GIAC

GXPN
GIAC Exploit Researcher and Advanced Penetration Tester

Questions And Answers PDF Format:

For More Information – Visit link below:
https://www.certsgrade.com/

Version = **Product**

Latest Version: 6.0

Question: 1

When using the Sulley framework for fuzzing, what is an effective strategy to improve code coverage?
Response:

A. Increasing the payload size indiscriminately
B. Using more precise and context-aware test cases
C. Decreasing the duration of each test case
D. Focusing testing on stable software components

Answer: B

Question: 2

Which Python feature is most beneficial for writing modular and reusable penetration testing scripts?
Response:

A. Decorators
B. List comprehensions
C. Object-oriented programming (OOP)
D. Dynamic typing

Answer: C

Question: 3

Why is it important for penetration testers to understand shellcode in both Windows and Linux environments?
Response:

A. To support cross-platform software development
B. To enhance the performance of operating systems
C. To execute exploits and gain control over systems
D. To ensure compatibility with antivirus software

Answer: C

Question: 4

How do DEP (Data Execution Prevention) and ASLR (Address Space Layout Randomization) complicate exploitation of Windows stack overflows?
Response:

A. DEP prevents execution of code from non-executable memory regions
B. ASLR randomizes the addresses of stack, heap, and libraries
C. Both mechanisms encrypt data on the stack
D. They reduce the efficiency of garbage collection

Answer: A,B

Question: 5

What is the function of Windows Heap protections that complicates exploitation?
Response:

A. Segmenting the heap into multiple sub-heaps
B. Using randomized addresses for heap allocation
C. Encrypting heap data
D. Logging heap allocations and deallocations

Answer: B

Question: 6

Which of the following are ways to interact with or exploit client environments using tools like PowerShell?
(Choose Two)
Response:

A. Script-based automation of administrative tasks
B. Modifying the Windows registry
C. Sending spear-phishing emails
D. Kernel-level exploitation

Answer: A,B

Question: 7

In the context of Linux, what is a common characteristic of shellcode?
Response:

A. It is usually written in Java
B. It often includes zero bytes
C. It is executed in the user space of the OS
D. It is predominantly GUI-based

Answer: C

Question: 8

In exploiting network protocols, what are effective methods to attack client systems?
(Choose Two)
Response:

A. DNS spoofing
B. Phishing
C. Ransomware deployment
D. Session hijacking

Answer: A,D

Question: 9

What tools are commonly used to automate the process of generating exploits for stack buffer overflows?
(Choose Two)
Response:

A. Metasploit
B. gdb
C. IDA Pro
D. Fuzzers

Answer: A,C

Question: 10

What is the impact of a successful stack overflow attack on a Windows system?
Response:

A. Temporary increase in system performance
B. Arbitrary code execution under the context of the affected process
C. Enhanced security logging
D. Automatic patching of the vulnerability

Answer: B