# PT0-003最新考證，PT0-003熱門認證


P.S. KaoGuTi在Google Drive上分享了免費的2026 CompTIA PT0-003考試題庫：https://drive.google.com/open?id=1_eAdbRXSpaStQzV1sv8B8-2c2cAryZxy

“如果放棄了，那比賽同時也就結束了。”這是來自安西教練的一句大家都熟知的名言。比賽是這樣，同樣考試也是這樣的。有很多人因為沒有充分的時間準備考試從而放棄了參加PT0-003認證考試。但是，如果使用了好的資料，即使只有很短的時間來準備，你也完全可以以高分通過PT0-003考試。不相信嗎？KaoGuTi的考古題就是這樣的資料。趕快試一下吧。

## CompTIA PT0-003 考試大綱：

| 主題 | 簡介 |
|---|---|
| 主題 1 | • Engagement Management: In this topic, cybersecurity analysts learn about pre-engagement activities, collaboration, and communication in a penetration testing environment. The topic covers testing frameworks, methodologies, and penetration test reports. It also explains how to analyze findings and recommend remediation effectively within reports, crucial for real-world testing scenarios. |

| | |
|---|---|
| 主題 2 | • Attacks and Exploits: This extensive topic trains cybersecurity analysts to analyze data and prioritize attacks. Analysts will learn how to conduct network, authentication, host-based, web application, cloud, wireless, and social engineering attacks using appropriate tools. Understanding specialized systems and automating attacks with scripting will also be emphasized. |
| 主題 3 | • Post-exploitation and Lateral Movement: Cybersecurity analysts will gain skills in establishing and maintaining persistence within a system. This topic also covers lateral movement within an environment and introduces concepts of staging and exfiltration. Lastly, it highlights cleanup and restoration activities, ensuring analysts understand the post-exploitation phase's responsibilities. |
| 主題 4 | • Vulnerability Discovery and Analysis: In this section, cybersecurity analysts will learn various techniques to discover vulnerabilities. Analysts will also analyze data from reconnaissance, scanning, and enumeration phases to identify threats. Additionally, it covers physical security concepts, enabling analysts to understand security gaps beyond just the digital landscape. |
| 主題 5 | • Reconnaissance and Enumeration: This topic focuses on applying information gathering and enumeration techniques. Cybersecurity analysts will learn how to modify scripts for reconnaissance and enumeration purposes. They will also understand which tools to use for these stages, essential for gathering crucial information before performing deeper penetration tests. |



## PT0-003熱門認證 - PT0-003考題套裝

我們KaoGuTi CompTIA的PT0-003考試培訓資料給所有需要的人帶來最大的成功率，通過微軟的PT0-003考試是一個具有挑戰性的認證考試。現在除了書籍，互聯網被認為是一個知識的寶庫，在KaoGuTi你也可以找到屬於你的知識寶庫，這將是一個對你有很大幫助的網站，你會遇到複雜的測試方面的試題，我們KaoGuTi可以幫助你輕鬆的通過考試，它涵蓋了所有必要的知識CompTIA的PT0-003考試。

## 最新的 CompTIA PenTest+ PT0-003 免費考試真題 (Q254-Q259):

**問題 #254**
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.
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.

**答案：**

解題說明：
Explanation:
A computer screen shot of a computer Description automatically generated
A screen shot of a computer Description automatically generated
A computer screen with white text Description automatically generated
An orange screen with white text Description automatically generated

**問題 #255**
A security analyst needs to perform a scan for SMB port 445 over a/16 network. Which of the following commands would be the BEST option when stealth is not a concern and the task is time sensitive?

- A. Nmap -p 445 -max -sT 172. 21.0.0/16
- B. Nmap -s 445 -Pn -T5 172.21.0.0/16
- C. Nmap -sV --script=smb* 172.21.0.0/16

- D. Nmap -p 445 -n -T4 -open 172.21.0.0/16

**答案：D**

解題說明：
Nmap is a tool that can perform network scanning and enumeration by sending packets to hosts and analyzing their responses. The command Nmap -p 445 -n -T4 -open 172.21.0.0/16 would scan for SMB port
445 over a /16 network with the following options:
-p 445 specifies the port number to scan.
-n disables DNS resolution, which can speed up the scan by avoiding unnecessary queries.
-T4 sets the timing template to aggressive, which increases the speed of the scan by sending packets faster and waiting less for responses.
-open only shows hosts that have open ports, which can reduce the output and focus on relevant results. The other commands are not optimal for scanning SMB port 445 over a /16 network when stealth is not a concern and the task is time sensitive.

**問題 #256**
A penetration tester has been provided with only the public domain name and must enumerate additional information for the public-facing assets.
INSTRUCTIONS
Select the appropriate answer(s), given the output from each section.
Output 1

**答案：**

解題說明：
See all the solutions below in Explanation.
Explanation:
A screenshot of a computer Description automatically generated
A screenshot of a computer Description automatically generated
A screenshot of a computer Description automatically generated

**問題 #257**
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?

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

**答案：D**

解題說明：
* EPSS and CVSS Analysis:
* EPSS (Exploit Prediction Scoring System) indicates the likelihood of exploitation.
* CVSS (Common Vulnerability Scoring System) represents the severity of the vulnerability.
* Rationale:
* Target 1 has the highest EPSS score (0.6) combined with a moderately high CVSS score (4), making it the most likely to be attacked.
* Other options either have lower EPSS or CVSS scores, reducing their likelihood of being exploited.
CompTIA Pentest+ References:
* Domain 2.0 (Information Gathering and Vulnerability Identification)

**問題 #258**
A penetration tester wants to use PowerView in an AD environment. Which of the following is the most likely reason?

- A. To escalate privileges
- B. To collect local hashes
- C. To decrypt stored passwords
- D. To enumerate user groups

**答案：D**

解題說明：
PowerView is a PowerShell tool used for Active Directory enumeration. It is part of the PowerSploit framework and allows penetration testers to gather detailed information about the AD environment, including user accounts, groups, computers, shares, and trust relationships.
PowerView is most commonly used to:
* Enumerate domain users, groups, and memberships
* Identify privileged users and group memberships
* Discover domain trusts and permissions
According to the CompTIA PenTest+ PT0-003 Official Study Guide (Chapter 8 - Post-Exploitation and Lateral Movement):
"PowerView is a post-exploitation tool used primarily for Active Directory reconnaissance, including user and group enumeration, identifying domain trusts, and mapping out the AD structure."

**問題 #259**
.....

P.S. KaoGuTi在Google Drive上分享了免費的2026 CompTIA PT0-003考試題庫：https://drive.google.com/open?id=1_eAdbRXSpaStQzV1sv8B8-2c2cAryZxy