PT0-002 Q&As

CompTIA PenTest+ Certification Exam

Pass CompTIA PT0-002 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.pass4itsure.com/pt0-002.html

100% Passing Guarantee
100% Money Back Assurance

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

QUESTION 1

During a test of a custom-built web application, a penetration tester identifies several vulnerabilities. Which of the following would be the most interested in the steps to reproduce these vulnerabilities?

A. Operations staff

B. Developers

C. Third-party stakeholders

D. C-suite executives

Correct Answer: B

The developers would be the most interested in the steps to reproduce the web application vulnerabilities, because they are responsible for fixing the code and implementing security best practices. The steps to reproduce the vulnerabilities would help them understand the root cause of the problem, test the patches, and prevent similar issues in the future. The other options are less interested in the technical details of the vulnerabilities, as they have different roles and responsibilities. The operations staff are more concerned with the availability and performance of the web application, the third-party stakeholders are more interested in the business impact and risk assessment of the vulnerabilities, and the C-suite executives are more focused on the strategic and financial implications of the vulnerabilities123.

QUESTION 2

Which of the following tools provides Python classes for interacting with network protocols?

A. Responder

B. Impacket

C. Empire

D. PowerSploit

Correct Answer: B

Impacket is a tool that provides Python classes for interacting with network protocols, such as SMB, DCE/RPC, LDAP, Kerberos, etc. Impacket can be used for network analysis, packet manipulation, authentication spoofing, credential dumping, lateral movement, and remote execution. Reference: https://github.com/SecureAuthCorp/impacket

QUESTION 3

A penetration tester is looking for a particular type of service and obtains the output below:

I Target is synchronized with 127.127.38.0 (reference clock) I Alternative Target Interfaces:

I 10.17.4.20

I Private Servers (0)

I Public Servers (0)

I Private Peers (0)

I Public Peers (0)

I Private Clients (2)

I 10.20.8.69 169.254.138.63

I Public Clients (597)

I 4.79.17.248 68.70.72.194 74.247.37.194 99.190.119.152

I 12.10.160.20 68.80.36.133 75.1.39.42 108.7.58.118

I 68.56.205.98

I 2001:1400:0:0:0:0:0:1 2001:16d8:ddOO:38:0:0:0:2

I 2002:db5a:bccd:l:21d:e0ff:feb7:b96f 2002:b6ef:81c4:0:0:1145:59c5:3682

I Other Associations (1)

|_ 127.0.0.1 seen 1949869 times, last tx was unicast v2 mode 7

Which of the following commands was executed by the tester?

A. nmap-sU-pU:517-Pn-n--script=supermicro-ipmi-config

B. nmap-sU-pU:123-Pn-n--script=ntp-monlist

C. nmap-sU-pU:161-Pn-n--script