Revisión práctica de IDS

por Sacha Fuentes

Índice

- Introducción a los IDS
- Presentación de varios IDS:
  - Snort
  - Logcheck
  - Bsign
- Técnicas para burlar IDS

Qué es un IDS?

- Sistema de detección de intrusos
- Monitorizar en busca de intentos de posibles malos usos o accesos no autorizados
- En términos informáticos, proceso de seguridad que monitoriza en busca de intentos de comprometer el sistema

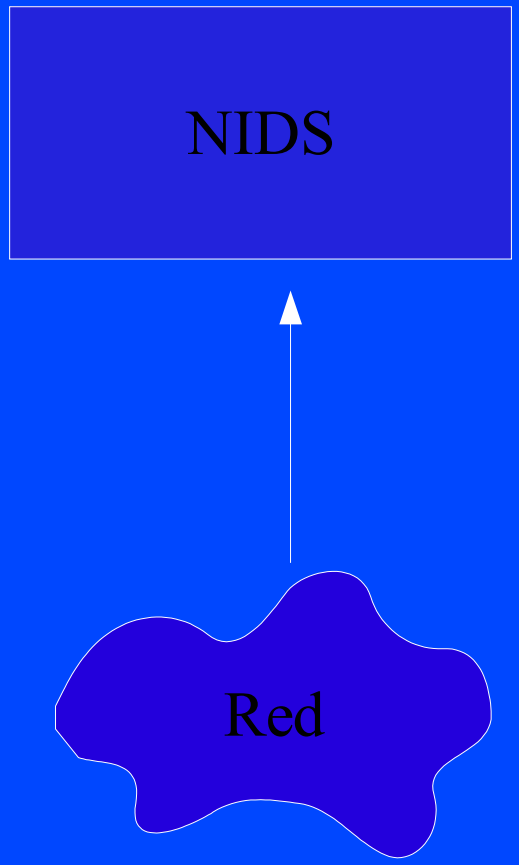
Porqué es necesario un IDS?

- Alerta ante ataques
- Capacidad de reacción
- Análisis posterior en caso de intrusión
- No debe ser sustituto de una política de seguridad

Tipos de IDS

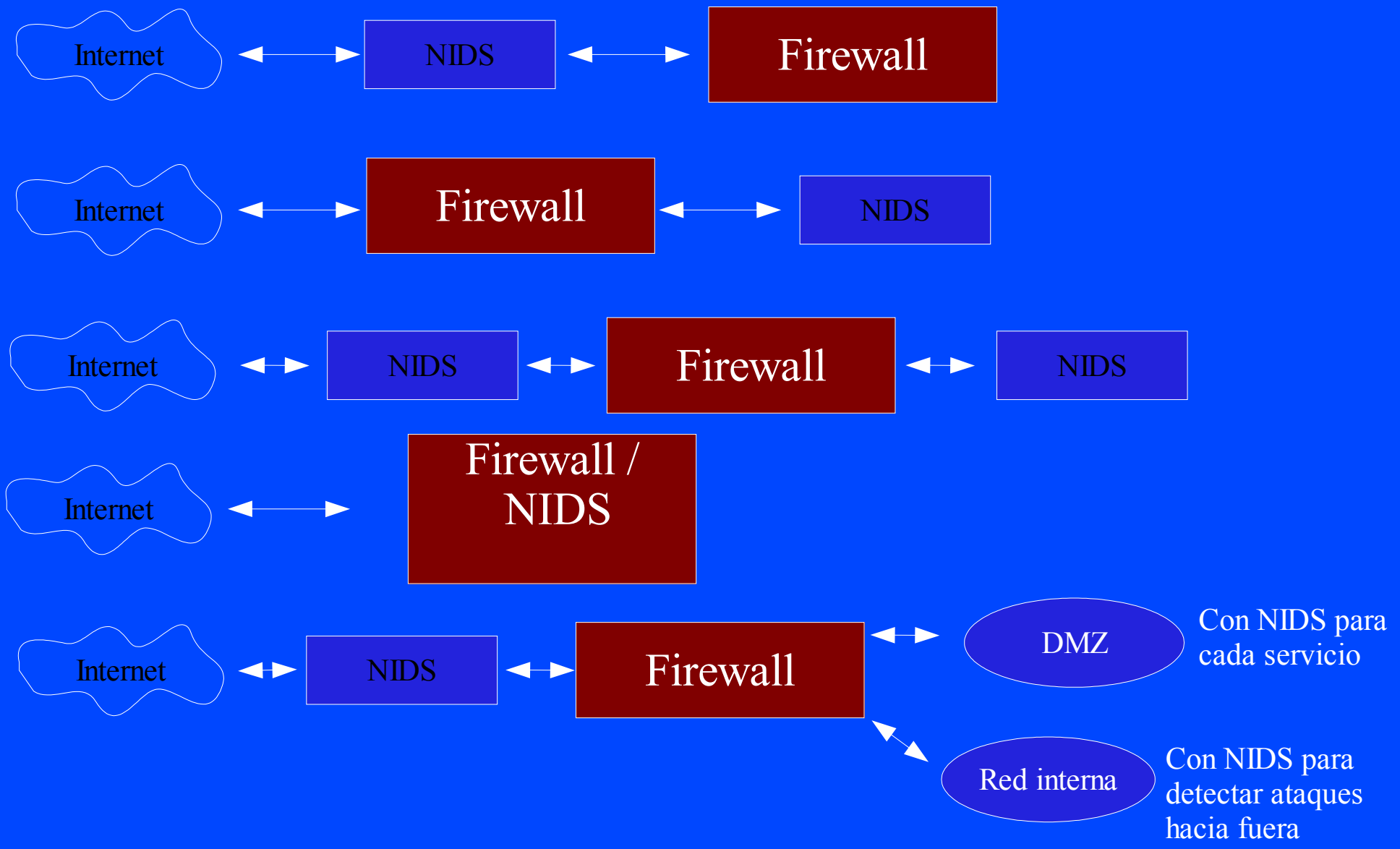
- HIDS (Host intrusion Detection System)
  - Información recogida en un solo host
- NIDS (Network Intrusion Detection System)
  - Información recogida a través de la red
- DIDS (Distributed Intrusion Detection System)
  - Sensores distribuidos en diferentes puntos de la red

