



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.lead4pass.com/pt0-001.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 consultant is identifying versions of Windows operating systems on a network. Which of the following Nmap commands should the consultant run?

- A. `nmap -T4 -v -sU -iL /tmp/list.txt -Pn --script smb-system-info`
- B. `nmap -T4 -v -iL /tmp/list.txt -Pn --script smb-os-discovery`
- C. `nmap -T4 -v -6 -iL /tmp/liat.txt -Pn --script smb-os-discovery -p 135-139`
- D. `nmap -T4 -v --script smb-system-info 192.163.1.0/24`

Correct Answer: B

QUESTION 2

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 profiles. For which of the following types of attack would this information be used?

- A. Exploit chaining
- B. Session hijacking
- C. Dictionary
- D. Karma

Correct Answer: C

QUESTION 3

A company received a report with the following finding: While on the internal network, the penetration tester was able to successfully capture SMB broadcasted user ID and password information on the network and decode this information. This allowed the penetration tester to then join their own computer to the ABC domain.

Which of the following remediations are appropriate for the reported findings? (Select TWO)

- A. Set the Schedule Task Service from Automatic to Disabled
- B. Enable network-level authentication
- C. Remove the ability from Domain Users to join domain computers to the network
- D. Set the netlogon service from Automatic to Disabled
- E. Set up a SIEM alert to monitor Domain joined machines
- F. Set "Digitally sign network communications" to Always



Correct Answer: BC

QUESTION 4

A client requests that a penetration tester emulate a help desk technician who was recently laid off. Which of the following BEST describes the abilities of the threat actor?

- A. Advanced persistent threat
- B. Script kiddie
- C. Hactivist
- D. Organized crime

Correct Answer: B

Reference <https://www.sciencedirect.com/topics/computer-science/disgruntled-employee>

QUESTION 5

A penetration tester executed a vulnerability scan against a publicly accessible host and found a web server that is vulnerable to the DROWN attack. Assuming this web server is using the IP address 127.212.31.17, which of the following should the tester use to verify a false positive?

- A. `Openssl s_client -tls1_2 -connect 127.212.31.17:443`
- B. `Openssl s_client -ss12 -connect 127.212.31.17:443`
- C. `Openssl s_client -ss13 -connect 127.212.31.17:443`
- D. `Openssl s_server -tls1_2 -connect 127.212.31.17:443`

Correct Answer: A

QUESTION 6

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 7

A penetration tester is testing a web application and is logged in as a lower-privileged user. The tester runs arbitrary JavaScript within an application, which sends an XMLHttpRequest, resulting in exploiting features to which only an administrator should have access. Which of the following controls would BEST mitigate the vulnerability?

- A. Implement authorization checks.
- B. Sanitize all the user input.
- C. Prevent directory traversal.
- D. Add client-side security controls

Correct Answer: A

QUESTION 8

DRAG DROP

A technician is reviewing the following report. Given this information, identify which vulnerability can be definitively confirmed to be a false positive by dragging the “false positive” token to the “Confirmed” column for each vulnerability that is a false positive.

Select and Place:

Vulnerability	Vulnerability description	Operating System	Confirmed
Directory traversal	A vulnerability was found in the IIS server	Linux	<input type="checkbox"/>
Default credentials	User:admin Pass:admin on CISCO AP	IOS	<input type="checkbox"/>
Weak SSH encryption	SSH clients can negotiate weak ciphers	Windows	<input type="checkbox"/>
Expired certificate	The RDP service certificate has expired	Linux	<input type="checkbox"/>
Writable network share	Unauthenticated users can write to the NFS share	HPUX	<input type="checkbox"/>

False positive

Correct Answer:



Vulnerability	Vulnerability description	Operating System	Confirmed
Directory traversal	A vulnerability was found in the IIS server	Linux	False positive
Default credentials	User:admin Pass:admin on CISCO AP	IOS	
Weak SSH encryption	SSH clients can negotiate weak ciphers	Windows	
Expired certificate	The RDP service certificate has expired	Linux	False positive
Writable network share	Unauthenticated users can write to the NFS share	HPUX	

False positive

QUESTION 9

Consumer-based IoT devices are often less secure than systems built for traditional desktop computers.

