Eccouncil

312-50
Certified Ethical Hacker Exam (CEH v10)

➢**Up to Date products, reliable and verified.**
➢**Questions and Answers in PDF Format.**

For More Information – Visit link below:
https://www.examkill.com/

Version product

Question: 1

Email is transmitted across the Internet using the Simple Mail Transport Protocol. SMTP does not encrypt email, leaving the information in the message vulnerable to being read by an unauthorized person. SMTP can upgrade a connection between two mail servers to use TLS. Email transmitted by SMTP over TLS is encrypted. What is the name of the command used by SMTP to transmit email over TLS?

A. OPPORTUNISTICTLS STARTTLS
B. FORCETLS
C. UPGRADETLS

Answer: B

Question: 2

Developers at your company are creating a web application which will be available for use by anyone on the Internet, The developers have taken the approach of implementing a Three-Tier Architecture for the web application. The developers are now asking you which network should the Presentation Tier (front-end web server) be placed in?

A. isolated vlan network
B. Mesh network
C. DMZ network
D. Internal network

Answer: A

Question: 3

Your business has decided to add credit card numbers to the data it backs up to tape. Which of the following represents the best practice your business should observe?

A. Hire a security consultant to provide direction.
B. Do not back up cither the credit card numbers or then hashes.
C. Back up the hashes of the credit card numbers not the actual credit card numbers.
D. Encrypt backup tapes that are sent off-site.

Answer: A

Question: 4

What is the main security service a cryptographic hash provides?

A. Integrity and ease of computation
B. Message authentication and collision resistance
C. Integrity and collision resistance
D. Integrity and computational in-feasibility

Answer: D

Question: 5

A pen tester is configuring a Windows laptop for a test. In setting up Wireshark, what river and library are required to allow the NIC to work in promiscuous mode?

A. Libpcap
B. Awinpcap
C. Winprom
D. Winpcap

Answer: D

Question: 6

What is one of the advantages of using both symmetric and asymmetric cryptography in SSL/TLS?

A. Symmetric algorithms such as AES provide a failsafe when asymmetric methods fail.
B. Asymmetric cryptography is computationally expensive in comparison. However, it is well-suited to securely negotiate keys for use with symmetric cryptography.
C. Symmetric encryption allows the server to securely transmit the session keys out-of-band.
D. Supporting both types of algorithms allows less-powerful devices such as mobile phones to use symmetric encryption instead.

Answer: D

Question: 7

When a security analyst prepares for the formal security assessment - what of the following should be done in order to determine inconsistencies in the secure assets database and verify that system is compliant to the minimum security baseline?

A. Data items and vulnerability scanning
B. Interviewing employees and network engineers
C. Reviewing the firewalls configuration
D. Source code review

Answer: A

Question: 8

Why containers are less secure that virtual machines?

A. Host OS on containers has a larger surface attack.
B. Containers may full fill disk space of the host.
C. A compromise container may cause a CPU starvation of the host.
D. Containers are attached to the same virtual network.

Answer: A

Question: 9

These hackers have limited or no training and know how to use only basic techniques or tools.
What kind of hackers are we talking about?

A. Black-Hat Hackers A
B. Script Kiddies
C. White-Hat Hackers
D. Gray-Hat Hacker

Answer: C

Question: 10

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. Bob 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. Confidentiality

C. Integrity
D. Non-Repudiation

Answer: D

Question: 11

In the field of cryptanalysis, what is meant by a "rubber-hose" attack?

A. Attempting to decrypt cipher text by making logical assumptions about the contents of the original plain text.
B. Extraction of cryptographic secrets through coercion or torture.
C. Forcing the targeted key stream through a hardware-accelerated device such as an ASIC.
D. A backdoor placed into a cryptographic algorithm by its creator.

Answer: B

Question: 12

What type of analysis is performed when an attacker has partial knowledge of inner-workings of the application?

A. Black-box
B. Announced
C. White-box
D. Grey-box

Answer: D

Question: 13

Which of the following steps for risk assessment methodology refers to vulnerability identification?

A. Determines if any flaws exist in systems, policies, or procedures
B. Assigns values to risk probabilities; Impact values.
C. Determines risk probability that vulnerability will be exploited (High. Medium, Low)
D. Identifies sources of harm to an IT system. (Natural, Human. Environmental)

Answer: C

Question: 14

Log monitoring tools performing behavioral analysis have alerted several suspicious logins on a Linux server occurring during non-business hours. After further examination of all login activities, it is noticed that none of the logins have occurred during typical work hours. A Linux administrator who is investigating this problem realizes the system time on the Linux server is wrong by more than twelve hours. What protocol used on Linux servers to synchronize the time has stopped working?

A. Time Keeper
B. NTP
C. PPP
D. OSPP

Answer: B

Question: 15

What is the minimum number of network connections in a multi homed firewall?

A. 3
B. 5
C. 4
D. 2

Answer: A

Question: 16

Which of the following DoS tools is used to attack target web applications by starvation of available sessions on the web server?
The tool keeps sessions at halt using never-ending POST transmissions and sending an arbitrarily large content-length header value.

A. My Doom
B. Astacheldraht
C. R-U-Dead-Yet?(RUDY)
D. LOIC

Answer: C

Question: 17

During the process of encryption and decryption, what keys are shared?
During the process of encryption and decryption, what keys are shared?

A. Private keys
B. User passwords
C. Public keys
D. Public and private keys

Answer: C

Question: 18

You need a tool that can do network intrusion prevention and intrusion detection, function as a network sniffer, and record network activity, what tool would you most likely select?

A. Nmap
B. Cain & Abel
C. Nessus
D. Snort

Answer: D

Question: 19

How is the public key distributed in an orderly, controlled fashion so that the users can be sure of the sender's identity?

A. Hash value
B. Private key
C. Digital signature
D. Digital certificate

Answer: D

Question: 20

The network team has well-established procedures to follow for creating new rules on the firewall. This includes having approval from a manager prior to implementing any new rules. While reviewing the

firewall configuration, you notice a recently implemented rule but cannot locate manager approval for it. What would be a good step to have in the procedures for a situation like this?

A. Have the network team document the reason why the rule was implemented without prior manager approval.
B. Monitor all traffic using the firewall rule until a manager can approve it.
C. Do not roll back the firewall rule as the business may be relying upon it, but try to get manager approval as soon as possible.
D. Immediately roll back the firewall rule until a manager can approve it

Answer: D

Question: 21

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

Question: 22

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. Leave it as it Is and contact the incident response te3m right away
B. Block the connection to the suspicious IP Address from the firewall
C. Disconnect the email server from the network
D. Migrate the connection to the backup email server

Answer: C