NIDS - Arquitectura



- Monitoriza todo el tráfico de un segmento de red
- Filtra el tráfico
- Detecta tráfico maligno, habitualmente mediante un conjunto de reglas
- Lanza alertas

NIDS – Dónde colocarlo



NIDS – Dónde colocarlo

- Red conexionada mediante hub o mediante switch

- Seguridad de la máquina que hace de NIDS

HIDS

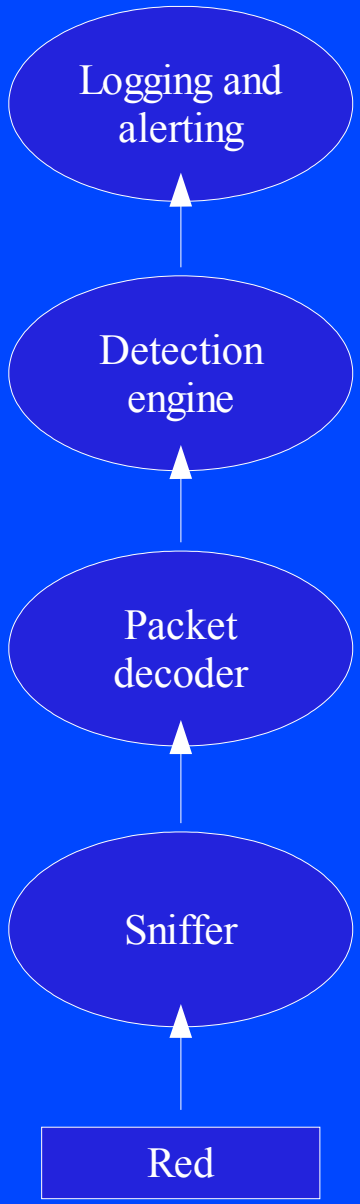
- Monitor de red
  - Como un NIDS pero sólo examina el tráfico local

- Monitor de sistema
  - Monitor de entradas
  - Monitor de actividad de root
  - Monitor de ficheros

