SKILLCERTPRO
IT CERTIFICATION TRAININGS

0

Information Security / By SkillCertPro

Practice Set 15

Your results are here!! for" CEHv11 Practice Test 15 "

0 of 65 questions answered correctly

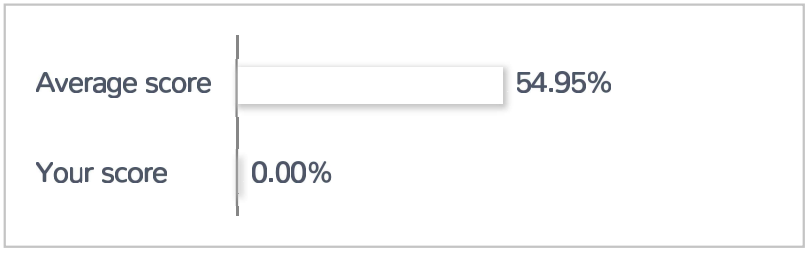
Your time: 00:00:01

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

It is defined as the process of identifying, analyzing, prioritizing, and resolving events that take place in an organization.

- Internal Procedure
- **Incident Management Process**
- Security Policy
- Metrics

Unattempted

Incident management is a set of defined processes to identify, analyze, prioritize, and resolve security incidents to restore and prevent further damage in service operations.

2. Question

This is called a “Collision attack” in cryptography

- **Finding two inputs producing the same hash.**
- Getting the public key
- Breaking the hash into three parts to get the plaintext value.
- Breaking the hash into two parts, with the same bytes in each part to get the private key.

Unattempted

A collision attack is an attempt to find two input strings of a hash function that produce the same hash result.

3. Question

A large financial company recently requires its employees to perform file transfers using protocols that encrypts traffic. As a security analyst, you suspect that some of the employees are still performing file transfers using unencrypted protocols. You have positioned a network sniffer to capture traffic from the laptops used by employees in the data ingest department. Using Wire shark to examine the captured traffic, which command can be used as a display filter to find unencrypted file transfers?

- **tcp.port ==21**
- tcp.port ==21 || tcp.port ==22
- tcp.port = 23
- tcp.port != 21

Unattempted

Wireshark filter “tcp.port == 21” will show traffic from ports 21 which is used for FTP.

4. Question

What is the most efficient way of cracking passwords for Windows Server 2003 Active Directory (AD) users?

- Hybrid attack
- Dictionary attack
- Brute force attack
- **Rainbow table attack**

Unattempted

A rainbow table attack is a hacking method that involves the use of a rainbow hash table. This table contains the values used to encrypt the passwords before adding them to the database.

5. Question

Angel is an expert when it comes to password weaknesses and key loggers. She was then assigned to conduct a password assessment to XYZ company. She suspects that weak passwords are the norm throughout the company. Which of the following options suggests that Angel can retrieve passwords from the company’s hosts and servers?

- Software only, they are the most effective.

- Passwords are always best obtained using Hardware key loggers.
- **Hardware, Software, and Sniffing.**
- Hardware and Software Keyloggers.

Unattempted

Different types of keylogger planted into the environment would retrieve the passwords for Angel.

6. Question

Which of the following belongs to the 5 Phases of Ethical Hacking:

- **Scanning**
- **Reconnaissance**
- Escalating
- **Covering track**

Unattempted

The Phases of hacking are: Phase 1-Reconnaissance Phase 2-Scanning Phase 3-Gaining Access Phase 4-Maintaining Access Phase 5-Covering Tracks

7. Question

A black hat hacker changes the profile information of a targeted victim on the targeted website. The attacker uses this string to update the victim's profile to a text file and then submit the data to the attacker's database.

```
< iframe src="http://www.vulnweb.com/updateif.php" style="display:none"></iframe>
```

What is this type of attack (that can use either HTTP GET or HTTP POST) called?

