# 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.pass4itsure.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 was able to compromise a server and escalate privileges. Which of the following should the tester perform AFTER concluding the activities on the specified target? (Choose two.)

A. Remove the logs from the server.

B. Restore the server backup.

C. Disable the running services.

D. Remove any tools or scripts that were installed.

E. Delete any created credentials.

F. Reboot the target server.

Correct Answer: DE

**QUESTION 2**

A penetration tester has established an on-path position between a target host and local network services but has not been able to establish an on-path position between the target host and the Internet. Regardless, the tester would like to subtly redirect HTTP connections to a spoofed server IP. Which of the following methods would BEST support the objective?

A. Gain access to the target host and implant malware specially crafted for this purpose.

B. Exploit the local DNS server and add/update the zone records with a spoofed A record.

C. Use the Scapy utility to overwrite name resolution fields in the DNS query response.

D. Proxy HTTP connections from the target host to that of the spoofed host.

Correct Answer: D

**QUESTION 3**

A penetration tester has been hired to configure and conduct authenticated scans of all the servers on a software company\\'s network. Which of the following accounts should the tester use to return the MOST results?

A. Root user

B. Local administrator

C. Service

D. Network administrator

Correct Answer: C

**QUESTION 4**

An exploit developer is coding a script that submits a very large number of small requests to a web server until the server is compromised. The script must examine each response received and compare the data to a large number of strings to determine which data to submit next. Which of the following data structures should the exploit developer use to make the string comparison and determination as efficient as possible?

A. A list

B. A tree

C. A dictionary

D. An array

Correct Answer: C

data structures are used to store data in an organized form, and some data structures are more efficient and suitable for certain operations than others. For example, hash tables, skip lists and jump lists are some dictionary data structures

that can insert and access elements efficiently3.

For string comparison, there are different algorithms that can measure how similar two strings are, such as Levenshtein distance, Hamming distance or Jaccard similarity4. Some of these algorithms can be implemented using data structures

such as arrays or hashtables 5.

**QUESTION 5**

Which of the following tools would help a penetration tester locate a file that was uploaded to a content management system?

A. DirBuster

B. Open VAS

C. Scout Suite

D. CeWL

Correct Answer: A

DirBuster is a tool that can brute-force directories and filenames on web servers. It can help a penetration tester locate a file that was uploaded to a content management system by trying different combinations of paths and names until it finds a match. DirBuster can also use wordlists to speed up the process and discover hidden files or directories. References: The Official CompTIA PenTest+ Instructor Guide (Exam PT0- 002) eBook, page 156