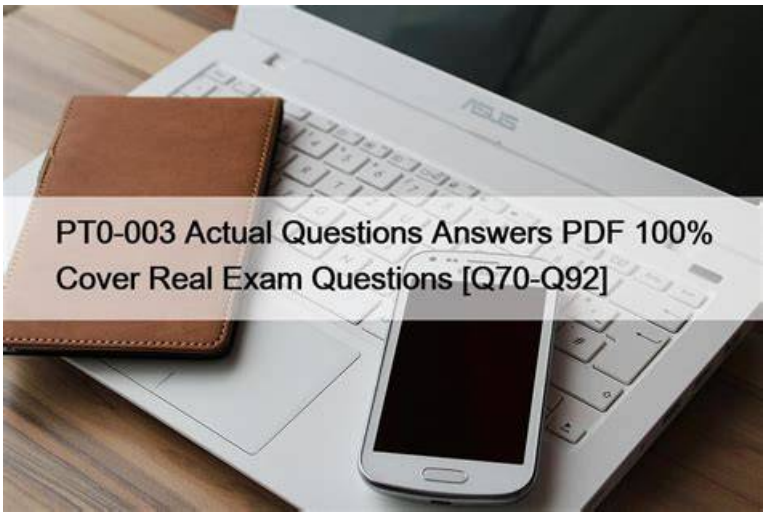
PT0-003 Actual Questions & New PT0-003 Exam Pass4sure



BTW, DOWNLOAD part of Exams-boost PT0-003 dumps from Cloud Storage: https://drive.google.com/open?id=1sLAKXEIHW82UGoiHEfj2MBHBPUs46daJ

Just download the CompTIA PenTest+ Exam (PT0-003) PDF dumps file and start the CompTIA PenTest+ Exam (PT0-003) exam questions preparation right now. Whereas the other two CompTIA PenTest+ Exam (PT0-003) practice test software is concerned, both are the mock CompTIA PT0-003 Exam Dumps and help you to provide the real-time CompTIA PenTest+ Exam (PT0-003) exam environment for preparation.

CompTIA PT0-003 Exam Syllabus Topics:

Section	Weight	Objectives
Topic 1: Exploitation and Post-Exploitation	25%	- Exploitation techniques • 1. Wireless, IoT and cloud exploitation • 2. Network and application exploitation • 3. Password attacks and privilege escalation - Post-exploitation activities • 1. Persistence mechanisms • 2. Data collection and exfiltration • 3. Covering tracks and evasion
Topic 2: Engagement Management	13%	- Pre-engagement activities • 1. Legal and ethical compliance • 2. Rules of engagement • 3. Target selection and assessment types • 4. Scope definition - Collaboration and communication • 1. Reporting requirements • 2. Stakeholder communication • 3. Escalation processes

Topic 3: Reporting and Communication	27%	- Report development • 1. Technical findings documentation • 2. Executive summary creation • 3. Remediation recommendations - Deliverables and follow-up • 1. Presentation of findings • 2. Compliance and regulatory reporting • 3. Retesting and validation
Topic 4: Reconnaissance and Enumeration	18%	- Tools and scripting • 1. Reconnaissance tools usage • 2. Automation for enumeration • 3. Script analysis and modification - Information gathering techniques • 1. Host and service enumeration • 2. Network reconnaissance • 3. Open-source intelligence (OSINT)
Topic 5: Vulnerability Discovery and Analysis	17%	- Vulnerability scanning • 1. Cloud and hybrid environment scanning • 2. Authenticated and unauthenticated scans • 3. Static and dynamic analysis - Vulnerability validation and prioritization • 1. False positive elimination • 2. AI and emerging technology vulnerabilities • 3. Risk rating and prioritization frameworks

New PT0-003 Exam Pass4sure | PT0-003 Certification Test Questions

The pass rate is 98.65%, and we pass guarantee and money back guarantee if you fail to pass the exam by using PT0-003 learning materials of us. We have a broad market in the world with the high quality of PT0-003 exam dumps, and if you choose us we will help you pass the exam just one time. In addition PT0-003 Training Materials of us also have free update for one year after purchasing. We also have the professional service stuff to answer all questions of you. If you have a try, you will never regret.

CompTIA PenTest+ Exam Sample Questions (Q370-Q375):

NEW QUESTION # 370
Which of the following file formats is used to store metadata such as camera details, GPS coordinates, and timestamps within image files?

- A. COFF
- B. ELF
- C. EXIF
- D. GIF

Answer: C

Explanation:
Metadata extraction allows attackers to collect sensitive information from digital files.

* EXIF (Exchangeable Image File Format) (Option A):
* EXIF metadata contains camera details, GPS coordinates, timestamps, and software versions used to edit the file.
* Attackers use tools like ExifTool to extract metadata for reconnaissance.

NEW QUESTION # 371
A penetration tester finished a security scan and uncovered numerous vulnerabilities on several hosts. Based on the targets' EPSS and CVSS scores, which of the following targets is the most likely to get attacked?
Host | CVSS | EPSS
Target 1 | 4 | 0.6
Target 2 | 2 | 0.3
Target 3 | 1 | 0.6
Target 4 | 4.5 | 0.4

- A. Target 4: CVSS Score = 4.5 and EPSS Score = 0.4
- B. Target 3: CVSS Score = 1 and EPSS Score = 0.6
- C. Target 1: CVSS Score = 4 and EPSS Score = 0.6
- D. Target 2: CVSS Score = 2 and EPSS Score = 0.3

Answer: C

Explanation:
Based on the CVSS (Common Vulnerability Scoring System) and EPSS (Exploit Prediction Scoring System) scores, Target 1 is the most likely to get attacked.

