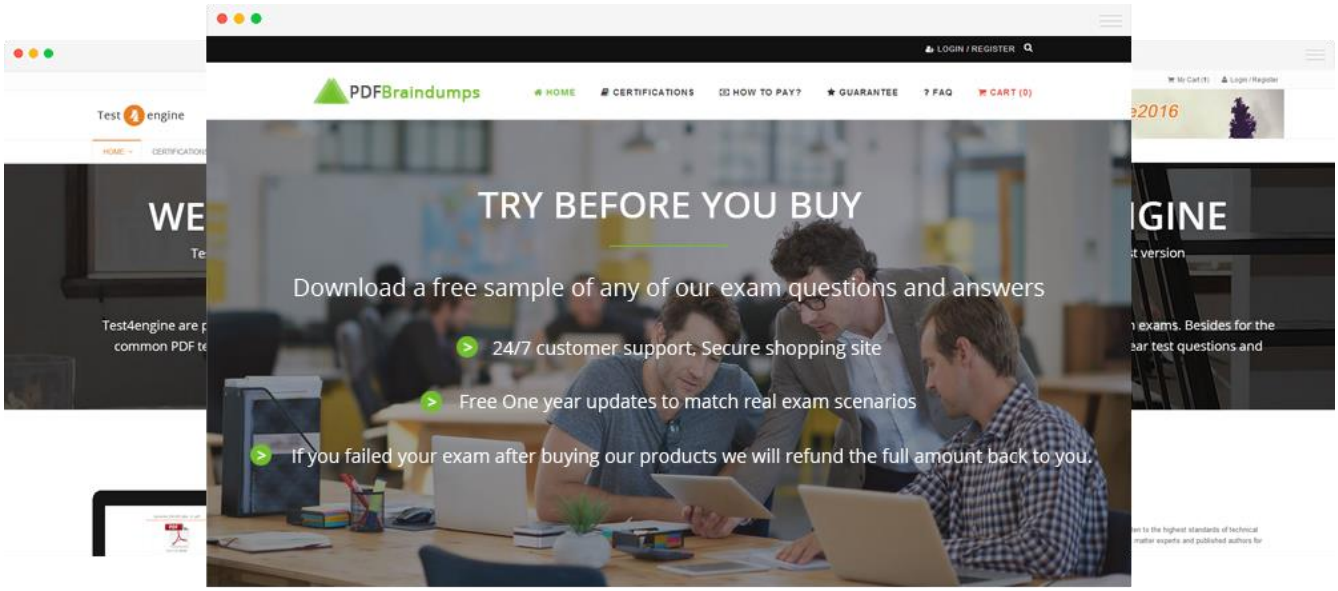
PDFBraindumps



Latest Pdf Braindumps

- LRP-614
- C-SRM-72
- BCABA
- ACMP-6.3
- JN0-740
- 1z0-100
- 250-405
- FM0-308
- DS-200
- C_SRM_72
- SDM_2002001040
- ACMP_6.3
- ST0-250
- 1z0-062
- H12-221
- A4120-784
- M2180-716

Top Certifications

- ISEB Certification
- HCNP
- OCE
- IFPUG Certifications
- NVIDIA Certifications
- dotMobi Certification
- Network+
- SCMA
- IBM Certified Integrat
- MCSD
- CCDH
- NCLP
- IBM Certified Advanc
- XMLMaster Certificat
- eserver Certified Spe
- CS5
- SAP-Certifications
- CHA
- Network Appliance N

Top Vendors

- ISEB
- Fortinet
- ASTQB
- Ericsson
- Aruba
- Liferay
- Data Center Universit
- Novell
- HRCI
- Huawei
- CIW
- RSA
- Patchlink
- MYSQL
- International Consorti
- ISM
- Acme-Packet
- CheckPoint

http://www.pdfbraindumps.com

Latest pdf braindumps provider, high pass rate

Exam : **312-50v11**

Title : Certified Ethical Hacker Exam (CEH v11)

