



Vendor: GAQM

Exam Code: CEH-001

Exam Name: Certified Ethical Hacker (CEH)

Version: DEMO

QUESTION 1

You run nmap port Scan on 10.0.0.5 and attempt to gain banner/server information from services running on ports 21, 110 and 123.

Here is the output of your scan results:

```
PORT      STATE      SERVICE      VERSION
21/tcp    open       ftp          vsftpd 2.0.7
110/tcp   open       pop3         Courier pop3d
123/tcp   closed     ntp

Device type: general purpose
Running: Linux 2.8.X

OS details: Linux 2.8.18, Linux 2.8.20 - 2.8.24
Uptime: 65.658 days (since Mon Jun 19 00:43:29 2011)
Network Distance: 0 hops
Service Info: OS: Unix
```

Which of the following nmap command did you run?

- A. nmap -A -sV -p21, 110, 123 10.0.0.5
- B. nmap -F -sV -p21, 110, 123 10.0.0.5
- C. nmap -O -sV -p21, 110, 123 10.0.0.5
- D. nmap -T -sV -p21, 110, 123 10.0.0.5

Answer: C

QUESTION 2

How do you defend against Privilege Escalation?

- A. Use encryption to protect sensitive data
- B. Restrict the interactive logon privileges
- C. Run services as unprivileged accounts
- D. Allow security settings of IE to zero or Low
- E. Run users and applications on the least privileges

Answer: ABCE

QUESTION 3

What does ICMP (type 11, code 0) denote?

- A. Source Quench
- B. Destination Unreachable
- C. Time Exceeded
- D. Unknown Type

Answer: C

QUESTION 4

You are the security administrator of Jaco Banking Systems located in Boston.

You are setting up e-banking website (<http://www.ejacobank.com>) authentication system. Instead of issuing banking customer with a single password, you give them a printed list of 100 unique passwords. Each time the customer needs to log into the e-banking system website, the customer enters the next password on the list. If someone sees them type the password using shoulder surfing, MiTM or keyloggers, then no damage is done because the password will not be accepted a second time. Once the list of 100 passwords is almost finished, the system automatically sends out a new password list by encrypted e-mail to the customer.

You are confident that this security implementation will protect the customer from password abuse.

Two months later, a group of hackers called "HackJihad" found a way to access the one-time password list issued to customers of Jacob Banking Systems. The hackers set up a fake website (<http://www.e-jacobank.com>) and used phishing attacks to direct ignorant customers to it. The fake website asked users for their e-banking username and password, and the next unused entry from their one-time password sheet. The hackers collected 200 customer's username/passwords this way. They transferred money from the customer's bank account to various offshore accounts. Your decision of password policy implementation has cost the bank with USD 925, 000 to hackers. You immediately shut down the e-banking website while figuring out the next best security solution

What effective security solution will you recommend in this case?

- A. Implement Biometrics based password authentication system.
Record the customers face image to the authentication database
- B. Configure your firewall to block logon attempts of more than three wrong tries
- C. Enable a complex password policy of 20 characters and ask the user to change the password immediately after they logon and do not store password histories
- D. Implement RSA SecureID based authentication system

Answer: D

QUESTION 5

More sophisticated IDSs look for common shellcode signatures. But even these systems can be bypassed, by using polymorphic shellcode. This is a technique common among virus writers - it basically hides the true nature of the shellcode in different disguises.

How does a polymorphic shellcode work?

- A. They encrypt the shellcode by XORing values over the shellcode, using loader code to decrypt the shellcode, and then executing the decrypted shellcode
- B. They convert the shellcode into Unicode, using loader to convert back to machine code then executing them
- C. They reverse the working instructions into opposite order by masking the IDS signatures
- D. They compress shellcode into normal instructions, uncompress the shellcode using loader code and then executing the shellcode

Answer: A

QUESTION 6

SYN Flood is a DOS attack in which an attacker deliberately violates the three-way handshake and opens a large number of half-open TCP connections. The signature of attack for SYN Flood contains:

- A. The source and destination address having the same value
- B. A large number of SYN packets appearing on a network without the corresponding reply packets

- C. The source and destination port numbers having the same value
- D. A large number of SYN packets appearing on a network with the corresponding reply packets

Answer: B

QUESTION 7

Which of the following type of scanning utilizes automated process of proactively identifying vulnerabilities of the computing systems present on a network?

- A. Port Scanning
- B. Single Scanning
- C. External Scanning
- D. Vulnerability Scanning

Answer: D

QUESTION 8

The following script shows a simple SQL injection. The script builds an SQL query by concatenating hard-coded strings together with a string entered by the user:

```
var ShipCity;  
ShipCity = Request.form ("ShipCity");  
var sql = "select * from OrdersTable where ShipCity = '" + ShipCity + "'";
```

The user is prompted to enter the name of a city on a Web form. If she enters Chicago, the query assembled by the script looks similar to the following:

```
SELECT * FROM OrdersTable WHERE ShipCity = 'Chicago'
```

How will you delete the OrdersTable from the database using SQL Injection?

