Cyber Attacks – Getting to the lingo.

Advanced Persistent Threats (APT): The term Advanced Persistent Threat was coined in 2005 by an USAF security analyst [9]. According to the US National Institute of Standards and Technology (NIST), an APT is an adversary that possesses sophisticated levels of expertise and significant resources to create opportunities to achieve its objectives using multiple attack vectors. It pursues objectives over an extended period of time; adapts to efforts of the defenders and maintains an adequate level of interaction aligned with its objectives. The attack cycle encircles target selection, target research, target penetration, command and control, target discovery, data exfiltration, intelligence dissemination and information exploitation.
Arbitrary/remote code execution: Attackers use techniques to install malware remotely in order to take partial or complete control of a system.
ARP poisoning: Address Resolution Protocol poisoning misleads interconnection devices about the real MAC of a machine. ARP contains only two types of messages: ARP request and ARP reply. Attackers create ARP reply packets using spoofed MAC addresses to poison ARP cache on any network system. VLAN segregation prevents this type of attack.
Bluejacking: It is the process of sending text messages using a private Bluetooth device without the owner's consent. In addition to text messaging, some Bluetooth devices can include sound. The best security strategy is to operate the device in a non-discovery mode.
Bluesnarfing: Unauthorized access to a Bluetooth device or data theft from any Bluetooth connection. This attack will take place as long the device is on and set to discovery mode. Linux users can launch this type of attack using hcitool and ObexFTP tools.
Buffer overflow: This usually happens whenever an application receives more input than it can handle. The result is a system memory error that exposes a vulnerability that later can be exploited to write malicious code. Normally the sequence attack is primarily causing the buffer overflow, then is sending a long NOOP (No Operation) command, inserting the malicious code and finally by triggering the code execution.
Client-side attacks: This type of attack can be launched using a client application aiming to access specific servers or databases. This can be avoided if proper input validation and stored procedures are in place. Client-side attacks are based on transitive trust access that allows forest trust relationships in all Active Directory domains.
Cookies and attachments: Cookies can store web browsing history and sensitive data including usernames, passwords and session IDs that are instrumental for additional attacks like session hijacking. Malicious attachments can trigger malware attacks like viruses, Trojans and worms.
Cross-site Request Forgery (XSRF): Attackers fool users by creating malicious HTML links and redirecting the victims to perform specific actions. A security measure is to create expiration cookies and to prevent automatic log on. 169 R. Sabillon et. al / International Journal of Computer Networks and Communications Security, 4 (6), June 2016
Cross-site Scripting (XSS): This attack redirects end users to malicious webpages, by encoding , Error! Filename not specified., tags and embedding HTML or JavaScript code into websites or emails. Once the link is open then the code will run on the user's computer. Local cookies can be read after the script is executed. Web developers must block HTML and JavaScript tags by hardening input validation on webpages.
Denial-of-Service (DoS): Attack that inhibits legitimate users from accessing computer services. Normally DoS target connectivity or network bandwidth by overflowing server traffic, resources, nodes or services. Some techniques to launch the DoS attacks include SYN flood, bandwidth, service request, ICMP, P2P, permanent DoS, smurf, app level and buffer overflow.
Directory/command injection:

These attacks use commands to manipulate an application via the Operating System or the deletion of directories, subdirectories or files. A good security measure is to implement input validation.
Distributed Denial-of-Service (DDoS): DDoS are launched using several zombie computers (botnet- derived from roBOT NETwork) attacking a specific target. During a DDoS the target computer will sustain extreme network traffic, memory and processors usage. To detect outbound traffic, use the command line tool netstat –a
DNS poisoning: Domain Name System poisoning is an attack that modifies or corrupts cached DNS results. The major risks are the propagation of poisoned DNS information to the Internet Service Providers and be cached in their servers.
Domain Name kiting: This practice allows attackers to register domain names and delete them after the five-day free trial. During the free period, domain tasting will generate traffic and likewise generate revenue without paying for the domain registration.
Evil twin: Rogue access point attack that configures a WAP (Wireless Access Point) with the same SSID (Service Set Identifier) of a valid WAP. Attackers set these devices in public places with free Wi-Fi. Sensitive information is stolen from the users that connect to the evil twin.
Flash cookies: Because Adobe Flash cookies can be set to never expire; they represent a high risk to steal user's browsing history. Flash cookies are normally 5 MB in comparison to regular cookies that only store 1,024 bytes of information. Flash cookies are able to recreate deleted cookies.
Fuzz Testing: It is used to detect system vulnerabilities that can be later exploited. This attack transmits strings of data from scripting to specific applications.
Hash injection: It is an attack that injects an altered hash to authenticate into a local session in order to access network resources. Attackers will log onto the domain controller, accessing the Active Directory and manipulating domain accounts.
Header manipulation: Flags are modified within data packets granting legitimate rights to attackers. Dual authentication prevents manipulating user's data.
ICMP flooding: DoS attack that sends Internet Control Message Protocol (ICMP) packets with spoof source addresses so TCP/IP requests stop. Once the ICMP threshold is reached the router no longer accepts the ICMP echo requests.
Information disclosure: These attacks allow perpetrators to obtain valuable information about a system. Some examples include revealing passwords, shoulder-surfing, loss of thumb drives, laptop theft, message insecurity over HTTP, sharing of confidential policies, data leakage and social engineering information disclosure.
Integer overflow: This attack is the result when an arithmetic operation exceeds the maximum value of an integer used for storage. This exploit can be used for buffer overflow, infinitive loops and data corruption.
(Initialization Vector) attack: This exploit takes place on Wi-Fi networks using the WEP (Wired Equivalent Privacy) security protocol. WEP has known vulnerabilities. The attackers use packet injection for cracking the small IV for keys and obtaining the encryption key.
Jamming interference: This attack can be part of a major Wireless Denial of Service (WDoS) attack. Attackers use malicious nodes to block access to the medium and likewise interfere with wireless or wired reception. Sophistication increases from continual transmission interference to exploiting protocol vulnerabilities.

