Seguridad en Redes
Practica 3.4

David Antuña Rodríguez
Javier Carrión García

1 Sniffer y packet logger

El modo sniffer de snort tiene las siguientes opciones.

- -v
  Es la opción que permite iniciar snort en modo sniffer, imprimirá las cabeceras TCP/IP de los paquetes.
- -d
  Con esta opción snort también mostrara los datos no solo las cabeceras.
- -e
  Añadira a la información mostrada las cabeceras de la capa **data link**, la segunda de las siete que componen el modelo OSI.

Si en lugar de sniffer queremos iniciar snort en modo packet logger tenemos que especificar el directorio en el que debe almacenar los paquetes, de este modo snort sabrá que debe iniciarse en modo packet logger.

```
sudo snort -dev -l ./log
```

2 NIDS basado en reglas

```
[**] [1:366:7] ICMP PING *NIX [**]
[Classification: Misc activity] [Priority: 3]
04/08-12:59:32.544418 192.168.1.3 -> 192.168.1.2
ICMP TTL:64 TOS:0x0 ID:58668 IpLen:20 DgmLen:84 DF
Type:8  Code:0  ID:5123   Seq:13  ECHO
```

La regla con SID 366 estaba en el fichero */etc/snort/rules/icmp-info.rules*.

```
alert icmp $EXTERNAL_NET any -> $HOME_NET any (msg:"ICMP PING *NIX";
itype:8; content:"|10 11 12 13 14 15 16 17 18 19 1A 1B 1C 1D 1E 1F|";
depth:32; classtype:misc-activity; sid:366; rev:7;)
```

```
[**] [1:384:5] ICMP PING [**]
[Classification: Misc activity] [Priority: 3]
04/08-12:59:32.544418 192.168.1.3 -> 192.168.1.2
ICMP TTL:64 TOS:0x0 ID:58668 IpLen:20 DgmLen:84 DF
Type:8  Code:0  ID:5123   Seq:13  ECHO
```

La regla con SID 384 estaba en el fichero */etc/snort/rules/icmp-info.rules*.

```
alert icmp $EXTERNAL_NET any -> $HOME_NET any (msg:"ICMP PING";
icode:0; itype:8; classtype:misc-activity; sid:384; rev:5;)
```

```
[**] [1:408:5] ICMP Echo Reply [**]
[Classification: Misc activity] [Priority: 3]
04/08-12:59:32.544506 192.168.1.2 -> 192.168.1.3
ICMP TTL:64 TOS:0x0 ID:28244 IpLen:20 DgmLen:84
Type:0  Code:0  ID:5123  Seq:13  ECHO REPLY
```

La regla con SID 408 estaba en el fichero */etc/snort/rules/icmp-info.rules*.

```
alert icmp $EXTERNAL_NET any -> $HOME_NET any (msg:"ICMP Echo Reply";
icode:0; itype:0; classtype:misc-activity; sid:408; rev:5;)
```

Para localizar las reglas hemos empleado el comando grep, tan solo es necesario decirle entre las comillas la cadena buscada en este caso el sid de la regla, en lugar de XXX se pone el SID a buscar. Al utilizar la opción "-r" realiza una busqueda en todos los ficheros del directorio.

```
sudo grep -r "sid:XXX" /etc/snort/rules
```

3 Definición de nuevas reglas

```
Type:8  Code:0  ID:5159  Seq:1  ECHO

[**] [1:10000001:1] Special ping [**]
[Priority: 0]
04/08-13:49:47.186519 192.168.1.3 -> 192.168.1.2
ICMP TTL:100 TOS:0x0 ID:61808 IpLen:20 DgmLen:228 DF
Type:8  Code:0  ID:5159  Seq:1  ECHO

[**] [1:408:5] ICMP Echo Reply [**]
```

Figure 3.1 : Alerta generada por la nueva regla.

Para activarla hemos enviado un ping de atacante a victima pero lo hemos modificado para que tuviese el tiempo de vida y tamaño buscados.

```
ping -t 100 -s 200 -c 1 192.168.1.2
```

4 Preprocesadores

```
[**] [1:1418:11] SNMP request tcp [**]
[Classification: Attempted Information Leak] [Priority: 2]
04/08-13:56:34.688210 192.168.1.3:38817 -> 192.168.1.2:161
TCP TTL:37 TOS:0x0 ID:13036 IpLen:20 DgmLen:44
******S* Seq: 0x84FF097F  Ack: 0x0  Win: 0x400  TcpLen: 24
TCP Options (1) => MSS: 1460
[Xref => http://cve.mitre.org/cgi-bin/cvename.cgi?name=2002-0013][Xref => http://c
://www.securityfocus.com/bid/4089][Xref => http://www.securityfocus.com/bid/4088]

[**] [1:1421:11] SNMP AgentX/tcp request [**]
[Classification: Attempted Information Leak] [Priority: 2]
04/08-13:56:34.695568 192.168.1.3:38817 -> 192.168.1.2:705
TCP TTL:54 TOS:0x0 ID:51288 IpLen:20 DgmLen:44
******S* Seq: 0x84FF097F  Ack: 0x0  Win: 0x400  TcpLen: 24
TCP Options (1) => MSS: 1460
[Xref => http://cve.mitre.org/cgi-bin/cvename.cgi?name=2002-0013][Xref => http://c
://www.securityfocus.com/bid/4089][Xref => http://www.securityfocus.com/bid/4088]
```

Figure 4.1 : Alerta con sfportscan activado.

