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.leads4pass.com/pt0-001.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 is connected to a client\\'s local network and wants to passively identify cleartext protocols and potentially sensitive data being communicated across the network. Which of the following is the BEST approach to take?

A. Run a network vulnerability scan.

B. Run a stress test.

C. Run an MITM attack.

D. Run a port scan.

Correct Answer: C

Reference: https://www.sciencedirect.com/topics/computer-science/encrypted-protocol

QUESTION 2

A penetration tester has compromised a system and wishes to connect to a port on it from the attacking machine to control the system Which of the following commands should the tester run on the compromised system?

A. nc looalhot 4423

B. nc -nvlp 4423 -?/bin/bash

C. nc 10.0.0.1 4423

D. nc 127.0.0.1 4423 -e /bin/bash

Correct Answer: B

QUESTION 3

A penetration tester is performing a code review. Which of the following testing techniques is being performed?

A. Dynamic analysis

B. Fuzzing analysis

C. Static analysis

D. Run-time analysis

Correct Answer: C

Reference: https://smartbear.com/learn/code-review/what-is-code-review/

QUESTION 4

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 profile s. 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 5

During an internal network penetration test, a tester recovers the NTLM password hash tor a user known to have full administrator privileges on a number of target systems Efforts to crack the hash and recover the plaintext password have been unsuccessful Which of the following would be the BEST target for continued exploitation efforts?

A. Operating system Windows 7 Open ports: 23, 161

B. Operating system Windows Server 2016 Open ports: 53, 5900

C. Operating system Windows 8 1 Open ports 445, 3389

D. Operating system Windows 8 Open ports 514, 3389

Correct Answer: C

QUESTION 6

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 -1 8080 -r 80 100.170.60.5

B. ike-scan -A -t 1 --sourceip=apoof_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 7

A penetration tester has been assigned to perform an external penetration assessment of a company. Which of the following steps would BEST help with the passive-information-gathering process? (Choose two.)

A. Wait outside of the company\\'s building and attempt to tailgate behind an employee.

B. Perform a vulnerability scan against the company\\'s external netblock, identify exploitable vulnerabilities, and attempt to gain access.

C. Use domain and IP registry websites to identify the company\\'s external netblocks and external facing applications.

D. Search social media for information technology employees who post information about the technologies they work with.

E. Identify the company\\'s external facing webmail application, enumerate user accounts and attempt password guessing to gain access.

Correct Answer: DE

QUESTION 8

An organization has requested that a penetration test be performed to determine if it is possible for an attacker to gain a foothold on the organization\\'s server segment. During the assessment, the penetration tester identifies tools that appear to have been left behind by a prior attack. Which of the following actions should the penetration tester take?

A. Attempt to use the remnant tools to achieve persistence.

B. Document the presence of the left-behind tools in the report and proceed with the test.

C. Remove the tools from the affected systems before continuing on with the test.

D. Discontinue further testing and report the situation to management.

Correct Answer: A

QUESTION 9

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: C

QUESTION 10

A penetration tester, who is not on the client\\'s network. is using Nmap to scan the network for hosts that are in scope. The penetration tester is not receiving any response on the command:

nmap 100.100/1/0-125

Which of the following commands would be BEST to return results?

A. nmap -Pn -sT 100.100.1.0-125

B. nmap -sF -p 100.100.1.0-125

C. nmap -sV -oA output 100.100.10-125

D. nmap 100.100.1.0-125 -T4

Correct Answer: A

QUESTION 11

A penetration tester is required to exploit a WPS implementation weakness. Which of the following tools will perform the attack?

A. Karma

B. Kismet

C. Pixie

D. NetStumbler

Correct Answer: D

Reference: https://en.wikipedia.org/wiki/NetStumbler

QUESTION 12

Given the following Python script:

```
#!/usr/bin/python
import socket as skt
for port in range(1,1024):
    try:
        sox=skt.socket(skt.AF_INET,skt.SOCK_STREAM)
        sox.settimeout(1000)
        sox.connect(('127.0.0.1',port))
        print '%d:OPEN' % (port)
        sox.close
    except: continue
```

Which of the following is where the output will go?

A. To the screen

B. To a network server

C. To a file

D. To /dev/null

Correct Answer: C

QUESTION 13

A web application scanner reports that a website is susceptible to clickjacking. Which of the following techniques would BEST prove exploitability?

A. Redirect the user with a CSRF.

B. Launch the website in an iFRAME.

C. Pull server headers.

D. Capture and replay a session ID.

Correct Answer: B

Reference: https://www.imperva.com/learn/application-security/clickjacking/

QUESTION 14

A senior employee received a suspicious email from another executive requesting an urgent wire transfer. Which of the following types of attacks is likely occurring?

A. Spear phishing

B. Business email compromise

C. Vishing

D. Whaling

Correct Answer: A

Reference: https://www.welivesecurity.com/2020/03/13/415pm-urgent-message-ceo-fraud/

QUESTION 15

During the information gathering phase of a network penetration test for the corp.local domain, which of the following commands would provide a list of domain controllers?

A. nslookup -type=srv _ldap._tcp.dc._msdcs.corp.local

B. nmap -sV -p 389 - -script=ldap-rootdse corp.local

C. net group "Domain Controllers" /domain

D. gpresult /d corp.local /r "Domain Controllers"

Correct Answer: A