**Module 1 Threats, Attacks & Vulnerabilities**

**1.21 Social Engineering Attacks**

**Attack types (All)**

* Social engineering

1. Phishing, Spear phishing, Whaling, Vishing, Tailgating, Impersonation, Dumpster Diving, Shoulder Surfing

* Application/Service attacks

1. Buffer Overflow, Injection, Cross-site scripting, Cross-sit request forgery, Privilege escalation, Impersonation/Masquerading, Replay, Driver manipulation (Shimming, Refactoring)

* Cryptographic attacks

1. Birthday, Known plain text/Cipher text, Rainbow tables, Dictionary, Brute force, Pass the hash

* Hijacking & related attacks

1. Clickjacking, Session hijacking, URL hijacking, Typo squatting, MAC spoofing, IP spoofing

* Network/Wireless attacks

1. DoS, DDoS, Main-in-the-middle, Amplification, DNS poisoning, Domain hijacking, ARP poisoning, Initialisation vector (IV), Evil twin, Rogue AP, Jamming, Bluejacking, Bluesnarfing

**Social Engineering**

* Process where intruders gain access to facilities, network, systems, data & even employees by exploiting trusting nature of people
* Use of deception to manipulate individuals into divulging confidential/personal information that may be used for fraudulent purposes

**Social Engineering Attack Types**

* Online

1. Phishing, Vishing, Whaling, Spear phishing
2. Spoofing

* Offline/Physical

1. Tailgating
2. Impersonation
3. Dumpster diving
4. Shoulder surfing

* Either

**Communications Spoofing/Fraud**

* Phishing – sending emails purporting to be from reputable companies to induce individuals to reveal personal information
* Spear Phishing – sending emails ostensibly from known/trusted sender to induce targeted individuals to reveal confidential information
* Whaling – phishing attack that specifically aimed at wealthy/powerful/prominent individuals
* Vishing – making phone calls/leaving voice messages purporting to be from reputable companies
* Pharming – traffic redirected to spoofed website
* Variants – SmiShing (SMS phishing)
* Hoax – malicious actors issuing false warnings to alarm users
* Swatting – fraudulent calls to police to dispatched swarm of police to specific address
* Watering Hole Attack – security exploit where attackers seek to compromise specific group of end users by infecting websites members of group visits

**Social Engineering Attacks (Physical)**

* Tailgating – gaining entry to electronically locked systems by following someone through door they just unlocked
* Dumpster Diving – foraging in garbage for discarded items that may still be valuable/useful/used to commit fraud
* Shoulder Surfing – watching someone “over their shoulder” when they enter sensitive data eg. Password/credit card information

**Social Engineering Principles**

* Reasons for effectiveness

1. Authority
2. Intimidation
3. Consensus/Social Proof
4. Scarcity
5. Familiarity/Liking
6. Trust
7. Urgency
8. Reciprocity

**Social Engineering Prevention**

* User education
* “Trust, but verify”
* “If you see something, say something”