SKILLCERTPRO
IT CERTIFICATION TRAININGS

0

Information Security / By SkillCertPro

Practice Set 6

Your results are here!! for" CEHv11 Practice Test 6 "

0 of 65 questions answered correctly

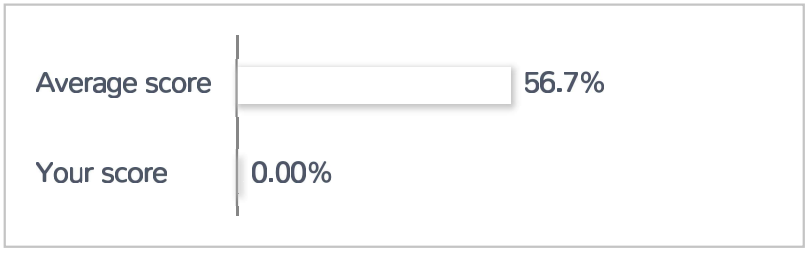
Your time: 00:00:02

Your Final Score is : 0

You have attempted : 0

Number of Correct Questions : 0 and scored 0

Number of Incorrect Questions : 0 and Negative marks 0



You can review your answers by clicking view questions.

Important Note : Open Reference Documentation Links in New Tab (Right Click and Open in New Tab).

Restart Test | View Answers

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34

35 36 37 38 39 40 41 42 43 44 45 46 47 48 49 50 51

52 53 54 55 56 57 58 59 60 61 62 63 64 65

Correct Incorrect

Review Question Summary

1. Question

Which of the following is the successor of SSL?

- RSA
- GRE
- IPSec
- **TLS**

Unattempted

2. Question

Which security strategy requires using several, varying methods to protect IT systems against attacks?

- **Defense in depth**
- Exponential backoff algorithm
- Covert channels
- Three-way handshake

Unattempted

3. Question

What type of vulnerability/attack is it when the malicious person forces the user's browser to send an authenticated request to a server?

- Cross-site scripting

- Server side request forgery
- Session hijacking
- **Cross-site request forgery**

Unattempted

4. Question

Which of the following is the structure designed to verify and authenticate the identity of individuals within the enterprise taking part in a data exchange?

- biometrics
- SOA
- single sign on
- **PKI**

Unattempted

5. Question

Steve, a scientist who works in a governmental security agency, developed a technological solution to identify people based on walking patterns and implemented this approach to a physical control access. A camera captures people walking and identifies the individuals using Steve's approach. After that, people must approximate their RFID badges. Both the identifications are required to open the door. In this case, we can say:

- **The solution implements the two authentication factors: physical object and physical characteristic**
- Although the approach has two phases, it actually implements just one authentication factor
- Biological motion cannot be used to identify people
- The solution will have a high level of false positives

Unattempted

6. Question

This international organization regulates billions of transactions daily and provides security guidelines to protect personally identifiable information (PII). These security controls provide a baseline and prevent low-level hackers sometimes known as script kiddies from causing a data breach. Which of the following organization is being described?

- **Payment Card Industry (PCI)**
- International Security Industry Organization (ISIO)
- Institute of Electrical and Electronics Engineers(IEEE)
- Center for Disease Control (CDC)

Unattempted

7. Question

Hackers often raise the trust level of a phishing message by modeling the email to look similar to the internal email used by the target company. This includes using logos, formatting, and names of the target company. The phishing message will often use the name of the company CEO, President, or Managers. The time a hacker spends performing research to locate this information about a company is known as?

- Enumeration
- Exploration
- **Reconnaissance**
- Investigation

Unattempted

8. Question

Peter is surfing the internet looking for information about DX Company. Which hacking process is Peter doing?

- Scanning
- System Hacking
- **Footprinting**
- Enumeration

Unattempted

9. Question

What is not a PCI compliance recommendation?

