Free Questions for ECSAv10 by actualtestdumps

Shared by Hubbard on 20-10-2022

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

An attacker injects malicious query strings in user input fields to bypass web service authentication mechanisms and to access back-end databases. Which of the following attacks is this?

Options:

A- Frame Injection Attack

B- LDAP Injection Attack

C- XPath Injection Attack

D- SOAP Injection Attack

Answer:

D

Question 2

Question Type: MultipleChoice

Transmission Control Protocol (TCP) is a connection-oriented four layer protocol. It is responsible for breaking messages into segments, re-assembling them at the destination station, and re-sending. Which one of the following protocols does not use the TCP?

Options:

A- Reverse Address Resolution Protocol (RARP)

B- HTTP (Hypertext Transfer Protocol)

C- SMTP (Simple Mail Transfer Protocol)

D- Telnet

Answer:

A

Question 3

Question Type: **MultipleChoice**

Michael works for Kimball Construction Company as senior security analyst. As part of yearly security audit, Michael scans his network for vulnerabilities. Using Nmap, Michael conducts XMAS scan and most of the ports scanned do not give a response. In what state are these ports?

Options:

A- Filtered

B- Stealth

C- Closed

D- Open

Answer:

D

Question 4

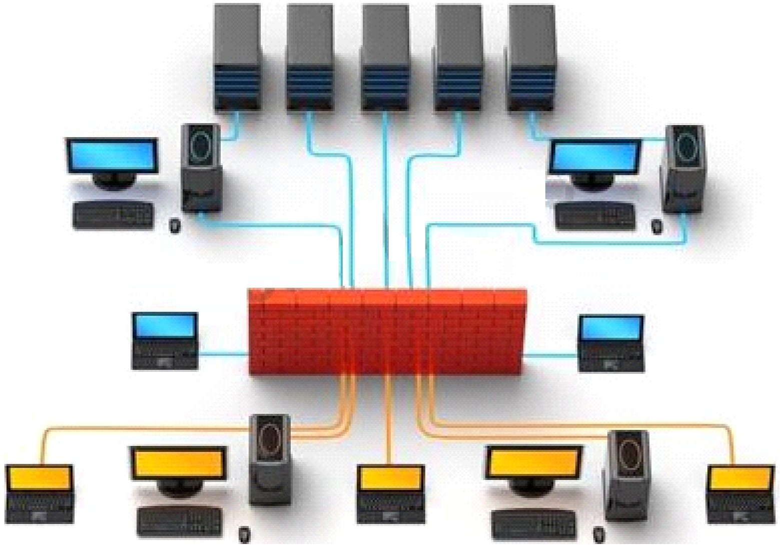
Question Type: **MultipleChoice**

Information gathering is performed to:

i) Collect basic information about the target company and its network

ii) Determine the operating system used, platforms running, web server versions, etc.

iii) Find vulnerabilities and exploits



Which of the following pen testing tests yields information about a company's technology infrastructure?

Options:

