Advanced Skill Certificate in Cyber Psychology and Security Assessments

Understanding Cybersecurity Threats and Vulnerabilities

Advance Persistent Threat (APT): A type of cyber threat in which an unauthorized user gains access to a network and remains undetected for a period of time while stealing sensitive data or disrupting operations. APTs are often carried out by well-resourced and trained attackers, such as nation-state actors.

Related terms: Cyber attack, cybercrime, advanced threat, persistent threat

Concept: An APT is a sophisticated and targeted cyber attack that is carried out over an extended period of time. The attacker typically gains access to the network through a spear-phishing email or other social engineering technique, and then moves laterally within the network to establish a foothold and gain access to sensitive data or systems. APTs are often difficult to detect and can cause significant damage, making them a major concern for organizations.

Example: A nation-state actor may carry out an APT against a corporation in order to steal intellectual property or trade secrets. The attacker may gain access to the corporation's network through a spear-phishing email, and then spend several months moving laterally within the network and escalating privileges in order to gain access to the desired data.

Malware: Software that is designed to disrupt, damage, or gain unauthorized access to a computer system. Malware can take many forms, including viruses, worms, Trojan horses, and ransomware.

Related terms: Virus, worm, Trojan horse, ransomware, spyware, adware, scareware

Concept: Malware is a general term that refers to any type of software that is designed to cause harm to a computer system. Malware can be spread through email attachments, infected websites, or removable media, and can cause a wide range of problems, from annoying pop-ups to complete system crashes. Some types of malware, such as ransomware, are designed to extort money from victims by encrypting their files and demanding a ransom payment in exchange for the decryption key.

Example: A hacker may create a Trojan horse program that appears to be a legitimate software installer, but actually installs malware on the victim's computer when run. The hacker can then use the malware to gain remote access to the victim's computer and steal sensitive data or use the computer to carry out further attacks.

Phishing: The practice of sending fraudulent emails or messages that appear to be from a legitimate source

in order to trick the recipient into providing sensitive information or clicking on a malicious link.

Related terms: Spear-phishing, whaling, smishing, vishing

Concept: Phishing is a social engineering attack that uses email or messaging platforms to trick victims into providing sensitive information, such as usernames and passwords, or clicking on malicious links. Phishing attacks often use urgency or fear to manipulate the victim into taking the desired action, such as claiming that their account will be closed if they do not provide the requested information.

Example: A hacker may send a phishing email that appears to be from a victim's bank, claiming that there has been suspicious activity on their account and asking them to verify their identity by clicking on a link and providing their username and password. The link actually leads to a fake login page controlled by the hacker, who can then use the stolen credentials to gain access to the victim's account.

Ransomware: A type of malware that encrypts the victim's files and demands a ransom payment in exchange for the decryption key.

Related terms: Malware, encryption, decryption, ransom demand

Concept: Ransomware is a type of malware that is designed to extort money from victims by encrypting their files and demanding a ransom payment in exchange for the decryption key. Ransomware attacks can be devastating for organizations, as they can result in the loss of critical data and disrupt operations for an extended period of time.

Example: A hacker may infect a corporation's network with ransomware by sending a spear-phishing email to an employee. Once the ransomware is installed, it begins encrypting the corporation's files, making them inaccessible. The hacker then demands a ransom payment, typically in the form of cryptocurrency, in exchange for the decryption key.

Social Engineering: The use of manipulation, deception, or coercion to trick someone into divulging sensitive information or taking a desired action.

Related terms: Phishing, spear-phishing, whaling, smishing, vishing, pretexting

Concept: Social engineering is a type of attack that relies on manipulating human behavior rather than exploiting technical vulnerabilities. Social engineering attacks can take many forms, including phishing emails, phone calls, or in-person interactions. The goal of a social engineering attack is to trick the victim into providing sensitive information, such as usernames and passwords, or taking a desired action, such as clicking on a malicious link.

Example: A hacker may use social engineering techniques to trick an employee of a corporation into providing their login credentials. The hacker might call the employee pretending to be a representative of

the corporation's IT department and claim that there has been a security breach. The hacker can then use the stolen credentials to gain access to the corporation's network and steal sensitive data.

Spear-Phishing: A type of phishing attack that is targeted at a specific individual or group of individuals.

Related terms: Phishing, whaling, smishing, vishing, social engineering

Concept: Spear-phishing is a more targeted form of phishing attack that is tailored to the specific victim or group of victims. Spear-phishing attacks often use personalized information, such as the victim's name, job title, or interests, to make the attack more convincing. Spear-phishing attacks can be particularly dangerous, as they are more likely to succeed in tricking the victim into providing sensitive information or clicking on a malicious link.

Example: A hacker may carry out a spear-phishing attack against a corporation's CEO by sending an email that appears to be from the CEO's assistant. The email might contain a link to a fake login page that is designed to steal the CEO's login credentials.

Vulnerability: A weakness in a computer system or network that can be exploited by an attacker to gain unauthorized access or disrupt operations.

Related terms: Exploit, attack surface, zero-day vulnerability, patch management

Concept: A vulnerability is a weakness in a computer system or network that can be exploited by an attacker to gain unauthorized access or disrupt operations. Vulnerabilities can be caused by a variety of factors, including outdated software, misconfigured systems, or human error. Identifying and addressing vulnerabilities is a critical component of cybersecurity.

Example: A vulnerability in a corporation's web server might allow an attacker to gain unauthorized access to the server and steal sensitive data. The corporation can mitigate this vulnerability by applying security patches and configuring the server securely.

Whaling: A type of spear-phishing attack that is targeted at high-level executives or other high-value targets.

Related terms: Phishing, spear-phishing, whaling, smishing, vishing, social engineering

Concept: Whaling is a more targeted form of spear-phishing attack that is tailored to high-level executives or other high-value targets. Whaling attacks often use personalized information, such as the victim's name, job title, or interests, to make the attack more convincing. Whaling attacks can be particularly dangerous, as they are more likely to succeed in tricking the victim into providing sensitive information or clicking on a malicious link.

Example: A hacker may carry out a whaling attack against a corporation's CFO by sending an email that appears to be from the CEO. The email might contain a link to a fake invoice that is designed to steal the CFO's login credentials.

Zero-Day Vulnerability: A vulnerability in a computer system or network that is unknown to the vendor or security community.

Related terms: Vulnerability, exploit, attack surface, patch management

Concept: A zero-day vulnerability is a vulnerability in a computer system or network that is unknown to the vendor or security community. Zero-day vulnerabilities are particularly dangerous, as they can be exploited by attackers before they are discovered and patched. Identifying and addressing zero-day vulnerabilities is a critical component of cybersecurity.

Example: A hacker might discover a zero-day vulnerability in a popular software application and use it to carry out a series of attacks against unsuspecting victims. The vendor would not be aware of the vulnerability until it was reported by a security researcher or discovered through an attack.