CEH-001 Q&As

Certified Ethical Hacker (CEH)

Pass GAQM CEH-001 Exam with 100% Guarantee

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

https://www.certbus.com/ceh-001.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by GAQM Official Exam Center

QUESTION 1

Under what conditions does a secondary name server request a zone transfer from a primary name server?

A. When a primary SOA is higher that a secondary SOA

B. When a secondary SOA is higher that a primary SOA

C. When a primary name server has had its service restarted

D. When a secondary name server has had its service restarted

E. When the TTL falls to zero

Correct Answer: A

QUESTION 2

In order to attack a wireless network, you put up an access point and override the signal of the real access point. As users send authentication data, you are able to capture it. What kind of attack is this?

A. WEP attack

B. Drive by hacking

C. Rogue access point attack

D. Unauthorized access point attack

Correct Answer: C

QUESTION 3

Jack Hacker wants to break into Brown Co.\\'s computers and obtain their secret double fudge cookie recipe. Jack calls Jane, an accountant at Brown Co., pretending to be an administrator from Brown Co. Jack tells Jane that there has been a

problem with some accounts and asks her to verify her password with him \\'\\'just to double check our records.\\'\\' Jane does not suspect anything amiss, and parts with her password. Jack can now access Brown Co.\\'s computers with a valid user

name and password, to steal the cookie recipe.

What kind of attack is being illustrated here?

A. Reverse Psychology

B. Reverse Engineering

C. Social Engineering

D. Spoofing Identity

E. Faking Identity

Correct Answer: C

QUESTION 4

Erik notices a big increase in UDP packets sent to port 1026 and 1027 occasionally. He enters the following at the command prompt.

$ nc -l -p 1026 -u -v

In response, he sees the following message.

cell(?(c)????STOPALERT77STOP! WINDOWS REQUIRES IMMEDIATE ATTENTION.

Windows has found 47 Critical Errors.

To fix the errors please do the following:

1.

Download Registry Repair from: www.reg-patch.com

2.

Install Registry Repair

3.

Run Registry Repair

4.

Reboot your computer

FAILURE TO ACT NOW MAY LEAD TO DATA LOSS AND CORRUPTION!

What would you infer from this alert?

A. The machine is redirecting traffic to www.reg-patch.com using adware

B. It is a genuine fault of windows registry and the registry needs to be backed up

C. An attacker has compromised the machine and backdoored ports 1026 and 1027

D. It is a messenger spam. Windows creates a listener on one of the low dynamic ports from 1026 to 1029 and the message usually promotes malware disguised as legitimate utilities

Correct Answer: D

QUESTION 5

What are the differences between SSL and S-HTTP?

A. SSL operates at the network layer and S-HTTP operates at the application layer

B. SSL operates at the application layer and S-HTTP operates at the network layer

C. SSL operates at the transport layer and S-HTTP operates at the application layer

D. SSL operates at the application layer and S-HTTP operates at the transport layer

Correct Answer: C

QUESTION 6

E-mail scams and mail fraud are regulated by which of the following?

A. 18 U.S.C. par. 1030 Fraud and Related activity in connection with Computers

B. 18 U.S.C. par. 1029 Fraud and Related activity in connection with Access Devices

C. 18 U.S.C. par. 1362 Communication Lines, Stations, or Systems

D. 18 U.S.C. par. 2510 Wire and Electronic Communications Interception and Interception of Oral Communication

Correct Answer: A

QUESTION 7

You are attempting to map out the firewall policy for an organization. You discover your target system is one hop beyond the firewall. Using hping2, you send SYN packets with the exact TTL of the target system starting at port 1 and going up to port 1024. What is this process known as?

A. Footprinting

B. Firewalking

C. Enumeration

D. Idle scanning

Correct Answer: B

QUESTION 8

When utilizing technical assessment methods to assess the security posture of a network, which of the following techniques would be most effective in determining whether end-user security training would be beneficial?

A. Vulnerability scanning

B. Social engineering

C. Application security testing

D. Network sniffing

Correct Answer: B

QUESTION 9

Ursula is a college student at a University in Amsterdam. Ursula originally went to college to study engineering but later changed to marine biology after spending a month at sea with her friends. These friends frequently go out to sea to follow and harass fishing fleets that illegally fish in foreign waters. Ursula eventually wants to put companies practicing illegal fishing out of business. Ursula decides to hack into the parent company\\'s computers and destroy critical data knowing fully well that, if caught, she probably would be sent to jail for a very long time. What would Ursula be considered?

A. Ursula would be considered a gray hat since she is performing an act against illegal activities.

B. She would be considered a suicide hacker.

C. She would be called a cracker.

D. Ursula would be considered a black hat.

Correct Answer: B

QUESTION 10

Which of the following is used to indicate a single-line comment in structured query language (SQL)?

A. -

B. ||

C. %%

D. \\'\\'

Correct Answer: A

QUESTION 11

Which of the following lists are valid data-gathering activities associated with a risk assessment?

A. Threat identification, vulnerability identification, control analysis

B. Threat identification, response identification, mitigation identification

C. Attack profile, defense profile, loss profile

D. System profile, vulnerability identification, security determination

Correct Answer: A

QUESTION 12

Which of the following ensures that updates to policies, procedures, and configurations are made in a controlled and documented fashion?

A. Regulatory compliance

B. Peer review

C. Change management

D. Penetration testing

Correct Answer: C

QUESTION 13

How can you determine if an LM hash you extracted contains a password that is less than 8 characters long?

A. There is no way to tell because a hash cannot be reversed

B. The right most portion of the hash is always the same

C. The hash always starts with AB923D

D. The left most portion of the hash is always the same

E. A portion of the hash will be all 0\\'s

Correct Answer: B

QUESTION 14

To scan a host downstream from a security gateway, Firewalking:

A. Sends a UDP-based packet that it knows will be blocked by the firewall to determine how specifically the firewall responds to such packets

B. Uses the TTL function to send packets with a TTL value set to expire one hop past the identified security gateway

C. Sends an ICMP \\'\\'administratively prohibited\\'\\' packet to determine if the gateway will drop the packet without comment.

D. Assesses the security rules that relate to the target system before it sends packets to any hops on the route to the gateway

Correct Answer: B

QUESTION 15

Which of the statements concerning proxy firewalls is correct?

A. Proxy firewalls increase the speed and functionality of a network.

B. Firewall proxy servers decentralize all activity for an application.

C. Proxy firewalls block network packets from passing to and from a protected network.

D. Computers establish a connection with a proxy firewall which initiates a new network connection for the client.

Correct Answer: D

To Read the Whole Q&As, please purchase the Complete Version from Our website.

Try our product !

100% Guaranteed Success
100% Money Back Guarantee
365 Days Free Update
Instant Download After Purchase
24x7 Customer Support
Average 99.9% Success Rate
More than 800,000 Satisfied Customers Worldwide
Multi-Platform capabilities - Windows, Mac, Android, iPhone, iPod, iPad, Kindle

We provide exam PDF and VCE of Cisco, Microsoft, IBM, CompTIA, Oracle and other IT Certifications.
You can view Vendor list of All Certification Exams offered:

https://www.certbus.com/allproducts

Need Help

Please provide as much detail as possible so we can best assist you.
To update a previously submitted ticket: