**Password attacks**

An attacker can bypass authentication in vulnerable system by using several methods

**Password guessing (devinette de mot de passe):** To perform password guessing, an attacker can either manually enter passwords or use a software tool to automate the process.

**Brute force attacks**: These attacks are performed by computer programs that are called "**password crackers**." A password cracker performs a brute force crack by systematically trying every possible password until it succeeds.

For example, it may start by trying all one-character passwords, then moving to two-character passwords, and so on, trying all possible combinations until they crack the password.

**Dictionary attacks:** It use word lists to structure log in attempts. Word lists can contain millions of words, including words from natural language dictionaries and sports team names, profanity, and slang. In some ways, however, a dictionary attack is similar to a brute-force attack. It is an automated process that is performed by a password cracker program.

**Phishing attacks:** For example, a phishing email can direct victims to visit a malicious fake web site where they are asked to enter their personal information, such as their password or credit card, social security, and bank account numbers. An attacker may set up a web site that is of interest to the victim, and when the victim is lured to create an account on the attacker's site, the attacker captures the password knowing that many people reuse the same password, or major portions of it, for all their web accounts.

Password attacks can be online or offline

**Online password attacks:**

An attacker makes repeated attempts to log in. The activity is visible to the authentication system, so the system can automatically lock the account after too many bad guesses. Account lockout disables the account and makes it unavailable for further attacks during the lockout period. It is also worth mentioning that online password attacks can actually be used as a form of DoS.

**Offline password attacks**

* *Offline password* attacks are far more dangerous
* In an offline attack, the attacker captures the password or the encrypted form of the password
* The attacker can then make countless attempts to crack the password without being noticed
* Some common password attack tools that are openly available include: Cain and Abel, John the Ripper, OphCrack, and L0phtCrack.

**countermeasure against password attacks**

* Many authentication systems require a certain degree of password complexity
* A common approach to reduce the risk of password brute-force attacks is to lock the account or increase the delay between login attempts when there have been repeated failures.
* Two-factor authentication: requires the attackers to have something more than the password to authenticate to the system. For example, requiring not only a password and username, but also something that only the user has.

**DNS based attacks**

DNS (Rappel)

**RR Resource records:**

* unit of information entry in DNS zone files.
* Basic building blocks of hostname and IP information and are used to resolve all DNS queries

Resource records type:

* A: associe le nom d’hôte à l’addresse ip
* PTR : associe l’adresse ip au nom
* MX : où délivré le courrier pour l’adresse user@domain
* CNAME : associe un nom alternatif au nom réel de l’hôte
* TXT : tout texte descriptif
* NS (name server) :

3 rôles impliqués dans le DNS

**Resolver**:

* Prends la demande de l’application et formate la demande dans le paquet UDP.
* Envoie la demande au cache DNS

**Server cache ou récursif** :

* Renvoie la réponse si elle est déjà connue ou recherche un serveur autoritaire qui a l’information
* Cache le résultat pour les requêtes futurs

**Serveur autoritaire** : contient l’information réelle mise dans le DNS par le propriétaire du domaine

Malware uses DNS in these three ways:

* To gain CnC.
* To exfiltrate data.
* To redirect the victim's traffic.

**DNSChanger:**

* a Trojan that changes the DNS settings on the infected host.
* **The DNSChanger Trojan** replaces the name servers with their own in order to direct web and other requests from the infected host to a set of attacker-controlled servers that can intercept, inspect, and modify the infected host traffic

**DNS open resolver** is a DNS server that allows DNS clients that are not part of its administrative domain to use that server to perform recursive name resolution

DNS open resolvers are vulnerable to multiple malicious activities, including the following:

* DNS cache poisoning attacks
* DNS amplification and reflection attacks
* DNS resource utilization attacks

**DNS cache poisoning attacks**

* It occurs when an attacker sends falsified and usually spoofed RR information to a DNS resolver.
* Once the DNS resolver receives the falsified RR information, it is stored in the DNS cache for the lifetime (TTL) set in the RR.
* Attackers use this exploitation technique to redirect users from legitimate sites to malicious sites or to inform the DNS resolver to use a malicious name server that is providing RR information for malicious activities.

(RR: When a DNS resolver sends a query asking for information, an authoritative or a non-authoritative server may respond with a DNS query response message and the relevant resource record (RR) data or an error. The RR contains a 32-bit Time to Live (TTL) field that is used to inform the resolver how long the RR may be cached until the resolver needs to send a DNS query asking for the information again. This field can be used maliciously by setting the value for an RR to a short or long TTL value.)

* **DNS amplification and reflection attack** uses DNS open resolvers to increase the volume of attacks and to hide the true source of an attack—actions that typically result in a DoS or DDoS (Distributed Denial of Service) attack.
* **DNS resource utilization attack** is a DoS attack that consumes the resources on the DNS open resolvers. Examples of such resources include CPU, memory, and socket buffers. This DoS attack consumes all the available resources to negatively impact the operations of the DNS open resolver.

**Countermeasures:**

* Internal DNS server within an organization should be prevented from acting as a DNS open resolver.
* BIND is a software product of Internet Systems Consortium, Inc. BIND implements the DNS protocol. Microsoft Windows servers can also implement the DNS protocol. An organization using their own managed local DNS servers can help analysts capture and log the DNS data.
* Organizations can prevent the use of non-authorized DNS servers, and prevent users from doing DNS lookups through other non-locally managed DNS servers.

