Cyber-attack types

# Denial of Service

A denial of service (DoS) attack overwhelms a systems resources so that it cannot respond to service requests. A distributed denial of service (DDoS) is a DoS attack launched from several other host machines controlled by the attacker.

A DoS-attack is not directly beneficial for the attacker but the effect of it may be beneficial (may be used as blackmailing, take a system offline or just service denial).

Examples of DoS-attacks are:

* TCP SYN flood attack
* Teardrop attack
* Smurf attack
* Ping-of-detach attack
* Botnets

# Man-in-the-middle (MitM) attack

A man in the middle attack occurs when a hacker inserts itself between the communication of a client and a server. Common types are:

* Session hijacking (used on identified session or with DDoS-attack on identified target)
  + A client connects to a server.
  + An attacker get control over the client.
  + The attacker disconnects client from the server attacker replaces clients IP with its own IP and spoofs the client’s sequence numbers.
  + The attacker continues dialog with the server believing it is still communicating with the client.
* IP Spoofing

Used to convince a system that it is communicating with a known, trusted entity and thus provide access to the system. The attacker sends a packet with the IP source address of a known, trusted host (instead its own IP source address) to a target host. The target might accept the packet and act upon it.

* Replay

An attack intercepts and saves old messages and tried to send them later impersonating one of the participants (can be countered with timestamps or a string that changes the time).

Generally, encryption and digital certification provides an effective safeguard against MitM attacks. To solve a compromised public key, certification authorities and hash functions were created.

If a person P\_A want to send a message to person P\_B and P\_B want to be sure that only P\_B can read the message and that the message are from P\_A following method can be used:

1. P\_A creates a symmetric key and encrypts it with P’s public key.
2. P\_A send the encrypted symmetric key to P\_B.
3. P\_A computes a hash function of the message and digitally signs it.
4. P\_A encrypts his message and the message’s hash using symmetrical key and send the entire thing to P\_B.
5. P\_B is able to receive the symmetric key from P\_A because only he has the private key to decrypt the encryption.
6. P, and only P, can decrypt the symmetrically encrypted message and signed hash because he has the symmetric key.
7. He is able to verify That the message has not been altered because he can compute the hash of received message and compare it with the digitally signed one.
8. P is able to prove himself that P\_A was the sender because only P\_A can sign the hash so that it is verified with P\_A public key.

# Phishing

The attack “Phishing” is the practice of sending out emails that appear to be from trusted sources with the goal of gaining personal information or influencing users to do something. This attack combines social engineering with technical tricking. Phishing can involve links, instructions or downloadable malicious content.

More targeted phishing where attacks could be more personal etc. have gotten the name “Spear phishing”. Email spoofing (when information in the “from” field is falsified) can be used.

To reduce the risk of being phished use critical thinking, hovering over the links, analyze the email headers and sandboxing.

# Drive-by attack

A common method for spreading malware. Commonly a malicious script is planted into HTML or PHP code on a website and is used to directly install malware or redirect the user to a hacker-controlled site. A drive-by download can take advantage of an app, OS, or a web browser that contains security flaws.

To reduce the chance of being affected by a drive-by attack, keep applications, operating systems and browsers up to date and avoid website which may contain malicious code.

# Password attack

Accessing someone’s password either by guessing or by “sniffing”. This can be done in 2 methods:

* Brute-force attack
* Dictionary attack

Use password best-practices!

# SQL injection attack

Common issue with database driven websites. An SQL injection attack occurs when a hacker executes a SQL query to the database via the input data from the client to server. SQL commands are inserted into data plane input to tun predefined SQL commands. A successful SQL injection attack can read, insert, execute, recover and in some cases issue commands to the operating system.

SQL attacks works mostly if a website uses dynamic SQL.

To protect yourself against SQL injection attacks, apply least0privalage model of permissions in your databases. Stick to stores procedures (make sure those procedures do not include any dynamic SQL) and prepared statements (parameterized queries). Validate input data against a white list at application level.

