PT0-002^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.geekcert.com/pt0-002.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by CompTIA Official Exam Center

- **Instant Download** After Purchase
- **100% Money Back** Guarantee
- **365 Days** Free Update
- **800,000+** Satisfied Customers

QUESTION 1

Given the following code:

$p = (80, 110, 25)

$network = (192.168.0)

$range = 1 .. 254

$ErrorActionPreference = \\'silentlycontinue\\'

$Foreach ($add in $range)

$Foreach ($x in $p)

{ {$ip = "{0} . {1} -F $network, $add"

If (Test-Connection -BufferSize 32 -Count 1 -quiet -ComputerName $ip)

{$socket = new-object System.Net. Sockets. TcpClient (andip, $x)

If ($socket. Connected) { $ip $p open"

$socket. Close () }

}

}}

Which of the following tasks could be accomplished with the script?

A. Reverse shell

B. Ping sweep

C. File download

D. Port scan

Correct Answer: D

The script is performing a port scan on the network 192.168.0.0/24, by testing the connectivity of three ports (80, 110, 25) on each IP address in the range 1-254. A port scan is a technique used to identify open ports and services on a target host or network. It can be used for reconnaissance, vulnerability assessment, or penetration testing.

QUESTION 2

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

Netcat and cURL are tools that will help the tester prepare an attack for this scenario, as they can be used to establish a TCP connection, send payloads, and receive responses from the target web server. Netcat is a versatile tool that can create TCP or UDP connections and transfer data between hosts. cURL is a tool that can transfer data using various protocols, such as HTTP, FTP, SMTP, etc. The tester can use these tools to exploit the PHP script that executes shell commands with the value of the "item" variable.

QUESTION 3

A penetration tester utilized Nmap to scan host 64.13.134.52 and received the following results:

```
# nmap -T4 -v -oG - scanme.nmap.org
# Nmap 5.35DC18 scan initiated [time] as: nmap -T4 -A -v -cG -
scanme.nmap.org
# Ports scanned: TCP(1000;1, 3-4, 6-7, …,,65389) UDP (0;) PROTOCOLS(0;)
Host: 64.13.134.52 (scanme.nmap.org)   Status: Up
Host: 64.13.134.52 (scanme.nmap.org)
Ports:
22/open/tcp
25/closed/tcp
53/open/tcp
70/closed/tcp
80/open/tcp
113/closed/tcp
31337/closed/tcp
Ignored State: filtered (993) OS: Linux 2.6.13 - 2.6.31 Seq Index: 204 IP ID
Seq: All zeros
# Nmap done at [time] -- 1 IP address (1 host up) scanned in 21.90 seconds
```

Based on the output, which of the following services are MOST likely to be exploited? (Choose two.)

A. Telnet

B. HTTP

C. SMTP

D. DNS

E. NTP

F. SNMP

Correct Answer: BD

QUESTION 4

A penetration tester is able to use a command injection vulnerability in a web application to get a reverse shell on a system After running a few commands, the tester runs the following:

python -c \\'import pty; pty.spawn("/bin/bash")\\'

Which of the following actions Is the penetration tester performing?

A. Privilege escalation

B. Upgrading the shell

C. Writing a script for persistence

D. Building a bind shell

Correct Answer: B

The penetration tester is performing an action called upgrading the shell, which means improving the functionality and interactivity of the shell. By running the python command, the penetration tester is spawning a new bash shell that has features such as tab completion, command history, and job control. This can help the penetration tester to execute commands more easily and efficiently.

QUESTION 5

A penetration tester exploited a vulnerability on a server and remotely ran a payload to gain a shell. However, a connection was not established, and no errors were shown on the payload execution. The penetration tester suspected that a network device, like an IPS or next-generation firewall, was dropping the connection. Which of the following payloads are MOST likely to establish a shell successfully?

A. windows/x64/meterpreter/reverse_tcp

B. windows/x64/meterpreter/reverse_http

C. windows/x64/shell_reverse_tcp

D. windows/x64/powershell_reverse_tcp

E. windows/x64/meterpreter/reverse_https

Correct Answer: B

These two payloads are most likely to establish a shell successfully because they use HTTP or HTTPS protocols, which are commonly allowed by network devices and can bypass firewall rules or IPS signatures. The other payloads use TCP

protocols, which are more likely to be blocked or detected by network devices.