Vendor: EC-Council

Exam Code: 312-50v13

Exam Name: Certified Ethical Hacker Exam (CEH v13)

Version: DEMO

QUESTION 1
A security consultant is conducting an authorized assessment for a healthcare billing provider in Phoenix, Arizona. While monitoring internal traffic, he observes an authenticated employee interacting with a sensitive web-based management portal over TCP.

During the session, the consultant carefully crafts and injects packets into the ongoing communication stream. Shortly afterward, the legitimate user experiences irregular responses from the application, and the server begins processing commands originating from the consultant's injected traffic as though they were part of the established session.

The technique does not involve credential guessing or forcing the user to reauthenticate. Instead, it targets the communication channel already in progress.

From a network-level perspective, what type of session hijacking technique is being demonstrated?

A. UDP Hijacking
B. RST Hijacking
C. Blind Hijacking
D. TCP/IP Hijacking

Answer: D
Explanation:
The scenario describes injecting crafted packets into an already established TCP session so that the server accepts them as part of the ongoing communication without requiring reauthentication. This behavior reflects TCP/IP hijacking, where an attacker manipulates or injects traffic within an active TCP session to take control of or influence the communication stream.

QUESTION 2
At Redwood Financial Group in Boston, Massachusetts, the security leadership team is formalizing a continual security strategy composed of four coordinated activities. During implementation planning, one team is assigned responsibility for reviewing operational data across the enterprise environment to recognize irregular patterns that may indicate malicious activity. Within this model, which activity is responsible for this responsibility?

A. Predict
B. Protect
C. Respond
D. Detect

Answer: D
Explanation:
This activity focuses on continuously analyzing operational data to identify anomalies and indicators of malicious behavior. In a security operations lifecycle, this corresponds to detection, where monitoring systems and analytics are used to recognize suspicious patterns and potential threats within the environment.

QUESTION 3
FILL BLANK

Scenario

Instructions

You have been hired as a part of the Red Team at CEHORG, an IT and ITES organization that deals with advanced research and development in the field of information security. It has offices all over the country connected in real-time by its network infrastructure.

Your organization is worried about rising cybersecurity incidents and has entrusted you with a comprehensive security audit of the complete infrastructure.

CEHORG's internal network consists of several subnets housing various organizational units like any large organization. The front office is connected to a separate subnet that connects to the company's public-facing computers. The company has installed multiple kiosks to help customers understand their products and services. The front office also has Wi-Fi connectivity to cater to the users who carry their smartphones and laptops.

The CEHORG's internal network is made up of Militarized and Demilitarized zones. As a security precaution and by design, all the internal resource zones are configured with different subnet IPs. The militarized zone houses the application servers that provide application frameworks for various departments. The Demilitarized Zone contains public-facing systems of the organization, such as web and mail servers. The headquarters' network topology and protocols are replicated worldwide in all its satellite offices for efficient communication with the headquarters.

Description

CEH Practical exam presents you with 20 challenges built on the ethical hacking domains covered in the C|EH program. The exam hosts multiple hidden machines, each containing a set of vulnerable applications and services. You must apply your knowledge and skills in various ethical hacking domains and solve the challenges. The exam duration is 6 hours. Each challenge in CEH Practical weighs 10 points, and you are required to solve a minimum of 14 challenges out of 20, which would sum up to 140 points, to become a CEH (Practical) Credential Holder.

On the cyber range, you will have access to Ethical Hacker Workstations, **EH Workstation - 1** and **EH Workstation - 2**. **EH Workstation - 1** is a Parrot Security machine and **EH Workstation - 2** is a Windows 11 machine. You can switch to these machines from the Resources tab.

Please note that there are a maximum of 3 attempts for each challenge.