- Cross-Site Scripting
- **Cross-Site Request Forgery**
- SQL Injection
- Browser Hacking

Unattempted

Cross-site request forgery, also known as CSRF is a type of malicious exploit that allows an attacker to trick users to perform actions that they do not intend to. Some examples are changing the email address and/or password, or making a funds transfer. Depending on the nature of the action, the attacker might be able to gain full control over the user's account.

8. Question

Jia is a certified ethical hacker at SIA Global Security. She was contacted by a startup company to perform a technical assessment on their network. What is the best approach for checking vulnerabilities on a Windows-based computer?

- Create a disk image of a clean Windows installation
- **Use a scan tool such as Nessus**
- Check MITRE.org for the latest list of CVE findings
- Utilize the built-in Windows Update tool

Unattempted

Nessus performs vulnerability, configuration, and compliance assessments. It supports various technologies such as operating systems, network devices, hypervisors, databases, tablets/phones, web servers, and critical infrastructure

9. Question

John has successfully compromised a server having an IP address of 10.10.0.7. He wants to enumerate all machines in the same network quickly. Which of the following Nmap command must he use?

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

Unattempted

The command "nmap -T4 -F" is used to scan faster than a normal scan because it uses the aggressive timing template and scans fewer ports

10. Question

The new chief security officer asks for a report of all the computers on the network with missing patches and weak passwords. Which of the following scanner can generate this report?

- **Vulnerability scanner**
- Port scanner
- Virus scanner
- Malware scanner

Unattempted

Vulnerability scanning is a method used to check whether a system is exploitable by identifying its vulnerabilities. A vulnerability scanner consists of a scanning engine and a catalog. These tools generally target vulnerabilities that secure host configurations can fix easily, updated security patches, and a clean Web document.

11. Question

What are the three types of compliance that the Open Source Security Testing Methodology Manual (OSSTMM) recognizes?

- Legislative, Contractual, Regulatory
- **Legislative, Contractual, Standards based**
- Legislative, Regulatory, Standards based
- Contractual, Regulatory, Standards based

Unattempted

The OSSTMM recognizes three types of compliance:

1. Legislative. Compliance with legislation is in accordance to the region where the legislation can be enforced. The strength and commitment to the legislation comes from previously successful legal arguments and appropriately set and just enforcement measures. Examples are Sarbanes-Oxley, HIPAA, and the various Data Protection and Privacy legislation.
2. Contractual. Compliance to contractual requirements are in accordance to the industry or within the group that requires the contract and may take action to enforce compliance. An example is the payment card industry data security standard (PCI DSS) promoted and required by VISA and MasterCard.
3. Standards based. Compliance to standards is in accordance with the business or organization where the compliance to standards is enforced as policy. Examples are the OSSTMM, ISO 27001/5, and ITIL.

12. Question

Angel has successfully compromised a server on a network and opened a shell. She wants to identify all operating systems running on the network. Unfortunately, as she attempts to fingerprint all machines in the network using the nmap syntax below, it is not going through. What seems to be wrong in her syntax?

```
invictus@victim_server:~$ nmap -T4 -O 10.10.0.0/24
TCP/IP fingerprinting (for OS scan) xxxxxxx xxxxxx xxxxxxxxx
QUITTING!
```

- The outgoing TCP/IP fingerprinting is blocked by the host firewall.
- This is a common behavior for a corrupted Nmap application.
- The Nmap syntax is wrong.
- **OS Scan requires root privileges.**

Unattempted

The requested scan type requires root privileges.

13. Question

The normal (default) speed of scanning for open ports is by using which of the following command?

- **-T3**
- -O
- -T5
- -S

Unattempted

Timing and Performance	
-T0	Paranoid (0) Intrusion Detection System evasion
-T1	Sneaky (1) Intrusion Detection System evasion
-T2	Polite (2) slows down the scan to use less bandwidth and use less target machine resources
-T3	Normal (3) which is default speed
-T4	Aggressive (4) speeds scans; assumes you are on a reasonably fast and reliable network
-T5	Insane (5) speeds scan; assumes you are on an extraordinarily fast network

14. Question

There are two types of sniffing: Passive and Active sniffing. Which of the following is/are an example of Active sniffing?

