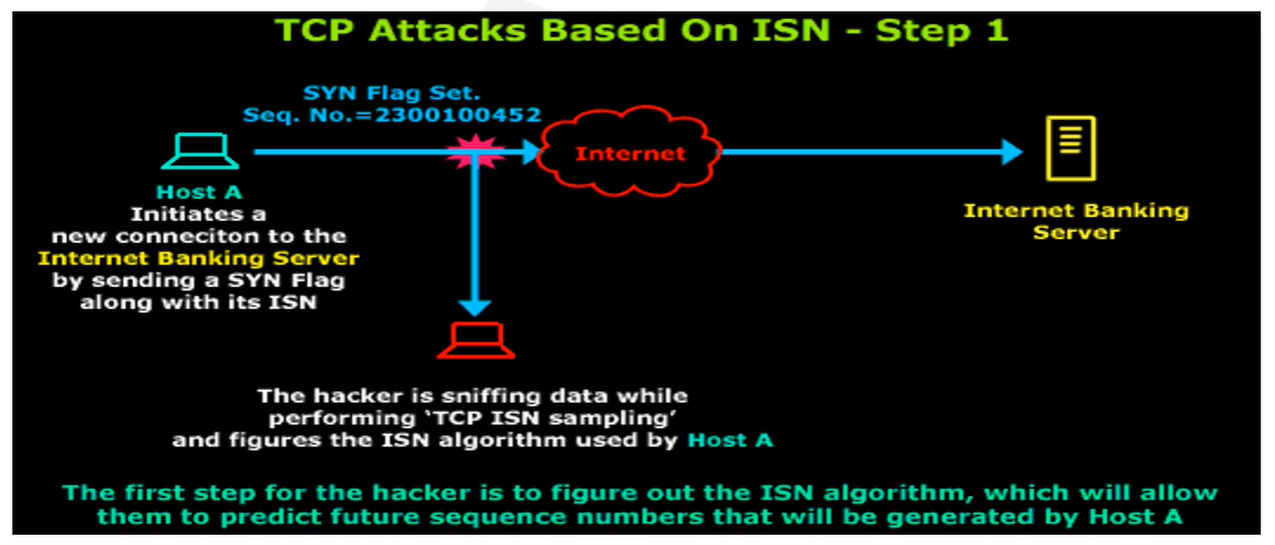
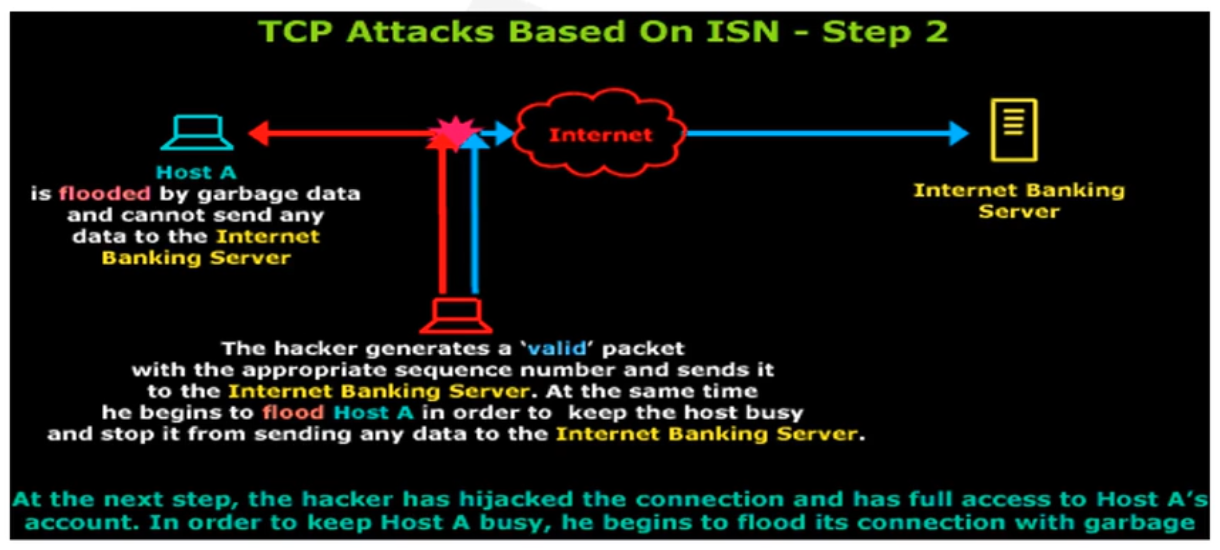
**Module 9 Session Hijacking**

**9.0 Hijacking**

**Session Hijacking**

1. Attacker tries to takeover active session from client
2. Steps
   1. Sniff – sniff traffic between client & server
   2. Monitor – monitor traffic & predict sequence numbers
   3. Desynchronise
      1. Desynchronise client session so cant get back to server
      2. TCP reset
      3. FIN flag
   4. Predict
      1. Predict session token
      2. Take over session
   5. Inject
      1. Inject packets to server pretending to be client
3. Example
   1. 
   2. 

**Spoofing VS Hijacking**

1. Spoofing – intent to sniff traffic
2. Hijacking – intent to take over entire session

**Session Hijacking Tools**

1. Ettercap
   1. Packet sniffer & session hijacking
2. Ferret
3. Burp Suite

**Session Hijacking Prevention**

1. Unpredictable session IDs
2. Limiting incoming connections
3. Reduce remote access
4. Regenerate session keys after authentication complete
   1. Though gets kind of expensive
5. IPSec – encrypt communications

**IPSec**

1. Transport mode – IP header not encrypted & can be used with NAT
2. Tunnel mode – entire original packet encrypted & doesn’t work with NAT

**Authentication Header**

1. Protocol that guarantees integrity & authentication of IP packet sender

**Encapsulating Security Payload (ESP)**

1. Protocol that provides integrity, authenticity & confidentiality to entire packet in tunnel mode

**IKE (Internet Key Exchange)**

1. Protocol that produces keys for encryption process

**Oakley**

1. Protocol that uses Diffie-Hellman to create master & session keys