



# 312-50<sup>Q&As</sup>

Ethical Hacker Certified

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

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

<https://www.pass4itsure.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

-  **Instant Download** After Purchase
-  **100% Money Back** Guarantee
-  **365 Days** Free Update
-  **800,000+** Satisfied Customers



**QUESTION 1**

Under what conditions does a secondary name server request a zone transfer from a primary name server?

- A. When a primary SOA is higher than a secondary SOA
- B. When a secondary SOA is higher than a primary SOA
- C. When a primary name server has had its service restarted
- D. When a secondary name server has had its service restarted
- E. When the TTL falls to zero

Correct Answer: A

Understanding DNS is critical to meeting the requirements of the CEH. When the serial number that is within the SOA record of the primary server is higher than the Serial number within the SOA record of the secondary DNS server, a zone transfer will take place.

---

**QUESTION 2**

Ethernet switches can be adversely affected by rapidly bombarding them with spoofed ARP responses. The port to MAC Address table (CAM Table) overflows on the switch and rather than failing completely, moves into broadcast mode, then the hacker can sniff all of the packets on the network.

Which of the following tool achieves this?

- A. ./macof
- B. ./sniffof
- C. ./dnsiff
- D. ./switchsnarf

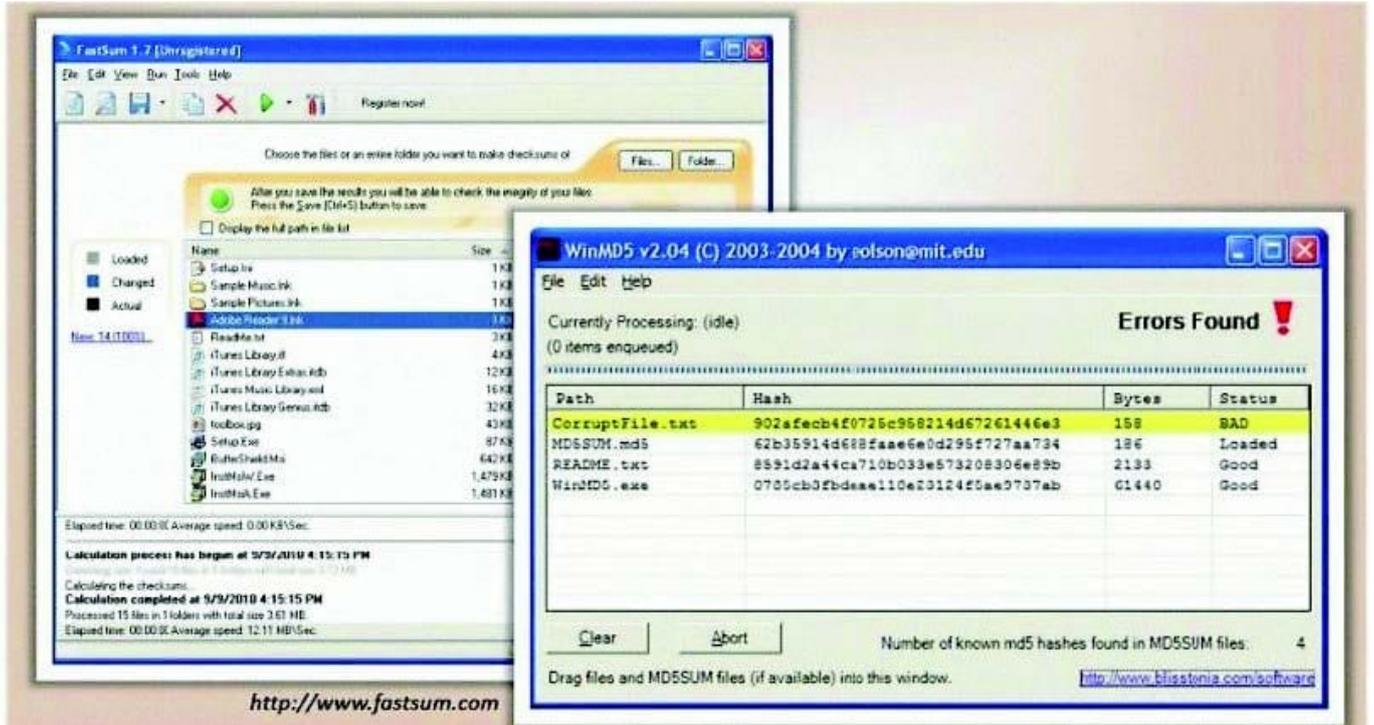
Correct Answer: A

macof floods the local network with random MAC addresses (causing some switches to fail open in repeating mode, facilitating sniffing).

---

**QUESTION 3**

You generate MD5 128-bit hash on all files and folders on your computer to keep a baseline check for security reasons?



What is the length of the MD5 hash?

- A. 32 bit
- B. 64 byte
- C. 48 char
- D. 128 kb

Correct Answer: C

#### QUESTION 4

In the context of Windows Security, what is a '\\null\' user?

- A. A user that has no skills
- B. An account that has been suspended by the admin
- C. A pseudo account that has no username and password
- D. A pseudo account that was created for security administration purpose

Correct Answer: C

NULL sessions take advantage of "features" in the SMB (Server Message Block) protocol that exist primarily for trust relationships. You can establish a NULL session with a Windows host by logging on with a NULL user name and password.



Using these NULL connections allows you to gather the following information from the host: \* List of users and groups \* List of machines \* List of shares \* Users and host SID\\' (Security Identifiers) NULL sessions exist in windows networking to

allow: \* Trusted domains to enumerate resources \* Computers outside the domain to authenticate and enumerate users \* The SYSTEM account to authenticate and enumerate resources

NetBIOS NULL sessions are enabled by default in Windows NT and 2000. Windows XP and 2003 will allow anonymous enumeration of shares, but not SAM accounts.

---

## QUESTION 5

Buffer X is an Accounting application module for company can contain 200 characters. The programmer makes an assumption that 200 characters are more than enough. Because there were no proper boundary checks being conducted.

Dave decided to insert 400 characters into the 200-character buffer which overflows the buffer. Below is the code snippet:

Void func (void)

```
{int i; char buffer [200];
```

```
for (i=0; i
```