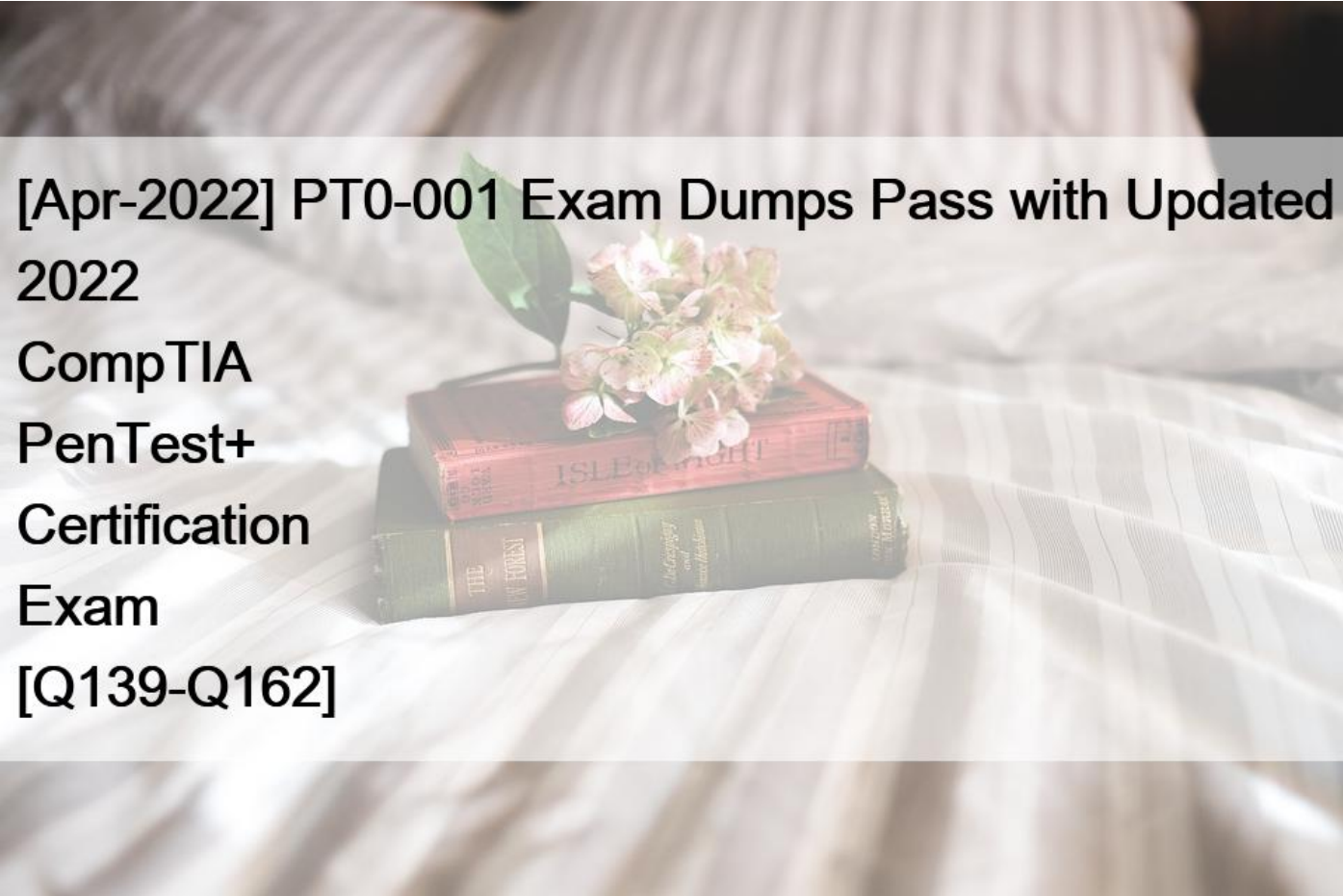


[Apr-2022 PT0-001 Exam Dumps Pass with Updated 2022 CompTIA PenTest+ Certification Exam [Q139-Q162]



