Eccouncil 312-50 Practice Questions

Shared by Avila on 17-08-2026

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

What is the algorithm used by LM for Windows2000 SAM?

Options:

A- MD4
B- DES
C- SHA
D- SSL

Answer:

B

Question 2

Question Type: MultipleChoice

A company's Web development team has become aware of a certain type of security vulnerability in their Web software. To mitigate the possibility of this vulnerability being exploited, the team wants to modify the software requirements to disallow users from entering HTML as input into their Web application.

What kind of Web application vulnerability likely exists in their software?

Options:

A- Cross-site scripting vulnerability
B- SQL injection vulnerability
C- Web site defacement vulnerability
D- Gross-site Request Forgery vulnerability

Answer:

A

Explanation:

There is no single, standardized classification of cross-site scripting flaws, but most experts distinguish between at least two primary flavors of XSS flaws: non-persistent and persistent. In this issue, we consider the non-persistent cross-site scripting vulnerability.

The non-persistent (or reflected) cross-site scripting vulnerability is by far the most basic type of web vulnerability. These holes show up when the data provided by a web client, most commonly in HTTP query parameters (e.g. HTML form submission), is used immediately by server-side scripts to parse and display a page of results for and to that user, without properly sanitizing the content.

Because HTML documents have a flat, serial structure that mixes control statements, formatting, and the actual content, any non-validated user-supplied data included in the resulting page without proper HTML encoding, may lead to markup injection. A classic example of a potential vector is a site search engine: if one searches for a string, the search string will typically be redisplayed verbatim on the result page to indicate what was searched for. If this response does not properly escape or reject HTML control characters, a cross-site scripting flaw will ensue.

Question 3

Question Type: MultipleChoice

Heather's company has decided to use a new customer relationship management tool. After performing the appropriate research, they decided to purchase a subscription to a cloud-hosted solution. The only administrative task that Heather will need to perform is the management of user accounts. The provider will take care of the hardware, operating system, and software administration including patching and monitoring. Which option best is this type of solution?

Options:

A- SaaS
B- IaaS
C- CaaS
D- PasS

Answer:

A

Explanation:

Software as a service (SaaS) allows users to attach to and use cloud-based apps over the web. Common examples ar email, calendaring and workplace tool (such as Microsoft workplace 365).

SaaS provides a whole software solution that you get on a pay-as-you-go basis from a cloud service provider. You rent the use of an app for your organisation and your users connect with it over the web, typically with an internet browser. All of the underlying infrastructure, middleware, app software system and app knowledge ar located within the service provider's knowledge center. The service provider manages the hardware and software system and with the appropriate service agreement, can make sure the availability and also the security of the app and your data as well. SaaS allows your organisation to induce quickly up and running with an app at token upfront cost.

Common SaaS scenarios

This tool having used a web-based email service like Outlook, Hotmail or Yahoo! Mail, then you have got already used a form of SaaS. With these services, you log into your account over the web, typically from an internet browser. the e-mail software system is found on the service provider's network and your messages ar hold on there moreover. you can access your email and hold on messages from an internet browser on any laptop or Internet-connected device.

The previous examples are free services for personal use. For organisational use, you can rent productivity apps, like email, collaboration and calendaring; and sophisticated business applications like client relationship management (CRM), enterprise resource coming up with (ERP) and document management. You buy the use of those apps by subscription or per the level of use.

Advantages of SaaS

Gain access to stylish applications. to supply SaaS apps to users, you don't ought to purchase, install, update or maintain any hardware, middleware or software system. SaaS makes even sophisticated enterprise applications, like ERP and CRM, affordable for organisations that lack the resources to shop for, deploy and manage the specified infrastructure and software system themselves.

Pay just for what you utilize. you furthermore may economize because the SaaS service automatically scales up and down per the level of usage.

Use free shopper software system. Users will run most SaaS apps directly from their web browser without needing to transfer and install any software system, though some apps need plugins. this suggests that you simply don't ought to purchase and install special software system for your users.

Mobilise your hands simply. SaaS makes it simple to ''mobilise'' your hands as a result of users will access SaaS apps and knowledge from any Internet-connected laptop or mobile device. You don't ought to worry concerning developing apps to run on differing types of computers and devices as a result of the service supplier has already done therefore. additionally, you don't ought to bring special experience aboard to manage the safety problems inherent in mobile computing. A fastidiously chosen service supplier can make sure the security of your knowledge, no matter the sort of device intense it.

Access app knowledge from anyplace. With knowledge hold on within the cloud, users will access their info from any Internet-connected laptop or mobile device. And once app knowledge is hold on within the cloud, no knowledge is lost if a user's laptop or device fails.

