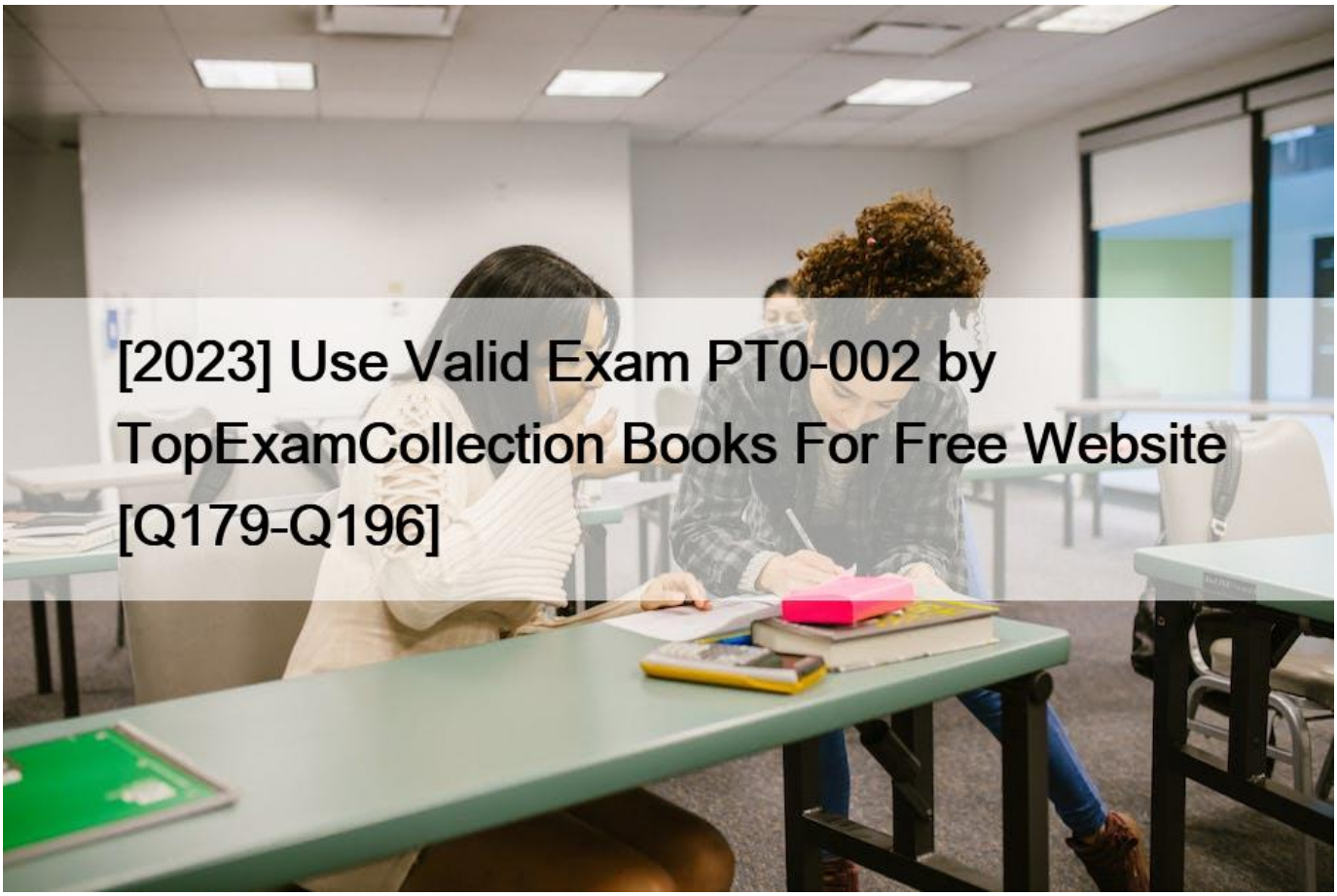
[2023 Use Valid Exam PT0-002 by TopExamCollection Books For Free Website [Q179-Q196



