Date:

Module Name: Network Defense and Countermeasures (NDC)

Q.1) How many predefined chains are in “raw” table?

A: 3
B: 5
C: 4
D: 2

Q.2) “mangle” table is used for?

A: Packet Forwarding
B: To alter QOS bits in TCP Header
C: Masquerading
D: None of the above

Q.3) What is the default policy of a user defined chain in any table?

A: DROP
B: ACCEPT
C: Reject
D: No default policy

Q.4) How to rename a user defined chain?

A: Iptables –E <old_name> <new_name>
B: Iptables –R <old_name> <new_name>
C: Iptables –S <old_name> <new_name>
D: It’s not possible to rename a user defined chain

Q.5) How the MAC module is used in iptables?

A: –m mac –mac-address xx : xx : xx : xx : xx : xx
B: –m mac –mac-addr xx : xx : xx : xx : xx: xx
C: –m mac –mac-destination xx : xx : xx : xx : xx : xx
D: –m mac –mac-source xx : xx : xx : xx : xx : xx

Q.6) Packet filter firewall work up to which layer?

A: Transport layer (Layer 4)
B: Network layer (Layer 3)
C: Application layer (Layer 5)
D: Data Link layer (Layer 2)

Q.7) Iptables is a

A: Host based firewall

B: Network firewall
C: Both a) and b)
D: None of the a) and b)

Q.8) Which type of firewall can restrict spread of computer worms and Trojans?
A: Application layer firewall
B: Packet filter firewall
C: Stateful firewall
D: NAT firewall

Q.9) Which of the following rule is syntactically incorrect?
A: Iptables –A INPUT –j LOG
B: Iptables –A INPUT –sport 80 –j DROP
C: Iptables –A INPUT –p tcp –sport 80 –j DROP
D: Iptables –A OUTPUT –p tcp –sport 70 –j DROP

Q.10) "Iptables –F " What does this command will do? Choose the most appropriate answer.
A: Flush all the rules in all chains of all tables
B: Flush all the rules of all INPUT chains of all tables
C: Flush all the rules of all OUTPUT chains of all tables
D: Flush all the rules of all chains of filter table

Q.11) If one wants to block all the traffic routed through his system, in which table he should put the rule?
A: PREROUTING
B: POSTROUTING
C: INPUT
D: FORWARD

Q.12) What tells a firewall how to reassemble a data stream that has been divided into packets?
A: The header checksum field in the packet header
B: The destination IP address
C: The number in header's identification field
D: None of the above

Q.13) What is the most effective security approach for a stateless packet filter?
A: Deny all except specified hosts
B: Allow all except specified hosts
C: Allow access to only specified destination servers

D: Deny access to all destination except specified servers

Q.14) The practice of designing operational aspects of a system to work with a minimal amount of system privilege is called?

A: Access denied
B: Least privilege
C: Failover firewall
D: IP Forwarding

Q.15) A stateful firewall maintains a ________, which is a list of active connections.

A: Routing table
B: State table
C: Connection table
D: Bridging table

Q.16) Which one is not the functionalities of UTM.

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

Q.17) Which one is an example of UTM.

A: Untangle
B: sonicwall
C: checkpoint
D: All of These

Q.18) What is a false negative?

A: Results when an attack or an intrusion goes undetected
B: An alert sent to an incorrect management station
C: Results when the IDS system reports an alarm, although an actual intrusion doesn’t occur on the network
D: There is no such thing as a false negative

Q.19) Known vulnerabilities in a application / software are identified by

A: CVE ID (Common Vulnerabilities and Exposure)
B: Common Vulnerability Scoring System (CVSS)
C: Exploitable Score
D: None of these above

Q.20) A _____ will monitor network traffic and compare it against an established baseline.