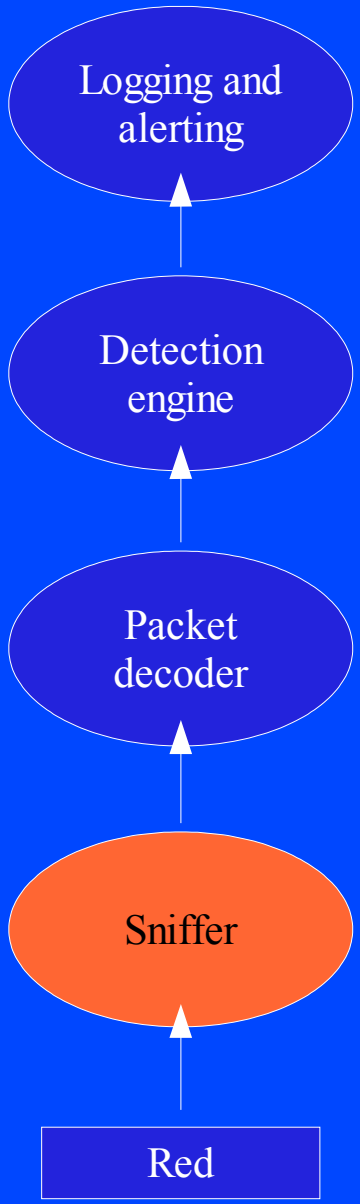
Snort

- Tipo NIDS. Funciona mediante un conjunto de reglas a través de las cuales se hace pattern-matching con los paquetes
- Licencia GPL
- Su creador da soporte comercial a través de la compañía Sourcefire

Snort - Arquitectura



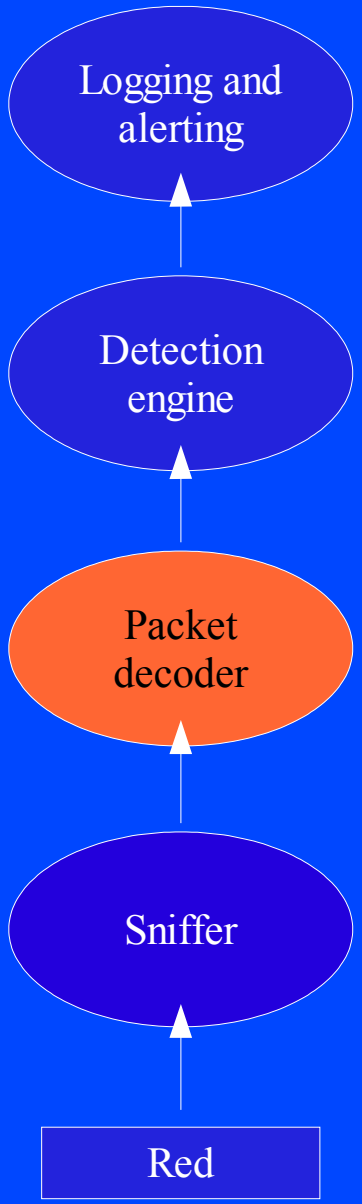
Snort - Arquitectura



Sniffer:

- Utiliza libpcap -> multiplataforma
- Interface de red en modo promiscuo

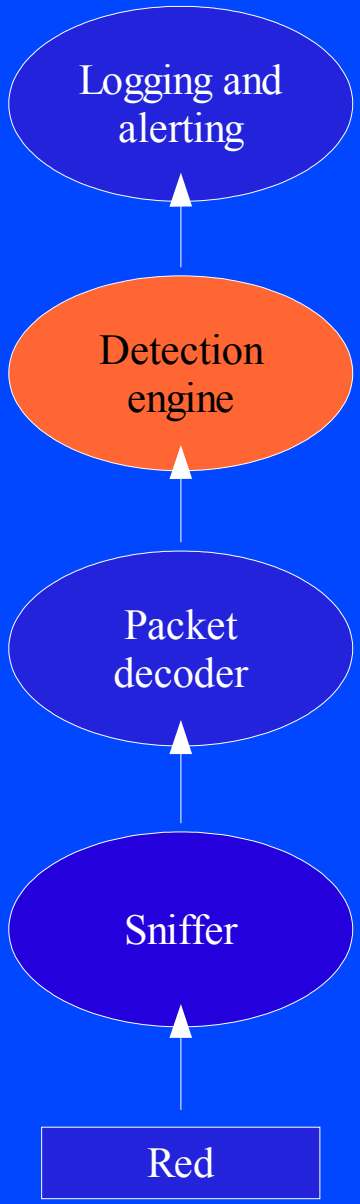
Snort - Arquitectura



Packet decoder:

