# PT0-002$^{\text{Q\&As}}$

CompTIA PenTest+ Certification Exam

## Pass CompTIA PT0-002 Exam with 100% Guarantee

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

**https://www.pass2lead.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 discovered that a client uses cloud mail as the company\\'s email system. During the penetration test, the tester set up a fake cloud mail login page and sent all company employees an email that stated their inboxes were full and directed them to the fake login page to remedy the issue. Which of the following BEST describes this attack?

A. Credential harvesting

B. Privilege escalation

C. Password spraying

D. Domain record abuse

Correct Answer: A

**QUESTION 2**

A penetration tester discovers during a recent test that an employee in the accounting department has been making changes to a payment system and redirecting money into a personal bank account. The penetration test was immediately stopped. Which of the following would be the BEST recommendation to prevent this type of activity in the future?

A. Enforce mandatory employee vacations

B. Implement multifactor authentication

C. Install video surveillance equipment in the office

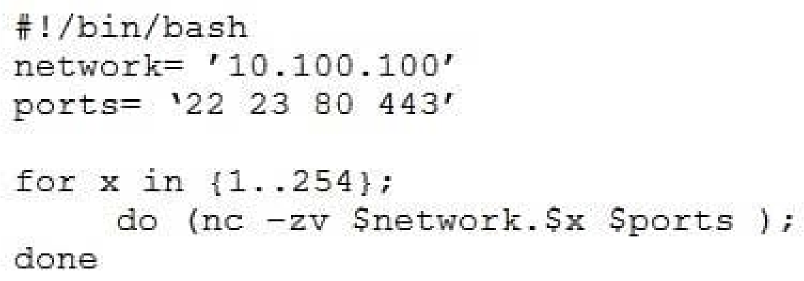
D. Encrypt passwords for bank account information

Correct Answer: A

If the employee already works in the accounting department, MFA will not stop their actions because they\\'ll already have access by virtue of their job.

**QUESTION 3**

A penetration tester writes the following script: Which of the following is the tester performing?



```
#!/bin/bash
network= ’10.100.100’
ports= ‘22 23 80 443’

for x in {1..254};
     do (nc -zv $network.$x $ports );
done
```

A. Searching for service vulnerabilities

B. Trying to recover a lost bind shell

C. Building a reverse shell listening on specified ports

D. Scanning a network for specific open ports

Correct Answer: D

-z zero-I/O mode [used for scanning]

-v verbose

example output of script:

10.0.0.1: inverse host lookup failed: Unknown host (UNKNOWN) [10.0.0.1] 22 (ssh) open (UNKNOWN) [10.0.0.1] 23 (telnet) : Connection timed out

https://unix.stackexchange.com/questions/589561/what-is-nc-z-used-for

**QUESTION 4**

A penetration tester will be performing a vulnerability scan as part of the penetration test on a client\\'s website. The tester plans to run several Nmap scripts that probe for vulnerabilities while avoiding detection. Which of the following Nmap options will the penetration tester MOST likely utilize?

A. -8 -T0

B. --script "http*vuln*"

C. -sn

D. -O -A

Correct Answer: B

**QUESTION 5**

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