Proyecto Seguridad en Redes y Sistemas
2015

DETECCIÓN DE INTRUSOS CON SNORT

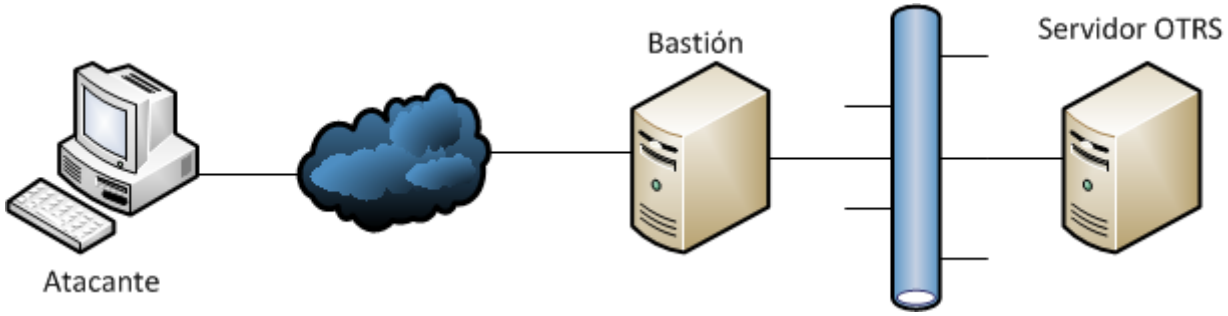
Juan Clavero

Contenido

- Introducción
- Conceptos previos
- Escenario Planteado
- Ataque
- Análisis
- Conclusión

Introducción

- Problema
- Objetivos
- Metodología
- Tareas

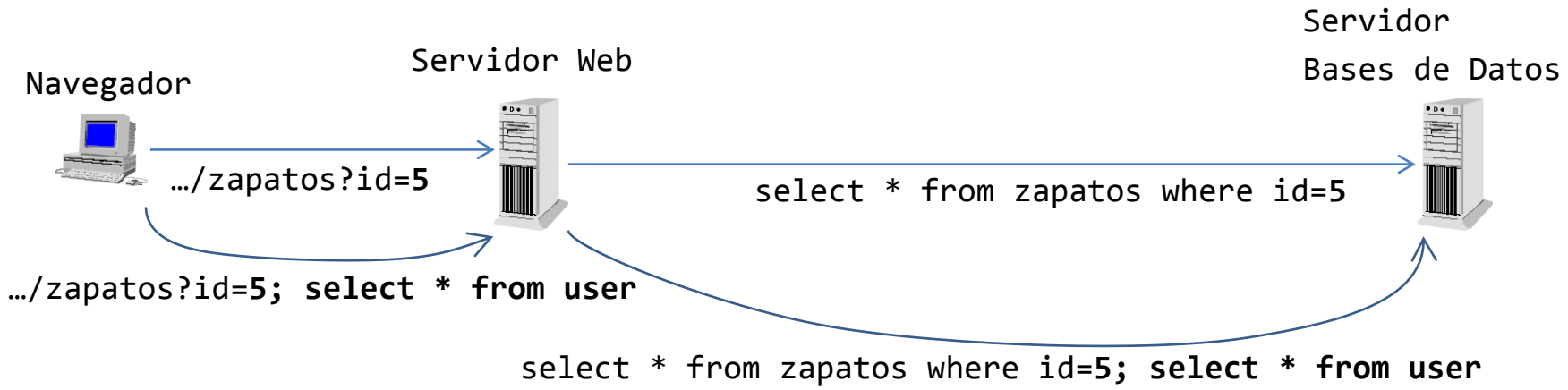


Conceptos Previos

- Sistema detección intrusos (IDS)
  - Clasificación por ubicación:
    - De red (Network IDS)
    - De equipo (Host IDS)
  - Clasificación por funcionamiento:
    - Patrones conocidos
    - Anomalías

