32: Lab 32: Assisted - Performing penetration testing

Security+ (Exam SY0-701)

Solve ×

Congratulations, you passed!

Duration: 57 minutes, 24 seconds

☑ How many "change to parent" operations are needed to create a relative URL reference to view the `passwd` file? *Score: 1*

- ○ 3
- ○ 4
- ○ 5
- ◉ 6
- ○ 7

Congratulations, you have answered the question correctly.

☑ What is the result of the *whoami* command injected in this step? *Score: 1*

- ○ jaime
- ○ localhost
- ○ 172.16.0.201
- ◉ www-data

Congratulations, you have answered the question correctly.

☑ **Use a script to confirm upload of /root/world.png** *Score: 1*

Select the **Score** button to validate this task:

```
File upload confirmed ...
Task complete
```

☑ **Use a script to confirm upload of special.php** *Score: 1*

Select the **Score** button to validate this task:

```
File upload confirmed ...
Task complete
```

☑ **use a script to confirm the existence of /root/shell.php** *Scr*

Select the **Score** button to validate this task:

```
Path found ... checking contents
Contents matched …
Task complete
```

Confirm web shell connection *Score: 1*

Select the **Score** button to validate this task:

```
Handler active ...
Task complete
```

What is th Solve ✕ eges context for the established web shell? *Score: 1*

www-data

Congratulations, you have answered the question correctly.

What is the point of the string "../../../../../../" used in an attack? *Score: 1*

- ○ Use command obfuscation to avoid keyword filters
- ○ Use special characters to avoid metacharacter escaping
- ◉ Use directory traversal to reach the root directory
- ○ Trick the system into granting access to the file using root privileges

Congratulations, you have answered the question correctly.

Which of the following characters can be used to stack commands in a command injection attack? (Select all that apply) *Score: 1*

- ☐ ?
- ☐ /
- ☑ ;
- ☑ &&
- ☐ ^
- ☑ |
- ☐ +

Congratulations, you have answered the question correctly.

What is the most significant concern of a file upload vulnerability? *Score: 1*

- ○ An attacker's ability to change user passwords.
- ○ An attacker learning the OS and software identities.
- ○ An attacker changing website contents (i.e., defacement)
- ◉ An attacker being able to run malicious code on the web server.

Congratulations, you have answered the question correctly.

Exploiting systems using directory traversal, command injection, file upload, and web shell injection technique is typically performed during what phase of penetration testing? *Score: 1*

- ○ Reconnaissance
- ○ Scanning
- ○ Vulnerability detection,
- ◉ Gaining access
- ○ Post-exploit activities

Congratulations, you have answered the question correctly.

Score: 1

Injecting a web shell can be accomplished by taking advantage of what discovered vulnerability?

- (●) File upload
- ( ) Adversary in the middle (AitM)
- ( ) Brute force password cracking
- ( ) Direct

Solve ×

Congratulations, you have answered the question correctly.