Fast2Test
FIRST TEST, FIRST PASS!

# Fast2Test


### Instant Download

After Payment, our system will send you the products you purchase in mailbox in a minute after payment. If not received within 2 hours, please contact us.

### 365 Days Free Updates

Free update is available within 365 days after your purchase. After 365 days, you will get 50% discounts for updating.


### Money Back Guarantee

Full refund if you fail the corresponding exam in 60 days after purchasing. And Free get any another product.

### Security & Privacy

We respect customer privacy. We use McAfee's security service to provide you with utmost security for your personal information & peace of mind.

We're not the only ones **happy** about Fast2test Practice Materials ...

**62316+** customers in 100+ countries use Fast2test Self Test Engine. Meet our customers.

https://tw.fast2test.com

高效的考試材料是最高通過率的考試題庫

**Exam** : **212-82**

**Title** : Certified Cybersecurity Technician

**Vendor** : ECCouncil

**Version** : DEMO

**NO.1** Malachi, a security professional, implemented a firewall in his organization to trace incoming and outgoing traffic. He deployed a firewall that works at the session layer of the OSI model and monitors the TCP handshake between hosts to determine whether a requested session is legitimate. Identify the firewall technology implemented by Malachi in the above scenario.

**A.** Next generation firewall (NGFW)

**B.** Circuit-level gateways

**C.** Network address translation (NAT)

**D.** Packet filtering

***Answer:*** B

Explanation:

A circuit-level gateway is a type of firewall that works at the session layer of the OSI model and monitors the TCP handshake between hosts to determine whether a requested session is legitimate. It does not inspect the contents of each packet, but rather relies on the session information to filter traffic

**NO.2** Which of the following are examples of physical security controls? (Select all that apply)

**A.** Security guards

**B.** Firewalls

**C.** Biometric access control

**D.** Encryption algorithms

***Answer:*** AC

**NO.3** Analyze the executable file ShadowByte.exe located in the Downloads folder of the Attacker Machine-I and determine the Linker Info value of the file. (Practical Question)

**A.** 04.25

**B.** 2.25

**C.** 3.5

**D.** 6.2

***Answer:*** B

**NO.4** RAT has been setup in one of the machines connected to the network to steal the important Sensitive corporate docs located on Desktop of the server, further investigation revealed the IP address of the server 20.20.10.26. Initiate a remote connection using thief client and determine the number of files present in the folder.

Hint: Thief folder is located at: Z:\CCT-Tools\CCT Module 01 Information Security Threats and Vulnerabilities\Remote Access Trojans (RAT)\Thief of Attacker Machine-1.

**A.** 2

**B.** 4

**C.** 3

**D.** 5

***Answer:*** C

Explanation:

3 is the number of files present in the folder in the above scenario. A RAT (Remote Access Trojan) is a type of malware that allows an attacker to remotely access and control a compromised system or

network. A RAT can be used to steal sensitive data, spy on user activity, execute commands, install other malware, etc. To initiate a remote connection using thief client, one has to follow these steps: Navigate to the thief folder located at Z:\CCT-Tools\CCT Module 01 Information Security Threats and Vulnerabilities\Remote Access Trojans (RAT)\Thief of Attacker Machine-1. Double-click on thief.exe file to launch thief client.
Enter 20.20.10.26 as IP address of server.
Enter 1234 as port number.
Click on Connect button.
After establishing connection with server, click on Browse button.
Navigate to Desktop folder on server.
Count number of files present in folder.
The number of files present in folder is 3, which are:
Sensitive corporate docs.docx
Sensitive corporate docs.pdf
Sensitive corporate docs.txt

**NO.5** Riley sent a secret message to Louis. Before sending the message, Riley digitally signed the message using his private key. Louis received the message, verified the digital signature using the corresponding key to ensure that the message was not tampered during transit. Which of the following keys did Louis use to verify the digital signature in the above scenario?

**A.** Riley's public key

**B.** Louis's public key

**C.** Riley's private key

**D.** Louis's private key

***Answer:*** A

Explanation:
Riley's public key is the key that Louis used to verify the digital signature in the above scenario. A digital signature is a cryptographic technique that verifies the authenticity and integrity of a message or document. A digital signature is created by applying a hash function to the message or document and then encrypting the hash value with the sender's private key. A digital signature can be verified by decrypting the hash value with the sender's public key and comparing it with the hash value of the original message or document.Riley's public key is the key that corresponds to Riley's private key, which he used to sign the message. Louis's public key is the key that corresponds to Louis's private key, which he may use to encrypt or decrypt messages with Riley.
Louis's private key is the key that only Louis knows and can use to sign or decrypt messages.
Riley's private key is the key that only Riley knows and can use to sign or encrypt messages.

