Construção de redes seguras

[Intrusion Detection System – IDS 2](#_Toc41823450)

[IDS – Host Based Detection 2](#_Toc41823451)

[IDS – Network Based Detection 3](#_Toc41823452)

# Intrusion Detection System – IDS

* O objetivo das firewall é prevenir acessos não autorizados
* IDS são uma segunda linha de defesa quando as firewalls são comprometidas.
* IDS monitorizam as redes e procuram por atividades suspeitas notificando quando existe intrusão e tomando medidas de proteção
* Existem dois tipo de IDS:
* Host based – instalam software no computador para analisar o trafego recebido pelo computador
* Network based – utilizam probes para monitorizar o trafego na rede
* Dois métodos implementados:
* Profile based IDS (anomaly detection) – o administrador configura um perfil básico de comportamento na rede. O trafego que não encaixar neste perfil é referido como uma anomalia. Isto identifica maior número de false positivos
* Signatura based IDS – analisa o conteúdo dos pacotes e compara com uma base de dados e verifica se pode estar a perante um ataque
* Existem soluções hibridas

# IDS – Host Based Detection

* Capacidade de monitorizar a atividade do sistema, logs e trafego de rede recebido.
* Performance do host
* Nem todos os ataques têm origem na rede – um atacante pode ter acesso físico à maquina
* Vantagem
* Capacidade de detetar quando o ataque tem sucesso
* Desvantagem
* Visibilidade limitada – não consegue detetar ataques a outros hosts
* Hosts comprometidos – atacante pode desativar o IDS
* Limitações do sistema operativo – suporte para todos os SO

# IDS – Network Based Detection

* São utilizadas probes/sensores instalados ao longo da rede
* Estas probes analisam o tarefo da rede à procura de um perfil ou assinatura
* Vantagens:
* Host based detection não consegue detetar ping sweep ou port scan em múltiplos hosts na rede
* Não utilizam recursos da maquina para fazer a deteção
* Desvantagens
* Largura de banda – capacidade de receber e analisar todo trafego
* Fragmentação de pacotes – manipular o tamanho dos fragmentos - overlap
* Manipulação de TTL – enviar pacotes apenas para o sensor para enganar
* Encriptação

6