Module Name-1 : (60 Minutes)

Q1. When discussing IDS / IPS, what is a signature?

a. An electronic signature used to authenticate the identity of a user on the network.

b.Attack-definitionfile8

c. It refers to "normal," baseline network behaviour

d. None of the above

Q2. 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

Q3. ______ is placed at a strategic point or points within the network to monitor traffic to and from all devices on the network.

a. HIDS

b. Anomaly-based IDS

c. Passive IDS

d. NIDS

Q4. 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

Q5. What is the length of TTL field of IP header (in bits)

a. 4

b. 8

c. 6

d. 13

Q6. What is the total length of TCP header in bytes

a. 16

b. 20

c. 40

d. 60

Q7. 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

Q8. Which of the following is not a capability of network-based IDS?
a. Can detect denial-of-service attacks

b. Can decrypt and read encrypted traffic

c. Can decode UDP and TCP packets

d. Can be tuned to a particular network environment

Q9. alert tcp $EXTERNAL_NET any -> 192.168.1.0/24 111 (msg: "mountd access"; content: "|00 01|"; sid:1000001;)
The above signature / rules applies to the which traffic (movement of packet)

a. External Network to Home Network

b. External Network to External Network

c. Home Network to External Network

d. Home Network to Home Network

Q10. Which of following is not the rule action type of snort rule
a. alert

b. log

c. drop

d. direction

Q11. 18:52:08.730624 24.147.188.237.4797 > my.host.26.224.3879:S 546052661:546052661(0) win 32120 <mss 1460,sackOK,timestamp 59927143 0,nop,wscale 0> (DF) (ttl 48, id 63341)

```
18:52:08.730691      my.host.26.224.3879      >
24.147.188.237.4797: R 0:0(0) ack 546052662
win 0 (ttl 255, id 784)
```

The above tcpdump output indicates:

a. The target host does not exist
b. The target host rejected ACK number 546052662
c. The target host does not have a service running on port 3879
d. The target host does not have a service running on port 4797

Q12. The _____ option of Tcpdump is used to print the link-layer header.

a. –S

b. –nn

c. -e

d. –X

Q13. Write the command to capture only 500 packets from dump. pcap using tcpdump.

a. tcpdump -n 500

b.tcpdump -c 500

c.tcpdump -n 500 dump.pcap

d. tcpdump -c 500 dump.pcap

Q14. Print or capture only SYN-ACK packet coming at your interface using tcpdump:

a. tcpdump 'tcp[13]=18'

b. tcpdump 'tcp[13]=16'

c. tcpdump 'tcp[13]=2'

d. tcpdump 'tcp[13]=8'

Q15. tcpdump is used for capturing packet of layer:

a. application layer

b. network layer

c. physical layer

d. transport layer

Q16. Which of the following is true for anomaly-based IDS?
a. They alert administrators about the deviations from "normal" traffic behavior.
b. The technology is mature and reliable enough to use on production networks.
c. They scan network traffic or packets to identify matches with attack-definition files.
d. None of the above..

Q17. In IDS/IPS, anomalies are also referred to as __________, surprise, aberrant, deviation, peculiarity, etc.

a.Outliers

b. Normal distribution

c. Mean

d. Box plot

Q18. Anomaly detection technique based on:

a. Signature sets

b. Training data

c. Packet analysis

d. Deviated data

Q19. Which of the following best describes an attack that alter the content of two critical files?

a. Integrity

b. Confidentiality

c. Availability

d. Authentication

Q20.------------------is the business impact and the probability of that vulnerability being exploited.

a. Threat

b. Vulnerability

c. Exploit

4. Risk

Q21. How many built-in tables are in iptables

a. two

b. three

c. four

d .five

Q22. Which of the following structure is correct in IP tables?

a. Rules -> Chains -> Tables
b.Chains -> Tables -> Rules
c. Tables -> Chains -> Rules
d. None of the above

Q23. Which one is not a target in iptables ?

a. ACCEPT

b. DROP

c. FILTER

d. RETURN

Q24. How many chains are there in mangle table

a. two

b. three

c. four

d. five

Q25. For bandwidth management using iptable, which module is used ?
a. limit

b. quota

c. bandwidth

d. None of the above

Q26. In iptables, the __________ table is responsible for the alteration of quality of service bits in the TCP header

a.FILTER

b.NAT

c.MANGLE

d.RAW

Q27. In a ___________, the destination IP address is maintained and the source IP address is changed.

