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

CompTIA PenTest+ Certification Exam

Pass CompTIA PT0-002 Exam with 100% Guarantee

QUESTION 1

A consulting company is completing the ROE during scoping. Which of the following should be included in the ROE?

A. Cost ofthe assessment

B. Report distribution

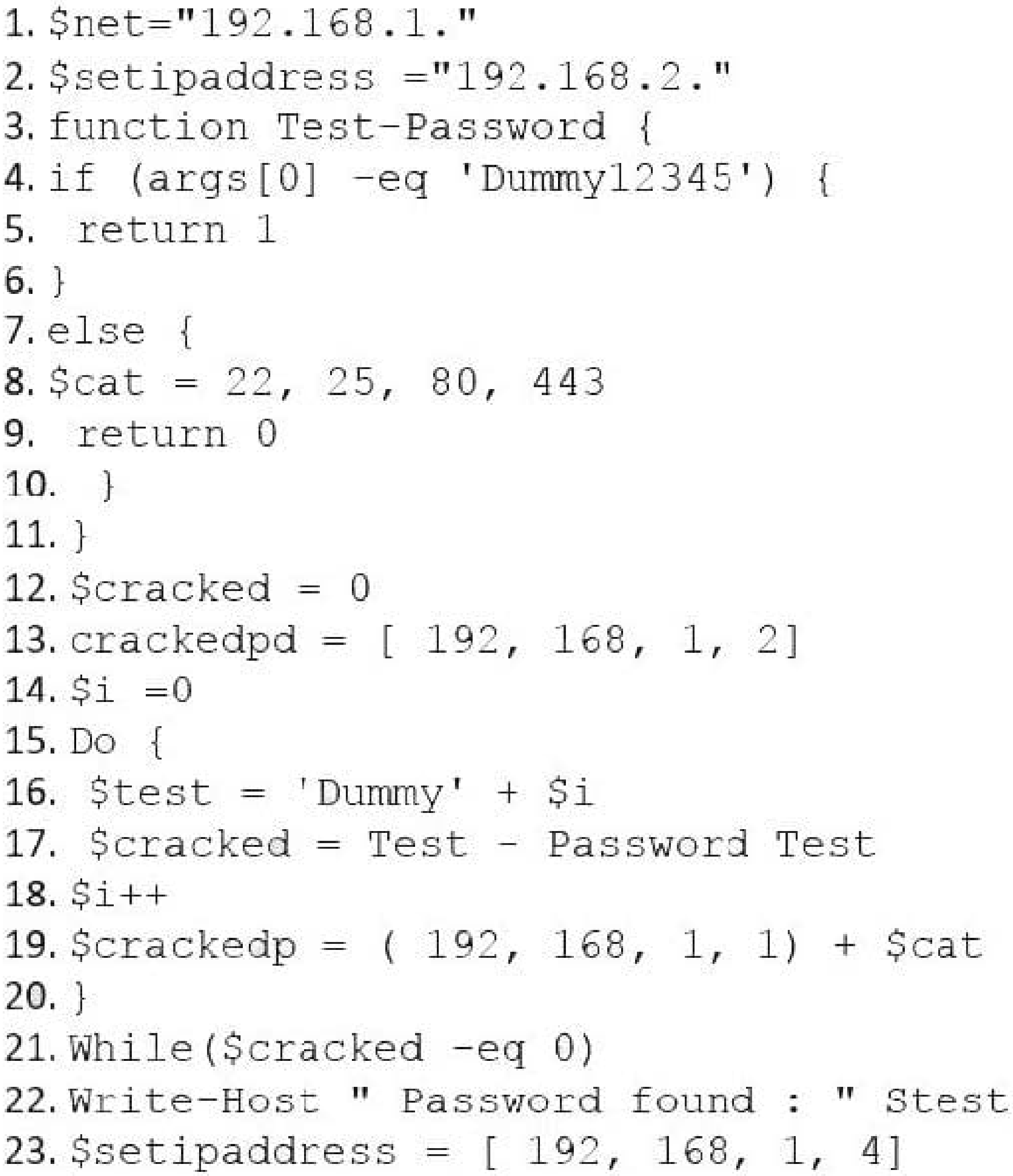
C. Testing restrictions

D. Liability

Correct Answer: B

QUESTION 2

The following PowerShell snippet was extracted from a log of an attacker machine:



```
1. $net="192.168.1."
2. $setipaddress ="192.168.2."
3. function Test-Password {
4. if (args[0] -eq 'Dummy12345') {
5.  return 1
6. }
7. else {
8. $cat = 22, 25, 80, 443
9.  return 0
10.  }
11. }
12. $cracked = 0
13. crackedpd = [ 192, 168, 1, 2]
14. $i =0
15. Do {
16.  $test = 'Dummy' + $i
17.  $cracked = Test - Password Test
18. $i++
19. $crackedp = ( 192, 168, 1, 1) + $cat
20. }
21. While($cracked -eq 0)
22. Write-Host " Password found : " Stest
23. $setipaddress = [ 192, 168, 1, 4]
```

A penetration tester would like to identify the presence of an array. Which of the following line numbers would define the array?

A. Line 8

B. Line 13

C. Line 19

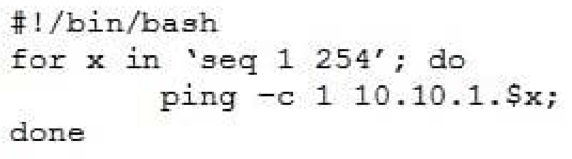
D. Line 20

Correct Answer: A

https://learn.microsoft.com/en-us/powershell/module/microsoft.powershell.core/about/about_arrays?view=powershell-7.3

QUESTION 3

A penetration tester writes the following script:



```
#!/bin/bash
for x in ‘seq 1 254’; do
        ping -c 1 10.10.1.$x;
done
```

Which of the following objectives is the tester attempting to achieve?

A. Determine active hosts on the network.

B. Set the TTL of ping packets for stealth.

C. Fill the ARP table of the networked devices.

D. Scan the system on the most used ports.

Correct Answer: A

QUESTION 4

A penetration tester is starting an assessment but only has publicly available information about the target company. The client is aware of this exercise and is preparing for the test. Which of the following describes the scope of the assessment?

A. Partially known environment testing

B. Known environment testing

C. Unknown environment testing

D. Physical environment testing

Correct Answer: C

QUESTION 5

A penetration tester conducted an assessment on a web server. The logs from this session show the following:

http://www.thecompanydomain.com/servicestatus.php?serviceID=892andserviceID=892 ` ; DROP TABLE SERVICES;-

Which of the following attacks is being attempted?

A. Clickjacking

B. Session hijacking

C. Parameter pollution

D. Cookie hijacking

E. Cross-site scripting

Correct Answer: C

PT0-002 Practice Test PT0-002 Study Guide PT0-002 Exam Questions