- Decodifica paquetes y los guarda en memoria
- Trata muchos tipos de protocolos (Ethernet, PPP,...) y paquetes (IP, ARP,...)
- Los paquetes decodificados son tratados mediante preprocesadores

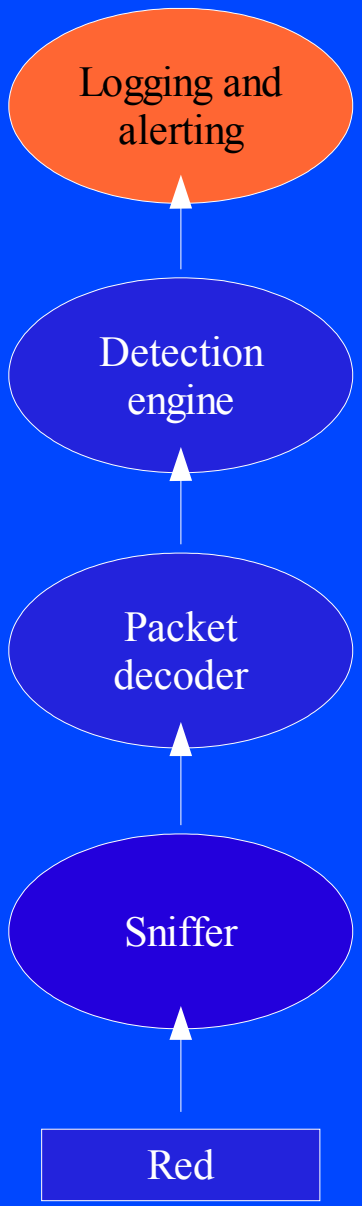
Snort - Arquitectura



Detection engine:

- Compara paquetes leídos con reglas
- Reglas agrupadas por categorias
- Cuando el paquete coincide con alguna de las reglas se pasa a la siguiente capa

Snort - Arquitectura



Logging and alerting:

- Muchos tipos de salidas
  - Ficheros de texto
  - Syslog
  - SMB
  - XML
  - Bases de datos
  - ...

Logcheck

- Tipo HIDS
- Monitorización de logs
- Envía mails con la actividad sospechosa

Bsign

- Comprobación de integridad y autenticidad de ficheros
- Guarda el hash en el propio fichero (solo ejecutables) y una firma del hash
- Funciona mediante un sistema de clave pública

Bsign - Digsig

- Módulo del kernel (Linux)
- Permite que el kernel solo cargue ejecutables con firma correcta
- No permite la ejecución de ejecutables sin firma

Técnicas para burlar IDS

- Normalmente, basadas en que el IDS no vea lo mismo que el destino
- Suelen aprovecharse de diferencias en el modo de tratar alguna de las capas por las que pasa la información
- El IDS necesita saber como funcionan todos los sistemas que monitoriza