a.DNAT

b.SNAT

c.Switching

d.Bridging

Q28. Using which command ,we can change default iptables policy ?

a. iptables -X DROP

b. iptables -P DROP

c. iptables -D DROP

d. All of the above

Q29. Which command is used to save iptables rule

a. iptables-store

b. save-iptables

c. iptables-save

d.iptables-submit

Q30. Which among the following is not a functionality of UTM.

a. Content Filtering

b. Network bandwidth management

c. Network Link management

d. Spyware filtering

Q31. Which one is not an example of UTM.

a. Untangle

b. sonicwall

c. checkpoint

d. tripwire

Q32. Honeypots are used to:

a. Attract attackers by simulating systems with open network services

b. Monitor network usage by employees

c. Process alarms from other IDSs

d. Attract customers to e-commerce sites

Q33. At which two traffic layers do IDSes generate signatures?

a. Application layer

b. Network layer & Transport layer

c. Session layer & application layer

d. Transport layer & application layer

Q34. -------------------- firewalls are also known as first generation firewalls.

a. Packet filtering

b. Application layer filtering

c. Session layer

d. Border

Q35. Which of the following is an IPsec protocol

a. SSH

b. TLS

c. AH

d. SFTP

Q36. Which of the following is an IPsec mode?

a.Encryption mode

b. Encapsulation mode

c. Tunnel mode

d. Cyclic chaining mode

Q37. Which of the following is a requirement for a trusted VPN?

a. No one other than the trusted VPN provider can affectthe creation or modification of apath in the VPN

b. No on eother than the trusted VPN provider can change the data, inject data,or delete data on a path in the VPN.

c. The routing and addressing used in a trusted VPN must be established before the VPN is created.

d. All of the above

Q38. -------------------is a system that has been hardened to resist attack, and which is installed on a network in such a way that it is expected to potentially come under attack.

a. Bastian host

b. Proxy

c. Gateway

d. Firewall

Q39. In tunnel mode............................

a. Only the payload of the packet is encrypted
b. Entire packet is encrypted
c. Payload is never encrypted
d. None of the above

Q40. -------------------is not an access attack

a. Snooping
b. Eavesdropping
c. DoS
d. Non repudiation

Q41. Which of the following can not be used as an IDS sensor?

a.Windump
b.TCPdump
c.Libpcap
d. Nmap

Q42. A false positive can be defined as

a) an alert that indicates nefarious activity on a system that, upon further inspection, turns out to represent legitimate network traffic or behavior.
b) an alert that indicates nefarious activity on a system that is not running on the network.
c) the lack of an alert for nefarious activity.
d) Both a and b

Q43. The protocol identifier number assigned to ICMP in the standard IP packet is

a. 1
b. 17

c. 8
d. 23

Q44. Which of the following is not a capability of network-based IDS?
a. Can detect denial-of-service attacks

b. Can decrypt and read encrypted traffic

c. Can decode UDP and TCP packets

d. Can be tuned to a particular network environment

Q45. 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

Q46. What is the default MTU size in 802.3 Ethernet

a. 1500

b.2000

c. 65535

d. 3000

Q47. Assault on system security that derives from an intelligent threat is

a. Exploit
b. Attack
c.ToE
d. Vulnerability

Q48. What is the total length of UDP header in bytes

a. 16

b. 20

c. 8

d. 12

Q49. 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

Q50. alert tcp $EXTERNAL_NET any -> 192.168.1.0/24 111 (msg: “mountd access”; content: “|00 01|”; sid:1000001;)
In the above signature / rules content field is a

a. Hexadecimal string

b. String

c. Digit

d. None of the above

Q51. Which of following is not a protocol field of snort rule header

a. TCP

b. ICMP

c. UDP

d. HTTP

Q52. Command to capture all udp packets with destination port 53 and write it to dump.pcap is

a) tcpdump udp and dst port 53 -w dump.pcap

b) tcpdump udp and port 53 -r dump.pcap

c) tcpdump protocol udp and 53 -w dump.pcap

d) none of these

Q53. The _____ option of Tcpdump is used to print the link-layer header.

