312-50V7^{Q&As}

Ethical Hacking and Countermeasures (CEHv7)

Pass EC-COUNCIL 312-50V7 Exam with 100% Guarantee

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

https://www.pass2lead.com/312-50v7.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

![Pass2Lead](https://Pass2Lead.com)
QUESTION 1

ICMP ping and ping sweeps are used to check for active systems and to check

A. if ICMP ping traverses a firewall.

B. the route that the ICMP ping took.

C. the location of the switchport in relation to the ICMP ping.

D. the number of hops an ICMP ping takes to reach a destination.

Correct Answer: A

QUESTION 2

Which of the following describes the characteristics of a Boot Sector Virus?

A. Moves the MBR to another location on the RAM and copies itself to the original location of the MBR

B. Moves the MBR to another location on the hard disk and copies itself to the original location of the MBR

C. Modifies directory table entries so that directory entries point to the virus code instead of the actual program

D. Overwrites the original MBR and only executes the new virus code

Correct Answer: B

QUESTION 3

Neil is an IT security consultant working on contract for Davidson Avionics. Neil has been hired to audit the network of Davidson Avionics. He has been given permission to perform any tests necessary. Neil has created a fake company ID badge and uniform. Neil waits by one of the company\\'s entrance doors and follows an employee into the office after they use their valid access card to gain entrance. What type of social engineering attack has Neil employed here?

A. Neil has used a tailgating social engineering attack to gain access to the offices

B. He has used a piggybacking technique to gain unauthorized access

C. This type of social engineering attack is called man trapping

D. Neil is using the technique of reverse social engineering to gain access to the offices of Davidson Avionics

Correct Answer: A

QUESTION 4

Which of the following is a strong post designed to stop a car?

![Pass2Lead](https://Pass2Lead.com)
A. Gate

B. Fence

C. Bollard

D. Reinforced rebar

Correct Answer: C

QUESTION 5

After a client sends a connection request (SYN) packet to the server, the server will respond (SYN- ACK) with a sequence number of its choosing, which then must be acknowledged (ACK) by the client. This sequence number is predictable; the attack connects to a service first with its own IP address, records the sequence number chosen, and then opens a second connection from a forged IP address. The attack doesn\'t see the SYN-ACK (or any other packet) from the server, but can guess the correct responses. If the source IP address is used for authentication, then the attacker can use the one-sided communication to break into the server. What attacks can you successfully launch against a server using the above technique?

A. Denial of Service attacks

B. Session Hijacking attacks

C. Web page defacement attacks

D. IP spoofing attacks

Correct Answer: B

QUESTION 6

A tester is attempting to capture and analyze the traffic on a given network and realizes that the network has several switches. What could be used to successfully sniff the traffic on this switched network? (Choose three.)

A. ARP spoofing

B. MAC duplication

C. MAC flooding

D. SYN flood

E. Reverse smurf attack

F. ARP broadcasting

Correct Answer: ABC

QUESTION 7

![Pass2Lead](https://Pass2Lead.com)
What is the problem with this ASP script (login.asp)?

```
strsql = "SELECT * FROM Users where where Username='" + Login1.UserName
+ "' and Pass='" + password + "'
try
{
OleDbConnection con = new OleDbConnection(connectionstring);
con.Open();
OleDbCommand cmd = new OleDbCommand(strsql, con);
OleDbDataReader dr = cmd.ExecuteReader();
if (dr.HasRows)
{
If (dr.Read())
{
Session["username"] = Login1.UserName;
Response.Redirect("Mainpage.aspx", false);
else
{
Response.Redirect("Login.aspx", false);
}
}
}
dr.Dispose();
con.Close();
}
catch (Exception ex)
{
ClientScript.RegisterStartupScript(this.GetType(), "msg",
"<script>alert('" + ex.Message + "'</script>");
```