Vendor : EC-COUNCIL

Version : DEMO

NO.1 Mr. Omkar performed tool-based vulnerability assessment and found two vulnerabilities. During analysis, he found that these issues are not true vulnerabilities.
What will you call these issues?
A. False negatives
B. True negatives
C. True positives
D. False positives
Answer: D

NO.2 What is the main security service a cryptographic hash provides?
A. Message authentication and collision resistance
B. Integrity and ease of computation
C. Integrity and computational in-feasibility
D. Integrity and collision resistance
Answer: C

NO.3 You are trying to break into a highly classified top-secret mainframe computer with highest security system in place at Merclyn Barley Bank located in Los Angeles.
You know that conventional hacking doesn't work in this case, because organizations such as banks are generally tight and secure when it comes to protecting their systems.
In other words, you are trying to penetrate an otherwise impenetrable system.
How would you proceed?
A. Try to hang around the local pubs or restaurants near the bank, get talking to a poorly-paid or disgruntled employee, and offer them money if they'll abuse their access privileges by providing you with sensitive information
B. Try to conduct Man-in-the-Middle (MiTM) attack and divert the network traffic going to the Merclyn Barley Bank's Webserver to that of your machine using DNS Cache Poisoning techniques
C. Launch DDOS attacks against Merclyn Barley Bank's routers and firewall systems using 100, 000 or more "zombies" and "bots"
D. Look for "zero-day" exploits at various underground hacker websites in Russia and China and buy the necessary exploits from these hackers and target the bank's network
Answer: A

NO.4 Bob, your senior colleague, has sent you a mail regarding a deal with one of the clients. You are requested to accept the offer and you oblige. After 2 days, Bab denies that he had ever sent a mail. What do you want to ""know"" to prove yourself that it was Bob who had send a mail?
A. Authentication
B. Non-Repudiation
C. Integrity
D. Confidentiality
Answer: B

NO.5 When you are getting information about a web server, it is very important to know the HTTP Methods (GET, POST, HEAD, PUT, DELETE, TRACE) that are available because there are two critical

methods (PUT and DELETE). PUT can upload a file to the server and DELETE can delete a file from the server. You can detect all these methods (GET, POST, HEAD, DELETE, PUT, TRACE) using NMAP script engine. What Nmap script will help you with this task?

A. http-methods
B. http enum
C. http-git
D. http-headers
Answer: A

NO.6 The security administrator of ABC needs to permit Internet traffic in the host 10.0.0.2 and UDP traffic in the host
10.0.0.3. He also needs to permit all FTP traffic to the rest of the network and deny all other traffic. After he applied his ACL configuration in the router, nobody can access the ftp, and the permitted hosts cannot access the Internet. According to the next configuration, what is happening in the network?

```
access-list 102 deny tcp any any
access-list 104 permit udp host 10.0.0.3 any
access-list 110 permit tcp host 10.0.0.2 eq www any
access-list 108 permit tcp any eq ftp any
```

A. The ACL for FTP must be before the ACL 110
B. The first ACL is denying all TCP traffic and the other ACLs are being ignored by the router
C. The ACL 110 needs to be changed to port 80
D. The ACL 104 needs to be first because is UDP
Answer: B

NO.7 Eric has discovered a fantastic package of tools named Dsniff on the Internet. He has learnt to use these tools in his lab and is now ready for real world exploitation. He was able to effectively intercept communications between the two entities and establish credentials with both sides of the connections. The two remote ends of the communication never notice that Eric is relaying the information between the two. What would you call this attack?

A. ARP Proxy
B. Interceptor
C. Poisoning Attack
D. Man-in-the-middle
Answer: D

NO.8 When analyzing the IDS logs, the system administrator noticed an alert was logged when the external router was accessed from the administrator's Computer to update the router configuration. What type of an alert is this?

