Date:

Module Name: Network Defense and Countermeasures (NDC)

Q.1) Network layer firewall works as a -

A: Frame Filter
B: Packet Filter
C: Both A and B
C: None of the mentioned

Q.2) One advantage of setting up Dual Firewall DMZ (DMZ with two firewalls) -

A: You can control where traffic goes in the three networks
B: You can do stateful packet filtering
C: You can do load balancing
D: Improved network performance

Q.3) Which of the following is the most important security aspect of using Network Address Translation (NAT)?

A: It unites network nodes logically into the same broadcast domain
B: It hides the internal network from the outside world
C: It allows users to be grouped by department rather than location
D: It allows external users to access necessary information

Q.4) Which of the following are true about firewalls ?

A: It can be either a hardware or software device
B: Monitors incoming and outgoing traffic
C: Follows a set of rules
D: All of the above

Q.5) A packet filtering firewall operates at -

A: Network Layer
B: Network and Transport Layer
C: Transport Layer
D: Transport and Application Layer

Q.6) Which of the following firewalls keeps track of the connection state?

A: Application layer firewall
B: Packet filtering firewall
C: Router enhanced firewall
D: Stateful packet filtering firewall

Q.7) Which firewall inspects packets at deeper level -

A: Static packet filtering firewall
B: Stateful packet filtering firewall
C: Gateway/Proxy firewall
D: Both B and C

Q.8) Which of the following, best describes the difference between an intrusion detection system and a firewall?

A: IDSs control the information coming in and out of the network, whereas firewalls actually prevent attacks
B: Firewalls control the information coming in and out of the network, whereas IDSs identify unauthorized activity
C: Firewalls control the information coming in and out of the network, whereas IDSs actually prevent attacks
D: IDSs control the information coming in and out of the network, whereas firewalls identify unauthorized activity

Q.9) Which of the following is true about circuit-level firewall?

A: Operates at the transport layer of OSI model
B: It monitors TCP/UDP sessions
C: Both A and B
D: None

Q.10) Which of the following are examples of a bastion host ?

A: Web Server
B: DNS Server
C: Proxy Server
D: All of the above

Q.11) Which of the following best describes a demilitarized zone (DMZ) ?

A: A small network between the database servers and file servers
B: A small network between the internal network and the Internet
C: A portion of the internal network that uses web-based technologies
D: A portion of the internal infrastructure used in business-to-business relationships

Q.12) Which of the following are advantages of using NAT?

1. Translation introduces switching path delays.
2. Conserves legally registered addresses.
3. Causes loss of end-to-end IP traceability.

4. Increases flexibility when connecting to the Internet.
5. Certain applications will not function with NAT enabled.
6. Reduces address overlap occurrence.

A: 1, 3 and 4 B: 3, 5 and 6 C: 5 and 6 D: 2, 4 and 6

Q.13) Which of the followings are main features of Iptables -

1. Stateless packet filtering (IPv4 and Ipv6)
2. Stateful packet filtering (IPv4 and Ipv6)
3. Network address and port translation (NAT/NAPT)
4. Maintains three tables (Mangle, Filter & NAT)

A: 1, 3 and 4 B: 2, 3 and 4 C: Only 2 and 4 D: All of the above

Q.14) Built-in chains in NAT tables -

A: Prerouting, Postrouting and Input
B: Prerouting, Postrouting and Output
C: Prerouting, Postrouting and Forward
D: Prerouting, Postrouting, Input, Output and Forward

Q.15) Which is the default table in iptables command -

A: NAT Table
B: Filter Table
C: Mangle Table
D: None

Q.16) The default snap length in tcpdump(built with IPv4) is_____ (in bytes).

A: 56
B: 68
C: 128
D: 32

Q.17) Which of following is not a protocol field of snort rule header

A: TCP
B: ICMP
C: UDP
D: HTTP

Q.18) Which of the following cannot be used as an IDS Sensor?

A: Windump
B: TCPDump
C: Libpcap
D: Nmap

Q.19) The _____ can be defined as sophisticated class of network security implementation that not only has the ability to detect the presence of intruders and their actions, but also to prevent them from successfully launching any attack.

A: Firewall
B: IPS
C: VPN
D: IDS

Q.20) The _____ mode is the configuration of a network card wherein a setting is enabled so that the card passes all traffic it receives to the CPU rather than just packets addressed to it.

