recap

Threat domains

Its an **area of control, authority or protection that attackers can exploit to gain access to a system.**

Cyber threat categories include *software attacks and errors, sabotage, human error, theft, hardware failures, utility interruption, and natural disasters.*

Internal threats are usually carried out by current or former employees and other contract partners.

The source of an external threat typically stems from amateur or skilled attackers who can exploit vulnerabilities in networked devices, or use social engineering techniques.

A user domain includes anyone with access to an organizations information system.

*Common user threats include poorly enforced security policies, data theft, unauthorized downloads and media, unauthorized VPNs and websites, and destruction of systems, applications, or data.*

*Individual devices, LANs and private and public clouds are also bulnerable to attack.*

There are complex threats such as an APT and an algorithm attack. Cybercriminals use backdoor programs to gain unauthorized access to a system by bypassing the normal authentication procedures.

**Backdoors grant cybercriminals continued access to a system, even if the organization has fixed the original vulnerability used to attack the system.**

Most rootkits can also modify system forensics and monitoring tools, making them very hard to detect.

Deception

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

Pretexting individual lies to gain access to privileged data

Quid pro quo attacks request for personal info in exchange for smt.

Identity fraud using a persons stolen identity to obtain goods

**Tactics**

Impersonating an authority figure  
 intimidation

Consensus (everyone is doing it)

Pretending smt is scarce or that a situation is urgent

Building familiarity and trust with an employee

Shoulder surfing

Dumpster diving

Piggybacking or tailgating

Invoice scams, watering hole attacks, typosquatting, prepending,…

Cyber attacks

Malware code that can be used to steal data, bypass access controls, cause harm/compromise

Virus program that, when executed, replicates, and attaches itself to other files by inserting its own code into it

Worm malicious software program that replicates by independently exploiting vulnerabilities in networks.

Trojan horse malware that carries out malicious operations by masking its true intent

Logic bomb malicious program that waits for a trigger to set off the malicious code

Ramsomware hold os or data captive until a payment is made

DoS attacks creating an overwhelming quantity of traffic or by sending maliciously formatted packets that cannot be identified causing the device to run slowly or crash

DDoS attacks are similar but originate from multiple coordinated sources

DNS attacks include spoofing and hijacking

Layer 2 attacks

Include MAC address, ARP and IP spoofing, MAC flooding, man-in-the-middle, man-in-the-mobile

Zero-day-attacks exploit software vulnerabilities before they become known.

Keyboard logging logs keystrokes and configures the keylogger software to send the log

To defend against these attacks use firewalls, stay current on upgrades and patches, distribute the workload across server systems, and block external ICMP packets with firewalls.

Wireless and mobile device attacks

Grayware unwanted application that behaves in an annoying or undesirable manner

SMiShing fake text msg which prompt you to visit a malicious website or call

Rogue access point wireless access point instakked in a secure netwirk without authorization

Evil twin attack attackers access point is set up to look like a better connection option

Radio frequency jamming deliberately jamming the transmission of a radio or satelite station to prevent a wireless signal

Bluejacking sends unauthorized msg or shocking imgs to another bluetooth device

Bluesnarfing attacker copies info from a targets device using bluetooth

WEP and WPA security protovols that were designed to secure wireless networks

Unlike WEP an attacker cannot recover WPA2 encryption key by observing network traffic

To defend against wireless and mobile device attacks: change default configurations. Restrict access point placement by placing these devices outside the firewall or in a DMZ. Use WLAN tools to detect rogue access points or unauthorized workstations. Have a policy for guest access to a Wi-Fi network. Employees should use a remote access VPN for WLAN access.

Application and other attacks

XSS vulnerability found in many web applications. Types of code injection attacks inlude XML, SQL, DLL and LDAP

Buffer overflow occurs when data is written beyond the limits of a buffer

Remote code execution is exploiting application vulnerabilities to execute any command with the privileges of the authorized user

Other attacks include CSRF, rece condition, improper input handling, error handling, API, replay, directory traversal, and resource exhaustion

Write solid code to defend against an application attack. Treat and validate all input from outside of a function as if it is hostile. Keep all software up to date.

Spam unsolicited email that is usually a method of advertising.some is sent in bulk by pc infected with viruses or worms

Phishing user is contacted using email or instant msg by a threat actor masquerading as a legitimate person

Spear phishing sends customized emails to a specific person based on info the attacker knows about them

Other scams include vishing, pharming, whaling

Use antivirus software to defend against email and browser attacks. Never assume that email attachments are safe. Always scan attachments before opening them. Become a member of the Anti-Phishing Working Group (APWG). All software should be kept up-to-date