Cyber Law & Security

ASSIGNMENT - 1

SRIJA RAHA
CSE 8th Sem
Roll-51

1) Distinguish between conventional crime and cyber crime. List motives behind cyber crime.

Ans:-

	Conventional Crime	Cyber Crime
Scale :	Attacks in physical world can victimize one or two groups or individual	Thousands of sites can be attacked at once.
Reach :	Attacks are performed in areas nearly to the criminal	Attacks can be performed all over the world
Speed :	Organized crimes take some time to plan out	Crimes can be conducted at machine speed
Perception and media effect :	Victims are usually always symphathized with	Blame is often put on victims for lack of security and awareness.

Motives behind cyber crimes are :-

* Financial : If the adversary can make money out the attack e.g stealing bank details.
* Ideological : Adversary might want to sabotage the system to further their propaganda or eliminate perceived threats.
* Political : Adversary might benefit from knowing intimate secrets of an organization.

* Prestige and curiosity : Sometimes, adversary might want to assert superiority or be enticed by some interesting technological footprint.

2) Explain the difference between hackers, crackers and phreakers.

Ans:) Hackers, They break the security of a network/ machine. It can get complex, but they learn some easier tricks than the hard brute force methods.

Crackers :- They have mastered the black art of removing copy protection from other people's programs. It is different from piracy, as crackers must remove all copy protection or figure out ways around it.

Phreakers : Phreakers are people who break the phone company's security, to get access to control the phones. They use it to make free phone calls, or get operator powers.

3) Describe different Phishing techniques.

Ans:) Five common phishing techniques are:-

a) Breach of Trust : False emails are send out. When victims click on the malicious links and enters credentials, nothing useful happens.

b) False lottery : User is sent bait that is too good to pass up. It usually references a trusting organization. However, on clicking link, malware loads.

c) Data Update : Malware is sent in the form of email attachment which might lead to massive security breaches.

d) Sentimental Abuse : Sometimes, bogus donations are asked for on behalf of something sentimental to the victim. These are dangerous as they might steal credit card essentials.

e) Impersonation : Email is sent while posing as someone trusted by the intended victim.

4) Explain website spoofing

Ans:) Website spoofing is the act of creating a website, as a hoax, with the intention of misleading readers that the that the website has been created by a different person or organization. The spoof website imitates the design of the target website. Even URL is shown to be similar.

To make it harder to detect, attacker often creates a 'shadow copy' of the World Wide Web

by having all of the victim's traffic go through the attacker's machine, causing the attacker to obtain the victim's sensitive information.

5) Write down the types of Phishing Scams.

Ans:) Different types of phishing scams are:-

- Spear phishing: phishing attempts directed at specific individuals or companies. In contrast to bulk phishing, spear phishing attackers often gather and use personal information about their targets to increase their probability of success.
- Clone phishing: Here, a legitimate, and previously delivered email containing an attachment or link has had its content and recipient address taken and used to create an almost identical or cloned email. The attachment or link is replaced by malicious content.
- Whaling: this is a term coined for spear phishing attacks directed specifically at senior executives and other high profile targets. Content is crafted to target the person's role in the company.

6) Distinguish between virus and worms.

Ans)

	Virus	Worms
Meaning	The virus attaches itself to executable files and transfers from one system to the other.	A worm is a malicious program that replicates itself and can spread to different computers via network.
Human action	Needed	Not required.
Speed of Spreading	Slow	Fast
Removing malware	Antivirus, formatting	Virus removal tool, formatting.
Protect the System	Antivirus software	Antivirus, firewall