1) Describe how a slowloris attack works. *(10 pts)*

It attempts to monopolize by sending HTTP requests that never complete. This eventually consumes Web server’s connection capacity.

2) One of the classic methods of Denial of Service attacks is flooding. Describe what the key requirement in a single source system ICMP flood is. *(10 pts)*

A higher-capacity network than the target.

3) Describe how a Denial of Service reflector attack works. *(10 pts)*

The attacker sends packets to a known service with a spoofed source address of the target.

4) Describe how a DoS amplifier attack works. *(10 pts)*

When the reflector attacks generates a much larger response than the original request.

5) Describe how a DoS SIP flood attack works. *(10 pts)*

By exploiting the fact a single INVITE request triggers considerable resource consumption.

6) Identify 4 classes of intruders as per the book. *(20 pts)*

Cyber Criminals, Activists, State Sponsored, Other (Hackers)

7) Host-based intrusion detection uses two general approaches, anomaly detection and signature detection. *(20 pts)*

   a. Describe how Anomaly detection works

   Statistical analysis of observed behavior using knowledge systems and machine learning.

   b. Describe how Signature detection works.

   By defining a set of rules to attacks patterns that can be used to decide that a given behavior is that of an intruder.

8) Describe how network-based intrusion detection works. *(10 pts)*

By monitoring traffic at specific points on a network, packet by packet.