SSI. Práctica 6.

Uso del escaner de vulnerabilidades OpenVAS y del detector de intrusiones SNORT.

Comesaña Figueiras, Rubén.

Fernández Díaz, Iago.

Paquete1

Regla de snort:

```
alert udp $EXTERNAL_NET any -> $HOME_NET 2140 (
                                        msg:"BACKDOOR DeepThroat 3.1 Connection attempt";
                                        content:"00";
                                        depth:2; reference:mcafee,98574;
                                         reference:nessus,10053;
                                         classtype:misc-activity;
                                         sid:1980;
                                         rev:4;)
```

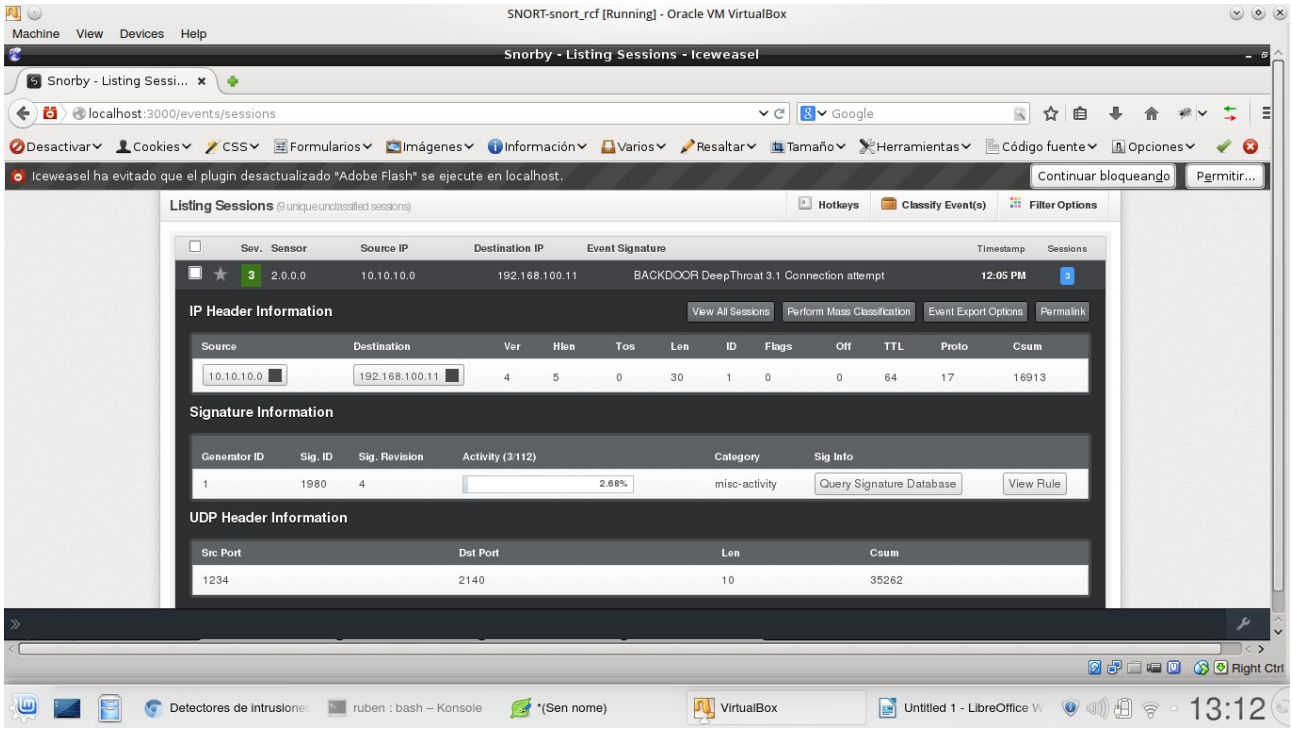
Esta regla provoca una alerta con mensaje " BACKDOOR DeepThroat 3.1 Connection attempt " cuando detecta un paquete con contenido "00" sobre el puerto UDP 2140 de la red local, procedente de cualquier otro puerto de una máquina con una IP de una red externa.