Técnicas para burlar IDS

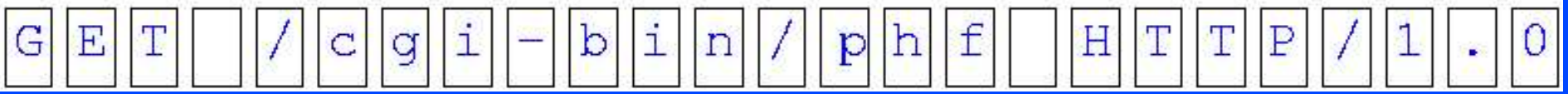
Nivel transporte

- TCP Splitting

Petición enviada en un paquete normal

```
GET /cgi-bin/phf HTTP/1.0
```

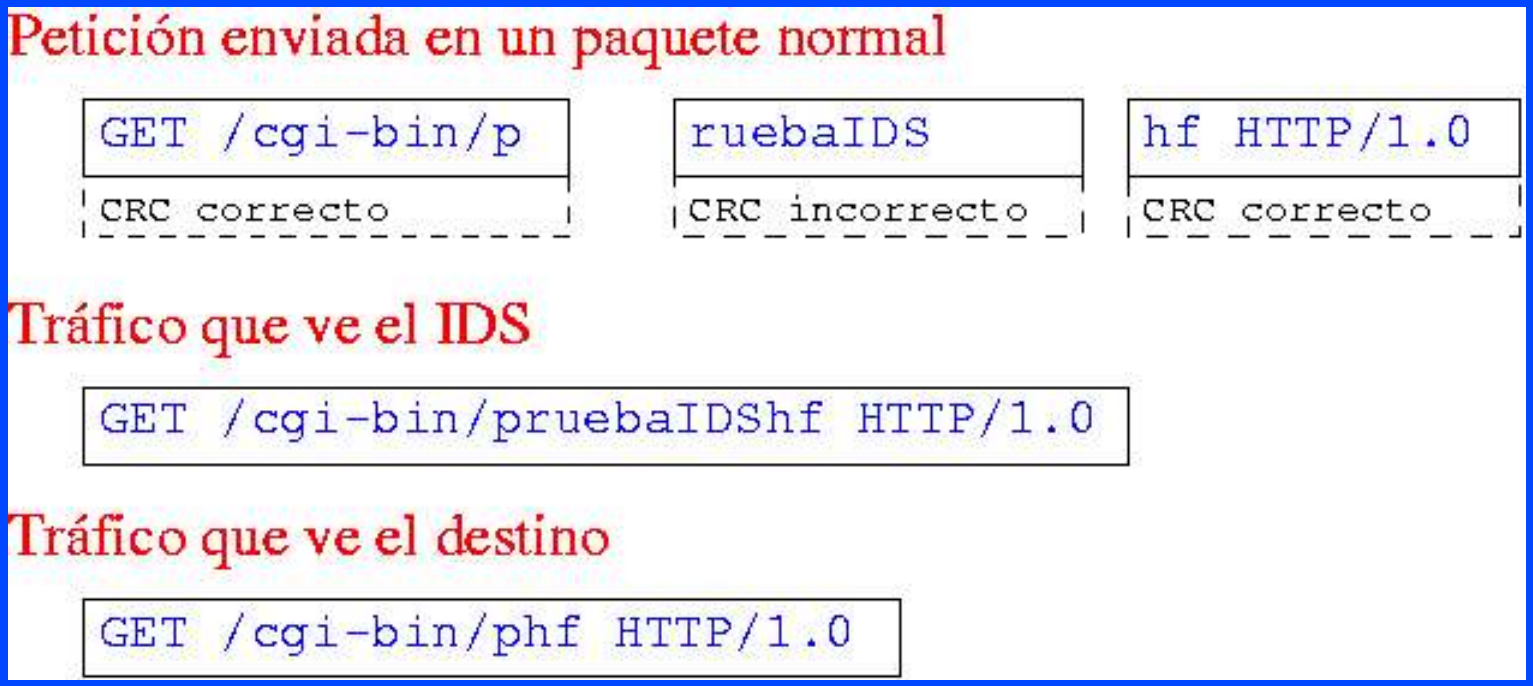
Petición enviada en diferentes paquetes



Técnicas para burlar IDS

Nivel transporte

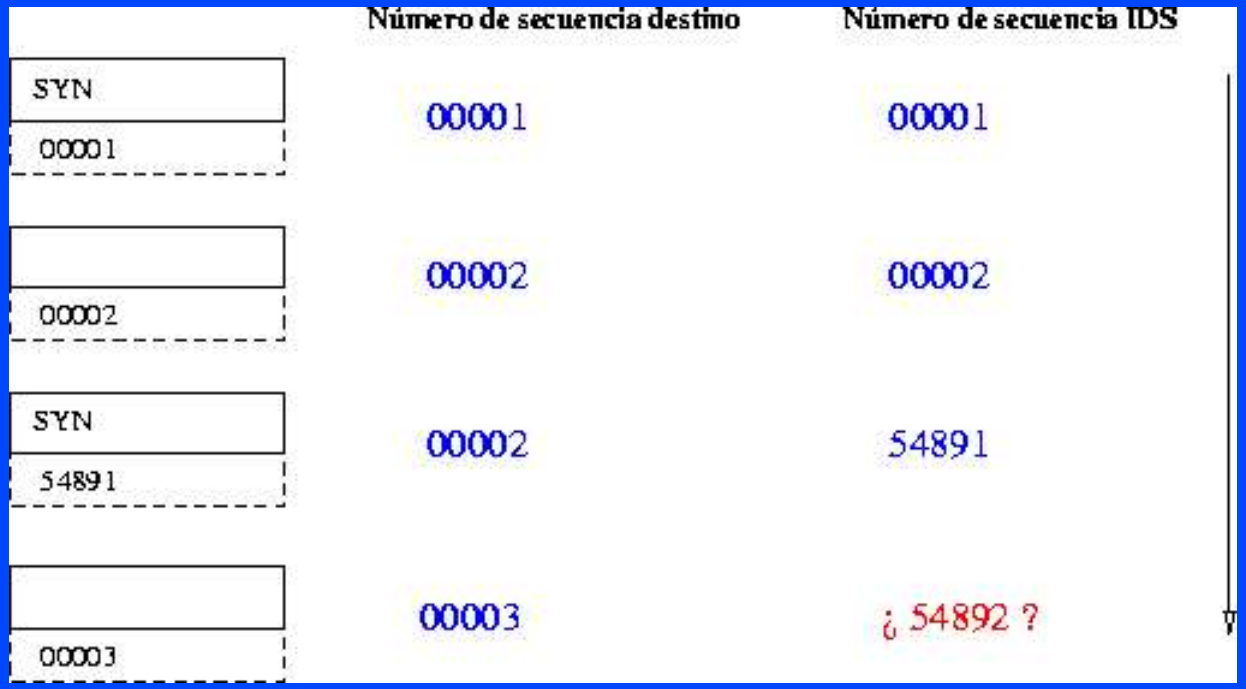
- Inserción



Técnicas para burlar IDS

Nivel transporte

- Desincronización



Técnicas para burlar IDS

Nivel transporte

- Final de conexión falso

Técnicas para burlar IDS

Nivel transporte

- Fragmentación

Fragmento 1

```
GET /cgi-bin/pru
```

Fragmento 2

```
hf HTTP/1.0
```

Paquete completo solapado

```
GET /cgi-bin/phf HTTP/1.0
```

Fragmento 1

```
GET /cgi-bin/p
```

Fragmento 2a

```
rueba HTTP/1.0
```

Fragmento 2b

```
hf HTTP/1.0
```

Paquete completo

```
GET /cgi-bin/phf HTTP/1.0
```

Técnicas para burlar IDS

Nivel aplicación HTTP

- Cambio de método

```
HEAD /cgi-bin/phf HTTP/1.0
```

- Codificación de URI

```
GET /%63%67%69-%62%69%6e/%70%68%66 HTTP/1.0
```

- Inserción de caracteres redundantes

