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

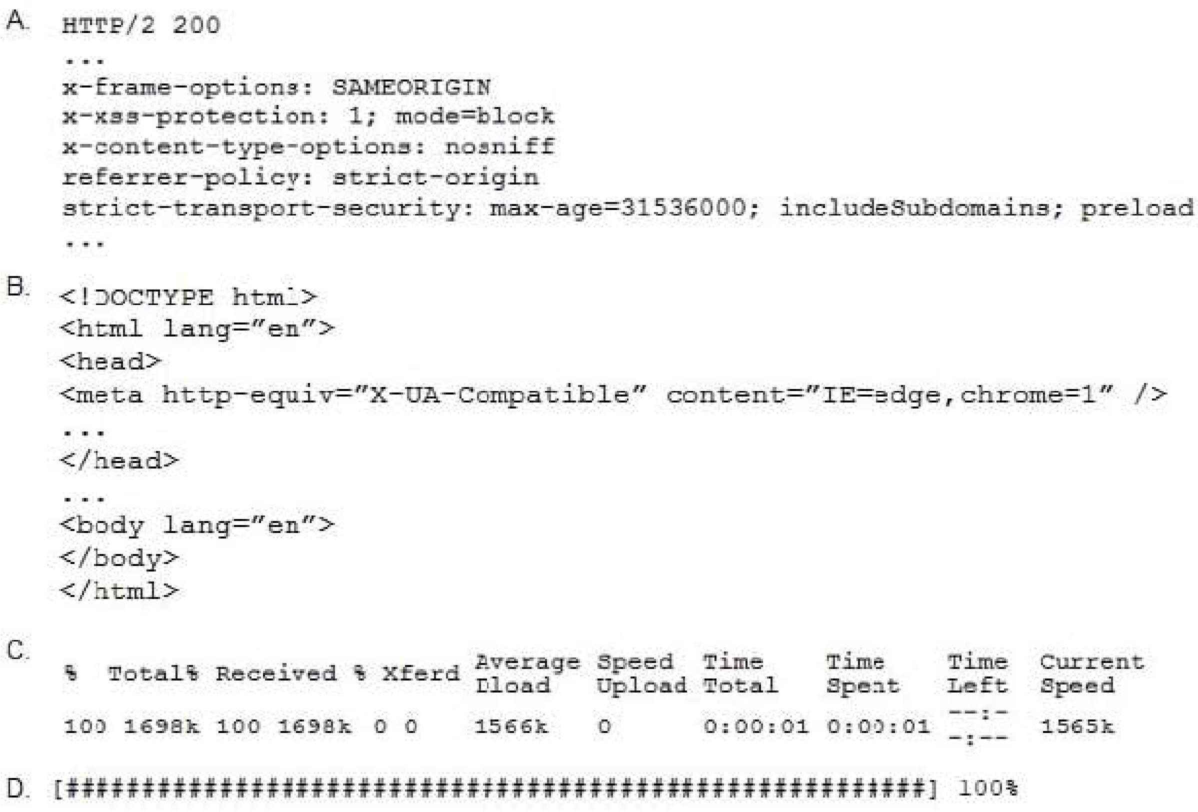
Following Questions and Answers are all new published by CompTIA Official Exam Center

QUESTION 1

A penetration tester performs the following command:

curl-I-http2 https://www.comptia.org

Which of the following snippets of output will the tester MOST likely receive?



A.

```
HTTP/2 200
...
x-frame-options: SAMEORIGIN
x-xss-protection: 1; mode=block
x-content-type-options: nosniff
referrer-policy: strict-origin
strict-transport-security: max-age=31536000; includeSubdomains; preload
...
```

B.

```
<!DOCTYPE html>
<html lang="en">
<head>
<meta http-equiv="X-UA-Compatible" content="IE=edge,chrome=1" />
...
</head>
...
<body lang="en">
</body>
</html>
```

C.

```
                                         Average Speed  Time      Time      Time   Current
%   Total%  Received  % Xferd            Dload   Upload Total     Spent     Left   Speed

100 1698k   100 1698k  0  0              1566k   0      0:00:01   0:00:01   --:--  1565k
                                                                            -:--
```

D.

```
[########################################################] 100%
```

A. Option A

B. Option B

C. Option C

D. Option D

Correct Answer: A

Reference: https://research.securitum.com/http-2-protocol-it-is-faster-but-is-it-also-safer/

QUESTION 2

A company is concerned that its cloud service provider is not adequately protecting the VMs housing its software development. The VMs are housed in a datacenter with other companies sharing physical resources. Which of the following attack types is MOST concerning to the company?

A. Data flooding

B. Session riding

C. Cybersquatting

D. Side channel

Correct Answer: D

https://www.techtarget.com/searchsecurity/definition/side-channel-attack#:~:text=Side%2Dchannel%20attacks%20can%20even,share%20the%20same%20physical%20hardware

---

QUESTION 3

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 4

A penetration tester is exploring a client\\'s website. The tester performs a curl command and obtains the following:

```
*
 Connected to 10.2.11.144 (::1) port 80 (#0)
> GET /readmine.html HTTP/1.1
> Host: 10.2.11.144
> User-Agent: curl/7.67.0
> Accept: */*
>
*
 Mark bundle as not supporting multiuse
```

Which of the following tools would be BEST for the penetration tester to use to explore this site further?

A.

Burp Suite

B.

DirBuster

C.

WPScan

D.

OWASP ZAP

Correct Answer: C

Reference: https://tools.kali.org/web-applications/burpsuite

QUESTION 5

A company requires that all hypervisors have the latest available patches installed. Which of the following would BEST explain the reason why this policy is in place?

A. To provide protection against host OS vulnerabilities

B. To reduce the probability of a VM escape attack

C. To fix any misconfigurations of the hypervisor

D. To enable all features of the hypervisor

Correct Answer: B

A hypervisor is a type of virtualization software that allows multiple virtual machines (VMs) to run on a single physical host machine. If the hypervisor is compromised, an attacker could potentially gain access to all of the VMs running on that host, which could lead to a significant data breach or other security issues. One common type of attack against hypervisors is known as a VM escape attack. In this type of attack, an attacker exploits a vulnerability in the hypervisor to break out of the VM and gain access to the host machine. From there, the attacker can potentially gain access to other VMs running on the same host. By ensuring that all hypervisors have the latest available patches installed, the company can reduce the likelihood that a VM escape attack will be successful. Patches often include security updates and vulnerability fixes that address known issues and can help prevent attacks.