**NO.6** Jordan, a network administrator in an organization, was instructed to identify network-related issues and improve network performance. While troubleshooting the network, he received a message indicating that the datagram could not be forwarded owing to the unavailability of IP-related services (such as FTP or web services) on the target host, which of the following network issues did Jordan find in this scenario?

**A.** Time exceeded message

**B.** Destination unreachable message

**C.** Unreachable networks

**D.** Network cable is unplugged

***Answer:*** B

Explanation:

Destination unreachable message is the network issue that Jordan found in this scenario. Destination unreachable message is a type of ICMP message that indicates that the datagram could not be forwarded owing to the unavailability of IP-related services (such as FTP or web services) on the target host. Destination unreachable message can be caused by various reasons, such as incorrect routing, firewall blocking, or host configuration problems.

**NO.7** Ruben, a crime investigator, wants to retrieve all the deleted files and folders in the suspected media without affecting the original files. For this purpose, he uses a method that involves the creation of a cloned copy of the entire media and prevents the contamination of the original media. Identify the method utilized by Ruben in the above scenario.

**A.** Sparse acquisition

**B.** Bit-stream imaging

**C.** Drive decryption

**D.** Logical acquisition

***Answer:*** B

Explanation:

Bit-stream imaging is the method utilized by Ruben in the above scenario. Bit-stream imaging is a method that involves creating a cloned copy of the entire media and prevents the contamination of the original media. Bit-stream imaging copies all the data on the media, including deleted files and folders, hidden partitions, slack space, etc., at a bit level. Bit-stream imaging preserves the integrity and authenticity of the digital evidence and allows further analysis without affecting the original media. Sparse acquisition is a method that involves creating a partial copy of the media by skipping empty sectors or blocks. Drive decryption is a method that involves decrypting an encrypted drive or partition using a password or a key. Logical acquisition is a method that involves creating a copy of the logical files and folders on the media using file system commands.

**NO.8** An attacker used the ping-of-death (PoD) technique to crash a target Android device. The network traffic was captured by the SOC team and was provided to you to perform a detailed analysis. Analyze the android.pcapng file located In the Documents folder of the Attacker machine-2 and determine the length of PoD packets In bytes. (Practical Question)

**A.** 52

**B.** 056

**C.** 58

**D.** 54

***Answer:*** D

**NO.9** A software company has implemented a wireless technology to track the employees' attendance by recording their in and out timings. Each employee in the company will have an entry card that is embedded with a tag. Whenever an employee enters the office premises, he/she is required to swipe the card at the entrance. The wireless technology uses radio-frequency electromagnetic waves to transfer data for automatic identification and for tracking tags attached to objects. Which of the following technologies has the software company implemented in the above

scenario?

**A.** WiMAX

**B.** RFID

**C.** Bluetooth

**D.** Wi-Fi

***Answer:*** B

Explanation:

RFID (Radio Frequency Identification) is the wireless technology that the software company has implemented in the above scenario. RFID uses radio-frequency electromagnetic waves to transfer data for automatic identification and for tracking tags attached to objects. WiMAX (Worldwide Interoperability for Microwave Access) is a wireless technology that provides high- speed broadband access over long distances. Bluetooth is a wireless technology that enables short-range data communication between devices, such as phones, laptops, printers, etc. Wi-Fi (Wireless Fidelity) is a wireless technology that allows devices to connect to a local area network or the internet using radio waves.

**NO.10** A software company develops new software products by following the best practices for secure application development. Dawson, a software analyst, is responsible for checking the performance of applications in the client's network to determine any issue faced by end users while accessing the application.

Which of the following tiers of the secure application development lifecycle involves checking the application performance?

