finds confidential information leaked over the web. Jason says this happened about a month ago. Stephanie visits the said URLs, but she finds nothing. She is very concerned about this, since someone should be held accountable if there was sensitive information posted on the website. Where can Stephanie go to see past versions and pages of a website?

A. She should go to the web page Samspade.org to see web pages that might no longer be on the website.
B. If Stephanie navigates to Search.com; she will see old versions of the company website.
C. Stephanie can go to Archive.org to see past versions of the company website.
D. AddressPast.com would have any web pages that are no longer hosted on the company's website.

Correct Answer: C

QUESTION 23

Dan is conducting penetration testing and has found a vulnerability in a Web Application which gave him the sessionID token via a cross site scripting vulnerability. Dan wants to replay this token. However, the session ID manager (on the server) checks the originating IP address as well. Dan decides to spoof his IP address in order to replay the sessionID. Why do you think Dan might not be able to get an interactive session?

A. Dan cannot spoof his IP address over TCP network.
B. The scenario is incorrect as Dan can spoof his IP and get responses.
C. The server will send replies back to the spoofed IP address.
D. Dan can establish an interactive session only if he uses a NAT.

Correct Answer: C

QUESTION 24

Jason works in the sales and marketing department for a very large advertising agency located in Atlanta. Jason is working on a very important marketing campaign for his company's largest client. Before the project could be completed and implemented, a competing advertising company comes out with the exact same marketing materials and advertising, thus rendering all the work done for Jason's client unusable. Jason is questioned about this and says he has no idea how all the material ended up in the hands of a competitor. Without any proof, Jason's company cannot do anything except move on. After working on another high profile client for about a month, all the marketing and sales material again ends up in the hands of another competitor and is released to the public before Jason's company can finish the project. Once again, Jason says that he had nothing to do with it and does not know how this could have happened. Jason is given leave with pay until they can figure out what is going on. Jason's supervisor decides to go through his email and finds a number of emails that were sent to the competitors that ended up with the marketing material. The only items in the emails were attached jpg files, but nothing

else. Jason's supervisor opens the picture files, but cannot find anything out of the ordinary with them. What technique has Jason most likely used?

A. Stealth Rootkit Technique
B. ADS Streams Technique
C. Snow Hiding Technique
D. Image Steganography Technique

Correct Answer: D

QUESTION 25
What type of Virus is shown here?

