also use the DNS stealth techniques described in the table to carry out their attacks.

DNS Stealth Techniques	Description
Fast Flux	Threat actors use this technique to hide their phishing and malware delivery sites behind a quickly-changing network of compromised DNS hosts. The DNS IP addresses are continuously changed within minutes. Botnets often employ Fast Flux techniques to effectively hide malicious servers from being detected.
Double IP Flux	Threat actors use this technique to rapidly change the hostname to IP address mappings and to also change the authoritative name server. This increases the difficulty of identifying the source of the attack.
Domain Generation Algorithms	Threat actors use this technique in malware to randomly generate domain names that can then be used as rendezvous points to their command and control (C&C) servers.

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

DNS Attacks (Cont.)

DNS Domain Shadowing Attacks: Domain shadowing involves the threat actor gathering domain account credentials in order to silently create multiple sub-domains to be used during the attacks. These subdomains typically point to malicious servers without alerting the actual owner of the parent domain.

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

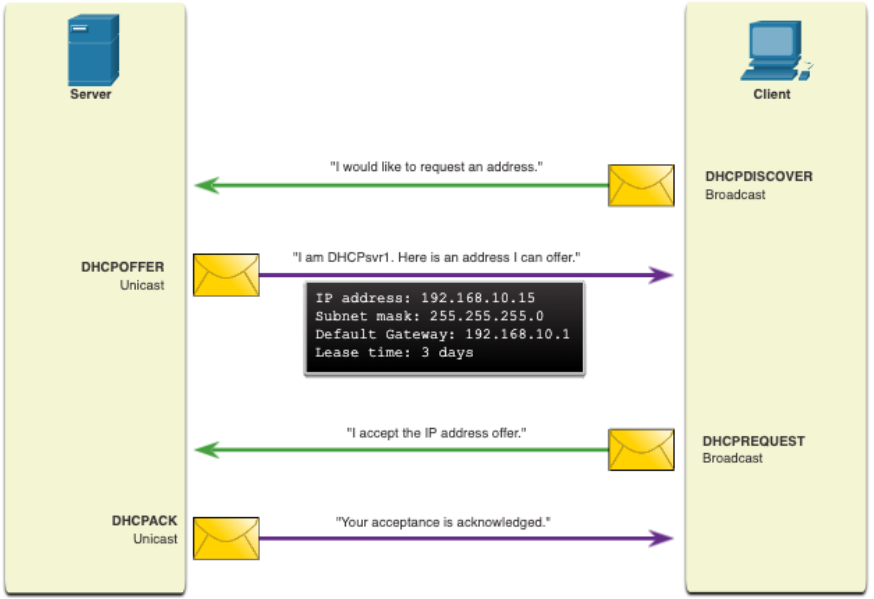
DNS Tunneling

- Threat actors who use DNS tunneling place non-DNS traffic within DNS traffic. This method often circumvents security solutions when a threat actor wishes to communicate with bots inside a protected network, or exfiltrate data from the organization. This is how DNS tunneling works for CnC commands sent to a botnet:
  1. The command data is split into multiple encoded chunks.
  2. Each chunk is placed into a lower level domain name label of the DNS query.
  3. Because there is no response from the local or networked DNS for the query, the request is sent to the ISP's recursive DNS servers.
  4. The recursive DNS service will forward the query to the threat actor's authoritative name server.
  5. The process is repeated until all the queries containing the chunks of are sent.
  6. When the threat actor's authoritative name server receives the DNS queries from the infected devices, it sends responses for each DNS query, which contain the encapsulated, encoded CnC commands.
  7. The malware on the compromised host recombines the chunks and executes the commands hidden within the DNS record.
- To stop DNS tunneling, the network administrator must use a filter that inspects DNS traffic. Pay close attention to DNS queries that are longer than average, or those that have a suspicious domain name.

