Vendor:CIW

Exam Code:1D0-571

Exam Name:CIW V5 Security Essentials

Version: Demo

QUESTION 1

Irina has contracted with a company to provide Web design consulting services. The company has asked her to use several large files available via an HTTP server. The IT department has provided Irina with user name and password, as well as the DNS name of the HTTP server. She then used this information to obtain the files she needs to complete her task using Mozilla Firefox. Which of the following is a primary risk factor when authenticating with a standard HTTP server?

A. HTTP usescleartext transmission during authentication, which can lead to a man-in-the- middle attack.

B. Irina has used the wrong application for this protocol, thus increasing the likelihood of a man-in- the-middle attack.

C. A standard HTTP connection uses public-key encryption that is not sufficiently strong, inviting the possibility of a man-in-the-middle attack.

D. Irina has accessed the Web server using a non-standard Web browser.

Correct Answer: A

QUESTION 2

Which choice lists typical firewall functions?

A. Creating a VLAN and configuring the intrusion-detection system

B. Issuing alerts and limiting host access

C. Logging traffic and creating a choke point

D. Implementing the security policy and scanning the internal network

Correct Answer: C

QUESTION 3

You purchased a network scanner six months ago. In spite of regularly conducting scans using this software, you have noticed that attackers have been able to compromise your servers over the last month. Which of the following is the most likely explanation for this problem?

A. The network scanner needs to be replaced.

B. The network scanner is no substitute for scans conducted by an individual.

C. The network scanner has atrojan.

D. The network scanner needs an update.

Correct Answer: D

QUESTION 4

You want to create a certificate for use in a Secure Sockets Layer (SSL) session. Which of the following is responsible for verifying the identity of an individual and also issuing the certificate?

A. Kerberos server

B. Certificate authority

C. Certificate revocation entity

D. Certificate repository

Correct Answer: B

QUESTION 5

A security breach has occurred involving the company e-commerce server. Customer credit card data has been released to unauthorized third parties. Which of the following lists the appropriate parties to inform?

A. Shareholders, law enforcement agencies and company employees

B. Affected customers, credit card companies and law enforcement agencies

C. The Internet Service Provider, ICANN and company shareholders

D. External securityconsultants, company board members and affected customers
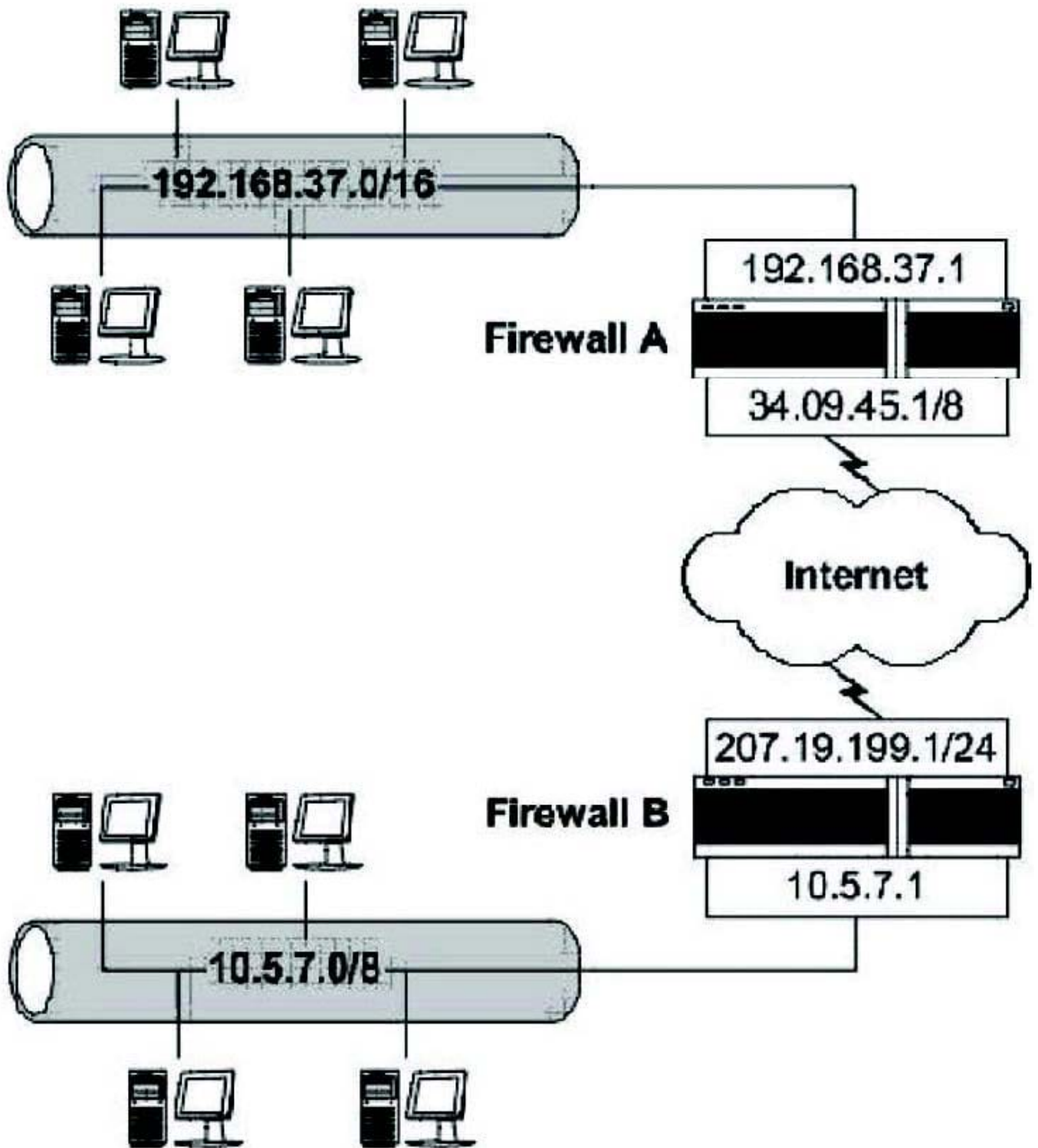
Correct Answer: B

