CS356 – Computer Security  
Chapters 9&10

Please answer the following questions:

1) Identify four types of firewalls and provide a description of each? *(40 pts)*

Packet filtering firewall – applies a set of rules to each incoming and outgoing packet.

Stateful Inspection firewall – records information about each TCP connection to create a profile for packets to be checked against.

Application level gateway or application proxy – relays application-level traffic between endpoints of a connection. This traffic is checked that the traffic is using the application correctly.

Circuit level gateway or circuit proxy – relays traffic between endpoints of a TCP connection and examines the contents of that traffic for correctness.

2) Identify two applications that would exist in the DMZ. Why do they need to be there? *(20 pts)*

Web server, Email server, Database server

Because they need to be exposed to the world outside the internal firewall.
3) What information is stored on the stack that makes it particularly susceptible to buffer overflow attacks? (10 pts)

The return address of the function being called.
Parameters being passed to a system function.

4) Define each of the following terms: (20 pts)

a) Shellcode
Code supplied by the attacker and saved in the buffer being overflowed.

b) NOP sled
A run of NOP instructions leading to the shellcode. Landing anywhere in the sled will result in the shellcode being executed.

5) Setting the no-execute bit for the MMU to stop buffer overflows is an example of:

a) Compile time defense

b) Run-time defense