A: Host-based IDS
B: Signature-based IDS
C: Anomaly-based IDS
D: Network-based IDS

Q.21) Print or capture only PSH+ACK packet coming at your interface using tcpdump:

A: tcpdump 'tcp[13]=18'
B: tcpdump 'tcp[13]=16'
C: tcpdump 'tcp[13]=24'
D: tcpdump 'tcp[13]=8'

Q.22) Which of the following describes a passive, host-based IDS?

A: Runs on the local system
B: Does not interact with the traffic around it
C: Can look at system event and error logs
D: All of the above

Q.23) You are running Snort in your network to capture network traffic. Based on the following capture, what type of traffic was 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 IpLen: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.24) Which of the following keyword is not the part of snort rule header

A: Protocol
B: Content
C: Port
D: Direction Operator

Q.25) Command to capture all udp packets with destination port 53 and write it to dump.pcap is

A: tcpdump -p udp and dst port 53 -w dump.pcap
B: tcpdump -p udp and port 53 -r dump.pcap
C: tcpdump protocol udp and 53 -w dump.pcap
D: none of these

Q.26) 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.27) 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.28) What is an IPS signature?
A: A message digest encrypted with the sender's private key
B: A set of rules used to detect typical intrusive activity
C: A binary pattern specific to a virus
D: An appliance that provides anti-x services

Q.29) Which of the following is important for organizations looking to implement IDS or IPS?
A: Willingness of the organization to invest in the overall technology, including training and maintenance
B: Creation of written policies outlining the objectives of the IDS or IPS
C: Identification of critical assets and resources
D: All of the above

Q.30) Whichof the following is an advantage of anomaly detection?
A: Rules are easy to define.
B: Custom protocols can be easily analyzed.
C: The engine can scale as the rule set grows.
D: Malicious activity that falls within normal usage patterns is detected.

Q.31) The mechanism in TCP/IP used to track which fragments belong to a given stream is ____
A: Fragment Offset
B: Fragment flag bit
C: Fragment Identification

D: Fragment Option

Q.32) Given a packet that contains the string “silkworm” detected in a telnet data stream and the following two rules:

alert tcp any any -> any 23 (msg:”Silk1”; content:”silk”;)

alert tcp any any -> any any (msg:”Silk2”; content:”silkworm”;)

Which rule contains the most specific content item and would be selected first if the detection engine had to decide which one to alert on?

A: Silk1
B: Silk2
C: They would alert concurrently
D: There is no match

Q.33) A buffer overflow attack can result in which of the following outcomes?

A: Elevated privileges on the target host
B: Denial of service on the target host
C: Both A & B
D: Neither A or B

Q.34) It is important to understand the affect/impact of networking devices in order to have a successful IDS/IPS deployment. Which of the following is NOT true about network devices:

A: Switches only present a datagram to a port for which it is destined
B: Hubs only present a datagram to a port for which it is destined
C: Routers forward datagrams based on the destination IP address
D: Taps replicate data right off the wire

Q.35) There are four primary components of Snort. Which of the following is NOT one of them:

A: Sniffer
B: Postprocessors
C: Detection engine
D: Output module

Q.36) Running Snort from the command line gives you the ability to read PCAP formatted files. Which of the items below does NOT correctly represent how you could read PCAPs in from the command line?

A: --pcap-file=<file>
B: --pcap-xml=<XML file>
C: --pcap-list=<list>
D: --pcap-dir=<directory>

Q.37) What are the two main types of intrusion detection systems based on detection methodology ?

A: Protocol-based and host-based
B: Misuse and Anomaly
C: Active and reactive
D: Intelligent and passive

Q.38) Which of the following is HTTP method.

A: CONNECT
B: METHOD
C: TAIL
D: 200 OK

Q.39) Which of the following choices best describes what an IPSec VPN generally consists of?

A: An agreement between two parties
B: A secure, private tunnel between a remote endpoint and a gateway
C: A secure, private tunnel between two companies
D: Routers and remote clients

Q.40) _________ is a collection of protocols designed by the IETF (Internet Engineering Task Force) to provide security for a packet at the network level.

A: IPSec
B: SSL
C: PGP
D: None of the above