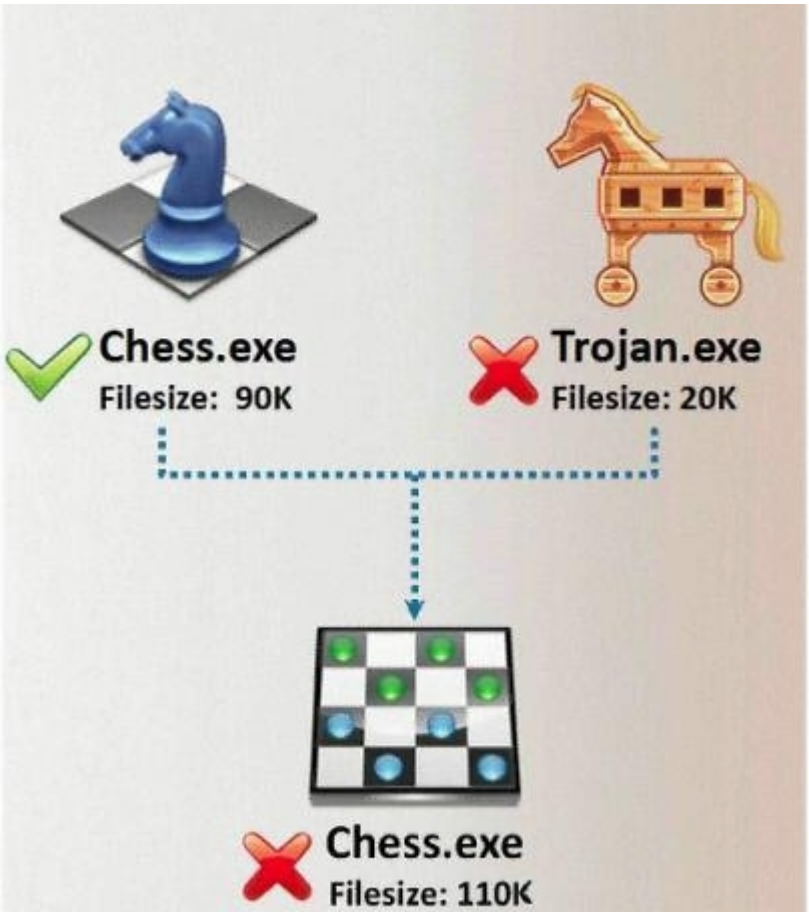


A. Mixer
B. Converter
C. Wrapper
D. Zipper

Correct Answer: C

QUESTION 42

Syslog is a standard for logging program messages. It allows separation of the software that generates messages from the system that stores them and the software that reports and analyzes them. It also provides devices, which would otherwise be unable to communicate a means to notify administrators of problems or performance. What default port Syslog daemon listens on?

System Messages from the previous week

Thursday, July 20, 2006 12:21:25 PM CDT

Lists all system messages reported during the past 7 days

Number of records reported: 5

▼TimeStamp	ID	Severity	Server	Component	Error Co
Monday, July 17, 2006 2:49:30 PM CDT	870ef3dd1c10e5c6:19ee8a:10c7e0883f7:-7ff8	Fatal	dhcp-uaus09-147-76	Logging	ERROR
Monday, July 17, 2006 12:36:59 PM CDT	870ef3dd1c10e5c6:1983ad7:10c7d8ece05:-7ffb	Fatal	dhcp-uaus09-147-76	Logging	ERROR
Thursday, July 20, 2006 12:20:46 PM CDT	2fe1c4f202a318cd:15ad36d:10c8c6040be:-7fc0	Fatal	dhcp-uaus09-147-110	Logging	ERROR
Thursday, July 20, 2006 9:43:14 AM CDT	2fe1c4f202a318cd:15ad36d:10c8c6040be:-7fdd	Fatal	dhcp-uaus09-147-110	Logging	ERROR

A. 242
B. 312
C. 416
D. 514

Correct Answer: D

QUESTION 43

This attack uses social engineering techniques to trick users into accessing a fake Web site and divulging personal information. Attackers send a legitimate-looking e-mail asking users to update their information on the company's Web site, but the URLs in the e-mail actually point to a false Web site.

A. Wiresharp attack
B. Switch and bait attack
C. Phishing attack
D. Man-in-the-Middle attack

Correct Answer: C

QUESTION 44

Which of the following statements would NOT be a proper definition for a Trojan Horse?

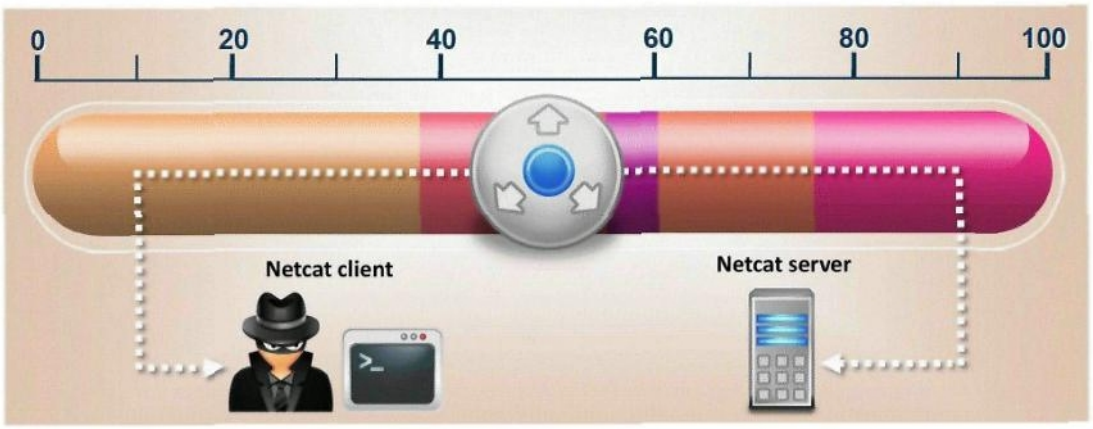
A. An authorized program that has been designed to capture keyboard keystroke while the user is unaware of such activity being performed.
B. An unauthorized program contained within a legitimate program. This unauthorized program performs functions unknown (and probably unwanted) by the user.
C. A legitimate program that has been altered by the placement of unauthorized code within it; this code performs functions unknown (and probably unwanted) by the user.
D. Any program that appears to perform a desirable and necessary function but that (because of unauthorized code within it that is unknown to the user) performs functions unknown

