QUESTIONS & ANSWERS

Kill your exam at first Attempt

KILL EXAMS

CompTIA

PT0-001

CompTIA PenTest+ Certification

QUESTION: 65
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

Answer: A

QUESTION: 66
A tester has determined that null sessions are enabled on a domain controller. Which of the following attacks can be performed to leverage this vulnerability?

A. RID cycling to enumerate users and groups
B. Pass the hash to relay credentials
C. Password brute forcing to log into the host
D. Session hijacking to impersonate a system account

Answer: C

QUESTION: 67
A client asks a penetration tester to add more addresses to a test currently in progress. Which of the following would defined the target list?

A. Rules of engagement
B. Master services agreement
C. Statement of work
D. End-user license agreement

Answer: D

QUESTION: 68
After successfully capturing administrator credentials to a remote Windows machine, a penetration tester attempts to access the system using PSExec but is denied permission. Which of the following shares must be accessible for a successful PSExec connection?

A. IPCS and C$
B. C$ and ADMINS
C. SERVICES and ADMINS
D. ADMINS and IPCS

Answer: C

QUESTION: 69
In a physical penetration testing scenario, the penetration tester obtains physical access to a laptop following .s a potential NEXT step to extract credentials from the device?

A. Brute force the user's password.
B. Perform an ARP spoofing attack.
C. Leverage the BeEF framework to capture credentials.
D. Conduct LLMNR/NETBIOS-ns poisoning.

Answer: D

QUESTION: 70
A penetration tester ran the following Nmap scan on a computer nmap -sV 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.

Answer: A

QUESTION: 71
A penetration testet is attempting to capture a handshake between a client and an access point by monitoring a WPA2-PSK secured wireless network The (ester is monitoring the correct channel tor the identified network but has been unsuccessful in capturing a handshake Given this scenario, which of the following attacks would BEST assist the tester in obtaining this handshake?

A. Karma attack
B. DE authentication attack
C. Fragmentation attack
D. SSID broadcast flood

Answer: B

QUESTION: 72
A penetration tester is perform initial intelligence gathering on some remote hosts prior to conducting a vulnerability < The tester runs the following command
nmap -D 192.168.1.1,192.168.1.2,192.168.1.3 -sV -o —max rate 2 192. 168.130
Which ol the following BEST describes why multiple IP addresses are specified?

A. The network is submitted as a /25 or greater and the tester needed to access hosts on two different subnets
B. The tester is trying to perform a more stealthy scan by including several bogus addresses
C. The scanning machine has several interfaces to balance the scan request across at the specified rate
D. A discovery scan is run on the first set of addresses, whereas a deeper, more aggressive scan is run against the latter host.

Answer: C

QUESTION: 73
A penetration tester has compromised a host. Which of the following would be the correct syntax to create a Netcat listener on the device?

A. nc -lvp 4444 /bin/bash
B. nc -vp 4444 /bin/bash
C. nc -p 4444 /bin/bash
D. nc -lp 4444 -e /bin/bash

Answer: D