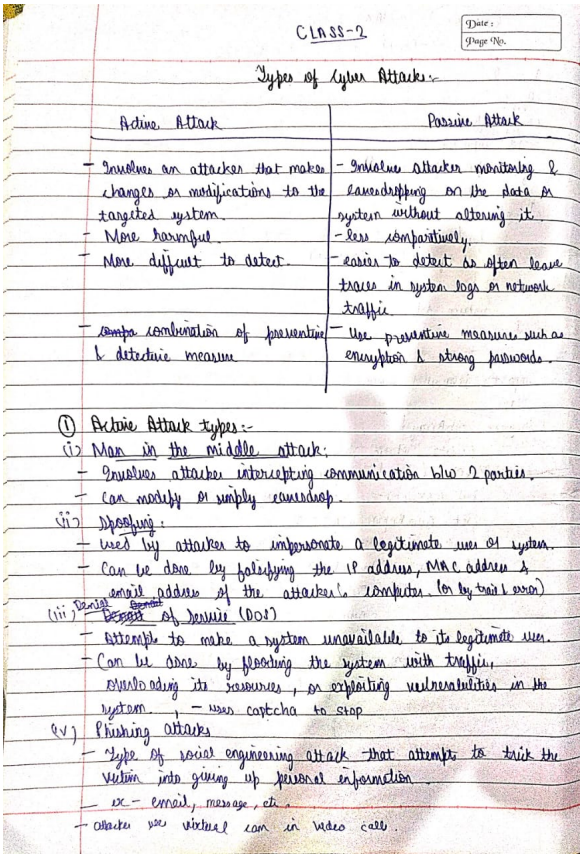
Class 2 - 23/08/2023

Today we learnt about types of attacks, the categories of hackers, the various basic terminologies in cyber security and the phases of hacking:

Here are the screenshots from my short notes from the class:



CLASS-2

Types of Cyber Attacks:-

Active Attack	Passive Attack
- Involves an attacker that makes changes or modifications to the targeted system. - More harmful. - More difficult to detect. - Requires combination of preventive & detective measures	- Involves attacker monitoring & eavesdropping on the data in system without altering it. - less comparatively. - easier to detect as often leave traces in system logs or network traffic. - Use preventive measures such as encryption & strong passwords.

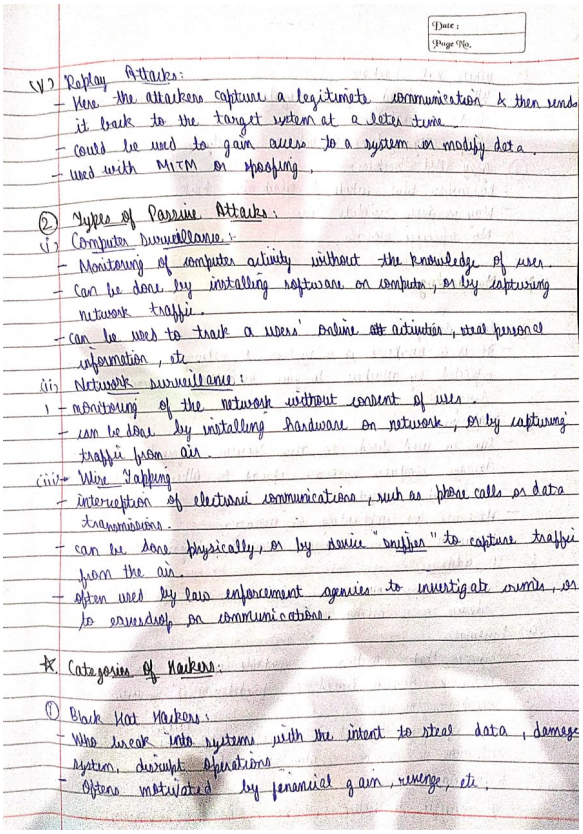
① Active Attack types:-

(i) Man in the middle attack:
- Involves attacker intercepting communication b/w 2 parties.
- Can modify or simply eavesdrop.

