Raj
DATE / /
PAGE

1. Explain different types of tool used by attacker?

Ans→ • Malware :- It is a term that describes malicious software, including spyware, ransomeware, viruses, & worms. Malware breaches a network through a vulnerability, typically when a user clicks a dangerous link or email attachment that then installs risky software.

• Denial of service attack :- A denial of service attack fills systems, servers, or networks with traffic that enhaust resources & band-width. That makes the system incapa-ble to fulfill legitimate requests. Attackers also use multiple compromised devices to launch this attack. This is known as a distri-buted-denial-of-service (DDoS) attack.

DATE / /
PAGE

- SQL Injection :- A SQL injection happens when an attacker inserts malicious code into a server that uses SQL & forces the server to reveal information it normally would not. An attacker could carry out a SQL injection simply by submitting malicious code into a vulnerable website search box.

- Zero-day exploit :- It hits after a network vulnerability is announced but before a patch or solution is implemented. Attackers target the disclosed vulnerability during this window of time. Zero day exploit vulnerability threat detection requires constant awarness.

- URL Interpretation :- It is a type of attack where we can change the certain part of a URL, & one can make a web server to deliver web pages for which he/she is

Raj
DATE / /
PAGE

not authorized to browse.

- Session hijacking:- It is a security attack on a user session over a protected network. Web applications create cookies to store the state & user sessions. By stealing the cookies, an attacker can have access to all of the user data.

- Phishing:- Phishing is a type of attack which attempts to steal sensitive information like user login credentials & credit card number. It occurs when an attacker is masquerading as a trustworthy entity in electronic communication.

And many more such as Brute force, DNS spoofing, Dictionary attack, file inclusion attacks, man-in-the-middle attacks etc.

Raj
DATE / /
PAGE

2. Explain different types of malware?

Ans→ • Ransomware:- Ransomware is a software that uses encryption to disable a target's access to its data until a random is paid. The victim organisation is rendered partially or totally unable to operate until it pays, but there is no guarantee that payment will result in necessary decryption key or that the decryption key provided will function properly.
Example:- RYUK.

• Fileless Malware:- It doesn't install anything initially, instead, it makes changes to files that are native to the operating system, such as Powershell or WMI. Because the OS recognises the edited files as legitimate, a fileless attack is not caught by antivirus software & because these attacks are stealthy, they are up to

Raj
DATE / /
PAGE

ten times more successful than tradition-al malware attacks.
Example :- Astaroth.

- Spyware :- Spyware collect information about users' activities without their knowledge or consent. This can include password pins, payment information & unstructured messages.
Example :- Dark Hotel.

- Trojan :- A trojan disguises itself as desirable code or software. Once download by unsuspecting users, trojan can take control of victims's system for malicious purposes. Trojans may hide in games, apps, or even software patches, or they may be embedded in attachments included in phishing emails.
Example :- Emotet.

- Keyloggers :- It is a type of Spyware that monitors user activity. Keyloggers

Raj
DATE / /
PAGE

have legitimate uses; businesses can use them to monitor employee activity & families may use them to keep track of children's online behaviors. Key loggers can be inserted into a system through phishing, Social engineering or malicious downloads

Example: olympic Vision.

And many more such Adware (fireball), worms (stuxnet), Rootkits (Zacinlo), Bots (Echobot), Mobile malware (Tsiada) etc.