312-50V12 Q&As

Certified Ethical Hacker Exam (CEHv12)

Pass EC-COUNCIL 312-50V12 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.geekcert.com/312-50v12.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by EC-COUNCIL Official Exam Center

- **Instant Download** After Purchase
- **100% Money Back** Guarantee
- **365 Days** Free Update
- **800,000+** Satisfied Customers

QUESTION 1

Gilbert, a web developer, uses a centralized web API to reduce complexity and increase the Integrity of updating and changing data. For this purpose, he uses a web service that uses HTTP methods such as PUT. POST. GET. and DELETE and can improve the overall performance, visibility, scalability, reliability, and portability of an application. What is the type of web-service API mentioned in the above scenario?

A. JSON-RPC

B. SOAP API

C. RESTful API

D. REST API

Correct Answer: C

*REST is not a specification, tool, or framework, but instead is an architectural style for web services that serves as a communication medium between various systems on the web. *RESTful APIs, which are also known as RESTful services, are designed using REST principles and HTTP communication protocols RESTful is a collection of resources that use HTTP methods such as PUT, POST, GET, and DELETE

RESTful API: RESTful API is a RESTful service that is designed using REST principles and HTTP communication protocols. RESTful is a collection of resources that use HTTP methods such as PUT, POST, GET, and DELETE. RESTful API is also designed to make applications independent to improve the overall performance, visibility, scalability, reliability, and portability of an application. APIs with the following features can be referred to as to RESTful APIs: o Stateless: The client end stores the state of the session; the server is restricted to save data during the request processing o Cacheable: The client should save responses (representations) in the cache. This feature can enhance API performance pg. 1920 CEHv11 manual.

https://cloud.google.com/files/apigee/apigee-web-api-design-the-missing-link-ebook.pdf

The HTTP methods GET, POST, PUT or PATCH, and DELETE can be used with these templates to read, create, update, and delete description resources for dogs and their owners. This API style has become popular for many reasons. It is straightforward and intuitive, and learning this pattern is similar to learning a programming language API. APIs like this one are commonly called RESTful APIs, although they do not display all of the characteristics that define REST (more on REST later).

QUESTION 2

Becky has been hired by a client from Dubai to perform a penetration test against one of their remote offices. Working from her location in Columbus, Ohio, Becky runs her usual reconnaissance scans to obtain basic information about their network. When analyzing the results of her Whois search, Becky notices that the IP was allocated to a location in Le Havre, France. Which regional Internet registry should Becky go to for detailed information?

A. ARIN

B. APNIC

C. RIPE

D. LACNIC

Correct Answer: C

Regional Internet Registries (RIRs):

ARIN (American Registry for Internet Numbers)

AFRINIC (African Network Information Center)

APNIC (Asia Pacific Network Information Center)

RIPE (Réseaux IP Européens Network Coordination Centre)

LACNIC (Latin American and Caribbean Network Information Center)

QUESTION 3

This TCP flag instructs the sending system to transmit all buffered data immediately.

A. SYN

B. RST

C. PSH

D. URG

E. FIN

Correct Answer: C

QUESTION 4

Bobby, an attacker, targeted a user and decided to hijack and intercept all their wireless communications. He installed a fake communication tower between two authentic endpoints to mislead the victim. Bobby used this virtual tower to interrupt the data transmission between the user and real tower, attempting to hijack an active session, upon receiving the users request. Bobby manipulated the traffic with the virtual tower and redirected the victim to a malicious website. What is the attack performed by Bobby in the above scenario?

A. Wardriving

B. KRACK attack

C. jamming signal attack

D. aLTEr attack

Correct Answer: D

aLTEr attacks are usually performed on LTE devices Attacker installs a virtual (fake) communication tower between two authentic endpoints intending to mislead the victim This virtual tower is used to interrupt the data transmission between

