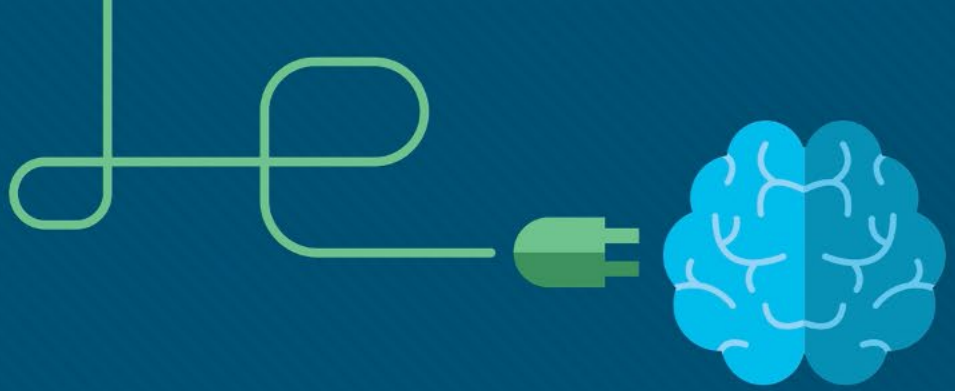


Module 1: Cybersecurity Threats, Vulnerabilities, and Attacks

Cybersecurity Essentials 3.0

Module Objectives

Module Title: Cybersecurity Threats, Vulnerabilities, and Attacks

Module Objective: Explain how threat actors execute some of the most common types of cyber attacks.

Topic Title	Topic Objective
Common Threats	Explain the threats, vulnerabilities, and attacks that occur in the various domains.
Deception	Identify the different deception methods used by attackers to deceive their victims.
Cyber Attacks	Describe some common types of network attacks.
Wireless and Mobile Device Attacks	Describe common types of wireless and mobile device attacks.
Application Attacks	Describe types of application attacks.

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

1.1 Common Threats

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Threat Domains

A ‘threat domain’ is considered an area of control, authority, or protection that attackers can exploit to gain access to a system.

Attackers can exploit systems within a domain through:

- Direct, physical access to systems and networks.
- Wireless networking extends beyond an organization’s boundaries.
- Bluetooth or near-field communication (NFC) devices.
- Malicious email attachments.
- Less secure elements within an organization’s supply chain.
- An organization’s social media accounts.
- Removable media such as flash drives.
- Cloud-based applications.

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Types of Cyber Threats

Category	Types of Cyber Threats
Software Attacks	• A successful denial-of-service (DoS attack). • A computer virus.
Software Errors	• A software bug. • An application going offline. • A cross-site script or illegal file server share.
Sabotage	• An authorized user compromising an organization's primary database. • The defacement of an organization's website.
Human Error	• Inadvertent data entry errors. • A firewall misconfiguration.
Theft	• Laptops or equipment being stolen from an unlocked room.
Hardware Failures	• Hard drive crashes
Utility Interruption	• Electrical power outages. • Water damage resulting from sprinkler failure.
Natural Disasters	• Severe storms such as hurricanes or tornados. • Earthquakes. • Floods. • Fires.

Internal vs External Threats

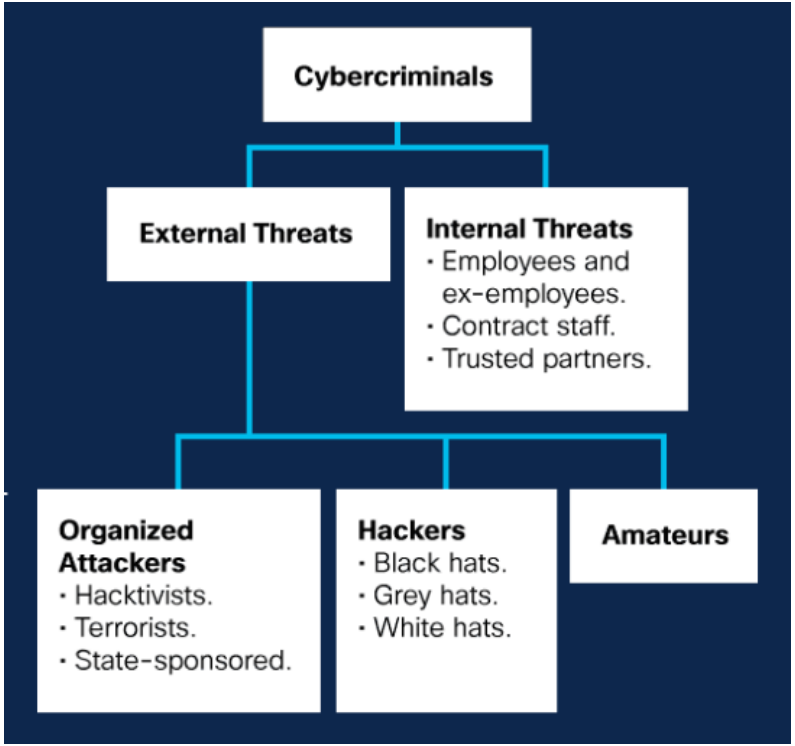
Valuable, sensitive information is personnel records, intellectual property, and financial data.

