Vendor: CompTIA

Exam Code:PT0-002

Exam Name: CompTIA PenTest+ Certification Exam

Version: Demo

QUESTION 1

A penetration tester received a 16-bit network block that was scoped for an assessment. During the assessment, the tester realized no hosts were active in the provided block of IPs and reported this to the company. The company then provided an updated block of IPs to the tester. Which of the following would be the most appropriate NEXT step?

A. Terminate the contract.

B. Update the ROE with new signatures. Most Voted

C. Scan the 8-bit block to map additional missed hosts.

D. Continue the assessment.

Correct Answer: B

QUESTION 2

A penetration tester discovers passwords in a publicly available data breach during the reconnaissance phase of the penetration test. Which of the following is the best action for the tester to take?

A. Add thepasswords to an appendix in the penetration test report.

B. Do nothing. Using passwords from breached data is unethical.

C. Contactthe client and inform them of the breach.

D. Use thepasswords in a credential stuffing attack when the external penetration test begins.

Correct Answer: C

Upon discovering passwords in a publicly available data breach during the reconnaissance phase, the most ethical and constructive action for the penetration tester is to contact the client and inform them of the breach. This approach allows the client to take necessary actions to mitigate any potential risks, such as forcing password resets or enhancing their security measures. Adding the passwords to a report appendix (option A) without context or action could be seen as irresponsible, while doing nothing (option B) neglects the tester\\'s duty to inform the client of potential threats. Using the passwords in a credential stuffing attack (option D) without explicit permission as part of an agreed testing scope would be unethical and potentially illegal.

QUESTION 3

During an assessment, a penetration tester emailed the following Python script to CompTIA\\'s employees:

import pyHook, sys, logging, pythoncom, datetime

log_file=\\'C:\\Windows\\Temp\\log_comptia.txt\\' def KbrdEvent(event):

logging.basicConfig(filename=log_file,level=logging.DEBUG, format=\\'%(messages)s\\') chr(event.Ascii)

logging.log(10, chr(event.Ascii))

```
return True

hooks_manager = pyHook.HookManager()

hooks_manager.KeyDown = KbrdEvent

hooks_manager.HookKeyboard()

pythoncom.PumpMessages()
```

Which of the following is the intended effect of this script?

A. Debugging an exploit

B. Keylogging

C. Collecting logs

D. Scheduling tasks

Correct Answer: B

The provided Python script is designed to function as a keylogger, which is a type of surveillance software that has the capability to record every keystroke made on a computer. The script uses the pyHook library to hook into and monitor all keyboard events. When a key is pressed, the KbrdEvent function is triggered, which logs the ASCII value of the pressed key to a file named log_comptia.txt located in C:\\Windows\\Temp. The script is configured to continuously monitor keyboard events and log them, making its intended effect keylogging, rather than debugging an exploit, collecting logs in a general sense, or scheduling tasks.

QUESTION 4

A penetration tester is reviewing the logs of a proxy server and discovers the following URLs: https://test.comptia.com/profile.php?userid=1546 https://test.cpmptia.com/profile.php?userid=5482 https://test.comptia.com/profile.php?userid=3618 Which of the following types of vulnerabilities should be remediated?

A. Insecure direct object reference

B. Improper error handling

C. Race condition

D. Weak or default configurations

Correct Answer: A

Insecure Direct Object References (IDOR) occur when an application provides direct access to objects based on user-supplied input. In the provided URLs, the userid parameter is directly referenced, which can allow attackers to manipulate these references to access unauthorized data. This vulnerability can lead to unauthorized access to other users\\' profiles by simply changing the userid parameter value. The other vulnerabilities listed (Improper error handling, Race condition, Weak or default configurations) do not directly relate to the issue demonstrated by the URLs.

QUESTION 5

A penetration testing firm performs an assessment every six months for the same customer. While performing network scanning for the latest assessment, the penetration tester observes that several of the target hosts appear to be residential connections associated with a major television and ISP in the area. Which of the following is the most likely reason for the observation?

