312-50Q&As

Ethical Hacker Certified

Pass EC-COUNCIL 312-50 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.passapply.com/312-50.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by EC-COUNCIL Official Exam Center

QUESTION 1

Bank of Timbukut 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 Timbukut. 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= 0x9062757944CCB811
Login of user mike, sessionID= 0x90627679855B5C64
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 used a generator module to pass results to the Web Server and exploited Web Application CGI vulnerability.

C. The Hacker first attempted logins with suspected user names, then used SQL injection to gain access to valid login IDs

D. 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.

Correct Answer: C

Typing things like ` or 1=1 in the login field is evidence of a hacker trying out if the system is vulnerable to SQL injection.

QUESTION 2

This TCP flag instructs the sending system to transmit all buffered data immediately.

A. SYN

B. RST

C. PSH

D. URG

E. FIN

Correct Answer: C

QUESTION 3

Neil is closely monitoring his firewall rules and logs on a regular basis. Some of the users have complained to Neil that there are a few employees who are visiting offensive web site during work hours, without any consideration for others. Neil knows that he has an up-to-date content filtering system and such access should not be authorized. What type of technique might be used by these offenders to access the Internet without restriction?

A. They are using UDP that is always authorized at the firewall

B. They are using an older version of Internet Explorer that allow them to bypass the proxy server

C. They have been able to compromise the firewall, modify the rules, and give themselves proper access

D. They are using tunneling software that allows them to communicate with protocols in a way it was not intended

Correct Answer: D

This can be accomplished by, for example, tunneling the http traffic over SSH if you have a SSH server answering to your connection, you enable dynamic forwarding in the ssh client and configure Internet Explorer to use a SOCKS Proxy for network traffic.

QUESTION 4

If an attacker\\'s computer sends an IPID of 31400 to a zombie (Idle Scanning) computer on an open port, what will be the response?

A. 31400

B. 31402

C. The zombie will not send a response

D. 31401

Correct Answer: D

QUESTION 5

War dialing is one of the oldest methods of gaining unauthorized access to the target systems, it is one of the dangers most commonly forgotten by network engineers and system administrators. A hacker can sneak past all the expensive firewalls and IDS and connect easily into the network. Through wardialing an attacker searches for the devices located

in the target network infrastructure that are also accessible through the telephone line.

`Dial backup\\' in routers is most frequently found in networks where redundancy is required. Dial-on- demand routing(DDR) is commonly used to establish connectivity as a backup.

As a security testers, how would you discover what telephone numbers to dial-in to the router?

A. Search the Internet for leakage for target company\\'s telephone number to dial-in

B. Run a war-dialing tool with range of phone numbers and look for CONNECT Response

C. Connect using ISP\\'s remote-dial in number since the company\\'s router has a leased line connection established with them

D. Brute force the company\\'s PABX system to retrieve the range of telephone numbers to dial-in

Correct Answer: B

Use a program like Toneloc to scan the company\\'s range of phone numbers.