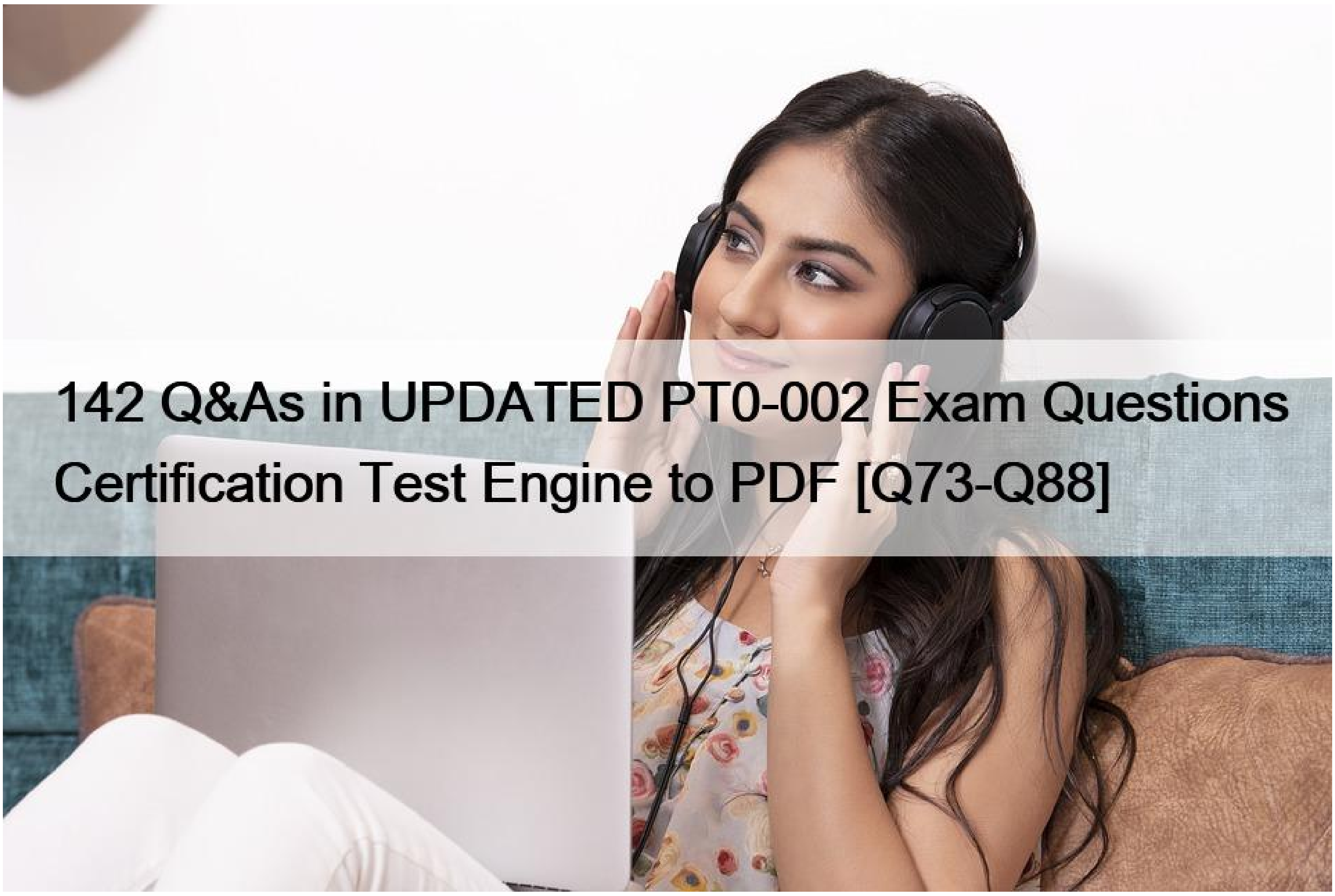
142 Q&As in UPDATED PT0-002 Exam Questions Certification Test Engine to PDF [Q73-Q88


142 Q&As in UPDATED PT0-002 Exam Questions
Certification Test Engine to PDF [Q73-Q88]

142 Q&As in UPDATED PT0-002 Exam Questions Certification Test Engine to PDF Get The Important Preparation Guide With PT0-002 Dumps NO.73 A red team gained access to the internal network of a client during an engagement and used the Responder tool to capture important dat

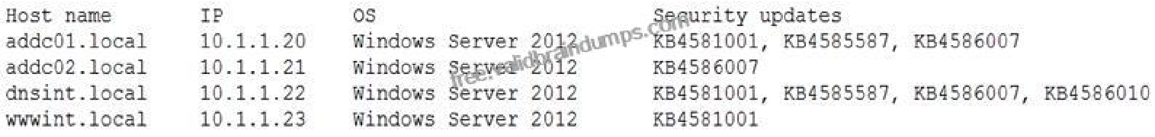
a. Which of the following was captured by the testing team?
* Multiple handshakes
* IP addresses
* Encrypted file transfers
* User hashes sent over SMB

NO.74 A red-team tester has been contracted to emulate the threat posed by a malicious insider on a company&#8217;s network, with the constrained objective of gaining access to sensitive personnel files. During the assessment, the red-team tester identifies an artifact indicating possible prior compromise within the target environment.

Which of the following actions should the tester take?
* Perform forensic analysis to isolate the means of compromise and determine attribution.
* Incorporate the newly identified method of compromise into the red team&#8217;s approach.

* Create a detailed document of findings before continuing with the assessment.
* Halt the assessment and follow the reporting procedures as outlined in the contract.

