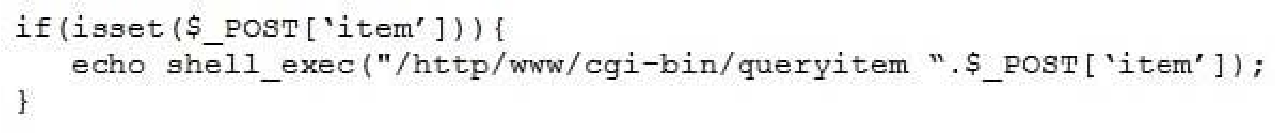
PT0-002^{Q&As}

CompTIA PenTest+ Certification Exam

Pass CompTIA PT0-002 Exam with 100% Guarantee

QUESTION 1

A penetration tester finds a PHP script used by a web application in an unprotected internal source code repository. After reviewing the code, the tester identifies the following:



```
if(isset($_POST[‘item’])){
   echo shell_exec("/http/www/cgi-bin/queryitem “.$_POST[‘item’]);
}
```

Which of the following tools will help the tester prepare an attack for this scenario?

A. Hydra and crunch

B. Netcat and cURL

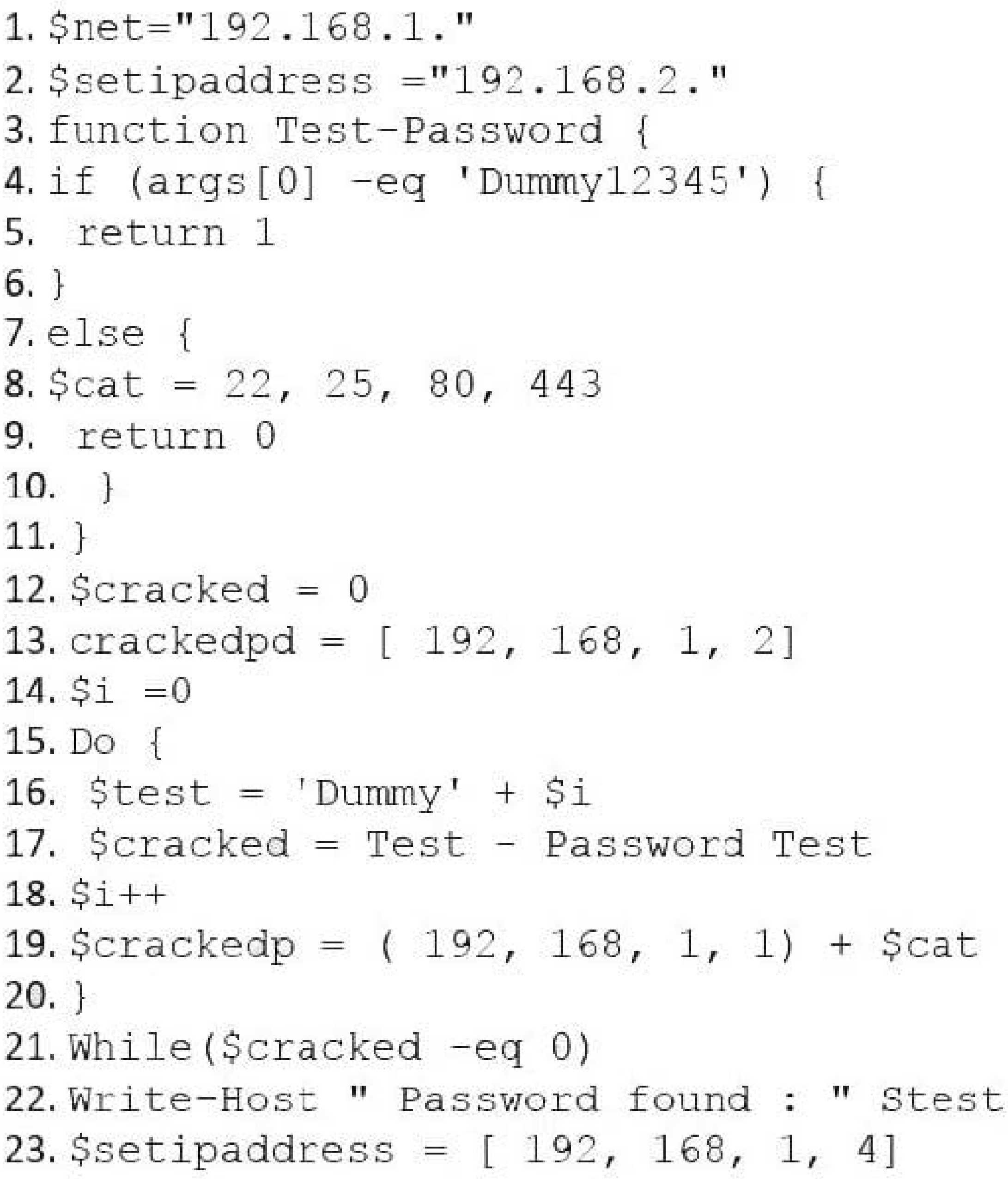
C. Burp Suite and DIRB

D. Nmap and OWASP ZAP

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

Which of the following tools provides Python classes for interacting with network protocols?

A. Responder

B. Impacket

C. Empire

D. PowerSploit

Correct Answer: B

Reference: https://github.com/SecureAuthCorp/impacket

QUESTION 4

A penetration tester was hired to perform a physical security assessment of an organization\\'s office. After monitoring the environment for a few hours, the penetration tester notices that some employees go to lunch in a restaurant nearby and leave their belongings unattended on the table while getting food.

Which of the following techniques would MOST likely be used to get legitimate access into the organization\\'s building without raising too many alerts?

A. Tailgating

B. Dumpster diving

C. Shoulder surfing

D. Badge cloning

Correct Answer: D

QUESTION 5

A company obtained permission for a vulnerability scan from its cloud service provider and now wants to test the security of its hosted data.

Which of the following should the tester verify FIRST to assess this risk?

A. Whether sensitive client data is publicly accessible

B. Whether the connection between the cloud and the client is secure

C. Whether the client\\'s employees are trained properly to use the platform

D. Whether the cloud applications were developed using a secure SDLC

Correct Answer: A