入侵偵測技術 – 簡介

- 入侵偵測技術
  - 異常偵測 (Anomaly Detection)：
    - 如果訊息的行為超出正常範圍之外，或出現有『不應該出現的動作』，則判斷為入侵行為。
  - 誤用偵測 (Misuse Detection)：特徵偵測
    - 如果訊息的行為與其它入侵行為相同 (或類似)時，則判斷為入侵行為。
    - 比對已知的『入侵行為』