Available target networks:

10.10.55.0/24
192.168.44.0/24
192.168.200.0/24

Exclusions:

10.10.55.1, 10.10.55.2
192.168.44.1, 192.168.44.2
192.168.200.1, 192.168.200.2

The credentials to access **EH Workstation - 1** (Parrot Security) machine are as below:

Username: attacker **Password**: toor

The credentials to access **EH Workstation - 2** (Windows 11) are as below:

Username: Admin **Password:** Pa$$w0rd

The credentials to access **OpenVAS** on **EH Workstation - 1** (Parrot Security) machine are as below:

Username: admin **Password:** password

To open **OpenVAS** tool, click **Applications** at the top of the **Desktop** window and navigate to **Pentesting → Vulnerability Analysis → Openvas - Greenbone → Start Greenbone Vulnerability Manager Service** to launch **OpenVAS** tool.

Note: You can use username.txt and password.txt available on the Desktop of the **EH Workstation - 1** (Parrot Security) machine for any credentials/password cracking attempt.

Flags

Challenge:

You are assigned to investigate a large-scale DDoS attack targeting the IP address 172.22.10.10. The objective is to analyze the network traffic to identify the malicious packets involved and determine the IP address of the attacker machine running Windows as its operating system. The network capture file, Mystic-capture.pcapng, is located in the Documents directory of the “EH Workstation - 2” (Windows 11) machine. (Format: NN*NN*NN*NN)

Answer: 10.10.55.11

QUESTION 4
FILL BLANK

Scenario

Instructions

You have been hired as a part of the Red Team at CEHORG, an IT and ITES organization that deals with advanced research and development in the field of information security. It has offices all over the country connected in real-time by its network infrastructure.

Your organization is worried about rising cybersecurity incidents and has entrusted you with a comprehensive security audit of the complete infrastructure.

CEHORG’s internal network consists of several subnets housing various organizational units like any large organization. The front office is connected to a separate subnet that connects to the company’s public-facing computers. The company has installed multiple kiosks to help customers understand their products and services. The front office also has Wi-Fi connectivity to cater to the users who carry their smartphones and laptops.

The CEHORG's internal network is made up of Militarized and Demilitarized zones. As a security precaution and by design, all the internal resource zones are configured with different subnet IPs. The militarized zone houses the application servers that provide application frameworks for various departments. The Demilitarized Zone contains public-facing systems of the organization, such as web and mail servers. The headquarters’ network topology and protocols are replicated worldwide in all its satellite offices for efficient communication with the headquarters.

Description

CEH Practical exam presents you with 20 challenges built on the ethical hacking domains covered in the C|EH program. The exam hosts multiple hidden machines, each containing a set

of vulnerable applications and services. You must apply your knowledge and skills in various ethical hacking domains and solve the challenges. The exam duration is 6 hours. Each challenge in CEH Practical weighs 10 points, and you are required to solve a minimum of 14 challenges out of 20, which would sum up to 140 points, to become a CEH (Practical) Credential Holder.

On the cyber range, you will have access to Ethical Hacker Workstations, **EH Workstation - 1** and **EH Workstation - 2**. **EH Workstation - 1** is a Parrot Security machine and **EH Workstation - 2** is a Windows 11 machine. You can switch to these machines from the Resources tab.

Please note that there are a maximum of 3 attempts for each challenge.

Available target networks:

10.10.55.0/24
192.168.44.0/24
192.168.200.0/24

Exclusions:

10.10.55.1, 10.10.55.2
192.168.44.1, 192.168.44.2
192.168.200.1, 192.168.200.2

The credentials to access **EH Workstation - 1** (Parrot Security) machine are as below:

Username: attacker **Password**: toor

The credentials to access **EH Workstation - 2** (Windows 11) are as below:

Username: Admin **Password:** Pa$$w0rd

The credentials to access **OpenVAS** on **EH Workstation - 1** (Parrot Security) machine are as below:

Username: admin **Password:** password

To open **OpenVAS** tool, click **Applications** at the top of the **Desktop** window and navigate to **Pentesting → Vulnerability Analysis → Openvas - Greenbone → Start Greenbone Vulnerability Manager Service** to launch **OpenVAS** tool.

Note: You can use username.txt and password.txt available on the Desktop of the **EH Workstation - 1** (Parrot Security) machine for any credentials/password cracking attempt.

