Date: 20-07-16

Course-end Re-examination

Course Name: PG-DITISS
Module Name: Network Defense and Countermeasures
Time: 9:30-10:30 AM MM-40

Q.No.1) iptables is

A. integrated with the kernel of the operating system
B. integrated with kernel
C. part of the operating system
D. any of the above

Q.No.2) "mangle" table is used for

A. Packet forwarding
B. To alter QOS bit in TCP header
C. Masquerading
D. None

Q.No.3) Which statement(s) is correct for DROP and REJECT target in iptables
I) DROP – Packet is dropped & no information regarding the drop is sent to the sender
II) REJECT – Packet is dropped and information (error) message is sent to the sender

A. I only
B. II only
C. Both
D. None

Q.No.4) FORWARD chain is used in which table(s)

A. filter, mangle
B. nat, filter
C. filter, nat, mangle
D. mangle, raw

Q.No.5) Which statement(s) is correct
I) " iptables -F " with no argument flushes all the chains in the table
II) " iptables -X "with no argument deletes all non-builtin chains in a table

A. I only
B. II only
C. Both
D. None

Course-end Re-examination

Q.No.6) 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.No.7) iptables -A FORWARD-s 192.168.10.0/24-i eth1-p tcp - dport 80-j ACCEPT, what will we get with this sentence?

A. Accepting https ports
B. We accept that from the private IP's on the local network you can reach any web server configured by default.
C. Accepting the ip 192.168.10.0/24 go to ports 80
D. Accepting that the ports will 192.168.10.0/24 ip https

Q.No.8) "-i (–in-interface) <interface>" It is the interface on which packet should arrive. This option is valid only for

A. FORWARD
B. PREROUTING
C. INPUT
D. all of the above

Q.No.9) A _____ blocks all incoming traffic to any host but itself.

A. Proxy Server
B. Packet Filter
C. Circuit Level Gateway
D. Application Gateway

Q.No.10) In order to drop ICMP packets which are arriving on eth0 faster than 1 per second. Which of the following iptables commands is used if default policy for the input chain is ACCEPT.

I) iptables -t filter -A INPUT -i eth0 -p icmp --icmp-type echo-request -m limit --limit 1/second -j DROP
II) iptables -t filter -A INPUT -i eth0 -p icmp --icmp-type echo-request -j ACCEPT
III) iptables -A INPUT -i eth0 -p icmp --icmp-type echo-request -m limit --limit 1/second -j DROP
IV) iptables -A INPUT -i eth0 -p icmp --icmp-type echo-request -j DROP

A. I only
B. I, II
C. III only
D. I, IV

Q.No.11) Traffic in a VPN is NOT...

A. Invisible from public networks.
B. Logically separated from other traffic.
C. Accessible from unauthorized public networks.
D. Restricted to a single protocol in IPSec.

Q.No.12) Which layer of the OSI reference model does PPTP work at?

A. Layer 1
B. Layer 2
C. Layer 3
D. Layer 4

Q.No.13) What are the two modes of IP Security?

A. transport and certificate
B. transport and tunnel
C. certificate and tunnel
D. preshared and transport

Q.No.14) In the _____ mode, IPSec protects the whole IP packet, including the original IP header.

A. transport
B. tunnel
C. either transport or tunnel
D. neither transport nor tunnel

Course-end Re-examination

Q.No.15) SSL provides _____.

a) message integrity
b) confidentiality
c) compression

A. only b and c
B. only a and c
C. a, b and c
D. only a and b

Q.No.16) Which one is an example of UTM?

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

Q.No.17) 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.No.18) 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.No.19) 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

Course-end Re-examination

Q.No.20) 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.No.21) 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.No.22) 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.No.23) Which of the following keyword is not the part of snort rule header

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

Q.No.24) 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

Course-end Re-examination

Q.No.25) 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.No.26) 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.No.27) 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.No.28) 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.No.29) 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.

Course-end Re-examination

Q.No.30) 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.No.31) 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.No.32) 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.No.33) 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.No.34) 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

Course-end Re-examination

Q.No.35) 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.No.36) 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.No.37) Which of the following is HTTP method?

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

Q.No.38) What is the length of 802.3 ethernet CRC

A. 4
B. 6
C. 12
D. 14

Q.No.39) What is the length of TTL field of IP header (in bits)

A. 4
B. 8
C. 6
D. 13

Q.No.40) Which one is not the functionalities of UTM.
A. Content Filtering
B. Network bandwidth management
C. Network Link management
D. Spyware filtering