**[Apr-2022] PT0-001 Exam Dumps Pass with Updated
2022
CompTIA
PenTest+
Certification
Exam
[Q139-Q162]**

[Apr-2022] PT0-001 Exam Dumps Pass with Updated 2022 CompTIA PenTest+ Certification Exam
Free PT0-001 Exam Dumps to Pass Exam Easily

Difficulty in writing PT0-001 Exam

Candidates face many problems when they start preparing for the CompTIA PT0-001 exam. If a candidate wants to prepare his for the CompTIA PT0-001 exam without any problem and get good grades in the exam. Then they have to choose the best **CompTIA PT0-001 exam dumps** for real exam questions practice. There are many websites that are offering the latest CompTIA PT0-001 exam questions and answers but these questions are not verified by CompTIA certified experts and that's why many are failed in their just first attempt. VCEPrep is the best platform which provides the candidate with the necessary CompTIA PT0-001 questions that will help him to pass the CompTIA PT0-001 exam on the first time. The candidate will not have to take the CompTIA PT0-001 exam twice because with the help of **CompTIA PT0-001 exam dumps** Candidate will have every valuable material required to pass the CompTIA PT0-001 exam. We are providing the latest and actual questions and that is the reason why this is the one that he needs to use and there are no chances to fail when a candidate will have valid braindumps from VCEPrep. We have the guarantee that the questions that we have will be the ones that will pass candidate in the CompTIA PT0-001 exam in the very first attempt.

NEW QUESTION 139

A company requested a penetration tester review the security of an in-house-developed Android application. The penetration tester received an APK file to support the assessment.

The penetration tester wants to run SAST on the APK file. Which of the following preparatory steps must the penetration tester do FIRST? (Select TWO)

- * Convert to JAR
- * Decompile
- * Cross-compile the application
- * Convert JAR files to DEX
- * Re-sign the APK
- * Attach to ADB

NEW QUESTION 140

The results of a basic compliance scan show a subset of assets on a network. This data differs from what is shown on the network architecture diagram, which was supplied at the beginning of the test. Which of the following are the MOST likely causes for this difference? (Select TWO)

- * Storage access
- * Limited network access
- * Misconfigured DHCP server
- * Incorrect credentials
- * Network access controls

NEW QUESTION 141

After successfully enumerating users on an Active Directory domain controller using enum4linux a penetration tester wants to conduct a password-guessing attack Given the below output:

```
enum4linux_output.txt:  
Starting enum4linux v0.8.2 ( https://labs.portcullis.co.uk/application/enum4linux/ ) on Mon Feb 5 11:36:22  
  
---- Users on 192.168.2.55 ----  
index: 0x1 RID: 0x1f4 acb: 0x210 Account: Administrator Name: Administrator account for administering the computer  
index 0x2 RID: 0x3ee acb: 0x10 Account test Name: test  
index 0x3 RID: 0x3ed acb: 0x215 Account: Guest Name: Guest Desc: Built-in account for guest access to the computer  
index 0x4: RID: 0x1f5 acb: 0x214 Account: Test_User Name: Test User Account: Desc:  
  
user:[Administrator] rid:[0x1f4]  
user:[test] rid:[0x3ee]  
user:[Guest] rid:[0x3ed]  
user:[Test_User] rid:[0x1f5]
```

Which of the following can be used to extract usernames from the above output prior to conducting the attack?

- * cat enum4linux_output.txt > grep -v user | sed ‘s/[//’ | sed ‘s/[//’ | sed ‘s/[//’ | sed ‘s/[//’ 2> usernames.txt
- * grep user enum4linux_output.txt | awk ‘{print \$1}’ | cut -d[-S2 | cut -d[-f1 > username.txt
- * grep -i rid v< enum4linux_output.txt ’ | cut -d: -S2 | cut -d[-f1 > usernames.txt
- * cut -d: -f2 enum4linux_output.txt | awk ‘{print \$2}’ | cut -d: -f1 > usernames.txt

NEW QUESTION 142

A manager calls upon a tester to assist with diagnosing an issue within the following Python script:

```
#!/usr/bin/python
```

```
s = '#Administrator#'
```

The tester suspects it is an issue with string slicing and manipulation Analyze the following code segment and drag and drop the correct output for each string manipulation to its corresponding code segment Options may be used once or not at all

Code segment	Output		
s[4:8]		ita	imda
s[4:12:2]		inis	nist
s[3::-1]		nsrt	rota
s[-7:-2]		snmA	trat

Code segment	Output		
s[4:8]	nsrt	ita	imda
s[4:12:2]	snmA	inis	nist
s[3::-1]	trat	nsrt	rota
s[-7:-2]	imda	snmA	trat

NEW QUESTION 143

A tester has captured a NetNTLMv2 hash using Responder Which of the following commands will allow the tester to crack the hash using a mask attack?

