Week 10 - Explain different ways to use Social Engineering (vectors) and denial of service attacks(DOS)

Vishing

Vishing is when you use social engineering over the phone to gain access to personal and/or financial information.

Phishing

Phishing is when scammers try to gain access to usernames, passwords and other personal information where they appear to be someone who has trust enough for the other parts to give up their information. This can also be done by setting up fake sites and other ways.

Smishing

Like phishing but primarily through sms and text messages

Impersonation

Er hvor man udgiver sig for at være en anden med det mål at få fysisk adgang til et system eller bygning.

Discuss ways to detect social engineering attempts (principles)

Reciprocity

Reciprocity means “inclination and want to return a good dead with another good dead”. That means that you can do something nice for someone in order to manipulate them to give you something nice back, i.e. you ask for something that might be company information.

Commitment and consistency

People have a tendency to be very consistent in their behavior, and really want to live up to that in their personal life. This can override logic, because people value and respect people with integrity. For example, you might try and sway people to do something they normally wouldnt, if you gradually up the stakes by giving them something for free then asking for money after a while for the same thing.

Social proof
Herd mentality. You want to fit in, so you might to stupid things in order to feel like you fit in.

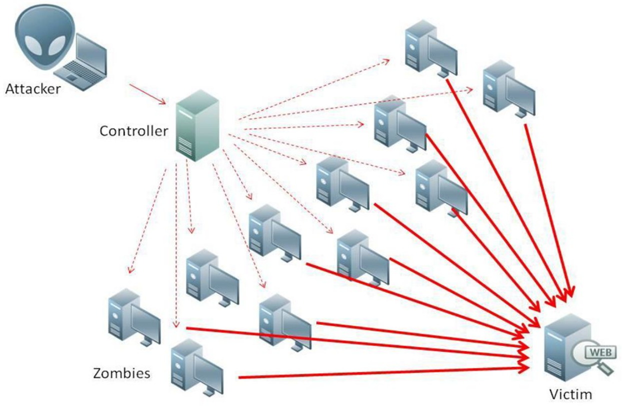
Authority
Most people, some more than others, have a great tendency to obay authorities. This can be seen as an example in war, when people can be made to do awfully cruel things because their leader told them. This can be used to blackmail or demand people to do things they normally wouldn't.

Scarcity
Buy now, or else you might miss the opportunity, is an example of using scarcity to make people do what you want.

Explain the most common DoS strategies

Crash Service
To make a service crash, in relation to **Flood Service** witch makes a service slow and flooded with requests that overloads the system

Distributed attacks
An army of “zombies” can be sent do make requests in order to overload a service. Can be hard to stop since there are so many different ips



Discuss Application layer attacks

Application layer attacks is a way of using a DOS attack to the application layer of, for example, a website. If you attack functions on a website in order to deactivate them, they can cause large confusion and disruption.

Network layer attacks

In a network layer attack, the attacker tries to get unauthorized access to an orginizations network in order to gain access to sensitive data. The attacker can then choose to remain subtle, and only access the information data, or he can be destructive and change or delete files or information.

common means to minimize threads of DoS

- Outsourcing DDoS prevention (f.eks. Cloudflare)
- A good understanding of how to configure a network

Some nice links

https://www.social-engineer.org/framework/attack-vectors/
https://www.social-engineer.org/framework/influencing-others/influence-tactics/reciprocity/