- [ ] Hub-based networks
- [ ] Mac flooding
- [ ] DNS poisoning
- [ ] DHCP attacks

Unattempted

Active sniffing involves sending out multiple network probes to identify access points. The following are examples of different active sniffing techniques:

MAC flooding

DNS poisoning

RP poisoning

DHCP attacks

Switch port stealing

Spoofing attack

15. Question

It is a wireless network detector, packet sniffer, and intrusion detection system (IDS) and is commonly found on Linux-based system.

- Netstumbler
- Abel
- Nessus
- **Kismet**

Unattempted

Kismet is a wireless network detector, packet sniffer, and intrusion detection system (IDS) that works with any wireless card supporting raw monitoring (rfmon) mode.

16. Question

Anna is using the nslookup command to list all DNS information such as Name Servers, host names, MX records, CNAME records, glue records (delegation for child Domains), zone serial number, and TimeToLive (TTL) records for a Domain. Anna is accomplishing which of the following?

- **A zone transfer**
- A zone update
- A zone estimate
- A zone harvesting

Unattempted

Zone transfer is the process of copying the contents of the zone file on a primary DNS server to a secondary DNS server. Using zone transfer provides fault tolerance by synchronizing the zone file in a primary DNS server with the zone file in a secondary DNS server.

17. Question

Which of the following biometrics scan is used on the eye to measure the layer of blood vessels?

- Signature kinetics scan
- Iris scan
- Facial recognition scan
- **Retinal scan**

Unattempted

Retinal scans capture capillaries deep within the eye by using unique near-infrared cameras.

18. Question

Theon logged in as a local admin on a Windows 7 system and needs to launch the Computer Management Console from command line. Which of the following command will he use?

- c:\gpedit
- c:\services.msc
- **c:\compmgmt.msc**
- c:\ncpa.cpl

Unattempted

To open the Computer Management Console from command line just type compmgmt.msc in your run box or at the command line.

19. Question

A large company is planning to use Blackberry phones as their corporate mobile phones. They assigned Paul, a security analyst, to evaluate the possible threats they might encounter. To do this, he will use Blackjacking attack to demonstrate how a cybercriminal can bypass the perimeter defenses and gain access to the corporate's network. Which of the following tool will he use to perform a Blackjacking attack?

- BBCrack
- Paros Proxy
- Blooover
- **BBProxy**

Unattempted

Blackberry users have been warned that the security of Blackberry wireless e-mail devices is at risk due to a hacking tool, BBProxy.

20. Question

Which of the following is/are NOT an example of active reconnaissance?

- Ping
- Netcat
- Traceroute
- **Spyse**

Unattempted

Active reconnaissance is the opposite of passive reconnaissance wherein the information is gathered by directly engaging with the potential target. This may be done via manual testing or automated scanning using tools such as Nmap, ping, traceroute, and netcat.

21. Question

Which of the following is a type of SQL injection attack?

- **Blind**
- **Error-based**
- Check
- **Union**

Unattempted

Union-based, Error-based, and Blind are all types of SQL injection attacks.

22. Question

Proxy tool provides a lot of advantages when testing web applications. It allows you manually test every request and analyze the response to find vulnerabilities. It also allows you to test parameters and headers manually to get more precise results than when using web vulnerability scanners. What proxy tool will help you find web vulnerabilities?

- **Burpsite**
- Proxychains
- Maskgen
- Dimitry

Unattempted

Burp Suite is an integrated platform for performing security testing of web applications. Its various tools work seamlessly together to support the entire testing process, from initial mapping and analysis of an application's attack surface to finding and exploiting security vulnerabilities.

23. Question

Diffie-Hellman (DH) groups determine the strength of the key used in the key exchange process. Which of the following is the correct bit size of the Diffie-Hellman (DH) group 14?