(ii) Spoofing:
- Used by attacker to impersonate a legitimate user or system.
- Can be done by falsifying the IP address, MAC address & email address of the attacker's computer. (or by trial & error)

(iii) Denial of Service (DOS)
- Attempts to make a system unavailable to its legitimate user.
- Can be done by flooding the system with traffic, overloading its resources, or exploiting vulnerabilities in the system. - uses captcha to stop

(iv) Phishing attacks
- Type of social engineering attack that attempts to trick the victim into giving up personal information.
- ex - email, message, etc.
- attacker use virtual cam in video call.



(v) Replay Attacks:
- Here the attackers captures a legitimate communication & then sends it back to the target system at a later time.
- could be used to gain access to a system or modify data.
- used with MITM or spoofing.

② Types of Passive Attacks:

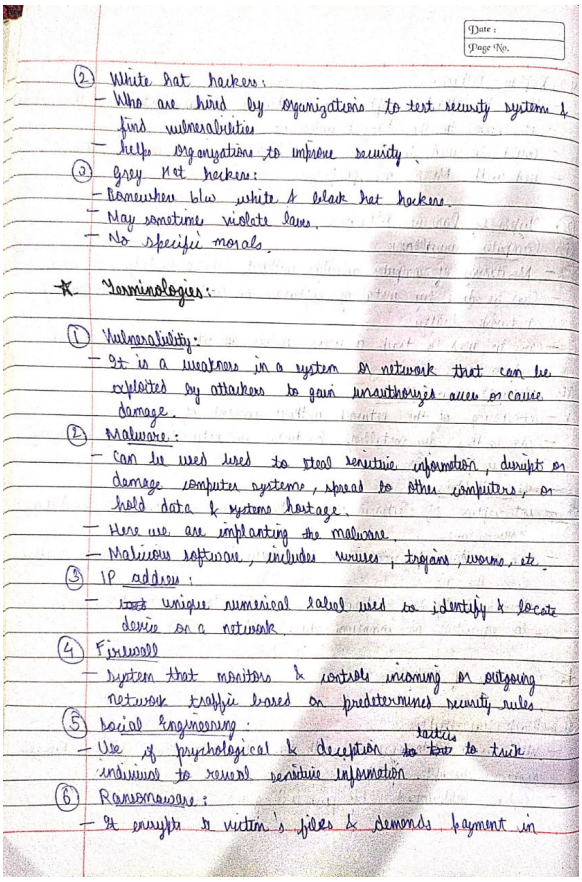
(i) Computer Surveillance:-
- Monitoring of computer activity without the knowledge of user.
- Can be done by installing software on computer, or by capturing network traffic.
- can be used to track a users' online activities, steal personal information, etc.

(ii) Network surveillance:
- monitoring of the network without consent of user.
- can be done by installing hardware on network, or by capturing traffic from air.

(iii) Wire Tapping
- interception of electronic communications, such as phone calls or data transmissions.
- can be done physically, or by device "sniffer" to capture traffic from the air.
- often used by law enforcement agencies to investigate crimes, or to eavesdrop on communications.

★ Categories of Hackers:

① Black Hat Hackers:
- Who break into systems with the intent to steal data, damage system, disrupt operations.
- Often motivated by financial gain, revenge, etc.



② White hat hackers:
- Who are hired by organizations to test security systems & find vulnerabilities
- Help organizations to improve security.

③ Grey Hat hackers:
- Somewhere blw white & black hat hackers.
- May sometimes violate laws.
- No specific morals.

★ Terminologies:

① Vulnerability:
- It is a weakness in a system or network that can be exploited by attackers to gain unauthorized access or cause damage.

② Malware:
- Can be used used to steal sensitive information, disrupt or damage computer systems, spread to other computers, or hold data & systems hostage.
- Here we are implanting the malware.
- Malicious software, includes viruses, trojans, worms, etc.

③ IP address:
- ~~not~~ unique numerical label used to identify & locate device on a network.

④ Firewall
- System that monitors & controls incoming or outgoing network traffic based on predetermined security rules.

⑤ Social Engineering:
- Use of psychological & deception tactics to trick to trick individual to reveal sensitive information

⑥ Ransomware:
- It encrypts a victim's files & demands payment in exchange for the decryption key.