A. False positive
B. True negative
C. False negative
D. True positive
Answer: A

Explanation:
True Positive - IDS referring a behavior as an attack, in real life it is True Negative - IDS referring a behavior not an attack and in real life it is not False Positive - IDS referring a behavior as an attack, in real life it is not False Negative - IDS referring a behavior not an attack, but in real life is an attack.
False Negative - is the most serious and dangerous state of all !!!!

NO.9 Which Nmap option would you use if you were not concerned about being detected and wanted to perform a very fast scan?
A. -A
B. -T5
C. -O
D. -T0
Answer: B

NO.10 in the Common Vulnerability Scoring System (CVSS) v3.1 severity ratings, what range does medium vulnerability fall in?
A. 3.0-6.9
B. 3.9-6.9
C. 40-6.0
D. 4.0-6.9
Answer: D
Explanation:

CVSS v2.0 Ratings

Severity	Base Score Range
Low	0.0-3.9
Medium	4.0-6.9
High	7.0-10.0

CVSS v3.0 Ratings

Severity	Base Score Range
None	0.0
Low	0.1-3.9
Medium	4.0-6.9
High	7.0-8.9
Critical	9.0-10.0

NO.11 What is the way to decide how a packet will move from an untrusted outside host to a protected inside that is behind a firewall, which permits the hacker to determine which ports are open and if the packets can pass through the packet-filtering of the firewall?
A. Man-in-the middle attack
B. Firewalking
C. Session hijacking
D. Network sniffing
Answer: B

NO.12 Which method of password cracking takes the most time and effort?
A. Shoulder surfing

B. Rainbow tables
C. Dictionary attack
D. Brute force
Answer: D

NO.13 env x='(){ :;};echo exploit' bash -c 'cat/etc/passwd'
What is the Shellshock bash vulnerability attempting to do on a vulnerable Linux host?
A. Display passwd content to prompt
B. Add new user to the passwd file
C. Changes all passwords in passwd
D. Removes the passwd file
Answer: A

NO.14 Some clients of TPNQM SA were redirected to a malicious site when they tried to access the TPNQM main site. Bob, a system administrator at TPNQM SA, found that they were victims of DNS Cache Poisoning. What should Bob recommend to deal with such a threat?
A. Client awareness
B. The use of DNSSEC
C. The use of security agents in clients' computers
D. The use of double-factor authentication
Answer: B

NO.15 Within the context of Computer Security, which of the following statements describes Social Engineering best?
A. Social Engineering is the means put in place by human resource to perform time accounting
B. Social Engineering is a training program within sociology studies
C. Social Engineering is the act of publicly disclosing information
D. Social Engineering is the act of getting needed information from a person rather than breaking into a system
Answer: D

NO.16 SQL injection (SQLi) attacks attempt to inject SQL syntax into web requests, which may Bypass authentication and allow attackers to access and/or modify data attached to a web application.
Which of the following SQLI types leverages a database server's ability to make DNS requests to pass data to an attacker?
A. Time-based blind SQLI
B. Union-based SQLI
C. Out-of-band SQLI
D. In-band SQLI
Answer: C
Explanation:
Out-of-band SQL injection occurs when an attacker is unable to use an equivalent channel to launch

the attack and gather results. ... Out-of-band SQLi techniques would believe the database server's ability to form DNS or HTTP requests to deliver data to an attacker. Out-of-band SQL injection is not very common, mostly because it depends on features being enabled on the database server being used by the web application. Out-of-band SQL injection occurs when an attacker is unable to use the same channel to launch the attack and gather results.
Out-of-band techniques, offer an attacker an alternative to inferential time-based techniques, especially if the server responses are not very stable (making an inferential time-based attack unreliable).
Out-of-band SQLi techniques would rely on the database server's ability to make DNS or HTTP requests to deliver data to an attacker. Such is the case with Microsoft SQL Server's xp_dirtree command, which can be used to make DNS requests to a server an attacker controls; as well as Oracle Database's UTL_HTTP package, which can be used to send HTTP requests from SQL and PL/SQL to a server an attacker controls.

