1(a) One of the fundamental security design principles is the *least common mechanism*. Briefly explain what this principle means, and its implications. [2 Marks].

1 mark for definition, 1 mark for implication

Least common mechanism means that the design should minimize the functions shared by different users, providing mutual security. This principle helps reduce the number of unintended communication paths and reduces the amount of hardware and software on which all users depend, thus making it easier to verify if there are any undesirable security implications.

1(b) List and briefly explain three common types of attack surfaces. [3 Marks]

1 mark for each

- Network attack surface: This category refers to vulnerabilities over an enterprise network, wide-area network, or the Internet. Included in this category are network protocol vulnerabilities, such as those used for a denial-of-service attack, disruption of communications links, and various forms of intruder attacks.
- Software attack surface: This refers to vulnerabilities in application, utility, or operating system code. A particular focus in this category is Web server software.
- Human attack surface: This category refers to vulnerabilities created by personnel or outsiders, such as social engineering, human error, and trusted insiders.

2(a) List three characteristics of UDP protocol. [3 Marks]
1 mark for each - any 3 will do

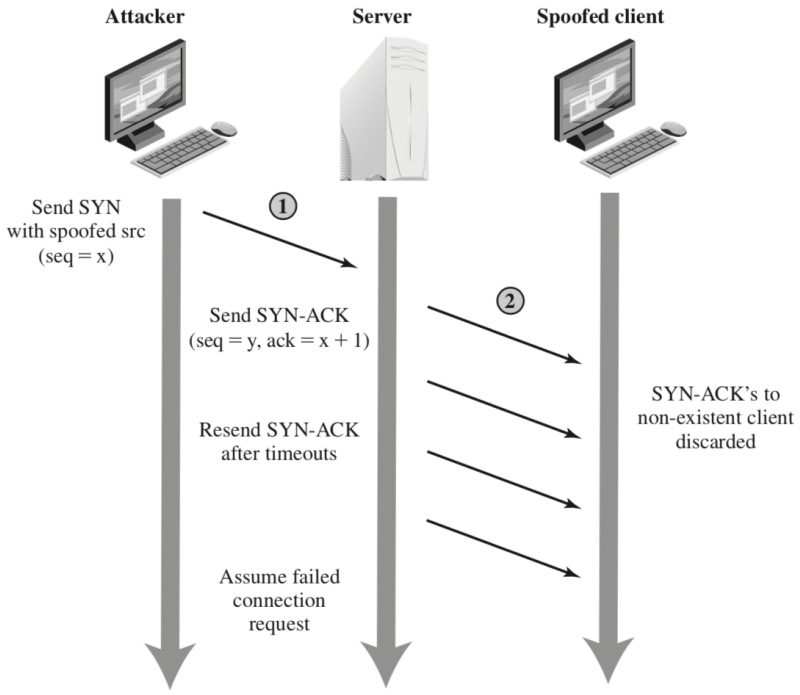
- It is a connectionless ‘‘best-effort’’ communications protocol
- It does not check to see if the receiving machine is ready to receive data, or let it know that the data is about to arrive. Also, it does not check whether the data was received, or in the right order.
- Its size can be up to 65,535 bytes long
- It has no error detection or correction
- It has a smaller overhead than TCP

2(b) What was *TTL* designed for and how does it work? [2 Marks]
1 mark for what was designed for - 1 mark for how it works
The first two can be used for the design question, the last three for how it works.

- Originally was introduced to avoid cycles (in routing)
- In IPv4, It was designed to specify time (in second) that datagram is allowed to travel
- Most routers process the packet in less than a second, however based on the protocol, each router subtracts 1 from the value of TTL, before forwarding it to the next hop.
- When TTL is equal 0, it is considered that it has traveled a closed loop, and it is discarded $\rightarrow$ essentially TTL can be used as a hop counter.
- The initial value of TTL is set by the higher level protocol that created the packet.

