FORTINET NSE Training Institute

FORTINET NSE 1 ASSOCIATE

Key Cybersecurity Terms

(20 August 2020)

Advanced threat protection (ATP) – relies on multiple types of security technologies, products, and research, each performing a different role, but still working seamlessly together to combat attacks from the core of the network to the end user device. The three-part framework is conceptually simple—prevent, detect, mitigate; however, it covers a broad set of both advanced and traditional tools for network, application and endpoint security, threat detection, and mitigation.

Advanced persistent threat (APT) – a network attack in which an unauthorized person gains access to a network and stays there undetected for a long period of time. Typically, their intention is to steal data rather than to cause damage to the network or organization. These attacks target organizations in sectors with high-value information, such as national defense, manufacturing, and the financial industry.

Anti-virus/Anti-malware (AV/AM) – provides protection against virus, spyware, and other types of malware attacks in web, email, and file transfer traffic. Responsible for detecting, removing, and reporting on malicious code. By intercepting and inspecting application-based traffic and content, antivirus protection ensures that malicious threats hidden within legitimate application content are identified and removed from data streams before they can cause damage. Using AV/AM protection at client servers/devices adds an additional layer of security.

Attack signature – a characteristic or distinctive pattern of attack that can be searched for using an automated set of rules that have been matched to previously identified attacks.

Attack surface – the sum of the different points where an unauthorized user can try to enter and attack a computer environment. While in the context of cybersecurity, we are referencing the software and hardware of a computer environment, an attack surface is also applicable elsewhere. For example, doors and windows represent the attack surface of a house because they are the points from which an intruder can enter.

Authentication – the process of determining whether someone or something is actually who or what they claim to be. In computer networks, the purpose of authentication is to make sure that only known and authorized persons and devices have access to the network. (Contrast this with *authorization*)

Authentication Token – also known as hardware token, security token, USB token, cryptographic token, software token, virtual token, or key fob, and are used to prove a person's identity electronically. The token is used in addition to or in place of a password for stronger authentication, to prove that the person is who they claim to be.

Authorization – a security mechanism used to determine user/client privileges or access levels related to system resources, including computer programs, files, services, data, and application features. Authorization is normally preceded by authentication for user identity verification.

Behavior monitoring – observing activities of users, information systems, and processes and measuring the activities against organizational policies and rule, baselines of normal activity, thresholds, and trends.

Bot/Botnet – a type of software application or script that performs tasks on command, allowing an attacker to take control remotely of an affected computer. A collection of these infected computers is known as a "botnet" and is controlled by the hacker or "bot-herder".

Breach – the moment a hacker successfully exploits a vulnerability in a computer or device, and gains access to its files and network.

Cipher – a cryptographic algorithm used to encrypt data or information.

Clickbait – an online advertisement, which may be false, and whose main purpose is to attract users to another website. Sometimes this website or the advertisement itself contains malware.

Credential (or Account) Harvesting – a targeted attack that steals a large number of usernames, passwords, and email addresses.

Credential Stuffing – a spearphishing attack using stolen credentials, often monetized by selling credentials on dark web forums, and beneficial in establishing bona fides for targeting other high-value accounts, especially executives and finance department employees, to harvest their credentials and gain unauthorized access to devices and networks.

Cross-site scripting (XSS) – a type of security vulnerability typically found in web applications. XSS attacks enable attackers to inject client-side scripts into web pages viewed by other users. A cross-site scripting vulnerability may be used by attackers to bypass access controls such as the same-origin policy. XSS effects vary in range from petty nuisance to significant security risk, depending on the sensitivity of the data handled by the vulnerable site and the nature of any security mitigation implemented by the site's owner network.

Distributed Denial of Service (DDoS) – a form of cyber-attack. This attack aims to make a service, such as a website, unusable by inundating it with malicious traffic or data from multiple sources (often botnets).

Deep Packet Inspection (DPI) – is the act of examining the payload or data portion of a network packet as it passes through a firewall or other security device. DPI identifies and classifies network traffic based on signatures in the payload. It examines packets for protocol errors, viruses, spam, intrusions, or policy violations.

Deepfake – an audio or video clip that has been edited and manipulated to seem real or believable. They can easily convince people into believing a certain story or theory that may have political or financial consequences.

Drive-by – refers to the unintentional download of a virus or malicious software (malware) onto your computer or mobile device. A drive-by download will usually take advantage of (or “exploit”) a browser, app, or operating system that is out of date and has a security flaw. This initial code that is downloaded is often very small (so you probably wouldn’t notice it), since its job is often simply to contact another computer where it can pull down the rest of the code on to your smartphone, tablet, or computer. Often, a web page will contain several different types of malicious code, in hopes that one of them will match a weakness on your computer.

