GPEN Q&As

GIAC Certified Penetration Tester

QUESTION 1

Which of the following enables an inventor to legally enforce his right to exclude others from using his invention?

A. Artistic license

B. Spam

C. Patent

D. Phishing

Correct Answer: C

QUESTION 2

Which of the following describe the benefits to a pass-the-hash attack over traditional password cracking?

A. No triggering of IDS signatures from the attack privileges at the level of theacquired password hash and no corruption of the LSASS process.

B. No triggering of IDS signatures from the attack, no account lockout and use ofnative windows file and print sharing tools on the compromised system.

C. No account lockout, privileges at the level of the acquired password hash and useof native windows file and print Sharif tools on the compromised system.

D. No account lockout, use of native file and print sharing tools on the compromisedsystem and no corruption of the LSASS process.

Correct Answer: D

QUESTION 3

Which of the following tools allows you to download World Wide Web sites from the Internet to a local computer?

A. Netcraft

B. HTTrack

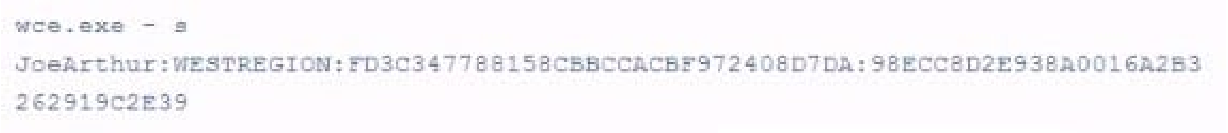
C. Netstat

D. Cheops-ng

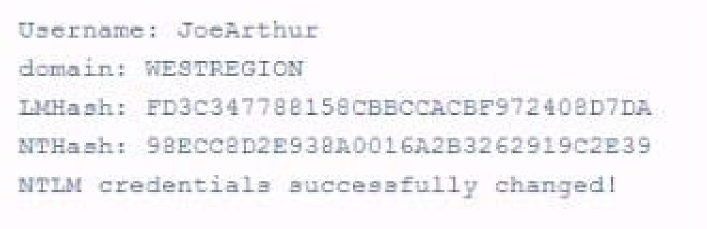
Correct Answer: B

QUESTION 4

A pen tester is able to pull credential information from memory on a Windows system. Based on the command and output below, what advantage does this technique give a penetration tester when trying to access another windows system on the network?



```
wce.exe - s
JoeArthur:WESTREGION:FD3C347788158CBBCCACBF972408D7DA:98ECC8D2E938A0016A2B3
262919C2E39
```



```
Username: JoeArthur
domain: WESTREGION
LMHash: FD3C347788158CBBCCACBF972408D7DA
NTHash: 98ECC8D2E938A0016A2B3262919C2E39
NTLM credentials successfully changed!
```

A. The technique is more effective through perimeter firewalls than otherauthentication attacks.

B. It allows the tester to escalate the privilege level of the account,

C. Access to the system can be gained without password guessing or cracking.

D. Salts are removed from the hashes to allow for faster, offline cracking

Correct Answer: A

QUESTION 5

Which of the following TCP packet sequences are common during a SYN (or half-open) scan?

A. The source computer sends SYN and the destination computer responds with RST

B. The source computer sends SYN-ACK and no response Is received from the destination computer

C. The source computer sends SYN and no response is received from the destination computer

D. The source computer sends SYN-ACK and the destination computer responds with RST-ACK

A. A,B and C

B. A and C

C. C and D

D. C and D

Correct Answer: C

[GPEN VCE Dumps](#) [GPEN Exam Questions](#) [GPEN Braindumps](#)