EC0-479 – EC-Council Certified Security Analyst (ECSA)

http://www.Pass-Guaranteed.com

QUESTION: 1

After passively scanning the network of Department of Defense (DoD), you switch over to active scanning to identify live hosts on their network. DoD is a lage organization and should respond to any number of scans. You start an ICMP ping sweep by sending an IP packet to the broadcast address. Only five hosts responds to your ICMP pings; definitely not the number of hosts you were expecting.

Why did this ping sweep only produce a few responses?

A. Only IBM AS/400 will reply to this scan
B. Only Windows systems will reply to this scan
C. A switched network will not respond to packets sent to the broadcast address
D. Only Unix and Unix-like systems will reply to this scan

Answer: D

QUESTION: 2

You are carrying out the last round of testing for your new website before it goes live. The website has many dynamic pages and connects to a SQL backend that accesses your product inventory in a database. You come across a web security site that recommends inputting the following code into a search field on web pages to check for vulnerabilities:

<script>alert("This is a test.")</script>

When you type this and click on search, you receive a pop-up window that says:

"This is a test."

What is the result of this test?

A. Your website is vulnerable to CSS
B. Your website is not vulnerable
C. Your website is vulnerable to SQL injection
D. Your website is vulnerable to web bugs

Answer: A

QUESTION: 3

Meyer Electronics Systems just recently had a number of laptops stolen out of their office. On these laptops contained sensitive corporate information regarding patents and company strategies. A month after the laptops were stolen, a competing company was found to have just developed products that almost exactly duplicated products that Meyer produces.

What could have prevented this information from being stolen from the laptops?

A. EFS Encryption
B. DFS Encryption
C. IPS Encryption
D. SDW Encryption

Answer: A

QUESTION: 4

You are the network administrator for a small bank in Dallas, Texas. To ensure network security, you enact a security policy that requires all users to have 14 character passwords. After giving your users 2 weeks notice, you change the Group Policy to force 14 character passwords. A week later you dump the SAM database from the standalone server and run a password-cracking tool against it. Over 99% of the passwords are broken within an hour.

Why were these passwords cracked so quickly?

A. Passwords of 14 characters or less are broken up into two 7-character hashes
B. A password Group Policy change takes at least 3 weeks to completely replicate throughout a network
C. Networks using Active Directory never use SAM databases so the SAM database pulled was empty
D. The passwords that were cracked are local accounts on the Domain Controller
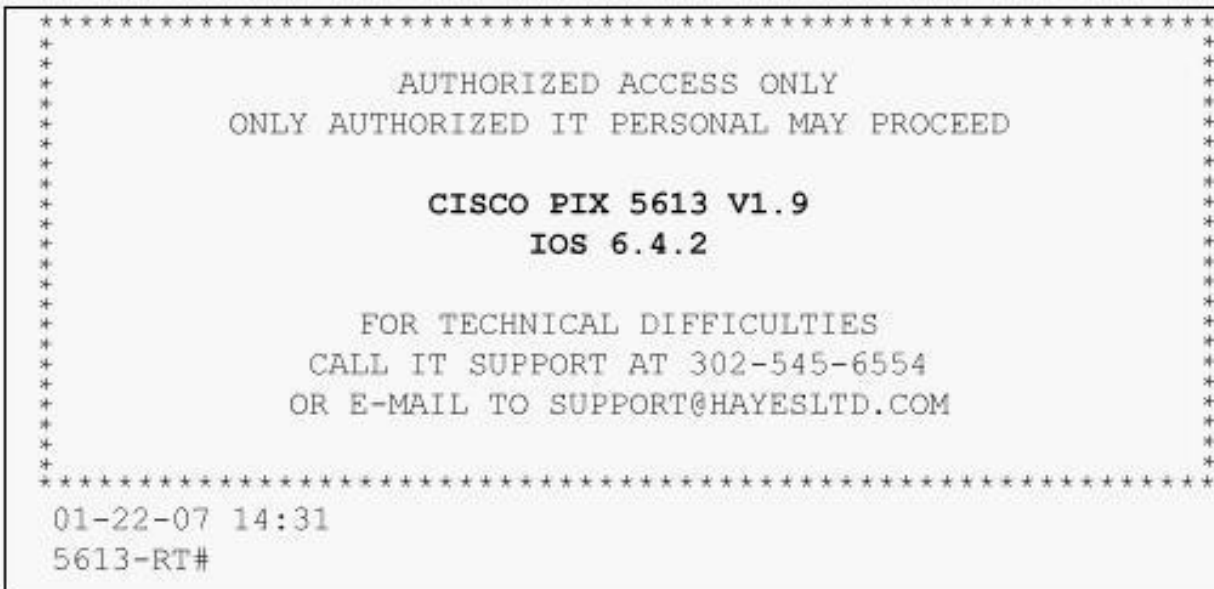
Answer: A

QUESTION: 5

Click on the Exhibit Button

Paulette works for an IT security consulting company that is currently performing an audit for the firm ACE Unlimited. Paulette's duties include logging on to all the company's network equipment to ensure IOS versions are up-to-date and all the other security settings are as stringent as possible. Paulette presents the following screenshot to her boss so he can inform the client about necessary changes needs to be made.

From the screenshot, what changes should the client company make?


```
*****************************************************************
*                                                               *
*                  AUTHORIZED ACCESS ONLY                       *
*           ONLY AUTHORIZED IT PERSONAL MAY PROCEED             *
*                                                               *
*                  CISCO PIX 5613 V1.9                          *
*                      IOS 6.4.2                                *
*                                                               *
*                FOR TECHNICAL DIFFICULTIES                     *
*            CALL IT SUPPORT AT 302-545-6554                    *
*            OR E-MAIL TO SUPPORT@HAYESLTD.COM                  *
*                                                               *
*****************************************************************
01-22-07 14:31
5613-RT#
```

A. Remove any identifying numbers, names, or version information
B. The banner should have more detail on the version numbers for the network equipment
C. The banner should not state "only authorized IT personnel may proceed"
D. The banner should include the Cisco tech support contact information as well

Answer: A

100% Pass-Guaranteed or Your Money Back!!!