Encryption – the process of converting readable information into unintelligible code in order to protect the privacy of the data.

Exploit – a malicious application or script that can be used to take advantage of a computer’s vulnerability

Firewall – a hardware appliance or software application that is intended to prevent unauthorized access or illicit malware from writing to a computer, device, or network.

Identity Theft – steals Personally Identifiable Information (PII), typically for economic gain.

Impersonator – a person who pretends to be someone else for entertainment or fraud.

Intrusion Detection System (IDS) – software that automatically alerts administrators when someone or something is trying to compromise an information system.

Intrusion Prevention System (IPS) – a system that monitors a network for malicious activities, logs the information, attempts to block the activity, and reports it.

Juice Jacking – a security exploit in which an infected USB charging station is used to compromise connected devices.

Keylogger – a technology that tracks and records consecutive key strokes on a keyboard.

Malicious code – program code intended to perform an unauthorized function or process that will have an adverse impact on the confidentiality, integrity, or availability of an information system.

Malware – malicious software that brings harm to a computer system. Types of malware include worms, viruses, Trojans, spyware, adware, and ransomware.

Next Generation Firewall (NGFW) – a class of firewall, as software or hardware, that is capable of detecting and blocking complicated attacks by enforcing security measures at the protocol, port, and application level.

Passive attack – an actual assault perpetrated by an intentional threat source that attempts to learn or make use of information from a system, but does not attempt to alter the system, its resources, its data, or its operations.

Phishing – weaponized email that masquerades as reputable, lures targeted groups into taking an action, and only requires one victim to be successful.

Pretexting – fabricated scenario that convinces a targeted victim to disclose privileged information.

Ransomware – malware payload that prevents access to computer systems and demands a sum of money to be paid to retrieve the data. Email is the predominate attack vector because it relies on a single click to circumvent controls.

Rogue AP – a wireless access point that has been installed on a secure network without the authorization of a local network administrator, whether added by a well-meaning employee or by a malicious attacker.

Rogue Security Software – a victim is convinced to purchase fake malware removal but instead installs malware on their device.

Rootkit – another kind of malware that allows cybercriminals to remotely control your computer. Rootkits are especially damaging because they are hard to detect, making it likely that this type of malware could live on your computer for a long time.

Secure Socket Layer (SSL)-Encrypted Traffic Inspection – protects endpoint clients as well as Web and application servers from potentially hidden threats. SSL inspection intercepts and inspects encrypted traffic for threats before routing it to its destination. It can be applied to client-oriented traffic, such as users connected through a cloud-based site, or to Web and application server traffic. Using SSL inspection allows policy enforcement on encrypted Web content to prevent potential intrusion from malicious traffic hidden in SSL content. While SSL inspection adds security by screening for threats attempting to bypass protections by riding on encrypted traffic, the resultant tradeoff is a decrease in throughput speed.

Secure web gateway – an on-premise or cloud-delivered network security service. Sitting between users and the Internet, secure web gateways provide advanced network protection by inspecting web requests against company policy to ensure malicious applications and websites are blocked and inaccessible. A secure web gateway includes essential security technologies such as URL filtering, application control, data loss prevention, antivirus, and https inspection to provide organizations with strong web security.

Security Information and Event Management (SIEM) – also known as Security Incident and Event Management, it provides a comprehensive and centralized view of the security scenario of an IT infrastructure, to identify, monitor, record and analyze security events or incidents in real-time. Most SIEM systems deploy multiple collection agents to gather security-related events from end-user devices, servers, network equipment and specialized security equipment like firewalls, AV/AM or IPS. The collectors forward events to a centralized management console, which performs inspections, flags anomalies, and notifies the IRT (Incident Response Team) of any security violating events.

Sandbox – a security mechanism for separating running programs to an area segmented off from the device/network operating system and applications. It is used to execute untested code, or untrusted programs from unverified third parties, suppliers, untrusted users, and untrusted websites. The sandbox limits the actions and resources available to the constrained item, allowing the item to be evaluated, while preventing any harm or damage to be caused to the host system or related data or storage devices.

Smishing – also known as SMS phishing; occurs when a cell phone receives a SMS (Instant Message or IM) from a fake person or entity. The unsuspecting cell phone user will respond to a fake SMS and visit a URL, inadvertently downloading malware and installing a Trojan without the user's knowledge. Phishing is all about extracting useful information, so in the case of SMS phishing, the Trojan harvests the data areas of the cellphone and transmits them to the person who created the Trojan at the earliest opportunity.