A- Searching for web page posting patterns

B- Analyzing the link popularity of the company's website

C- Searching for trade association directories

D- Searching for a company's job postings

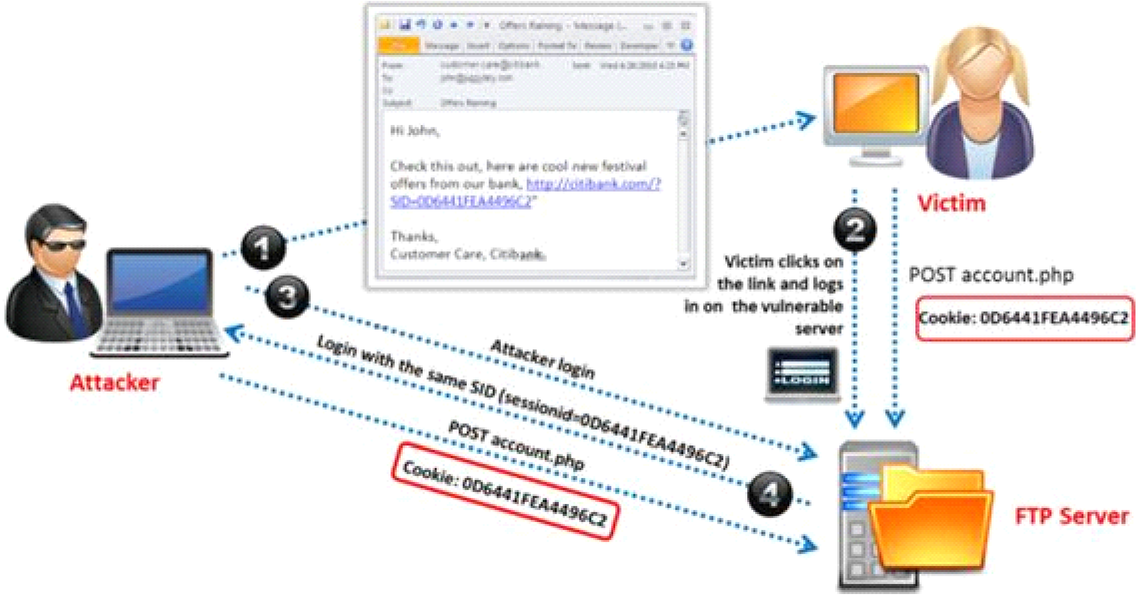
Answer:

D

Question 5

Question Type: MultipleChoice

Identify the attack represented in the diagram below:



Hi John,

Check this out, here are cool new festival offers from our bank, http://citibank.com/?SID=0D6441FEA4496C2"

Thanks,
Customer Care, Citibank.

Options:

A- Input Validation

B- Session Hijacking

C- SQL Injection

D- Denial-of-Service

Answer:

B

Question 6

Question Type: **MultipleChoice**

Which among the following information is not furnished by the Rules of Engagement (ROE) document?

Options:

A- Techniques for data collection from systems upon termination of the test

B- Techniques for data exclusion from systems upon termination of the test

C- Details on how data should be transmitted during and after the test

D- Details on how organizational data is treated throughout and after the test

Answer:

A

Question 7

Question Type: **MultipleChoice**

In a virtual test environment, Michael is testing the strength and security of BGP using multiple routers to mimic the backbone of the Internet. This project will help him write his doctoral thesis on "bringing down the Internet".

Without sniffing the traffic between the routers, Michael sends millions of RESET packets to the routers in an attempt to shut one or all of them down. After a few hours, one of the routers finally shuts itself down.

What will the other routers communicate between themselves?

Options:

A- More RESET packets to the affected router to get it to power back up

B- RESTART packets to the affected router to get it to power back up

C- The change in the routing fabric to bypass the affected router

D- STOP packets to all other routers warning of where the attack originated

Answer:

