Easily To Pass New PT0-002 Verified & Correct Answers [Feb 07, 2023 [Q20-Q44

Easily To Pass New PT0-002 Verified & Correct Answers [Feb 07, 2023
Free PT0-002 Exam Files Downloaded Instantly

The difficulties you can face while writing the CompTIA PT0-002 Certification Exam

The CompTIA PT0-002 Certification Exam is a tough exam. The difficulties of the CompTIA PT0-002 Certification Exam are as given here. The candidate doesn't know how and from where to start writing the actual CompTIA PT0-002 Certification Exam. The candidate doesn't know what the questions are and how to answer them. Unawareness about the topic of the CompTIA PT0-002 Certification Exam will result in failure. The candidate has to face many problems while writing the PT0-002 Certification Exam. It is difficult to predict the time required to complete the PT0-002 Certification Exam. The CompTIA PT0-002 Certification Exam is written by the expert, and the candidate has to face many difficulties while writing the PT0-002 Certification Exam. The candidates don't know about the resources that they can use to prepare for the CompTIA PT0-002 Certification Exam. If you are facing all these difficulties, keep calm and start reading from the **PT0-002 Dumps**.

NO.20 During an assessment, a penetration tester obtains a list of 30 email addresses by crawling the target company’s website and then creates a list of possible usernames based on the email address format. Which of the following types of attacks would MOST likely be used to avoid account lockout?

* Mask
* Rainbow
* Dictionary
* Password spraying

NO.21 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?

* Socat
* tcpdump

* Scapy
* dig

NO.22 A company recruited a penetration tester to configure wireless IDS over the network. Which of the following tools would BEST test the effectiveness of the wireless IDS solutions?
* Aircrack-ng
* Wireshark
* Wifite
* Kismet

NO.23 A penetration tester is scanning a corporate lab network for potentially vulnerable services. Which of the following Nmap commands will return vulnerable ports that might be interesting to a potential attacker?
* nmap 192.168.1.1-5 -PU22-25,80
* nmap 192.168.1.1-5 -PA22-25,80
* nmap 192.168.1.1-5 -PS22-25,80
* nmap 192.168.1.1-5 -Ss22-25,80

PS/PA/PU/PY are host discovery flags which use TCP SYN/ACK, UDP or SCTP discovery respectively. And since the ports in the options are mostly used by TCP protocols, then it’s either the PS or PA flag. But since we need to know if the ports are live, sending SYN packet is a better alternative. Hence, I choose PS in this case.

NO.24 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?
* Clarify the statement of work.
* Obtain an asset inventory from the client.
* Interview all stakeholders.
* Identify all third parties involved.

NO.25 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.

NO.26 Which of the following assessment methods is MOST likely to cause harm to an ICS environment?
* Active scanning
* Ping sweep
* Protocol reversing
* Packet analysis

NO.27 Performing a penetration test against an environment with SCADA devices brings additional safety risk because the:
* devices produce more heat and consume more power.
* devices are obsolete and are no longer available for replacement.
* protocols are more difficult to understand.
* devices may cause physical world effects.

NO.28 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

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

https://scapy.readthedocs.io/en/latest/introduction.html#about-scapy

NO.29 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?
* Run nmap with the -o, -p22, and -sC options set against the target
* Run nmap with the -sV and -p22 options set against the target
* Run nmap with the –script vulners option set against the target
* Run nmap with the -sA option set against the target

NO.30 During the reconnaissance phase, a penetration tester obtains the following output:

Reply from 192.168.1.23: bytes=32 time<54ms TTL=128

Reply from 192.168.1.23: bytes=32 time<53ms TTL=128

Reply from 192.168.1.23: bytes=32 time<60ms TTL=128

Reply from 192.168.1.23: bytes=32 time<51ms TTL=128

Which of the following operating systems is MOST likely installed on the host?
* Linux
* NetBSD
* Windows
* macOS

NO.31 Which of the following situations would require a penetration tester to notify the emergency contact for the engagement?
* The team exploits a critical server within the organization.
* The team exfiltrates PII or credit card data from the organization.
* The team loses access to the network remotely.
* The team discovers another actor on a system on the network.

NO.32 A penetration tester was hired to perform a physical security assessment of an organization’s office. After monitoring the environment for a few hours, the penetration tester notices that some employees go to lunch in a restaurant nearby and leave their belongings unattended on the table while getting food. Which of the following techniques would MOST likely be used to get legitimate access into the organization’s building without raising too many alerts?
* Tailgating
* Dumpster diving
* Shoulder surfing
* Badge cloning

NO.33 A large client wants a penetration tester to scan for devices within its network that are Internet facing. The client is

specifically looking for Cisco devices with no authentication requirements. Which of the following settings in Shodan would meet the client’s requirements?
* “cisco-ios” “admin+1234”
* “cisco-ios” “no-password”
* “cisco-ios” “default-passwords”
* “cisco-ios” “last-modified”

NO.34 Which of the following describe the GREATEST concerns about using third-party open-source libraries in application code? (Choose two.)
* The libraries may be vulnerable
* The licensing of software is ambiguous
* The libraries’ code bases could be read by anyone
* The provenance of code is unknown
* The libraries may be unsupported
* The libraries may break the application

NO.35 A penetration tester who is working remotely is conducting a penetration test using a wireless connection. Which of the following is the BEST way to provide confidentiality for the client while using this connection?
* Configure wireless access to use a AAA server.
* Use random MAC addresses on the penetration testing distribution.
* Install a host-based firewall on the penetration testing distribution.
* Connect to the penetration testing company’s VPS using a VPN.