- Use encryption to protect all transmission of card holder data over any public network.
- **Rotate employees handling credit card transactions on a yearly basis to different departments.**
- Limit access to card holder data to as few individuals as possible.
- Use a firewall between the public network and the payment card data.

Unattempted

10. Question

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?

- Back up the hashes of the credit card numbers not the actual credit card numbers.
- Encrypt backup tapes that are sent off-site.
- **Hire a security consultant to provide direction.**
- Do not back up either the credit card numbers or their hashes.

Unattempted

11. Question

Initiating an attack against targeted business and organizations, threat actors compromise a carefully selected website by inserting an exploit resulting in malware infection. The attackers run exploits on well-known and trusted sites likely to be visited by their targeted victims. Aside from carefully choosing sites to compromise, these attacks are known to incorporate zero-day exploits that target unpatched vulnerabilities. Thus, the targeted entities are left with little or no defense against these exploits. What type of attack is outlined in the scenario?

- Heartbeat Attack

- Watering Hole Attack
- Spear Phishing Attack
- Shellshock Attack

Unattempted

12. Question

Jim's company regularly performs backups of their critical servers. But the company cannot afford to send backup tapes to an off-site vendor for long-term storage and archiving. Instead, Jim's company keeps the backup tapes in a safe in the office. Jim's company is audited each year, and the results from this year's audit show a risk because backup tapes are not stored off-site. The Manager of Information Technology has a plan to take the backup tapes home with him and wants to know what two things he can do to secure the backup tapes while in transit?

- Encrypt the backup tapes and transport them in a lock box.
- Degauss the backup tapes and transport them in a lock box.
- Encrypt the backup tapes and use a courier to transport them.
- Hash the backup tapes and transport them in a lock box.

Unattempted

13. Question

What kind of detection techniques is being used in antivirus software that identifies malware by collecting data from multiple protected systems and instead of analyzing files locally it's made on the provider's environment?

- Honypot based
- Behavioral based
- Heuristics based
- Cloud based

Unattempted

14. Question

Which of the following is an extremely common IDS evasion technique in the web world?

- Port Knocking
- Spyware
- **Unicode Characters**
- Subnetting

Unattempted

15. Question

Which of the following Linux commands will resolve a domain name into IP address?

- >host -t AXFR hackeddomain.com
- >host-t ns hackeddomain.com
- >host -t soa hackeddomain.com
- **>host-t a hackeddomain.com**

Unattempted

16. Question

You are a Penetration Tester and are assigned to scan a server. You need to use a scanning technique wherein the TCP Header is split into many packets so that it becomes difficult to detect what the packets are meant for. Which of the below scanning technique will you use?

- TCP Scanning
- Inverse TCP flag scanning
- ACK flag scanning
- **IP Fragment Scanning**

Unattempted

17. Question

The collection of potentially actionable, overt, and publicly available information is known as

- Real intelligence
- Human intelligence
- **Open-source intelligence**
- Social intelligence

Unattempted

18. Question

This asymmetry cipher is based on factoring the product of two large prime numbers. What cipher is described above?

- **RSA**
- MD5
- RC5
- SHA

Unattempted

19. Question

Shellshock allowed an unauthorized user to gain access to a server. It affected many Internet-facing services, which OS did it not directly affect?

- Linux
- **Windows**
- Unix
- OS X

Unattempted

20. Question

Code injection is a form of attack in which a malicious user:

- Gets the server to execute arbitrary code using a buffer overflow
- **Inserts text into a data field that gets interpreted as code**
- Inserts additional code into the JavaScript running in the browser
- Gains access to the codebase on the server and inserts new code

Unattempted

21. Question

In which of the following password protection technique, random strings of characters are added to the password before calculating their hashes?

- Key Stretching
- Double Hashing
- **Salting**
- Keyed Hashing

Unattempted

22. Question

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?

