Reconnaissance

- Reconnaissance obtains information about the intended victim.
- In a targeted attack the attacker will typically start with completely unobtrusive methods, such as searching whois information, phone directories, job listings etc.
- They will then dig deeper using tools such as ping sweeps, port and vulnerability scanners

Social Engineering

- Social Engineering is the use of deception to manipulate individuals into divulging confidential or personal information.
- It typically involves nothing more technical than the use of a telephone or email.
- The attacker will often pretend to be somebody else to trick the victim.

Phishing

- Phishing is a Social Engineering attack where the attacker pretends to be from a reputable company to get individuals to reveal personal information, such as passwords and credit card numbers.
- The victim is often directed to enter their details into the attacker’s website which looks like the reputable company’s legitimate website.

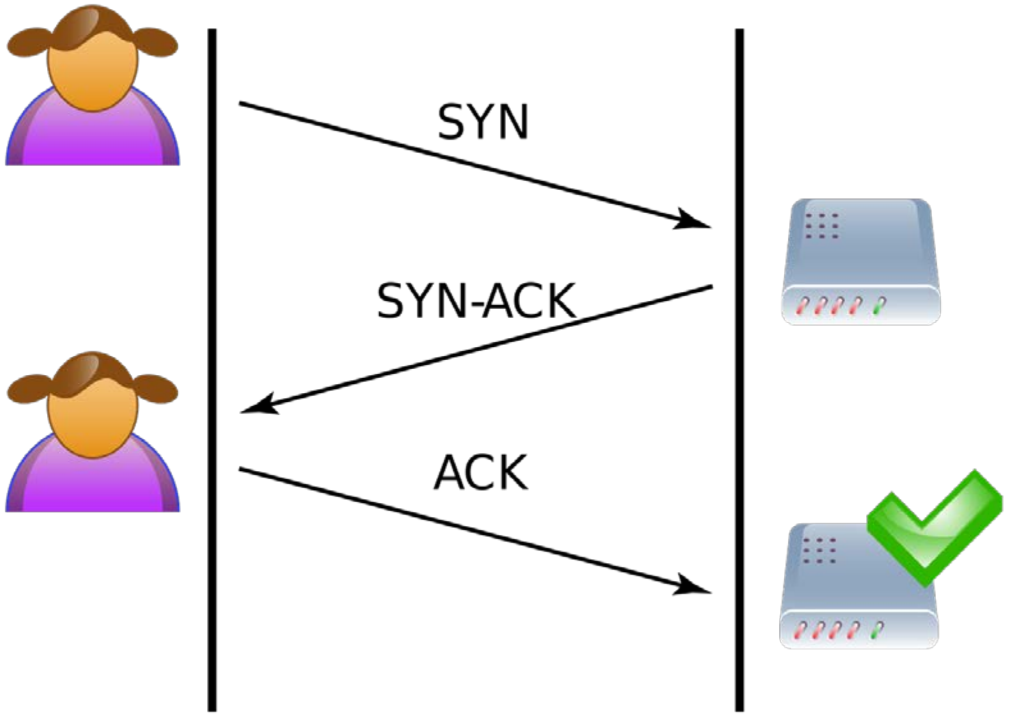
Data Exfiltration

- Data exfiltration is where data leaves an organization without authorization
- This can be by a hacker who has compromised a system
- Or by an internal staff member, either maliciously or by accident (for example sending an email which includes secret information, or leaving a USB stick on a bus)