⑦ Virtual Private Network (VPN)
- A secured encrypted connection blw a device & a remote servers that allows users to securely access the internet and protect their online activity & data from being monitored and intercepted.

⑧ Pen testing:
- To evaluate the security of the system & identify vulnerabilities that could be exploited by malicious actors.

⑨ Anti-Virus:
- software designed to detect, prevent, & remove malicious software.
- disadvantage: updates come 1 day late.

Task-2: Top 10 Most Notorious Hackers of all time
① Kevin Mitnik ② Anonymous
③ Adrian Lamo ④ Albert Gonzalez
⑤ Matthew Bevan & Richard Pryce
⑥ Jeanson James Ancheta
⑦ Michael Calce ⑧ Kevin Poulsen
⑨ Jonathon James ⑩ Ad TRA

★ Phases of Hacking:
① Reconnaissance: Gathering info. about target system. Can be gathered using various methods like social engineering.
② Scanning: Scanning the target for some vulnerabilities. Can be done using tools like port scanners.
③ Gaining Access: Attempts to gain access of the target system. Can be done using malwares, etc.
④ Maintaining Access: Maintain the access. Can be done by installing malwares, etc.
⑤ Clearing Tracks: Can be done by deleting logs, modifying files, etc.

Task 2: Top 10 notorious hackers in the world

1. **Kevin Mitnick:** Mitnick is a well-known hacker who was convicted of computer fraud and hacking into major telecommunications companies. He is considered to be a black hat hacker. After serving prison time, he transformed into a white hat hacker, contributing to cybersecurity awareness through consulting and speaking engagements.
2. **Anonymous:** Anonymous is a decentralized international hacktivist collective that is known for its cyberattacks against governments, corporations, and other organizations. Their actions have ranged from advocating for freedom of information to engaging in controversial cyberattacks. They are considered to be a gray hat hacker collective.

3. **Adrian Lamo:** Lamo was a hacker who was known for his work exposing security vulnerabilities in computer systems. Lamo's actions sparked ethical debates about responsible disclosure and the role of hackers in law enforcement. He was arrested in 2009 for hacking into The New York Times and other media organizations. He is considered to be a gray hat hacker.
4. **Albert Gonzalez:** Gonzalez is a hacker who was convicted of stealing credit card numbers from major retailers. His criminal activities led to one of the largest data breaches in history, highlighting the severity of financial cybercrime. He is considered to be a black hat hacker.
5. **Matthew Bevan and Richard Pryce:** Dubbed as "The U.K. Hackers," Bevan and Pryce were accused of hacking into U.S. military systems during the 1990s. Bevan and Pryce are hackers who were known for their work on the PhonePhreak community. They were arrested in 1994 for hacking into AT&T's network. They are considered to be gray hat hackers.
6. **Jeanson James Ancheta:** Ancheta is a hacker who was convicted of hacking into NASA's Jet Propulsion Laboratory. Ancheta created a botnet infecting thousands of computers worldwide, which he then used for various illegal activities, including ad fraud and distributed denial-of-service attacks, showcasing the potential for widespread cyber threats. He is considered to be a black hat hacker.
7. **Michael Calce:** Calce is a hacker who was known as "MafiaBoy". Calce gained notoriety for launching distributed denial-of-service attacks against major websites, including Yahoo! and Amazon, at the age of 15. He is considered to be a black hat hacker.
8. **Kevin Poulsen:** Poulsen is a hacker who was known for his work on Phrack magazine. He was arrested in 1991 for hacking into Pacific Bell's voicemail system. He is considered to be a gray hat hacker. After serving his sentence, he became a white hat hacker, journalist, and editor, advocating for responsible hacking practices.
9. **Jonathan James:** James was a hacker who was convicted of hacking into NASA and the Department of Defense. He committed suicide in 2008 while awaiting sentencing. He is considered to be a gray hat hacker.
10. **ASTRA:** ASTRA is a hacker collective that is known for its work on exposing security vulnerabilities in computer systems. They are considered to be a white hat

hacker collective.