Question 4

Question Type: MultipleChoice

Lewis, a professional hacker, targeted the loT cameras and devices used by a target venture-capital firm. He used an information-gathering tool to collect information about the loT devices connected to a network, open ports and services, and the attack surface are

a. Using this tool, he also generated statistical reports on broad usage patterns and trends. This tool helped Lewis continually monitor every reachable server and device on the Internet, further allowing him to exploit these devices in the network. Which of the following tools was employed by Lewis in the above scenario?

Options:

A- Censys
B- Wapiti
C- NeuVector
D- Lacework

Answer:

A

Explanation:

Censys scans help the scientific community accurately study the Internet. The data is sometimes used to detect security problems and to inform operators of vulnerable systems so that they can fixed

Question 5

Question Type: MultipleChoice

While using your bank's online servicing you notice the following string in the URL bar:

''http: // www. MyPersonalBank. com/ account?id=368940911028389&Damount=10980&Camount=21''

You observe that if you modify the Damount & Camount values and submit the request, that data on the web page reflects the changes.

Which type of vulnerability is present on this site?

Options:

A- Cookie Tampering
B- SQL Injection
C- Web Parameter Tampering
D- XSS Reflection

Answer:

C

Question 6

Question Type: MultipleChoice

A security analyst is investigating a potential network-level session hijacking incident. During the investigation, the analyst finds that the attacker has been using a technique in which they injected an authentic-looking reset packet using a spoofed source IP address and a guessed acknowledgment number. As a result, the victim's connection was reset. Which of the following hijacking techniques has the attacker most likely used?

Options:

A- TCP/IP hijacking
B- UDP hijacking
C- RST hijacking
D- Blind hijacking

Explanation:
The attacker has most likely used RST hijacking, which is a type of network-level session hijacking technique that exploits the TCP reset (RST) mechanism. TCP reset is a way of terminating an established TCP connection by sending a packet with the RST flag set, indicating that the sender does not want to continue the communication. RST hijacking involves sending a forged RST packet to one or both ends of a TCP connection, using a spoofed source IP address and a guessed acknowledgment number, to trick them into believing that the other end has closed the connection.As a result, the victim's connection is reset and the attacker can take over the session or launch a denial-of-service attack12.
The other options are not correct for the following reasons:
A . TCP/IP hijacking: This option is a general term that refers to any type of network-level session hijacking technique that targets TCP/IP connections. RST hijacking is a specific type of TCP/IP hijacking, but not the only one.Other types of TCP/IP hijacking include SYN hijacking, source routing, and sequence prediction3.
B . UDP hijacking: This option is not applicable because UDP is a connectionless protocol that

does not use TCP reset mechanism. UDP hijacking is a type of network-level session hijacking technique that targets UDP connections, such as DNS or VoIP.UDP hijacking involves intercepting and modifying UDP packets to redirect or manipulate the communication between the sender and the receiver4.
D . Blind hijacking: This option is not accurate because blind hijacking is a type of network-level session hijacking technique that does not require injecting RST packets. Blind hijacking involves guessing the sequence and acknowledgment numbers of a TCP connection without being able to see the responses from the target.Blind hijacking can be used to inject malicious data or commands into an active TCP session, but not to reset the connection5.

Answer:

C

Explanation:

1: RST Hijacking - an overview | ScienceDirect Topics

2: TCP Reset Attack - an overview | ScienceDirect Topics

3: TCP/IP Hijacking - an overview | ScienceDirect Topics

4: UDP Hijacking - an overview | ScienceDirect Topics

5: Blind Hijacking - an overview | ScienceDirect Topics

Question 7

Question Type: MultipleChoice

You are a cybersecurity consultant for a healthcare organization that utilizes Internet of Medical Things (loMT) devices, such as connected insulin pumps and heart rate monitors, to provide improved patientcare. Recently, the organization has been targeted by ransomware attacks. While the IT infrastructure was unaffected due to robust security measures, they are worried that the loMT devices could be potential entry points for future

attacks. What would be your main recommendation to protect these devices from such threats?

Options:

A- Implement multi-factor authentication for all loMT devices.
B- Disable all wireless connectivity on loMT devices.
C- Use network segmentation to isolate loMT devices from the main network.

