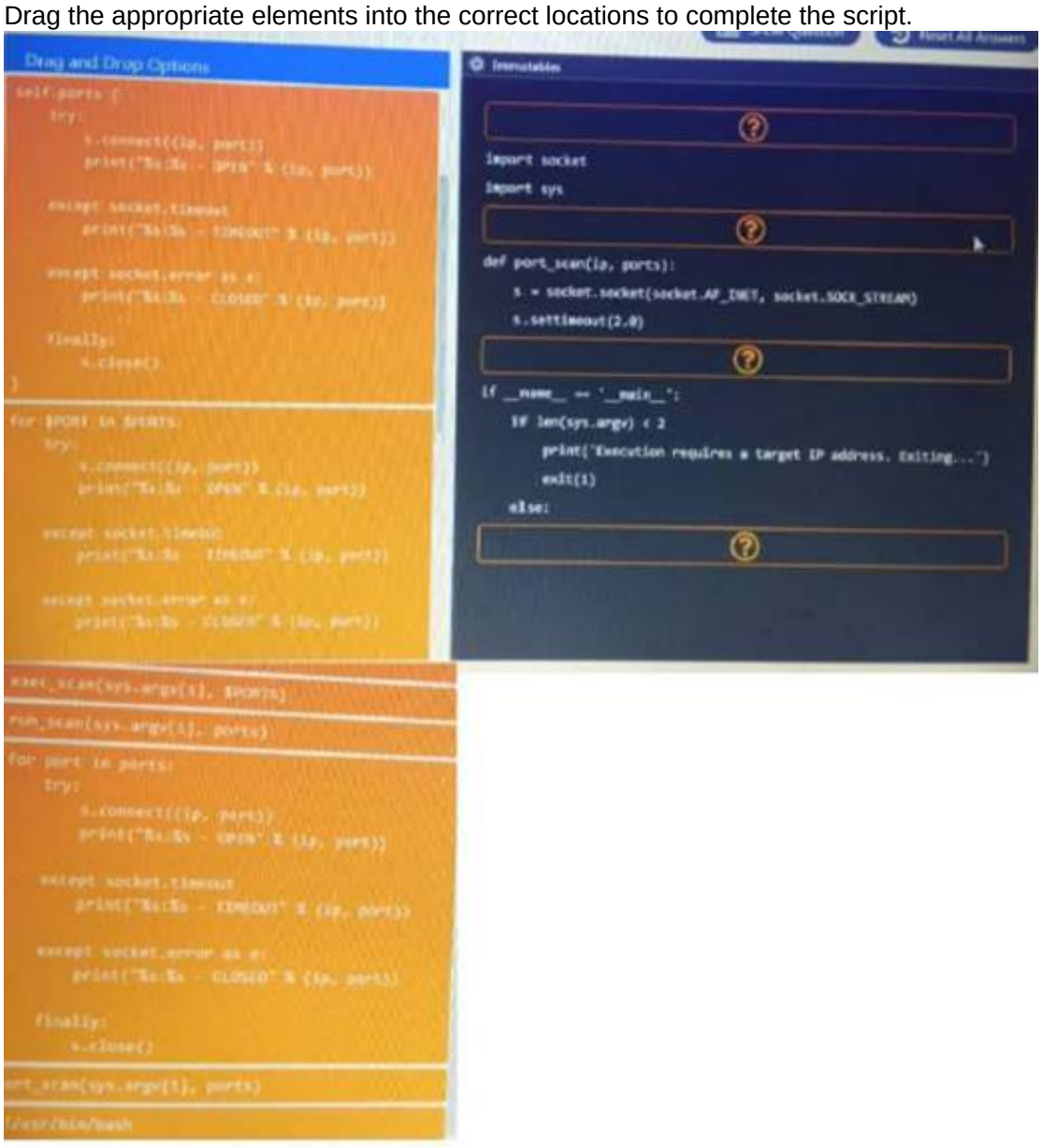
CompTIA

Exam Questions PT0-001

CompTIA PenTest+ Certification Exam

NEW QUESTION 1
DRAG DROP
During a penetration test, you gain access to a system with a limited user interface. This machine appears to have access to an isolated network that you would like to port scan. INSTRUCTIONS:
Analyze the code segments to determine which sections are needed to complete a port scanning script.
Drag the appropriate elements into the correct locations to complete the script.