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

DHCP

- DHCP servers dynamically provide IP configuration information to clients.
- In the figure, a client broadcasts a DHCP discover message. The DHCP responds with a unicast offer that includes addressing information the client can use. The client broadcasts a DHCP request to tell the server that the client accepts the offer. The server responds with a unicast acknowledgment accepting the request.



© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

DHCP Attacks

- A **DHCP spoofing attack** occurs when a rogue DHCP server is connected to the network and provides false IP configuration parameters to legitimate clients. A rogue server can provide a variety of misleading information:
  - **Wrong default gateway** - Threat actor provides an invalid gateway, or the IP address of its host to create a MITM attack. This may go entirely undetected as the intruder intercepts the data flow through the network.
  - **Wrong DNS server** - Threat actor provides an incorrect DNS server address pointing the user to a malicious website.
  - **Wrong IP address** - Threat actor provides an invalid IP address, invalid default gateway IP address, or both. The threat actor then creates a DoS attack on the DHCP client.

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

DHCP Attacks (Cont.)

Assume a threat actor has successfully connected a rogue DHCP server to a switch port on the same subnet as the target clients. The goal of the rogue server is to provide clients with false IP configuration information.

1. The client broadcasts a DHCP Discover request looking for a response from a DHCP server. Both servers receive the message.
2. The legitimate and rogue DHCP servers each respond with valid IP configuration parameters. The client replies to the first offer received
3. The client received the rogue offer first. It broadcasts a DHCP request accepting the parameters from the rogue server. The legitimate and rogue server each receive the request.
4. Only the rogue server unicasts a reply to the client to acknowledge its request. The legitimate server stops communicating with the client because the request has already been acknowledged.

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

3.9 Network Security Best Practices

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Confidentiality, Availability, and Integrity

- Network security consists of protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction.
- Most organizations follow the CIA information security triad:
  - **Confidentiality** - Only authorized individuals, entities, or processes can access sensitive information. It may require using cryptographic encryption algorithms such as AES to encrypt and decrypt data.
  - **Integrity** - Refers to protecting data from unauthorized alteration. It requires the use of cryptographic hashing algorithms such as SHA.
  - **Availability** - Authorized users must have uninterrupted access to important resources and data. It requires implementing redundant services, gateways, and links.

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

The Defense-in-Depth Approach

- To ensure secure communications across both public and private networks, you must secure devices including routers, switches, servers, and hosts. Most organizations employ a defense-in-depth approach to security. It requires a combination of networking devices and services working together.
- Several security devices and services are implemented.
  - VPN
  - ASA Firewall
  - IPS
  - ESA/WSA
  - AAA Server
- All network devices including the router and switches are hardened.
- You must also secure data as it travels across various links.

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Firewalls

A firewall is a system, or group of systems, that enforces an access control policy between networks.

Allow traffic from any external address to the web server.

Allow traffic to FTP server.

Allow traffic to SMTP server.

Allow traffic to internal IMAP server.

Deny all inbound traffic with network addresses matching internal-registered IP addresses.

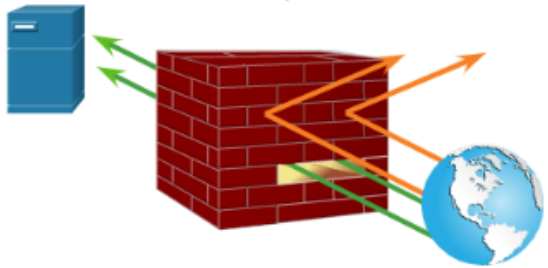
Deny all inbound traffic to server from external addresses.

Deny all inbound ICMP echo request traffic.

Deny all inbound MS Active Directory queries.

Deny all inbound traffic to MS SQL server queries.

Deny all MS Domain Local Broadcasts.



© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

IPS

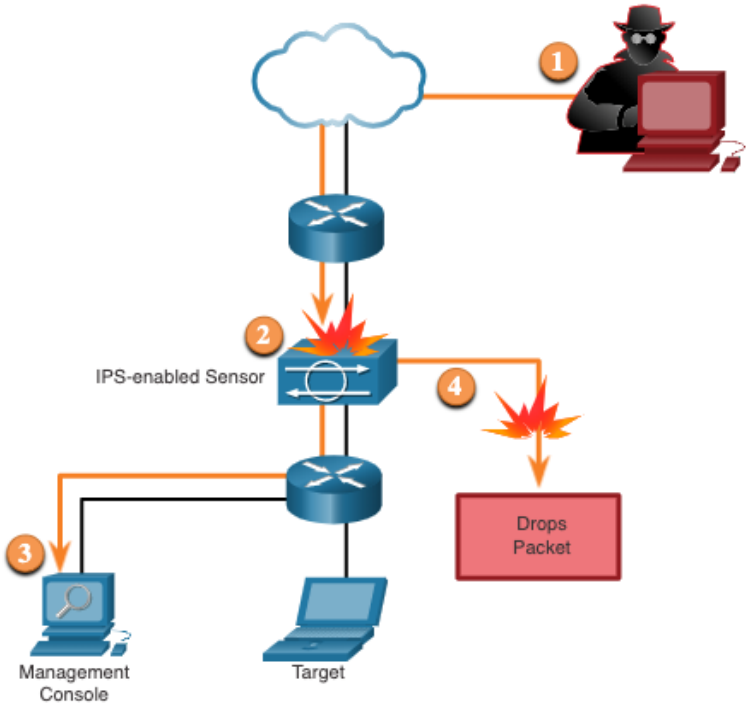
- To defend against fast-moving and evolving attacks, you may need cost-effective detection and prevention systems integrated into the entry and exit points of the network.
- IDS and IPS technologies share several characteristics. IDS and IPS technologies are both deployed as sensors. An IDS or IPS sensor can be in the form of several different devices:
  - A router configured with Cisco IOS IPS software
  - A device specifically designed to provide dedicated IDS or IPS services
  - A network module installed in an adaptive security appliance (ASA), switch, or router
  - IDS and IPS technologies detect patterns in network traffic using signatures, which is a set of rules that used to detect malicious activity. IDS and IPS technologies can detect atomic signature patterns (single-packet) or composite signature patterns (multi-packet).

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

IPS (Cont.)

The figure shows how an IPS handles denied traffic.

1. The threat actor sends a packet destined for the target laptop.
2. The IPS intercepts the traffic and evaluates it against known threats and the configured policies.
3. The IPS sends a log message to the management console.
4. The IPS drops the packet.



© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Content Security Devices

- The Cisco **Email Security Appliance (ESA)** is a special device designed to monitor Simple Mail Transfer Protocol (SMTP). The Cisco ESA is constantly updated by real-time feeds from the Cisco Talos. This threat intelligence data is pulled by the Cisco ESA every three to five minutes.
- The Cisco **Web Security Appliance (WSA)** is a mitigation technology for web-based threats. The Cisco WSA combines advanced malware protection, application visibility and control, acceptable use policy controls, and reporting.
- Cisco WSA provides complete control over how users access the internet. The WSA can perform blacklisting of URLs, URL-filtering, malware scanning, URL categorization, web application filtering, and encryption and decryption of web traffic.

