METHODS OF INFILTRATION

(1) ***SOCIAL ENGINEERING:*** manipulation of people into performing an action by different methods like :

- PRETEXTING : call someone and lie on to gain access to privileged data

-TAILGATING : Follow authorized person into secure physical location

-SOMETHING FOR SOMETHING : attackers ask for personal information to exchange it with something else

(2) ***DENIAL OF SERVICE DOS:***

Interruption of network services to users, devices and applications by:

-OVER HELMING TRAFFIC: when there is a large amount of data are being sent by large rate that the RX can't handle that make the server (Service) slower and can't Response to every request

- MALICIOUS FORMATTED PACKET: The attacker sends packets that have errors so that the receiver may crash or be very slow

(3) ***DISTRIBUTED DENIAL OF SERVICE DDOS:***

attackers build a network of infected hosts(Zombies) which in turn effects other real hosts

(4) ***BAT NET :***

Bats infect other computers by unsafe website by malware attachments or media files

BAT NET is a group of bats connected through the internet and are used to spread malwares, DDoS and Brute Force Password attack

(5) ***ON – PATH:***

has Two Types:

-MAN IN THE MIDDLE : Take control of a device without user knowledge and capture user data before it reach the destination

-MAN IN THE MOBILE : same as the first type but with mobile phones they capture the two step verification SMS

(6) ***SEARCH ENGINE OPTIMIZATION :***

the attackers try to put the malicious websites in the top of your search result so that the probability to open it by the user be higher

(7) ***WI-FI PASSWORD CRACK***

(8) ***PASSWORD ATTACK***

- PASSWORD SPRAYING : the attacker try most common password to different accounts so in most often he can't guess the right password

-DICTIONARY ATTACK : the attacker try every word in the dictionary by a systematic way and this may take long time and may be can't find the right password

-BRUTE-FORCE ATTACK :the attacker try every possible combination of letters, numbers and symbols

-RAINBOW ATTACK : The attacker compare the hash of the password with standard hashes that another attackers already attacks and save it

(9) ***ADVANCED PERSISTENT THREATS APT*** :

Complex, Well Encoded

Deploy Customized Malware on one or more targeted systems and remain un detected