**Unit 5**

1. Firewalls can be of \_\_\_\_\_\_\_ kinds.  
a) 1  
b) 2  
c) 3  
d) 4

Answer: c  
Explanation: Firewalls are of three kinds – one is the hardware firewalls, another is software firewalls and the other is a combination of both hardware and software.

2. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ is the kind of firewall is connected between the device and the network connecting to internet.  
a) Hardware Firewall  
b) Software Firewall  
c) Stateful Inspection Firewall  
d) Microsoft Firewall

Answer: a  
Explanation: Hardware firewalls are those firewalls that need to be connected as additional hardware between the device through which the internet is coming to the system and the network used for connecting to the internet.

3. \_\_\_\_\_\_\_\_\_ is software that is installed using an internet connection or they come by-default with operating systems.  
a) Hardware Firewall  
b) Software Firewall  
c) Stateful Inspection Firewall  
d) Microsoft Firewall

Answer: b  
Explanation: Software firewalls are those kinds of firewalls that are installed in the system using internet connection as we install normal applications and update them. Some operating system vendors provide default firewalls with their operating systems.

4. Which of the following is not a software firewall?  
a) Windows Firewall  
b) Outpost Firewall Pro  
c) Endian Firewall  
d) Linksys Firewall

Answer: d  
Explanation: Windows Firewall, Outpost Firewall Pro and Endian Firewall are software firewalls that are installed in the system. Linksys firewall is not an example of a software firewall.

5. Firewall examines each \_\_\_\_\_\_\_\_\_\_\_\_ that are entering or leaving the internal network.  
a) emails users  
b) updates  
c) connections  
d) data packets

Answer: d  
Explanation: Firewalls examines each data packets that are entering or leaving the internal network which ultimately prevents unauthorized access.

6. A firewall protects which of the following attacks?  
a) Phishing  
b) Dumpster diving  
c) Denial of Service (DoS)  
d) Shoulder surfing

Answer: c  
Explanation: Firewalls are used to protect the computer network and restricts illicit traffic. Denial of Service (DoS) attack is one such automated attack which a firewall with proper settings and the updated version can resist and stop from getting executed.

7. There are \_\_\_\_\_\_ types of firewall.  
a) 5  
b) 4  
c) 3  
d) 2

Answer: b  
Explanation: There are four types of firewall based on their working and characteristics. These are Packet Filtering Firewalls, Circuit Level Gateway Firewalls, Application level Gateway Firewalls, and Stateful Multilayer Inspection Firewalls.

8. Packet filtering firewalls are deployed on \_\_\_\_\_\_\_\_  
a) routers  
b) switches  
c) hubs  
d) repeaters

Answer: a  
Explanation: Packet filtering firewalls are deployed on routers that help in connecting internal network worldwide via the internet.

9. In the \_\_\_\_\_\_\_\_\_\_\_\_\_\_ layer of OSI model, packet filtering firewalls are implemented.  
a) Application layer  
b) Session layer  
c) Presentation layer  
d) Network layer

Answer: d  
Explanation: In the network layer, which is the third layer of the OSI (Open Systems Interconnection) model, packet filtering firewalls are implemented.

10. The \_\_\_\_\_\_\_\_\_\_ defines the packet filtering firewall rules.  
a) Access Control List  
b) Protocols  
c) Policies  
d) Ports

Answer: a  
Explanation: The Access Control List is a table containing rules that instruct the firewall system to provide the right access. It checks all the packets and scans them against the defined rule set by Network administrator in the packet filtering firewall.

11. ACL stands for \_\_\_\_\_\_\_\_\_\_\_\_\_  
a) Access Condition List  
b) Anti-Control List  
c) Access Control Logs  
d) Access Control List

Answer: d  
Explanation: The Access Control List is a table containing to check all the packets and scans them against the defined rule set by Network administrator in any particular system or firewall.

12. When a packet does not fulfil the ACL criteria, the packet is \_\_\_\_\_\_\_\_\_  
a) resend  
b) dropped  
c) destroyed  
d) acknowledged as received

Answer: b  
Explanation: In the packet filtering firewall, when the rules defined by the Access Control List is not meet by any data packet, the packet is dropped & logs are updated in the firewall.

13. Network administrators can create their own ACL rules based on \_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_ and \_\_\_\_\_\_\_  
a) Address, Protocols and Packet attributes  
b) Address, Protocols and security policies  
c) Address, policies and Packet attributes  
d) Network topology, Protocols and data packets

Answer: a  
Explanation: Network administrators can create their own ACL rules based on Address, Protocols and Packet attributes. This is generally done where the specific customised type of data packets need to pass through firewall screening.