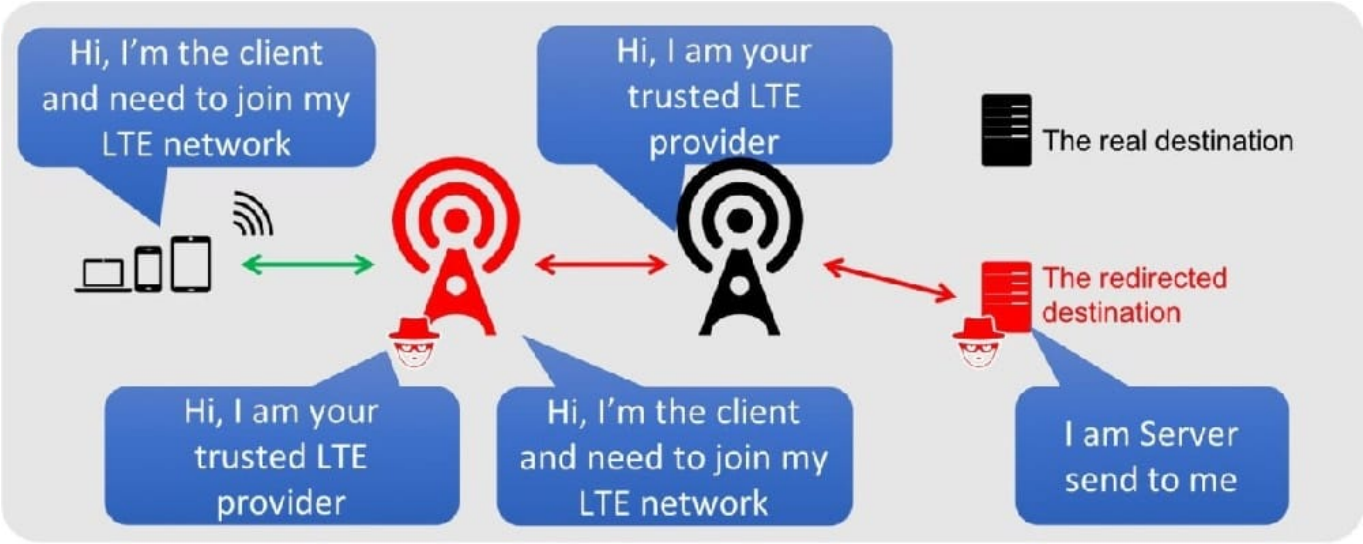
the user and real tower attempting to hijack the active session.

https://alter-attack.net/media/breaking_lte_on_layer_two.pdf The new aLTEr attack can be used against nearly all LTE connected endpoints by intercepting traffic and redirecting it to malicious websites together with a particular approach for

Apple iOS devices.

This attack works by taking advantage of a style flaw among the LTE network -- the information link layer (aka: layer-2) of the LTE network is encrypted with AES-CTR however it\\'s not integrity-protected, that is why an offender will modify the

payload. As a result, the offender is acting a classic man-in-the-middle wherever they\\'re movement as a cell tower to the victim.



QUESTION 5

Attacker Lauren has gained the credentials of an organization\\'s internal server system, and she was often logging in during irregular times to monitor the network activities. The organization was skeptical about the login times and appointed security professional Robert to determine the issue. Robert analyzed the compromised device to find incident details such as the type of attack, its severity, target, impact, method of propagation, and vulnerabilities exploited. What is the incident handling and response (IHandR) phase, in which Robert has determined these issues?

A. Preparation

B. Eradication

C. Incident recording and assignment

D. Incident triage

Correct Answer: D

Triage is that the initial post-detection incident response method any responder can execute to open an event or false positive. Structuring an efficient and correct triage method can reduce analyst fatigue, reduce time to reply to and right

incidents, and ensure that solely valid alerts are promoted to "investigation or incident" status.

Every part of the triage method should be performed with urgency, as each second counts once in the inside of a crisis.

However, triage responders face the intense challenge of filtering an unwieldy input supply into a condensed trickle of

events. Here are some suggestions for expediting analysis before knowledge is validated:

Organization: reduce redundant analysis by developing a workflow that may assign tasks to responders. Avoid sharing an email box or email alias between multiple responders. Instead use a workflow tool, like those in security orchestration,

automation, and response (SOAR) solutions, to assign tasks. Implement a method to re-assign or reject tasks that are out of scope for triage. Correlation: Use a tool like a security info and even management (SIEM) to mix similar events. Link

potentially connected events into one useful event. Data Enrichment: automate common queries your responders perform daily, like reverse DNS lookups, threat intelligence lookups, and IP/domain mapping. Add this knowledge to the event

record or make it simply accessible. Moving full speed ahead is that the thanks to get through the initial sorting method however a a lot of detailed, measured approach is necessary throughout event verification. Presenting a robust case to be

accurately evaluated by your security operations center (SOC) or cyber incident response team (CIRT) analysts is key. Here are many tips for the verification:

Adjacent Data: Check the data adjacent to the event. for example, if an end has a virus signature hit, look to visualize if there\\'s proof the virus is running before career for more response metrics. Intelligence Review: understand the context

around the intelligence. simply because an ip address was flagged as a part of a botnet last week doesn\\'t mean it still is an element of a botnet today. Initial Priority: Align with operational incident priorities and classify incidents appropriately.

ensure the right level of effort is applied to every incident. Cross Analysis: look for and analyze potentially shared keys, like science addresses or domain names, across multiple knowledge sources for higher knowledge acurity.