Quiz 1: Security

**IPtables**

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. 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.

3. 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.

4. 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.

5. 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.

6. 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.

7. 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.

8. Wireshark is a \_\_\_\_\_\_\_\_\_\_\_\_ tool.  
a) network protocol analysis  
b) network connection security  
c) connection analysis  
d) defending malicious packet-filtering

Answer: a  
Explanation: Wireshark is popular standardized network protocol analysis tools that allow in-depth check and analysis of packets from different protocols used by the system.

9. \_\_\_\_\_\_\_\_\_\_ is a popular tool used for discovering networks as well as in security auditing.  
a) Ettercap  
b) Metasploit  
c) Nmap  
d) Burp Suit

Answer: c  
Explanation: Network Mapper (Nmap) is a popular open-source tool used for discovering network as well as security auditing. It can be used for either a single host network or large networks.

**Firewall**

1. Network layer firewall works as a \_\_\_\_\_\_\_\_\_\_  
a) Frame filter  
b) Packet filter  
c) Content filter  
d) Virus filter

Answer: b  
Explanation: As you know, firewalls are available as hardware appliances, as software-only, or a combination of the two. In every case, the purpose of a firewall is to isolate your trusted internal network (or your personal PC) from the dangers of unknown resources on the Internet and other network connections that may be harmful. The firewall prevents unauthorized access to your internal, trusted network from outside threats.

2. Network layer firewall has two sub-categories as \_\_\_\_\_\_\_\_\_  
a) State full firewall and stateless firewall  
b) Bit oriented firewall and byte oriented firewall  
c) Frame firewall and packet firewall  
d) Network layer firewall and session layer firewall

Answer: a  
Explanation: Most network layer firewalls can operate as stateful or stateless firewalls, creating two subcategories of the standard network layer firewall. Stateful firewalls have the advantage of being able to track packets over a period of time for greater analysis and accuracy — but they require more memory and operate more slowly. Stateless firewalls do not analyze past traffic and can be useful for systems where speed is more important than security, or for systems that have very specific and limited needs. For example, a computer that only needs to connect to a particular backup server does not need the extra security of a stateful firewall.

3. Which of the following is / are the types of firewall?  
a) Packet Filtering Firewall  
b) Dual Homed Gateway Firewall  
c) Screen Host Firewall  
d) Dual Host Firewall

Answer: a  
Explanation: A firewall can be a PC, a midrange, a mainframe, a UNIX workstation, a router, or combination of these. Depending on the requirements, a firewall can consist of one or more of the following functional components: Packet-filtering router

4. A proxy firewall filters at \_\_\_\_\_\_\_\_\_  
a) Physical layer  
b) Data link layer  
c) Network layer  
d) Application layer

Answer: d  
Explanation: The application firewall is typically built to control all network traffic on any layer up to the application layer. It is able to control applications or services specifically, unlike a stateful network firewall, which is – without additional software – unable to control network traffic regarding a specific application. There are two primary categories of application firewalls, network-based application firewalls and host-based application firewalls.

5. A packet filter firewall filters at \_\_\_\_\_\_\_\_\_\_  
a) Physical layer  
b) Data link layer  
c) Network layer or Transport layer  
d) Application layer

Answer: c  
Explanation: In computing, a firewall is a network security system that monitors and controls the incoming and outgoing network traffic based on predetermined security rules.[1] A firewall typically establishes a barrier between a trusted, secure internal network and another outside network, such as the Internet, that is assumed not to be secure or trusted.[2] Firewalls are often categorized as either network firewalls or host-based firewalls.

**SSL/TLS**

1. \_\_\_\_\_\_\_\_\_\_\_ ensures the integrity and security of data that are passing over a network.  
a) Firewall  
b) Antivirus  
c) Pentesting Tools  
d) Network-security protocols

Answer: d  
Explanation: The methods and processes in securing network data from unauthorized content extraction are controlled by network-security protocols.

2. Which of the following is not a strong security protocol?  
a) HTTPS  
b) SSL  
c) SMTP  
d) SFTP

Answer: c  
Explanation: SMTP (is abbreviated as Simple Mail Transfer Protocol) is a standard protocol to transmit electronic mail and is a widely used mail transmitting protocol.

4. \_\_\_\_\_\_\_\_\_\_ is a set of conventions & rules set for communicating two or more devices residing in the same network?  
a) Security policies  
b) Protocols  
c) Wireless network  
d) Network algorithms

Answer: b  
Explanation: Network protocols are designed with mechanisms for identifying devices and make connections between them. In addition, some proper rules are defined as to how data packets will be sent and received.

5. TSL (Transport Layer Security) is a cryptographic protocol used for securing HTTP/HTTPS based connection.  
a) True  
b) False

Answer: a  
Explanation: TLS which has now become SSL (Secure Socket Layer) is one of the popular cryptographic protocols developed to provide security to computer network while communication.

6. HTTPS is abbreviated as \_\_\_\_\_\_\_\_\_  
a) Hypertexts Transfer Protocol Secured  
b) Secured Hyper Text Transfer Protocol  
c) Hyperlinked Text Transfer Protocol Secured  
d) Hyper Text Transfer Protocol Secure

Answer: d  
Explanation: Hyper Text Transfer Protocol Secure (HTTPS) is a security protocol which maintains security when data is sent from browser to server and vice versa. It denotes that all communication setup between the browser and the server is encrypted.

7. SSL primarily focuses on \_\_\_\_\_\_\_  
a) integrity and authenticity  
b) integrity and non-repudiation  
c) authenticity and privacy  
d) confidentiality and integrity

Answer: a  
Explanation: SSL primarily focuses on maintaining the integrity of the data. Also, it maintains authenticity which helps the customers feel secure to communicate over the internet.

8. In SSL, what is used for authenticating a message?  
a) MAC (Message Access Code)  
b) MAC (Message Authentication Code)  
c) MAC (Machine Authentication Code)  
d) MAC (Machine Access Code)

Answer: b  
Explanation: For authenticating in SSL, a short message known as MAC (Message Authentication Code) is used for authenticating a message; where both the sender & the receiver need to implement the same key in order to start communicating.

9. \_\_\_\_\_\_\_\_\_\_ is used for encrypting data at network level.  
a) IPSec  
b) HTTPS  
c) SMTP  
d) S/MIME

Answer: a  
Explanation: IPSec (Secure Internet Protocol) is used for securing data at the network level by using 3 different protocols. These are Encapsulating Secure Payload (ESP), Authentication Header, and Internet Key Exchange (IKE).

12. Why did SSL certificate require in HTTP?  
a) For making security weak  
b) For making information move faster  
c) For encrypted data sent over HTTP protocol  
d) For sending and receiving emails unencrypted

Answer: c  
Explanation: In the case of HTTP connection, data are sent as plain-text, which is easily readable by hackers, especially when it is credit card details and personal information. But with the incorporation of SSL certificate, communication becomes secure and data sent and received are encrypted.

13. SFTP is abbreviated as \_\_\_\_\_\_\_\_  
a) Secure File Transfer Protocol  
b) Secured File Transfer Protocol  
c) Secure Folder Transfer Protocol  
d) Secure File Transferring Protocol

Answer: a  
Explanation: It is a secured FTP, where communication is made secured using SSH (Secure Shell) which helps in secure transferring of files in both local as well as remote systems.

14. The full form of SSL is  
a) Serial Session Layer  
b) Secure Socket Layer  
c) Session Secure Layer  
d) Series Socket Layer

Answer: b  
Explanation: SSL stands for Secure Sockets Layer.