A. Cavity Virus
B. Macro Virus
C. Boot Sector Virus
D. Metamorphic Virus
E. Sparse Infector Virus

Correct Answer: E

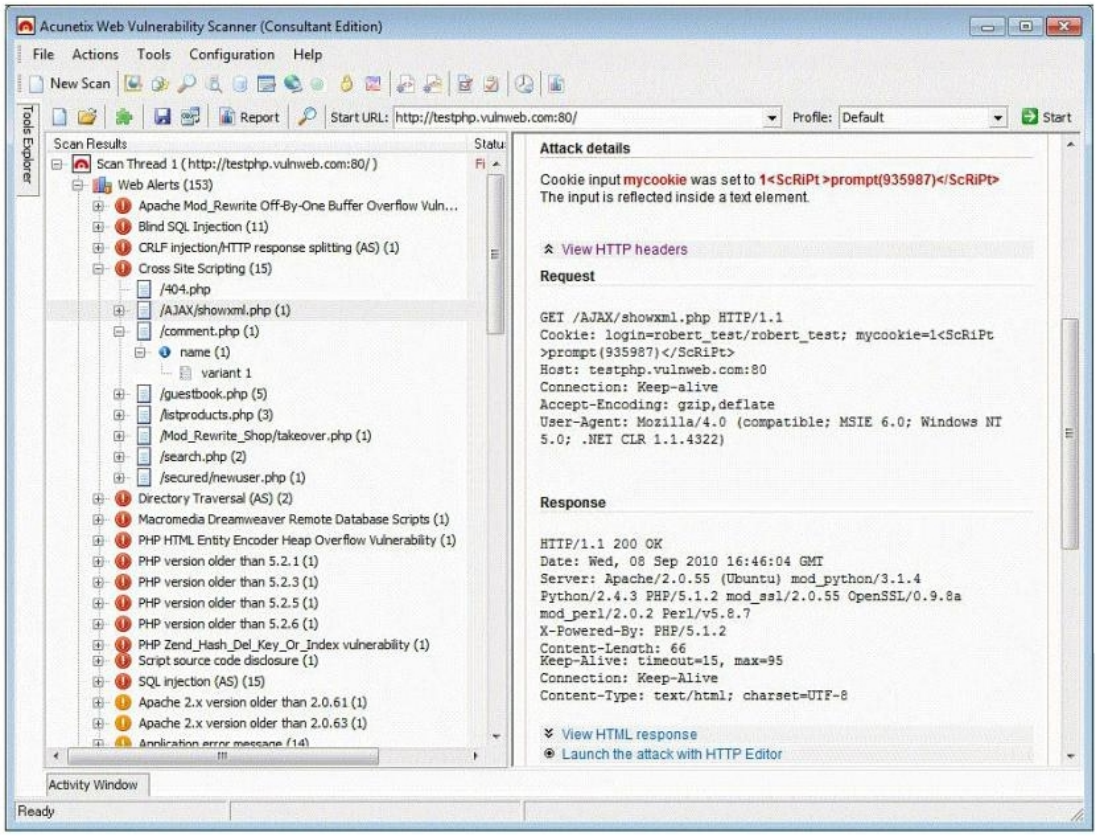
QUESTION 26
An attacker finds a web page for a target organization that supplies contact information for the company. Using available details to make the message seem authentic, the attacker drafts e-mail to an employee on the contact page that appears to come from an individual who might reasonably request confidential information, such as a network administrator. The email asks the employee to log into a bogus page that requests the employee's user name and password or click on a link that will download spyware or other malicious programming. Google's Gmail was hacked using this technique and attackers stole source code and sensitive data from Google servers. This is highly sophisticated attack using zero-day exploit vectors, social engineering and malware websites that focused on targeted individuals working for the company. What is this deadly attack called?

A. Spear phishing attack
B. Trojan server attack
C. Javelin attack
D. Social networking attack

Correct Answer: A

QUESTION 27

Vulnerability scanners are automated tools that are used to identify vulnerabilities and misconfigurations of hosts. They also provide information regarding mitigating discovered vulnerabilities.



Which of the following statements is incorrect?

A. Vulnerability scanners attempt to identify vulnerabilities in the hosts scanned.
B. Vulnerability scanners can help identify out-of-date software versions, missing patches, or system upgrades.
C. They can validate compliance with or deviations from the organization's security policy.
D. Vulnerability scanners can identify weakness and automatically fix and patch the vulnerabilities without user intervention.