NO.75 A penetration tester conducted a vulnerability scan against a client&#8217;s critical servers and found the following:



```
Host name      IP          OS                    Security updates
addc01.local   10.1.1.20   Windows Server 2012   KB4581001, KB4585587, KB4586007
addc02.local   10.1.1.21   Windows Server 2012   KB4586007
dnsint.local   10.1.1.22   Windows Server 2012   KB4581001, KB4585587, KB4586007, KB4586010
wwwint.local   10.1.1.23   Windows Server 2012   KB4581001
```

Which of the following would be a recommendation for remediation?
* Deploy a user training program
* Implement a patch management plan
* Utilize the secure software development life cycle
* Configure access controls on each of the servers

NO.76 A penetration tester is exploring a client&#8217;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=&#8221;en&#8221;>

```
<head>

<meta name=&#8221;viewport&#8221; content=&#8221;width=device-width&#8221; />

<meta http-equiv=&#8221;Content-Type&#8221; content=&#8221;text/html; charset=utf-8&#8243; />

<title>WordPress &#8250; ReadMe</title>

<link rel=&#8221;stylesheet&#8221; href=&#8221;wp-admin/css/install.css?ver=20100228&#8243; type=&#8221;text/css&#8221; />

</head>
```

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

* Burp Suite
* DirBuster
* WPScan
* OWASP ZAP

NO.77 A penetration tester runs the unshadow command on a machine. Which of the following tools will the tester most likely use NEXT?

* John the Ripper
* Hydra
* Mimikatz
* Cain and Abel

NO.78 Which of the following tools would be MOST useful in collecting vendor and other security-relevant information for IoT devices to support passive reconnaissance?

* Shodan
* Nmap
* WebScarab-NG
* Nessus

NO.79 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?

* nmap -vv sUV -p 53, 123-159 10.10.1.20/24 -oA udpscan
* nmap -vv sUV -p 53,123,161-162 10.10.1.20/24 -oA udpscan
* nmap -vv sUV -p 53,137-139,161-162 10.10.1.20/24 -oA udpscan
* nmap -vv sUV -p 53, 122-123, 160-161 10.10.1.20/24 -oA udpscan

NO.80 A penetration tester has been contracted to review wireless security. The tester has deployed a malicious wireless AP that mimics the configuration of the target enterprise WiFi. The penetration tester now wants to try to force nearby wireless stations to connect to the malicious AP. Which of the following steps should the tester take NEXT?

* Send deauthentication frames to the stations.
* Perform jamming on all 2.4GHz and 5GHz channels.
* Set the malicious AP to broadcast within dynamic frequency selection channels.
* Modify the malicious AP configuration to not use a pre-shared key.

https://steemit.com/informatica/@jordiurbina1/tutorial-hacking-wi-fi-wireless-networks-with-wifislax

NO.81 A penetration tester has been given eight business hours to gain access to a client&#8217;s financial system. Which of the following techniques will have the highest likelihood of success?

- Attempting to tailgate an employee going into the client&#8217;s workplace
- Dropping a malicious USB key with the company&#8217;s logo in the parking lot
- Using a brute-force attack against the external perimeter to gain a foothold
- Performing spear phishing against employees by posing as senior management

NO.82 A penetration tester wants to perform reconnaissance without being detected. Which of the following activities have a MINIMAL chance of detection? (Choose two.)

- Open-source research
- A ping sweep
- Traffic sniffing
- Port knocking
- A vulnerability scan
- An Nmap scan

NO.83 A penetration tester obtained the following results after scanning a web server using the dirb utility:

```
&#8230;

GENERATED WORDS: 4612

&#8212;-

Scanning URL: http://10.2.10.13/ &#8212;-

+

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)

&#8230;

DOWNLOADED: 4612 &#8211; FOUND: 4
```

Which of the following elements is MOST likely to contain useful information for the penetration tester?

- index.html
- about
- info

* home.html

NO.84 A penetration tester was able to gain access successfully to a Windows workstation on a mobile client&#8217;s laptop. Which of the following can be used to ensure the tester is able to maintain access to the system?
* schtasks /create /sc /ONSTART /tr C:TempWindowsUpdate.exe
* wmic startup get caption,command
* crontab -l; echo &#8220;@reboot sleep 200 && ncat -lvp 4242 -e /bin/bash&#8221;) | crontab 2>/dev/null
* sudo useradd -ou 0 -g 0 user

NO.85 Which of the following should a penetration tester consider FIRST when engaging in a penetration test in a cloud environment?
* Whether the cloud service provider allows the penetration tester to test the environment
* Whether the specific cloud services are being used by the application
* The geographical location where the cloud services are running
* Whether the country where the cloud service is based has any impeding laws

NO.86 A penetration tester is explaining the MITRE ATT&CK framework to a company&#8217;s chief legal counsel.

Which of the following would the tester MOST likely describe as a benefit of the framework?
* Understanding the tactics of a security intrusion can help disrupt them.
* Scripts that are part of the framework can be imported directly into SIEM tools.
* The methodology can be used to estimate the cost of an incident better.
* The framework is static and ensures stability of a security program overtime.

NO.87 A penetration tester has been given an assignment to attack a series of targets in the 192.168.1.0/24 range, triggering as few alarms and countermeasures as possible.

Which of the following Nmap scan syntaxes would BEST accomplish this objective?
* nmap -sT -vvv -O 192.168.1.2/24 -PO
* nmap -sV 192.168.1.2/24 -PO
* nmap -sA -v -O 192.168.1.2/24
* nmap -sS -O 192.168.1.2/24 -T1

NO.88 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 firewall or IPS blocked the scan.
* The penetration tester used unsupported flags.
* The edge network device was disconnected.
* The scan returned ICMP echo replies.

Prepare With Top Rated High-quality PT0-002 Dumps For Success in Exam:
https://www.validbraindumps.com/PT0-002-exam-prep.html]