PT0-001 Q&As

CompTIA PenTest+ Exam

Pass CompTIA PT0-001 Exam with 100% Guarantee

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

https://www.pass2lead.com/pt0-001.html

100% Passing Guarantee
100% Money Back Assurance

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

- **Instant Download** After Purchase
- **100% Money Back** Guarantee
- **365 Days** Free Update
- **800,000+** Satisfied Customers

QUESTION 1

During an internal penetration test, several multicast and broadcast name resolution requests are observed traversing the network. Which of the following tools could be used to impersonate network resources and collect authentication requests?

A. Ettercap

B. Tcpdump

C. Responder

D. Medusa

Correct Answer: C

QUESTION 2

During the information gathering phase of a network penetration test for the corp.local domain, which of the following commands would provide a list of domain controllers?

A. nslookup -type=srv _ldap._tcp.dc._msdcs.corp.local

B. nmap -sV -p 389 - -script=ldap-rootdse corp.local

C. net group "Domain Controllers" /domain

D. gpresult /d corp.local /r "Domain Controllers"

Correct Answer: A

QUESTION 3

When considering threat actor scoping prior to an engagement, which of the following characteristics makes an APT challenging to emulate?

A. Development of custom zero-day exploits and tools

B. Leveraging the dark net for non-attribution

C. Tenacity and efficacy of social engineering attacks

D. Amount of bandwidth available for DoS attacks

Correct Answer: C

QUESTION 4

Which of the following vulnerabilities are MOST likely to be false positives when reported by an automated scanner on a static HTML web page? (Choose two.)

A. Missing secure flag for a sensitive cookie

B. Reflected cross-site scripting

C. Enabled directory listing

D. Insecure HTTP methods allowed

E. Unencrypted transfer of sensitive data

F. Command injection

G. Disclosure of internal system information

H. Support of weak cipher suites

Correct Answer: FG

QUESTION 5

Given the following HTTP response:

http/1.0 200 OKServer: ApacheSet-Cookie: AUTHID=879DHUT74D9A7C; http-onlyContent-type: text/htmlConnection: Close

Which of the following aspects of an XSS attack would be prevented?

A. Client-side website defacement

B. Session hijacking

C. Cross-site request forgery

D. JavaScript keylogging

Correct Answer: A

Reference: https://securityboulevard.com/2020/08/the-httponly-flag-protecting-cookies-against-xss/