Internal threats

- Accidentally or intentionally carried out by current or former employees and other contract partners.
- Operation of servers or network infrastructure devices are compromised by connecting infected media or by accessing malicious emails or websites.

External threats

- It usually comes from amateur or skilled attackers.
- Attacks can exploit vulnerabilities in networked devices or can use social engineering techniques.



© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

User Threats and Vulnerabilities

A user domain includes anyone accessing an organization's information system, including employees, customers, and contract partners. Users are the weakest link in information security systems, posing a significant threat to the confidentiality, integrity, and availability of an organization's data.

Examples of User Threats are:

- No awareness of security policies
- Poorly enforced security policies
- Data theft
- Unauthorized activity: downloads, media, VPNs, websites
- Destruction of systems, applications, or data

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Threats to Devices

- Devices left powered on and unattended.
- Downloading files, photos, music or videos from unreliable sources.
- Software with vulnerabilities installed on an organization's devices.
- New viruses, worms and other type of malware.
- Insertion of unauthorized USB drives, CDs or DVDs on networking devices.
- No policies in place to protect an organization's IT infrastructure.
- Use of outdated hardware or software

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Threats to the Local Area Network

Examples of threats to the LAN include:

- Unauthorized access to wiring closets, data centers, and computer rooms.
- Unauthorized access to systems, applications, and data.
- Network operating system or software vulnerabilities and updates.
- Rogue users gain unauthorized access to wireless networks.
- Exploits of data in transit.
- LAN servers with different hardware or operating systems.
- Unauthorized network probing and port scanning.
- Misconfigured firewalls.

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Threats to the Private Cloud

The private cloud domain includes any private servers, resources, and IT infrastructure available to members of a single organization via the Internet.

Threats to the private cloud domain include:

- Unauthorized network probing and port scanning.
- Unauthorized access to resources.
- Router, firewall, or network device operating system or software vulnerabilities.
- Router, firewall, or network device configuration errors.
- Remote users access an organization's infrastructure and download sensitive data.

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Threats to the Public Cloud

The public cloud domain is the entire computing services hosted by a cloud, service, or Internet provider that are available to the public and shared across organizations.

Three subscription-based models of public cloud services that organizations may choose to use:

- Software as a Service (SaaS): provides organizations with software (stored in the cloud) that is centrally hosted and accessed by users via a web browser, app, or other software.
- Platform as a Service (PaaS): It allows an organization to develop, run and manage its applications on the service's hardware using its tools.
- Infrastructure as a Service (IaaS): provides virtual computing resources such as hardware, software, servers, storage, and other infrastructure components. An organization will buy access to them.

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Threats to Applications

The application domain includes all the critical systems, applications, and data used by an organization to support operations.

Common threats to applications include:

- Someone gaining unauthorized access to data centers, computer rooms, wiring closets or systems.
- Server downtime during maintenance periods.
- Network operating system software vulnerabilities.
- Data loss.
- Client-server or web application development vulnerabilities.

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Threat Complexity

Software vulnerabilities occur because of programming mistakes, protocol vulnerabilities, or system misconfigurations.

Some of the attack methods by cybercriminals are:

- Advanced persistent threat (APT): a continuous attack that uses elaborate espionage tactics involving multiple actors and sophisticated malware.

- Algorithm attacks: take advantage of algorithms in a piece of legitimate software to generate unintended behaviors.

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Backdoors and Rootkits

Cybercriminals also use many different types of malware to carry out their attacks. Some common types are:

Backdoors

- Cybercriminals use programs to gain unauthorized access to a system by bypassing the standard authentication procedures.
- A remote administrative tool (RAT) program runs on the user's machine to install a backdoor to provide administrative control over a target computer.