3(a) Using a diagram, explain how **SYN spoofing** attack works. Explain how SYN cookies can counter these attacks? [3 Marks]

2 marks for what it is, 1 mark for the countermeasure



A SYN spoofing attack generates a very large number of SYN connection request packets with forged source addresses. For each of these, the server records the details of the TCP connection request and sends the SYN-ACK packet to the claimed source address, and add this connection to its knownTCP connection table. Once this table is full, any future requests, including legitimate requests from other users, are rejected. The table entries will time out and be removed, which in normal network usage corrects temporary overflow problems.

It is possible to specifically defend against the SYN spoofing attack by using a modified version of the TCP connection handling code. Instead of saving the connection details on the server, critical information about the requested connection is cryptographically encoded in a cookie that is sent as the servers initial sequence number. This is sent in the SYN-ACK packet from the server back to the client. When a legitimate client responds with an ACK packet containing the incremented sequence number cookie, the server is then able to reconstruct the information about the connection that it normally would have saved in the known TCP connections table

3(b) What is *Slowloris* attack? List one countermeasure to this attack. [2 Marks]

1 mark for what it is, 1 mark for the countermeasure

Slowloris exploits the common server technique of using multiple threads to support multiple requests to the same server application. It attempts to monopolize all of the available request handling threads on the Web server by sending HTTP requests that never complete. Since each request consumes a thread, the Slowloris attack eventually consumes all of the Web servers connection capacity, effectively denying access to legitimate users.

There are a number of countermeasures that can be taken against Slowloris type attacks, including limiting the ratef incoming connections from a particular host; varying the timeout on connections as a function of the number of connections; and delayed binding. Delayed binding is performed by load balancing software.

4(a) An NIDS sensor is placed just inside the external firewall of a large organization LAN, and before DMZ and internal network. List two of advantages of this placement. [2 Marks]

1 mark each for any of the two

- Sees attacks, originating from the outside world, that penetrate the networks perimeter defenses (external firewall).
- Highlights problems with the network firewall policy or performance.
- Sees attacks that might target the Web server or ftp server.
- Even if the incoming attack is not recognized, the IDS can sometimes recognize the outgoing traffic that results from the compromised server.

4(b) List and briefly define the three broad categories of classification approaches used by anomaly detection systems. [3 Marks]

1 mark for each

- Statistical: Analysis of the observed behavior using univariate, multivariate, or time-series models of observed metrics.
- Knowledge based: Approaches use an expert system that classifies observed behavior according to a set of rules that model legitimate behaviour.
- Machine-learning: Approaches automatically determine a suitable classification model from the training data using data mining techniques.

5(a) Any effective firewall must at least meet three basic design requirements. Describe each. [3 marks]

1 mark for each

- All traffic from inside to outside, and vice versa, must pass through the firewall.
- Only authorized traffic, as per the local security policy, will be allowed to pass.
- The firewall itself is immune to penetration.

5(b) Packet filters are list of rules based on matches to packet header fields. Suppose you are given the following rule set:

Rule	Dir	Src Add	Src Port	Dest Add	Dest Port	Proto -col	Flag Bits	Action
1	Out	Int	> 1023	Ext	80	TCP	Any	Allow
2	In	Ext	80	Int	> 1023	TCP	ACK, RST SYN/ACK, FIN	Allow
3	Either	Any	Any	Any	Any	Any	Any	Deny

Describe the effect of each rule. [2 Marks]

- Rule #1: Http clients on any internal machine with a TCP source port > 1023 are allowed to send outgoing packets to http servers of any machines using TCP port 80, with any TCP flag set
- Rule #2: Http servers on any external machines with TCP port 80 can reply, i. e. send incoming messages to http clients on any internal machines running on ports > 1023, as long as the TCP flags are set to ACK, RST, SYN/ACK, and FIN (i.e. they are part of a http session initiated by the internal client)
- Rule #3: Any other packets, excepts those allowed by rules #1 and #2 are denied