social engineering is the ability to trick people into giving sensitive information without them noticing ,and example of this would be red teaming as they try to use all possible means to access a secured system and social engineering is one of them

OSINT(open source intelligence) is the ability to gather information that is publicly available on the Internet from source like social media platforms then analyzing it to obtain intelligence,for example gaining information about where you live from your facebook posts ,or hobbies and place you like to vist which is crucial information to use social engineering ,thats why you should always be careful of what you post

Bug bounty is a practice where companies hire freelancers from platforms like HackerOne,bug crowd,bug zero and etc... to help them find bugs in their software(more famous in websites,and recently appeared in mobile application) and they pay them according to the danger level of the bug found

CTF(capture the flag) is a cyber security event where people need to complete a goal(completing the goal is the same as finding the flag) and they can simulate real life scenarios and happens in different cyber security fields like pentesting websites,networks,mobile apps and etc...

when starting in the cyber security field you need to study the following basics regardless of your specialization:

basics of networks
basics of programming
basics of operating systems(linux)

important definitions:

vulnerability is a weakness in the system that causes it no to do it intended purpose and it could be used maliciously

exploit is action of using those vulnerabilities maliciously

session is time between successfully exploiting the system and leaving the system

payload is the tool or attack used to conduct the exploit

zero day is a type of vulnerability that is very difficult to fix ,and its discovered for the first time

security through obscurity is a practice where you hide the type of defensive mechanisms in the system to make it harder to find vulnerabilities

authentication is a way to verify your identity so the system can be sure that you are not a pen tester

authorization is level of access you have in the system, depending on your role,the higher your level the more access you have to it

script is something that does a specific function

a program has GUI where you can perform many different functions like microsoft office

normal web is about 16% of the entire internet which normal browsers like google and fire fox can access

the deep web includes any websites that cant be access from google search

the dark web include the parts of the web that crimes may occur as selling illegal objects,and it requires specific software to access and high security so you dont get viruses

specific definitions

administrator is someone who has full access for the system while the user can only use the functions allowed to him by the administrator(in window)

root is the same thing as an administrator but for linux

privilege is the level of authority given by an administrator to a user,and pen testers could try to increase their privilege to control the entire system

eavesdropping is the ability when a user can spy on the activity of other users and record them(mostly in networks)

DOS is an attack when a user wants to overwhelm the system with too many requests,so that other users cant use it (uses one device)

DDOS is the same as DOS but uses multiple devices and is more powerful

server is the place where different ports are stored

ports can provide many services for the user

services are the actions that the user want to do

protocol is the language used between the user and the port so that the port performs smoothly

HTTP is a type of prtocol used in web services and its unsecure while HTTPS is secured as it encrypts the information

status codes are used to know if the connection between user and the server was successful and to know the errors if thy occur

shellcode is the script used to exploit a vulnerability

encoding preserves data readability can be reversed by using the reverse of the algorithm used for encoding

encryption changes the data in anyway that cant be understood without knowing the key

hashing is encrypting the data in such a way thats not reversible and used a way of verification

hashing techniques are used make the hashing more complex,for example by adding extra data to the input

VPN is the network between two devices which is very secured with powerful encryptions called cryptography

tunnel is a way to transfer data between two devices in a direct way that isnt detected by public networl

malware is type of software thats designed to harm the system or user and there are many types like(trojan,worm,virus,ransomware)

bypass and evasion mean that the attack has successfully avoided the defense layers of the system

NEW TERMS

1-an IP (Internet Protocol) address is a unique string of numbers separated by periods like (IPv4) or colons like (IPv6) that identifies each device connected to the internet or a local network and its used for unique identification of devices

and they can be classified by different aspects like
Based on Addressing Scheme (IPv4 vs. IPv6)
Based on Usage (Public vs. Private)
Based on Assignment Method (Static vs. Dynamic)

2-LAN means local networks, ip addresses can be assigned manually by the administrator of the system (static IP) or automatically by a DHCP server and devices within the same network communicate directly using their local IP addresses.

2-Dynamic Host Configuration Protocol (DHCP) is a network server that automatically assigns ip address and other networking parameters to client devices which decrease error that could result from doing it manually

3-WAN: for devices on different networks, the data must travel through multiple routers across the internet and each router makes independent decisions about the best route for the packets based on the destination IP address

4- packet is the basic unit of data thats group together and transfered to other devices through the internet qnd its size depends on the structure of the network

5-Network Address Translation(NAT) is a process where multiple local IP addresses are mapped to a single public IP address. This conserves IP addresses and adds a layer of security by hiding internal IP addresses from the external network.

6-IP spoofing is a technique used to bypass security measures and launch attacks, or gain unauthorized access to systems by pretending to be a trusted IP address, and do malicious activities

7-public key cryptography is a method of encrypting or signing data with two different keys and making one of the keys, the public key, available for anyone to use. The other key is known as the private key. Data encrypted with the public key can only be decrypted with the private key.

8-puplic key certificate includes the public key and information about it and information about the identity of its owner (called the subject), and the digital signature of an entity that has verified the certificate's contents (called the issuer). If the device examining the certificate trusts the issuer and finds the signature to be a valid signature of that issuer, then it can use the included public key to communicate securely with the certificate's subject, and its used in email encryption and code signing

9-Transport Layer Security (TLS) is a cryptographic protocol designed to provide communications security over a computer network, such as the Internet. The protocol is widely used in applications such as email, instant messaging, and voice over IP, but its use in securing HTTPS remains the most publicly visible.

10-Code injection is an attack that injects code into an application and that injected code is then interpreted by the application, changing the way a program executes,the attack typically exploits a vulnerability that allows the processing of data that isnt suitable for the application