**Module 1 Threats, Attacks & Vulnerabilities**

**1.23 Network & Wireless Attacks**

**Hijacking & Related Attacks**

* Clickjacking – tricking web user into clicking spoofed button/graphic
* Session hijacking (Cookie hijacking) – exploiting valid computer session/session key to gain unauthorised access to information/services
* URL hijacking/Type Squatting – act of registering domains that are similar to those to known entity but based on misspelling/typographical error (Eg. G00gle.com, gooogle.com)

**Network Hijacking Attacks**

* MAC Spoofing

1. Technique for changing factory-assigned MAC address of network interface on networked device
2. Media Access Control (MAC) address is hard-coded on Network Interface Card (NIC). Many drivers allow MAC address to be changed

* IP Spoofing

1. Technique used to gain unauthorised access to machines, whereby attacker illicitly impersonates another machine by manipulating IP packets
2. Involves modifying the packet header with forged (spoofed) source IP address, a checksum & order value

* ARP Spoofing

1. Attacker sends fake ARP (Address Resolution Protocol) messages over local area network
2. Results in linking of attacker’s MAC address with IP address of legit computer/server on network

**Man-in-the-Middle Attacks**

* Attack where attacker secretly relays & possibly alters communication between 2 parties who believe they are directly communicating with each other
* Attacker may either observe (confidentiality attack) or alter (integrity attack)

**Denial of Service (DoS) Attacks**

* Preventing access to resources by users authorised to use them. Attacking system’s availability
* May accomplish:

1. Deny access to information, apps, systems or communications
2. Bring down website while communications & systems continue to operate
3. Crash OS (simple reboot may restore server to normal operation)
4. Fill communications channel of network & prevent access by authorised users

**Distributed Denial of Service (DDoS) Attacks**

* DoS attack utilising multiple compromised computer systems as sources of attack traffic
* Amplifies concept of DoS attack by using multiple computer systems (often through botnets) to conduct attack against single organisation

**DoS & DDoS (Prevention)**

* Work with ISP/network provider
* Border protection/intrusion detection & prevention system
* Update network appliances, OS & apps
* End users’ systems are up-to-date & deploy anti-virus – bot prevention

**Amplification attacks**

* Goal of attacker is to get response to their request in greater than 1:1 ratio so additional bandwidth traffic works to congest & slow responding server down
* Ratio achieved known as amplification factor, & high numbers are possible with UDP based protocols such as NTP, CharGen & DNS
* Usually employed as part of DDoS attack

**Domain Hijacking/DNS Poisoning/DNS Spoofing**

* AKA Resolution attacks
* Poisoning – when attacker alters domain-name-to-IP-address mappings in DNS system to redirect traffic to rogue system/perform DoS attack
* Spoofing – when attacker sends false replies to requesting system in place of valid DNS response
* Protect any internal DNS servers
* Use authoritative DNS sources

**Wireless Attacks**

* Evil Twin – rogue wireless access point poses as legit wireless service provider to intercept information that users transmit
* Rogue AP – any wireless access point added to your network that has not been authorised
* Initialisation Vector (IV)

1. Arbitrary number that can be used along with secret key for data encryption
2. This number, AKA nonce, is employed only once in any session
3. If IV is weak, as in WEP, it may be reused

* Jamming – causing interference with wireless signal

**PAN Wireless Attacks**

* Bluejacking – sending of unsolicited messages (think spam) over Bluetooth connection
* Bluesnarfing

1. Gaining of unauthorised access through Bluetooth connection
2. Intercepting data through Bluetooth connection