Flags

Challenge:

You are assigned to extract the password of a user, Matthew, from a web application, cinema.cehorg.com, which is vulnerable to an SQL injection attack. Note: You have already registered on the website with the credentials Sarah/abc123. (Format: NNNNNNNN)

Answer: 12345678

QUESTION 5
Anthony works as a security consultant for a financial services firm in Chicago, Illinois. During an

internal engagement, he reviews traffic logs and observes repeated connection attempts to a service that appears to provide directory-related information beyond a single domain. The responses suggest that the underlying database contains entries representing objects across the entire organization rather than being limited to a single segment.

As Anthony continues his assessment, he notices that administrators commonly connect to this service when troubleshooting directory-related issues. The service listens on a dedicated port and allows object searches across multiple domains without requiring prior knowledge of the specific domain name. Which service is Anthony most likely enumerating?

A. Microsoft RPC Endpoint Mapper (TCP/UDP 135)
B. Global Catalog Service (TCP/UDP 3268)
C. Lightweight Directory Access Protocol (TCP/UDP 389)
D. Session Initiation Protocol (TCP/UDP 5060, 5061)

Answer: B
Explanation:
The Global Catalog Service provides a forest-wide directory that contains partial replicas of all objects across multiple domains, enabling searches without requiring specific domain targeting. It is commonly used in Active Directory environments for cross-domain queries and troubleshooting, and it listens on a dedicated port designed for directory-wide enumeration.

QUESTION 6
A city utility billing portal in Raleigh, North Carolina includes a search field used to retrieve customer records. During an authorized penetration test, an assessor submits repeated instances of a character commonly interpreted within SQL statements as part of the input value.

The application does not display detailed error messages, yet certain submissions result in irregular response behavior and partial rendering of results. The tester suspects the input may be affecting how the SQL command is internally constructed.

Which black-box testing technique is being applied?

A. Sending special characters to detect SQL modification behavior
B. Sending arbitrary data to detect truncation issues
C. Using right square bracket characters to detect identifier handling issues
D. Sending isolated quotation characters to detect unsanitized input

Answer: D
Explanation:
The tester is injecting a single character that is commonly used to terminate or alter SQL string boundaries, such as a quotation mark. Observing changes in application behavior or response structure without error visibility indicates attempts to detect whether user input is properly sanitized or escaped, which is characteristic of testing for unsanitized input through quote-based SQL injection probing.

QUESTION 7
A security consultant is performing an authorized assessment of a regional healthcare provider's patient portal in Portland, Oregon. During testing, he observes that authenticated users are assigned session identifiers embedded within URL parameters after login.

To evaluate the robustness of the session management implementation, he initiates multiple authentication requests in rapid succession using controlled test accounts. He then compares the

issued identifiers and notices that although parts of the value remain constant, certain segments change in a predictable progression over time.

By analyzing the incremental pattern across a controlled batch of issued identifiers generated within the same time window, he is able to anticipate future valid identifiers without capturing traffic from other users.

Which token prediction mechanism best explains the weakness identified in this scenario?

A. Small Token Space
B. Timestamp-based Tokens
C. Seguential Tokens
D. Weak Random Number Generator (PRNG)

Answer: C
Explanation:
The scenario describes session identifiers that change in a predictable progression over time, allowing an attacker to anticipate future values. This behavior is characteristic of sequential token generation, where identifiers are produced in an incremental or partially deterministic sequence rather than being securely randomized.

QUESTION 8
During an executive-level incident review at HarborTech Industries in Baltimore, Maryland, analysts categorize key elements of a recent intrusion. They identify the organization that orchestrated the attack, document the malicious infrastructure used to reach internal systems, outline the technical approach employed to exploit weaknesses, and specify which internal business unit was affected. Within the Diamond Model of Intrusion Analysis, which element represents the technical approach used to carry out the attack?

A. Adversary
B. Infrastructure
C. Capability
D. Victim

Answer: C
Explanation:
In the Diamond Model of Intrusion Analysis, the capability element represents the tools, techniques, or methods used by the adversary to execute the attack. It describes how the intrusion is carried out from a technical standpoint, including exploits, malware, or procedures applied during the operation.