Conceptos Previos

- Inyección SQL



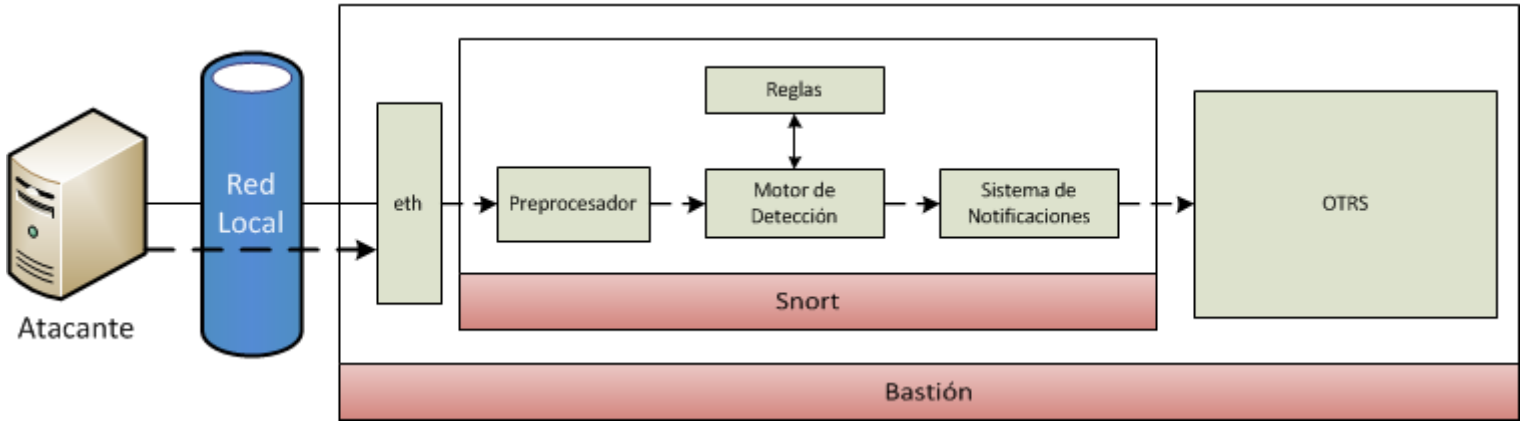
…/zapatos?id=5 **and 1=0**

…/zapatos?id=5 **and 1=1**

- Denegación de Servicio (DoS)

Escenario planteado

- Bastión



- Atacante

Escenario planteado

- Reglas de Snort
  - Inyección SQL

cabecera:
```
log tcp any any -> $LOCAL $HTTP_PORTS
```

opción:
```
(msg:"SQL Injection - Comments and text delimiter";
flow:to_server; pcre:"/(\%27)|(\')|(\-\-)|(%23)|(#)/i";
sid:1000001; rev:1;)
```

  - DoS

cabecera:
```
log tcp any any -> $LOCAL $HTTP_PORTS
```

opción:
```
(msg:"Possible TCP DoS"; flow: to_server; flags: S;
detection_filter:track by_src, count 50, seconds 1;
sid:1000003;rev:1;)
```

Ataque

- Inyección SQL

```
sqlmap http://$VICTIM/otrs/index.pl?Action=AgentTicketZoom;TicketID=1
```

interfaz visualizar ticket

- DoS
  - HTTP

```
hping3 -c 100 -d 120 -S -p 80 --flood $VICTIM
```

  - ICMP

```
ping $VICTIM -i 0 -f -c 1000
```

Análisis

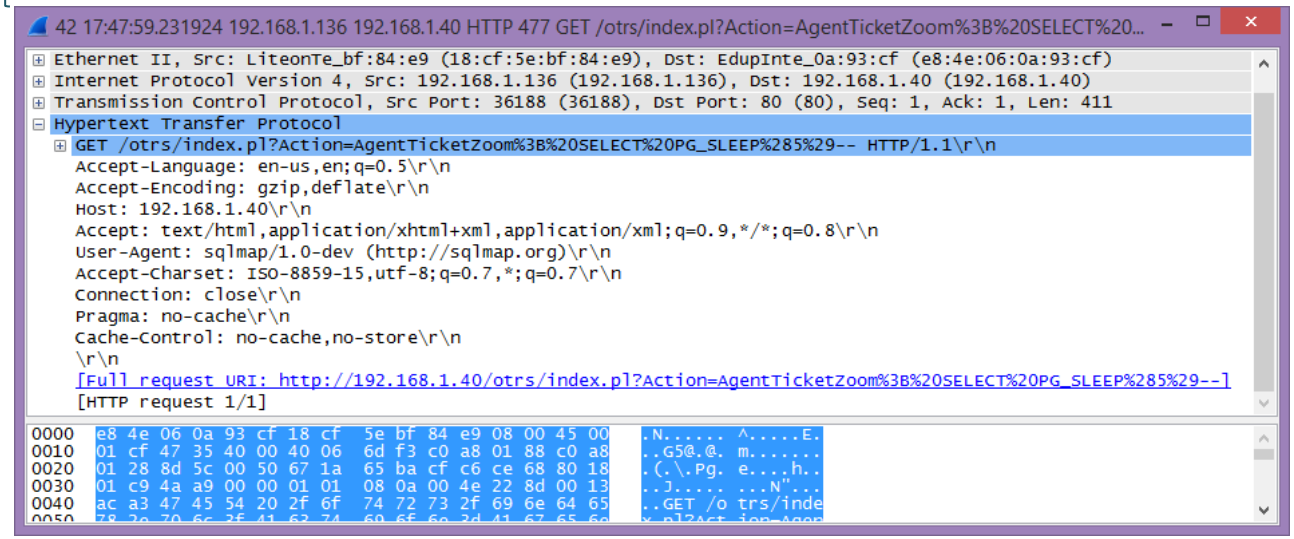
- Muestras: Inyección SQL

Id de la regla

Timestamp, origen y destino

Extracto del contenido del paquete

```
[**] [1:1000001:1] SQL Injection - Comments and text delimiter [**]
[Priority: 0]
05/26-19:47:59.231924 192.168.1.136:36188 -> 192.168.1.40:80
TCP TTL:64 TOS:0x0 ID:18229 IpLen:20 DgmLen:463 DF
***AP*** Seq: 0x671A65BA  Ack: 0xCFC6CE68  Win: 0x1C9  TcpLen: 32
TCP Options (3) => NOP NOP TS: 5120653 1289379
```



Conclusión

- Evaluado la necesidad de seguridad del escenario,
- Estudiado y valorado las alternativas disponibles,
- Instalación y configuración del aplicativo principal y de snort,
- Diseñado y ejecutado un plan de pruebas adecuado,
- Comprobado el funcionamiento de snort