a. –S

b. –nn

c. -e

d. –X

Q54. Print or capture only SYN packet coming at your interface using tcpdump:

a. tcpdump 'tcp[13]=18'

b. tcpdump 'tcp[13]=16'

c. tcpdump 'tcp[13]=2'

d. tcpdump 'tcp[13]=8'

Q55. tcpdump -tt :

a) prints the time in unformatted timestamp in dump line.

b) does print the time in dump line

c) Print a timestamp in default format proceeded by date on each dump line

d) Print a delta (micro-second resolution) between current and previous line on each dump line

Q56. Anomaly detection is applicable in a variety of domains, such as intrusion detection, __________, fault detection, system health monitoring, event detection in sensor networks, and detecting eco-system disturbances

a. tort

b. fraud

c. negligence

d. neutral reportage

Q57. Which security control is a consequence of nonmalicious activity generally representing an error?

a. true positive

b.false positive

c.true negative

d. false negative

Q58. Which of the following is true for anomaly-based IDS?
a. They alert administrators about the deviations from "normal" traffic behavior.
b. The technology is mature and reliable enough to use on production networks.
c. They scan network traffic or packets to identify matches with attack-definition files.
d. None of the above..

Q59. On a VPN, traffic is encrypted and decrypted at:

a. End points of the tunnel only

b. User's machines

c. Each device at each hop

d. The data link layer of access devices

Q60. Which of the following best describes an attack that alter the content of two critical files?

a. Integrity

b. Confidentiality

c. Availability

d. Authentication

Q61. IPsec provides which options as security services?

a. ESP and AH

b.ESP and AP

c.EA and AH

d.EA and AP

Q62. Which of the following is an IPsec mode?

a. Encryption mode

b. Encapsulation mode

c. Transport mode

d. Cyclic chaining mode

Q63. How many built-in tables are in iptables

a. two

b. three

c. four

d .five

Q64. Which one is not a target in iptables ?

a. ACCEPT

b. DROP

c. FILTER

d. RETURN

Q65. How many chains are there in NAT table

a. two

b. three

c.four
d. five

Q66. In iptables, the __________ table is responsible for the alteration of quality of service bits in the TCP header

a.FILTER

b.NAT

c.MANGLE

d.RAW

Q67. In a ___________, the source IP address is maintained and the destination IP address is changed.

a.DNAT

b.SNAT

c.Switching

d.Bridging

Q68. A ___________ allows a host on the "outside" to connect to a host on the "inside".

a. DNAT

b. SNAT

c. Switching

d. Bridging

Q69. Which command is used to save iptables rule

a. iptables-store

b. save-iptables

c. iptables-save

d.iptables-submit

Q70. Probably the simplest physical attack on the computer system is:

a. Accessing an Ethernet jack to attack the network
b. Using an imitation to fool a biometric authenticator
c. Installing a virus on the CCTV system
d. Outright theft of the computers

Q71. Which among the following is not a functionality of UTM.

a. Spyware filtering

b. Content Filtering

c. Network bandwidth management

d. Network Link management

Q72. What is the three-way handshake sequence used to initiate TCP connections?

a. ACK, SYN/ACK, ACK
b. SYN, SYN/ACK, ACK
c. SYN, SYN, ACK/ACK
d. ACK, SYN/ACK, SYN

Q73. Honeypots are used to:

a. Attract attackers by simulating systems with open network services

b. Monitor network usage by employees

c. Process alarms from other IDSs

d. Attract customers to e-commerce sites

Q74. -------------------- firewalls are also known as first generation firewalls.

a. Packet filtering

b. Application layer filtering

c. Session layer

d. Border

Q75. Application proxy firewalls falls under the category of

a. First generation firewalls

b. Second generation firewalls

c. Third generation firewalls

d. Fourth generation firewalls

Q76. Weakness in a mechanism that can threaten CIA triads of an asset is known asa.

a. Vulnerability

b. Confidentiality

c. Integrity

d. Availability

Q77. Netfilter is a ---------------------------- module

a. user space

b.kernel space

c.Application space

d. link space

Q78. -------------------is not an access attack

a. Snooping
b. Eavesdropping
c. DoS
d. Non repudiation

Q79. Which among the following authentication is the weakest?
a. Token
b. Retina scan
c.Passwords
d. Pass phrase

Q80. Which of the following bit is set ON when the connection is terminated due to the abnormal conditions

a. FIN
b. SYN
c. ACK
d. RST