PT0-001$^{Q\&As}$

CompTIA PenTest+ Exam

Pass CompTIA PT0-001 Exam with 100% Guarantee

QUESTION 1

A penetration tester must assess a web service. Which of the following should the tester request during the scoping phase?

A. XSD

B. After-hours contact escalation

C. WSDLfile

D. SOAP project file

Correct Answer: C

QUESTION 2

Which of the following reasons does penetration tester needs to have a customer\\'s point-of -contact information available at all time? (Select THREE).

A. To report indicators of compromise

B. To report findings that cannot be exploited

C. To report critical findings

D. To report the latest published exploits

E. To update payment information

F. To report a server that becomes unresponsive

G. To update the statement o(work

H. To report a cracked password

Correct Answer: ACF

QUESTION 3

A malicious user wants to perform an MITM attack on a computer. The computer network configuration is given below:

IP: 192.168.1.20 NETMASK: 255.255.255.0 DEFAULT GATEWAY: 192.168.1.254 DHCP: 192.168.1.253 DNS: 192.168.10.10, 192.168.20.10

Which of the following commands should the malicious user execute to perform the MITM attack?

A. arpspoof -c both -r -t 192.168.1.1 192.168.1.20

B. arpspoof -t 192.168.1.20 192.168.1.254

C. arpspoof -c both -t 192.168.1.20 192.168.1.253

D. arpspoof -r -t 192 .168.1.253 192.168.1.20

Correct Answer: B

Reference: https://www.hackers-arise.com/single-post/2017/07/25/Man-the-Middle-MiTM- Attack-with-ARPspoofing

QUESTION 4

A penetration tester, who is not on the client\\'s network. is using Nmap to scan the network for hosts that are in scope. The penetration tester is not receiving any response on the command:

nmap 100.100/1/0-125

Which of the following commands would be BEST to return results?

A. nmap -Pn -sT 100.100.1.0-125

B. nmap -sF -p 100.100.1.0-125

C. nmap -sV -oA output 100.100.10-125

D. nmap 100.100.1.0-125 -T4

Correct Answer: A

QUESTION 5

A penetration tester is preparing to conduct API testing Which of the following would be MOST helpful in preparing for this engagement?

A. NiktO

B. WAR

C. W3AF

D. Swagger

Correct Answer: D

Reference: https://blog.securelayer7.net/api-penetration-testing-with-owasp-2017-test-cases/