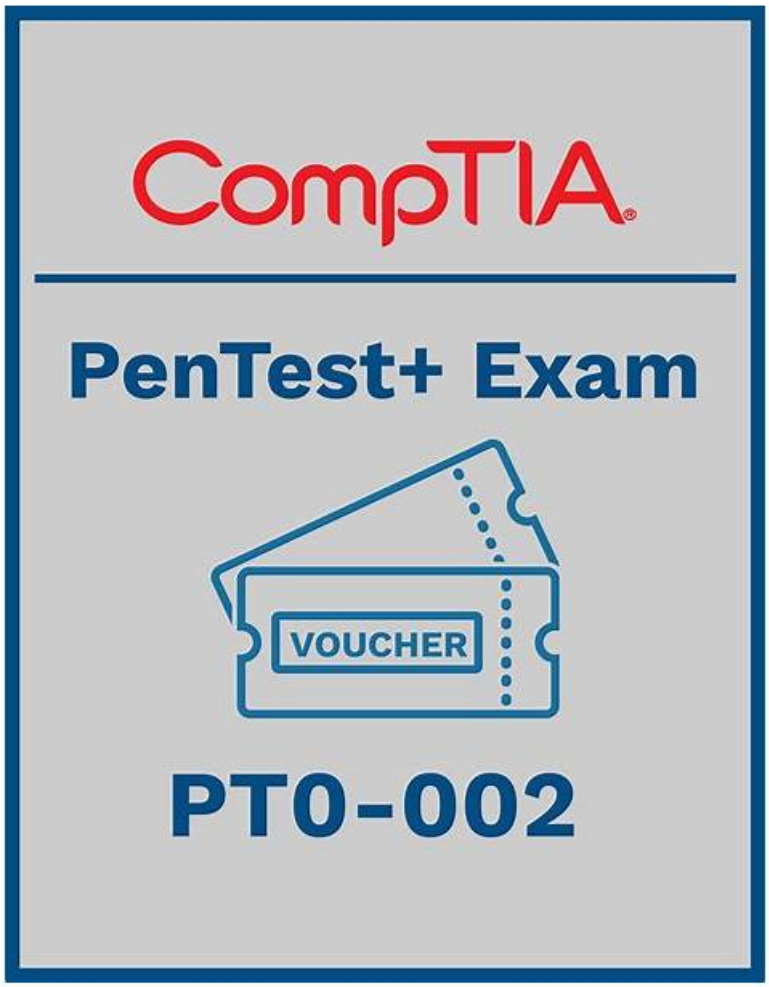
Valid PT0-002 Exam Voucher & Valid Exam PT0-002 Registration



What's more, part of that Prep4sureGuide PT0-002 dumps now are free: https://drive.google.com/open?id=1tR4DBLFJoovjxFX3i3MGFfKbT9wGT3-Q

Through our investigation and analysis of the real problem over the years, our PT0-002 prepare questions can accurately predict the annual PT0-002 exams. In the actual exam process, users will encounter almost half of the problem is similar in our products. Even if the syllabus is changing every year, the PT0-002 quiz guide's experts still have the ability to master propositional trends. Believe that such a high hit rate can better help users in the review process to build confidence, and finally help users through the qualification examination to obtain a certificate. All in all, we want you to have the courage to challenge yourself, and our PT0-002 Exam Prep will do the best for the user's expectations.

We will continue to pursue our passion for better performance and human-centric technology of latest PT0-002 quiz prep. And we guarantee you to pass the PT0-002 exam for we have confidence to make it with our technological strength. A good deal of researches has been made to figure out how to help different kinds of candidates to get the PT0-002 Certification. We have made classification to those faced with various difficulties, aiming at which we adopt corresponding methods. According to the statistics shown in the feedback chart, the general pass rate for latest PT0-002 test prep is 98%.

>> Valid PT0-002 Exam Voucher <<

Valid Exam PT0-002 Registration, PT0-002 Exam Pass4sure

Our CompTIA PT0-002 exam dumps give help to give you an idea about the actual CompTIA PenTest+ Certification (PT0-002) exam. You can attempt multiple CompTIA PenTest+ Certification (PT0-002) exam questions on the software to improve your

performance. Prep4sureGuide has many CompTIA PenTest+ Certification (PT0-002) practice questions that reflect the pattern of the real CompTIA PenTest+ Certification (PT0-002) exam. Prep4sureGuide allows you to create a CompTIA PenTest+ Certification (PT0-002) exam dumps according to your preparation. It is easy to create the CompTIA PT0-002 practice questions by following just a few simple steps. Our CompTIA PenTest+ Certification (PT0-002) exam dumps are customizable based on the time and type of questions.

