التاريخ: / /  الموضوع:

# Summarization of 1st cyber security session.

Social engineering: is in everybody's life from a child to a grown adult is the mean of persuation in summary and awareness of cyber attacks.

OSINT: (open source intelligence) available information mostly related to social media

Bug bounty: (connected to web application penteration system) Freelancers get paid from a certain company to investigate and find out any bugs or vulnerability in their systems so they can fix them, the freelancer (security researcher) rates the complexity or influence of the bug from low (doesn't have a grand effect on the users info.) to critical which is the highest level (can't be found easily in big companys). After they find the bug the company gives them a [bounty] thanks to their contributions.

CTF (Capture the flag) a cyber security competition where you have to do a task to reach the flag. Some challenges may be like some stuff in the real word [stuff here means things you may get asked to search for in a company you're working with in real life]. These tasks have many ( ). like

- Hacking (pentesting) a website, a system, a network or a mobile app.
- Reverse engineering: Reverse the job of a certain system to find the flag.
- Hypiography: break the hashing
- Investigation of cyber attacks
- OSINT

التاريخ: / /  الموضوع: _____

In general definitions:

→ Hacker: is an feature in a person who loves to find information or someone who is curious about how a specific something works.

→ White hacker: someone whose principal is clean and innocent without any mean of harm (ethical hacker)

→ Black hacker: someone who takes advantage of any vulnerability and uses them to harm others or for his personal gains (crackers)

→ User: any person who uses anything or any platform and knows the info he uses daily

→ Malicious user: doesn't have technical skills like the black hackers but overall they're the same in wanting to harm other people or in this case other users of a special platform.

→ Attack: local: attacking in the surrounding area
Remote: penetration of a foriegn system or device far away from you can be in another country using (RCE)

→ Vulnerabilities: a kind of bug that leads to a specific error in the system

→ Exploit: using the vulnerabilities of the system in an unethical way

→ session: the time taken to exploit without being caught

→ payload: The harm that is intended toward the system

→ Zero day: a specific kind of vulnerability that only one notices and can't be solved easily

→ security through obscurity: giving the least amount of information needed to keep the important data safe from being exposed.

→ Authentication: making sure the data entered is the right data

→ Authorization: making sure authority to the data is in the right hands

→ Script: using the terminal of the program which is faster

→ normal program: using the program using the GUI or the icons in the daily use

التاريخ: / /  الموضوع:

# Summarization of 1st cyber security session.

Social engineering: is in everybody's life from a child to a grown adult it's the mean of persuation in summary and awarness of cyber attacks.

OSINT: (open source intelligence) available information mostly related to social media.

Bug bounty: (connected to web application perturation system) Freelancers get paid from a certain company to investigate and find out any bugs or vulnerability in their systems so they can fix them, the freelancer (security researcher) rates the complexity or influence of the bug from low (doesn't have a grand effect on the users info.) to critical which is the highest level (can't be found easily in big companys). After they find the bug the company gives them a [bounty] thanks to their contributions.

C.T.F (Capture the flag) a cyber security competition where you have to do a task to reach the flag. Some challenges may be like some stuff in the real word [stuff here means things you may get asked to search for in a company you're working with in real life]. These tasks have many ( ). like

- Hacking (pentesting) - a website, - a system, a network or a mobile app.
- Reverse engineering: Reverse the job of a certain system to find the flag.
- Hyptography: break the hashing
- Investigation of cyber attacks
- OSINT

التاريخ: / /  الموضوع:

Normal web: shows only 16% of the estimated results
deepweb: shows the 100% of the result
darkweb: the bad part of the deep web
Root: equivelant to administrator in Linux
Administrator: someone who is in charge of everything on windows
User: someone who use an operating system for personal use.
permessions: every use has access to his data only can't access other data
privilage (privilage escalation) privilage is giving to the administrator so they can access all the data, privilage escalation is the way of make an ordinary user have access like the administrator
eavesdropping: someone who gets a hold of data between two devices without their permession and without them noticing it (MITM)
DOS → (denial of service) prevention of a service from other users except one-self
DDOS → (couple denial of service) multiple device performing DOS on a system
Server → The system where one needs a specific service
port → place in a system where the service is performed
protocol → way of communication between user and the port to perform the service
HTTP → web server protocol (unsecure)
HTTPS → web server protocol (secure) using encryption.
status code → A way of understanding between a user and a server
shell code → a specific type of script which is mostly used during exploit
encoding → changing shape of data but it is still readable and can be reversed (decoding)
encryption → " " " " can't be read unless you know the way of encryption
Hashing → unreversable encryption (un understandable text indicates specific data)
Hashing techniques: (salt (static) (dynamic) or pepper)
Sniffing → (wire shark (GUI), TCP Dump (CLI)) awaiting some kind of mistake in the system by constantly watching the data being shared across servers.

الموضوع: _____ التاريخ: / /

Cryptography: hashing of connections

VPN: virtual private network only you and the server can access using cryptography

Tunnel: like VPN but between two devices only no one outside can access

Malwares: harmful softwares with different types and examples but most lead to stealing data