A. Mastered
B. Not Mastered

Answer: A

NEW QUESTION 2
During a penetration test, a tester runs a phishing campaign and receives a shell from an internal PC running Windows 10 OS. The tester wants to perform credential harvesting with Mimikazt. Which of the following registry changes would allow for credential caching in memory?
A)

```
reg add HKLM\System\ControlSet002\Control\SecurityProviders\WDigest /v UseLogoCredential /t
REG_DWORD /d 0
```

B)

```
reg add HKCU\System\CurrentControlSet\Control\SecurityProviders\WDigest /v UseLogoCredential /t
REG_DWORD /d 1
```

C)

```
reg add HKLM\Software\CurrentControlSet\Control\SecurityProviders\WDigest /v UseLogoCredential
/t REG_DWORD /d 1
```

D)

```
reg add HKLM\System\CurrentControlSet\Control\SecurityProviders\WDigest /v UseLogoCredential /t
REG_DWORD /d 1
```

A. Option A
B. Option B
C. Option C
D. Option D

Answer: D

NEW QUESTION 3
In which of the following components is an explogted vulnerability MOST likely to affect multiple running application containers at once?

A. Common libraries

B. Configuration files
C. Sandbox escape
D. ASLR bypass

Answer: D

NEW QUESTION 4
A penetration tester was able to retrieve the initial VPN user domain credentials by phishing a member of the IT department. Afterward, the penetration tester obtained hashes over the VPN and easily cracked them using a dictionary attack Which of the following remediation steps should be recommended? (Select THREE)

A. Mandate all employees take security awareness training
B. Implement two-factor authentication for remote access
C. Install an intrusion prevention system
D. Increase password complexity requirements
E. Install a security information event monitoring solution.
F. Prevent members of the IT department from interactively logging in as administrators
G. Upgrade the cipher suite used for the VPN solution

Answer: BDG

NEW QUESTION 5
A software development team recently migrated to new application software on the on-premises environment Penetration test findings show that multiple vulnerabilities exist If a penetration tester does not have access to a live or test environment, a test might be better to create the same environment on the VM Which of the following is MOST important for confirmation?

A. Unsecure service and protocol configuration
B. Running SMB and SMTP service
C. Weak password complexity and user account
D. Misconfiguration

Answer: A

NEW QUESTION 6
After several attempts, an attacker was able to gain unauthorized access through a biometric sensor using the attacker's actual fingerprint without explogtation. Which of the following is the MOST likely explanation of what happened?

A. The biometric device is tuned more toward false positives
B. The biometric device is configured more toward true negatives
C. The biometric device is set to fail closed
D. The biometnc device duplicated a valid user's fingerpnn

Answer: A

NEW QUESTION 7
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 cente

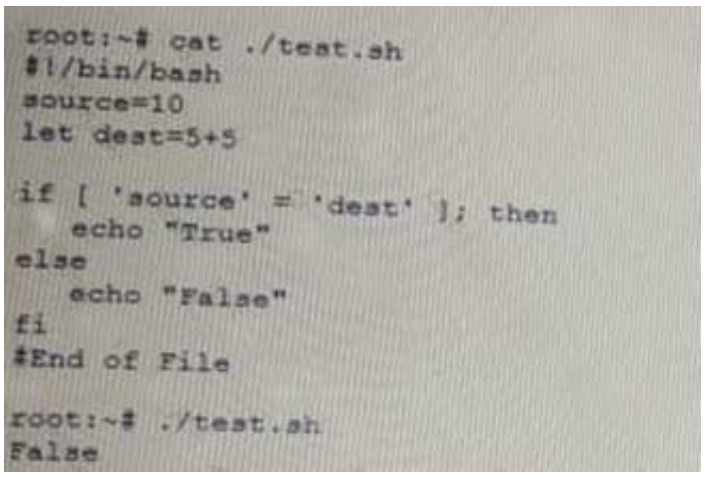
Answer: AB

NEW QUESTION 8
A security consultant found a SCADA device in one of the VLANs in scope. Which of the following actions would BEST create a potentially destructive outcome against device?