NO.36 A penetration tester writes the following script:

```
#!/bin/bash
for x in 'seq 1 254'; do
        ping -c 1 10.10.1.$x;
done
```

Which of the following objectives is the tester attempting to achieve?
* Determine active hosts on the network.
* Set the TTL of ping packets for stealth.
* Fill the ARP table of the networked devices.
* Scan the system on the most used ports.

NO.37 Deconfliction is necessary when the penetration test:
* determines that proprietary information is being stored in cleartext.
* occurs during the monthly vulnerability scanning.
* uncovers indicators of prior compromise over the course of the assessment.
* proceeds in parallel with a criminal digital forensic investigation.

This will then enable the PenTest to continue so that additional issues can be found, exploited, and analyzed.

NO.38 Which of the following can be used to store alphanumeric data that can be fed into scripts or programs as input to penetration-testing tools?
* Dictionary
* Directory
* Symlink

* Catalog
* For-loop

NO.39 A penetration tester utilized Nmap to scan host 64.13.134.52 and received the following results:

```
# nmap -T4 -v -oG - scanme.nmap.org
# Nmap 5.35DC18 scan initiated [time] as: nmap -T4 -A -v -cG -
scanme.nmap.org
# Ports scanned: TCP(1000;1, 3-4, 6-7, …,,65389) UDP (0;) PROTOCOLS(0;)
Host: 64.13.134.52 (scanme.nmap.org)  Status: Up
Host: 64.13.134.52 (scanme.nmap.org)
Ports:
22/open/tcp
25/closed/tcp
53/open/tcp
70/closed/tcp
80/open/tcp
113/closed/tcp
31337/closed/tcp
Ignored State: filtered (993) OS: Linux 2.6.13 - 2.6.31 Seq Index: 204 IP ID
Seq: All zeros
# Nmap done at [time] -- 1 IP address (1 host up) scanned in 21.90 seconds
```


Based on the output, which of the following services are MOST likely to be exploited? (Choose two.)
* Telnet
* HTTP
* SMTP
* DNS
* NTP
* SNMP

NO.40 A penetration tester is examining a Class C network to identify active systems quickly. Which of the following commands should the penetration tester use?
* nmap ?sn 192.168.0.1/16
* nmap ?sn 192.168.0.1-254
* nmap ?sn 192.168.0.1 192.168.0.1.254
* nmap ?sN 192.168.0.0/24

NO.41 A consultant is reviewing the following output after reports of intermittent connectivity issues:

? (192.168.1.1) at 0a:d1:fa:b1:01:67 on en0 ifscope [ethernet]

? (192.168.1.12) at 34:a4:be:09:44:f4 on en0 ifscope [ethernet]

? (192.168.1.17) at 92:60:29:12:ac:d2 on en0 ifscope [ethernet]

? (192.168.1.34) at 88:de:a9:12:ce:fb on en0 ifscope [ethernet]

? (192.168.1.136) at 0a:d1:fa:b1:01:67 on en0 ifscope [ethernet]

? (192.168.1.255) at ff:ff:ff:ff:ff:ff on en0 ifscope [ethernet]

? (224.0.0.251) at 01:02:5e:7f:ff:fa on en0 ifscope permanent [ethernet]

? (239.255.255.250) at ff:ff:ff:ff:ff:ff on en0 ifscope permanent [ethernet] Which of the following is MOST likely to be reported by the consultant?

* A device on the network has an IP address in the wrong subnet.
* A multicast session was initiated using the wrong multicast group.
* An ARP flooding attack is using the broadcast address to perform DDoS.
* A device on the network has poisoned the ARP cache.

NO.42 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 ( 192.168.1.1 )
Host is up (0.0035s latency).
Not shown: 996 filtered ports

Port     State     Service     Version
22/tcp   open      ssh         OpenSSH 6.6.1p1
53/tcp   open      domain      dnsmasq 2.72
80/tcp   open      http        lighttpd
443/tcp  open      ssl/http    httpd

Service Info: OS: Linux: Device: router; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/.
Nmap done: 1 IP address (1 host up) scanned in 18.45 seconds
```


Which of the following would be the BEST conclusion about this device?

* This device may be vulnerable to the Heartbleed bug due to the way transactions over TCP/22 handle heartbeat extension packets, allowing attackers to obtain sensitive information from process memory.
* This device is most likely a gateway with in-band management services.
* This device is most likely a proxy server forwarding requests over TCP/443.
* This device may be vulnerable to remote code execution because of a butter overflow vulnerability in the method used to extract DNS names from packets prior to DNSSEC validation.

NO.43 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”

NO.44 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?

* Attempting to tailgate an employee going into the client’s workplace
* Dropping a malicious USB key with the company’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

CompTIA PenTest+ Exam Certification Details:

Number of Questions85Books / TrainingCompTIA PenTest+ Certification TrainingExam NameCompTIA PenTest+Passing Score750 / 900Duration165 minsExam Price$381 (USD)Schedule ExamCompTIA Marketplace

Pearson VUE

Who can take the CompTIA PT0-002 Certification Exam?

The targeted audience for the CompTIA PT0-002 Certification Exam is the candidates who are looking for a career in the information technology field. The candidate should be having good knowledge about networking, the operating system, network security, storage, virtualization, cloud computing, mobile device, and cloud computing. Multifactor authentication is a mandatory requirement for the CompTIA PT0-002 Certification Exam. **PT0-002 Dumps** suggest that the individuals who have job titles like Network Engineer, System Engineer, Server Engineer, Database Administrator, Computer Network Engineer, Computer Network Administrator, Security Analyst, and Network Security Engineer can take the CompTIA PT0-002 Certification Exam.

100% Pass Guaranteed Free PT0-002 Exam Dumps: https://www.test4engine.com/PT0-002_exam-latest-braindumps.html]