Creación del paquete 1

```
>>> ip1=IP()
>>> ip1.src="10.10.10.0"
>>> ip1.dst="192.168.100.11"
>>> udp1=UDP()
>>> udp1.sport=12345
>>> udp1.dport=2140
>>> payload1="00"
>>> paquete1=ip1/udp1/payload1
>>> send(paquete1)

>>> paquete1.show()
###[ IP ]###
  version= 4
  ihl= None
  tos= 0x0
  len= None
  id= 1
  flags=
  frag= 0
  ttl= 64
  proto= udp
  chksum= None
  src= 10.10.10.0
  dst= 192.168.100.11
  \options\
###[ UDP ]###
     sport= 1234
     dport= 2140
     len= None
     chksum= None
###[ Raw ]###
        load= '00'
```

Comprobaciones:




```
mysql> select * from signature;
+--------+-------------+-------------------------------------------------+-------------+---------+---------+---------+-------------
+
| sig_id | sig_class_id | sig_name                                        | sig_priority | sig_rev | sig_sid | sig_gid | events_count |
+--------+-------------+-------------------------------------------------+-------------+---------+---------+---------+-------------
+
|      1 |            1 | SNMP AgentX/tcp request                         |            2 |      11 |    1421 |       1 |            1 |
|      2 |            1 | SNMP request tcp                                |            2 |      11 |    1418 |       1 |            1 |
|      3 |            2 | ICMP PING undefined code                        |            3 |       8 |     365 |       1 |            5 |
|      4 |            2 | ICMP Echo Reply undefined code                  |            3 |       7 |     409 |       1 |            5 |
|      5 |            2 | ICMP PING                                       |            3 |       5 |     384 |       1 |            5 |
|      6 |            2 | ICMP Echo Reply                                 |            3 |       5 |     408 |       1 |            5 |
|      7 |            2 | ICMP Destination Unreachable Port Unreachable   |            3 |       7 |     402 |       1 |            5 |
|      8 |            1 | SCAN nmap XMAS                                  |            2 |       7 |    1228 |       1 |            5 |
|      9 |            3 | BAD-TRAFFIC same SRC/DST                        |            2 |       8 |     527 |       1 |           59 |
|     10 |         NULL | Prueba SSI 2014                                 |         NULL |       1 | 9000999 |       1 |            3 |
|     11 |            2 | BACKDOOR DeepThroat 3.1 Connection attempt      |            3 |       4 |    1980 |       1 |            3 |
+--------+-------------+-------------------------------------------------+-------------+---------+---------+---------+-------------
+
11 rows in set (0.00 sec)
```

Paquete 2

Regla de Snort:

```
alert udp $EXTERNAL_NET 3344 -> $HOME_NET 3345 (
                                        msg:"BACKDOOR Matrix 2.0 Client connect";
                                        content:"activate";
                                        reference:arachnids,83;
                                        classtype:misc-activity;
                                        sid:161;
                                        rev:4;)
```

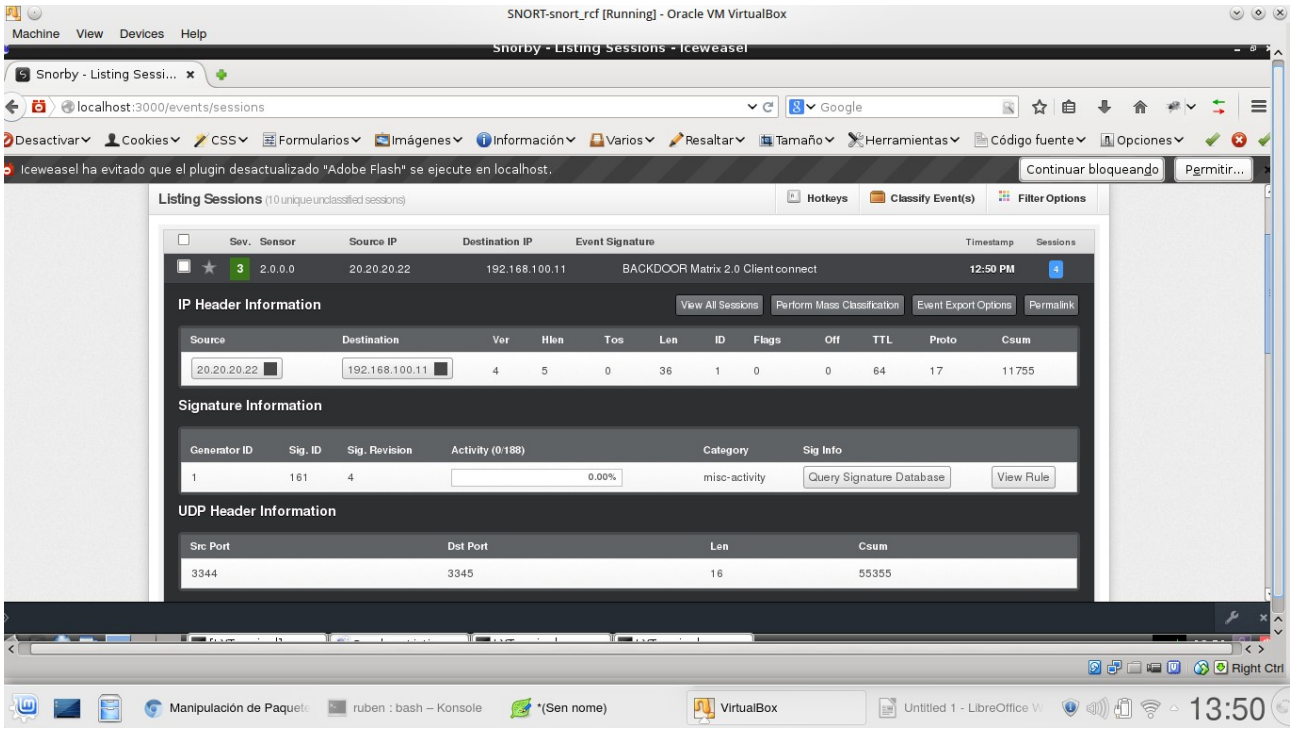
Esta regla muestra una alerta con el mensaje “BACKDOOR Matrix 2.0 Client connect”, cuando detecta el contenido “activate” en un paquete UDP que procede del puerto 3344 de una IP de una red externa y tiene como destino el puerto UDP 3345 de una máquina de la red local.