Para activar el preprocesador arpspoof hemos incluido las siguientes lineas en el fichero */etc/snort/snort.conf*.

```
preprocessor arpspoof
preprocessor arpspoof_detect_host: 192.168.1.1 08:00:27:66:bf:ba
preprocessor arpspoof_detect_host: 192.168.1.2 08:00:27:1f:21:c9
preprocessor arpspoof_detect_host: 192.168.1.3 08:00:27:62:95:fc
```

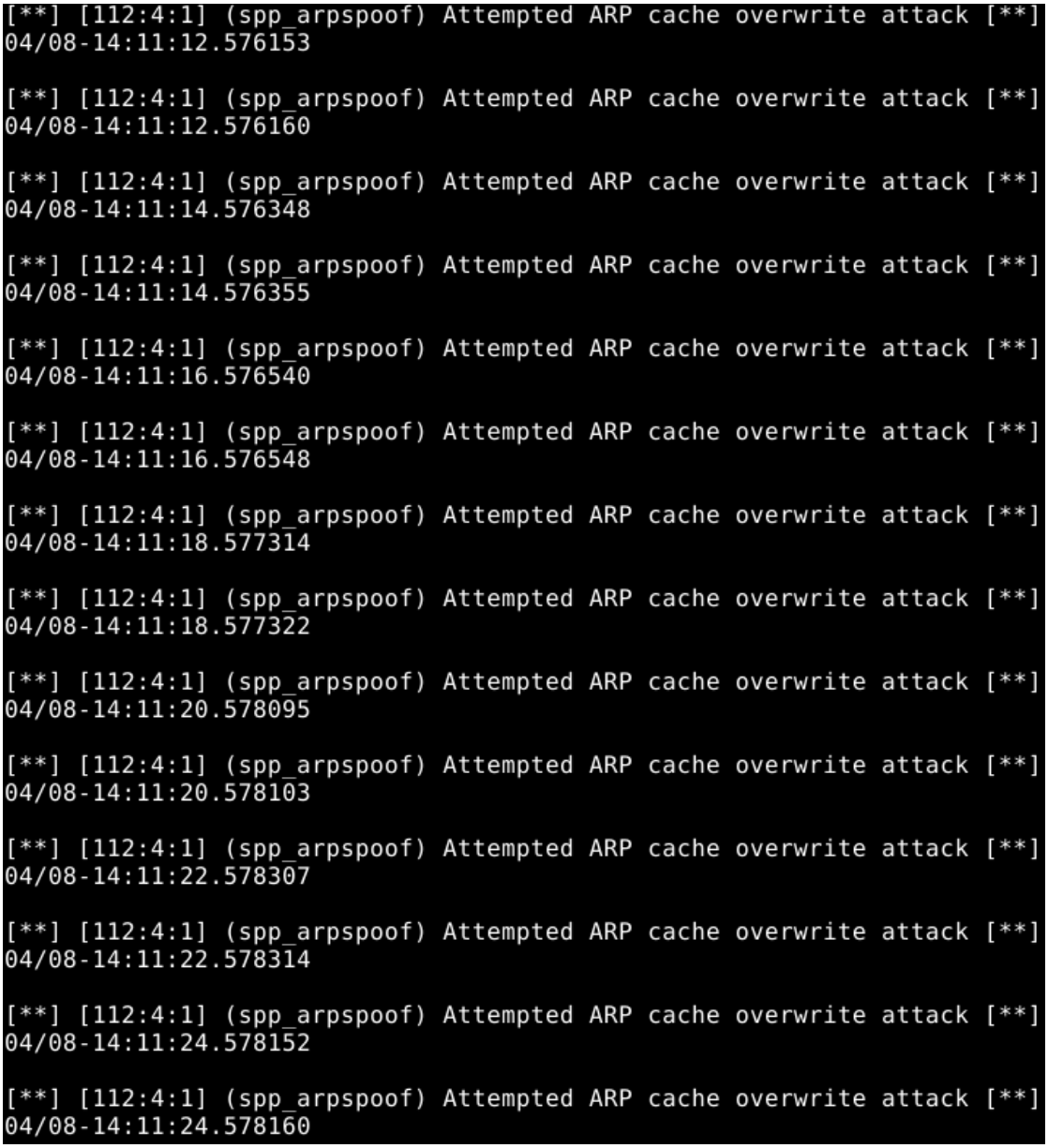

Figure 4.2 : Alerta con arpspoof activado.