QUESTION 9
A regional hospital network is conducting incident containment after discovering that an internal file server was accessed by unauthorized actors. While forensic analysis is ongoing, a security engineer must immediately protect sensitive medical records stored on a mounted partition without shutting down the system.

The solution must support strong encryption (including 256-bit AES), allow creation of encrypted containers within existing storage volumes, and provide the capability to conceal protected data inside standard-looking volumes to reduce visibility during continued investigation.

Select the disk encryption tool that best satisfies these operational and security requirements.

A. FileVault
B. Rohos Disk Encryption
C. VeraCrypt
D. BitLocker Drive Encryption

Answer: C
Explanation:
VeraCrypt supports strong encryption such as AES-256, allows creation of encrypted containers within existing volumes, and provides hidden volumes inside standard encrypted containers to conceal sensitive data. This combination enables both protection and plausible deniability while keeping the system operational during incident response.

QUESTION 10
An internal review at a financial analytics firm in Minneapolis, Minnesota, uncovered unusual query patterns directed at the company's directory services infrastructure. Security engineer Olivia Grant examined the logs and discovered that a user account had been issuing structured directory queries to retrieve lists of user objects, group memberships, and organizational units.

Further inspection revealed that the account was able to access information about privileged groups containing the word "Admin" in their titles. The activity did not involve password guessing or authentication bypass, but rather systematic directory lookups to map internal user and group relationships.

What type of enumeration is illustrated in this scenario?

A. VoIP Enumeration
B. LDAP Enumeration
C. SMTP Enumeration
D. DNS Enumeration

Answer: B
Explanation:
The activity involves structured queries against directory services to retrieve user objects, group memberships, and organizational units, which is characteristic of LDAP enumeration. This technique leverages directory queries to map internal identity structures and identify privileged groups without bypassing authentication.

QUESTION 11
During an authorized security assessment of a smart thermostat manufacturer in Denver, Colorado, a certified ethical hacker receives a firmware image extracted from a production device for further evaluation.

The tester begins by examining the binary file to determine its format and architecture. Basic inspection commands are executed against the image to review embedded human-readable content and observe low-level binary structure before proceeding with deeper analysis.

Within the firmware analysis workflow, which stage is the tester performing?

A. Extract the Filesystem
B. Obtain Firmware
C. Analyze Firmware
D. Emulate Firmware

Answer: C
Explanation:
The tester is inspecting the firmware image using analysis commands to identify its structure, format, and embedded content. This corresponds to the firmware analysis stage, where the extracted firmware is examined at a low level to understand its composition before deeper actions like extraction or emulation are performed.

QUESTION 12
A fintech startup in Austin, Texas authorizes a controlled red team engagement to evaluate the resilience of its web-based loan management platform. At the outset of the engagement, the assessment team concentrates on developing a structural understanding of the application.

They examine publicly exposed endpoints, observe server responses under different navigation paths, identify accessible directories, and document the relationships between client-side scripts, form parameters, and backend behaviors. Error handling patterns and response variations are cataloged to understand how user interactions are processed across various components of the platform.

The collected information is used to guide strategic planning for subsequent phases of the engagement.

Within the web application hacking methodology, which phase is most accurately demonstrated in this scenario?

A. Maintaining Access
B. Scanning
C. Gaining Access
D. Reconnaissance

Answer: B
Explanation:
The activity focuses on actively interacting with the application to identify endpoints, directories, parameters, and response behaviors while mapping how the system behaves. This corresponds to the scanning phase, where structured probing is used to analyze application structure and discover attack surfaces for later exploitation planning.

QUESTION 13
A DevOps engineer at a Toronto-based SaaS provider deploys a multi-tenant application within a shared orchestration environment. During a security assessment, a penetration tester discovers that a compromised workload is able to access host-level system resources and interact with adjacent workloads beyond its intended isolation controls.

Further investigation reveals that the workload was launched with elevated privileges and insufficient runtime restrictions, allowing the attacker to cross the intended isolation boundary and gain unauthorized access to the underlying infrastructure.

Which cloud attack technique best describes this security weakness?

