REMA

29/08/25

Assignment - 1.

1) What is Malware ?

→ Malware is a short for 'Malicious Software' which refers to any software intentionally designed to cause damage to a Computer, Server or Network.

→ It can disrupt or damage devices, steal sensitive information, or even gain Unauthorized access to systems.

2) Explain the intent of Malware.

→

(1) Data theft :-

→ Stealing sensitive data or information like passwords or financial data.

(2) Disruption :-

→ Causing system downtime or performance issues.

(3) Espionage :-

→ Collecting intelligence or spying on user activity.

(4) Profit:-

→ Financial gains through activities like Ransom or Stealing Credentials for Unauthorized use.

3) What are the different types of Malware? Give a brief description of any three types.

→ Types of Malware:-

(1) Viruses. (3) Trojans
(2) Worms (4) Ransomware.
(5) Adware (6) Spyware.

(1) Viruses:-

→ These are self-replicating programs that attach themselves to clean files and spread to other files or systems.

(2) Worms:-

→ Worms Replicate themselves but Unlike viruses, they don't need to attach a file. They spread autonomously across Networks and can slow down or crash systems.

(3) Trojans:-

→ These are deceptive programs that appear as legitimate software but carry out harmful actions without the user's knowledge.

4) What is Ransomware and how does it typically infect a system?

→ Ransomware is a type of Malware that locks or encrypts the victim's files, making them inaccessible until a ransom is paid.

→ It typically infects a system through Malicious email attachments, phising links, or compromised software downloads.

→ Once the system is infected, the user is presented with a ransome note demanding payment in Exchange for decrypting the files or Restoring access.

5) Why is Reverse Engineering important in malware Analysis?

→ Reverse Engineering is crucial in malware analysis because it helps researchers understand how the malware operates, what vulnerabilities

it Exploits, and how to defend against it.

→ By analyzing the code and behaviours of Malware, Experts can develop better detection methods, create decryption tools for Malware ransomware, and design defenses to prevent future infections.

6) What are the General Steps involved in the reverse Engineering process?

→

(1) initial Analysis :-

→ Examine the malware's behaviours. (e.g., What files it creates, how it communicates or what systems changes it makes)

(2) static Analysis :-

→ Study the Malware's code without Executing it to understand its structure and identify potential threats.

(3) Dynamic Analysis :-

→ Run the Malware in a Controlled Environment (Sandbox) to observe its behaviour in Real time.

(4) Disassembly and decompilation:-

→ Break down the code into a human-readable format to understand its inner workings.

(5) Behavioral Analysis:-

→ Examine the effects of the Malware on a system to identify indicators of compromise.

7). Explain the interoperability in Reverse Engineering.

→ Interoperability in Reverse Engineering refers to the ability of different software tools, techniques, and platforms to work together during the analysis process.

→ For Example, Integrating disassemblers, debuggers, and Network monitoring tools to Examine the behaviour and code of Malware more effectively.

8). Under what legal Circumstances can Reverse Engineering be Conducted?

→ Reverse Engineering is generally subject to legal restrictions, particularly in cases involving proprietary software.

→ Under legal Circumstances :-

(1) Security Research :-

→ For the purpose of improving Software Security ~~Under test~~ and detecting Vulnerabilities.

(2) Interoperability :-

→ To Create Compatible Software or systems.

(3) Fair use :-

→ In Some Cases, If Reverse Engineering is done for Educational purposes or Under Specific licenses, it may be allowed.

9). How Can Reverse Engineering help address Compatibility issues?

→ Reverse Engineering Can help address Compatibility issues by allowing developers to understand how different Software or system works, Enabling them to Create solutions that allow disparate systems to Communicate or function together.

→ For Example, Reverse Engineering can be used to develope patches or workarounds when new hardware or Software needs to be Compatible with legacy systems.

→ Reverse Engineering provides a detailed Understanding of how legacy systems, hardware, or software work, enabling the development of Solutions to address Compatibility issues.

→ This process allow developers to bridge the gap between old and new technologies, adapt Software ~~tools~~ to works accross platforms, and overcome proprietary barriers.