NO.17 Scenario: Joe turns on his home computer to access personal online banking. When he enters the URL www.bank.com. the website is displayed, but it prompts him to re-enter his credentials as if he has never visited the site before. When he examines the website URL closer, he finds that the site is not secure and the web address appears different. What type of attack he is experiencing?.
A. Dos attack
B. DHCP spoofing
C. DNS hijacking
D. ARP cache poisoning
Answer: C

NO.18 Your company was hired by a small healthcare provider to perform a technical assessment on the network.
What is the best approach for discovering vulnerabilities on a Windows-based computer?
A. Create a disk image of a clean Windows installation
B. Use a scan tool like Nessus
C. Check MITRE.org for the latest list of CVE findings
D. Use the built-in Windows Update tool
Answer: B

NO.19 The company ABC recently contracts a new accountant. The accountant will be working with the financial statements. Those financial statements need to be approved by the CFO and then they will be sent to the accountant but the CFO is worried because he wants to be sure that the information sent to the accountant was not modified once he approved it. Which of the following options can be useful to ensure the integrity of the data?
A. The CFO can use a hash algorithm in the document once he approved the financial statements
B. The CFO can use an excel file with a password
C. The financial statements can be sent twice, one by email and the other delivered in USB and the accountant can compare both to be sure is the same document
D. The document can be sent to the accountant using an exclusive USB for that document
Answer: A

NO.20 George is a security professional working for iTech Solutions. He was tasked with securely transferring sensitive data of the organization between industrial systems. In this process, he used a short-range communication protocol based on the IEEE 203.15.4 standard. This protocol is used in devices that transfer data infrequently at a low rate in a restricted area, within a range of 10-100 m. What is the short-range wireless communication technology George employed in the above scenario?

A. Zigbee

B. NB-IoT

C. LPWAN

D. MQTT

Answer: A

Explanation:

Zigbee could be a wireless technology developed as associate open international normal to deal with the unique desires of affordable, low-power wireless IoT networks. The Zigbee normal operates on the IEEE 802.15.4 physical radio specification and operates in unauthorised bands as well as a pair of.4 GHz, 900 MHz and 868 MHz.

The 802.15.4 specification upon that the Zigbee stack operates gained confirmation by the Institute of Electrical and physical science Engineers (IEEE) in 2003. The specification could be a packet-based radio protocol supposed for affordable, battery-operated devices. The protocol permits devices to speak in an exceedingly kind of network topologies and may have battery life lasting many years.

The Zigbee three.0 Protocol

The Zigbee protocol has been created and ratified by member corporations of the Zigbee Alliance.Over three hundred leading semiconductor makers, technology corporations, OEMs and repair corporations comprise the Zigbee Alliance membership. The Zigbee protocol was designed to supply associate easy-to-use wireless information answer characterised by secure, reliable wireless network architectures.

THE ZIGBEE ADVANTAGE

The Zigbee 3.0 protocol is intended to speak information through rip-roaring RF environments that area unit common in business and industrial applications. Version 3.0 builds on the prevailing Zigbee normal however unifies the market-specific application profiles to permit all devices to be wirelessly connected within the same network, no matter their market designation and performance. what is more, a Zigbee 3.0 certification theme ensures the ability of product from completely different makers. Connecting Zigbee three.0 networks to the information science domain unveil observance and management from devices like smartphones and tablets on a local area network or WAN, as well as the web, and brings verity net of Things to fruition.

Zigbee protocol options include:

Support for multiple network topologies like point-to-point, point-to-multipoint and mesh networks Low duty cycle - provides long battery life Low latency Direct Sequence unfold Spectrum (DSSS) Up to 65,000 nodes per network

128-bit AES encryption for secure information connections

Collision avoidance, retries and acknowledgements

This is another short-range communication protocol based on the IEEE 203.15.4 standard. Zig-Bee is used in devices that transfer data infrequently at a low rate in a restricted area and within a range of 10-100 m.

