Exam Questions PT0-001

CompTIA PenTest+ Certification Exam

https://www.2passeasy.com/dumps/PT0-001/

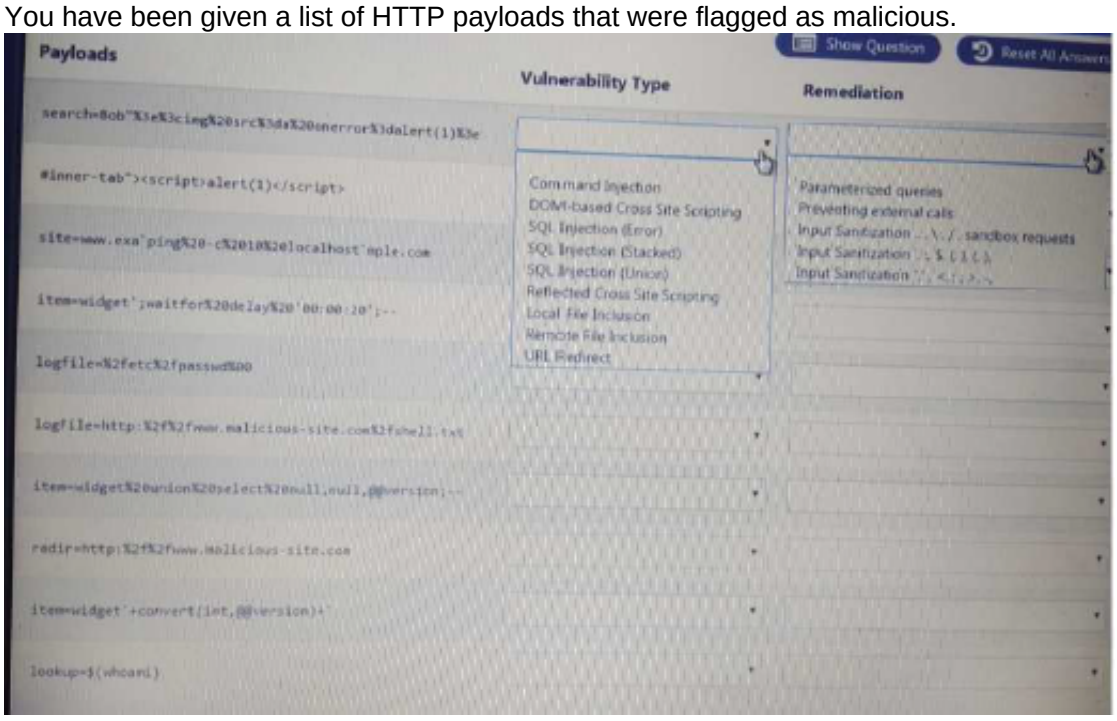
NEW QUESTION 1
DRAG DROP
Place each of the following passwords in order of complexity from least complex (1) to most complex (4), based on the character sets represented Each password may be used only once

A. Mastered
B. Not Mastered

Answer: A
Explanation:

Zverlory
Zverl0ry
zv3rlory
Zv3r!0ry

NEW QUESTION 2
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.



A. Mastered
B. Not Mastered

Answer: A

NEW QUESTION 3
A constant wants to scan all the TCP Pots 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 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
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)

```
dig -q any _kerberos._tcp.internal.comptia.net
```

B)

```
dig -q any _lanman._tcp.internal.comptia.net
```

C)

```
dig -q any _ntlm._tcp.internal.comptia.net
```

D)

```
dig -q any _smtp._tcp.internal.comptia.net
```

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

Answer: A

NEW QUESTION 6
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 7
A penetration tester has successfully explogted 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 I clear
C. rm -f ./history
D. history -c

Answer: D

NEW QUESTION 8
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 9
A recently concluded penetration test revealed that a legacy web application is vulnerable lo SQL injection Research indicates that completely remediating the vulnerability would require an architectural change, and the stakeholders are not m a position to risk the availability of the application Under such circumstances, which of the following controls are low-effort, short-term solutions to minimize the SQL injection risk? (Select TWO).