Rootkits

- Modify the operating system to create a backdoor, which attackers can use to access the computer remotely.
- Most use software vulnerabilities to access resources that should not be accessible (privilege escalation) and modify system files.

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Threat Intelligence and Research Sources

The United States Computer Emergency Readiness Team (US-CERT) and the U.S. Department of Homeland Security sponsored a dictionary of common vulnerabilities and exposures (CVE). Some other threat intelligence sources are:

- The dark web: An encrypted web content that requires specific software, authorization, or configurations to access, which is not indexed by conventional search engines.

- Indicator of compromise (IOC): IOCs such as malware signatures or domain names provide evidence of security breaches and details about them.

- Automated Indicator Sharing (AIS): Cybersecurity and Infrastructure Security Agency (CISA) capability enable the real-time exchange of cybersecurity threat indicators using a standardized and structured language called STIX and TAXII.

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

1.2 Deception

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Social Engineering

Social engineering is a non-technical strategy that attempts to manipulate individuals into performing specific actions or divulging confidential information.

Some common types of social engineering attacks are:

- Pretexting: This occurs when an individual lies to gain access to confidential data.
- Something for something (quid pro quo): Involves a request for personal information in exchange for something, like a gift.
- Identity fraud: Uses a person's stolen identity to obtain goods or services by deception.

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Social Engineering Tactics

Cybercriminals rely on several social engineering tactics to gain access to sensitive information:

- Authority
- Intimidation
- Consensus
- Scarcity
- Urgency
- Familiarity
- Trust

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Shoulder Surfing and Dumpster Diving

Shoulder Surfing

- A simple attack involves observing or looking over a target's shoulder to gain valuable information such as PINs, access codes, or credit card details.

- Criminals do not always have to be near their victim-to-shoulder surf — they can use binoculars or security cameras to obtain this information.

Dumpster Diving

- The process of going through a target's trash to see discarded information.

- Documents containing sensitive information should be shredded or stored in burn bags until destroyed by fire after a certain period.

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Impersonation and Hoaxes

Cybercriminals have many other deception techniques to help them succeed.

Impersonation

- Act of tricking someone into doing something they would not ordinarily do by pretending to be someone else.

- Criminals can also use impersonation to attack others.

Hoax

- An act intended to deceive or trick someone can cause just as much disruption as an actual security breach.

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Piggybacking and Tailgating

They occur when a criminal follows an authorized person to gain physical entry into a secure location or a restricted area.

Criminals can achieve this by:

- Giving the appearance of being escorted into the facility by an authorized person.
- Joining and pretending to be part of a large crowd that enters the facility.
- Targeting an authorized person who is careless about the rules of the facility.

One way of preventing this is to use two sets of doors (mantrap) which means individuals enter through an outer door and must close before gaining access through an inner door.

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Other Methods of Deception

Be aware that attackers have many more tricks up their sleeve to deceive their victims.

Some of these methods are:

- Invoice scam
- Watering hole attack
- Typosquatting
- Prepending
- Influence campaigns

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Defending Against Deception

Organizations must promote awareness of social engineering tactics and adequately educate employees on prevention measures. Here are some top tips:

- Never disclose confidential information or credentials via email, chat, text messages, in-person, or phone to unknown parties.
- Resist the urge to click on enticing emails and web links.
- Be wary of uninitiated or automatic downloads.
- Establish and educate employees on key security policies.
- Encourage employees to take ownership of security issues.
- Do not give in to pressure from unknown individuals.

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Lab - Explore Social Engineering Techniques

In this lab, you will complete the following objectives:

- Part 1: Explore Social Engineering Techniques
- Part 2: Create a Cybersecurity Awareness Poster

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

1.3 Cyber Attacks

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

What's the Difference?

Cybercriminals use many different types of malware to carry out attacks.

The three most common types of malware are:

Virus
- Type of computer program that, when executed, replicates and attaches itself to other files, such as a legitimate program, by inserting its code into it.

Worms
- It replicates by independently exploiting vulnerabilities in networks.

Trojan horse
- It carries out malicious operations by masking its true intent. It might appear legitimate but is, in fact, very dangerous.