- * hashcat -m 5600 -r rulea/beat64.rule hash.txt wordliat.txt
- * hashcax -m 5000 hash.txt
- * hashc&t -m 5600 -a 3 haah.txt ?a?a?a?a?a?a
- * hashcat -m 5600 -o resulta.txt hash.txt wordliat.txt

NEW QUESTION 144

A security analyst has uncovered a suspicious request in the logs for a web application. Given the following URL:

http://www.company-site.com/about.php?i=_V_V_V_V_VetcVpasswd

Which of the following attack types is MOST likely to be the vulnerability?

- * Directory traversal
- * Cross-site scripting
- * Remote file inclusion
- * User enumeration

NEW QUESTION 145

A penetration tester runs the following on a machine:

```
a.txt:
corp/username%password
corp/John Doe%password
corp/Jane Doe %password

command:
for i in $(cat a.txt); do echo $i; done | wc -l
```

Which of the following will be returned?

- * 1
- * 3
- * 5
- * 6

NEW QUESTION 146

A penetration tester has gained access to a marketing employee's device. The penetration tester wants to ensure that if the access is discovered, control of the device can be regained.

Which of the following actions should the penetration tester use to maintain persistence to the device? (Select TWO.)

- * Place an entry in HKLMSoftwareMicrosoftCurrentVersionRun to call au57d.ps1.
- * Place an entry in C:windowssystem32driversetchosts for 12.17.20.10 badcomptia.com.
- * Place a script in C:users%username%localappdata\roaming\tempau57d.ps1.
- * Create a fake service in Windows called RTAudio to execute manually.
- * Place an entry for RTAudio in HKLMCurrentControlSet\Services\RTAudio.
- * Create a schedule task to call C:windowssystem32driversetchosts.

NEW QUESTION 147

A penetration tester is checking a script to determine why some basic persisting.

The expected result was the program outputting `“True.”`

```
root:~# cat ./test.sh
#!/bin/bash
source=10
let dest=5+5

if [ 'source' = 'dest' ]; then
    echo "True"
else
    echo "False"
fi
#End of File

root:~# ./test.sh
False
```

Given the output from the console above, which of the following explains how to correct the errors in the script? (Select TWO)

- * Change `fi` to `Endlf`
- * Remove the `let` in front of `dest=5+5`;
- * Change the `=` to `-eq`;
- * Change `*source*` and `dest` to `$source`; and `$dest`;
- * Change `else` to `elif`.

NEW QUESTION 148

After performing a security assessment for a firm, the client was found to have been billed for the time the client's test environment was unavailable. The Client claims to have been billed unfairly. Which of the following documents would MOST likely be able to provide guidance in such a situation?

- * SOW
- * NDA
- * EULA
- * BRA

NEW QUESTION 149

A penetration tester has been asked to conduct OS fingerprinting with Nmap using a company-provided text file that contains a list of IP addresses. Which of the following are needed to conduct this scan? (Choose two.)

- * `-O`
- * `-iL`
- * `-sV`
- * `-sS`
- * `-oN`
- * `-oX`

NEW QUESTION 150

A penetration tester attempts to perform a UDP port scan against a remote target using an Nmap tool installed onto a non-Kali Linux image. For some reason, the UDP scan falls to start. Which of the following would MOST likely help to resolve the issue?

- * Install the latest version of the tool.
- * Review local iptables for existing drop rules.
- * Relaunch the tool with elevated privileges.
- * Enable both IPv4 and IPv6 forwarding.

NEW QUESTION 151

In a physical penetration testing scenario, the penetration tester obtains physical access to a laptop following .s a potential NEXT step to extract credentials from the device?

