PT0-001 Q&As

CompTIA PenTest+ Exam

QUESTION 1

A penetration tester wants to check manually if a “ghost” vulnerability exists in a system. Which of the following methods is the correct way to validate the vulnerability?

A. Download the GHOST file to a Linux system and compile

gcc -o GHOST

test i:

./GHOST

B. Download the GHOST file to a Windows system and compile

gcc -o GHOST GHOST.c

test i:

./GHOST

C. Download the GHOST file to a Linux system and compile

gcc -o GHOST GHOST.c

test i:

./GHOST

D. Download the GHOST file to a Windows system and compile

gcc -o GHOST

test i:

./GHOST

Correct Answer: C

QUESTION 2

An attacker uses SET to make a copy of a company\\'s cloud-hosted web mail portal and sends an email m to obtain the CEO s login credentials Which of the following types of attacks is this an example of?

A. Elicitation attack

B. Impersonation attack

C. Spear phishing attack

D. Drive-by download attack

Correct Answer: A

Reference: https://www.social-engineer.org/framework/influencing-others/elicitation/

QUESTION 3

A security analyst was provided with a detailed penetration report, which was performed against the organization\\'s DMZ environment. It was noted on the report that a finding has a CVSS base score of 10.0.

Which of the following levels of difficulty would be required to exploit this vulnerability?

A. Very difficult; perimeter systems are usually behind a firewall.

B. Somewhat difficult; would require significant processing power to exploit.

C. Trivial; little effort is required to exploit this finding.

D. Impossible; external hosts are hardened to protect against attacks.

Correct Answer: C

Reference https://nvd.nist.gov/vuln-metrics/cvss

QUESTION 4

A tester has captured a NetNTLMv2 hash using Responder Which of the following commands will allow the tester to crack the hash using a mask attack?

A. hashcat -m 5600 -r rulea/beat64.rule hash.txt wordliat.txt

B. hashcax -m 500 hash.txt

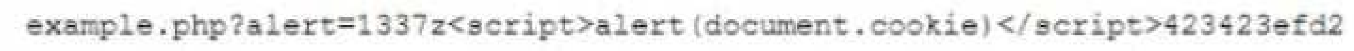
C. hashcandt -m 5600 -a 3 haah.txt ?a?a?a?a?a?a?a?a

D. hashcat -m 5600 -o reaulta.txt hash.txt wordliat.txt

Correct Answer: C

QUESTION 5

While reviewing logs, a web developer notices the following user input string in a field:



```
example.php?alert=1337z<script>alert(document.cookie)</script>423423efd2
```

Which of the following types of attacks was done to the website?

A. XSS injection

B. Blind XSS

C. Reflected XSS

D. Persistent XSS

Correct Answer: A