A. Launch an SNMP password brute force attack against the device.
B. Lunch a Nessus vulnerability scan against the device.
C. Launch a DNS cache poisoning attack against the device.
D. Launch an SMB explogt against the devic

Answer: A

NEW QUESTION 9
A penetration tester is checking a script to determine why some basic persisting. The expected result was the program outputting "True."

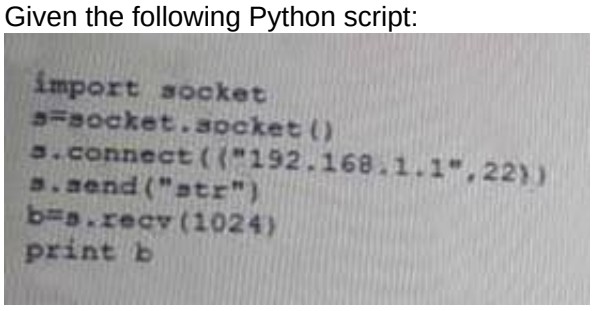


Given the output from the console above, which of the following explains how to correct the errors in the script? (Select TWO)

A. Change fi' to 'Endlf
B. Remove the 'let' in front of 'dest=5+5'.
C. Change the '=" to '-eq'.
D. Change •source* and 'dest' to "Ssource" and "Sdest"
E. Change 'else' to 'eli

Answer: BC

NEW QUESTION 10
Given the following Python script:



Which of the following actions will it perform?

A. ARP spoofing
B. Port scanner
C. Reverse shell
D. Banner grabbing

Answer: A

NEW QUESTION 10
While engaging clients for a penetration test from highly regulated industries, which of the following is usually the MOST important to the clients from a business perspective?

A. Letter of engagement and attestation of findings
B. NDA and MSA
C. SOW and final report
D. Risk summary and executive summary

Answer: D

NEW QUESTION 12
An attacker uses SET to make a copy of a company's cloud-hosted web mail portal and sends an email m to obtain the CEO s login credentials Which of the following types of attacks is this an example of?

A. Elicitation attack
B. Impersonation attack
C. Spear phishing attack
D. Drive-by download attack

Answer: B

NEW QUESTION 13
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. Explogt chaining
B. Session hijacking
C. Dictionary
D. Karma

Answer: B

NEW QUESTION 16
A penetration tester wants to target NETBIOS name service. Which of the following is the most likely command to explogt the NETBIOS name service?

A. arPspoof
B. nmap
C. responder
D. burpsuite

Answer: C

NEW QUESTION 19
A penetration tester locates a few unquoted service paths during an engagement. Which of the following can the tester attempt to do with these?

A. Attempt to crack the service account passwords.
B. Attempt DLL hijacking attacks.
C. Attempt to locate weak file and folder permissions.
D. Attempt privilege escalation attack

Answer: D

NEW QUESTION 22
A client asks a penetration tester to add more addresses to a test currently in progress. Which of the following would defined the target list?

A. Rules of engagement
B. Master services agreement
C. Statement of work
D. End-user license agreement

Answer: D

NEW QUESTION 25
A penetration tester is perform initial intelligence gathering on some remote hosts prior to conducting a vulnerability < The tester runs the following command
nmap -D 192.168.1.1,192.168.1.2,192.168.1.3 -sV -o —max rate 2 192. 168.130
Which ol the following BEST describes why multiple IP addresses are specified?

A. The network is submitted as a /25 or greater and the tester needed to access hosts on two different subnets
B. The tester is trying to perform a more stealthy scan by including several bogus addresses
C. The scanning machine has several interfaces to balance the scan request across at the specified rate
D. A discovery scan is run on the first set of addresses, whereas a deeper, more aggressive scan is run against the latter host.

Answer: C

NEW QUESTION 29
A penetration tester has compromised a host. Which of the following would be the correct syntax to create a Netcat listener on the device?

A. nc -lvp 4444 /bin/bash
B. nc -vp 4444 /bin/bash
C. nc -p 4444 /bin/bash
D. nc -lp 4444 -e /bin/bash

Answer: D

NEW QUESTION 30
.....

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questons and Answers in PDF Format

PT0-001 Practice Exam Features:

* PT0-001 Questions and Answers Updated Frequently

* PT0-001 Practice Questions Verified by Expert Senior Certified Staff

* PT0-001 Most Realistic Questions that Guarantee you a Pass on Your FirstTry

* PT0-001 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year