- Nmap
- **Snort**
- Nessus
- Cain & Abel

Unattempted

23. Question

Security Policy is a definition of what it means to be secure for a system, organization or other entity. For Information Technologies, there are sub-policies like Computer Security Policy, Information Protection Policy, Information Security Policy, network Security Policy, Physical Security Policy, Remote Access Policy, and User Account Policy. What is the main theme of the sub-policies for Information Technologies?

- **Confidentiality, Integrity, Availability**
- Authenticity, Confidentiality, Integrity
- Authenticity, Integrity, Non-repudiation
- Availability, Non-repudiation, Confidentiality

Unattempted

24. Question

Which component of IPsec performs protocol-level functions that are required to encrypt and decrypt the packets?

- IPsec Policy Agent
- **Internet Key Exchange (IKE)**
- Oakley
- IPsec driver

Unattempted

25. Question

What is the most common method to exploit the “Bash Bug” or “ShellShock” vulnerability?

- SYN Flood
- **Through Web servers utilizing CGI (Common Gateway Interface) to send a malformed environment variable to a vulnerable Web server**
- Manipulate format strings in text fields
- SSH

Unattempted

26. Question

Which of the following is an adaptive SQL Injection testing technique used to discover coding errors by inputting massive amounts of random data and observing the changes in the output?

- Static Testing
- Function Testing
- Dynamic Testing
- **Fuzzing Testing**

Unattempted

27. Question

During a recent security assessment, you discover the organization has one Domain Name Server (DNS) in a Demilitarized Zone (DMZ) and a second DNS server on the internal network. What is this type of DNS configuration commonly called?

- DNS Scheme
- DNSSEC
- **Split DNS**
- DynDNS

Unattempted

28. Question

This tool is an 802.11 WEP and WPA-PSK keys cracking program that can recover keys once enough data packets have been captured. It implements the standard FMS attack along with some optimizations like KoreK attacks, as well as the PTW attack, thus making the attack much faster compared to other WEP cracking tools. Which of the following tools is being described?

- Airguard
- wificracker

- WLAN-crack
- **Aircrack-ng**

Unattempted

29. Question

The following is part of a log file taken from the machine on the network with the IP address of 192.168.0.110:

```
Time:June 16 17:30:15 Port:20 Source:192.168.0.105 Destination:192.168.0.110 Protocol:TCP
Time:June 16 17:30:17 Port:21 Source:192.168.0.105 Destination:192.168.0.110 Protocol:TCP
Time:June 16 17:30:19 Port:22 Source:192.168.0.105 Destination:192.168.0.110 Protocol:TCP
Time:June 16 17:30:21 Port:23 Source:192.168.0.105 Destination:192.168.0.110 Protocol:TCP
Time:June 16 17:30:22 Port:25 Source:192.168.0.105 Destination:192.168.0.110 Protocol:TCP
Time:June 16 17:30:23 Port:80 Source:192.168.0.105 Destination:192.168.0.110 Protocol:TCP
Time:June 16 17:30:30 Port:443 Source:192.168.0.105 Destination:192.168.0.110 Protocol:TCP
```

What type of activity has been logged?

- **Port scan targeting 192.168.0.110**
- Denial of service attack targeting 192.168.0.105
- Port scan targeting 192.168.0.105
- Teardrop attack targeting 192.168.0.110

Unattempted

30. Question

Firewalls are the software or hardware systems that are able to control and monitor the traffic coming in and out the target network based on pre-defined set of rules. Which of the following types of firewalls can protect against SQL injection attacks?

- Stateful firewall
- Packet firewall
- Data-driven firewall
- **Web application firewall**

Unattempted

31. Question

An attacker, using a rogue wireless AP, performed an MITM attack and injected an HTML code to embed a malicious applet in all HTTP connections. When users accessed any page, the applet ran and exploited many machines. Which one of the following tools the hacker probably used to inject HTML code?