- * Brute force the user's password.
- * Perform an ARP spoofing attack.
- * Leverage the BeEF framework to capture credentials.
- * Conduct LLMNR/NETBIOS-ns poisoning.

NEW QUESTION 152

A company hires a penetration tester to determine if there are any vulnerabilities in its new VPN concentrator installation with an external IP of 100.170.60.5. Which of the following commands will test if the VPN is available?

- * fpipe.exe -l 8080 -r 80 100.170.60.5
- * ike-scan -A -t 1 --sourceip=spoof_ip 100.170.60.5
- * nmap -sS -A -f 100.170.60.5
- * nc 100.170.60.5 8080 /bin/sh

NEW QUESTION 153

A company hires a penetration tester to determine if there are any vulnerabilities in its new VPN concentrator installation with an external IP of 100.170.60.6. Which of the following commands will test if the VPN is available?

- * fpipe.exe -l 8080 -r 80 100.170.60.5
- * ike-scan -A -t 1 --sourceip=spoof_ip 100.170.60.5
- * nmap -sS -A -f 100.170.60.5
- * nc 100.170.60.5 8080 /bin/sh

NEW QUESTION 154

A penetration tester has run multiple vulnerability scans against a target system. Which of the following would be unique to a credentialed scan?

- * Exploits for vulnerabilities found
- * Detailed service configurations
- * Unpatched third-party software
- * Weak access control configurations

NEW QUESTION 155

A recently concluded penetration test revealed that a legacy web application is vulnerable to SQL injection. Research indicates that completely remediating the vulnerability would require an architectural change, and the stakeholders are not in a position to risk the availability of the application. Under such circumstances, which of the following controls are low-effort, short-term solutions to minimize the SQL injection risk? (Select TWO).

- * Identify and eliminate inline SQL statements from the code.
- * Identify and eliminate dynamic SQL from stored procedures.
- * Identify and sanitize all user inputs.
- * Use a whitelist approach for SQL statements.
- * Use a blacklist approach for SQL statements.
- * Identify the source of malicious input and block the IP address.

NEW QUESTION 156

A penetration tester is performing a code review against a web application Given the following URL and source code:

```
URL: http://example.com/dnslookup?domain=example1.com&server=192.168.1.1  
if (is_admin(COOKIES['sessioncookie'])) {  
    $a="dig a"+GETREQUESTPARAM["domain"]+"@"+GETREQUESTPARAM["server"]  
    print systemfunction($a)
```

Which of the following vulnerabilities is present in the code above?

- * SQL injection
- * Cross-site scripting
- * Command injection
- * LDAP injection

NEW QUESTION 157

Instructions:

Analyze the code segments to determine which sections are needed to complete a port scanning script.

Drag the appropriate elements into the correct locations to complete the script.

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

During a penetration test, you gain access to a system with a limited user interface. This machine appears to have access to an isolated network that you would like to port scan.

```
Drag and Drop Options
exec_scan(sys.argv[1], $SPORTS)

port_scan(sys.argv[1], ports)

export SPORTS = 21, 22

self .ports (
  try:
    s.connect((ip, port))
    print("%s:%s - OPEN" % (ip, port))

  except socket.timeout
    print("%s:%s - TIMEOUT" % (ip, port))

  except socket.error as e:
    print("%s:%s - CLOSED" % (ip, port))

  finally:
    s.close()
)

for $PORT in $SPORTS:
  try:
    s.connect((ip, port))
    print("%s:%s - OPEN" % (ip, port))

  except socket.timeout
    print("%s:%s - TIMEOUT" % (ip, port))

  except socket.error as e:
    print("%s:%s - CLOSED" % (ip, port))

  finally:
    s.close()
)

#!/usr/bin/python

#!/usr/bin/ruby

ports = [21, 22]

run_scan(sys.argv[1], ports)

#!/usr/bin/bash

{:ports => 21 :ports => 22}

for port in ports:
  try:
    s.connect((ip, port))
    print("%s:%s - OPEN" % (ip, port))

  except socket.timeout
    print("%s:%s - TIMEOUT" % (ip, port))

  except socket.error as e:
    print("%s:%s - CLOSED" % (ip, port))

  finally:
    s.close()