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Logic Bombs

- A malicious program that waits for a trigger, such as a specified date or database entry, to set off the malicious code. Until this trigger event happens, the logic bomb will remain inactive.
- Once activated, it implements a malicious code that causes harm to a computer in various ways. It can sabotage database records, erase files and attack operating systems or applications.
- Logic bombs attack and destroy the hardware components in a device or server, including the cooling fans, CPU, memory, hard drives, and power supplies were recently discovered.

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Ransomware

- Designed to hold a computer system or the data it contains captive until completed payment.
- It usually works by encrypting data so the owner cannot access it.
- A demanded ransom paid through an untraceable payment system, the cybercriminal provides a program that decrypts files or sends an unlock code – but many victims do not gain access to their data even after paying.
- Some versions of ransomware can take advantage of specific system vulnerabilities to lock it down.
- Spread through phishing emails that encourage downloading malicious attachments or a software vulnerability.

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Denial of Service Attacks

The type of network attack is relatively simple to conduct, even for an unskilled attacker. They usually result in some interruption to network services, causing a significant loss of time and money.

The two main types of DoS attacks are:

- The overwhelming quantity of traffic: When a network, host, or application sends an enormous amount of data at a rate it cannot handle, it causes a slow transmission or response or causes the device or service to crash.

- Maliciously formatted packets: Sends a maliciously formatted packet, and the receiver will be unable to handle it.

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Domain Name System

- Many essential technical services are needed for a network to operate, such as routing, addressing, and domain naming. These are prime targets for attack.
- Cybercriminals can take advantage of vulnerabilities in DNS services to launch the following attacks:

Domain reputation	The DNS is used by DNS servers to translate a domain name into a numerical IP address so that computers can understand it. If a DNS server does not know an IP address, it will ask another DNS server. An organization needs to monitor its domain reputation, including its IP address, to help protect against malicious external domains.
DNS spoofing (DNS cache poisoning)	Attack in which false data is introduced into a DNS resolver cache — the temporary database on a computer's operating system that records recent visits to websites and other Internet domains. These poison attacks exploit a weakness in the DNS software that causes the DNS servers to redirect traffic for a specific domain to the attacker's computer.
Domain hijacking	When an attacker wrongfully gains control of a target's DNS information, they can make unauthorized changes to it.
Uniform resource location (URL)	A unique identifier for finding a specific resource on the Internet. Redirecting a URL commonly happens for legitimate purposes.

Layer 2 Attacks

Attackers often take advantage of vulnerabilities in layer two security.

Some examples of attacks are:

Spoofing
- MAC address spoofing
- ARP spoofing
- IP spoofing

MAC Flooding
- It compromises the data transmitted to a device. An attacker floods the network with fake MAC addresses, compromising the security of the network switch.

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Man-in-the-Middle and Man-in-the-Mobile Attacks

Attackers can intercept or modify communications between two devices to steal information from or impersonate one of the devices.

MitM (Man-in-the-Middle)

- It happens when a cybercriminal takes control of a device without the user's knowledge.
- With this level of access, an attacker can intercept, manipulate and relay false information between the sender and the intended destination.

MitMO (Man-in-the-Mobile)

- A MitMO variation is a type of attack used to take control of a user's mobile device.
- When infected, the mobile device instructs to exfiltrate user-sensitive information and send it to the attackers.

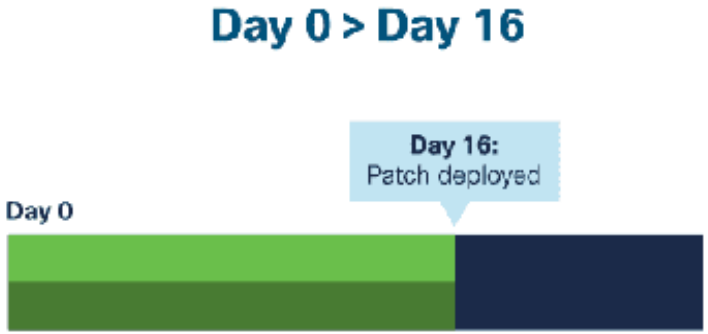
© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Zero-Day Attacks

•It exploits software vulnerabilities before they become known or before the software vendor discloses them.

•A network is highly vulnerable to attack between the time an exploit is discovered (zero hours) and the time it takes for the software vendor to develop and release a patch that fixes this exploit.

•Defending against such fast-moving attacks requires network security professionals to adopt a more sophisticated and holistic view of any network architecture.



© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Keyboard Logging

- It refers to recording or logging every key struck on a computer's keyboard.
- Cybercriminals log keystrokes via software installed on a computer system or through hardware devices that are physically attached to a computer and configure the keylogger software to send the log file to the criminal.
- Because it has recorded all keystrokes, this log file can reveal usernames, passwords, websites visited, and other sensitive information.
- Many anti-spyware suites can detect and remove unauthorized key loggers.

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Defending Against Attacks

Organizations can take several steps to defend against various attacks. These include:

- Configure firewalls to remove any packets from outside the network with addresses indicating that they originated inside the network.
- Ensure patches and upgrades are current.
- Distribute the workload across server systems.
- Network devices use ICMP packets to send error and control messages. Organizations can block external ICMP packets with their firewalls to prevent DoS and DDoS attacks.

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

1.4 Wireless and Mobile Device Attacks

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Grayware and Smishing

Grayware

- Any unwanted application that behaves in an annoying or undesirable manner.

- And while grayware may not carry any recognizable malware, it may still pose a risk to the user by, for example, tracking your location or delivering unwanted advertising.

Short message service phishing or SMiShing

- Another tactic used by attackers is to trick you.

- Fake text messages prompt you to visit a malicious website or call a fraudulent phone number, which may result in malware being downloaded onto your device or sharing personal information.

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Rogue Access Points

A rogue access point is a wireless access point installed on a secure network without explicit authorization.

Some ways of installing a rogue access point are:

- An attacker often uses social engineering tactics to gain physical access to an organization's network infrastructure and install the rogue access point.
- The access point can be set up as a MitM device to capture your login information.
- An evil twin attack describes a situation where the attacker's access point is set up to look like a better connection option. Once you connect to the evil access point, the attacker can analyze your network traffic and execute MitM attacks.

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Radio Frequency Jamming

- Wireless signals are susceptible to electromagnetic interference (EMI), radio frequency interference (RFI), and even lightning strikes or noise from fluorescent lights.
- Attackers can take advantage of this fact by deliberately jamming the transmission of a radio or satellite station to prevent a wireless signal from reaching the receiving station.
- In order to successfully jam the signal, the frequency, modulation, and power of the RF jammer need to be equal to that of the device that the attacker is seeking to disrupt.

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Bluejacking and Bluesnarfing

Due to the limited range of Bluetooth, an attacker must be within range of their target.

Some ways that they can exploit a target's device without their knowledge are:

- Bluejacking uses wireless Bluetooth technology to send unauthorized messages or shocking images to another Bluetooth device.
- Bluesnarfing occurs when an attacker copies information, such as emails and contact lists, from a target's device using a Bluetooth connection.

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Attacks Against Wi-Fi Protocols

Wired equivalent privacy (WEP) and Wi-Fi protected access (WPA) are security protocols designed to secure wireless networks.

- WEP was developed to provide a WLAN with a level of protection by encrypting the data
- WEP used a key for encryption, but WEP had no provision for key management giving criminals access to a large amount of traffic data.
- To address this and replace WEP, WPA and then WPA2 was developed as improved security protocols.
- Unlike with WEP, an attacker cannot recover WPA2's encryption key by observing network traffic.

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Wi-Fi and Mobile Defense

There are several steps that organizations and users need to take to defend against wireless and mobile device attacks:

- Take advantage of basic wireless security features such as authentication and encryption by changing the default configuration settings.
- Restrict access point placement by placing these devices outside the firewall or within a demilitarized zone — a perimeter network that protects an organization's LAN from untrusted devices.
- Use WLAN tools such as NetStumbler to detect rogue access points or unauthorized workstations.
- Develop a policy for guest access to an organization's Wi-Fi network.
- Employees in an organization should use a remote access VPN for WLAN access.

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

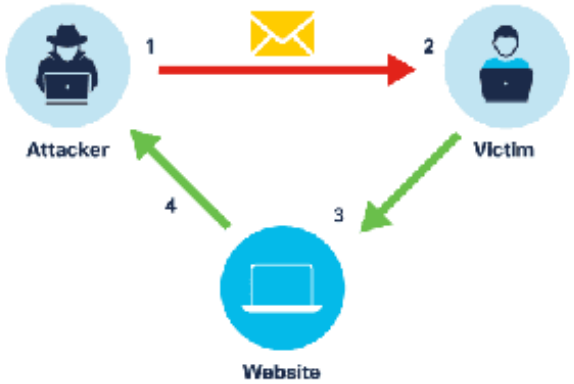
1.5 Application Attacks

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Cross-Site Scripting

Cross-site scripting (XSS) is a common vulnerability in many web applications. This is how it works:

- Cybercriminals exploit the XSS vulnerability by injecting scripts containing malicious code into a web page.
- The victim accesses the web page, and the malicious scripts unknowingly pass to their browser.
- The malicious script can access any cookies, session tokens, or other sensitive information about the user, which is sent back to the cybercriminal.
- Armed with this information, the cybercriminal can impersonate the user.



© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Code Injection

- Injection attacks exploit weaknesses in databases such as Structured Query Language (SQL) or an Extensible Markup Language (XML) that modern websites use to store and manage data.

- Some common types of injection attacks are:

XML injection attack	It can corrupt the data on the XML database and threaten the security of the website. It works by interfering with an application's processing of XML data or query entered by a user. Cybercriminals can manipulate this query by programming it to suit their needs.
SQL injection attack	Cybercriminals can carry out this attack on websites or any SQL database by inserting a malicious SQL statement in an entry field. It takes advantage of a vulnerability in which the application does not correctly filter the data entered by a user for characters in an SQL statement.
DLL injection attack	DLL injection allows a cybercriminal to trick an application into calling a malicious DLL file, which executes as part of the target process.
LDAP injection attack	LDAP is an open protocol for authenticating user access to directory services. This attack exploits input validation vulnerabilities by injecting and executing queries to LDAP servers, giving cybercriminals an opportunity to extract sensitive information from an organization's LDAP directory.

Buffer Overflow

- Buffers are memory areas allocated to an application.
- A buffer overflow occurs when data is written beyond the limits of a buffer. By changing data beyond the boundaries of a buffer, the application can access memory allocated to other processes.
- This can lead to a system crash, data compromise, or provide escalation of privileges.
- These memory flaws can also give attackers complete control over a target's device.

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Remote Code Executions

- Remote code execution allows a cybercriminal to take advantage of application vulnerabilities to execute any command with the privileges of the user running the application on the target device.
- Privilege escalation exploits a bug, design flaw, or misconfiguration in an operating system or software application to access usually restricted resources.
- The Metasploit Project is a computer security project that provides information about security vulnerabilities and aids penetration testing.
- Among the tools, they developed the Metasploit Framework, which can be used to create and execute exploit code against a remote target.

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Other Application Attacks

- Every piece of information that an attacker receives about a targeted system or application can be used as a valuable weapon for launching a dangerous attack.
- Some other types of application attacks are:

Cross-site request forgery (CSRF)	It describes the malicious exploit of a website where unauthorized commands are submitted from a user's browser to a trusted web application.
Race condition attack (time of check – TOC or time of use - TOU)	This attack happens when a computing system that is designed to handle tasks in a specific sequence is forced to perform two or more operations simultaneously.
Improper input handling attack	Data inputted by a user that is not properly validated can affect the data flow of a program and cause critical vulnerabilities in systems and applications that result in buffer overflow or SQL injection attacks.
Erro handling attack	Attackers can use error messages to extract specific information such as the hostnames of internal systems and directories or files that exist on a given web server — as well as database, table and field names that can be used to craft SQL injection attacks.

Other Application Attacks (Cont.)

Application programming interface (API) attack	An API delivers a user response to a system and sends the system's response back to the user. An API attack occurs when a cybercriminal abuses an API endpoint.
Replay attack	This describes a situation where a valid data transmission is maliciously or fraudulently repeated or delayed by an attacker, who intercepts, amends and resubmits the data to get the receiver to do whatever they want.
Directory traversal attack	Directory traversal occurs when an attacker read files on the webserver outside of the directory of the website. An attacker can then use this information to download server configuration files containing sensitive information, potentially expose more server vulnerabilities or even take control of the server!
Resource exhaustion attacks	These attacks are computer security exploits that crash, hang or otherwise interfere with a targeted program or system. Rather than overwhelming network bandwidth like a DoS attack, resource exhaustion attacks overwhelm the hardware resources available on the target's server instead.

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Defending Against Application Attacks

You can take several actions to defend against an application attack.

Some of them are:

- The first defense against an application attack is to write solid code.
- Prudent programming practice involves treating and validating all input from outside of a function as if it is hostile.
- Keep all software, including operating systems and applications, up to date, and do not ignore update prompts. Remember that not all programs update automatically.