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

3.10 Cryptography

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Securing Communications

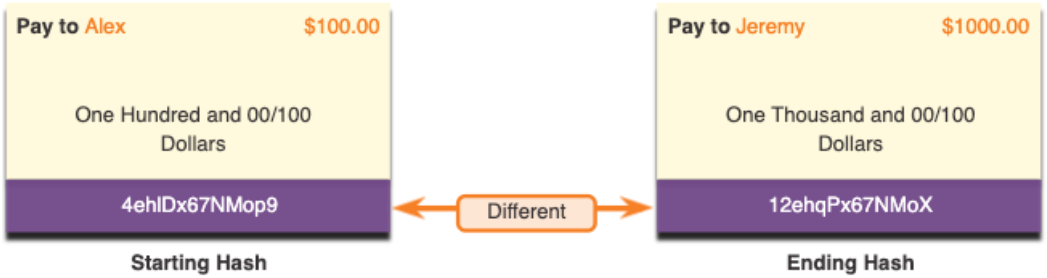
- Organizations must provide support to secure the data as it travels across links. This may include internal traffic, but it is even more important to protect the data that travels outside of the organization.
- These are the four elements of secure communications:
  - **Data Integrity** - Guarantees that the message was not altered. Integrity is ensured by implementing either Message Digest version 5 (MD5) or Secure Hash Algorithm (SHA) hash-generating algorithms.
  - **Origin Authentication** - Guarantees that the message is not a forgery and does come from whom it states. Many modern networks ensure authentication with protocols, such as hash message authentication code (HMAC).
  - **Data Confidentiality** - Guarantees that only authorized users can read the message. Data confidentiality is implemented using symmetric and asymmetric encryption algorithms.
  - **Data Non-Repudiation** - Guarantees that the sender cannot repudiate, or refute, the validity of a message sent. Nonrepudiation relies on the fact that only the sender has the unique characteristics or signature for how that message is treated.
- Cryptography can be used almost anywhere that there is data communication. In fact, the trend is toward all communication being encrypted.

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Data Integrity

- Hash functions are used to ensure the integrity of a message. They guarantee that message data has not changed accidentally or intentionally.
- In the figure, the sender is sending a $100 money transfer to Alex. The sender wants to ensure that the message is not altered on its way to the receiver.

1. The sending device inputs the message into a hashing algorithm and computes its fixed-length hash of 4ehiDx67NMop9.
2. This hash is then attached to the message and sent to the receiver. Both the message and the hash are in plaintext.
3. The receiving device removes the hash from the message and inputs the message into the same hashing algorithm. If the computed hash is equal to the one that is attached to the message, the message has not been altered during transit. If the hashes are not equal, then the integrity of the message can no longer be trusted.



© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

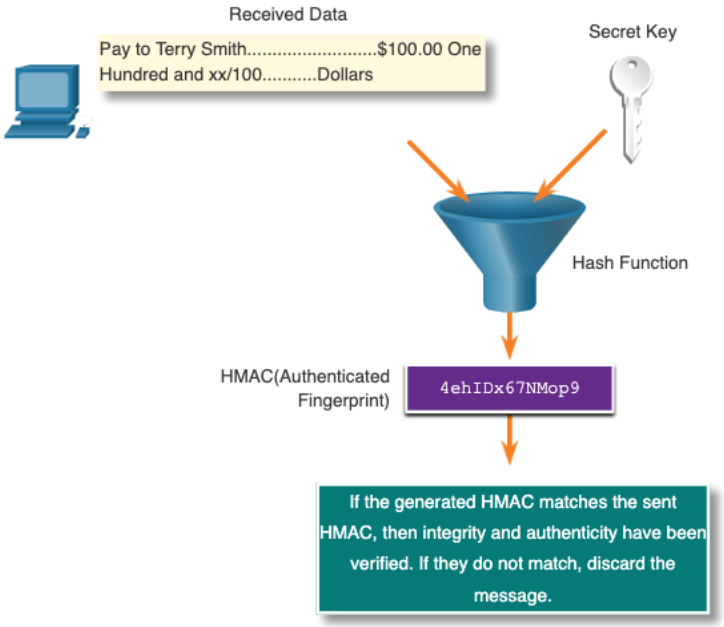
Hash Functions

- There are three well-known hash functions.
  - **MD5 with 128-bit Digest:** MD5 is a one-way function that produces a 128-bit hashed message. MD5 is a legacy algorithm that should only be used when no better alternatives are available. Use SHA-2 instead.
  - **SHA Hashing Algorithm:** SHA-1 is very similar to the MD5 hash functions. SHA-1 creates a 160-bit hashed message and is slightly slower than MD5. SHA-1 has known flaws and is a legacy algorithm. Use SHA-2 when possible.
  - **SHA-2:** This includes SHA-224 (224 bit), SHA-256 (256 bit), SHA-384 (384 bit), and SHA-512 (512 bit). SHA-256, SHA-384, and SHA-512 are next-generation algorithms and should be used whenever possible.
- While hashing can be used to detect accidental changes, it cannot be used to guard against deliberate changes. This means that anyone can compute a hash for any data, if they have the correct hash function.
- Therefore, hashing is vulnerable to man-in-the-middle attacks and does not provide security to transmitted data.

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Origin Authentication

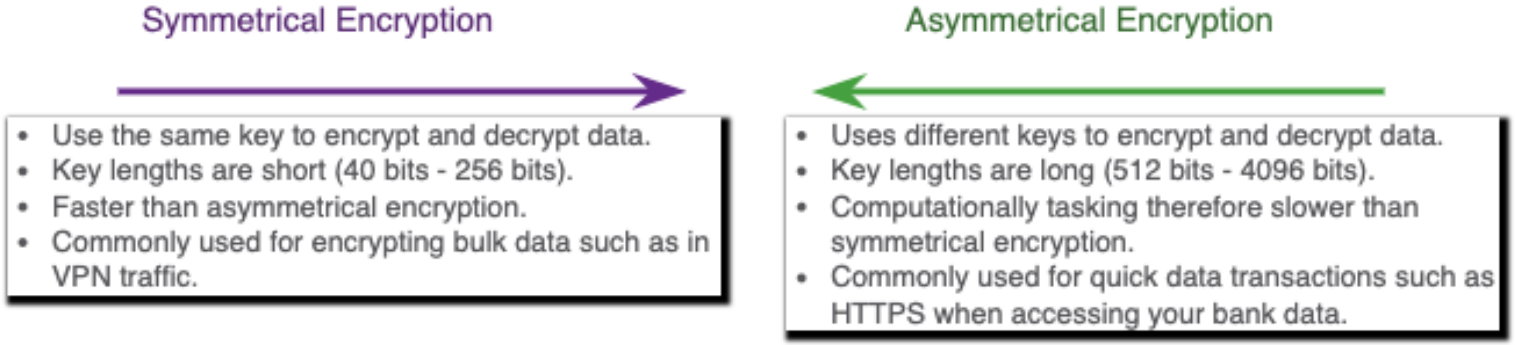
- To add authentication to integrity assurance, use a keyed-hash message authentication code (HMAC).
- An HMAC is calculated using any cryptographic algorithm that combines a cryptographic hash function with a secret key.
- Only parties who have access to that secret key can compute the digest of an HMAC function. This defeats man-in-the-middle attacks and provides authentication of the data origin.



© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Data Confidentiality

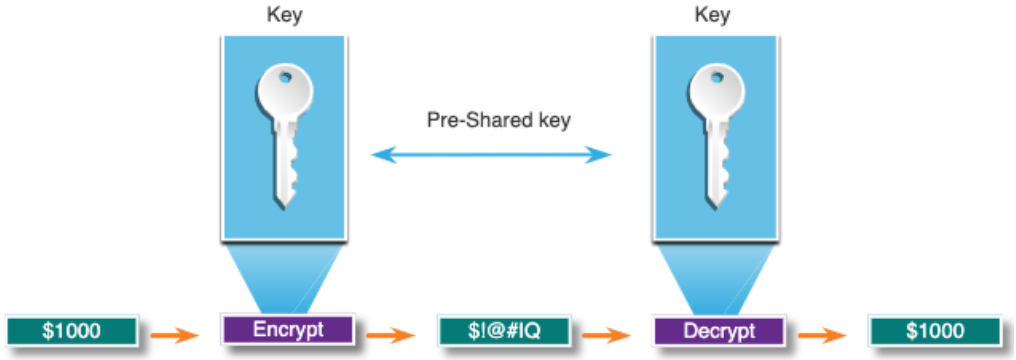
- There are two classes of encryption used to provide data confidentiality. These two classes differ in how they use keys.
- Symmetric encryption algorithms such as (DES), 3DES, and Advanced Encryption Standard (AES) are based on the premise that each communicating party knows the pre-shared key. Data confidentiality can also be ensured using asymmetric algorithms, including Rivest, Shamir, and Adleman (RSA) and the public key infrastructure (PKI).
- The figure highlights some differences between each encryption algorithm method.



© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Symmetric Encryption

- Symmetric algorithms use the same pre-shared key, also called a secret key, to encrypt and decrypt data. A pre-shared key is known by the sender and receiver before any encrypted communications can take place.
- Symmetric encryption algorithms are commonly used with VPN traffic because they use less CPU resources than asymmetric encryption algorithms.
- When using symmetric encryption algorithms, the longer the key, the longer it will take for someone to discover the key. To ensure that the encryption is safe, use a minimum key length of 128 bits.



© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Symmetric Encryption (Cont.)

Symmetric Encryption Algorithms	Description
Data Encryption Algorithm (DES)	This is a legacy symmetric encryption algorithm. It can be used in stream cipher mode but usually operates in block mode by encrypting data in 64-bit block size. A stream cipher encrypts one byte or one bit at a time.
3DES (Triple DES)	This is a newer version of DES, but it repeats the DES algorithm process three times. It is considered very trustworthy when implemented using very short key lifetimes.
Advanced Encryption Standard (AES)	AES is a secure and more efficient algorithm than 3DES. It is a popular and recommended symmetric encryption algorithm. It offers nine combinations of key and block length by using a variable key length of 128-, 192-, or 256-bit key to encrypt data blocks that are 128, 192, or 256 bits long.
Software-Optimized Encryption Algorithm (SEAL)	SEAL is a faster alternative symmetric encryption algorithm to DES, 3DES, and AES. It uses a 160-bit encryption key and has a lower impact on the CPU compared to other software-based algorithms.
Rivest ciphers (RC) series algorithms	This algorithm was developed by Ron Rivest. Several variations have been developed, but RC4 is the most prevalent in use. RC4 is a stream cipher and is used to secure web traffic in SSL and TLS.

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Asymmetric Encryption

- Asymmetric algorithms, also called public-key algorithms, are designed so that the key that is used for encryption is different from the key that is used for decryption.
- Asymmetric algorithms use a public key and a private key. The complementary paired key is required for decryption. Data encrypted with the public key requires the private key to decrypt. Asymmetric algorithms achieve confidentiality, authentication, and integrity by using this process.
- Because neither party has a shared secret, very long key lengths must be used. Asymmetric encryption can use key lengths between 512 to 4,096 bits. Key lengths greater than or equal to 1,024 bits can be trusted while shorter key lengths are considered unreliable.

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Asymmetric Encryption (Cont.)

- Examples of protocols that use asymmetric key algorithms include:
  - **Internet Key Exchange (IKE) -** This is a fundamental component of IPsec VPNs.
  - **Secure Socket Layer (SSL) -** This is now implemented as IETF standard Transport Layer Security (TLS).
  - **Secure Shell (SSH) -** This protocol provides a secure remote access connection to network devices.
  - **Pretty Good Privacy (PGP) -** This computer program provides cryptographic privacy and authentication. It is often used to increase the security of email communications.
- Asymmetric algorithms are substantially slower than symmetric algorithms. Their design is based on computational problems, such as factoring extremely large numbers or computing discrete logarithms of extremely large numbers.
- Because they are slow, asymmetric algorithms are typically used in low-volume cryptographic mechanisms, such as digital signatures and key exchange.

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Asymmetric Encryption (Cont.)