NEW QUESTION # 372
An assessment has been completed, and all reports and evidence have been turned over to the client. Which of the following should be done NEXT to ensure the confidentiality of the client's information?

- A. Publish the findings after the client reviews the report
- B. Encrypt and store any client information for future analysis
- C. Follow the established data retention and destruction process
- D. Report any findings to regulatory oversight groups

Answer: B

Explanation:
After completing an assessment and providing the report and evidence to the client, it is important to follow the established data retention and destruction process to ensure the confidentiality of the client's information.
This process typically involves securely deleting or destroying any data collected during the assessment that is no longer needed, and securely storing any data that needs to be retained. This helps to prevent unauthorized access to the client's information and protects the client's confidentiality.
Reporting any findings to regulatory oversight groups may be necessary in some cases, but it should be done only with the client's permission and in accordance with any relevant legal requirements. Publishing the findings before the client has reviewed the report is also not recommended, as it may breach the client's confidentiality and damage their reputation. Encrypting and storing client information for future analysis is also not recommended unless it is necessary and in compliance with any legal or ethical requirements.

NEW QUESTION # 373
A tester completed a report for a new client. Prior to sharing the report with the client, which of the following should the tester request to complete a review?

- A. The customer's designated contact
- B. A team member
- C. A generative AI assistant
- D. A cybersecurity industry peer

Answer: B

Explanation:
Before sharing a report with a client, it is crucial to have it reviewed to ensure accuracy, clarity, and completeness. The best choice for this review is a team member.
Internal Peer Review:
Familiarity with the Project: A team member who worked on the project or is familiar with the methodologies used can provide a detailed and context-aware review.
Quality Assurance: This review helps catch any errors, omissions, or inconsistencies in the report before it reaches the client.
Alternative Review Options:
A Generative AI Assistant: While useful for drafting and checking for language issues, it may not fully understand the context and technical details of the penetration test.
The Customer's Designated Contact: Typically, the client reviews the report after the internal review to provide their perspective and request clarifications or additional details.
A Cybersecurity Industry Peer: Although valuable, this option might not be practical due to confidentiality concerns and the peer's lack of specific context regarding the engagement. In summary, an internal team member is the most suitable choice for a thorough and contextually accurate review before sharing the report with the client.

NEW QUESTION # 374
The following file was obtained during reconnaissance:

```
# adduser.conf
DSHELL=/bin/zsh
DHOME=/home
GROUPHOMES=no
LETTERHOMES=no
SKEL=/etc/systemd-conf/temp-skeleton
FIRST_SYSTEM_UID=100
LAST_SYSTEM_UID=999
FIRST_SYSTEM_GID=100
LAST_SYSTEM_GID=999
FIRST_UID=1000
LAST_UID=2999
FIRST_GID=1000
LAST_GID=2999
USERGROUPS=yes
USERS_GID=100
DIR_MODE=0777
SETGID_HOME=no
QUOTAUSER=""
SKEL_IGNORE_REGEX="dpkg-(old|new|dist|save)"
```


Which of the following is most likely to be successful if a penetration tester achieves non-privileged user access?

- A. Unauthorized access to execute binaries via sudo
- B. Hijacking the default user login shells
- C. Corrupting the skeleton configuration file
- D. Exposure of other users' sensitive data

Answer: D

Explanation:
DIR_MODE=0777 configures new home directories to be created world-readable, world-writable, and world-executable (rwxrwxrwx). With such permissive permissions, any unprivileged local user can traverse into other users' home directories, list files, read them, and even modify or replace them. That makes exposure of other users' sensitive data the most likely and immediate outcome once the tester has any local user account.
Why the other options are less likely:
B . Unauthorized sudo execution: Requires membership in sudo/wheel or explicit entries in /etc/sudoers. Nothing in the snippet indicates that, and file mode on home dirs doesn't grant sudo.
C . Hijacking default login shells: DSHELL=/bin/zsh only sets the default shell for new users. Replacing /bin/zsh or altering /etc/passwd would require root.
D . Corrupting the skeleton configuration: SKEL=/etc/systemd-conf/temp-skeleton is under /etc/..., which is root-owned on standard systems. A normal user cannot write there, so "corrupting the skeleton" is unlikely without privilege escalation.
Practical exploitation as a non-privileged user (illustrative):
Find world-writable homes
find /home -maxdepth 1 -type d -perm -0002 -ls
Read another user's files
cd /home/targetuser && ls -la && cat Documents/tax_return.pdf

(Depending on per-file permissions.)
CompTIA PenTest+ PT0-003 Objective Mapping (for study):
Domain 3.0 Attacks and Exploits

NEW QUESTION # 375
......

If you want to choose passing CompTIA certification PT0-003 exam to make yourself have a more stable position in today's competitive IT area and the professional ability become more powerful, you must have a strong expertise. And passing CompTIA certification PT0-003 exam is not very simple. Perhaps passing CompTIA Certification PT0-003 Exam is a stepping stone to promote yourself in the IT area, but it doesn't need to spend a lot of time and effort to review the relevant knowledge, you can choose to use our Exams-boost product, a training tool prepared for the IT certification exams.