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.pass4itsure.com/ceh-001.html

100% Passing Guarantee
100% Money Back Assurance

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

- **Instant Download** After Purchase
- **100% Money Back** Guarantee
- **365 Days** Free Update
- **800,000+** Satisfied Customers

QUESTION 1

What is the best defense against privilege escalation vulnerability?

A. Patch systems regularly and upgrade interactive login privileges at the system administrator level.

B. Run administrator and applications on least privileges and use a content registry for tracking.

C. Run services with least privileged accounts and implement multi-factor authentication and authorization.

D. Review user roles and administrator privileges for maximum utilization of automation services.

Correct Answer: C

QUESTION 2

Statistics from cert.org and other leading security organizations has clearly showed a steady rise in the number of hacking incidents perpetrated against companies.

What do you think is the main reason behind the significant increase in hacking attempts over the past years?

A. It is getting more challenging and harder to hack for non technical people.

B. There is a phenomenal increase in processing power.

C. New TCP/IP stack features are constantly being added.

D. The ease with which hacker tools are available on the Internet.

Correct Answer: D

QUESTION 3

You are performing a port scan with nmap. You are in hurry and conducting the scans at the fastest possible speed. However, you don\\'t want to sacrifice reliability for speed. If stealth is not an issue, what type of scan should you run to get very reliable results?

A. Stealth scan

B. Connect scan

C. Fragmented packet scan

D. XMAS scan

Correct Answer: B

QUESTION 4

What do you conclude from the nmap results below? Staring nmap V. 3.10ALPHA0 (www.insecure.org/map/) (The 1592 ports scanned but not shown below are in state: closed) Port State Service 21/tcp open ftp 25/tcp open smtp 80/tcp open http 443/tcp open https Remote operating system guess: Too many signatures match the reliability guess the OS. Nmap run completed ?1 IP address (1 host up) scanned in 91.66 seconds

A. The system is a Windows Domain Controller.

B. The system is not firewalled.

C. The system is not running Linux or Solaris.

D. The system is not properly patched.

Correct Answer: B

QUESTION 5

Samuel is the network administrator of DataX Communications, Inc. He is trying to configure his firewall to block password brute force attempts on his network. He enables blocking the intruder\\'s IP address for a period of 24 hours\\' time after more than three unsuccessful attempts. He is confident that this rule will secure his network from hackers on the Internet.

But he still receives hundreds of thousands brute-force attempts generated from various IP addresses around the world. After some investigation he realizes that the intruders are using a proxy somewhere else on the Internet which has been scripted to enable the random usage of various proxies on each request so as not to get caught by the firewall rule.

Later he adds another rule to his firewall and enables small sleep on the password attempt so that if the password is incorrect, it would take 45 seconds to return to the user to begin another attempt. Since an intruder may use multiple machines to brute force the password, he also throttles the number of connections that will be prepared to accept from a particular IP address. This action will slow the intruder\\'s attempts.

Samuel wants to completely block hackers brute force attempts on his network. What are the alternatives to defending against possible brute-force password attacks on his site?

A. Enforce a password policy and use account lockouts after three wrong logon attempts even though this might lock out legit users

B. Enable the IDS to monitor the intrusion attempts and alert you by e-mail about the IP address of the intruder so that you can block them at the Firewall manually

C. Enforce complex password policy on your network so that passwords are more difficult to brute force

D. You cannot completely block the intruders attempt if they constantly switch proxies

Correct Answer: D

QUESTION 6

Bob is acknowledged as a hacker of repute and is popular among visitors of "underground" sites. Bob is willing to share his knowledge with those who are willing to learn, and many have expressed their interest in learning from him. However, this knowledge has a risk associated with it, as it can be used for malevolent attacks as well.

In this context, what would be the most affective method to bridge the knowledge gap between the "black" hats or

crackers and the "white" hats or computer security professionals? (Choose the test answer)

A. Educate everyone with books, articles and training on risk analysis, vulnerabilities and safeguards.

B. Hire more computer security monitoring personnel to monitor computer systems and networks.

C. Make obtaining either a computer security certification or accreditation easier to achieve so more individuals feel that they are a part of something larger than life.

D. Train more National Guard and reservist in the art of computer security to help out in times of emergency or crises.

Correct Answer: A

QUESTION 7

While performing ping scans into a target network you get a frantic call from the organization\\'s security team. They report that they are under a denial of service attack. When you stop your scan, the smurf attack event stops showing up on the organization\\'s IDS monitor. How can you modify your scan to prevent triggering this event in the IDS?

A. Scan more slowly.

B. Do not scan the broadcast IP.

C. Spoof the source IP address.

D. Only scan the Windows systems.

Correct Answer: B

QUESTION 8

Tess King is using the nslookup command to craft queries to list all DNS information (such as Name Servers, host names, MX records, CNAME records, glue records (delegation for child Domains), zone serial number, TimeToLive (TTL) records, etc) for a Domain. What do you think Tess King is trying to accomplish? Select the best answer.

A. A zone harvesting

B. A zone transfer

C. A zone update

D. A zone estimate

Correct Answer: B

QUESTION 9

What does the following command in netcat do?

nc -l -u -p55555

A. logs the incoming connections to /etc/passwd file

B. loads the /etc/passwd file to the UDP port 55555

C. grabs the /etc/passwd file when connected to UDP port 55555

D. deletes the /etc/passwd file when connected to the UDP port 55555

Correct Answer: C

QUESTION 10

Rebecca is a security analyst and knows of a local root exploit that has the ability to enable local users to use available exploits to gain root privileges. This vulnerability exploits a condition in the Linux kernel within the execve() system call. There is no known workaround that exists for this vulnerability. What is the correct action to be taken by Rebecca in this situation as a recommendation to management?

A. Rebecca should make a recommendation to disable the () system call

B. Rebecca should make a recommendation to upgrade the Linux kernel promptly

C. Rebecca should make a recommendation to set all child-process to sleep within the execve()

D. Rebecca should make a recommendation to hire more system administrators to monitor all child processes to ensure that each child process can\\'t elevate privilege

Correct Answer: B

QUESTION 11

Which of the following is optimized for confidential communications, such as bidirectional voice and video?

A. RC4

B. RC5

C. MD4

D. MD5

Correct Answer: A

QUESTION 12

In which of the following should be performed first in any penetration test?

A. System identification

B. Intrusion Detection System testing

C. Passive information gathering

D. Firewall testing

Correct Answer: C

QUESTION 13

What are the default passwords used by SNMP? (Choose two.)

A. Password

B. SA

C. Private

D. Administrator

E. Public

F. Blank

Correct Answer: CE

QUESTION 14

How do you defend against ARP Spoofing? Select three.

A. Use ARPWALL system and block ARP spoofing attacks

B. Tune IDS Sensors to look for large amount of ARP traffic on local subnets

C. Use private VLANS

D. Place static ARP entries on servers, workstation and routers

Correct Answer: ACD

QUESTION 15

One of your team members has asked you to analyze the following SOA record. What is the version? Rutgers.edu.SOA NS1.Rutgers.edu ipad.college.edu (200302028 3600 3600 604800 2400.

A. 200303028

B. 3600

C. 604800

D. 2400

E. 60

F. 4800

Correct Answer: A