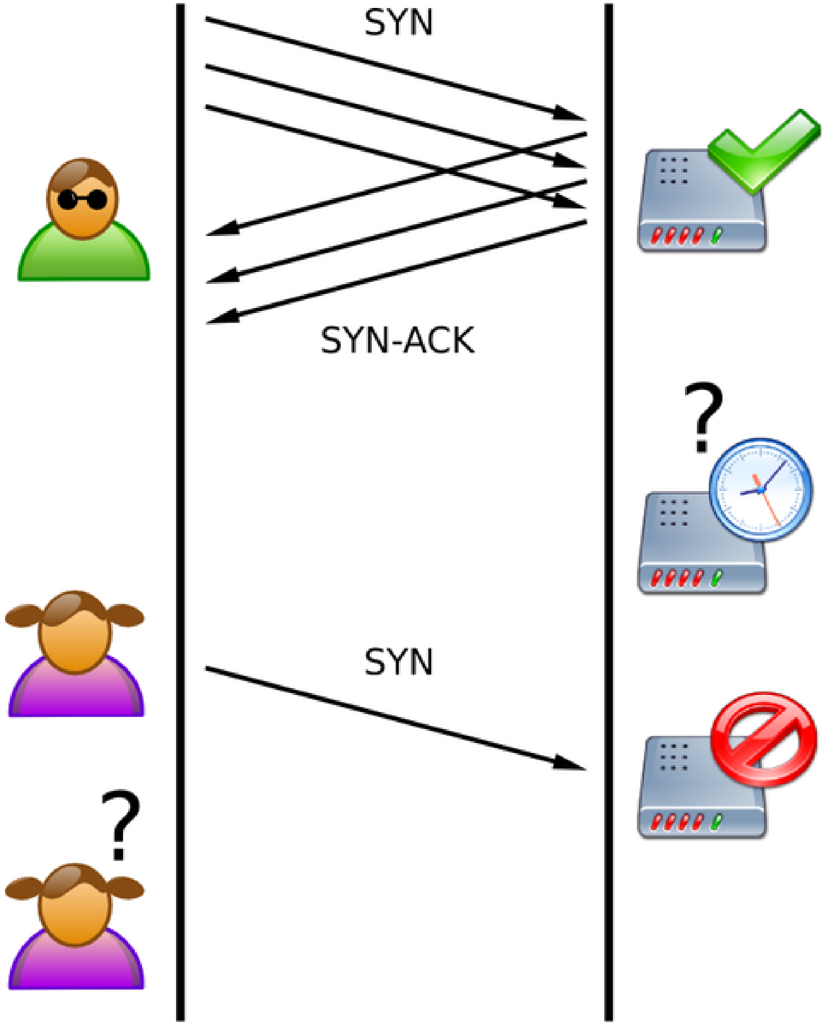
DoS Denial of Service

- A Denial of Service (DoS) attack prevents legitimate users from accessing an IT resource.
- It is typically a brute force style of attack which floods the target system with more traffic than it can handle.
- DoS attacks from a single source can be easily stopped by blocking traffic from that host.

TCP Three-Way Handshake



TCP Syn Flood Attack



DDoS Distributed Denial of Service

- A Distributed Denial of Service (DDoS) attack is a DoS attack from multiple sources.
- The attacker builds and controls a botnet army of infected zombie hosts.
- The botnet is built through malware such as worms and trojan horses.

DDoS and Botnets

- Infected hosts connect out to the attacker’s command and control server. This circumvents firewalls because the connection is initiated from the inside.
- The attacker now has control of the botnet to launch attacks.
- DDoS attacks are more difficult to mitigate against because the attack comes from multiple sources which could normally be expected to send legitimate traffic.

Spoofing

- Spoofing is where an attacker fakes their identity.
- Spoofing types include:
  - IP address spoofing
  - MAC address spoofing
  - Application spoofing (eg rogue DHCP server)

Reflection and Amplification Attacks

- A reflection attack is a DoS attack where the attacker spoofs the victim’s source address
- The attacker sends traffic supposedly from the victim which elicits a response from ‘reflectors’
- Amplification causes a large amount of response traffic to the victim

Man In The Middle Attacks

- In man in the middle attacks, the attacker inserts themselves into the communication path between legitimate hosts
- The attacker can then read and optionally modify the data
- ARP spoofing is a well known man in the middle attack

Password Attacks

- If an attacker has connectivity to a login window, they can attempt to gain access to the system behind it
- Enumeration techniques attempt to discover usernames
- Password cracking techniques attempt to learn user passwords
- Methods include:
  - Guessing
  - Brute Force
  - Dictionary attacks

Buffer Overflow Attacks

- Buffer overflow attacks send malformed and/or too much data to the target system
- This can cause a denial of service, or compromise of the target system

Packet Sniffers

- If an attacker has compromised a target system or inserted themselves into the network path, Packet Sniffers such as WireShark can be used to read the sent and received packets
- Any unencrypted sensitive information can be learned by the attacker
- They can use this to damage the organization or escalate their attack