**A.** Development

**B.** Staging

**C.** Testing

**D.** Quality assurance (QA)

***Answer:*** C

Explanation:

Testing is the tier of the secure application development lifecycle that involves checking the application performance in the above scenario. Secure application development is a process that involves designing, developing, deploying, and maintaining software applications that are secure and resilient to threats and attacks. Secure application development can be based on various models or frameworks, such as SDLC (Software Development Life Cycle), OWASP (Open Web Application Security Project), etc. Secure application development consists of various tiers or stages that perform different tasks or roles. Testing is a tier of the secure application development lifecycle that involves verifying and validating the functionality and security of software applications before releasing them to end users. Testing can include various types of tests, such as unit testing, integration testing, system testing, performance testing, security testing, etc.

Testing can be used to check the application performance and identify any errors, bugs, or vulnerabilities in the software applications. In the scenario, a software company develops new software products by following the best practices for secure application development. Dawson, a software analyst, is responsible for checking the performance of applications in the client's network to determine any issue faced by end users while accessing the application. This means that he performs testing for this purpose. Development is a tier of the secure application development lifecycle that involves creating and coding software applications according to the design and

specifications. Staging is a tier of the secure application development lifecycle that involves deploying software applications to a simulated or pre-production environment for testing or evaluation purposes. Quality assurance (QA) is a tier of the secure application development lifecycle that involves ensuring that software applications meet the quality standards and expectations of end users and stakeholders

**NO.11** An IoT device placed in a hospital for safety measures has sent an alert to the server. The network traffic has been captured and stored in the Documents folder of the "Attacker Machine-1". Analyze the IoTdeviceTraffic.pcapng file and identify the command the IoT device sent over the network.

**A.** Tempe_Low

**B.** Low_Tem p e

**C.** High_Tcmpe

**D.** Temp_High

***Answer:*** D

Explanation:

The IoT device sent the command Temp_High over the network, which indicates that the temperature in the hospital was above the threshold level. This can be verified by analyzing the IoTdeviceTraffic.pcapng file using a network protocol analyzer tool such as Wireshark. The command Temp_High can be seen in the data field of the UDP packet sent from the IoT device (192.168.0.10) to the server (192.168.0.1) at 12:00:03.

**NO.12** Alpha Finance, a leading banking institution, is launching anew mobile banking app. Given the sensitive financial data involved, it wants to ensure that Its application follows the best security practices. As the primary recommendation, which guideline should Alpha Finance prioritize?

**A.** Embedding an antivirus within the app

**B.** Employing multi-factor authentication (MFA) for user logins

**C.** Providing an in-app VPN for secure transactions

**D.** Encouraging users to update to the latest version of their OS

***Answer:*** B

**NO.13** An advanced persistent threat (APT) group known for Its stealth and sophistication targeted a leading software development company. The attack was meticulously planned and executed over several months. It involved exploiting vulnerabilities at both the application level and the operating system level. The attack resulted in the extraction of sensitive source code and disruption of development operations. Post-incident analysis revealed multiple attack vectors, including phishing, exploitation of unknown/unpatched vulnerabilities in software/hardware. and lateral movement within the network. Given the nature and execution of this attack, what was the primary method used by the attackers to initiate this APT?

**A.** Exploiting default passwords to gain initial access to the network.

**B.** Exploiting a zero-day vulnerability in the application used by developers.

**C.** Exploiting a known vulnerability in the firewall to bypass network defenses.

**D.** Compromising a third-party vendor with access to the company's development environment.

***Answer:*** B

**NO.14** A web application, www.moviescope.com. hosted on your tarqet web server is vulnerable to SQL injection attacks. Exploit the web application and extract the user credentials from the moviescope database. Identify the UID (user ID) of a user, John, in the database. Note: Vou have an account on the web application, and your credentials are samAest.

**A.** 3

**B.** 4

**C.** 2

**D.** 5

***Answer:*** B

Explanation:

4 is the UID (user ID) of a user, John, in the database in the above scenario. A web application is a software application that runs on a web server and can be accessed by users through a web browser. A web application can be vulnerable to SQL injection attacks, which are a type of web application attack that exploit a vulnerability in a web application that allows an attacker to inject malicious SQL statements into an input field, such as a username or password field, and execute them on the database server. SQL injection can be used to bypass authentication, access or modify sensitive data, execute commands, etc. To exploit the web application and extract the user credentials from the moviescope database, one has to follow these steps:

Open a web browser and type www.moviescope.com

Press Enter key to access the web application.

Enter sam as username and test as password.

Click on Login button.

Observe that a welcome message with username sam is displayed.

Click on Logout button.

Enter sam' or `1'='1 as username and test as password.

