Module 1 Glossary

New terms and their definitions: Course 5 Week 1

Adware: Software that displays advertisements and collects data

Attack: An actual attempt at causing harm to a system

Availability: Means that the information we have is readily accessible to those people that should have it

Backdoor: A way to get into a system if the other methods to get in a system aren't allowed, it's a secret entryway for attackers

Baiting: An attack that happens through actual physical contact, enticing a victim to do something

Botnet: A collection of one or more Bots

Bots: Machines compromised by malware that are utilized to perform tasks centrally controlled by an attacker

Brute force attacks: A common password attack which consists of just continuously trying different combinations of characters and letters until one gets access

CIA Triad: Confidentiality, integrity, and availability. Three key principles of a guiding model for designing information security policies

Confidentiality: Keeping things hidden

Cross-site scripting (XSS): A type of injection attack where the attacker can insert malicious code and target the user of the service

Denial-of-Service (DoS) attack: An attack that tries to prevent access to a service for legitimate users by overwhelming the network or server

Dictionary attack: A type of password attack that tries out words that are commonly used in passwords, like password, monkey, football

Distributed Denial-of-Service (DDoS) attack: A DoS attack using multiple systems

DNS Cache Poisoning Attack: It works by tricking a DNS server into accepting a fake DNS record that will point you to a compromised DNS server

Evil twin: The premise of an evil twin attack is for you to connect to a network that is identical to yours but that is controlled by an attacker. Once connected to it, they will be able to monitor your traffic

Exploit: Software that is used to take advantage of a security bug or vulnerability

Hacker: Someone who attempts to break into or exploit a system

Half-open attacks: A way to refer to SYN floods

Injection attacks: A common security exploit that can occur in software development and runs rampant on the web, where an attacker injects malicious code

Integrity: Means keeping our data accurate and untampered with

Keylogger: A common type of spyware that's used to record every keystroke you make

Logic bomb: A type of Malware that's intentionally installed

Malware: A type of malicious software that can be used to obtain your sensitive information or delete or modify files

Meddler in the middle (formerly known as Man in the Middle): An attack that places the attacker in the middle of two hosts that think they're communicating directly with each other

Password attacks: Utilize software like password crackers that try and guess your password

Phishing attack: It usually occurs when a malicious email is sent to a victim disguised as something legitimate

Ping flood: It sends tons of ping packets to a system. If a computer can't keep up with this, then it's prone to being overwhelmed and taken down

Ransomware: A type of attack that holds your data or system hostage until you pay some sort of ransom

Risk: The possibility of suffering a loss in the event of an attack on the system

Rogue Access Point (AP) Attack: An access point that is installed on the network without the network administrator's knowledge

Rootkit: A collection of software or tools that an admin would use

Screen lock: A security feature that helps prevent unwanted access by creating an action you have to do to gain entry

Session hijacking (cookie hijacking): A common meddler in the middle attack

Social engineering: An attack method that relies heavily on interactions with humans instead of computers

Spear phishing: Phishing that targets individual or group - the fake emails may contain some personal information like your name, or the names of friends or family

Spoofing: When a source is masquerading around as something else

Spyware: The type of malware that's meant to spy on you

SQL Injection Attack: An attack that targets the entire website if the website is using a SQL database

SYN flood: The server is bombarded with SYN packets

Tailgating: Gaining access into a restricted area or building by following a real employee in

Threat: The possibility of danger that could exploit a vulnerability

Trojan: Malware that disguises itself as one thing but does something else

Viruses: The best known type of malware

Vulnerability: A flaw in the system that could be exploited to compromise the system

Worms: They are similar to viruses except that instead of having to attach themselves onto something to spread, worms can live on their own and spread through channels like the network

0-Day Vulnerability (Zero Day): A vulnerability that is not known to the software developer or vendor, but is known to an attacker

Mark as completed