PT0-001Q&As

CompTIA PenTest+ Exam

Pass CompTIA PT0-001 Exam with 100% Guarantee

QUESTION 1

A penetration tester ran the following Nmap scan on a computer:

nmap -aV 192.168.1.5

The organization said it had disabled Telnet from its environment. However, the results of the Nmap scan show port 22 as closed and port 23 as open to SSH. Which of the following is the BEST explanation for what happened?

A. The organization failed to disable Telnet.

B. Nmap results contain a false positive for port 23.

C. Port 22 was filtered.

D. The service is running on a non-standard port.

Correct Answer: A

QUESTION 2

A penetration tester is preparing for an assessment of a web server\\'s security, which is used to host several sensitive web applications. The web server is PKI protected, and the penetration tester reviews the certificate presented by the server during the SSL handshake. Which of the following certificate fields or extensions would be of MOST use to the penetration tester during an assessment?

A. Subject key identifier

B. Subject alternative name

C. Authority information access

D. Service principal name

Correct Answer: C

Reference: http://www.pkiglobe.org/auth_info_access.html

QUESTION 3

A system security engineer is preparing to conduct a security assessment of some new applications. The applications were provided to the engineer as a set that contains only JAR files. Which of the following would be the MOST detailed method to gather information on the inner working of these applications?

A. Launch the applications and use dynamic software analysis tools, including fuzz testing

B. Use a static code analyzer on the JAR filet to look for code Quality deficiencies

C. Decompile the applications to approximate source code and then conduct a manual review

D. Review the details and extensions of the certificate used to digitally sign the code and the application

Correct Answer: A

QUESTION 4

An attacker performed a MITM attack against a mobile application. The attacker is attempting to manipulate the application\\'s network traffic via a proxy tool. The attacker only sees limited traffic as cleartext. The application log files indicate secure SSL/TLS connections are failing. Which of the following is MOST likely preventing proxying of all traffic?

A. Misconfigured routes

B. Certificate pinning

C. Strong cipher suites

D. Closed ports

Correct Answer: B

QUESTION 5

A client\\'s systems administrator requests a copy of the report from the penetration tester, but the systems administrator is not listed as a point of contact or signatory. Which of the following is the penetration tester\\'s BEST course of action?

A. Send the report since the systems administrator will be in charge of implementing the fixes.

B. Send the report and carbon copy the point of contact/signatory for visibility.

C. Reply and explain to the systems administrator that proper authorization is needed to provide the report.

D. Forward the request to the point of contact/signatory for authorization.

Correct Answer: C

QUESTION 6

When calculating the sales price of a penetration test to a client, which of the following is the MOST important aspect to understand?

A. The operating cost

B. The client\\'s budget

C. The required scope of work

D. The non-disclosure agreement

Correct Answer: C

QUESTION 7

A healthcare organization must abide by local regulations to protect and attest to the protection of personal health information of covered individuals. Which of the following conditions should a penetration tester specifically test for when performing an assessment? (Select TWO).

A. Cleartext exposure of SNMP trap data

B. Software bugs resident in the IT ticketing system

C. S/MIME certificate templates defined by the CA

D. Health information communicated over HTTP

E. DAR encryption on records servers

Correct Answer: DE

QUESTION 8

A penetration tester is utilizing social media to gather information about employees at a company. The tester has created a list of popular words used in employee profile s. For which of the following types of attack would this information be used?

A. Exploit chaining

B. Session hijacking

C. Dictionary

D. Karma

Correct Answer: C

QUESTION 9

A penetration tester is reviewing a Zigbee Implementation for security issues. Which of the following device types is the tester MOST likely testing?

A. Router

B. IoT

C. WAF

D. PoS

Correct Answer: B

QUESTION 10

A penetration tester runs the following from a compromised box \\'python -c -import pty;Pty.sPawn("/bin/bash").\\' Which of the following actions is the tester taking?

A. Removing the Bash history

B. Upgrading the shell

C. Creating a sandbox

D. Capturing credentials

Correct Answer: B

Reference: https://schu.media/2017/08/05/using-reverse-shell-to-get-access-to-your-server/

QUESTION 11

A client is asking a penetration tester to evaluate a new web application for availability. Which of the following types of attacks should the tester use?

A. TCP SYN flood

B. SQL injection

C. xss

D. XMAS scan

Correct Answer: B

Reference: https://www.softwaretestinghelp.com/getting-started-with-web-application-penetration-testing/

QUESTION 12

Joe, a penetration tester, was able to exploit a web application behind a firewall He is trying to get a reverse shell back to his machine but the firewall blocks the outgoing traffic Ports for which of the following should the security consultant use to have the HIGHEST chance to bypass the firewall?

A. HTTP

B. SMTP

C. FTP

D. DNS

Correct Answer: A

QUESTION 13

A web server is running PHP, and a penetration tester is using LFI to execute commands by passing parameters through the URL. This is possible because server logs were poisoned to execute the PHP system ( ) function. Which of the following would retrieve the contents of the passwd file?

A. \\'\\'andCMD_cat /etc/passwd--andid-34\\'\\'

B. \\'\\'andCMD=cat / etc/passwd%andid= 34\\'\\'

C. \\'\\'andCMD=cat ../../../../etc/passwd7id=34\\'

D. \\'\\'andsystem(CMD) \\'\\'cat /etc/passedandid=34\\'\\'

Correct Answer: A

QUESTION 14

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 15

A company\\'s corporate policies state that employees are able to scan any global network as long as it is done within working hours. Government laws prohibit unauthorized scanning. Which of the following should an employee abide by?

A. Company policies must be followed in this situation

B. Laws supersede corporate policies

C. Industry standards receding scanning should be followed

D. The employee must obtain written approval from the company\\'s Chief Information Security Officer (CISO) prior to scanning

Correct Answer: D

PT0-001 VCE Dumps PT0-001 Study Guide PT0-001 Braindumps