- 768 bit key
- 1536 bit key
- 1025 bit key
- **2048 bit key**

Unattempted

DH Group 1: 768-bit group
DH Group 2: 1024-bit group
DH Group 5: 1536-bit group
DH Group 14: 2048-bit group
DH Group 15: 3072-bit group

24. Question

Which of the following password cracking attacks takes the most time and effort?

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

Unattempted

In a brute force attack, cybercriminals try every combination of characters until the password is broken. Even though all passwords will be found, this attack is very time consuming.

25. Question

Which of the following describes Simple Object Access Protocol (SOAP)? Choose all that applies.

- [ ] Exchanges data between web services
- [ ] Provides a structured model for messaging
- [ ] Based on XML
- [ ] Only compatible with the application protocol HTTP

Unattempted

A SOAP client formulates a request for a service. This involves creating a conforming XML document, either explicitly or using Oracle SOAP client API. A SOAP client sends the XML document to a SOAP server. This SOAP request is posted using HTTP or HTTPS to a SOAP Request Handler running as a servlet on a Web server.

26. Question

This is considered the best way to protect Personally Identifiable Information (PII) from Web application vulnerabilities?

- ( ) Using encrypted communications protocols to transmit Personally Identifiable Information (PII)
- ( ) Using cryptographic storage to store all Personally Identifiable Information (PII)
- ( ) Using a security token to log into all Web applications that use Personally Identifiable Information (PII)
- ( ) Using full disk encryption on all hard drives to protect Personally Identifiable Information (PII)

Unattempted

It is a best practice that any Personally Identifiable Information (PII) must be encrypted

27. Question

Jann is a system administrator in a startup company. While analyzing the IDS logs, she noticed an alert was logged even when the external router was accessed from the administrator's computer to update the router configuration. What type of an alert is this?

- ( ) False negative
- ( ) True positve

- True negative
- **False positive**

Unattempted

False positives are mislabeled security alerts. These alerts indicate that there is a threat when in reality no attack has taken place. For example, an alert was triggered indicating a brute force attack, but later on, found out that it was just the user who mistyped the password a lot of times.

28. Question

SIA Global Security wants to check if it is possible to infiltrate their company. They want the attack to be realistic so they did not provide any information besides the company name. What is the first step of security testing the client?

- Escalation
- Scanning
- Enumeration
- **Reconnaissance**

Unattempted

The Phases of hacking are: Phase 1-Reconnaissance Phase 2-Scanning Phase 3-Gaining Access Phase 4-Maintaining Access Phase 5-Covering Tracks

29. Question

The hacker infected the server with a certain type of Trojan in order and use it in sending and hosting junk mails. What type of Trojan did the hacker use?

- **Botnet Trojan**
- Ransomware Trojans
- Banking Trojans
- Turtle Trojans

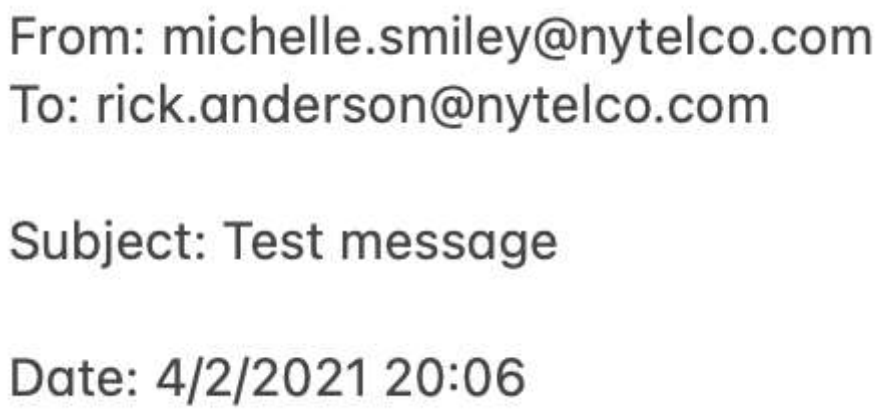
Unattempted

Botnet refers to the group of hijacked or infected computers, servers, mobile devices, and IoT (Internet of Things) devices that are being controlled by a hacker. Botnets are used to carry out malicious activities such

as account credential leakage, unauthorized access and clicking of ads, sending spam emails, and participating in DDoS (Distributed Denial of Service) attacks.