QUESTION 6

The best way to thwart a dictionary attack is by enforcing a:

A. strong password policy.

B. restricted access policy.

C. firewall configuration policy.

D. proxy server policy.

Correct Answer: A

QUESTION 7

Consider the following diagram involving two firewall-protected networks: Which of the following is necessary for each of the firewalls to allow private IP addresses to be passed on to the Internet?

A. Chargeback

B. Stateful multi-layer inspection

C. Masquerading

D. DMZ creation

Correct Answer: C

QUESTION 8

Which tool is best suited for identifying applications and code on a Web server that can lead to a SQL injection attack?

A. A vulnerability scanner

B. A packet sniffer

C. An intrusion-detection system

D. A network switch

Correct Answer: A

QUESTION 9

You have just deployed an application that uses hash-based checksums to monitor changes in the configuration scripts of a database server that is accessible via the Internet. Which of the following is a primary concern for this solution?

A. The extra hard disk space required to store the database of checksums

B. The amount of memory remaining now that the checksum-based application is running

C. The possibility of a bufferoverflow attack leading to a security breach

D. The security of the checksum database on a read-only media format

Correct Answer: D

QUESTION 10

Which of the following describes the practice of stateful multi-layer inspection?

A. Using a VLAN on a firewall to enable masquerading of private IP addresses

B. Prioritizing voice and video data to reduce congestion

C. Inspecting packets in all layers of the OSI/RM with a packet filter

D. Using Quality of Service (QoS) on a proxy-oriented firewall

Correct Answer: C

QUESTION 11

Consider the following image: From the information in this image, what type of attack is occurring?

```
james@jamey: ~                                            _ □ ✕

File  Edit  View  Terminal  Tabs  Help
james@jamey:~$ sudo john /etc/shadow
[sudo] password for james:
Created directory: /root/.john
Loaded 1 password hash (FreeBSD MD5 [32/32])
guesses: 0  time: 0:00:00:13 60% (2)  c/s: 6120  trying: Valerie3
guesses: 0  time: 0:00:00:14 64% (2)  c/s: 6132  trying: Bootsie5
guesses: 0  time: 0:00:00:18 80% (2)  c/s: 6151  trying: 7faust
guesses: 0  time: 0:00:00:19 84% (2)  c/s: 6159  trying: 5benoit
guesses: 0  time: 0:00:00:20 88% (2)  c/s: 6163  trying: Marlboros
guesses: 0  time: 0:00:00:22 96% (2)  c/s: 6163  trying: Lasering
guesses: 0  time: 0:00:00:23 (3)  c/s: 6114  trying: machons
guesses: 0  time: 0:00:00:24 (3)  c/s: 6108  trying: 49072007
guesses: 0  time: 0:00:00:25 (3)  c/s: 6103  trying: motin
guesses: 0  time: 0:00:00:26 (3)  c/s: 6106  trying: abent1
guesses: 0  time: 0:00:00:27 (3)  c/s: 6108  trying: sunkal
guesses: 0  time: 0:00:00:33 (3)  c/s: 6122  trying: molasa
guesses: 0  time: 0:00:00:34 (3)  c/s: 6118  trying: binams
guesses: 0  time: 0:00:00:35 (3)  c/s: 6117  trying: seacal
guesses: 0  time: 0:00:00:39 (3)  c/s: 6130  trying: suphiele
guesses: 0  time: 0:00:00:40 (3)  c/s: 6130  trying: croutier
guesses: 0  time: 0:00:00:43 (3)  c/s: 6147  trying: 46633313
guesses: 0  time: 0:00:00:44 (3)  c/s: 6154  trying: stumbown
guesses: 0  time: 0:00:00:45 (3)  c/s: 6159  trying: mr137
```

A. A man-in-the-middle attack

B. A brute-force attack

C. A connection-hijacking attack

D. A spoofingattackD.A spoofing attack

Correct Answer: B

QUESTION 12

A security breach has occurred in which a third party was able to obtain and misuse legitimate authentication information. After investigation, you determined that the specific cause for the breach was that end users have been placing their passwords underneath their keyboards. Which step will best help you resolve this problem?

A. Discipline specific end users as object lessons to the rest of the staff and reset passwords on all systems immediately.

B. Change all passwords on the company servers immediately and inform end users that their passwords will be changing on a regular basis.

C. Set passwords to expire at specific intervals and establish mandatory continual training sessions.

D. Inform end users that their passwords will be changing on a regular basis and require more complex passwords.

Correct Answer: C