14. One advantage of Packet Filtering firewall is \_\_\_\_\_\_\_\_\_\_  
a) more efficient  
b) less complex  
c) less costly  
d) very fast

Answer: c  
Explanation: Packet filtering firewalls are more advantageous because they are less costly and they use fewer resources and are used effectively in small networks.

15. Packet filtering firewalls work effectively in \_\_\_\_\_\_\_\_\_ networks.  
a) very simple  
b) smaller  
c) large  
d) very large complex

Answer: b  
Explanation: Packet Filtering Firewalls are applied within routers which connect the internal Network system with the outside network using the internet. It works effectively if the internal network is smaller in size.

16. Packet filtering firewalls are vulnerable to \_\_\_\_\_\_\_\_\_\_  
a) hardware vulnerabilities  
b) MiTM  
c) phishing  
d) spoofing

Answer: d  
Explanation: One popular disadvantage of the packet filtering technique is that it cannot support the complex models of rules and is spoofing attack-prone in some cases as well.

17. Circuit-level gateway firewalls are installed in \_\_\_\_\_\_\_ layer of OSI model.  
a) Application layer  
b) Session layer  
c) Presentation layer  
d) Network layer

Answer: b  
Explanation: In the session layer (which is the fifth layer) of the OSI model, circuit-level gateway firewalls are deployed for monitoring TCP sessions for 3-way handshakes.

18. Which of these comes under the advantage of Circuit-level gateway firewalls?  
a) They maintain anonymity and also inexpensive  
b) They are light-weight  
c) They’re expensive yet efficient  
d) They preserve IP address privacy yet expensive

Answer: a  
Explanation: For a private network, or for organizations, circuit-level gateway firewalls maintain anonymity. They’re also inexpensive as compared to other firewall types.

19. Which of the following is a disadvantage of Circuit-level gateway firewalls?  
a) They’re expensive  
b) They’re complex in architecture  
c) They do not filter individual packets  
d) They’re complex to setup

Answer: c  
Explanation: Circuit-level gateway firewalls don’t filter packets individually which gives the attacker a chance to take access in the network.

20. \_\_\_\_\_\_\_\_\_\_\_\_\_ gateway firewalls are deployed in application-layer of OSI model.  
a) Packet Filtering Firewalls  
b) Circuit Level Gateway Firewalls  
c) Application-level Gateway Firewalls  
d) Stateful Multilayer Inspection Firewalls

Answer: c  
Explanation: Application level Gateway Firewalls are deployed in the application-layer of OSI model for protecting the network for different protocols of the application layer.

21. Application level gateway firewalls protect the network for specific \_\_\_\_\_\_\_\_\_\_\_\_\_  
a) application layer protocol  
b) session layer protocol  
c) botnet attacks  
d) network layer protocol

Answer: a  
Explanation: Some specific application layer protocols need protection from attacks which is done by the application level gateway firewall in the application layer of the OSI model.

22. Application level gateway firewalls are also used for configuring cache-servers.  
a) True  
b) False

Answer: a  
Explanation: As caching servers, the application level gateway firewalls are configured that helps in increasing the network performance making it smooth for logging traffic.

23. Packet filtering firewalls are also called \_\_\_\_\_\_\_\_\_\_\_\_  
a) first generation firewalls  
b) second generation firewalls  
c) third generation firewalls  
d) fourth generation firewalls

Answer: a  
Explanation: Packet filtering firewalls are also called the first generation firewalls. It came into the picture around the 1980s. Packet filtering technique cannot support the complex models of rules and is spoofing attack-prone in some cases as well.

24. Application layer firewalls are also called \_\_\_\_\_\_\_\_\_\_\_\_  
a) first generation firewalls  
b) second generation firewalls  
c) third generation firewalls  
d) fourth generation firewalls

Answer: c  
Explanation: Application layer firewalls are also called third generation firewalls. They came into the picture in around 1995-1998. Application level gateway firewalls are helped in making the network performance smooth for logging traffic.

**Intrusion Detection System**

1.What are drawbacks of the host based IDS ?

A.)    Unselective logging of messages may increase the audit burdens

   B.) Selective logging runs the risk of missed attacks

   C.) They are very fast to detect

D.)      They have to be programmed for new patterns

Answer: Option 'A'

Unselective logging of messages may increase the audit burdens

2.What are the different ways to classify an IDS ?