30. Question

A telco company based in New York City hired you to evaluate the security of their email gateway. To do this, you created a test email and send it across the Internet to one of their employee. The recipient employee is aware of the said evaluation.



After a few minutes, the employee received your test email. This proves that the email gateway of the telco company allows?

- **Email Spoofing**
- Email Harvesting
- Email Masquerading
- Email Phishing

Unattempted

Email spoofing is a technique used in spam and phishing attacks to trick users into thinking a message came from a person or entity they either know or can trust. In spoofing attacks, the sender forges email headers so that client software displays the fraudulent sender address, which most users take at face value.

31. Question

Peterson discovered an active server that is currently in the same network as the machine he recently exploited. He pings it but there was no response. What could be the main issue?

- **The ICMP is disabled on the target server.**
- The TCP/IP does not support ICMP.

- The ping command requires root privileges
- The ARP is disabled on the target server.

Unattempted

The ping command sends an ICMP echo request to a device on the network, and the device immediately responds with an ICMP echo reply. If there was no response after the ping, the ICMP may be disabled on the target server.

32. Question

Which of the following commands will start the Nessus client in the background so that the Nessus server can be configured on a Linux device.

- **nessus &**
- nessus -d
- nessus *s
- nessus +

Unattempted

In Linux, to start a process in the background you will use &.

33. Question

Which of the following command is used to create a scheduled task in Windows System?

- nc
- hping3
- telnet
- **Schtasks**

Unattempted

Schtasks allows an administrator to create, delete, query, change, run, and end scheduled tasks on a local or remote system

34. Question

Which of the following special character is sent to web application to check for SQL Injection vulnerability.

- Semicolon
- **Single quotation**
- Exclamation point
- Backlash

Unattempted

Injection attacks can be prevented by doing a source code validation or review. This will allow you to determine the injection flaws and mitigate them before deploying the code into production.

35. Question

Which system consists of a publicly available set of databases that contain domain name registration contact information?

- IANA
- IETF
- CAPTCHA
- **WHOIS**

Unattempted

WHOIS is a query and response protocol that is widely used for querying databases that store the registered users or assignees of an Internet resource, such as a domain name, an IP address block or an autonomous system, but is also used for a wider range of other information.

36. Question

Which of the following is an example of active reconnaissance?

- Dumpster Diving
- Packet Sniffing
- None of the above
- **Nmap**

Unattempted

Nmap is a powerful active reconnaissance tool. This tool can be used to gather lots of information about the target. Let's see how we can use Nmap in our favor.

37. Question

This is a hardware requirement that either an IDS/IPS system or a proxy server must have in order to function properly.

- Fast network interface cards (NIC)
- **Dual-homed**
- Similar RAM
- Fast processor

Unattempted

Dual-homed or dual-homing refers to an Ethernet device that has more than one network interface used for redundancy purposes. In firewall technology, it is one of the firewall architectures used for implementing preventive security.

38. Question

It is the practice of exposing known security vulnerabilities of a certain system or network with the authorized or owner's permission

- Red hat hacking
- **White hat hacking**
- Gray hat hacking
- Black hat hacking

Unattempted

The goal of white hat hacking is to check for security vulnerabilities of a certain system or network to help the owners address and fix these before being discovered by malicious hackers.

39. Question

Angel has successfully compromised a machine on the network and found a server that is alive on the same network. She tried to ping it but didn't get any response back. What is happening?

- You need to run the ping command with root privileges.
- TCP/IP doesn't support ICMP.
- **The ICMP could be disabled on the target server.**
- The ARP is disabled on the target server.