D- Regularly change the IP addresses of all loMT devices.
Explanation:
Internet of Medical Things (IoMT) devices are internet-connected medical devices that can collect, transfer, and analyze data over a network. They can provide improved patient care and comfort, but they also pose security challenges and risks, as they can be targeted by cyberattacks, such as ransomware, that can compromise their functionality, integrity, or confidentiality. Ransomware is a type of malware that encrypts the victim's data or system and demands a ransom for its decryption or restoration. Ransomware attacks can cause serious harm to healthcare organizations, as they can disrupt their operations, endanger their patients, and damage their reputation.
To protect IoMT devices from ransomware attacks, the main recommendation is to use network segmentation to isolate IoMT devices from the main network. Network segmentation is a technique that divides a network into smaller subnetworks, each with its own security policies and controls. Network segmentation can prevent or limit the spread of ransomware from one subnetwork to another, as it restricts the communication and access between them. Network segmentation can also improve the performance, visibility, and manageability of the network, as it reduces the network congestion, complexity, and noise.
The other options are not as effective or feasible as network segmentation. Implementing multi-factor authentication for all IoMT devices may not be possible or practical, as some IoMT devices may not support or require user authentication, such as sensors or monitors. Disabling all wireless connectivity on IoMT devices may not be desirable or realistic, as some IoMT devices rely on wireless communication protocols, such as Wi-Fi, Bluetooth, or Zigbee, to function or transmit data. Regularly changing the IP addresses of all IoMT devices may not prevent or deter ransomware attacks, as ransomware can target devices based on other factors, such as their domain names, MAC addresses, or vulnerabilities.Reference:
What Is Internet of Medical Things (IoMT) Security?
5 Steps to Secure Internet of Medical Things Devices
Ransomware in Healthcare: How to Protect Your Organization
[Network Segmentation: Definition, Benefits, and Best Practices]

Answer:

C

Question 8

Question Type: MultipleChoice

Eric, a cloud security engineer, implements a technique for securing the cloud resources used by his organization. This technique assumes by default that a user attempting to access the network is not an authentic entity and verifies every incoming connection before allowing access to the network. Using this technique, he also imposed conditions such that employees can access only the resources required for their role.

What is the technique employed by Eric to secure cloud resources?

Options:

A- Serverless computing
B- Demilitarized zone
C- Container technology
D- Zero trust network

Answer:

D

Explanation:

Zero Trust Networks The Zero Trust model is a security implementation that by default assumes every user trying to access the network is not a trusted entity and verifies every incoming connection before allowing access to the network.It strictly follows the principle, ''Trust no one and validate before providing a cloud service or granting access permission.''It also allows companies to impose conditions, such as allowing employees to only access the appropriate resources required for their work role. (P.2997/2981)

Zero Trust is a strategic initiative that helps prevent successful data breaches by eliminating the concept of trust from an organization's network architecture. Rooted in the principle of ''never trust, always verify,'' Zero Trust is designed to protect modern digital environments by leveraging network segmentation, preventing lateral movement, providing Layer 7 threat prevention, and simplifying granular user-access control.

Question 9

Question Type: MultipleChoice

You work for Acme Corporation as Sales Manager. The company has tight network security restrictions. You are trying to steal data from the company's Sales database (Sales.xls) and transfer them to your home computer. Your company filters and monitors traffic that leaves from the internal network to the Internet. How will you achieve this without raising suspicion?

Options:

A- Encrypt the Sales.xls using PGP and e-mail it to your personal gmail account
B- Package the Sales.xls using Trojan wrappers and telnet them back your home computer
C- You can conceal the Sales.xls database in another file like photo.jpg or other files and send it out in an innocent looking email or file transfer using Steganography techniques
D- Change the extension of Sales.xls to sales.txt and upload them as attachment to your hotmail account

Answer:

C

Question 10

Question Type: MultipleChoice

What does the --oX flag do in an Nmap scan?

Options:

A- Perform an eXpress scan
B- Output the results in truncated format to the screen
C- Output the results in XML format to a file
D- Perform an Xmas scan

Answer:

C

Explanation:

https://nmap.org/book/man-output.html

-oX <filespec> - Requests that XML output be directed to the given filename.

Incorrect answers:

Run an express scanhttps://nmap.org/book/man-port-specification.html

There is no express scan in Nmap, but there is a fast scan.

-F (Fast (limited port) scan)

Specifies that you wish to scan fewer ports than the default. Normally Nmap scans the most common 1,000 ports for each scanned protocol. With -F, this is reduced to 100.

Or we can influence the intensity (and speed) of the scan with the -T flag.https://nmap.org/book/man-performance.html

-T paranoid|sneaky|polite|normal|aggressive|insane

Output the results in truncated format to the screenhttps://nmap.org/book/man-output.html

-oG <filespec> (grepable output)

It is a simple format that lists each host on one line and can be trivially searched and parsed with standard Unix tools such as grep, awk, cut, sed, diff, and Perl.

Run a Xmas scanhttps://nmap.org/book/man-port-scanning-techniques.html

Xmas scan (-sX)

Sets the FIN, PSH, and URG flags, lighting the packet up like a Christmas tree.