PT0-002$^{Q\&As}$

CompTIA PenTest+ Certification Exam

QUESTION 1

A penetration tester runs the unshadow command on a machine. Which of the following tools will the tester most likely use NEXT?

A. John the Ripper

B. Hydra

C. Mimikatz

D. Cain and Abel

Correct Answer: A

Reference: https://www.cyberciti.biz/faq/unix-linux-password-cracking-john-the-ripper/

QUESTION 2

A security engineer identified a new server on the network and wants to scan the host to determine if it is running an approved version of Linux and a patched version of Apache. Which of the following commands will accomplish this task?

A. nmap-f-sV-p80 192.168.1.20

B. nmap-sS-sL-p80 192.168.1.20

C. nmap-A-T4-p80 192.168.1.20

D. nmap-O-v-p80 192.168.1.20

Correct Answer: C

Reference: https://nmap.org/book/man-version-detection.html

QUESTION 3

A red team gained access to the internal network of a client during an engagement and used the Responder tool to capture important data. Which of the following was captured by the testing team?

A. Multiple handshakes

B. IP addresses

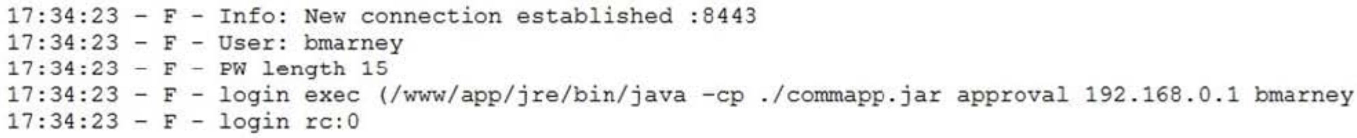
C. Encrypted file transfers

D. User hashes sent over SMB

Correct Answer: B

QUESTION 4

A penetration tester downloaded a Java application file from a compromised web server and identifies how to invoke it by looking at the following log:



```
17:34:23 - F - Info: New connection established :8443
17:34:23 - F - User: bmarney
17:34:23 - F - PW length 15
17:34:23 - F - login exec (/www/app/jre/bin/java -cp ./commapp.jar approval 192.168.0.1 bmarney
17:34:23 - F - login rc:0
```

Which of the following is the order of steps the penetration tester needs to follow to validate whether the Java application uses encryption over sockets?

A. Run an application vulnerability scan and then identify the TCP ports used by the application.

B. Run the application attached to a debugger and then review the application\\'s log.

C. Disassemble the binary code and then identify the break points.

D. Start a packet capture with Wireshark and then run the application.

Correct Answer: D

QUESTION 5

Deconfliction is necessary when the penetration test:

A. determines that proprietary information is being stored in cleartext.

B. occurs during the monthly vulnerability scanning.

C. uncovers indicators of prior compromise over the course of the assessment.

D. proceeds in parallel with a criminal digital forensic investigation.

Correct Answer: C

This will then enable the PenTest to continue so that additional issues can be found, exploited, and analyzed.