[2023] Use Valid Exam PT0-002 by TopExamCollection Books For Free Website
Free CompTIA PenTest+ PT0-002 Official Cert Guide PDF Download

CompTIA PenTest+ (PT0-002) Certification Exam is a vendor-neutral certification that validates the knowledge and skills of cybersecurity professionals involved in penetration testing and vulnerability management. PT0-002 exam is designed for cybersecurity professionals who want to develop core knowledge and skills in identifying, exploiting, reporting, and managing vulnerabilities in network infrastructures. CompTIA PenTest+ certification aims to provide professionals with the ability to plan and conduct penetration tests that simulate real-world attacks and find vulnerabilities that can be exploited by the attackers.

QUESTION 179

A penetration tester analyzed a web-application log file and discovered an input that was sent to the company’s web application. The input contains a string that says “WAITFOR.” Which of the following attacks is being attempted?
* SQL injection
* HTML injection

* Remote command injection
* DLL injection

Explanation

WAITFOR can be used in a type of SQL injection attack known as time delay SQL injection or blind SQL injection34. This attack works on the basis that true or false queries can be answered by the amount of time a request takes to complete. For example, an attacker can inject a WAITFOR command with a delay argument into an input field of a web application that uses SQL Server as its database. If the query returns true, then the web application will pause for the specified period of time before responding; if the query returns false, then the web application will respond immediately. By observing the response time, the attacker can infer information about the database structure and data1.

Based on this information, one possible answer to your question is A.

SQL injection, because it is an attack that exploits a vulnerability in a web application that allows an attacker to execute arbitrary SQL commands on the database server.

QUESTION 180

Which of the following would assist a penetration tester the MOST when evaluating the susceptibility of top-level executives to social engineering attacks?

* Scraping social media for personal details
* Registering domain names that are similar to the target company’s
* Identifying technical contacts at the company
* Crawling the company’s website for company information

Explanation

Scraping social media for personal details can help a penetration tester craft personalized and convincing social engineering attacks against top-level executives, who may share sensitive or confidential information on their profiles. Registering domain names that are similar to the target company’s can be used for phishing or typosquatting attacks, but not specifically against executives. Identifying technical contacts at the company can help with reconnaissance, but not with social engineering. Crawling the company’s website for company information can provide general background knowledge, but not specific details about executives.

QUESTION 181

A penetration tester will be performing a vulnerability scan as part of the penetration test on a client’s website.

The tester plans to run several Nmap scripts that probe for vulnerabilities while avoiding detection. Which of the following Nmap options will the penetration tester MOST likely utilize?

* -8 -T0
* –script “http*vuln*”
* -sn
* -O -A

Explanation

Nmap is a tool that can perform network scanning and enumeration by sending packets to hosts and analyzing their responses. The command Nmap -p 445 -n -T4 –open 172.21.0.0/16 would scan for SMB port 445 over a

/16 network with the following options:

-p 445 specifies the port number to scan.

-n disables DNS resolution, which can speed up the scan by avoiding unnecessary queries.

-T4 sets the timing template to aggressive, which increases the speed of the scan by sending packets faster and waiting less for responses.

-open only shows hosts that have open ports, which can reduce the output and focus on relevant results.

The other commands are not optimal for scanning SMB port 445 over a /16 network when stealth is not a concern and the task is time sensitive.