NO.21 Session splicing is an IDS evasion technique in which an attacker delivers data in multiple, small sized packets to the target computer, making it very difficult for an IDS to detect the attack signatures. Which tool can be used to perform session splicing attacks?
A. Whisker
B. tcpsplice
C. Hydra
D. Burp
Answer: A

NO.22 You are a Network Security Officer. You have two machines. The first machine (192.168.0.99) has snort installed, and the second machine (192.168.0.150) has kiwi syslog installed. You perform a syn scan in your network, and you notice that kiwi syslog is not receiving the alert message from snort. You decide to run wireshark in the snort machine to check if the messages are going to the kiwi syslog machine. What Wireshark filter will show the connections from the snort machine to kiwi syslog machine?
A. tcp.dstport= = 514 && ip.dst= = 192.168.0.150
B. tcp.srcport= = 514 && ip.src= = 192.168.150
C. tcp.dstport= = 514 && ip.dst= = 192.168.0.99
D. tcp.srcport= = 514 && ip.src= = 192.168.0.99
Answer: A

NO.23 Which of the following types of SQL injection attacks extends the results returned by the original query, enabling attackers to run two or more statements if they have the same structure as the original one?
A. Boolean-based blind SQL injection
B. Blind SQL injection
C. Error-based injection
D. Union SQL injection
Answer: D

NO.24 Sam, a professional hacker. targeted an organization with intention of compromising AWS IAM credentials. He attempted to lure one of the employees of the organization by initiating fake calls while posing as a legitimate employee. Moreover, he sent phishing emails to steal the AWS 1AM credentials and further compromise the employee's account. What is the technique used by Sam to compromise the AWS IAM credentials?
A. Social engineering
B. Password reuse
C. insider threat
D. Reverse engineering
Answer: A
Explanation:
Just like any other service that accepts usernames and passwords for logging in, AWS users are vulnerable to social engineering attacks from attackers. fake emails, calls, or any other method of social engineering, may find yourself with an AWS users' credentials within the hands of an attacker.

If a user only uses API keys for accessing AWS, general phishing techniques could still use to gain access to other accounts or their pc itself, where the attacker may then pull the API keys for aforementioned AWS user.
With basic opensource intelligence (OSINT), it's usually simple to collect a list of workers of an organization that use AWS on a regular basis. This list will then be targeted with spear phishing to do and gather credentials. an easy technique may include an email that says your bill has spiked 500th within the past 24 hours, "click here for additional information", and when they click the link, they're forwarded to a malicious copy of the AWS login page designed to steal their credentials.
An example of such an email will be seen within the screenshot below. it's exactly like an email that AWS would send to you if you were to exceed the free tier limits, except for a few little changes. If you clicked on any of the highlighted regions within the screenshot, you'd not be taken to the official AWS web site and you'd instead be forwarded to a pretend login page setup to steal your credentials.
These emails will get even more specific by playing a touch bit additional OSINT before causing them out. If an attacker was ready to discover your AWS account ID on-line somewhere, they could use methods we at rhino have free previously to enumerate what users and roles exist in your account with none logs contact on your side. they could use this list to more refine their target list, further as their emails to reference services they will know that you often use.
For reference, the journal post for using AWS account IDs for role enumeration will be found here and the journal post for using AWS account IDs for user enumeration will be found here.
During engagements at rhino, we find that phishing is one in all the fastest ways for us to achieve access to an AWS environment.

NO.25 John, a professional hacker, targeted CyberSol Inc., an MNC. He decided to discover the IoT devices connected in the target network that are using default credentials and are vulnerable to various hijacking attacks. For this purpose, he used an automated tool to scan the target network for specific types of IoT devices and detect whether they are using the default, factory-set credentials. What is the tool employed by John in the above scenario?
A. Azure IoT Central
B. AT&T IoT Platform
C. IoTSeeker
D. IoT Inspector
Answer: C

NO.26 While using your bank's online servicing you notice the following string in the URL bar: "http: // www. MyPersonalBank. com/ account?id=368940911028389&Damount=10980&Camount=21" You observe that if you modify the Damount & Camount values and submit the request, that data on the web page reflects the changes. Which type of vulnerability is present on this site?
A. Cookie Tampering
B. Web Parameter Tampering
C. SQL Injection
D. XSS Reflection
Answer: B

