DUMPSWHEEL

https://www.dumpswheel.com

Dumpswheel - IT Certification Company provides Braindumps pdf!

Exam : **312-50v10**

Title : Certified Ethical Hacker Exam (CEH v 10)

Vendor : EC-COUNCIL

Version : DEMO

NO.1 Which of the following is a wireless network detector that is commonly found on Linux?

A. Kismet

B. Abel

C. Netstumbler

D. Nessus

Answer: A

NO.2 A security consultant decides to use multiple layers of anti-virus defense, such as end user desktop anti-virus and E-mail gateway. This approach can be used to mitigate which kind of attack?

A. Forensic attack

B. ARP spoofing attack

C. Social engineering attack

D. Scanning attack

Answer: C

NO.3 Code injection is a form of attack in which a malicious user:

A. Inserts text into a data field that gets interpreted as code

B. Gets the server to execute arbitrary code using a buffer overflow

C. Inserts additional code into the JavaScript running in the browser

D. Gains access to the codebase on the server and inserts new code

Answer: A

NO.4 Sid is a judge for a programming contest. Before the code reaches him it goes through a restricted OS and is tested there. If it passes, then it moves onto Sid. What is this middle step called? **A.** Fuzzy-testing the code

B. Third party running the code

C. Sandboxing the code

D. String validating the code

Answer: A

NO.5 The Payment Card Industry Data Security Standard (PCI DSS) contains six different categories of control objectives. Each objective contains one or more requirements, which must be followed in order to achieve compliance. Which of the following requirements would best fit under the objective, "Implement strong access control measures"?

A. Regularly test security systems and processes.

B. Encrypt transmission of cardholder data across open, public networks.

C. Assign a unique ID to each person with computer access.

D. Use and regularly update anti-virus software on all systems commonly affected by malware.

Answer: C

NO.6 Which of the following act requires employer's standard national numbers to identify them on standard transactions?

A. SOX

B. HIPAA

C. DMCA

D. PCI-DSS

Answer: B

NO.7 Which of the following is an NMAP script that could help detect HTTP Methods such as GET, POST, HEAD, PUT, DELETE, TRACE?

A. http-git

B. http-headers

C. http enum

D. http-methods

Answer: D

NO.8 Fred is the network administrator for his company. Fred is testing an internal switch.
From an external IP address, Fred wants to try and trick this switch into thinking it already has established a session with his computer. How can Fred accomplish this?

A. Fred can accomplish this by sending an IP packet with the RST/SIN bit and the source address of his computer.

B. He can send an IP packet with the SYN bit and the source address of his computer.

C. Fred can send an IP packet with the ACK bit set to zero and the source address of the switch.

D. Fred can send an IP packet to the switch with the ACK bit and the source address of his machine.

Answer: D

NO.9 What is the process of logging, recording, and resolving events that take place in an organization?

A. Incident Management Process

B. Security Policy

C. Internal Procedure

D. Metrics

Answer: A

Explanation

The activities within the incident management process include:

References:
https://en.wikipedia.org/wiki/Incident_management_(ITSM)#Incident_management_procedure

NO.10 A hacker has managed to gain access to a Linux host and stolen the password file from /etc/passwd. How can he use it?

A. The password file does not contain the passwords themselves.

B. He can open it and read the user ids and corresponding passwords.

C. The file reveals the passwords to the root user only.

D. He cannot read it because it is encrypted.

Answer: A

NO.11 What is the most secure way to mitigate the theft of corporate information from a laptop that was left in a hotel room? **A.** Set a BIOS password.

B. Encrypt the data on the hard drive.

C. Use a strong logon password to the operating system.

D. Back up everything on the laptop and store the backup in a safe place.

Answer: B

NO.12 You are manually conducting Idle Scanning using Hping2. During your scanning you notice that almost every query increments the IPID regardless of the port being queried. One or two of the queries cause the IPID to increment by more than one value. Why do you think this occurs?

A. The zombie you are using is not truly idle.

B. A stateful inspection firewall is resetting your queries.

C. Hping2 cannot be used for idle scanning.

D. These ports are actually open on the target system.

Answer: A

NO.13 Darius is analysing IDS logs. During the investigation, he noticed that there was nothing suspicious found and an alert was triggered on normal web application traffic. He can mark this alert as:

A. False-Negative

B. False-Positive

C. True-Positive

D. False-Signature

Answer: A

NO.14 What is the proper response for a NULL scan if the port is closed?

A. SYN

B. ACK

C. FIN

D. PSH

E. RST

F. No response

Answer: E

NO.15 The Open Web Application Security Project (OWASP) is the worldwide not-for-profit charitable organization focused on improving the security of software. What item is the primary concern on OWASP's Top Ten Project Most Critical Web Application Security Risks?