A. Man-in-the-Cloud Attack
B. Side-Channel Attack
C. Container Escape
D. Golden SAML Attack

Answer: C
Explanation:
The scenario describes a compromised workload breaking out of its isolated environment and accessing host-level resources and other workloads. This indicates a failure of container isolation controls, which is characteristic of a container escape attack where an attacker leverages excessive privileges or runtime misconfiguration to break out of the container boundary and access the underlying host system.

QUESTION 14
Natalie Brooks is leading an authorized red team exercise for Sentinel Networks in Seattle. While briefing her team on different attacker profiles, she describes an individual who is new to cybersecurity, actively learning techniques through online communities, and experimenting with basic tools on low-risk targets to build practical skills without causing significant damage. Which hacker class best matches this profile?

A. Blue Hat hacker
B. Green Hat hacker
C. Gray Hat hacker
D. Red Hat hacker

Answer: B
Explanation:
A Green Hat hacker is typically a beginner in cybersecurity who is still learning and experimenting with tools and techniques. They often explore basic targets in low-risk environments to build skills and gain experience without advanced malicious intent or professional-level expertise.

QUESTION 15
During a red team assessment of a mid-sized insurance provider in Denver, Colorado, testers established persistent access on an internal developer workstation after exploiting a misconfigured automation service. To sustain command-and-control without triggering perimeter defenses, they configured a low-bandwidth outbound channel designed to blend into infrastructure traffic that is routinely permitted through egress controls.

Security operations later identified periodic outbound communication from the compromised host to a single unfamiliar external endpoint not associated with approved vendors or user activity. The traffic was distributed over time rather than bursty. Although the exchanges resembled legitimate service requests, packet inspection revealed irregular payload sizing and structured encoding patterns inconsistent with typical client behavior across the environment.

What covert communication technique was most likely used to sustain the red team's access?

A. ICMP Tunneling
B. TCP Sequence Tunneling
C. HTTR/S Tunneling
D. DNS Tunneling

Answer: D
Explanation:
The scenario describes low-bandwidth, periodic outbound communication to an external endpoint with structured encoding and traffic designed to blend into normal permitted egress traffic. This pattern is most consistent with DNS tunneling, where data is covertly encoded within DNS queries and responses to bypass network defenses and maintain command-and-control

communication.

QUESTION 16
A subscription-based analytics platform in Portland, Oregon provides enterprise clients with API access to project dashboards. Each dashboard is associated with a unique identifier included in client-side API requests when retrieving project data.

While evaluating access controls, a security analyst signs in using a standard user account and captures a legitimate API request used to retrieve a specific project dashboard. By altering only the identifier value within the request and replaying it through the same authenticated session, the analyst receives data belonging to a different client organization.

The session remains valid, and no elevated privileges are granted. The behavior indicates that access validation does not adequately verify whether the requesting user is authorized to access the referenced resource.

Identify the OWASP API security risk illustrated in this scenario.

A. Broken Object Level Authorization (BOLA)
B. Broken Object Property Level Authorization
C. Broken Function Level Authorization
D. Broken Authentication

Answer: A
Explanation:
The issue occurs when changing an object identifier in an authenticated request allows access to another organization's data without proper authorization checks. This reflects Broken Object Level Authorization, where the system fails to verify whether the user is permitted to access the specific resource being requested, even though authentication itself is valid.

QUESTION 17
A technology consulting firm in Charlotte, North Carolina experienced a targeted intrusion after an employee interacted with a carefully crafted phishing email. Security analysts reconstructed the sequence of events and determined that once the email attachment was opened, built-in scripting utilities were invoked to inject malicious instructions into an active system process.

No standalone malicious executables were discovered on disk. The injected instructions began running directly inside legitimate processes before any registry modifications or task scheduling changes were observed.

At this point in the attack sequence, which operational phase of the fileless attack lifecycle is being demonstrated?

A. Persistence
B. Point of Entry
C. Achieving Objectives
D. Code Execution

Answer: D
Explanation:
The scenario describes malicious instructions being executed directly in memory within legitimate processes after the phishing attachment is opened, without any on-disk artifacts or persistence mechanisms yet established. This corresponds to the code execution phase of a fileless attack

lifecycle, where the payload is actively running in a compromised process.