A.)       anomaly detection

B.)       signature based misuse

   C.) stack based

   D.) all of the mentioned

Show Answer

3. What are strengths of the host based IDS?

   A.) Attack verification

   B.) System specific activity

   C.) No additional hardware required

D.)       All of the mentioned

Answer: Option 'D'

All of the mentioned

4. What are strengths of Network based IDS?

   A.) Cost of ownership reduced

   B.) Malicious intent detection

   C.) Real time detection and response

   D.) All of the mentioned

5.What are characteristics of stack based IDS ?

   A.) They are integrated closely with the TCP/IP stack and watch packets

   B.) The host operating system logs in the audit information

   C.) It is programmed to interpret a certain series of packets

   D.) It models the normal usage of network as a noise characterization

6. What are drawbacks of signature based IDS ?

   A.) They are unable to detect novel attacks

   B.) They suffer from false alarms

   C.) They have to be programmed again for every new pattern to be detected

   D.) All of the mentioned

7. What are the different ways to intrude?

   A.) Buffer overflows

   B.) Unexpected combinations and unhandled input

   C.) Race conditions

D.)      All of the mentioned

Answer: Option 'D'

8.What is major drawback of anomaly detection IDS ?

   A.) These are very slow at detection

   B.) It generates many false alarms

   C.) It doesn’t detect novel attacks

   D.) None of the mentioned

9.What are major components of intrusion detection system?

   A.) Analysis Engine

   B.) Event provider

   C.) Alert Database

   D.) All of the mentioned

10. What are characteristics of Network based IDS ?

   A.) They look for attack signatures in network traffic

   B.) Filter decides which traffic will not be discarded or passed

   C.) It is programmed to interpret a certain series of packet

   D.) It models the normal usage of network as a noise characterization

11.What are the different ways to classify an IDS ?

   A.) Zone based

   B.) Host & Network based

   C.) Network & Zone based

   D.) Level based

1. A method used by an IDS that involves checking for a pattern to identify unauthorized activity
   1. **CORRECT:** Pattern Matching
   2. Session Splicing
   3. Protocol Decoding
   4. State Table
2. A list or table of stored by a router (or switch) that controls access to and from a network.
   1. State Table
   2. **CORRECT:** Access Control List (ACL)
   3. Session Splicing
   4. Packet Filter
3. An analysis method used by some IDS that looks for instances that are not considered normal behavior.
   1. Stateful Inspection
   2. **CORRECT:** Anomaly Detection
   3. Evasion
   4. Pattern Matching
4. Bypassing a device, or performing another action, to attack or place malware on a target network without being detected.
   1. Packet Filter
   2. State Table
   3. **CORRECT:** Evasion
   4. Honeypot
5. A type of firewall closely related to a packet filter that can track the status of a connection through use of a state table that keeps track of connection activities.
   1. Anomaly Detection
   2. Protocol Decoding
   3. **CORRECT:** Stateful Inspection
   4. State Table
6. A tool that uses the monitoring of network traffic, detection of unauthorized access attempts, and notification of unauthorized access attempts to network administrator.
   1. Anomaly Detection
   2. Access Control List (ACL)
   3. **CORRECT:** Intrusion Detection System (IDS)
   4. Session Splicing
7. A type of stateless inspection used in some routers and firewalls to limit flow of traffic to what is on the ACL.
   1. **CORRECT:** Packet Filter
   2. Proxy Server
   3. Evasion
   4. State Table
8. A way of looking at raw packet data.
   1. Proxy Server
   2. Session Splicing
   3. **CORRECT:** Protocol Decoding
   4. Pattern Matching
9. A server (or application) that intercepts the requests clients make of another server, fills the requests that it can, and then forwards the requests it can't handle on to the other server thus helping to improve performance and security.
   1. Honeypot
   2. **CORRECT:** Proxy Server
   3. Packet Filter
   4. State Table
10. A table in which data about connection activity is kept by a stateful firewall.
    1. Evasion
    2. **CORRECT:** State Table
    3. Honeypot
    4. Proxy Server
11. Something set up on a separate network (or in DMZ) to attract hackers and lure them away from the real network; it logs keystrokes, provides other information about an attacker, and also provides warning that someone is trying to attack your network.
    1. Proxy Server
    2. State Table
    3. Evasion
    4. **CORRECT:** Honeypot