QUESTION 182

A penetration tester runs a scan against a server and obtains the following output:

21/tcp open ftp Microsoft ftpd

| ftp-anon: Anonymous FTP login allowed (FTP code 230)

| 03-12-20 09:23AM 331 index.aspx

| ftp-syst:

135/tcp open msrpc Microsoft Windows RPC

139/tcp open netbios-ssn Microsoft Windows netbios-ssn

445/tcp open microsoft-ds Microsoft Windows Server 2012 Std

3389/tcp open ssl/ms-wbt-server

| rdp-ntlm-info:

| Target Name: WEB3

| NetBIOS_Computer_Name: WEB3

| Product_Version: 6.3.9600

|_ System_Time: 2021-01-15T11:32:06+00:00

8443/tcp open http Microsoft IIS httpd 8.5

| http-methods:

|_ Potentially risky methods: TRACE

|_http-server-header: Microsoft-IIS/8.5

|_http-title: IIS Windows Server

Which of the following command sequences should the penetration tester try NEXT?
* ftp 192.168.53.23
* smbclient \WEB3IPC$ -I 192.168.53.23 -U guest
* ncrack -u Administrator -P 15worst_passwords.txt -p rdp 192.168.53.23
* curl -X TRACE https://192.168.53.23:8443/index.aspx
* nmap –script vuln -sV 192.168.53.23

QUESTION 183

During an engagement, a penetration tester found the following list of strings inside a file:

```
3af068faa81326ffe6ca48e2ab36a779
48ec2f4f526303a9ded67938e6ce11c6
9493bf035c534197d9810a5e65a10682
C847b4a2e76ec1f9cbbbe3dd0d6d5e8
ed225542767a810e[illegible]bf640164b140
cfbe1fdd6e600c9c9abd8c947f272ef4
c05[illegible]a69bcc91f56a7e0a6c391ad79
9ee3564cbf15421ebabc43dcb67949ad
5a2ad0bcb902e20c4efcf057b01050be
4865a2ed25ed18515b7e97beb2b40346
b0236938a6518fc65b72159687e3a27b
9c96354712595ef2ff96675496d3a464
a5ab3f6c6159b85209ea0c186531a49f
9b38816e791f1400245f4c629a503bc8
d12e624a20d54fd3b34b89ee7169df17
```

Which of the following is the BEST technique to determine the known plaintext of the strings?
* Dictionary attack
* Rainbow table attack
* Brute-force attack
* Credential-stuffing attack

QUESTION 184

The following output is from reconnaissance on a public-facing banking website:

```
...
Start 2021-02-02 18:24:59 -->> 192.168.1.66:443 (192.168.1.66) <<--
rDNS (192.168.1.66): centralbankwebservice.local
Service detected: HTTP

Testing protocols via sockets except NPN+ALPN
SSLv2 not offered (OK)
SSLv3 not offered (OK)
TLS 1 offered (deprecated)
TLS 1.1 not offered
TLS 1.2 not offered and downgraded to a weaker protocol
TLS 1.3 not offered and downgraded to a weaker protocol
NPN/SPDY not offered
ALPN/HTTP2 not offered
Testing cipher categories
NULL ciphers (no encryption) not offered (OK)
Anonymous NULL Ciphers (no authentication) not offered (OK)
Export ciphers (w/o ADH+NULL) not offered (OK)
LOW: 64 Bit + DES, RC[2,4] (w/o export) offered (NOT ok)
Triple DES Ciphers / IDEA offered
Obsolete CBC ciphers (AES, ARIA etc.) offered
Strong encryption (AEAD ciphers) not offered

Testing robust (perfect) forward secrecy, (P)FS -- omitting Null Authentication/Encryption, 3DES, RC4
No ciphers supporting Forward Secrecy offered

Testing server preferences
Has server cipher order? no (NOT ok)
Negotiated protocol TLSv1
Negotiated cipher AES256-SHA (limited sense as client will pick)
...
```


Based on these results, which of the following attacks is MOST likely to succeed?

* A birthday attack on 64-bit ciphers (Sweet32)
* An attack that breaks RC4 encryption
* An attack on a session ticket extension (Ticketbleed)
* A Heartbleed attack

QUESTION 185

Penetration tester who was exclusively authorized to conduct a physical assessment noticed there were no cameras pointed at the dumpster for company. The penetration tester returned at night and collected garbage that contained receipts for recently purchased networking :. The models of equipment purchased are vulnerable to attack. Which of the following is the most likely next step for the penetration?