NO.27 Nedved is an IT Security Manager of a bank in his country. One day. he found out that there is

a security breach to his company's email server based on analysis of a suspicious connection from the email server to an unknown IP Address.
What is the first thing that Nedved needs to do before contacting the incident response team?
A. Block the connection to the suspicious IP Address from the firewall
B. Migrate the connection to the backup email server
C. Disconnect the email server from the network
D. Leave it as it Is and contact the incident response te3m right away
Answer: C

NO.28 Windows LAN Manager (LM) hashes are known to be weak.
Which of the following are known weaknesses of LM? (Choose three.)
A. Makes use of only 32-bit encryption.
B. Converts passwords to uppercase.
C. Hashes are sent in clear text over the network.
D. Effective length is 7 characters.
Answer: B,C,D

NO.29 Which of the following represents the initial two commands that an IRC client sends to join an IRC network?
A. LOGIN, NICK
B. USER, PASS
C. LOGIN, USER
D. USER, NICK
Answer: D

NO.30 Attacker Rony installed a rogue access point within an organization's perimeter and attempted to intrude into its internal network. Johnson, a security auditor, identified some unusual traffic in the internal network that is aimed at cracking the authentication mechanism. He immediately turned off the targeted network and tested for any weak and outdated security mechanisms that are open to attack. What is the type of vulnerability assessment performed by johnson in the above scenario?
A. Host-based assessment
B. Application assessment
C. Wireless network assessment
D. Distributed assessment
Answer: C
Explanation:
Wireless network assessment determines the vulnerabilities in an organization's wireless networks. In the past, wireless networks used weak and defective data encryption mechanisms. Now, wireless network standards have evolved, but many networks still use weak and outdated security mechanisms and are open to attack. Wireless network assessments try to attack wireless authentication mechanisms and gain unauthorized access. This type of assessment tests wireless networks and identifies rogue networks that may exist within an organization's perimeter. These assessments audit client-specified sites with a wireless network. They sniff wireless network traffic

and try to crack encryption keys. Auditors test other network access if they gain access to the wireless network.

NO.31 A company's policy requires employees to perform file transfers using protocols which encrypt traffic. You suspect some employees are still performing file transfers using unencrypted protocols because the employees do not like changes. You have positioned a network sniffer to capture traffic from the laptops used by employees in the data ingest department. Using Wireshark to examine the captured traffic, which command can be used as display filter to find unencrypted file transfers?
A. tcp.port = = 21 | | tcp.port = =22
B. tcp.port ! = 21
C. tcp.port = = 21
D. tcp.port = 23
Answer: C

NO.32 During the process of encryption and decryption, what keys are shared?
A. Public and private keys
B. User passwords
C. Public keys
D. Private keys
Answer: C

NO.33 A large mobile telephony and data network operator has a data center that houses network elements. These are essentially large computers running on Linux. The perimeter of the data center is secured with firewalls and IPS systems.
What is the best security policy concerning this setup?
A. The operator knows that attacks and down time are inevitable and should have a backup site.
B. Network elements must be hardened with user ids and strong passwords. Regular security tests and audits should be performed.
C. As long as the physical access to the network elements is restricted, there is no need for additional measures.
D. There is no need for specific security measures on the network elements as long as firewalls and IPS systems exist.
Answer: B

NO.34 PGP, SSL, and IKE are all examples of which type of cryptography?
A. Secret Key
B. Hash Algorithm
C. Digest
D. Public Key
Answer: D

NO.35 What is the most common method to exploit the "Bash Bug" or "Shellshock" vulnerability?
A. SYN Flood

B. Manipulate format strings in text fields
C. SSH
D. Through Web servers utilizing CGI (Common Gateway Interface) to send a malformed environment variable to a vulnerable Web server
Answer: D