# Cross-site scripting (XSS) attack

Use third-party web resources to run scrips in the victim’s web browser or scriptable application. Specifically, the attacker injects a payload with malicious JavaScript into a website’s database. When the victims request a page from the website, the website transmits the page, with the attacker’s payload as part of HTML body, to the victims browser, which then executes the malicious script. Examples are sending the victims cookie to an attacker’s server; the attacker can extract it and ise it for session hijacking. The most dangerous consequences occur when XSS is used to exploit additional vulnerabilities. These vulnerabilities can enable an attacker to not only steal cookies, but also log keystrokes, capture screenshots, discover and collect network information, remote access and control the victim’s machine.

# Eavesdropping attack

Interception of network traffic. By eavesdropping, an attacker can obtain passwords, credit card numbers and other confidential information that the user might be sending over the network.  
Eavesdropping can be passive or active:

Passive: A hacker detects information by listening to message transmission in the network.

Active: A hacker actively grabs the information by disguising himself as friendly unit and by sending queries to transmitters. This is called probing, scanning, or tampering.

Data encryption is the best countermeasure for eavesdropping.

# Birthday attack

Birthday attack are made against hash algorithms that are used to verify the integrity of a message, software, or digital signature. A message produced by a hash function produces a message digest (MD) of fixed length, independent of the length of the input message; this MD uniquely characterizes the message. The birthday attack refers to the probability of finding two random messages that generate the same MD when processed by a hash function. If an attacker calculates same MD for his message as the user has, he can safely replace the user’s message with his, and the receiver will not be able to detect the replacement even if he compares MDs.

# Malware attack

Malicious software can be described as unwanted software that is installed in your system without your consent. It can attach itself to legitimate code and propagate; it can lurk in useful application and replicate itself across the internet. Here are some of the most common types of malware:

* Macro viruses: Executing instructions within an applications (like MS Word or Excel) initialization sequence.
* File infectors: Attach themselves to executable code. Virus is installed when the code is executed. Another file infector are files with the same name as a legitimate executable but instead of running the legitimate program, a virus code will be executed.
* System or boot-records infectors: Attaches to the master boot record on hard disks. When a system is started it will look at the boot sector and load the virus into memory where it can propagate to other disks and computers.
* Polymorphic viruses: Uses a mutation engine and routines through varying cycles of encryption and decryption. The virus is difficult to detect but it has a high level of entropy due of the many modification of source code which can make it easy for antiviruses to find it.
* Stealth viruses: Take over system function to conceal themselves. They compromise malware detection software to report infected area as uninfected.
* Trojans: A program which hides in useful programs and usually has a malicious function. Trojans do not self-replicate. Trojans can establish a backdoor that can be exploited by attackers. For example, Trojan can be used to open a high-numbered port so the hacker can use it to listen and then perform the attack.
* Logic bombs: A malicious software appended to an application triggered by a logical condition or a specific time and date.
* Worms: Worms differ from viruses in that they do not attach to a host file but are self-contained programs that propagate across networks and computers. Worms are commonly spread through mail attachments; opening the attachment activates the worm program. A typical Work exploit involves the worm sending a copy of itself to every contact in an infected computer’s email address in addition to conducting malicious activities, a worm spreading across internet and overloading email servers can result in a DoS attacks against nodes in the network.
* Droppers: A program used to install viruses on computers. In many instances a dropper is not infected with malicious code itself and thus not detected by antivirus. A dropper may be connected to internet downloading and updating virus software that is resident in a compromised computer.
* Ransomware: Ransomware is a type of malware that blocks access to the victim’s data and threatens to publish or delete it unless a ransom is paid. While some simple computer ransomware can lock the system in a way that is not difficult for a knowledgeable person to reverse, more advanced malware uses a technique called cryptoviral extortion, which encrypts the victim’s files in a way that makes them nearly impossible to recover with decryption key.
* Adware: Software applications used by companies for marketing purposes. Advertising banners are displayed when any program is running.
* Spyware: A type of program that is installed to collect information about users, their computers, or their browsing habits. It tracks everything you do without your knowledge and send the data to a remote user. It can also download and install another malicious program from the internet. Spyware works like adware but is usually a separate program that is installed unknowingly when you install another freeware application.