312-50V11$^{\text{Q\&As}}$

Certified Ethical Hacker v11 Exam

Pass EC-COUNCIL 312-50V11 Exam with 100% Guarantee

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

QUESTION 1

Dorian Is sending a digitally signed email to Polly, with which key is Dorian signing this message and how is Poly validating It?

A. Dorian is signing the message with his public key. and Poly will verify that the message came from Dorian by using Dorian\\'s private key.

B. Dorian Is signing the message with Polys public key. and Poly will verify that the message came from Dorian by using Dorian\\'s public key.

C. Dorian is signing the message with his private key. and Poly will verify that the message came from Dorian by using Dorian\\'s public key.

D. Dorian is signing the message with Polys private key. and Poly will verify mat the message came from Dorian by using Dorian\\'s public key.

Correct Answer: C

QUESTION 2

Jason, an attacker, targeted an organization to perform an attack on its Internet-facing web server with the intention of gaining access to backend servers, which are protected by a firewall. In this process, he used a URL https://xyz.com/feed.php?url:externalsile.com/feed/to to obtain a remote feed and altered the URL input to the local host to view all the local resources on the target server. What is the type of attack Jason performed In the above scenario?

A. website defacement

B. Server-side request forgery (SSRF) attack

C. Web server misconfiguration

D. web cache poisoning attack

Correct Answer: B

Server-side request forgery (also called SSRF) is a net security vulnerability that allows an assaulter to induce the server-side application to make http requests to associate arbitrary domain of the attacker\\'s choosing. In typical SSRF examples, the attacker might cause the server to make a connection back to itself, or to other web-based services among the organization\\'s infrastructure, or to external third-party systems. Another type of trust relationship that often arises with server-side request forgery is where the application server is able to interact with different back-end systems that aren\\'t directly reachable by users. These systems typically have non- routable private informatics addresses. Since the back-end systems normally ordinarily protected by the topology, they typically have a weaker security posture. In several cases, internal back-end systems contain sensitive functionality that may be accessed while not authentication by anyone who is able to act with the systems. In the preceding example, suppose there\\'s an body interface at the back-end url https://192.168.0.68/ admin. Here, an attacker will exploit the SSRF vulnerability to access the executive interface by submitting the following request: POST /product/stock HTTP/1.0 Content-Type: application/x-www-form-urlencoded Content-Length: 118 stockApi=http://192.168.0.68/admin

QUESTION 3

Clark, a professional hacker, was hired by an organization lo gather sensitive Information about its competitors surreptitiously. Clark gathers the server IP address of the target organization using Whole footprinting. Further, he entered the server IP address as an input to an online tool to retrieve information such as the network range of the target organization and to identify the network topology and operating system used in the network. What is the online tool employed by Clark in the above scenario?

A. AOL

B. ARIN

C. DuckDuckGo

D. Baidu

Correct Answer: B

QUESTION 4

Which of the following Linux commands will resolve a domain name into IP address?

A. >host-t a hackeddomain.com

B. >host-t ns hackeddomain.com

C. >host -t soa hackeddomain.com

D. >host -t AXFR hackeddomain.com

Correct Answer: A

QUESTION 5

Mr. Omkar performed tool-based vulnerability assessment and found two vulnerabilities. During analysis, he found that these issues are not true vulnerabilities.

What will you call these issues?

A. False positives

B. True negatives

C. True positives

D. False negatives

Correct Answer: A