* Alert the target company of the discovered information.
* Verify the discovered information is correct with the manufacturer.
* Scan the equipment and verify the findings.
* Return to the dumpster for more information.

Explanation

The most likely next step for the penetration tester is to scan the equipment and verify the findings, which is a process of using tools or techniques to probe or test the target equipment for vulnerabilities or weaknesses that can be exploited. Scanning and verifying the findings can help the penetration tester confirm that the models of equipment purchased are vulnerable to attack, and identify the specific vulnerabilities or exploits that affect them. Scanning and verifying the findings can also help the penetration tester prepare for the next steps of the assessment, such as exploiting or reporting the vulnerabilities. Scanning and verifying the findings can be done by using tools such as Nmap, which can scan hosts and networks for ports, services, versions, OS, or other information1, or

Metasploit, which can exploit hosts and networks using various payloads or modules2. The other options are not likely next steps for the penetration tester. Alerting the target company of the discovered information is not a next step, but rather a final step, that involves reporting the findings and recommendations to the client after completing the assessment. Verifying the discovered information with the manufacturer is not a next step, as it may not provide accurate or reliable information about the vulnerabilities or exploits that affect the equipment, and it may also alert the manufacturer or the client of the assessment. Returning to the dumpster for more information is not a next step, as it may not yield any more useful or relevant information than what was already collected from the receipts.

QUESTION 186

A penetration tester who is conducting a vulnerability assessment discovers that ICMP is disabled on a network segment. Which of the following could be used for a denial-of-service attack on the network segment?
* Smurf
* Ping flood
* Fraggle
* Ping of death

Explanation

Fraggle attack is same as a Smurf attack but rather than ICMP, UDP protocol is used. The prevention of these attacks is almost identical to Fraggle attack.

Ref: https://www.okta.com/identity-101/fraggle-attack/

QUESTION 187

During enumeration, a red team discovered that an external web server was frequented by employees. After compromising the server, which of the following attacks would best support ————company systems?
* Aside-channel attack
* A command injection attack
* A watering-hole attack
* A cross-site scripting attack

Explanation

The best attack that would support compromising company systems after compromising an external web server frequented by employees is a watering-hole attack, which is an attack that involves compromising a website that is visited by a specific group of users, such as employees of a target company, and injecting malicious code or content into the website that can infect or exploit the users’ devices when they visit the website. A watering-hole attack can allow an attacker to compromise company systems by targeting their employees who frequent the external web server, and taking advantage of their trust or habit of visiting the website. A watering-hole attack can be performed by using tools such as BeEF, which is a tool that can hook web browsers and execute commands on them2. The other options are not likely attacks that would support compromising company systems after compromising an external web server frequented by employees. A side-channel attack is an attack that involves exploiting physical characteristics or implementation flaws of a system or device, such as power consumption, electromagnetic radiation, timing, or sound, to extract sensitive information or bypass security mechanisms. A command injection attack is an attack that exploits a vulnerability in a system or application that allows an attacker to execute arbitrary commands on the underlying OS or shell. A cross-site scripting attack is an attack that exploits a vulnerability in a web application that allows an attacker to inject malicious scripts into web pages that are viewed by other users.

QUESTION 188

Penetration-testing activities have concluded, and the initial findings have been reviewed with the client.

Which of the following best describes the NEXT step in the engagement?
* Acceptance by the client and sign-off on the final report
* Scheduling of follow-up actions and retesting
* Attestation of findings and delivery of the report
* Review of the lessons learned during the engagement

QUESTION 189

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?
* Line 8
* Line 13
* Line 19
* Line 20

Explanation

$X=2,4,6,8,9,20,5

$y=[System.Collections.ArrayList]$X

$y.RemoveRange(1,2) As you can see the arrat has no brackets and no periods. IT HAS SEMICOLLINS TO SEPERATE THE

LISTED ITEMS OR VALUES.