(and definitely unwanted) by the user.

Correct Answer: A

QUESTION 45

What is the correct command to run Netcat on a server using port 56 that spawns command shell when connected?



A. nc -port 56 -s cmd.exe
B. nc -p 56 -p -e shell.exe
C. nc -r 56 -c cmd.exe
D. nc -L 56 -t -e cmd.exe

Correct Answer: D

QUESTION 46

SNMP is a connectionless protocol that uses UDP instead of TCP packets (True or False)

A. true
B. false

Correct Answer: A

QUESTION 47

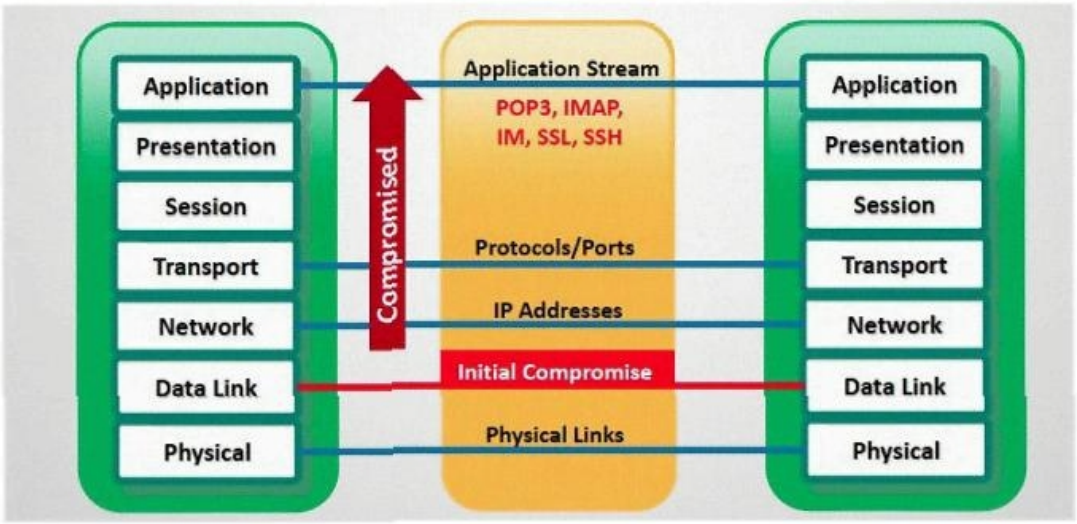
TCP/IP Session Hijacking is carried out in which OSI layer?

A. Data link layer
B. Transport layer

C. Network layer
D. Physical layer

Correct Answer: B

QUESTION 48
In which part of OSI layer, ARP Poisoning occurs?



A. Transport Layer
B. Data link Layer
C. Physical Layer
D. Application layer

Correct Answer: B
QUESTION 49
You want to hide a secret.txt document inside c:\windows\system32\tcpip.dll kernel library using ADS streams. How will you accomplish this?

A. copy secret.txt c:\windows\system32\tcpip.dll kernel>secret.txt
B. copy secret.txt c:\windows\system32\tcpip.dll:secret.txt
C. copy secret.txt c:\windows\system32\tcpip.dll |secret.txt
D. copy secret.txt >< c:\windows\system32\tcpip.dll kernel secret.txt

Correct Answer: B

QUESTION 50
You just purchased the latest DELL computer, which comes pre-installed with Windows 7,

McAfee antivirus software and a host of other applications. You want to connect Ethernet wire to your cable modem and start using the computer immediately. Windows is dangerously insecure when unpacked from the box, and there are a few things that you must do before you use it.

A. New installation of Windows should be patched by installing the latest service packs and hotfixes.
B. Key applications such as Adobe Acrobat, Macromedia Flash, Java, Winzip etc., must have the latest security patches installed.
C. Install a personal firewall and lock down unused ports from connecting to your computer.
D. Install the latest signatures for Antivirus software.
E. Configure "Windows Update" to automatic.
F. Create a non-admin user with a complex password and logon to this account.
G. You can start using your computer as vendors such as DELL, HP and IBM would have already installed the latest service packs.

Correct Answer: ACDEF

QUESTION 51
In the context of Trojans, what is the definition of a Wrapper?

A. An encryption tool to protect the Trojan.
B. A tool used to bind the Trojan with a legitimate file.
C. A tool used to calculate bandwidth and CPU cycles wasted by the Trojan.
D. A tool used to encapsulate packets within a new header and footer.

Correct Answer: B

QUESTION 52
Your computer is infected by E-mail tracking and spying Trojan. This Trojan infects the computer with a single file - emos.sys. Which step would you perform to detect this type of Trojan?