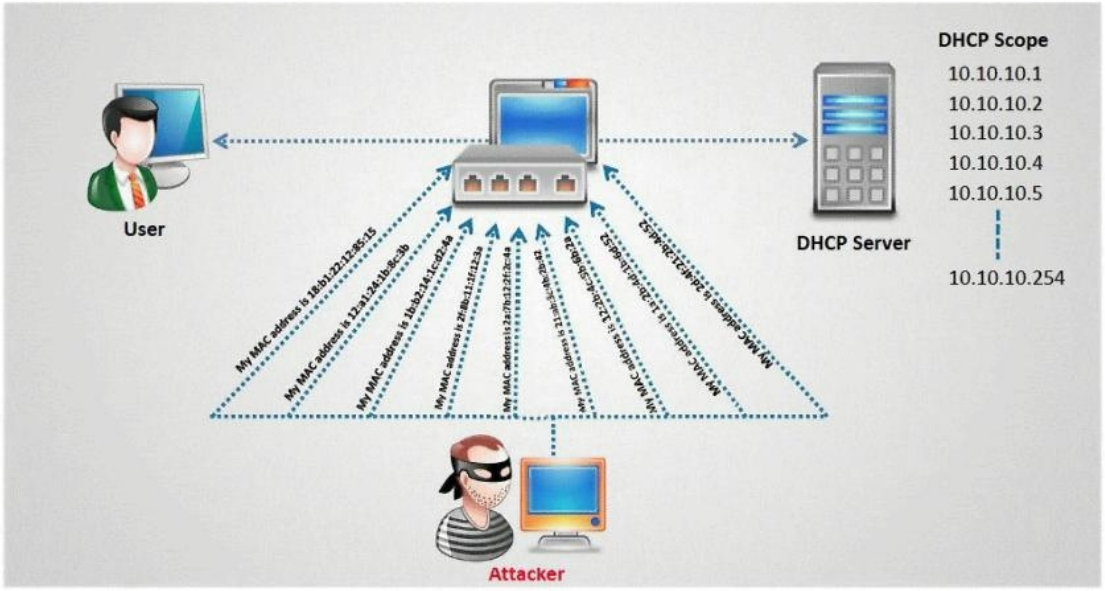
Correct Answer: D

QUESTION 28
How does traceroute map the route a packet travels from point A to point B?

A. Uses a TCP timestamp packet that will elicit a time exceeded in transit message.
B. Manipulates the value of the time to live (TTL) within packet to elicit a time exceeded in transit message.
C. Uses a protocol that will be rejected by gateways on its way to the destination.
D. Manipulates the flags within packets to force gateways into generating error messages.

Correct Answer: B

QUESTION 29
How do you defend against DHCP Starvation attack?

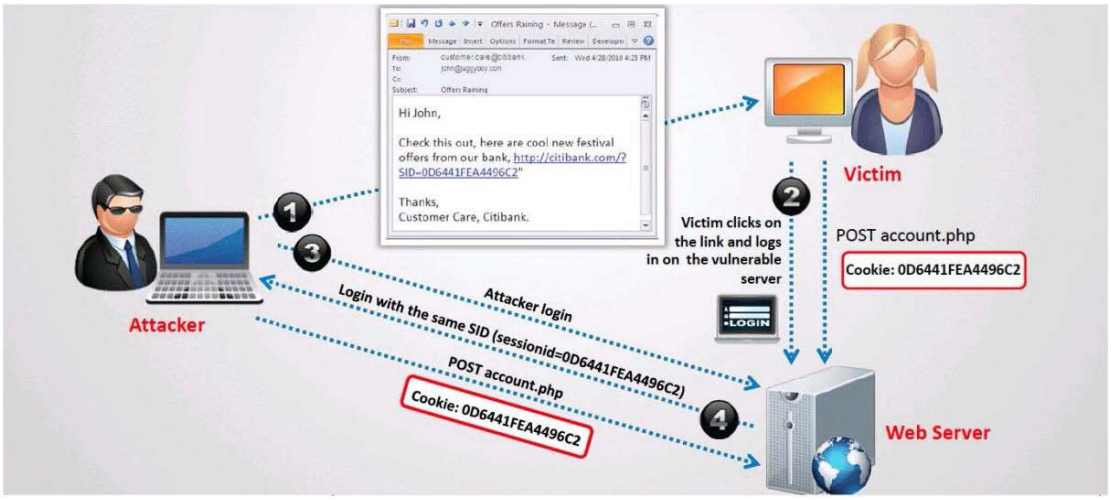


A. Enable ARP-Block on the switch.

B. Enable DHCP snooping on the switch.
C. Configure DHCP-BLOCK to 1 on the switch.
D. Install DHCP filters on the switch to block this attack.

Correct Answer: B

QUESTION 30
What type of session hijacking attack is shown in the exhibit?



A. Cross-site scripting Attack
B. SQL Injection Attack
C. Token sniffing Attack
D. Session Fixation Attack

Correct Answer: D

QUESTION 31
The SYN flood attack sends TCP connections requests faster than a machine can process them. Attacker creates a random source address for each packet SYN flag set in each packet is a request to open a new connection to the server from the spoofed IP address Victim responds to spoofed IP address, then waits for confirmation that never arrives (timeout wait is about 3 minutes) Victim's connection table fills up waiting for replies and ignores new connections Legitimate users are ignored and will not be able to access the server How do you protect your network against SYN Flood attacks?

A. SYN cookies. Instead of allocating a record, send a SYN-ACK with a carefully constructed sequence number generated as a hash of the clients IP address, port number, and other information. When the client responds with a normal ACK, that special sequence number will be included, which the server then verifies. Thus, the server first allocates memory on