Unattempted

The ping utility is implemented using the ICMP "Echo request" and "Echo reply" messages. Note: The Internet Control Message Protocol (ICMP) is one of the main protocols of the internet protocol suite. It is used by network devices, like routers, to send error messages indicating, for example, that a requested service is not available or that a host or router could not be reached.

40. Question

This attack occurs when the cybercriminal continuously sends a connection request to the target until all the ports are saturated, making the legitimate users unable to connect.

- **SYN Flood**
- Smurf
- ICMP Flood
- None of the above

Unattempted

A SYN flood occurs when a cybercriminal sends a connection request to the targeted server but fails to complete the connection through what is known as a three-way handshake. The incomplete handshake leaves the connected port unavailable for further requests. The cybercriminal will continue sending a connection request until all the ports are saturated, making the legitimate users unable to connect.

41. Question

Which of the following options is the most secure way for storing backup tapes?

- It must be stored in a vault for security purposes.

- **It must be stored in a climate controlled facility away from the site.**
- It must be stored at the center of the building for easier access.
- It must be stored in a climate controlled facility onsite for faster retrieval.

Unattempted

An effective disaster data recovery strategy should consist of producing backup tapes and housing them in an offsite storage facility. This way the data isn't compromised if a natural disaster affects the business' office. It is highly recommended that the backup tapes be handled properly and stored in a secure, climate-controlled facility. This provides peace of mind and gives the business almost immediate stability after a disaster.

42. Question

Which of the following types of firewalls ensures that the packets are part of the established session?

- Switch-level firewall
- Circuit-level firewall
- **Stateful inspection firewall**
- Application-level firewall

Unattempted

A stateful firewall is a network firewall that monitors the operating state and characteristics of network connections traversing it. The firewall is configured to distinguish legitimate packets for different types of connections. Only packets matching a known active connection (session) are allowed to pass the firewall.

43. Question

This type of hacker works only to cause fear and disruption of systems and networks.

- **Cyber terrorists**
- Black Hat Hacker
- Suicide Hacker
- State sponsored hackers

Unattempted

Cyber terrorists are hackers who are influenced by certain religious or political beliefs. They work to cause fear and disruption of systems and networks.

44. Question

Which of the following statements is TRUE about sniffers?

- **Sniffers operate on Layer 2 of the OSI model**
- Sniffers operate on Layer 3 of the OSI model
- Sniffers operate on both Layer 2 & Layer 3 of the OSI model.
- Sniffers operate on Layer 1 of the OSI model.

Unattempted

The OSI layer 2 is where packet sniffers collect their data.

45. Question

It is an entity or act with the potential to adversely damage a system through unauthorized access, destruction, disclosure, denial of service, or modification of data. Which of the following terms best matches the definition?

- Risk
- Attack
- Vulnerability
- **Threat**

Unattempted

A threat is any entity or malicious act with the potential to adversely damage organizational operations (including mission, functions, image, or reputation), organizational assets, or individuals through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service.

46. Question

Which of the following is/are an example of active reconnaissance?

- [ ] **Ping**

- [ ] Netcat
- [ ] Spyse
- [ ] Traceroute

Unattempted

Active reconnaissance is the opposite of passive reconnaissance wherein the information is gathered by directly engaging with the potential target. This may be done via manual testing or automated scanning using tools such as Nmap, ping, traceroute, and netcat.

47. Question

Which of the following asymmetry cipher is based on factoring the product of two large prime numbers?

- ○ RC5
- ○ RSA
- ○ MD5
- ○ SHA

Unattempted

RSA is based on the practical difficulty of factoring the product of two large prime numbers, the factoring problem.

48. Question

A cybercriminal is standing outside, near a secure entrance facility while pretending to have a tense conversation on his cell phone. An unsuspicious authorized employee badges in and the cybercriminal who is still on the phone, grabs the door as it begins to close, and enters the facility. What do you call this type of attack?