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.

CompTIA PenTest+ Certification Sample Questions (Q400-Q405):

NEW QUESTION # 400
A penetration tester uses Hashcat to crack hashes discovered during a penetration test and obtains the following output:
ad09cd16529b5f5a40a3e15344e57649f4a43a267a97f008af01af803603c4c8 : Summer2023 !!
7945bb2bb08731fc8d57680ffa4aefec91c784d231de029c610b778eda5ef48b:p@ssWord123
ea88ceab69cb2fb8bdcf9ef4df884af219fffbffab473ec13f20326dc6f84d13: Love-You999
Which of the following is the best way to remediate the penetration tester's discovery?

- A. Requiring passwords to follow complexity rules
- B. Encrypting the passwords with a stronger algorithm
- C. Setting the minimum password length to ten characters
- D. Implementing a blocklist of known bad passwords

Answer: D

Explanation:
The penetration tester's discovery of passwords vulnerable to hash cracking suggests a lack of robust password policies within the organization. Among the options provided, implementing a blocklist of known bad passwords is the most effective immediate remediation. This measure would prevent users from setting passwords that are easily guessable or commonly used, which are susceptible to hash cracking tools like Hashcat.
Requiring passwords to follow complexity rules (Option A) can be helpful, but attackers can still crack complex passwords if they are common or have been exposed in previous breaches. Setting a minimum password length (Option C) is a good practice, but length alone does not ensure a password's strength against hash cracking techniques. Encrypting passwords with a stronger algorithm (Option D) is a valid long-term strategy but would not prevent users from choosing weak passwords that could be easily guessed before hash cracking is even necessary.
Therefore, a blocklist addresses the specific vulnerability exposed by the penetration tester-users setting weak passwords that can be easily cracked. It's also worth noting that the best practice is a combination of strong, enforced password policies, user education, and the use of multi-factor authentication to enhance security further.

NEW QUESTION # 401
During a penetration test, the domain names, IP ranges, hosts, and applications are defined in the:

- A. SLA.
- B. ROE.
- C. SOW.
- D. NDA

Answer: B

Explanation:
https://mainnerve.com/what-are-rules-of-engagement-in-pen-testing/#:~:text=The%20ROE%20includes%20the%

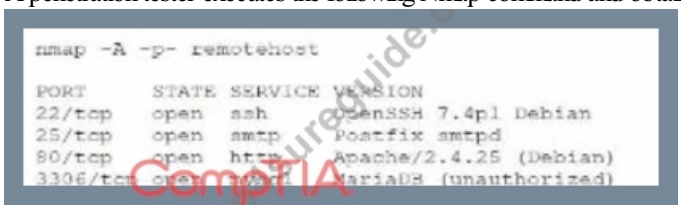
NEW QUESTION # 402
A penetration tester is testing a web application that is hosted by a public cloud provider. The tester is able to query the provider's metadata and get the credentials used by the instance to authenticate itself. Which of the following vulnerabilities has the tester exploited?

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

Answer: D

Explanation:
Server-side request forgery (SSRF) is the vulnerability that the tester exploited by querying the provider's metadata and getting the credentials used by the instance to authenticate itself. SSRF is a type of attack that abuses a web application to make requests to other resources or services on behalf of the web server. This can allow an attacker to access internal or external resources that are otherwise inaccessible or protected. In this case, the tester was able to access the metadata service of the cloud provider, which contains sensitive information about the instance, such as credentials, IP addresses, roles, etc.
Reference: https://owasp.org/www-community/attacks/Server_Side_Request_Forgery

NEW QUESTION # 403
A penetration tester executes the following Nmap command and obtains the following output:



Which of the following commands would best help the penetration tester discover an exploitable service?
A)

B)

C)