```
GET /cgi-bin//phf HTTP/1.0
```

Técnicas para burlar IDS

Nivel aplicación HTTP

- Inserción de caminos redundantes

```
GET /cgi-bin/./phf HTTP/1.0
GET /cgi-bin/redunda/../phf HTTP/1.0
```

- Formateo incorrecto

```
GET<tab>/cgi-bin/phf<tab>HTTP/1.0
```

- Cambio de separadores

```
GET /cgi-bin\phf HTTP/1.0
```

Técnicas para burlar IDS

Nivel aplicación HTTP

- Inserción de nulos

```
GET%00 /cgi-bin/phf HTTP/1.0
```

- Mayúsculas y minúsculas

```
GET /CGI-BIN/PHF HTTP/1.0
```

Técnicas para burlar IDS

Nivel aplicación HTTP

- Parámetros codificados

```
GET /cgi-bin/uncgi.cgi?parametro1=valor1 HTTP/1.0
```

codificado como

```
POST /cgi-bin/uncgi.cgi HTTP/1.0
Content-Encoding: base64

cGFyYW1ldHJvMT12YWxvcjE=
```

Técnicas para burlar IDS

Nivel aplicación

- Aplicación interactiva

```
cat /etc/passwd
```

codificado como

```
perl -e '$foo=pack(“C11”,47,101,116,99,47,112,97,
 115,115,119,100);@bam=`/bin/cat $foo`; print
 “@bam\n”;'
```

Técnicas para burlar IDS

Otras técnicas

- SSL
- Port Scanning
  - FTP Bounce Scanning
  - Slow scan