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Spam

- Spam (junk mail) is unsolicited email and, in most cases, is an advertising method.
- A lot of spam is sent in bulk by computers infected by viruses or worms — and often contains malicious links, malware, or deceptive content that aims to trick recipients into disclosing sensitive information.
- Almost all email providers filter spam, but it still consumes bandwidth. And even if you have implemented security features, some spam might get through to you.

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Spam (Cont.)

Some indicators of spam:

- The email has no subject line.
- The email asks you to update your account details.
- The email text contains misspelled words or strange punctuation.
- Links within the email are long and cryptic.
- The email looks like correspondence from a legitimate business, but there are tiny differences — or it contains information that does not seem relevant to you.
- The email asks you to open an attachment, often urgently.

If you receive an email containing one or more indicators, you should not open the email or any attachments.

Many organizations have an email policy that requires employees to report receipt of this type of email to their cybersecurity team for further investigation. If in doubt, always write.

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Phishing

Phishing is a form of fraudulent activity often used to steal personal information.

Phishing

- It occurs when a user is contacted by email or instant message — or in any other way — by someone masquerading as a legitimate person or organization.

- The intent is to trick the recipient into installing malware on their device or into sharing personal information, such as login credentials or financial information.

Spear phishing

- A highly targeted attack, spear phishing sends customized emails to a specific person based on information the attacker knows about them — which could be their interests, preferences, activities, and work projects.

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Vishing, Pharming and Whaling

Criminals make use of a wide range of techniques to try to gain access to your personal information.

Some of their common scams are:

- Vishing: This type of attack sees criminals use voice communication technology to encourage users to divulge information, such as credit card details.
- Farming: This attack deliberately misdirects users to a fake version of an official website.
- Whaling: A phishing attack targets high-profile individuals, such as senior executives within an organization, politicians, and celebrities.

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Defending Against Email and Browser Attacks

Some of the important actions that you can take to defend against email and browser attacks:

It is difficult to stop spam, but there are ways to reduce its effects:

- Most Internet service providers (ISPs) filter spam before it reaches the user's inbox.
- Many antivirus and email software programs automatically detect and remove dangerous spam from an email inbox.
- Organizations should educate employees about the dangers of unsolicited emails and make them aware of the risks of opening attachments.
- Always scan email attachments before opening them.

Become a member of the Anti-Phishing Working Group (APWG). It is an international association of companies focused on eliminating identity theft and fraud resulting from phishing and email spoofing.

All software should be kept up-to-date, with the latest security patches, to protect against known vulnerabilities.

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

There's More...

- Some other common attacks that cybercriminals can launch are:

Physical attacks	They are intentional, offensive actions used to destroy, expose, alter, disable, steal or gain unauthorized access to an organization's infrastructure or hardware.
Adversarial artificial intelligence attacks	Machine learning is a method of automation that allows devices to carry out analysis and perform tasks without specifically being programmed to do so. It uses mathematical models to predict outcomes. However, these models are dependent on the data that is inputted. If the data is tainted, it can have a negative impact on the predicted outcome. Attackers can take advantage of this to perpetrate attacks against machine learning algorithms.
Supply chain attacks	Many organizations interface with a third party for their systems management or to purchase components and software. Organizations may even rely on parts or components from a foreign source. Attackers often find ways to intercept these supply chains.
Cloud-based attacks	Rather than developing systems on their own premises, more and more organizations are making the move toward cloud-based computing. Attackers are constantly leveraging ways to exploit sensitive data stored on the cloud, as well as applications, platforms and infrastructure that is cloud-based, as we saw with SaaS, PaaS and IaaS.

1.6 Cybersecurity Threats, Vulnerabilities, and Attacks Summary

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

What Did I Learn in this Module?

- A threat domain is an area of control, authority, or protection that attackers can exploit to gain access to a system.
- Cyber threats are classified as internal and external threats. It includes software attacks and errors, sabotage, human error, theft, hardware failures, utility interruption, and natural disasters.
- Social engineering is a non-technical strategy that attempts to manipulate individuals into performing specific actions or divulging confidential information.
- Malware is any code that can be used to steal data, bypass access controls, or cause harm to or compromise a system.
- Grayware is an unwanted application that behaves in an annoying or undesirable manner. To defend against wireless and mobile device attacks: change default configurations.
- Code Injection attacks include XML, SQL, DLL, and LDAP. Write solid code to defend against an application attack.
- Use antivirus software to defend against email and browser attacks.

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Confidential