Social Media Deception – an attacker manipulates content and creates fake online profiles.

Spam – the abuse of electronic messaging systems, such as e-mail, text messaging, social networks or VoIP, to indiscriminately send unsolicited bulk messages. Most SPAM is advertising, but some may include malicious code, malicious hyperlinks or malicious attachments.

Spearphishing, Whaling, CEO Fraud, and Business Email Compromise (BEC) – a form of social engineering attack that is targeted to victims who have an existing digital relationship with an online entity such as a bank or retail website. A spear phishing message is often an e-mail although there are also text message and VoIP spear phishing attacks as well, which looks exactly like a legitimate communication from a trusted entity. The attack tricks the victim into clicking on a hyperlink to visit a company website only to be re-directed to a false version of the website operated by attackers. The false website will often look and operate similarly to the legitimate site and focus on having the victim provide their logon credentials and potentially other personal identity information such as answers to their security questions, an account number, their social security number, mailing address, email address and/or phone number. The goal of a spear phishing attack is to steal identity information for the purpose of account takeover or identity theft.

Spoofing – a fraudulent or malicious practice in which communication is sent from an unknown source disguised as a source known to the receiver, with the intent to gain an advantage or the trust of the receiver. It is most prevalent in communication mechanisms that lack a high level of security, such as IP address, MAC address, and email address.

Spyware – malware used to infiltrate a user's system without their knowledge, to monitor activity, collect keystrokes and passwords, and harvest data (account information, logins, financial data). Spyware exploits user and application vulnerabilities and is often attached to free online software downloads or to links that are clicked by users. It is also often used to disable firewall or anti-malware software while consuming CPU activity to increase an endpoint's vulnerability to attack.

Tailgating – unauthorized person who bypasses physical access controls, often by distracting and then closely following an authorized person into a controlled room or building.

Trojan Horse – a form of malware where a malicious payload is imbedded inside of a benign host file which is used to deceive users into downloading and installing malware. When a user accesses the host file, the malicious payload is automatically deposited onto their computer system, and allows the cyber-criminal to conduct a variety of attacks such as stealing or destroying data, installing more malware, modifying files, monitoring user activity, or conducting denial of service (DoS) on targeted web addresses.

Unified Threat Management (UTM) – an approach to information security that combines several key elements of network security hardware and software into a comprehensive security solution, including a single management and reporting point for the security administrator. This contrasts with the traditional method of having point solutions for each security function.

USB Baiting – compromised USB drives can be used to inject malicious code, redirect a user to phishing websites, or give a hacker access to a user's computer.

Virtual Private Network (VPN) – a tool that extends a private network across a public network and enables users to send and receive data across shared or public networks as if their computing devices were directly connected to the private network. Encryption is a common, although not an inherent, part of a VPN connection.

Virus – a type of malware aimed to corrupt, erase or modify information on a computer before spreading to others.

Virus Signature – a virus signature is the fingerprint of a virus. It is a set of unique data, or bits of code, that allow it to be identified. One signature may contain several virus signatures, which are algorithms or hashes that uniquely identify a specific virus. Antivirus software uses a virus signature to find a virus in a computer file system, allowing to detect, quarantine, and remove the virus.

Vishing – a form of phishing attack which takes place over VoIP. In this attack, the attacker uses VoIP systems to be able to call any phone number with no toll-charge expense. The attacker often falsifies their caller-ID in order to trick the victim into believing they are receiving a phone call from a legitimate or trustworthy source such as a bank, retail outlet, law enforcement or charity. The victims do not need to be using VoIP themselves in order to be attacked over their phone system by a vishing attack.

Waterhole – an attacker observes websites that a targeted group often visit, then finds a vulnerability to breach the webpage, and herds victims to that infected website.

Web Filtering – gives you the option to explicitly allow web sites, or to pass web traffic uninspected both to and from known-good web sites in order to accelerate traffic flows. The most advanced web content filtering technology enables a wide variety of actions to inspect, rate, and control perimeter web traffic at a granular level. Using web content filtering technology, these appliances can classify and filter web traffic using multiple pre-defined and custom categories.

Worm – a self-replicating, self-propagating, self-contained form of malware that uses networking mechanisms to spread itself to other systems. Generally, the damage caused by a worm is indirect and due to the worm's replication and distribution activities consuming all system resources. A worm can be used to deposit other forms of malware on each system it encounters.