A. Identify and eliminate inline SQL statements from the code.
B. Identify and eliminate dynamic SQL from stored procedures.
C. Identify and sanitize all user inputs.
D. Use a whitelist approach for SQL statements.
E. Use a blacklist approach for SQL statements.
F. Identify the source of malicious input and block the IP addres

Answer: DE

NEW QUESTION 10
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 10
Given the following script:

```
import pyHook, pythoncom, logging, sys

f="f.txt"
def OnKeyboardEvent(event):
        logging.basicConfig(filename=f,level=loggin.DEBUG,format='%(messages)')
        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 15
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 20
Which of the following reasons does penetration tester needs to have a customer's point-of -contact information available at all time? (Select THREE).

A. To report indicators of compromise
B. To report findings that cannot be explogted
C. To report critical findings
D. To report the latest published explogts
E. To update payment information
F. To report a server that becomes unresponsive
G. To update the statement o(work
H. To report a cracked password

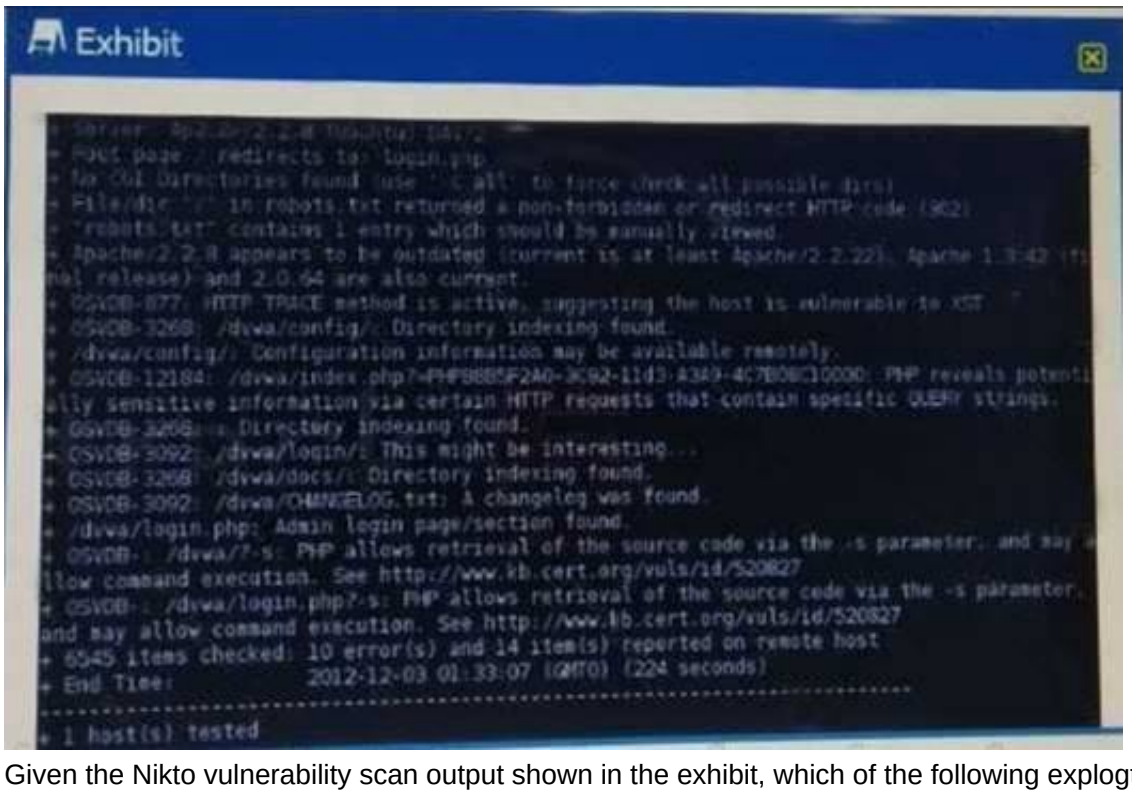
Answer: DEF

NEW QUESTION 25
A penetration tester is utilizing social media to gather information about employees at a company. The tester has created a list of popular words used in employee profile s. For which of the following types of attack would this information be used?

A. Explogt chaining
B. Session hijacking
C. Dictionary
D. Karma

Answer: B

NEW QUESTION 26
Click the exhibit button.



Given the Nikto vulnerability scan output shown in the exhibit, which of the following explogtation techniques might be used to explogt the target system? (Select TWO)

A. Arbitrary code execution
B. Session hijacking
C. SQL injection
D. Login credential brute-forcing
E. Cross-site request forgery

Answer: CE

NEW QUESTION 28
A tester has determined that null sessions are enabled on a domain controller. Which of the following attacks can be performed to leverage this vulnerability?

A. RID cycling to enumerate users and groups
B. Pass the hash to relay credentials
C. Password brute forcing to log into the host
D. Session hijacking to impersonate a system account

Answer: C

NEW QUESTION 29
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 ol 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 30
.....

THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual PT0-001 Exam Questions With Answers.

We Also Provide Practice Exam Software That Simulates Real Exam Environment And Has Many Self-Assessment Features. Order the PT0-001 Product From:

https://www.2passeasy.com/dumps/PT0-001/

Money Back Guarantee

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 FirstTry

* PT0-001 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year