Which of the following BEST describes the reasoning for this?

- A. Manufacturers developing IoT devices are less concerned with security.
- B. It is difficult for administrators to implement the same security standards across the board.
- C. IoT systems often lack the hardware power required by more secure solutions.
- D. Regulatory authorities often have lower security requirements for IoT systems.

Correct Answer: A

QUESTION 10

A penetration tester is designing a phishing campaign and wants to build list of users (or the target organization. Which of the following techniques would be the MOST appropriate? (Select TWO)

- A. Query an Internet WHOIS database.
- B. Search posted job listings.



- C. Scrape the company website.
- D. Harvest users from social networking sites.
- E. Socially engineer the corporate call center.

Correct Answer: CD

QUESTION 11

The following command is run on a Linux file system:

```
Chmod 4111 /usr/bin/sudo
```

Which of the following issues may be exploited now?

- A. Kernel vulnerabilities
- B. Sticky bits
- C. Unquoted service path
- D. Misconfigured sudo

Correct Answer: B

QUESTION 12

A security assessor is attempting to craft specialized XML files to test the security of the parsing functions during ingest into a Windows application. Before beginning to test the application, which of the following should the assessor request from the organization?

- A. Sample SOAP messages
- B. The REST API documentation
- C. A protocol fuzzing utility
- D. An applicable XSD file

Correct Answer: D

QUESTION 13

A company hires a penetration tester to determine if there are any vulnerabilities in its new VPN concentrator installation with an external IP of 100.170.60.5.

Which of the following commands will test if the VPN is available?



- A. `fpipe.exe -l 8080 -r 80 100.170.60.5`
- B. `ike-scan -A -t 1 --sourceip=apooof_ip 100.170.60.5`
- C. `nmap -sS -A -f 100.170.60.5`
- D. `nc 100.170.60.5 8080 /bin/sh`

Correct Answer: B

QUESTION 14

Which of the following is the MOST comprehensive type of penetration test on a network?

- A. Black box
- B. White box
- C. Gray box
- D. Red team
- E. Architecture review

Correct Answer: A

Reference: <https://purplesec.us/types-penetration-testing/>

QUESTION 15

A system security engineer is preparing to conduct a security assessment of some new applications. The applications were provided to the engineer as a set that contains only JAR files. Which of the following would be the MOST detailed method to gather information on the inner working of these applications?

- A. Launch the applications and use dynamic software analysis tools, including fuzz testing
- B. Use a static code analyzer on the JAR file to look for code Quality deficiencies
- C. Decompile the applications to approximate source code and then conduct a manual review
- D. Review the details and extensions of the certificate used to digitally sign the code and the application

Correct Answer: A

[Latest PT0-001 Dumps](#)

[PT0-001 Practice Test](#)

[PT0-001 Brindumps](#)



To Read the [Whole Q&As](#), please purchase the [Complete Version](#) from [Our website](#).

Try our product !

100% Guaranteed Success
100% Money Back Guarantee
365 Days Free Update
Instant Download After Purchase
24x7 Customer Support
Average 99.9% Success Rate
More than 800,000 Satisfied Customers Worldwide
Multi-Platform capabilities - [Windows](#), [Mac](#), [Android](#), [iPhone](#), [iPod](#), [iPad](#), [Kindle](#)

We provide exam PDF and VCE of Cisco, Microsoft, IBM, CompTIA, Oracle and other IT Certifications. You can view Vendor list of All Certification Exams offered:

<https://www.lead4pass.com/allproducts>

Need Help

Please provide as much detail as possible so we can best assist you.
To update a previously submitted ticket:



 <p>One Year Free Update Free update is available within One Year after your purchase. After One Year, you will get 50% discounts for updating. And we are proud to boast a 24/7 efficient Customer Support system via Email.</p>	 <p>Money Back Guarantee To ensure that you are spending on quality products, we provide 100% money back guarantee for 30 days from the date of purchase.</p>	 <p>Security & Privacy We respect customer privacy. We use McAfee's security service to provide you with utmost security for your personal information & peace of mind.</p>
---	---	--

Any charges made through this site will appear as Global Simulators Limited.
All trademarks are the property of their respective owners.
Copyright © lead4pass, All Rights Reserved.