入侵偵測技術 -異常型

- 異常偵測 (Anomaly Detection)
- 協定異常偵測 (Protocol Anomaly Detection)
  - 使用伺服器不支援之命令
  - 伺服器超出協定範位或預期的回應訊息
  - 封包重組會造成資料重疊或被覆蓋的現象
  - ICMP 封包超出正常比率
  - 異常封包標頭
  - 來源 IP, Port 與目的 IP, Port 相同
  - 在 HTTP, POP, IMAP 協定中出現 Shell 命令