- Aircrack-ng
- Wireshark
- Tcpdump
- **Ettercap**

Unattempted

32. Question

.....is an attack type for a rogue Wi-Fi access point that appears to be a legitimate one offered on the premises, but actually has been set up to eavesdrop on wireless communications. It is the wireless version of the phishing scam. An attacker fools wireless users into connecting a laptop or mobile phone to a tainted hotspot by posing as a legitimate provider. This type of attack may be used to steal the passwords of unsuspecting users by either snooping the communication link or by phishing, which involves setting up a fraudulent web site and luring people there. Fill in the blank with appropriate choice.

- Signal Jamming Attack
- **Evil Twin Attack**
- Collision Attack
- Sinkhole Attack

Unattempted

33. Question

You are monitoring the network of your organizations. You notice that: 1. There are huge outbound connections from your Internal Network to External IPs 2. On further investigation, you see that the external IPs are blacklisted 3. Some connections are accepted, and some are dropped 4. You find that it is a CnC communication Which of the following solution will you suggest?

- Clean the Malware which are trying to Communicate with the External Blacklist IP's
- **Both B and C**
- Block the Blacklist IP's @ Firewall
- Update the Latest Signatures on your IDS/IPS

Unattempted

34. Question

Which of the following program infects the system boot sector and the executable files at the same time?

- Polymorphic virus
- Macro virus
- Stealth virus
- **Multipartite Virus**

Unattempted

35. Question

Which method of password cracking takes the most time and effort?

- Rainbow tables
- Shoulder surfing
- Dictionary attack
- **Brute force**

Unattempted

36. Question

An attacker scans a host with the below command. Which three flags are set? (Choose three.) #nmap “”sX host.domain.com

- This is Xmas scan. URG, PUSH and FIN are set
- This is ACK scan. ACK flag is set
- This is Xmas scan. SYN and ACK flags are set
- This is SYN scan. SYN flag is set

Unattempted

37. Question

What term describes the amount of risk that remains after the vulnerabilities are classified and the countermeasures have been deployed?

- Residual risk
- Impact risk
- Inherent risk
- Deferred risk

Unattempted

38. Question

Bob, a network administrator at BigUniversity, realized that some students are connecting their notebooks in the wired network to have Internet access. In the university campus, there are many Ethernet ports available for professors and authorized visitors but not for students. He identified this when the IDS alerted for malware activities in the network. What should Bob do to avoid this problem?

- Disable unused ports in the switches
- Ask students to use the wireless network
- Separate students in a different VLAN
- Use the 802.1x protocol

Unattempted

39. Question

You are attempting to run an Nmap port scan on a web server. Which of the following commands would result in a scan of common ports with the least amount of noise in order to evade IDS?

- nmap -sP -p-65535 -T5
- **nmap -sT -O -T0**
- nmap -A --host-timeout 99 -T1
- nmap -A - Pn

Unattempted

40. Question

Which Nmap option would you use if you were not concerned about being detected and wanted to perform a very fast scan?

- -T0
- **-T5**
- -O
- -A

Unattempted

41. Question

In which of the following cryptography attack methods, the attacker makes a series of interactive queries, choosing subsequent plaintexts based on the information from the previous encryptions?

- Known-plaintext attack
- Ciphertext-only attack
- **Adaptive chosen-plaintext attack**
- Chosen-plaintext attack

Unattempted

Adaptive Chosen-plaintext Attack: Attacker makes a series of interactive queries, choosing subsequent plaintexts based on the information from the previous encryptions.

Reference: http://www.crypto-it.net/eng/attacks/chosen-plaintext.html

42. Question

Based on the below log, which of the following sentences are true? Mar 1, 2016, 7:33:28 AM 10.240.250.23 "" 54373 10.249.253.15 "" 22 tcp_ip

- Application is SSH and 10.240.250.23 is the server and 10.249.253.15 is the server
- **Application is SSH and 10.240.250.23 is the client and 10.249.253.15 is the server**
- Application is FTP and 10.240.250.23 is the client and 10.249.253.15 is the server
- SSH communications are encrypted it's impossible to know who is the client or the server

Unattempted

43. Question

Alice encrypts her data using her public key PK and stores the encrypted data in the cloud. Which of the following attack scenarios will compromise the privacy of her data?