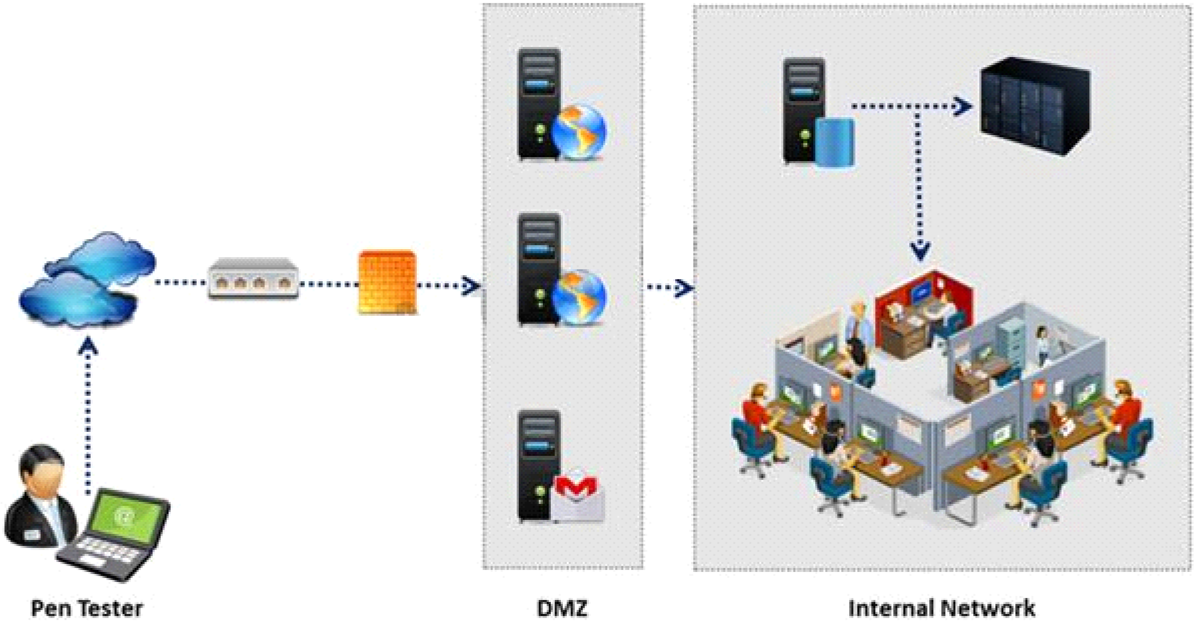
C

Question 8

Question Type: **MultipleChoice**

An external intrusion test and analysis identify security weaknesses and strengths of the client's systems and networks as they appear from outside the client's security perimeter, usually from the Internet.

The goal of an external intrusion test and analysis is to demonstrate the existence of known vulnerabilities that could be exploited by an external attacker.



During external penetration testing, which of the following scanning techniques allow you to determine a port's state without making a full connection to the host?

Options:

A- XMAS Scan

B- SYN scan

C- FIN Scan

D- NULL Scan

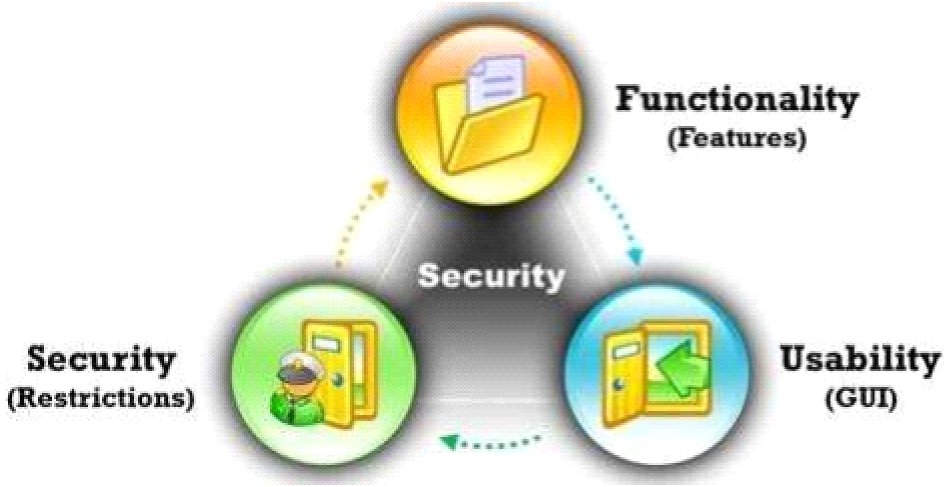
Answer:

B

Question 9

Question Type: **MultipleChoice**

Today, most organizations would agree that their most valuable IT assets reside within applications and databases. Most would probably also agree that these are areas that have the weakest levels of security, thus making them the prime target for malicious activity from system administrators, DBAs, contractors, consultants, partners, and customers.



Which of the following flaws refers to an application using poorly written encryption code to securely encrypt and store sensitive data in the database and allows an attacker to steal or modify weakly protected data such as credit card numbers, SSNs, and other authentication credentials?

