Endpoints: end-user devices such as laptops, smart phones, and printers.

**Buffer overflow attacks**

* **Buffer memory** is a temporary storage area in the main memory (RAM) that stores data transferring between two or more devices or between an application and a device.
* **Buffer overflow attacks**: best known form of software security vulnerability
* **Buffer overflow**: when a program attempts to put more data in a buffer than it can hold or when a program attempts to put data in a memory area past a buffer
* Buffer: is a sequential section of memory allocated to contain anything from a character string to an array of integers
* An attacker can provide input that is larger than expected, and the service will accept the input and write it to memory, filling up the associated buffer and also overwriting adjacent memory.

**Buffer overflows results:**

* Corruption of data
* Crash application
* Injection of malicious code in the buffer overflow, leading to a compromised system.

**Reconnaissance attacks:**

* A reconnaissance attack is an attempt to gather information about an intended victim before attempting a more intrusive attack
* Attackers can use **standard networking tools such as dig, nslookup, and whois** to gather public information about a target network from Domain Name System (DNS) registries.
* They can also use DNS queries to reveal such information as who owns a particular domain and which addresses have been assigned to that domain.
* Port scanning tools, such as the widely used nmap, can cycle through all well-known ports and provide a complete list of all services running on the host.
* Attackers can use the information that is obtained from a port scan to discover the vulnerabilities of a specific endpoint.
* They can also use vulnerability scanners, such as Nessus and OpenVAS, to locate vulnerabilities in potential target hosts.

**Malware**

Malware is malicious software that comes in several forms, including the following:

Viruses

* A virus is a type of malware that propagates by inserting a copy of itself into another program and becoming part of that program.
* It spreads from one computer to another, leaving infections as it travels. Viruses require human help for propagation

**Worms**

* Computer worms are similar to viruses in that they replicate functional copies of themselves and can cause the same type of damage.
* worms are standalone software and do not require a host program or human help to propagate.
* To spread, worms either exploit a vulnerability on the target system or use some kind of social engineering to trick users into executing them

**Trojan**

* Programs that pretend to do one thing but, when loaded, actually performs another, more malicious act.
* A software Trojan horse is based on this same concept. A user might think that a file looks harmless and is safe to run, but after the file is executed, it delivers a malicious payload
* The payload is executed if the attacker can get the victim to open the file or click the attachment

**Gaining Access and control**

* **Password spraying** involves taking a list of possible user accounts and trying very common passwords such as the season+year (Summer2016), or the companyname + year (Cisco2016), or companyname + 123 (Cisco123) to capitalize on any employee using a very weak password
* if attackers can gain access to an endpoint, they can also gain control of the endpoint and use it to launch more wide-spread attacks.
* The endpoint can become part of a botnet, which is a network of compromised systems that is used to perform distributed denial of service (DDoS) attacks.

**Gain access via social engineering**

* Social engineering is manipulating people and capitalizing on expected behaviors.

**Phishing**

phishing email pretends to be from a large, legitimate organization. The malicious website generally resembles that of the real organization. The goal is to get the victim to enter personal information such as account numbers, social security numbers, usernames, or passwords

**Types of phishing*:***

* **Spear phishing:** Emails are sent to smaller, more targeted groups. Spear phishing may even target a single individual.
* **Whaling:** Like spear phishing, whaling uses the concept of targeted emails; however, it increases the profile of the target. The target of a whaling attack is often one or more of the top executives of an organization.
* **Pharming:** Whereas phishing entices the victim to a malicious website, pharming lures victims by compromising name services. This can be done by injecting entries into local host files or by poisoning the DNS in some fashion, such as compromising the Dynamic Host Configuration Protocol (DHCP) servers that specify DNS servers to their clients. When victims attempt to visit a legitimate website, the name service instead provides the IP address of a malicious website.
* **Watering hole:** A watering hole attack leverages a compromised web server to target select groups. The first step of a watering hole attack is to determine the websites that the target group visits regularly. The second step is to compromise one or more of those websites. The attacker compromises the websites by infecting them with malware that can identify members of the target group. Only members of the target group are attacked. Other traffic is undisturbed. This makes it difficult to recognize watering holes by analyzing web traffic. Most traffic from the infected web site is benign.
* **Vishing:** Vishing uses the same concept as phishing, except that it uses voice and the phone system as its medium instead of email. For example, a visher may call a victim claiming that the victim is delinquent in loan payments and attempt to collect personal information such as the victim's social security number or credit card information.
* **Smishing:** Smishing uses the same concept as phishing, except that it uses short message service (SMS) texting as the medium instead of email.

**Gain Access via web-based attacks:**  method that attackers use to perform client-side web-based attacks involves manipulating Uniform Resource Identifier (URI) of the HTTP request. One common attack technique in which the attacker manipulates the URI is to use encoded characters to hide the attack.

**Exploits Kit:** An exploit kit is an automated framework attackers use to discover and exploit vulnerabilities in an endpoint, infect it with malware, and execute malicious code on it. Exploit kits may use a process that is known as drive-by download, commonly hidden in a malicious ad that is loaded on a legitimate webpage, which invisibly redirects a user’s browser to a malicious server hosting the exploit kit framework.

Shadow domain: a second-level domain that is registered by a malicious person using compromised domain registration information from a legitimate site

**Rootkits:**

A rootkit is the most complex attacker tool. Its goal is to completely hide the activities of the attacker on the local system. A rootkit takes control of the operating system by compromising the internal structure of the system.

**Privilege Escalator**

* After the initial access to an endpoint, attackers may be confined to using the privileges of employees with very limited access. The attackers cannot effectively spread throughout the network without escalating their privilege level.
* To protect against a privilege escalation, attack an organization can exercise a strong password policy that includes the requirement of unique passwords for multiple accounts.

**Post-Exploitation Phase**

Attackers will want to determine basic system information for the machine they are on, what user context they are running under, processes that are running, services on the system, and other network basics to learn about the machine and capabilities they have on it.

Some of the initial commands that are often run by an attacker who gains access to a machine: :

* **whoami:** shows the user account and domain information as applicable.
* **ipconfig:** shows the network configuration, gateway, DHCP, and DNS server information.
* **netstat –anop**: shows all active, listening, and closed network connections.
* **quser**: lists the users who are logged on to system.
* **tasklist**: lists all the running processes.
* **schtasks**: shows all the tasks set to run on the system at certain intervals.
* **sc:** lists all the services set to run on the system.
* **net start**: Starts services to run on a system.

attackers often use tools such as **PowerShell and Mimikatz** on compromised machines in order to gain a bigger foothold on the victim’s machine and network, and establish persistent access.

* Haut du formulaire
* Bas du formulaire