Keylogger attack:
This can be a hardware device or a small program that records user's keystrokes or screen content. If it is a physical device, the attacker must remove it in order to access the information. On the other hand, if the hidden program was installed on the victim's 170 R. Sabillon et. al / International Journal of Computer Networks and Communications Security, 4 (6), June 2016 computer – its DLL (Dynamic Link Library) file will record all keystrokes.

Lightweight Directory Application Protocol (LDAP) injection:
This attack targets Active Directory accounts so can be modified using LDAP commands.

Malicious add-ons:
We have to be very careful about any additional add-ons that the browsers will install on our computers. There have been cases in the past that browser add-ons installed malware on the client computers. Some measures include running additional scans, do not download from compromised sites and keep system with the latest security patches.

Malicious insider threat:
An insider attack using valid system access credentials can compromise data confidentiality. Motives include revenge, financial gain and industrial espionage. Insider threats are very difficult to detect but a mix of controls can be implemented like least privilege, proper segregation of duties, auditing, enforcement of legal and security policies, restricted access and critical data backup management.

Malware attacks:
Malicious software that is installed through different devious ways. There are several categories of malware, the most common are viruses, worms and Trojan horses.

Virus:
Malicious code that replicates by itself and needs execution in order to cause damage.

Worm: Self-replicating malicious code that spreads across the network without intervention or execution.

Trojan horse:
Trojans hide within a valid application that will get activated upon certain actions. These programs can even disable firewalls, create backdoors, activate botnets, generate fake traffic and delete system files.

Logic bomb:
Malicious scripts that will activate for a particular event. Normally, they are programmed to destroy the operating system, deletion and formatting of all network drives.

Rootkits:
Programs that hide other malware by modifying the operating system. Some rootkits are at the boot loader, library, hardware, application, firmware, kernel and hypervisor levels.

Spyware: This program gathers sensitive information about the user.

Rogueware:
These programs are also named scareware, the malicious programs masquerade as a security application and send messages of malware infection. After a system scan or trial expiration, users get asked to pay for a full version.

Ransomware:
Extortive malware that locks user's data in order to get payment for unlocking the data.

Man-in-the middle (MITM): This type of attack allows active interception of network traffic and sending malicious code to the client's machine. Kerberos prevent MITM attacks by enforcing authentication.

Misconfiguration attacks:
These attacks take advantage of wrong, default or compromised configurations to access systems, networks, computers, servers, mobile devices or interconnection devices.

Near field communication (NFC): There are a few attacks under NFC including eavesdropping, data corruption and smartphone viruses. NFC devices can communicate if the separation is

four centimeters or less. The biggest risk is card skimming due to the fact when mobile card readers are used to complete the online payments. NFC channels are also vulnerable to MITM attacks.

Packet sniffing: Attackers use protocol analyzer or sniffer programs like Wireshark, TCPDump and Sniff-O-Matic to capture and track network packets. Unencrypted data is the most vulnerable when using sniffers – captured packets can easily be read and analyzed data can also be used to plan further cyberattacks.

Password attacks:
These attacks use different techniques to crack server, network device, systems or user passwords. Weak passwords can be avoided if they use a long combination of capital/ small case letters, numbers and special characters. Cracking techniques include brute force, rule based, dictionary, hybrid and syllable attacks. Some password cracking tools are L0phtCrack, John the Ripper, Cain and Abel, Passscape and Aircrack.

Pharming:
This type of attack aims DNS servers; it is particularly a DNS poisoning attack that redirects traffic to a fraudulent website. Cyber crooks can take advantage of this by stealing confidential information of users.

Privilege escalation:
When hackers penetrate systems, they normally have limited access accounts and want to obtain full privilege accounts like super admin accounts. Elevated rights and permissions of attackers allow them to gain additional controls and remain unnoticed in the target system.

Rainbow attack:
Attackers check the stolen password validity during this type of attack. By using cryptanalysis techniques, the time-memory trade off calculates memory information, inserting the password hash table, comparing and matching passwords until they are cracked.

Replay attack:
Attackers replay data between communication sessions. Using the data, they can impersonate a user to obtain information. Kerberos block this type of attack using timestamped tickets.