Options:

A- SSI injection attack

B- Insecure cryptographic storage attack

C- Hidden field manipulation attack

D- Man-in-the-Middle attack

Answer:

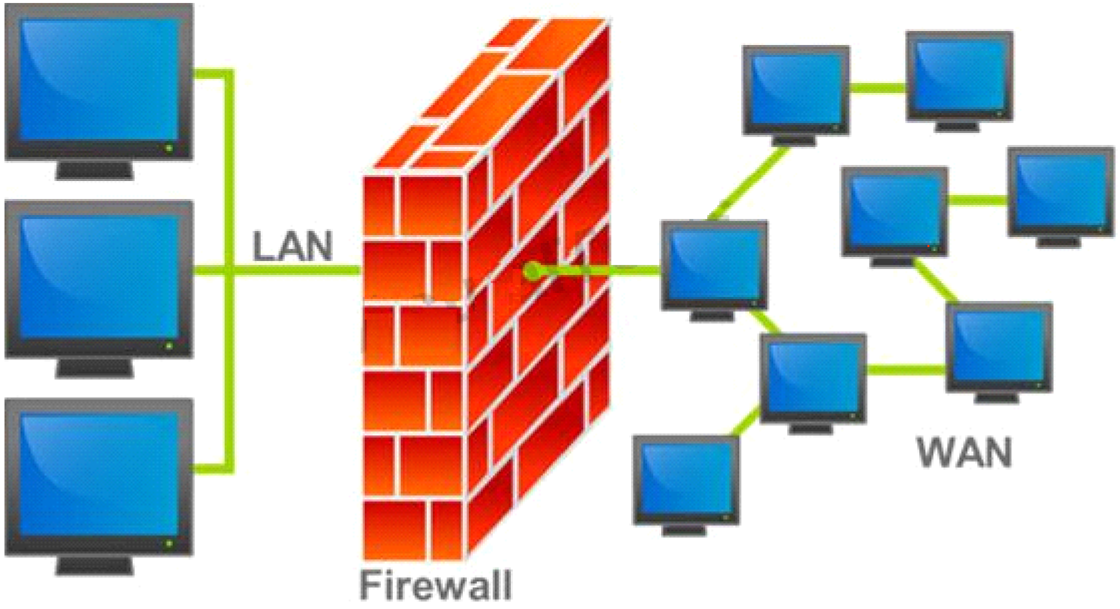
B

Question 10

Question Type: **MultipleChoice**

A firewall protects networked computers from intentional hostile intrusion that could compromise confidentiality or result in data corruption or denial of service. It examines all traffic routed between the two networks to see if it meets certain criteri

a. If it does, it is routed between the networks, otherwise it is stopped.



Why is an appliance-based firewall is more secure than those implemented on top of the commercial operating system (Software based)?

Options:

A- Appliance based firewalls cannot be upgraded

B- Firewalls implemented on a hardware firewall are highly scalable

C- Hardware appliances does not suffer from security vulnerabilities associated with the underlying operating system

D- Operating system firewalls are highly configured

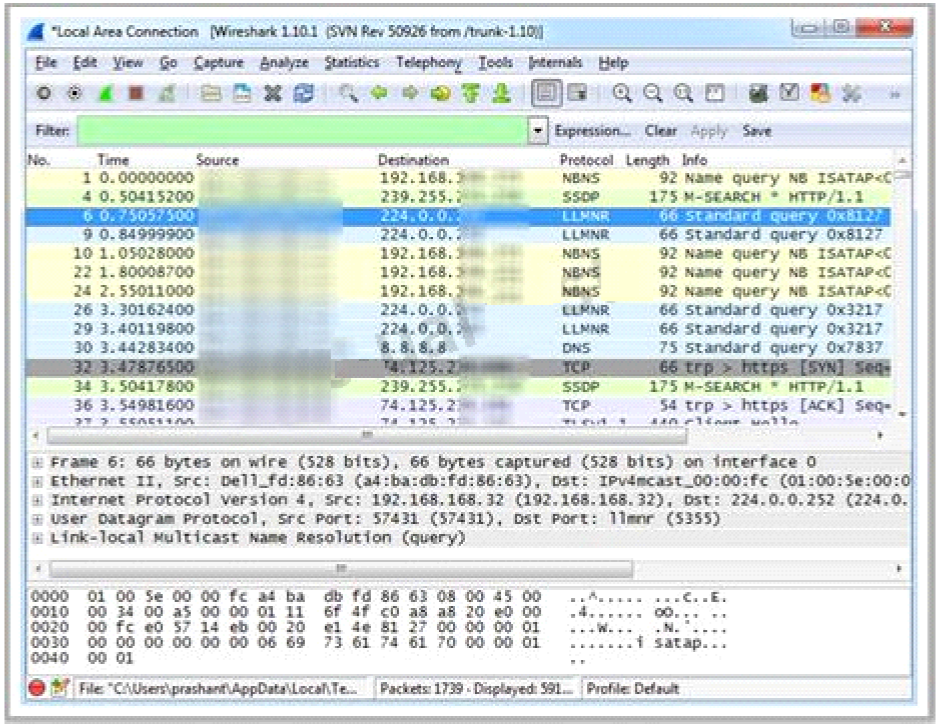
Answer:

