QUESTION 213

Bank of Timbuktu is a medium-sized, regional financial institution in Timbuktu. The bank has deployed a new Internet-accessible Web application recently. Customers can access their account balances, transfer money between accounts, pay bills and conduct online financial business using a Web browser. John Stevens is in charge of information security at Bank of Timbuktu. After one month in production, several customers have complained about the Internet enabled banking application. Strangely, the account balances of many of the bank's customers had been changed. However, money hasn't been removed from the bank; instead, money was transferred between accounts. Given this attack profile, John Stevens reviewed the Web application's logs and found the following entries:

```
Attempted login of unknown user: johnm
Attempted login of unknown user: susaR
Attempted login of unknown user: sencat
Attempted login of unknown user: pete'';
Attempted login of unknown user: ' or 1=1--
Attempted login of unknown user: '; drop table logins--
Login of user jason, sessionID= 0x75627578626F6F6B
Login of user daniel, sessionID= 0x98627579539E13BE
Login of user rebecca, sessionID= 0x90627579944CCB811
Login of user mike, sessionID= 0x90627579935FB5C64
Transfer Funds user jason
Pay Bill user mike
Logout of user mike
```

What kind of attack did the Hacker attempt to carry out at the bank?

A. Brute force attack in which the Hacker attempted guessing login ID and password from password cracking tools.
B. The Hacker attempted Session hijacking, in which the Hacker opened an account with the bank, then logged in to receive a session ID, guessed the next ID and took over Jason's session.
C. The Hacker used a generator module to pass results to the Web server and exploited Web application CGI vulnerability.
D. The Hacker first attempted logins with suspected user names, then used SQL Injection to gain access to valid bank login IDs.

Correct Answer: D

QUESTION 214

WWW wanderers or spiders are programs that traverse many pages in the World Wide Web by recursively retrieving linked pages. Search engines like Google, frequently spider web pages for indexing. How will you stop web spiders from crawling certain directories on your website?

A. Place robots.txt file in the root of your website with listing of directories that you don't want

to be crawled.

B. Place authentication on root directories that will prevent crawling from these spiders.

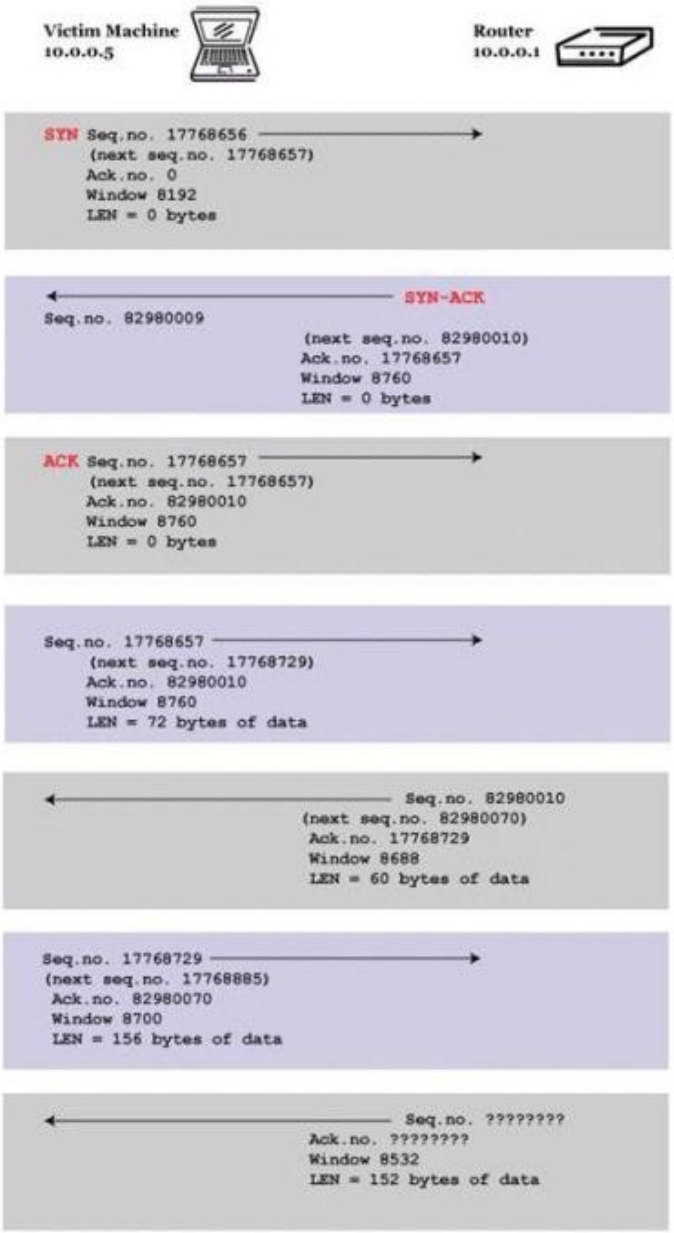
C. Enable SSL on the restricted directories which will block these spiders from crawling.

D. Place "HTTP:NO CRAWL" on the html pages that you don't want the crawlers to index.

Correct Answer: A

QUESTION 215

You are trying to hijack a telnet session from a victim machine with IP address 10.0.0.5 to Cisco router at 10.0.0.1. You sniff the traffic and attempt to predict the sequence and acknowledgement numbers to successfully hijack the telnet session. Here is the captured data in tcpdump.



What are the next sequence and acknowledgement numbers that the router will send to the victim machine?

A. Sequence number: 82980070 Acknowledgement number: 17768885A.
B. Sequence number: 17768729 Acknowledgement number: 82980070B.
C. Sequence number: 87000070 Acknowledgement number: 85320085C.
D. Sequence number: 82980010 Acknowledgement number: 17768885D.

Correct Answer: A

QUESTION 216

Hayden is the network security administrator for her company, a large finance firm based in

Miami. Hayden just returned from a security conference in Las Vegas where they talked about all kinds of old and new security threats; many of which she did not know of. Hayden is worried about the current security state of her company's network so she decides to start scanning the network from an external IP address. To see how some of the hosts on her network react, she sends out SYN packets to an IP range. A number of IPs responds with a SYN/ACK response. Before the connection is established she sends RST packets to those hosts to stop the session. She does this to see how her intrusion detection system will log the traffic. What type of scan is Hayden attempting here?

A. Hayden is attempting to find live hosts on her company's network by using an XMAS scan.
B. She is utilizing a SYN scan to find live hosts that are listening on her network.
C. The type of scan, she is using is called a NULL scan.
D. Hayden is using a half-open scan to find live hosts on her network.

Correct Answer: D

QUESTION 217

Web servers are often the most targeted and attacked hosts on organizations' networks. Attackers may exploit software bugs in the Web server, underlying operating system, or active content to gain unauthorized access.

Identify the correct statement related to the above Web Server installation?

A. Lack of proper security policy, procedures and maintenance.
B. Bugs in server software, OS and web applications.
C. Installing the server with default settings.
D. Unpatched security flaws in the server software, OS and applications.

Correct Answer: C

QUESTION 218
If an attacker's computer sends an IPID of 24333 to a zombie (Idle Scanning) computer on a closed port, what will be the response?

A. The zombie computer will respond with an IPID of 24334.
B. The zombie computer will respond with an IPID of 24333.
C. The zombie computer will not send a response.
D. The zombie computer will respond with an IPID of 24335.

Correct Answer: A
QUESTION 219
Jacob is looking through a traffic log that was captured using Wireshark. Jacob has come across what appears to be SYN requests to an internal computer from a spoofed IP address. What is Jacob seeing here?