- ○ Tailgating
- ○ Phishing
- ○ Masquerading
- ○ Whaling

Unattempted

Tailgaiting is an act where the unauthorized person was able to enter the premises without the authorized person's knowledge. To avoid Tailgating, employees should be wary of their surroundings.

49. Question

Operating System (OS) Fingerprinting helps a cracker because:

- It defines exactly what software you have installed.
- It opens a security-delayed window based on the port being scanned.
- It doesn't depend on the patches that have been applied to fix existing security holes.
- **It informs the cracker of which vulnerabilities he may be able to exploit on your system.**

Unattempted

OS fingerprinting is the process a hacker goes through to determine the type of operating system being used on a targeted computer. This is beneficial because it gives the hacker useful information about any security vulnerabilities of the operating system that can be exploited to launch an attack.

50. Question

Anna was hired as a Security Analyst at SIA Global Security. To secure the company's network, she set up a firewall and an IDS. Unfortunately, cybercriminals are still able to attack the network. After further investigation, she discovered that the IDS is not properly configured. This is why the alarms did not trigger when needed. What type of alert is the IDS giving?

- True Negative
- **False Negative**
- False Positive
- True Positive

Unattempted

False negative happens when no alarm was raised even though an attack has taken place.

51. Question

The extraction of passwords from a person by using coercion or torture?

- Ciphertext-only Attack
- Timing Attack
- Chosen-Cipher text Attack
- **Rubber Hose Attack**

Unattempted

The rubber hose attack is extracting secrets from people by use of torture or coercion.

52. Question

In user authentication, which of the following is considered as "something you have"?

- Fingerprint
- PIN
- **Smart Card**

Unattempted

Fingerprint is considered as "something you are",

PIN is considered as "something you know",

Smart Card is considered as "something you have"

53. Question

This act that states that all medical practices must ensure that all necessary measures are in place while saving, accessing, and sharing any electronic medical data to keep patient data secure.

- **Health Insurance Portability and Accountability Act**
- Control Objectives for Information and Related Technologies
- International Organization for Standardization and International Electro-Technical Commission
- Federal Information Security Management Act

Unattempted

Health Insurance Portability and Accountability Act (HIPAA) is a 1996 legislation in the United States that protects patients' health information from being disclosed without their consent or knowledge. It regulates the use and disclosure of Protected Health Information (PHI) held by "covered entities" (generally, health

care clearinghouses, employer-sponsored health plans, health insurers, and medical service providers that engage in certain transactions.)

54. Question

Which of the following is a characteristic of Public Key Infrastructure (PKI)?

- Public-key cryptosystems are faster than symmetric-key cryptosystems.
- **Public-key cryptosystems distribute public-keys using digital certificates.**
- Public-key cryptosystems do not require a secure key distribution channel.
- Public-key cryptosystems do not provide technical non-repudiation via digital signatures.

Unattempted

A digital certificate contains, among other things, the sender's public key, and can be used to identify the sender.

55. Question

These hackers are ready and willing to perform an attack for a "cause", even if they get caught and prosecuted.

- Cyber Terrorist
- State Sponsored Hacker
- Hacktivist
- **Suicide Hacker**

Unattempted

Suicide hackers are those who hack for some purpose and even don't bother to suffer long-term jail due to their activities.

56. Question

Which of the following commands runs snort in packet logger mode?

- **./snort -dev -l ./log**
- /snort -dev -p ./log

/snort -dev -o ./log

./snort -dev -h ./log

Unattempted

If you want to store the packages in binary mode for later analysis use "./snort –l ./log -b".

57. Question

Which of the following cyberattack takes advantage of a website vulnerability in which the site displays content that includes un-sanitized user-provided data.

Buffer Overflow attack

SQL Injection

Cross-site-scripting attack

URL Traversal attack

Unattempted

Cross-site scripting or XSS flaws occur whenever an application allows users to add custom code that includes data from untrusted sources without proper validation. Hackers inject malicious scripts into a victim's system by hiding them within legitimate requests. Hackers can also bypass authentication mechanisms, gain privileges, and then inject malicious scripts into specific web pages. These malicious scripts can hijack user sessions, deface websites, or redirect the user to malicious sites.