A

Question 11

Question Type: MultipleChoice

Which Wireshark filter displays all the packets where the IP address of the source host is 10.0.0.7?



*Local Area Connection [Wireshark 1.10.1 (SVN Rev 50926 from /trunk-1.10)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter:
Expression... Clear Apply Save

```
No.   Time        Source      Destination         Protocol Length Info
    1 0.00000000  [redacted]  192.168.[redacted]  NBNS      92 Name query NB ISATAP<C
    4 0.50415200  [redacted]  239.255.[redacted]  SSDP     175 M-SEARCH * HTTP/1.1
    6 0.75057500  [redacted]  224.0.0.[redacted]  LLMNR     66 Standard query 0x8127
    9 0.84999900  [redacted]  224.0.0.[redacted]  LLMNR     66 Standard query 0x8127
   10 1.05028000  [redacted]  192.168.[redacted]  NBNS      92 Name query NB ISATAP<C
   22 1.80008700  [redacted]  192.168.[redacted]  NBNS      92 Name query NB ISATAP<C
   24 2.55011000  [redacted]  192.168.[redacted]  NBNS      92 Name query NB ISATAP<C
   26 3.30162400  [redacted]  224.0.0.[redacted]  LLMNR     66 Standard query 0x3217
   29 3.40119800  [redacted]  224.0.0.[redacted]  LLMNR     66 Standard query 0x3217
   30 3.44283400  [redacted]  8.8.8.8             DNS       75 Standard query 0x7837
   32 3.47876500  [redacted]  74.125.2[redacted]  TCP       66 trp > https [SYN] Seq=
   34 3.50417800  [redacted]  239.255.[redacted]  SSDP     175 M-SEARCH * HTTP/1.1
   36 3.54981600  [redacted]  74.125.2[redacted]  TCP       54 trp > https [ACK] Seq=
   37 3.55051100  [redacted]  74.125.2[redacted]  TLSv1.1  440 Client Hello
```

```
⊞ Frame 6: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface 0
⊞ Ethernet II, Src: Dell_fd:86:63 (a4:ba:db:fd:86:63), Dst: IPv4mcast_00:00:fc (01:00:5e:00:0
⊞ Internet Protocol Version 4, Src: 192.168.168.32 (192.168.168.32), Dst: 224.0.0.252 (224.0.
⊞ User Datagram Protocol, Src Port: 57431 (57431), Dst Port: llmnr (5355)
⊞ Link-local Multicast Name Resolution (query)
```

```
0000  01 00 5e 00 00 fc a4 ba  db fd 86 63 08 00 45 00   ..^..... ...c..E.
0010  00 34 00 a5 00 00 01 11  6f 4f c0 a8 a8 20 e0 00   .4...... oO... ..
0020  00 fc e0 57 14 eb 00 20  e1 4e 81 27 00 00 00 01   ...W...  .N.'....
0030  00 00 00 00 00 00 06 69  73 61 74 61 70 00 00 01   .......i satap...
0040  00 01                                              ..
```

File: "C:\Users\prashant\AppData\Local\Te... | Packets: 1739 · Displayed: 591... | Profile: Default

Options:

A- ip.dst==10.0.0.7

B- ip.port==10.0.0.7

C- ip.src==10.0.0.7

D- ip.dstport==10.0.0.7

Answer:

C