A: Binary
B: ASCII
C: Promiscuous
D: PIF

Q.21) In IDS, the _____ are considered to be the first point of intrusion detection.

A: Analyzer
B: Agents
C: Sensors
D: Managers

Q.22) Which one is not the functionalities of UTM.

A: Content Filtering
B: Network bandwidth management
C: Network Link management
D: Spyware filtering

Q.23) What are the two main types of intrusion detection systems?

A: Signature-based and event-based
B: Network-based and host-based
C: Active and reactive
D: Intelligent and passive

Q.24) The command for capturing 10 http requests

A: tcpdump -i en1 -c 10 dst port 80
B: tcpdump -i en1 -p 10 dst port 80
C: tcpdump -i en1 -c 10 src port 80
D: tcpdump -i en1 -p 10 dst port 80

Q.25) You are running Snort in your network to capture network traffic. Based on the following capture, what type of traffic is captured?

04/17-08:47:35.481575 0:A0:CC:58:CC:BF -> 0:80:5F:26:5A:21 type:0x800 len:0x3E
192.168.0.204:4654 -> 192.168.0.1:443 TCP TTL:128 TOS:0x0 ID:27146 I pLen:20 DgmLen:48
******S* Seq: 0x52B6718E Ack: 0x0 Win: 0x4000 TcpLen: 28
TCP Options (4) => MSS: 1460 NOP NOP SackOK

A: A secure Web server response
B: A secure Web server request
C: An unsecured Web server response
D: An unsecured Web server request

Q.26) An IDS may be configured to report attack occurrences. You just received a notification that an attack occurred, but after checking, you find that it really wasn't an attack at all. What is the term for this type of alarm?

A: True positive
B: False positive
C: True negative
D: False negative

Q.27) What tool would you use to monitor for intrusions by reviewing computer system and event logs on a client computer?

A: Network-based
B: client-based
C: Honeypot
D: Host-based

Q.28) In IDS/IPS, anomalies are also referred to as _____, surprise, aberrant, deviation, peculiarity, etc.

A: Outliers
B: Normal distribution
C: Mean
D: Box plot

Q.29) Anomaly detection technique based on:

A: Signature sets
B: Packet analysis
C: Deviated data
D: Training data

Q.30) Which of the following is not a packet capture library?

A: libpcap
B: libpcre

C: libipq
D: libnetfilter_queue

Q.31) Which of following mode the snort engine can be run?

A: sniffer
B: packet logging
C: network-intrusion detection
D: All of these

Q.32) Which one is not an example of UTM.

A: Untangle
B: sonicwall
C: checkpoint
D: tripwire

Q.33) Which of the following function in libpcap is used to determine the IPv4 network number and mask associated with the network device

A: pcap_ipaddress
B: pcap_lookupnet
C: pcap_lookupdev
D: pcap_loop

Q.34) Your network administrator has installed a network-based IDS and a honey pot on the network. What is the written plan called that indicates who will monitor these tools and how users should react once a malicious attack has occurred?

A: Active response
B: Incident response
C: Monitoring and response
D: Security alert and response

Q.35) drop icmp $EXTERNAL_NET any -> $HOME_NET any (msg: icmp attack; content: !"virus"; sid:45764;)
the above signature block which of the following traffic.

A: Block all the ICMP traffic in the network
B: Block all the ICMP traffic coming from external network to internal network having payload contain "virus"
C: Block all the ICMP traffic coming from external network to internal network.
D: Block all the ICMP traffic coming from external network to internal network and packet payload that does not contain "virus".

Q.36) Which of the following is not HTTP method.

A: HEAD

B: TAIL
C: CONNECT
D: GET

Q.37) The ____ option of Tcpdump is used to print the link-layer header.

A: –S
B: –nn
C: -e
D: –X

Q.38) Which of the following is the action field of snort rule header.

A: tear
B: drop
C: disconnect
D: none of these

Q.39) Virtual private networks have one thing in common: They all share the same core set of technologies. Which of the following choices best describes that core set of technologies?

A: Tunneling and encryption
B: Tunneling, encryption, and authentication
C: Tunneling, encryption, and access control
D: Tunneling, encryption, authentication, and access control

Q.40) Which statement is true of IPSec transport mode?

A: The entire IP datagram is left intact.
B: Only the IP headers are encrypted, and the original IP payload is left intact.
C: Only the IP payload is encrypted, and the original IP headers are left intact.
D: The entire original IP datagram is encrypted, and it becomes the payload in a new IP packet.