Cyber Security Terms and Terminologies

Published on Friday, November 17, 2017

Spoofing

Spoofing is a type of illegitimate or unauthorized activity pretending to be original user which gives access to attacker to user's computer system or network & data or information, mostly by different means of falsifying data for attacker's advantages. Main objective is to deceive or trick the user into releasing sensitive information to steal personal information like password of bank account & credit cards, password for computer system or networks & other sensitive information.

Email spoofing-

Email spoofing (or phishing) is the most common & widely used spoofing attack, it is used when attackers are sending some mail to look like sent from genuine & trustworthy source. Attackers try to get personal details by sending dishonest mail & advertisements by the spoofed mail address. For example, a spoofed mail for some genuine bank will receive in your mail ID, asking for victims sensitive information.

Caller ID spoofing-

Caller ID spoofing is done by misleading the calling number of own into other incorrect number. It is done with the help of Voice over IP (VoIP) networks which allow attacker to forge their number details.

URL spoofing-

URL spoofing is done by setting up a fake website by an attacker, which assures victims to use their personal data to login & which will in turn send the sensitive data to attacker or install malware to their computer system. This type of spoofing generally performed when victim visits a directed website that exactly looks like a genuine and authenticate one, after that victims use their LoginID & Password which will be sent to the attacker along with some other sensitive information.

Phishing

Phishing is the illegitimate method of misleading a victim in mail or other electronic communication to obtain sensitive information e.g., login ID passwords, bank details, credit card details, etc. It is mostly carried out by email spoofing, which directs the victim to fake website that looks like genuine one & asking for their information.

We can avoid this type of phishing by checking the targeted URL for the required action. Writing a URL in address bar is a good practice to reduce this type of phishing risk.

Spear phishing-

Targeting a specific person or any organisation by gathering related information to increase probability of getting success is termed as spear phishing.

Clone phishing

Phishing attempted by identical or cloned email of previous trustworthy mail with some harmful attachment or having fake website URL or link to get personal information is termed as Clone phishing.

Whaling

Phishing attack done to top senior level executive of an organisation is called as Whaling.

Link manipulation

URLs similar to the real one is used to direct look alike fake website to get personal data, e.g., instead of 'www.facebok.com', one link in a receive mail can take the victim to 'www.facebookk.com', which has the same UI of 'facebook' & when the victim enters the login ID & password, it will be sent to the attacker.

Phone phishing-

Phone phishing is done by attackers by sending fake message to get the personal details of victim.

Hacking

Hacking is finding weakness in computer systems or networks & exploits it to gain unauthorised access.
One of the most infamous hacking was done recently during recent presidential election of USA. In which a series of E-mail chain of Hilary Clinton was published unanimously which sabotaged her presidential campaign. It was believed by some sources that it was a planned hacking by Russian hackers.

Ethical Hacking-

- Ethical Hacking is to check & exposes vulnerabilities in any software or system to help owners to fix security loopholes to protect their data or information, before any hacking attacks.
- Hacking done for ethical purposes will give very advantages in real time world.
- It is emerging as a new career opportunity for talented hackers. Many big International firms are paying these hackers to penetrate their own system &check or report any flaws and vulnerabilities possessed by any outside intruders.