A. The penetration tester misconfigured the network scanner.

B. The network scanning tooling is not functioning properly.

C. The IP ranges changed ownership.

D. The network scanning activity is being blocked by a firewall.

Correct Answer: C

When a penetration tester notices several target hosts appearing to be residential connections associated with a major television and ISP, it\\'s likely that the IP ranges initially assigned to the target organization have changed ownership and are now allocated to the ISP for residential use. This can happen due to reallocation of IP addresses by regional internet registries. Misconfiguration of the scanner (option A), malfunctioning of scanning tools (option B), or firewall blocking (option D) would not typically result in the discovery of residential connections in place of expected organizational targets.

QUESTION 6

A penetration tester has prepared the following phishing email for an upcoming penetration test:

```
Coworkers,

A security incident recently occurred on company property.

All employees are required to abide by company policies at all times.
To ensure maximum compliance, all employees are required to sign the
Security Policy Acceptance form (on-line here) before the end of this
month.

Please reach out if you have any questions or concerns.

Human Resources
```

Which of the following is the penetration tester using MOST to influence phishing targets to click on the link?

A. Familiarity and likeness

B. Authority and urgency

C. Scarcity and fear

D. Social proof and greed

Correct Answer: B

QUESTION 7

A penetration tester is starting an assessment but only has publicly available information about the target company. The client is aware of this exercise and is preparing for the test. Which of the following describes the scope of the assessment?

A. Partially known environment testing

B. Known environment testing

C. Unknown environment testing

D. Physical environment testing

Correct Answer: C

QUESTION 8

Which of the following members of a client organization are most likely authorized to provide a signed authorization letter prior to the start date of a penetration test?

A. The IT department

B. The executive management team and legal personnel

C. Organizational security personnel

D. The human resources team

Correct Answer: B

QUESTION 9

A penetration tester logs in as a user in the cloud environment of a company. Which of the following Pacu modules will enable the tester to determine the level of access of the existing user?

A. iam_enum_permissions

B. iam_privesc_scan

C. iam_backdoor_assume_role

D. iam_bruteforce_permissions

Correct Answer: A

The iam_enum_permissions module will enable the tester to determine the level of access of the existing user in the cloud environment of a company, as it will list all permissions associated with an IAM user3. IAM (Identity and Access Management) is a service that enables users to manage access and permissions for AWS resources. Pacu is a tool that can be used to perform penetration testing on AWS environments4. Reference: https://essay.utwente.nl/76955/1/Szabo_MSc_EEMCS.pdf (37)

QUESTION 10

Which of the following would MOST likely be included in the final report of a static application-security test that was written with a team of application developers as the intended audience?

A. Executive summary of the penetration-testing methods used

B. Bill of materials including supplies, subcontracts, and costs incurred during assessment

C. Quantitative impact assessments given a successful software compromise

D. Code context for instances of unsafe type-casting operations

Correct Answer: D

Code context for instances of unsafe type-casting operations would most likely be included in the final report of a static application-security test that was written with a team of application developers as the intended audience, as it would provide relevant and actionable information for the developers to fix the vulnerabilities. Type-casting is the process of converting one data type to another, such as an integer to a string. Unsafe type- casting can lead to errors, crashes, or security issues, such as buffer overflows or code injection.

QUESTION 11

A Chief Information Security Officer wants to evaluate the security of the company\\'s e- commerce application. Which of the following tools should a penetration tester use FIRST to obtain relevant information from the application without triggering alarms?

A. SQLmap

B. DirBuster

C. w3af

D. OWASP ZAP

Correct Answer: C

W3AF, the Web Application Attack and Audit Framework, is an open source web application security scanner that includes directory and filename bruteforcing in its list of capabilities.

QUESTION 12

A penetration tester has been hired to examine a website for flaws. During one of the time windows for testing, a network engineer notices a flood of GET requests to the web server, reducing the website\\'s response time by 80%. The network engineer contacts the penetration tester to determine if these GET requests are part of the test. Which of the following BEST describes the purpose of checking with the penetration tester?

A. Situational awareness

B. Rescheduling

C. DDoS defense

D. Deconfliction

Correct Answer: D

https://redteam.guide/docs/definitions/ Deconfliction is the process of coordinating activities and communicating information to avoid interference, confusion, or conflict among different parties involved in an operation. The network engineer contacted the penetration tester to check if the GET requests were part of the test, and to avoid any potential misunderstanding or disruption of the test or the website. The other options are not related to the purpose of checking with the penetration tester.