58. Question

What is a Boot Sector Virus?

It overwrites the original MBR and only executes the new virus code.

It moves the MBR to another location on the RAM and copies itself to the original location of the MBR.

It moves the MBR to another location on the hard disk and copies itself to the original location of the MBR.

It modifies directory table entries so that directory entries point to the virus code instead of the actual program.

Unattempted

A boot sector virus is a computer virus that infects a storage device's master boot record (MBR). The virus moves the boot sector to another location on the hard drive.

59. Question

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

- SSDP Scanning
- IDLE/IPID Scanning
- **Banner Grabbing**
- UDP Scanning

Unattempted

Banner grabbing is a technique used by hackers and security teams to gain information about a computer system on a network and services running on its open ports. A banner is a text displayed by a host server containing details like software type and version running in a system or server. The welcome screens divulge software version numbers and other system information on network hosts, giving cybercriminals a leg up on attacking the network.

60. Question

Which of the following is NOT an ideal choice for biometric controls?

- Iris patterns
- Voice
- Fingerprints
- **Height and weight**

Unattempted

Height and weight are not ideal choices for biometric controls. Even though these provide some information about the user, they lack distinctiveness and permanence to sufficiently differentiate the user from each other.

61. Question

Which of the following is a Windows command that can be used to list all the shared connections to which the current user has access?

- **NET USE**
- NET FILE
- NET VIEW
- NET CONFIG

Unattempted

The net use command is a Command Prompt command that's used to connect to, remove, and configure connections to shared resources, like mapped drives and network printers.

62. Question

Aleaj wants to do an ICMP scan on a remote computer using hping2. Which of the following syntax will allow her to do an ICMP scan?

- A. hping2 host.domain.com
- hping2 --set-ICMP host.domain.com
- **hping2 -i host.domain.com**
- hping2 -i host.domain.com

Unattempted

hping2 by default uses TCP. To send an ICMP scan, we can use the -1 (one mode). The correct syntax is hping2 -1 host.domain.com.

63. Question

Jane is a penetration tester from SIA Global Security. She was hired to do a risk assessment of a company's DMZ. The rules of engagement state that the vulnerability test can be done from an external IP address with no prior knowledge of the internal IT systems. Which of the following test is being performed?

- White box
- **Black box**
- Grey box

Yellow box

Unattempted

A black-box tester is unaware of the internal structure of the application to be tested, while a white-box tester has access to the internal structure of the application. A gray-box tester partially knows the internal structure, which includes access to the documentation of internal data structures as well as the algorithms used.

64. Question

Which of the following attack is possible if a token and a 4-digit personal identification number (PIN) are used to access a computer system? The token performs off-line checking for the correct PIN.

Smurf

Birthday

Man-in-the-middle

Brute force

Unattempted

In a brute force attack, cybercriminals try every combination of characters until the password is broken. Even though all passwords will be found, this attack is very time-consuming.

65. Question

Port scanning can be used in determining network vulnerabilities as part of a technical assessment. The TCP XMAS scan is used to identify listening ports on the targeted system. What happens if a scanned port is open?

The port will send a SYN.

The port will send an ACK.

The port will send an RST.

The port will ignore the packets.

Unattempted

Cybercriminals use TCP XMAS scan to determine if ports are closed on the target machine. This scan type is accomplished by sending TCP segments with all possible flags set in the packet header, generating packets that are illegal based on RFC 793. The RFC 793 expected behavior is that any TCP segment with an out-of-

state Flag sent to an open port is discarded, whereas segments with out-of-state flags sent to closed ports should be handled with a RST in response. This behavior should allow an attacker to scan for closed ports by sending certain types of rule-breaking packets (out of sync or disallowed by the TCB) and detect closed ports via RST packets.

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 →

REFUND POLICY
REFUND REQUEST
TERMS & CONDITIONS
PRIVACY POLICY

Privacy Policy