1) Define a firewall. State and discuss two generations of firewall. (7 marks)

A firewall is a network security system. It runs on the Network and Transport layer in the OSI model. It is used to prevent unauthorized users from accessing to a network. It allows users to set security policies and permissions. It allows users to set a proxy to allow or deny certain accesses. It also allows users to inspect inbound and outbound traffic.

Two generations of firewall are packet filters and stateful filters. Packet filters are first generation firewalls and is used to inspect TCP and UDP data packets that are transmitting across a network. If a data packet does not match a set of rules, packet filters will deny or reject the packet. Stateful filters are second generation firewalls and are also called circuit-level gateways. They record all connections and classify the states into a new connection, part of an existing connection and not part of any connection. Packets from fake connection will be denied from entering the Transport layer of the OSI model.

2) State and explain the three statuses for a service port. (9 marks)

1. Open ports. They are computer ports that are open for communication.
2. Closed ports. They are computer ports that responses but no service is running at the specific port.
3. Filtered ports. They are computer ports that are protected by a firewall.

3) State and explain four types of denial of service (DoS) attacks. (12 marks)

1. DNS attack. It is an attack where attackers send DNS requests and flood connections to a victim server exceeding the maximum payload or connection capacity that the victim server can handle.

2. Teardrop attack. It is an attack where attackers send excessive payload and causes data segments to become out of order, causing the victim server to potentially be unable to reassemble messages and thus crashing.

3. Smurf attack. It is an attack where attackers broadcast ping requests that have small payloads using servers and relay them to the victim server to form a larger payload, which exceed the maximum payload and ping requests that the victim server can handle.

4. SYN flood attack. It is an attack where attackers send SYN requests to a victim server which exceeds the SYN-RECEIVED queue capacity of the victim server, causing the victim server to only respond and send SYN-ACK replies to the malicious party.

4) State and explain four social engineering attacks. (12 marks)

1. Voice phishing. It is a social engineering attack which uses voice to convince and lure information out of victims by simply asking.
2. Photographing. It is a social engineering attack where photos are taken using a photo capturing tool without consent from the victim.
3. Voice recording. It is a social engineering attack where victim's voice is recorded using a voice recording tool without consent from the victim.
4. Space and time invasion. It is a social engineering attack where the victim is distracted for a period of time to create a window of opportunity for the malicious party to perform attacks.

5) Classify the following software applications into malicious-impact table. (10 marks)

	Non-malicious programs	Malicious programs
Harmless	Photo editor, Device manager, Recycle bin, Official BIOS firmware	Triada Trojan, Spy.Gen
Catastrophic/Harmful	Facebook messenger, WeChat, Unreal Game Engine	CrytoLocker