**Others attacks techniques (pas bien compris)**

* Fast flux
* Double IP flux
* Domain generation algorithms

Countermeasures to attacks techniques using fast flux, double IP flux, and DGA include the following:

* Monitor the DNS log for suspicious activities
* Deploy a solution, such as Cisco Umbrella

**DNS Tunneling**

DNS tunneling is where another protocol or data is hidden in the DNS packets. Typically, attackers will use DNS tunneling for stealthy data exfiltration in a data breach, or for the CnC traffic communications

**Web-Based Attacks**

* Cisco security researchers observed that popular websites were redirecting users to the Angler exploit kit through malvertising (bannières publicitaires).
* With malvertising, the victim's machine can become infected pre-click or post-click.
* Examples of pre-click malware include malware being embedded in the web page or drive-by downloads.
* An example of a post-click malvertisement is where the user clicks the add to visit the advertised site, and instead is directly infected, or redirected to a malicious site.
* Cybercriminals who are attempting to spread malware through malvertising might first use clean advertisements on trustworthy sites to gain a good reputation, then later insert the malicious code in the advertisement. After a mass infection has occurred, the malicious code in the advertisement is then removed to avoid detection, therefore infecting all visitors to the site only during a specific time period.
* Many web attacks make use of compromised legitimate web sites, created by the popular web development platform WordPress, to stage their cybercriminal activities.

**Countermeasures to web-based attacks:**

* web application developers must follow best security practices in developing their web applications, for example, referencing the best practices recommended by Open Web Application Security Project (OWASP).
* Keep the operating system and web browser versions up-to-date.
* Deploy services such as Cisco Umbrella to block the users from accessing malicious web sites.
* Deploy a web proxy security solution, such as the Cisco Web Security Appliance, to block users from accessing malicious web sites.
* Educate end users on how web-based attacks occur.

**HTTP 302 Cushioning**

Attackers often use legitimate HTTP functions, such as HTTP redirects, to carry out their attacks.

**HTTP redirection**: The browser interprets the **302 HTTP** response status code to mean that the requested resource has been temporarily relocated to the new location provided in the response. The browser is invited to make an identical request to the new URL that is specified in the location field

* Attackers can use the legitimate "302 Found" response to create a series of web redirections before the victim’s browser is finally redirected to the page that delivers the exploit to the victim's machine.

**Iframe:**

* An iFrame is an HTML element which allows website developers to load another web page.
* The iFrame HTML element is often used to insert content such as advertisements from another source into a web page.
* Injecting malicious HTML iFrames into legitimate websites has also become a common attack vector that is used in web-based attacks.

**Countermeasures to attacks using HTTP 302 cushioning:**

* Use a service such as Cisco Umbrella to block the users from accessing malicious web sites.
* Deploy a web proxy security solution, such as the Cisco Web Security Appliance (WSA) to block users from accessing malicious web sites.
* Educate end users on how the browser is redirected to a malicious web page that delivers the exploit to the victim's machine through a series of HTTP 302 redirections.

**Command Injection**

* Command injection attack executes arbitrary commands on the web server’s OS via a vulnerable web application
* SQL injection and XSS are two specific forms of command injection attacks
* It is usually possible when a web site allows added strings of characters or arguments without any input validation
* Countermeasures: applications developers should performs proper user input validation, deploying an IPS solution

**SQL Injection**

* An SQL injection attack consists of inserting a SQL query via the input data from the client to the application.
* A successful SQL injection exploit can read sensitive data from the database, modify database data, execute administration operations on the database, and, sometimes, issue commands to the operating system.
* Countermeasures: Deploy an IPS solution to detect and prevent malicious SQL injections.

**Cross-Site Scripting**

* XSS involves the injection of malicious scripts into web pages that are executed on the client-side in the user’s web browser.
* Malicious scripts can be used to gain access to user's systems or sensitive information, such as the session cookies. script.

Types of XSS attacks include:

* **Stored (persistent):** Stored XSS is the most damaging type because it is permanently stored in the XSS-infected server. The victim receives the malicious script from the server whenever they visit the infected web page.
* **Reflected (non-persistent):** Reflected XSS is the most common type of XSS attack. Reflected XSS attacks only require that the malicious script is embedded in a link. In order for the attack to succeed, the victim needs to click the infected link. Reflected XSS attacks are typically delivered to the victims via an email message, or through some other web site. When the victim is tricked into clicking the infected link, the malicious script is reflected back to the victim's browser, where it is executed

Countermeasures include the following:

* Deploy a service such as Cisco Umbrella to block the users from accessing malicious web sites.
* Deploy a web proxy security solution, such as the Cisco Web Security Appliance to block users from accessing malicious web sites.
* Deploy an IPS solution to detect and prevent malicious XSS or CSRF.
* Educate end users—for example, how to recognize phishing attacks.

**CSRF**

* CSRF is a type of attack that occurs when a malicious web site, email, blog, instant message, and so on, causes a user's web browser to perform an unwanted action on a trusted web site for which the user is currently authenticated.
* For example, the attacker compromises a web site (or creates an email) with a link that includes the malicious script. When the victim clicks the link, the malicious script accesses a third-party web site (for example, the victim's bank) that trusts the victim’s browser credentials (for example, the authentication cookie), resulting in the transfer of money from the bank account out to the attacker.

**Email-Based Attacks**

Email threats

* **Attachment-based:** Embedding malicious content in business appropriate files is most common for attachment-based attacks. Specifically crafted attacks come in targeted messages that include such malicious attachments.
* **Email spoofing** is the creation of email messages with a forged sender address that is meant to fool the recipient into providing money or sensitive information.
* **Spam** is unsolicited email or "junk" mail that you receive in your inbox. Spam generally contains advertisements, but it can also contain malicious files.
* **An open mail relay** is an SMTP server that is configured to allow anyone—not just known corporate users—on the Internet to send email. Therefore, it is important for the companies to ensure that their SMTP server (such as their exchange) is not set up as an open mail relay.
* **Homoglyphs** are text characters that have shapes which are identical or similar to each other. With the advanced phishing attacks today, phishing emails may contain homoglyphs