- A. Chicago'; drop table OrdersTable --
- B. Delete table'blah'; OrdersTable --
- C. EXEC; SELECT * OrdersTable > DROP --
- D. cmdshell'; 'del c:\sql\mydb\OrdersTable' //

Answer: A

QUESTION 9

What are the limitations of Vulnerability scanners? (Select 2 answers)

- A. There are often better at detecting well-known vulnerabilities than more esoteric ones
- B. The scanning speed of their scanners are extremely high
- C. It is impossible for any, one scanning product to incorporate all known vulnerabilities in a timely manner
- D. The more vulnerabilities detected, the more tests required
- E. They are highly expensive and require per host scan license

Answer: AC

QUESTION 10

Stephanie works as senior security analyst for a manufacturing company in Detroit. Stephanie manages network security throughout the organization. Her colleague Jason told her in confidence that he was able to see confidential corporate information posted on the external website <http://www.jeansclothesman.com>. He tries random URLs on the company's website and 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 Samspace.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

Answer: C

QUESTION 11

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

Answer: C

QUESTION 12

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

Answer: D

QUESTION 13

What type of Virus is shown here?



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

Answer: E

QUESTION 14



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.

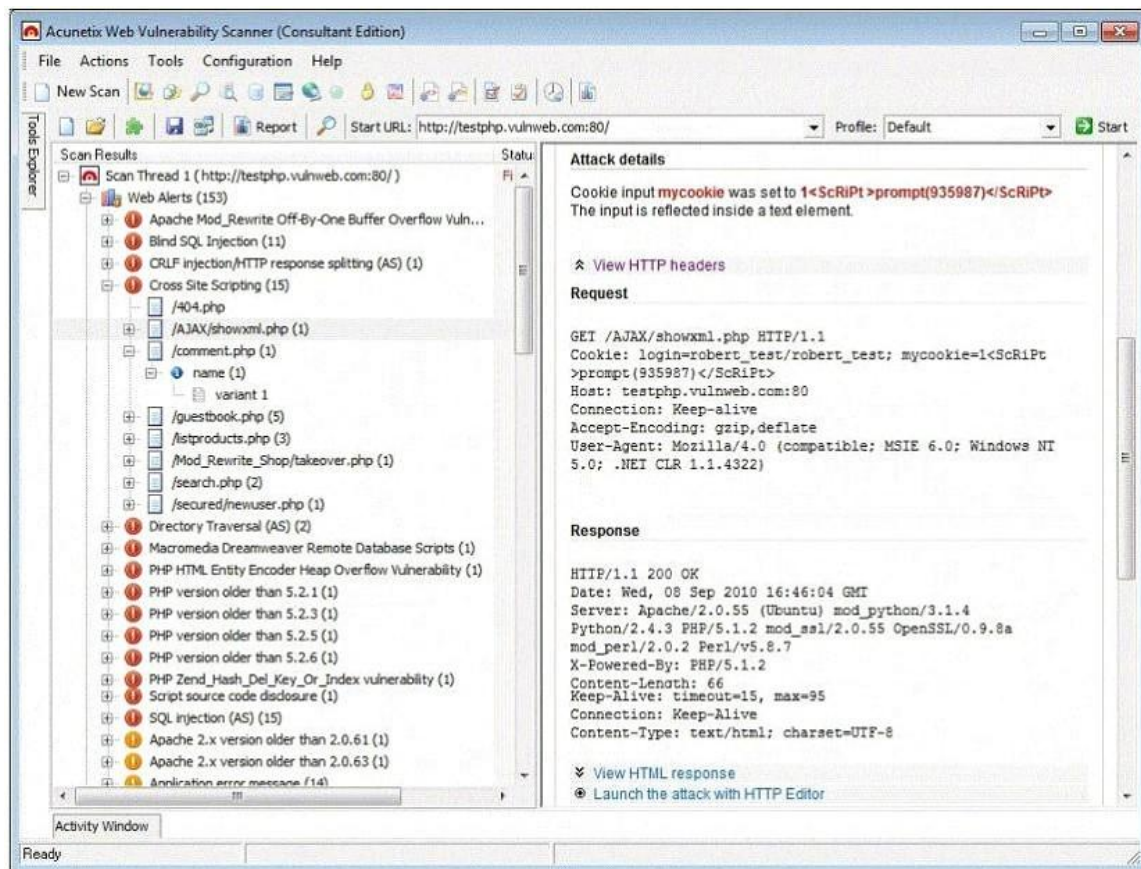
What is this deadly attack called?

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

Answer: A

QUESTION 15

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

Answer: D

Thank You for Trying Our Product

Braindump2go Certification Exam Features:

- ★ More than **99,900** Satisfied Customers Worldwide.
- ★ Average **99.9%** Success Rate.
- ★ **Free Update** to match latest and real exam scenarios.
- ★ **Instant Download** Access! No Setup required.
- ★ Questions & Answers are downloadable in **PDF** format and **VCE** test engine format.
- ★ Multi-Platform capabilities - **Windows, Laptop, Mac, Android, iPhone, iPod, iPad**.
- ★ **100%** Guaranteed Success or **100%** Money Back Guarantee.
- ★ **Fast**, helpful support **24x7**.



View list of all certification exams: <http://www.braindump2go.com/all-products.html>



10% Discount Coupon Code: BDN2014