ISEL
INSTITUTO SUPERIOR DE ENGENHARIA DE LISBOA

Deteção e prevenção de Intrusões

ISEL – Instituto Superior de Engenharia de Lisboa
Rua Conselheiro Emídio Navarro, 1 | 1959-007 Lisboa

NIDS

Network Intrusion Detection Systems

- Observam todo o tráfego que circula
- Procuram ataques potenciais
- Normalmente baseados em “assinaturas”
  - Procuram padrões de dados a circular na rede
  - Podem também procurar por padrões inesperados
- Quando existe uma suspeita é despoletado um alarme
  - Pode incluir uma captura de pacotes

- HIDS
  - Idênticos aos NIDS para para dispositivos

NIDS

Para o que não servem os NIDS?

- Não substituem as *firewalls,* políticas de segurança, atualização e *hardening* de sistemas
- Não são ferramentas de baixa manutenção
  - … ou de baixo custo
- Não servem para detetar todas as intrusões

NIDS

Implementação

- Introduzido como um analisador de tráfego passivo em pontos de agregação de tráfego
- Faz a identificação de padrões a partir da base de dados de regras e suas assinaturas
- As regras são aplicadas aos pacotes e eventos gerados quando uma regras é aplicável
- As regras identificam:
  - Protocolo, endereços, portos
  - *Payload*
  - Sequências de caracteres
  - Análise do fluxo de tráfego
  - Flags dos cabeçalhos
  - Qualquer campo no pacote

NIDS

Implementação

- Normalmente estabelece-se um quadro de referência para o tráfego numa rede
- A partir desse ponto é possível detetar situações anómalas
- Permite a deteção de ataques que exploram vulnerabilidades 0-day
- Os IDS podem também detetar variações inesperadas em protocolos que sejam conhecidos

NIPS

Network Intrusion Prevention Systems

- Tenta prevenir os ataques, em vez de apenas os detetar
- Fusão entre uma *firewall* e um IDS
- Inspeção de pacotes baseada em estados
  - Como nas *firewalls* dinâmicas
  - Nova versão de algo que já existe
- Existem algumas variantes que enviam TCP-Resets mas são consideradas piores que versões que atuam como uma *bridge*

NIPS

Para o que não servem os NIPS?

- Não substituem as *firewalls,* políticas de segurança, atualização e *hardening* de sistemas
- Não são ferramentas de baixa manutenção
  - … ou de baixo custo

NIPS

Implementação

- Normalmente introduzidos no perímetro da rede, antes ou depois de uma *firewall*
- Se for entre o operador e a *firewall* protegem os dispositivos colocados na DMZ
- Se for atrás da *firewall* protege a rede interna dos utilizadores da VPN e pode ajudar a identificar dispositivos internos que tenham sido comprometidos
- Requer especial atenção uma vez que os NIPS não são passivos e intercetam o tráfego
- Requerem *hardware* de alta performance que permita reduzir o impacto na comutação de pacotes

NIDS vs NIPS

- NIDS é mais neutro
  - Os falsos positivos do NIDS são alertas errados
  - Os falsos positivos do NIPS provocam quebras de conectividade
- O NIDS é melhor quando
  - Os *hosts* fazem parte da politica de segurança
    - Atualizados e protegidos
- O NIPS é melhor quando
  - Os *hosts* não fazem parte da política de segurança
  - Procuramos uma solução completa

Tipos

- Estáticos (sem estado)
  - Verificam cada pacote individualmente
  - Podem combinar os fragmentos para validar padrões/assinaturas
- Dinâmicos (com estado)
  - Encontram padrões/assinaturas em múltiplos pacotes
  - Identificam ataques que só existem quando a informação de uma sessão é analisada no seu todo
- Híbridos
  - Mistura de ambas as técnicas

Problemas de gestão dos NIDS/NIPS

- Falsos positivos
  - Exigem um esforço para ser eliminados

- Opções
  - Tornar as regras mais “apertadas”
  - Colocar uma exceção para aquela fonte em particular
  - Comentar a regra
  - Não fazer nada

Acesso aos padrões/assinaturas

- O segredos dos NIDS/NIPS está na base de dados dos padrões
- Normalmente funcionam sobre subscrição paga periodicamente
- Saber escrever novas regras para definir novos padrões é essencial
  - É preciso estar atento aos CERTs para perceber as vulnerabilidades que vão aparecendo

Colocação em produção

- Os NIDS/NIPS devem inspecionar todo o tráfego
  - Mas não são dispositivos de rede (*switches*, *routers*, …)
- Num ambiente com *switches* é difícil de encontrar um ponto onde todo o tráfego circule e possa ser intercetado
- Ethernet *taps*
  - É preciso fazer ou comprar
- Switch spanning/monitoring/mirror/copy port
  - Pode perder pacotes

Unified Threat Managment (UTM)

- Combina múltiplas tecnologias
  - *Firewall*, NIPS
  - VPN e Antivírus
  - Filtragem de SPAM e conteúdo Web
- Problemas
  - Expõem um conjunto de portos no extremo do perímetro
  - Tipicamente são servidores tradicionais a correr um sistema operativo normal
  - Ponto único de falha
- Úteis para ambientes pequenos

Resumo

- O NIDS e o NIPS fazem deteção de intrusões a partir de padrões/assinaturas
- Tanto os cabeçalhos como o conteúdo dos pacotes podem ser analisados
- NIPS é uma *firewall* dinâmica com uma base de dados de padrões/assinaturas
- Na aquisição de um destes produtos é obrigatório exigir a linguagem das assinaturas e o conteúdo destas
  - Para corrigir falsos positivos
  - Para otimizar o dispositivo para o ambiente local