Rogue access points:
Counterfeit WAPs are connected to networks to capture traffic. This rogue device will easily grant access to unauthorized users using wireless and wired networks of the victim.

Session hijacking:
This process seizes an active network or application session. By intercepting and taking control of an user‘s session, the attacker inserts malicious code to target server afterwards. Packet interception happens at the network level and HTTP session takeover at the application level in OSI model. Some prevention measures against session hijacking include the use of Secure Shell (SSH), HTTPS, log-out functionality implementation and data encryption.

Shrink wrap code attacks:
These attacks are aimed at applications immediately after its initial installation. The most common vulnerability is to exploit default code from libraries.

Smurf attack:
A DoS attack that spoofs the source host to flood the target computer with ping replies.

Social Engineering:
Hackers use social tactics to persuade people to reveal sensitive information that can be later used for malicious actions. Social engineering types include using human interaction, computers or mobile devices. Attackers normally pose as legitimate users, VIP executives or technical support analyst to commit their attacks. Best anti-social engineering strategies are education, security awareness training and enforcement of IT security policies.

Spear phishing:
This attack targets a specific user or a group of users. Normally uses an email that seems legitimate to ask for some wire transfer already approved by a top executive within a company.

Spim:
Spam instant messaging targets instant messaging apps such Yahoo Messenger, WhatsApp and Line. The attackers need mobile number confirmation if the users click the link. Best way to

deal with Spim is to ignore the messages and delete them.

Spoofing:
Cyberattacks can use spoofing in many ways, from changing IP addresses to changing Media Access Control (MAC) addresses to email address by hiding the attacker identity.

SQL injection:
These attacks are the highest web vulnerability impacts on the Internet. A flaw in the coding of a web application is exploited to allow additional data entry to generate unique SQL statements. Many relational databases are vulnerable to this attack including DB2, MySQL and SQL SRV. These attacks can avoid authentication, trigger code execution and affect data integrity.

SYN flooding:
Common DoS attacks use SYN to flood servers. It is based on the Transmission Control Protocol (TCP) handshake process that overflows the normal three-way handshake using SYN and ACK packets between hosts. Attackers never send the ACK part and otherwise they keep sending multiple SYN packets to get several halfopened connections causing a system crash.

Transitive access:
This access involves a trusted relationship within a network that can be exploited to attack core systems. Client-side attacks use transitive relationships whenever an attacker cannot aim a direct cyberattack.

Typo squatting:
This is a form of cybersquatting that reroutes users to malicious websites. Active domain names with typographical errors are created, registered as valid URLs and then uploaded as alternate websites to infect users with malware.

URL hijacking:
This attack is also known as Man-in-the-Browser attack. It triggers a Trojan to hijack the communication between the browser and the libraries. The extension files from the Trojan convert the Document Object Model (DOM) interface and modify the user values

Vishing:
This attack uses Voice over Internet Protocol (VoIP) or a phone system calls to trick users to give personal information in a similar way to phishing attacks. Attackers can spoof caller IDs to masquerade a phone call within a company. Personal information is at risk if the user provides the required information to validate some kind of financial transaction. 172 R. Sabillon et. al / International Journal of Computer Networks and Communications Security, 4 (6), June 2016

War chalking:
This technique is used to place special symbols on sidewalks or walls indicating an open Wi-Fi network.

War driving:
Attackers drive around to discover wireless networks for future exploits. Cantennas (Open-ended metal can antennae) are used to detect Wi-Fi networks.

Watering hole:
This attack identifies an organization website, exploits web vulnerabilities and installs malware that attacks silently the users.

WEP/WPA attacks:
These Wired Equivalent Privacy/ Wi-Fi Protected Access attacks use cracking tools to break 802.11 WEP secret keys. 40-bit to 512-bit keys can be cracked from captured data packets.

Whaling:
Whaling is a spear phishing attack that aims upper management executives. This attack targets a top executive by name using some kind of legal subpoena or customer complaint.

Wire sniffing:
This is a form of an active or passive wiretapping attack that monitors data traffic or alters data packets as required. Some vulnerable protocols to sniffing are HTTP, IMAP, Telnet, POP, FTP, SMTP and NNTP. Some measures to defend sniffing include physical restrictions, encryption, use of static IP addresses and IPv6 configuration.

WPS attacks:

Wi-Fi Protected Setup use buttons to connect to wireless networks and a secure WPA link. This Pin attack sets up a brute force method to crack into a WPA wireless network. Some countermeasures include disabling WPS or updating the access point firmware.
Xmas attack: The Christmas tree attack is a port scan type used as a reconnaissance attack and the gathered information is crucial for further cyberattacks. The particular features are the inclusion of bit sets and flags in the TCP packet header that will trigger responses about open ports.
XML injection: eXtensible Markup Language injection attacks are similar to SQL injection attacks. Major vulnerabilities include code insertion to input or export database data. In addition, XPath the XML query language can be entered using query statements for retrieval or modification of data.
Zero day: This attack exploits undisclosed software vulnerability that the vendor has not yet created a security patch to fix it. Best action plan against zero day vulnerabilities is to limit the amount of active protocols and services.