312-50V10$^{Q\&As}$

Certified Ethical Hacker Exam (C|EH v10)

Pass EC-COUNCIL 312-50V10 Exam with 100% Guarantee

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

https://www.geekcert.com/312-50v10.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

What is the following command used for?

net use \targetipc$ "" /u:""

A. Grabbing the etc/passwd file

B. Grabbing the SAM

C. Connecting to a Linux computer through Samba.

D. This command is used to connect as a null session

E. Enumeration of Cisco routers

Correct Answer: D

QUESTION 2

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?

A. Cross-site scripting vulnerability

B. Cross-site Request Forgery vulnerability

C. SQL injection vulnerability

D. Web site defacement vulnerability

Correct Answer: A

Many operators of particular web applications (e.g. forums and webmail) allow users to utilize a limited subset of HTML markup. When accepting HTML input from users (say, **very** large), output encoding (such as andlt;bandgt;veryandlt;/bandgt; large) will not suffice since the user input needs to be rendered as HTML by the browser (so it shows as "very large", instead of "**very** large"). Stopping an XSS attack when accepting HTML input from users is much more complex in this situation. Untrusted HTML input must be run through an HTML sanitization engine to ensure that it does not contain cross-site scripting code.

References: https://en.wikipedia.org/wiki/Crosssite_scripting#Safely_validating_untrusted_HTML_input

QUESTION 3

What attack is used to crack passwords by using a precomputed table of hashed passwords?

A. Brute Force Attack

B. Hybrid Attack

C. Rainbow Table Attack

D. Dictionary Attack

Correct Answer: C

QUESTION 4

It has been reported to you that someone has caused an information spillage on their computer. You go to the computer, disconnect it from the network, remove the keyboard and mouse, and power it down. What step in incident handling did you just complete?

A. Containment

B. Eradication

C. Recovery

D. Discovery

Correct Answer: A

QUESTION 5

When you are testing a web application, it is very useful to employ a proxy tool to save every request and response. You can manually test every request and analyze the response to find vulnerabilities. You can test parameter and headers manually to get more precise results than if using web vulnerability scanners.

What proxy tool will help you find web vulnerabilities?

A. Burpsuite

B. Maskgen

C. Dimitry

D. Proxychains

Correct Answer: A

Burp Suite is an integrated platform for performing security testing of web applications. Its various tools work seamlessly together to support the entire testing process, from initial mapping and analysis of an application\\'s attack surface, through to finding and exploiting security vulnerabilities.

References: https://portswigger.net/burp/