QUESTION 18
An enterprise collaboration platform used by a pharmaceutical distributor in Boston, Massachusetts relies on a centralized identity store to validate employee credentials. While reviewing the authentication workflow, a security tester notices that user-provided values are directly embedded into backend lookup expressions responsible for locating account records.

When specific logical operators and wildcard characters are introduced into the username field, the application's record-matching behavior changes. Instead of evaluating a single identity entry, the backend process begins matching a broader set of records than intended, altering the outcome of the authentication check.

The issue arises from improper handling of input within directory-based search logic.

From the following options, identify the injection technique illustrated in this scenario.

A. LDAP Injection
B. OS Command Injection
C. SQL Injection
D. XPath Injection

Answer: A
Explanation:
The scenario describes user input being inserted into directory lookup expressions against a centralized identity store, and the use of logical operators and wildcards altering how account records are matched. This behavior is characteristic of LDAP injection, where manipulation of directory search filters affects authentication and identity resolution logic.

QUESTION 19
At a biomedical analytics firm in Raleigh, North Carolina, security consultant Marcus Ellison was reviewing exposed services on a legacy Linux host located in a screened subnet. While mapping available services, he observed that the machine was responding to time synchronization queries from multiple internal systems.

Curious whether the service might reveal additional intelligence, Marcus issued targeted queries against the time service and received responses that exposed internal client addresses and system identifiers interacting with it. The information provided unexpected visibility into internal network structure without requiring authentication.

From the available options, what enumeration technique is illustrated in this scenario?

A. NFS Enumeration
B. NetBIOS Enumeration
C. SNMP Enumeration
D. NTP Enumeration

Answer: D
Explanation:
The activity involves querying a time synchronization service and receiving responses that include client and system details from systems interacting with it. This aligns with NTP enumeration, where time service responses can leak network information such as connected hosts and internal identifiers.

QUESTION 20
During an internal security review at a transportation authority in Columbus, Ohio, a red team analyst positioned himself on the same local network segment as several domain-joined administrative workstations. Over several hours, he recorded authentication exchanges as legitimate users performed their routine logon activities across the network. He later analyzed the captured traffic to recover valid credentials associated with privileged accounts. Based on the attacker's actions, how should this password attack be classified?

A. Passive Online Attack
B. Non-Electronic Attack
C. Active Online Attack
D. Offline Attack

Answer: A
Explanation:
The attacker is silently capturing authentication traffic on the same network segment without interacting with the authentication system or attempting repeated login attempts. The credentials are obtained by passively observing and analyzing network communications rather than actively engaging the target system, which characterizes a passive online attack.

QUESTION 21
During an authorized engagement at IronClad Financial Services in Charlotte, the red team successfully exploits a weakness and obtains administrative access to a critical server. After achieving this objective, the team installs a backdoor mechanism to ensure continued access even if the original vulnerability is remediated. The team documents this activity as part of demonstrating long-term adversary behavior within the approved scope. Within the CEH ethical hacking framework, which phase does this activity represent?

A. Reconnaissance
B. Vulnerability Scanning
C. Maintaining Access
D. Clearing Tracks

Answer: C
Explanation:
Installing a backdoor after gaining administrative access is a classic method used to preserve access to a compromised system over time. This activity corresponds to maintaining access, where persistence mechanisms are established to ensure continued control after the initial exploitation phase.

Thank You for Trying Our Product

Lead2pass Certification Exam Features:

★ More than **99,900** Satisfied Customers Worldwide.

★ Average **99.9%** Success Rate.

★ **Free Update** to match latest and real exam scenarios.

★ **Instant Download** Access! No Setup required.

★ Questions & Answers are downloadable in **PDF** format and **VCE** test engine format.

★ Multi-Platform capabilities - **Windows, Laptop, Mac, Android, iPhone, iPod, iPad**.

★ **100%** Guaranteed Success or **100%** Money Back Guarantee.

★ **Fast**, helpful support **24x7**.

View list of all certification exams: http://www.lead2pass.com/all-products.html

10% Discount Coupon Code: **ASTR14**