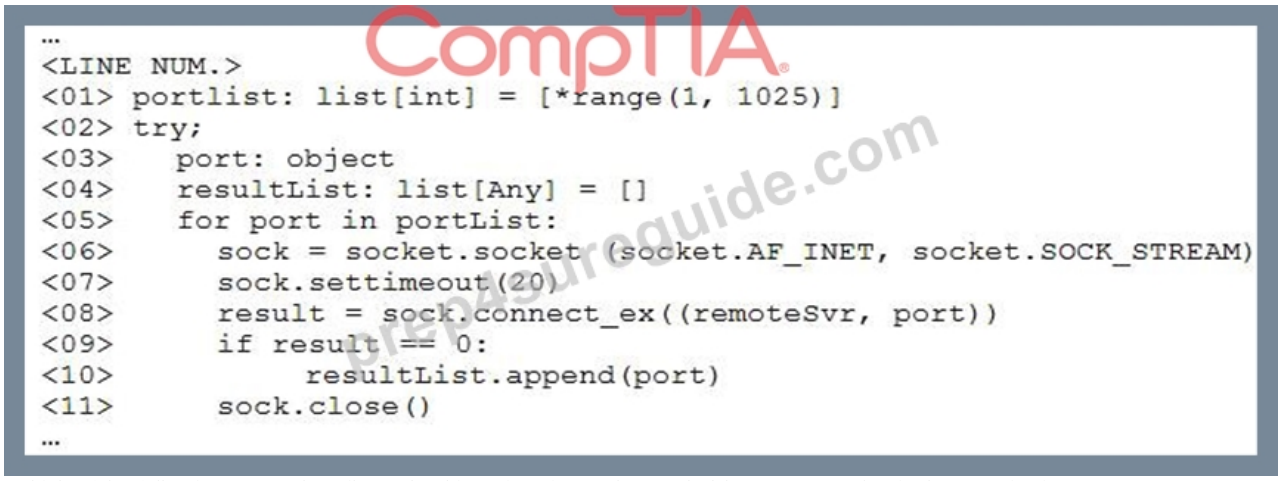
D)

- A. nmap -p 3306 -- script "http*vuln*" remotehost
- B. nmap -v -- script=mysql-info.nse remotehost
- C. nmap -v -p 25 -- soript smtp-enum-users remotehost
- D. nmap --ocript=omb-brute.noe remotehoat

Answer: B

Explanation:
The Nmap command in the question scans all ports on the remote host and identifies the services and versions running on them. The output shows that port 3306 is open and running MariaDB, which is a fork of MySQL. Therefore, the best command to discover an exploitable service would be to use the mysql-info.nse script, which gathers information about the MySQL server, such as the version, user accounts, databases, and configuration variables. The other commands are either misspelled, irrelevant, or too broad for the task. Reference: Best PenTest+ certification study resources and training materials, CompTIA PenTest+ PT0-002 Cert Guide, 101 Labs - CompTIA PenTest+: Hands-on Labs for the PT0-002 Exam

NEW QUESTION # 404
A penetration tester ran a simple Python-based scanner. The following is a snippet of the code:



Which of the following BEST describes why this script triggered a `probable port scan` alert in the organization's IDS?

- A. sock.settimeout(20) on line 7 caused each next socket to be created every 20 milliseconds.
- B. The remoteSvr variable has neither been type-hinted nor initialized.
- C. *range(1, 1025) on line 1 populated the portList list in numerical order.
- D. Line 6 uses socket.SOCK_STREAM instead of socket.SOCK_DGRAM

Answer: C

Explanation:
Port randomization is widely used in port scanners. By default, Nmap randomizes the scanned port order (except that certain commonly accessible ports are moved near the beginning for efficiency reasons)
https://nmap.org/book/man-port-specification.html

NEW QUESTION # 405
.....

Some people are worrying about that they cannot operate the windows software and the online test engine of the PT0-002 training engine smoothly. We ensure that you totally have no troubles in learning our PT0-002 study materials. All small buttons are designed to be easy to understand. Also, the layout is beautiful and simple. Complex designs do not exist in our PT0-002 Exam Guide. You can find that our content is easy to follow and practice.

www.passcollection.com ） open and search for ➥ PT0-002 □ to download for free □Real PT0-002 Questions

- www.stes.tyc.edu.tw, lms.theedgefirm.com, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, www.stes.tyc.edu.tw, learning.schrandersolutions.com, www.stes.tyc.edu.tw, club.gslxtfc.com.cn, academy.frenchrealm.com, Disposable vapes

2025 Latest Prep4sureGuide PT0-002 PDF Dumps and PT0-002 Exam Engine Free Share: https://drive.google.com/open?id=1tR4DBLFJoovjxFX3i3MGFfKbT9wGT3-Q