Click on Login button.

Observe that a welcome message with username admin is displayed, indicating that SQL injection was successful.

Click on Logout button.

Enter sam'; SELECT * FROM users; ?as username and test as password.

Click on Login button.

Observe that an error message with user credentials from users table is displayed.

The user credentials from users table are:

| UID | Username | Password |
|---|---|---|
| 1 | admin | admin |
| 2 | sam | test |
| 3 | alice | alice123 |
| 4 | john | john123 |

The UID that is mapped to user john is 4

**NO.15** Kason, a forensic officer, was appointed to investigate a case where a threat actor has bullied certain children online. Before proceeding legally with the case, Kason has documented all the

supporting documents, including source of the evidence and its relevance to the case, before presenting it in front of the jury.
Which of the following rules of evidence was discussed in the above scenario?
**A.** Authentic
**B.** Understandable
**C.** Reliable
**D.** Admissible
***Answer:*** D
Explanation:
Admissible is the rule of evidence discussed in the above scenario. A rule of evidence is a criterion or principle that determines whether a piece of evidence can be used in a legal proceeding or investigation. Admissible is a rule of evidence that states that the evidence must be relevant, reliable, authentic, and understandable to be accepted by a court or a jury.Admissible also means that the evidence must be obtained legally and ethically, without violating any laws or rights. In the scenario, Kason has documented all the supporting documents, including source of the evidence and its relevance to the case, before presenting it in front of the jury, which means that he has followed the admissible rule of evidence. Authentic is a rule of evidence that states that the evidence must be original or verifiable as genuine and not altered or tampered with.
Understandable is a rule of evidence that states that the evidence must be clear and comprehensible to the court or jury and not ambiguous or confusing. Reliable is a rule of evidence that states that the evidence must be consistent and trustworthy and not based on hearsay or speculation.

**NO.16** Andre, a security professional, was tasked with segregating the employees' names, phone numbers, and credit card numbers before sharing the database with clients. For this purpose, he implemented a deidentification technique that can replace the critical information in database fields with special characters such as asterisks (*) and hashes (#).
Which of the following techniques was employed by Andre in the above scenario?
**A.** Tokenization
**B.** Masking
**C.** Hashing
**D.** Bucketing
***Answer:*** B
Explanation:
Masking is the technique that Andre employed in the above scenario. Masking is a deidentification technique that can replace the critical information in database fields with special characters such as asterisks (*) and hashes (#). Masking can help protect sensitive data from unauthorized access or disclosure, while preserving the format and structure of the original data.Tokenization is a deidentification technique that can replace the critical information in database fields with random tokens that have no meaning or relation to the original data. Hashing is a deidentification technique that can transform the critical information in database fields into fixed-length strings using a mathematical function. Bucketing is a deidentification technique that can group the critical information in database fields into ranges or categories based on certain criteria.

**NO.17** Initiate an SSH Connection to a machine that has SSH enabled in the network. After connecting to the machine find the file flag.txt and choose the content hidden in the file. Credentials

for SSH login are provided below:
Hint:
Username: sam
Password: admin@l23

**A.** sam@bob

**B.** bob2@sam

**C.** bob@sam

**D.** sam2@bob

***Answer:*** C

Explanation:
Quid pro quo is the social engineering technique that Johnson employed in the above scenario. Social engineering is a technique that involves manipulating or deceiving people into performing actions or revealing information that can be used for malicious purposes. Social engineering can be performed through various methods, such as phone calls, emails, websites, etc. Quid pro quo is a social engineering method that involves offering a service or a benefit in exchange for information or access. Quid pro quo can be used to trick victims into believing that they are receiving help or assistance from a legitimate source, while in fact they are compromising their security or privacy.In the scenario, Johnson performed quid pro quo by claiming himself to represent a technical support team from a vendor and offering to help sibertech.org with a server issue, while in fact he prompted the victim to execute unusual commands and install malicious files, which were then used to collect and pass critical information to Johnson's machine.
Diversion theft is a social engineering method that involves diverting the delivery or shipment of goods or assets to a different location or destination. Elicitation is a social engineering method that involves extracting information from a target by engaging them in a conversation or an interaction. Phishing is a social engineering method that involves sending fraudulent emails or messages that appear to come from a trusted source, such as a bank, a company, or a person, and asking the recipient to click on a link, open an attachment, or provide personal or financial information.