

Exin

EHF
Ethical Hacking Foundation

- Up to Date products, reliable and verified.
- Questions and Answers in PDF Format.

Full Version Features:

- 90 Days Free Updates
- 30 Days Money Back Guarantee
- Instant Download Once Purchased
- 24 Hours Live Chat Support

For More Information:

<https://www.testsexpert.com/>

- **Product Version**

Latest Version: 6.0

Question: 1

Penetration testers sometimes use shells to communicate and find vulnerabilities in systems. One type of shells is so-called 'Bind Shells'. In certain scenario's these are ineffective. Why is that?

Response:

- A. Firewalls will block any traffic on a port the Bind Shells tries to communicate on
- B. Windows 7 and above cannot run shell commands anymore if the user is not an administrator
- C. Bind Shells only run on terminal based operating systems

Answer: A

Question: 2

Someone has breached a website and managed to keep it a secret. The hack was not part of an assignment and there was no permission. What is this person called?

Response:

- A. Black hat hacker
- B. Hacktivist
- C. Scriptkiddie
- D. White hat hacker

Answer: A

Question: 3

What is the primary goal of an Ethical Hacker?

Response:

- A. Avoiding detection
- B. Determining return on investment (ROI) for security measures
- C. Resolving security vulnerabilities
- D. Testing security controls

Answer: D

Question: 4

You are performing a penetration test and are asked to test the authentication strength of a storage device. You have not received the IP address of the host, but you were told that the system sends a message to the network's broadcast every five minutes.

What could you use to find the IP address of the host?

Response:

- A. Ncrack
- B. Netdiscover
- C. Wireshark

Answer: C

Question: 5

You have saved the output of an Nmap scan in XML format. What should you use to import the scan results within Metasploit?

Response:

- A. db_import
- B. nmap_import
- C. scan_import

Answer: A

Question: 6

A tester is conducting a penetration test on a web server. She begins the test with a banner grabbing attack. She has already verified that the web server is running a Linux distribution. However, the HTTP banner reports that it is running IIS version 8.

What type of defense is the web server administrator using?

Response:

- A. Folder redirection
- B. Port obfuscation
- C. Process redirection
- D. Service spoofing

Answer: D

Question: 7

When creating an XSS PoC, what is the function that provides a pop-up?

Response:

- A. popup()
- B. alert()
- C. window.popup()

Answer: B

Question: 8

What can be used to create a connection between your machine and the website you have your R57 shell running on?

Response:

- A. Eval function
- B. Backconnect shell
- C. Reverse shell

Answer: B

Question: 9

What is a function of the R57 shell?

Response:

- A. Implementing a web-based version of Metasploit
- B. Viewing and transferring files
- C. Viewing the webcams of visitors towards the website

Answer: B

Question: 10

A hacker managed to find an XSS vulnerability. Now she wants to take over sessions. Where does she need the data retrievable from?

Response:

-
- A. document.session
 - B. session.cookie
 - C. document.cookie

Answer: C

For More Information – Visit link below:
<https://www.testsexpert.com/>

16\$ Discount Coupon: **9M2GK4NW**

Features:

■ Money Back Guarantee.....



■ 100% Course Coverage.....



■ 90 Days Free Updates.....



■ Instant Email Delivery after Order.....

