312-50$^{\text{Q\&As}}$

Ethical Hacker Certified

Pass EC-COUNCIL 312-50 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.geekcert.com/312-50.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by EC-COUNCIL Official Exam Center

QUESTION 1

Bob reads an article about how insecure wireless networks can be. He gets approval from his management to implement a policy of not allowing any wireless devices on the network. What other steps does Bob have to take in order to successfully implement this? (Select 2 answer.)

A. Train users in the new policy.

B. Disable all wireless protocols at the firewall.

C. Disable SNMP on the network so that wireless devices cannot be configured.

D. Continuously survey the area for wireless devices.

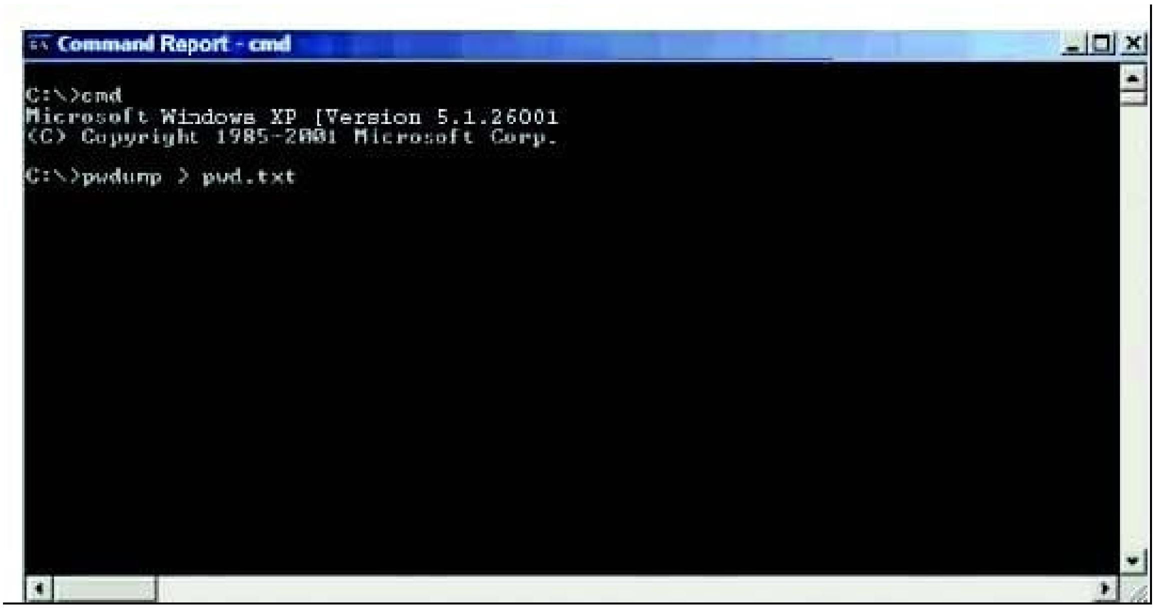
Correct Answer: AD

If someone installs a access point and connect it to the network there is no way to find it unless you are constantly surveying the area for wireless devices. SNMP and firewalls can not prevent the installation of wireless devices on the corporate network.

QUESTION 2

Michael is the security administrator for the for ABC company. Michael has been charged with strengthening the company\\'s security policies, including its password policies. Due to certain legacy applications. Michael was only able to enforce a password group policy in Active Directory with a minimum of 10 characters. He has informed the company\\'s employes, however that the new password policy requires that everyone must have complex passwords with at least 14 characters. Michael wants to ensure that everyone is using complex passwords that meet the new security policy requirements. Michael has just logged on to one of the network\\'s domain controllers and is about to run the following command:

What will this command accomplish?



```
C:\>cmd
Microsoft Windows XP [Version 5.1.26001
(C) Copyright 1985-2001 Microsoft Corp.

C:\>pwdump > pwd.txt
```

A. Dumps SAM password hashes to pwd.txt

B. Password history file is piped to pwd.txt

C. Dumps Active Directory password hashes to pwd.txt

D. Internet cache file is piped to pwd.txt

Correct Answer: A

Pwdump is a hack tool that is used to grab Windows password hashes from a remote Windows computer. Pwdump > pwd.txt will redirect the output from pwdump to a text file named pwd.txt

QUESTION 3

You are trying to compromise a Linux Machine and steal the password hashes for cracking with password brute forcing program. Where is the password file kept is Linux?

A. /etc/shadow

B. /etc/passwd

C. /bin/password

D. /bin/shadow

Correct Answer: A

/etc/shadow file stores actual password in encrypted format for user\\'s account with additional properties related to user password i.e. it stores secure user account information. All fields are separated by a colon (:) symbol. It contains one entry per line for each user listed in /etc/passwd file.

QUESTION 4

Google uses a unique cookie for each browser used by an individual user on a computer. This cookie contains information that allows Google to identify records about that user on its database. This cookie is submitted every time a user launches a Google search, visits a site using AdSense etc. The information stored in Google\\'s database, identified by the cookie, includes

How would you prevent Google from storing your search keywords?

A. Block Google Cookie by applying Privacy and Security settings in your web browser

B. Disable the Google cookie using Google Advanced Search settings on Google Search page

C. Do not use Google but use another search engine Bing which will not collect and store your search keywords

D. Use MAC OS X instead of Windows 7. Mac OS has higher level of privacy controls by default.

Correct Answer: A

QUESTION 5

ETHER: Destination address : 0000BA5EBA11 ETHER: Source address :

00A0C9B05EBD ETHER: Frame Length : 1514 (0x05EA) ETHER: Ethernet Type :

0x0800 (IP) IP: Version = 4 (0x4) IP: Header Length = 20 (0x14) IP:

Service Type = 0 (0x0) IP: Precedence = Routine IP: ...0.... = Normal Delay IP: ....0... = Normal Throughput IP: .....0.. = Normal Reliability IP: Total Length = 1500 (0x5DC) IP: Identification = 7652 (0x1DE4) IP: Flags Summary = 2 (0x2)

IP: ....0 = Last fragment in datagram IP: ......1. = Cannot fragment datagram IP:

Fragment Offset = (0x0) bytes IP: Time to Live = 127 (0x7F) IP: Protocol = TCP - Transmission Control IP: Checksum = 0xC26D IP: Source Address = 10.0.0.2 IP:

Destination Address = 10.0.1.201 TCP: Source Port = Hypertext Transfer Protocol TCP: Destination Port = 0x1A0B TCP: Sequence Number = 97517760 (0x5D000C0) TCP: Acknowledgement Number = 78544373 (0x4AE7DF5) TCP:

Data Offset = 20 (0x14) TCP: Reserved = 0 (0x0000) TCP: Flags = 0x10 : .A.... TCP: ..0..... = No urgent data TCP: ...1.... = Acknowledgement field significant TCP: ....0... = No Push function TCP:

.....0.. = No Reset TCP: ......0. = No Synchronize TCP: ....0 = No Fin TCP: Window = 28793 (0x7079) TCP: Checksum = 0x8F27 TCP: Urgent Pointer = 0 (0x0) An employee wants to defeat detection by a network-based IDS application. He

does not want to attack the system containing the IDS application. Which of the following strategies can be used to defeat detection by a network-based IDS application?

A. Create a SYN flood

B. Create a network tunnel

C. Create multiple false positives

D. Create a ping flood

Correct Answer: B

Certain types of encryption presents challenges to network-based intrusion detection and may leave the IDS blind to certain attacks, where a host-based IDS analyzes the data after it has been decrypted.

312-50 Study Guide 312-50 Exam Questions 312-50 Braindumps