```

```
o Immutables

import socket
import sys

def port_scan(ip, ports):
  s = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
  s.settimeout(2.0)

if name == '__main__':
  if len(sys.argv) < 2:
    print('Execution requires a target IP address.
    Exiting...')
    exit(1)
  else:

```

certify.vceprep.com

Drag and Drop Options

```
exec_scan(sys.argv[1], $SPORTS)
```

```
port_scan(sys.argv[1], ports)
```

```
export $SPORTS = 21, 22
```

```
self .ports (  
    try:  
        s.connect((ip, port))  
        print("%s:%s - OPEN" % (ip, port))  
  
    except socket.timeout  
        print("%s:%s - TIMEOUT" % (ip, port))  
  
    except socket.error as e:  
        print("%s:%s - CLOSED" % (ip, port))  
  
    finally:  
        s.close()  
)
```

```
for $PORT in $SPORTS:  
    try:  
        s.connect((ip, port))  
        print("%s:%s - OPEN" % (ip, port))  
  
    except socket.timeout  
        print("%s:%s - TIMEOUT" % (ip, port))  
  
    except socket.error as e:  
        print("%s:%s - CLOSED" % (ip, port))  
  
    finally:  
        s.close()
```

```
#!/usr/bin/python
```

```
#!/usr/bin/ruby
```

```
ports = [21, 22]
```

```
run_scan(sys.argv[1], ports)
```

```
#!/usr/bin/bash
```

```
{:ports => 21 :ports => 22}
```

```
for port in ports:  
    try:  
        s.connect((ip, port))  
        print("%s:%s - OPEN" % (ip, port))  
  
    except socket.timeout  
        print("%s:%s - TIMEOUT" % (ip, port))  
  
    except socket.error as e:  
        print("%s:%s - CLOSED" % (ip, port))  
  
    finally:  
        s.close()
```

Immutables

```
#!/usr/bin/python
```

```
import socket
```

```
import sys
```

```
ports = [21, 22]
```

```
def port_scan(ip, ports):  
    s = socket.socket(socket.AF_INET, socket.SOCK_STREAM)  
    s.settimeout(2.0)
```

```
    for port in ports:  
        try:  
            s.connect((ip, port))  
            print("%s:%s - OPEN" % (ip, port))  
  
        except socket.timeout  
            print("%s:%s - TIMEOUT" % (ip, port))  
  
        except socket.error as e:  
            print("%s:%s - CLOSED" % (ip, port))  
  
        finally:  
            s.close()
```

```
if name == '__main__':  
    if len(sys.argv) < 2  
        print('Execution requires a target IP address.  
Exiting...')  
        exit(1)  
    else:
```

```
run_scan(sys.argv[1], ports)
```

NEW QUESTION 158

A penetration tester needs to provide the code used to exploit a DNS server in the final report. In which of the following parts of the report should the penetration tester place the code?

- * Executive summary
- * Remediation
- * Conclusion
- * Technical summary

NEW QUESTION 159

A penetration tester has performed a pivot to a new Linux device on a different network. The tester writes the following command:

```
for m in {1..254..1};do ping -c 1 192.168.101.$m; done
```

Which of the following BEST describes the result of running this command?

- * Port scan
- * Service enumeration
- * Live host identification
- * Denial of service

NEW QUESTION 160

During testing, a critical vulnerability is discovered on a client's core server. Which of the following should be the NEXT action?

- * Disable the network port of the affected service.
- * Complete all findings, and then submit them to the client.
- * Promptly alert the client with details of the finding.
- * Take the target offline so it cannot be exploited by an attacker.

Explanation

NEW QUESTION 161

Which of the following is an important stakeholder to notify when penetration testing has begun?

- * System owner
- * Remediation manager
- * Compliance assessor
- * Patching team

NEW QUESTION 162

A tester identifies an XSS attack vector during a penetration test. Which of the following flags should the tester recommend to prevent a JavaScript payload from accessing the cookie?

- * Secure
- * Domain
- * Max-Age
- * HttpOnly

PT0-001 Exam Dumps, PT0-001 Practice Test Questions: <https://www.vceprep.com/PT0-001-latest-vce-prep.html>