1. How many predefined chains are in "raw" table?
   a) 3
   b) 5
   c) 4
   d) 2

   ANS: d)

2. "mangle" table is used for?
   a) Packet Forwarding
   b) To alter QOS bits in TCP Header
   c) Masquerading
   d) None of the above

   ANS: b)

3. What is the default policy of a user defined chain in any table?
   a) DROP
   b) ACCEPT
   c) Reject
   d) No default policy

   ANS: d)

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

   ANS: a)

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

   ANS: d)

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)

   ANS: b)

7. Iptables is a
   a) Host based firewall

b) Network firewall
c) Both a) and b)
d) None of the a) and b)

ANS: c)

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

   ANS: a)

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

   ANS: b)

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

    ANS: d)

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

    ANS: d)

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

    ANS: c)

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

ANS: a)

The practice of designing operational aspects of a system to work with a minimal amount of system privilege is called

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

ANS: b)

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

ANS: b)