- **Alice also stores her private key in the cloud, and Harry breaks into the cloud server as before**
- Agent Andrew subpoenas Alice, forcing her to reveal her private key. However, the cloud server successfully resists Andrew's attempt to access the stored data
- Hacker Harry breaks into the cloud server and steals the encrypted data
- None of these scenarios compromise the privacy of Alice's data

Unattempted

44. Question

Which one of the following Google advanced search operators allows an attacker to restrict the results to those websites in the given domain?

- [cache:]
- [link:]
- [inurl:]

- [site:]

Unattempted

45. Question

Which of the following attacks exploits web age vulnerabilities that allow an attacker to force an unsuspecting user's browser to send malicious requests they did not intend?

- Command Injection Attacks
- **Cross-Site Request Forgery (CSRF)**
- File Injection Attack
- Hidden Field Manipulation Attack

Unattempted

46. Question

What two conditions must a digital signature meet?

- Has to be the same number of characters as a physical signature and must be unique.
- **Has to be unforgeable, and has to be authentic.**
- Must be unique and have special characters.
- Has to be legible and neat.

Unattempted

47. Question

Which of the following will perform an Xmas scan using NMAP?

- nmap -sA 192.168.1.254
- nmap -sP 192.168.1.254
- nmap -sV 192.168.1.254
- **nmap -sX 192.168.1.254**

Unattempted

48. Question

Which is the first step followed by Vulnerability Scanners for scanning a network?

- OS Detection
- TCP/UDP Port scanning
- Firewall detection
- **Checking if the remote host is alive**

Unattempted

49. Question

An IT employee got a call from one of our best customers. The caller wanted to know about the company's network infrastructure, systems, and team. New opportunities of integration are in sight for both company and customer. What should this employee do?

- Disregarding the call, the employee should hang up.
- Since the company's policy is all about Customer Service, he/she will provide information.
- The employees cannot provide any information; but, anyway, he/she will provide the name of the person in charge.
- **The employee should not provide any information without previous management authorization.**

Unattempted

50. Question

A technician is resolving an issue where a computer is unable to connect to the Internet using a wireless access point. The computer is able to transfer files locally to other machines, but cannot successfully reach the Internet. When the technician examines the IP address and default gateway they are both on the 192.168.1.0/24. Which of the following has occurred?

- The computer is using an invalid IP address.

- The gateway and the computer are not on the same network.
- The computer is not using a private IP address.
- **The gateway is not routing to a public IP address.**

Unattempted

51. Question

A hacker has managed to gain access to a Linux host and stolen the password file from /etc/passwd. How can he use it?

- He can open it and read the user ids and corresponding passwords.
- **The password file does not contain the passwords themselves.**
- He cannot read it because it is encrypted.
- The file reveals the passwords to the root user only.

Unattempted

52. Question

The establishment of a TCP connection involves a negotiation called three-way handshake. What type of message does the client send to the server in order to begin this negotiation?

- ACK
- **SYN**
- RST
- SYN-ACK

Unattempted

53. Question

You have successfully comprised a server having an IP address of 10.10.0.5. You would like to enumerate all machines in the same network quickly. What is the best Nmap command you will use?

- nmap -T4 -F 10.10.0.0/24
- nmap -T4 -O 10.10.0.0/24
- nmap -T4 -q 10.10.0.0/24
- nmap -T4 -r 10.10.1.0/24

Unattempted

54. Question

Identify the web application attack where the attackers exploit vulnerabilities in dynamically generated web pages to inject client-side script into web pages viewed by other users.