A. The ASP script is vulnerable to Cross Site Scripting attack

B. The ASP script is vulnerable to Session Splice attack

C. The ASP script is vulnerable to XSS attack

D. The ASP script is vulnerable to SQL Injection attack
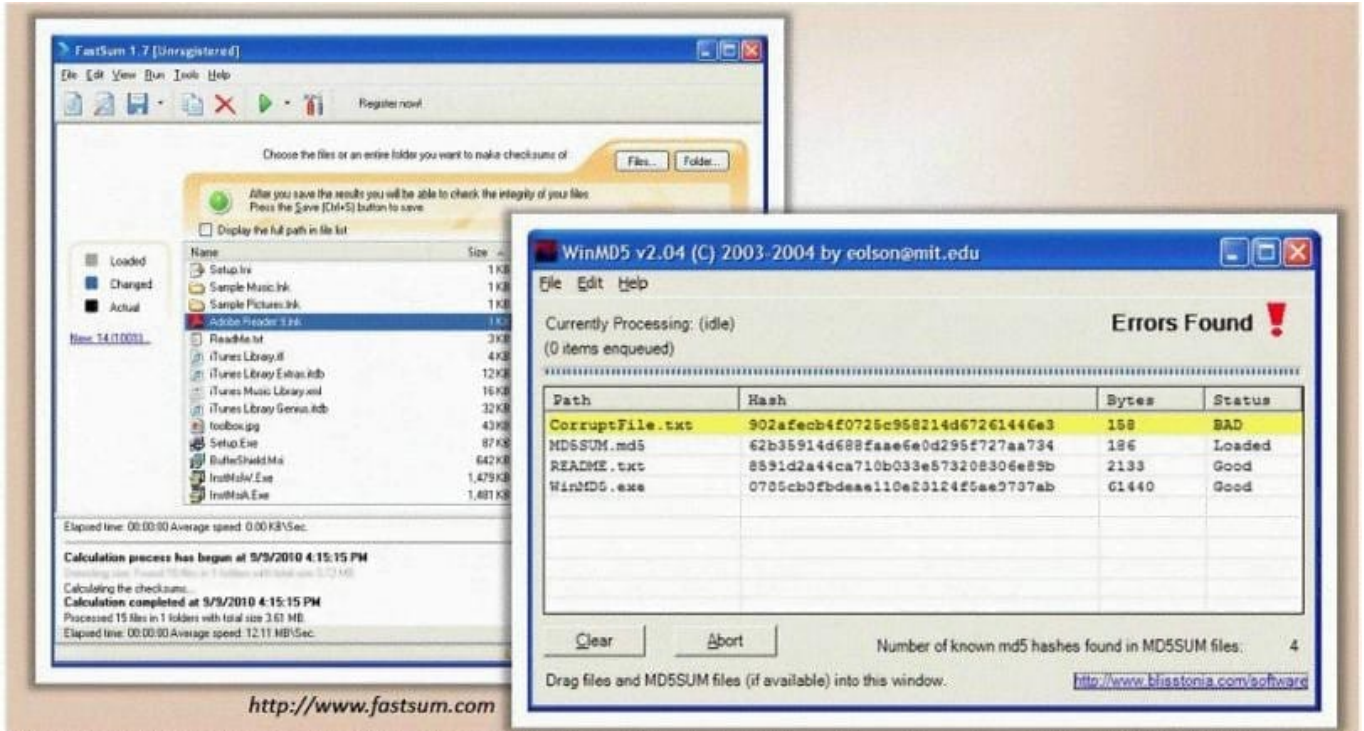
Correct Answer: D

QUESTION 8

A hacker is attempting to use nslookup to query Domain Name Service (DNS). The hacker uses the nslookup interactive mode for the search. Which command should the hacker type into the command shell to request the appropriate records?

A. Locate type=ns

B. Request type=ns

C. Set type=ns

D. Transfer type=ns

Correct Answer: C

QUESTION 9

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 character B. 64 byte

C. 48 char

D. 128 kb

Correct Answer: A

QUESTION 10

When using Wireshark to acquire packet capture on a network, which device would enable the capture of all traffic on the wire?

A. Network tap

B. Layer 3 switch

C. Network bridge

D. Application firewall

![Pass2Lead](https://Pass2Lead.com)
Correct Answer: A

QUESTION 11

Which Open Web Application Security Project (OWASP) implements a web application full of known vulnerabilities?

A. WebBugs

B. WebGoat

C. VULN_HTML

D. WebScarab

Correct Answer: B

QUESTION 12

Which statement is TRUE regarding network firewalls preventing Web Application attacks?

A. Network firewalls can prevent attacks because they can detect malicious HTTP traffic.

B. Network firewalls cannot prevent attacks because ports 80 and 443 must be opened.

C. Network firewalls can prevent attacks if they are properly configured.

D. Network firewalls cannot prevent attacks because they are too complex to configure.

Correct Answer: B

QUESTION 13

The fundamental difference between symmetric and asymmetric key cryptographic systems is that symmetric key cryptography uses which of the following?

A. Multiple keys for non-repudiation of bulk data

B. Different keys on both ends of the transport medium

C. Bulk encryption for data transmission over fiber

D. The same key on each end of the transmission medium

Correct Answer: D

QUESTION 14

Joseph has just been hired on to a contractor company of the Department of Defense as their Senior Security Analyst. Joseph has been instructed on the company\\\'s strict security policies that have been implemented, and the policies that

![Pass2Lead](https://Pass2Lead.com)
have yet to be put in place. Per the Department of Defense, all DoD users and the users of their contractors must use two-factor authentication to access their networks. Joseph has been delegated the task of researching and implementing the best two-factor authentication method for his company. Joseph\\'s supervisor has told him that they would like to use some type of hardware device in tandem with a security or identifying pin number. Joseph\\'s company has already researched using smart cards and all the resources needed to implement them, but found the smart cards to not be cost effective. What type of device should Joseph use for two-factor authentication?

A. Biometric device

B. OTP

C. Proximity cards

D. Security token

Correct Answer: D

QUESTION 15

While performing a ping sweep of a local subnet you receive an ICMP reply of Code 3/Type 13 for all the pings you have sent out. What is the most likely cause of this?

A. The firewall is dropping the packets

B. An in-line IDS is dropping the packets

C. A router is blocking ICMP

D. The host does not respond to ICMP packets

Correct Answer: C