Asymmetric Encryption Algorithm	Key Length	Description
Diffie-Hellman (DH)	512, 1024, 2048, 3072, 4096	The Diffie-Hellman algorithm allows two parties to agree on a key that they can use to encrypt messages they want to send to each other. The security of this algorithm depends on the assumption that it is easy to raise a number to a certain power, but difficult to compute which power was used given the number and the outcome.
Digital Signature Standard (DSS) and Digital Signature Algorithm (DSA)	512 - 1024	DSS specifies DSA as the algorithm for digital signatures. DSA is a public key algorithm based on the ElGamal signature scheme. Signature creation speed is similar to RSA but is 10 to 40 times slower for verification.
Rivest, Shamir, and Adleman encryption algorithms (RSA)	512 to 2048	RSA is for public-key cryptography that is based on the current difficulty of factoring very large numbers. It is the first algorithm known to be suitable for signing as well as encryption. It is widely used in electronic commerce protocols and is believed to be secure given sufficiently long keys and the use of up-to-date implementations.
ElGamal	512 - 1024	An asymmetric key encryption algorithm for public-key cryptography which is based on the Diffie-Hellman key agreement. A disadvantage of the ElGamal system is that the encrypted message becomes very big, about twice the size of the original message and for this reason it is only used for small messages such as secret keys.
Elliptical curve techniques	160	Elliptic curve cryptography can be used to adapt many cryptographic algorithms, such as Diffie-Hellman or ElGamal. The main advantage of elliptic curve cryptography is that the keys can be much smaller.

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

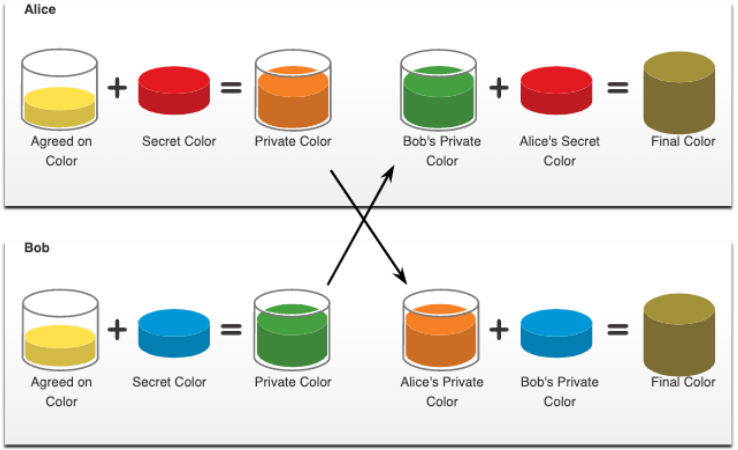
Diffie-Hellman

- Diffie-Hellman (DH) is an asymmetric mathematical algorithm where two computers generate an identical shared secret key without having communicated before. The new shared key is never actually exchanged between the sender and receiver.
- Here are three examples of instances when DH is commonly used:
  - Data is exchanged using an IPsec VPN.
  - Data is encrypted on the internet using either SSL or TLS.
  - SSH data is exchanged.
- DH security uses unbelievably large numbers in its calculations.
- Unfortunately, asymmetric key systems are extremely slow for any sort of bulk encryption. Therefore, it is common to encrypt the bulk of the traffic using a symmetric algorithm, such as 3DES or AES and then use the DH algorithm to create keys that will be used by the encryption algorithm.

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Diffie-Hellman (Cont.)

- The colors in the figure will be used instead of numbers to simplify the DH key agreement process. The DH key exchange begins with Alice and Bob agreeing on an arbitrary common color that does not need to be kept secret. The agreed upon color in our example is yellow.
- Next, Alice and Bob will each select a secret color. Alice chose red while Bob chose blue. These secret colors will never be shared with anyone. The secret color represents the chosen secret private key of each party.
- Alice and Bob now mix the shared common color (yellow) with their respective secret color to produce a private color. Therefore, Alice will mix the yellow with her red color to produce a private color of orange. Bob will mix the yellow and the blue to produce a private color of green.
- Alice sends her private color (orange) to Bob and Bob sends his private color (green) to Alice.
- Alice and Bob each mix the color they received with their own, original secret color (Red for Alice and blue for Bob.). The result is a final brown color mixture that is identical to the other's final color mixture. The brown color represents the resulting shared secret key between Bob and Alice.



© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

3.11 Module Practice and Quiz

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

What Did I Learn In This Module?

- Network security breaches can disrupt e-commerce, cause the loss of business data, threaten people's privacy, and compromise the integrity of information.
- Vulnerabilities must be addressed before they become a threat and are exploited. Mitigation techniques are required before, during, and after an attack.
- An attack vector is a path by which a threat actor can gain access to a server, host, or network. Attack vectors originate from inside or outside the corporate network.
- The term 'threat actor' includes hackers and any device, person, group, or nation state that is, intentionally or unintentionally, the source of an attack.
- Attack tools have become more sophisticated and highly automated. These new tools require less technical knowledge to implement.
- Common types of attacks are: eavesdropping, data modification, IP address spoofing, password-based, denial-of-service, man-in-the-middle, compromised-key, and sniffer.
- The three most common types of malware are worms, viruses, and Trojan horses.
- Networks are susceptible to the following types of attacks: reconnaissance, access, and DoS.
- Types of access attacks are: password, spoofing, trust exploitations, port redirections, man-in-the-middle, and buffer overflow.
- IP attack techniques include: ICMP, amplification and reflection, address spoofing, MITM, and session hijacking.

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

What Did I Learn In This Module?

- Threat actors use ICMP for reconnaissance and scanning attacks. They launch information-gathering attacks to map out a network topology, discover which hosts are active (reachable), identify the host operating system (OS fingerprinting), and determine the state of a firewall. Threat actors often use amplification and reflection techniques to create DoS attacks.
- TCP attacks include: TCPSYN Flood attack, TCP reset attack, and TCP Session hijacking. UDP Flood attacks send a flood of UDP packets, often from a spoofed host, to a server on the subnet. The result is very similar to a DoS attack.
- Any client can send an unsolicited ARP Reply called a “gratuitous ARP.” This mean that any host can claim to be the owner of any IP or MAC. A threat actor can poison the ARP cache of devices on the local network, creating an MITM attack to redirect traffic.
- DNS attacks include: open resolver attacks, stealth attacks, domain shadowing attacks, and tunneling attacks. To stop DNS tunneling, the network administrator must use a filter that inspects DNS traffic.
- A DHCP spoofing attack occurs when a rogue DHCP server is connected to the network and provides false IP configuration parameters to legitimate clients.
- Most organizations follow the CIA information security triad: confidentiality, integrity, and availability.
- To ensure secure communications across both public and private networks, you must secure devices including routers, switches, servers, and hosts. This is known as defense-in-depth.

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

What Did I Learn In This Module?

- A firewall is a system, or group of systems, that enforces an access control policy between networks.
- To defend against fast-moving and evolving attacks, you may need an intrusion detection systems (IDS), or the more scalable intrusion prevention systems (IPS).
- The four elements of secure communications are data integrity, origin authentication, data confidentiality, and data non-repudiation.
- Hash functions guarantee that message data has not changed accidentally or intentionally.
- Three well-known hash functions are MD5 with 128-bit digest, SHA hashing algorithm, and SHA-2.
- To add authentication to integrity assurance, use a keyed-hash message authentication code (HMAC). HMAC is calculated using any cryptographic algorithm that combines a cryptographic hash function with a secret key.
- Symmetric encryption algorithms using DES, 3DES, AES, SEAL, and RC are based on the premise that each communicating party knows the pre-shared key.
- Data confidentiality can also be ensured using asymmetric algorithms, including Rivest, Shamir, and Adleman (RSA) and the public key infrastructure (PKI). Diffie-Hellman (DH) is an asymmetric mathematical algorithm where two computers generate an identical shared secret key without having communicated before.

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential


CISCO