Name: AMEY THAKUR COMP Class: TE Div: B Roll No: 50

Subject: CSS Topic: IAT-2 Date: Page No: 1

Q6 A)

ARP spoofing

- ARP spoofing is type of attack in which a malicious actor sends falsified ARP (Address Resolution Protocol) message over local area network. This results in linking of attackers MAC address with IP address of legitimate computer or server on the network.

- Once attackers MAC address is connected to an authentic IP address. The attacker begin receiving any data which is intended for that IP address. ARP spoofing can easily malicious parties to intercept, modify or even stop data in transit. ARP spoofing attack can only occur on local area network that utilize the address resolution protocol.

TU3F1819127

Amey

ASSTMAT

Name: AMEY THAKUR COMPS Class: TE Div: B Roll No: 50

Subject: CSS Topic: IAT-2 Date: Page No: 2

Q6 A)

b)

Port Scanning

- The act of systematically scanning computers port since a port is a place where information goes into and out of computer, port scanning identifies open doors to a computer.

- Port scanning has legitimate uses in managing network, but port scanning also can be malicious in nature if someone is looking for weakened access point to break into computer.

Types of port scans.

1. Vanilla - The scanner attends to connect to all 65535 ports.
2. Strobe - A more focused scan looking only for known services to exploit fragmented packets.
3. UDP - The scanner looks for open UDP ports
4. Sweep - The scanner connects to same port on more than one machine. FTP bounce

TU3F1819127

Amey

Q6 B)

Cross Site Scripting (XSS)

- Cross site scripting (XSS) is a web security vulnerability that allows an attacker to compromise the interaction that user have with vulnerable application.
- It allows attacker to circumvent the same origin policy, which is designed to segregate different website from each other.
- XSS vulnerabilities normally allows an attacker to masquerade as a victim user, to carry out an action that user is able to perform and to access any of users data.
- If the victim user has previlaged access within the application then attacker might be able to gain full control over all application functionality and data

Types of Cross site scripting

1. Reflected XSS
2. Stored XSS
3. DOM-based XSS

Amey

① Reflected XSS
- Where malicious script come from current HTTP request.

② Stored XSS
- Where the malicious script come from website's database.

③ DOM-based XSS
- Where the vulnerability exists in client side code rather than server side code.

Amey
ASHWIN

Q6 B.

Virus

- A virus is a fragment of code embedded in a legitimate program.
- Virus are self replicating and are designed to infect other programs.
- They can wreak havoc in a system by modifying or destroying files causing system crashes and program malfunction.
- On reaching the target machine a virus dropper (usually trojan horse) inserts the virus into a system

Types of Viruses

① File virus -
- This type of virus infects the system by appending itself to the end of file.
- It changes the start of program so that the control jumps to its code after the execution of its code the control return backs to main program

② Program virus
- It gets active when program containing these virus gets open (.bin, .exe) once it gets open it starts copying itself and infect other program

~~Ans~~

(3) Multi partite virus

- Its a combination of boot sector and program virus.
- It infects the program file when its active it affects boot sector.

(4) Stealth virus

- "Dubbed brain" the first computer virus was stealth virus
- It tries to disguise itself so that antivirus software may not able to recognize it.

(5) Polymorphic virus

- It keeps on changing its pattern or signature to get undetected.