QUESTION 190

A penetration tester is assessing a wireless network. Although monitoring the correct channel and SSID, the tester is unable to capture a handshake between the clients and the AP. Which of the following attacks is the MOST effective to allow the penetration tester to capture a handshake?

* Key reinstallation
* Deauthentication
* Evil twin
* Replay

Explanation

Deauth will make the client connect again

QUESTION 191

A penetration tester wrote the following script to be used in one engagement:

```
#!/usr/bin/python
import socket,sys
ports = [21,22,23,25,80,139,443,445,3306,3389]
if len(sys.argv) == 2:
        target = socket.gethostbyname(sys.argv[1])
else:
        print("Too few arguments.")
        print("Syntax: python {} <>".format(sys.argv[0]))
        sys.exit()
try:
        for port in ports:
                s = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
                s.settimeout(2)
                results = s.connect_ex((target,port))
                if result == 0:
                        print("Port {} is opened".format(port))
except KeyboardInterrupt:
        print("Exiting...")
        sys.exit()
```


Which of the following actions will this script perform?

* Look for open ports.
* Listen for a reverse shell.
* Attempt to flood open ports.
* Create an encrypted tunnel.

QUESTION 192

A penetration tester was brute forcing an internal web server and ran a command that produced the following output:

```
$ dirb http://172.16.100.10:3000
-----------------
DURB v2.22
By The Dark Raver
-----------------
START_TIME: Wed Feb 3 13:06:18 2021
URL_BASE: http://172.16.100.10:3000
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt
-----------------
GENERATED WORDS: 4612
---- Scanning URL: http://172.16.100.10:3000 ----
+ http://172.16.100.10:3000/ftp (CODE:200|SIZE:11071)
+ http://172.16.100.10:3000/profile (CODE:500|SIZE:1151)
+ http://172.16.100.10:3000/promotion (CODE:200|SIZE:6586)
+ http://172.16.100.10:3000/robots.txt (CODE:200|SIZE:28)
+ http://172.16.100.10:3000 /Video (CODE:200|SIZE:10075518)

-----------------
END_TIME: Wed Feb 3 13:07:53 2021
DOWNLOADED: 4612 - FOUND: 5
```


However, when the penetration tester tried to browse the URL http://172.16.100.10:3000/profile, a blank page was displayed.

Which of the following is the MOST likely reason for the lack of output?
* The HTTP port is not open on the firewall.
* The tester did not run sudo before the command.
* The web server is using HTTPS instead of HTTP.
* This URI returned a server error.

QUESTION 193

A tester who is performing a penetration test on a website receives the following output:

Warning: mysql_fetch_array() expects parameter 1 to be resource, boolean given in /var/www/search.php on line 62 Which of the following commands can be used to further attack the website?
* <script>var adr= ‘../evil.php?test=’ + escape(document.cookie);</script>
* ../../../../../../../../../../etc/passwd
* /var/www/html/index.php;whoami
* 1 UNION SELECT 1, DATABASE(),3–

QUESTION 194

A security professional wants to test an IoT device by sending an invalid packet to a proprietary service listening on TCP port 3011. Which of the following would allow the security professional to easily and programmatically manipulate the TCP header length and checksum using arbitrary numbers and to observe how the proprietary service responds?
* Nmap
* tcpdump
* Scapy
* hping3

QUESTION 195

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 combinations of tools would the penetration tester use to exploit this script?

* Hydra and crunch
* Netcat and cURL
* Burp Suite and DIRB
* Nmap and OWASP ZAP

QUESTION 196

A penetration tester needs to access a building that is guarded by locked gates, a security team, and cameras. Which of the following is a technique the tester can use to gain access to the IT framework without being detected?

* Pick a lock.
* Disable the cameras remotely.
* Impersonate a package delivery worker.
* Send a phishing email.