PT0-002$^{Q\&As}$

CompTIA PenTest+ Certification Exam

Pass CompTIA PT0-002 Exam with 100% Guarantee

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

QUESTION 1

Which of the following BEST describe the OWASP Top 10? (Choose two.)

A. The most critical risks of web applications

B. A list of all the risks of web applications

C. The risks defined in order of importance

D. A web-application security standard

E. A risk-governance and compliance framework

F. A checklist of Apache vulnerabilities

Correct Answer: AC

Reference: https://www.synopsys.com/glossary/what-is-owasp-top-10.html

QUESTION 2

A penetration tester wants to test a list of common passwords against the SSH daemon on a network device. Which of the following tools would be BEST to use for this purpose?

A. Hashcat

B. Mimikatz

C. Patator

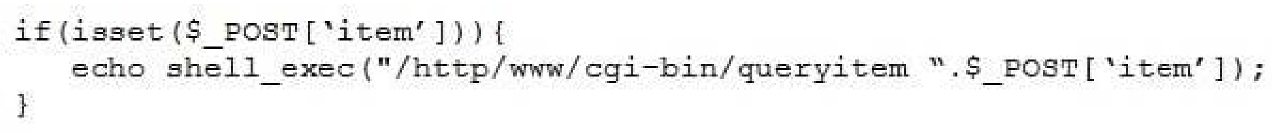
D. John the Ripper

Correct Answer: C

https://www.kali.org/tools/patator/

QUESTION 3

A penetration tester finds a PHP script used by a web application in an unprotected internal source code repository. After reviewing the code, the tester identifies the following:



```
if(isset($_POST[‘item’])){
    echo shell_exec("/http/www/cgi-bin/queryitem ".$_POST[‘item’]);
}
```

Which of the following tools will help the tester prepare an attack for this scenario?

A. Hydra and crunch

B. Netcat and cURL

C. Burp Suite and DIRB

D. Nmap and OWASP ZAP

Correct Answer: B

QUESTION 4

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 5

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-s 445-Pn-T5 172.21.0.0/16

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

C. Nmap-sV--script=smb* 172.21.0.0/16

D. Nmap-p 445-max-sT 172. 21.0.0/16

Correct Answer: C

The best option when stealth is not a concern and the task is time sensitive is to use the command: Nmap-sV--script=smb* 172.21.0.0/16. This command will use version detection and SMB scripts to scan for port 445 on the given IP range. The-sV option will cause Nmap to detect the version of services running on the ports, which is helpful for identifying vulnerabilities, and the--script=smb* option will cause Nmap to run all of the SMB related scripts. The-T4 option can be used to speed up the scan, as it increases the timing probes.

PT0-002 PDF Dumps PT0-002 Practice Test PT0-002 Exam Questions