- Cross-Site Request Forgery (CSRF)
- LDAP Injection attack
- Cross-Site Scripting (XSS)
- SQL injection attack

Unattempted

55. Question

Which of the following provides a security professional with most information about the system's security posture?

- Wardriving, warchalking, social engineering
- Port scanning, banner grabbing, service identification
- Phishing, spamming, sending trojans
- Social engineering, company site browsing, tailgating

Unattempted

56. Question

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?

- The use of double-factor authentication
- **The use of DNSSEC**
- Client awareness
- The use of security agents in clients' computers

Unattempted

57. Question

What is attempting an injection attack on a web server based on responses to True/False questions called?

- Classic SQLi
- Compound SQLi
- DMS-specific SQLi
- **Blind SQLi**

Unattempted

58. Question

Due to a slowdown of normal network operations, the IT department decided to monitor internet traffic for all of the employees. From a legal standpoint, what would be troublesome to take this kind of measure?

- All of the employees would stop normal work activities
- **Not informing the employees that they are going to be monitored could be an invasion of privacy.**
- IT department would be telling employees who the boss is
- The network could still experience traffic slow down.

Unattempted

59. Question

Chandler works as a pen-tester in an IT-firm in New York. As a part of detecting viruses in the systems, he uses a detection method where the anti-virus executes the malicious codes on a virtual machine to simulate CPU and memory activities. Which type of virus detection method did Chandler use in this context?

- Integrity checking
- Heuristic Analysis
- **Code Emulation**
- Scanning

Unattempted

60. Question

You are working as a Security Analyst in a company XYZ that owns the whole subnet range of 23.0.0.0/8 and 192.168.0.0/8. While monitoring the data, you find a high number of outbound connections. You see that IP's owned by XYZ (Internal) and private IP's are communicating to a Single Public IP. Therefore, the Internal IP's are sending data to the Public IP. After further analysis, you find out that this Public IP is a blacklisted IP, and the internal communicating devices are compromised. What kind of attack does the above scenario depict?

- Spear Phishing Attack
- Advanced Persistent Threats
- **Botnet Attack**
- Rootkit Attack

Unattempted

61. Question

Bob, your senior colleague, has sent you a mail regarding aa 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?

- Authentication
- Integrity
- **Non-Repudiation**

Confidentiality

Unattempted

62. Question

DNS cache snooping is a process of determining if the specified resource address is present in the DNS cache records. It may be useful during the examination of the network to determine what software update resources are used, thus discovering what software is installed. What command is used to determine if the entry is present in DNS cache?

dnsnooping ""rt update.antivirus.com

nslookup -fullrecursive update.antivirus.com

dns --snoop update.antivirus.com

nslookup -norecursive update.antivirus.com

Unattempted

63. Question

A hacker named Jack is trying to compromise a bank's computer system. He needs to know the operating system of that computer to launch further attacks. What process would help him?

Banner Grabbing

UDP Scanning

SSDP Scanning

IDLE/IPID Scanning

Unattempted

64. Question

You perform a scan of your company's network and discover that TCP port 123 is open. What services by default run on TCP port 123?

Network Time Protocol

- POP3
- DNS
- Telnet

Unattempted

65. Question

Which of the following Bluetooth hacking techniques does an attacker use to send messages to users without the recipient's consent, similar to email spamming?

- Bluejacking
- Bluesniffing
- Bluesnarfing
- Bluesmacking

Unattempted

Click Below to go to Next Practice Set

Pages: 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22

← Previous Post Next Post →

We help you to succeed in your certification exams

We have helped over thousands of working professionals to achieve their certification goals with our practice tests.

Skillcertpro

Quick Links

ABOUT US

FAQ

BROWSE ALL PRACTICE TESTS

CONTACT FORM

Important Links

REFUND POLICY

REFUND REQUEST

TERMS & CONDITIONS

PRIVACY POLICY

Privacy Policy