A. Injection

B. Cross Site Scripting

C. Cross Site Request Forgery

D. Path disclosure

Answer: A

Explanation
The top item of the OWASP 2013 OWASP's Top Ten Project Most Critical Web Application Security Risks is injection.

Injection flaws, such as SQL, OS, and LDAP injection occur when untrusted data is sent to an interpreter as part of a command or query. The attacker's hostile data can trick the interpreter into executing unintended commands or accessing data without proper authorization. References: https://www.owasp.org/index.php/Top_10_2013-Top_10

NO.16 A recent security audit revealed that there were indeed several occasions that the company's network was breached. After investigating, you discover that your IDS is not configured properly and therefore is unable to trigger alarms when needed. What type of alert is the IDS giving? **A.** True Positive

B. False Negative

C. False Positive

D. False Positive

Answer: B

Explanation

New questions

NO.17 A Network Administrator was recently promoted to Chief Security Officer at a local university. One of employee's new responsibilities is to manage the implementation of an RFID card access system to a new server room on campus. The server room will house student enrollment information that is securely backed up to an off-site location.

During a meeting with an outside consultant, the Chief Security Officer explains that he is concerned that the existing security controls have not been designed properly. Currently, the Network

Administrator is responsible for approving and issuing RFID card access to the server room, as well as reviewing the electronic access logs on a weekly basis.

Which of the following is an issue with the situation?

A. Segregation of duties

B. Undue influence

C. Lack of experience

D. Inadequate disaster recovery plan

Answer: A

NO.18 Which vital role does the U.S. Computer Security Incident Response Team (CSIRT) provide?

A. Incident response services to any user, company, government agency, or organization in partnership with the Department of Homeland Security

B. Maintenance of the nation's Internet infrastructure, builds out new Internet infrastructure, and decommissions old Internet infrastructure

C. Registration of critical penetration testing for the Department of Homeland Security and public and private sectors

D. Measurement of key vulnerability assessments on behalf of the Department of Defense (DOD) and State Department, as well as private sectors

Answer: A

NO.19 Which of the following is used to indicate a single-line comment in structured query language (SQL)?

A. -**B.** ||

C. %%

D. ''

Answer: A

NO.20 Supposed you are the Chief Network Engineer of a certain Telco. Your company is planning for a big business expansion and it requires that your network authenticate users connecting using analog modems, Digital Subscriber Lines (DSL), wireless data services, and Virtual Private Networks (VPN) over a Frame Relay network. Which AAA protocol would you implement?

A. TACACS+

B. DIAMETER

C. Kerberos **D.** RADIUS

Answer: D

NO.21 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

Answer: A

NO.22 Which of the following command line switch would you use for OS detection in Nmap?

A. -D

B. -O

C. -P

D. -X

Answer: B

NO.23 A security consultant is trying to bid on a large contract that involves penetration testing and reporting. The company accepting bids wants proof of work so the consultant prints out several audits that have been performed. Which of the following is likely to occur as a result? **A.** The consultant will ask for money on the bid because of great work.

B. The consultant may expose vulnerabilities of other companies.

C. The company accepting bids will want the same type of format of testing.

D. The company accepting bids will hire the consultant because of the great work performed.

Answer: B

NO.24 What type of vulnerability/attack is it when the malicious person forces the user's browser to send an authenticated request to a server?

A. Cross-site request forgery

B. Cross-site scripting

C. Session hijacking

D. Server side request forgery

Answer: A

NO.25 Which of the following is a hashing algorithm?

A. MD5

B. PGP

C. DES

D. ROT13

Answer: A

NO.26 A security engineer has been asked to deploy a secure remote access solution that will allow employees to connect to the company's internal network. Which of the following can be implemented to minimize the opportunity for the man-in-the-middle attack to occur?

A. SSL

B. Mutual authentication

C. IPSec

D. Static IP addresses

Answer: C

NO.27 On a Linux device, which of the following commands will start the Nessus client in the background so that the Nessus server can be configured?

A. nessus +

B. nessus *s

C. nessus &

D. nessus -d

Answer: C

NO.28 If an attacker uses the command SELECT*FROM user WHERE name = 'x' AND userid IS NULL; --'; which type of SQL injection attack is the attacker performing?

A. End of Line Comment

B. UNION SQL Injection

C. Illegal/Logically Incorrect Query

D. Tautology

Answer: D

NO.29 A hacker, who posed as a heating and air conditioning specialist, was able to install a sniffer program in a switched environment network. Which attack could the hacker use to sniff all of the packets in the network?

A. Fraggle

B. MAC Flood

C. Smurf

D. Tear Drop

Answer: B

NO.30 Least privilege is a security concept that requires that a user is

A. limited to those functions required to do the job.

B. given root or administrative privileges.

C. trusted to keep all data and access to that data under their sole control.

D. given privileges equal to everyone else in the department.

Answer: A