TestpassportQ&A

Higher Quality Better Service!

We offer free update service for one year

Http://www.testpassport.com

Exam : **PT0-001**

Title : CompTIA PenTest+ Certification Exam

Version : DEMO

1.In which of the following scenarios would a tester perform a Kerberoasting attack?
A. The tester has compromised a Windows device and dumps the LSA secrets.
B. The tester needs to retrieve the SAM database and crack the password hashes.
C. The tester has compromised a limited-privilege user and needs to target other accounts for lateral movement.
D. The tester has compromised an account and needs to dump hashes and plaintext passwords from the system.
Answer: C

2.A penetration tester is testing a web application and is logged in as a lower-privileged user. The tester runs arbitrary JavaScript within an application, which sends an XMLHttpRequest, resulting in exploiting features to which only an administrator should have access.
Which of the following controls would BEST mitigate the vulnerability?
A. Implement authorization checks.
B. Sanitize all the user input.
C. Prevent directory traversal.
D. Add client-side security controls
Answer: A

3.A penetration tester is performing an annual security assessment for a repeat client. The tester finds indicators of previous compromise.
Which of the following would be the most logical steps to follow NEXT?
A. Report the incident to the tester's immediate manager and follow up with the client immediately
B. Report the incident to the clients Chief Information Security Officer (CISO) immediately and alter the terms of engagement accordingly
C. Report the incident to the client's legal department and then follow up with the client's security operations team
D. Make note of the anomaly, continue with the penetration testing and detail it in the final report
Answer: A

4.A penetration tester wants to script out a way to discover all the RPTR records for a range of IP addresses.
Which of the following is the MOST efficient to utilize?
A. nmap -p 53 -oG dnslist.txt | cut -d “:” -f 4
B. nslookup -ns 8.8.8.8 << dnslist.txt
C. for x in (1…254); do dig -x 192.168. $x. $x; done
D. dig -r > echo “8.8.8.8” >> /etc/resolv/conf
Answer: C

5.After successfully exploiting a local file inclusion vulnerability within a web application a limited reverse shell is spawned back to the penetration tester's workstation.
Which of the following can be used to escape the limited shell and create a fully functioning TTY?
A. per1 -e ' : set shall=/bin/bash:shell'
B. php -r ,Sshell=f3hellopen("/bin/bash-);exec($9he:i)'

C. bash -i >fi /dev/localhosc Oil
D. python -c 'import pty;pcy.3pawn("/bin/bash")'
Answer: D