

GIAC GXPN

GIAC Exploit Researcher and Advanced Penetration Tester

Questions And Answers PDF Format:

For More Information – Visit link below:

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

Version = Product



Latest Version: 6.1

Question: 1

Which tool is most commonly used to exploit vulnerabilities in network protocols during penetration tests?

Response:

- A. Nmap
- B. Wireshark
- C. Scapy
- D. Metasploit

Answer: D

Question: 2

What method can an advanced penetration tester use to bypass MAC address filtering on a network?

Response:

- A. ARP poisoning
- B. MAC spoofing
- C. VLAN hopping
- D. Port scanning

Answer: B

Question: 3

You are exploiting a stack overflow vulnerability in a vulnerable program. Which approach would you take to successfully exploit the vulnerability?

Response:

- A. Overwrite the return address with the address of your shellcode
- B. Inject SQL commands directly into the stack
- C. Modify the heap to execute arbitrary code
- D. Perform a brute-force attack to guess the return address

Answer: A

Question: 4

Which two benefits does fuzzing provide during vulnerability assessment?

(Choose Two)

Response:

- A. Automation of vulnerability discovery
- B. Discovery of vulnerabilities that require detailed manual analysis
- C. Testing a broad range of input combinations
- D. Improving network traffic analysis

Answer: A,C

Question: 5

How can Python scripts enhance the functionality of a penetration test?

Response:

- A. By providing a graphical user interface
- B. By automating repetitive tasks
- C. By increasing the computational speed
- D. By reducing the amount of data stored

Answer: B

Question: 6

What is a typical use case for the sr1() function in Scapy?

Response:

- A. To send a packet and receive its answer
- B. To visualize packet flow
- C. To log packet data to a file
- D. To generate random packet data

Answer: A

Question: 7

In the context of advanced stack smashing, what is the purpose of using ROP?

Response:

- A. To execute shellcode in data sections
- B. To mitigate the effects of non-executable stacks
- C. To directly manipulate hardware registers
- D. To avoid detection by antivirus software

Answer: B

Question: 8

What is a common vulnerability in modern network protocols that can be exploited by attackers?

Response:

- A. Lack of encryption in Telnet sessions
- B. Secure Shell (SSH) misconfigurations
- C. TLS handshake failures
- D. Buffer overflow in HTTP/2

Answer: A

Question: 9

What method can an advanced penetration tester use to evade port-based NAC systems?

Response:

- A. Port scanning
- B. Tunneling traffic through allowed ports
- C. Encryption of traffic
- D. DHCP spoofing

Answer: B

Question: 10

What is a common vulnerability that can be exploited in cryptographic implementations during penetration tests?

Response:









- A. Buffer overflow
- B. Timing attack
- C. Cross-site scripting (XSS)

D. SQL injection

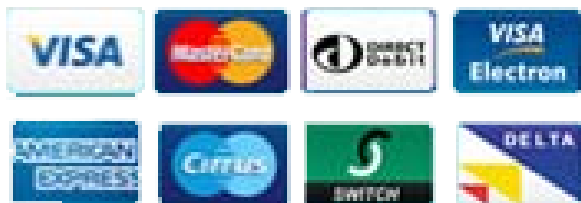
Answer: B

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

PRODUCT FEATURES

-  **100% Money Back Guarantee**
-  **90 Days Free updates**
-  **Special Discounts on Bulk Orders**
-  **Guaranteed Success**
-  **50,000 Satisfied Customers**
-  **100% Secure Shopping**
-  **Privacy Policy**
-  **Refund Policy**

16 USD Discount Coupon Code: NB4XKTMZ



Visit us at: <https://www.certsgrade.com/pdf/gxpn>