Creación del paquete 2:

```
>>> ip2=IP()
>>> ip2.src="10.10.10.0"
>>> ip2.dst="192.168.100.11"
>>> udp2=UDP()
>>> udp2.sport=3344
>>> udp2.dport=3345
>>> payload2="activate"
>>> paquete2=ip2/udp2/payload2
>>> send(paquete2)

>>> paquete2.show()
###[ IP ]###
  version= 4
  ihl= None
  tos= 0x0
  len= None
  id= 1
  flags=
  frag= 0
  ttl= 64
  proto= udp
  chksum= None
  src= 20.20.20.22
  dst= 192.168.100.11
  \options\
###[ UDP ]###
     sport= 3344
     dport= 3345
     len= None
     chksum= None
###[ Raw ]###
        load= 'activate'
>>>
```

Comprobaciones:




```
 sig_id | sig_class_id | sig_name                                          | sig_priority | sig_rev | sig_sid | sig_gid | events_count |
+--------+--------------+---------------------------------------------------+--------------+---------+---------+---------+--------------
+
|      1 |            1 | SNMP AgentX/tcp request                           |            2 |      11 |    1421 |       1 |            1 |
|      2 |            1 | SNMP request tcp                                  |            2 |      11 |    1418 |       1 |            1 |
|      3 |            2 | ICMP PING undefined code                          |            3 |       8 |     365 |       1 |            5 |
|      4 |            2 | ICMP Echo Reply undefined code                    |            3 |       7 |     409 |       1 |            5 |
|      5 |            2 | ICMP PING                                         |            3 |       5 |     384 |       1 |            5 |
|      6 |            2 | ICMP Echo Reply                                   |            3 |       5 |     408 |       1 |            5 |
|      7 |            2 | ICMP Destination Unreachable Port Unreachable     |            3 |       7 |     402 |       1 |            5 |
|      8 |            1 | SCAN nmap XMAS                                    |            2 |       7 |    1228 |       1 |            5 |
|      9 |            3 | BAD-TRAFFIC same SRC/DST                          |            2 |       8 |     527 |       1 |          142 |
|     10 |         NULL | Prueba SSI 2014                                   |         NULL |       1 | 9000999 |       1 |            3 |
|     11 |            2 | BACKDOOR DeepThroat 3.1 Connection attempt        |            3 |       4 |    1980 |       1 |            3 |
|     12 |            2 | BACKDOOR Matrix 2.0 Client connect                |            3 |       4 |     161 |       1 |            0 |
+--------+--------------+---------------------------------------------------+--------------+---------+---------+---------+--------------
+
```

Paquete 3

Regla de Snort:

```
alert udp $EXTERNAL_NET any -> $HOME_NET 69 (
                                msg:"TFTP NULL command attempt";
                                 content:"|00 00|";
                                depth:2;
                                 reference:bugtraq,7575;
                                classtype:bad-unknown;
                                sid:2339;
                                rev:2;)
```

Esta regla genera una alerta con mensaje TFTP NULL command attempt" cuando detecta un paquete UDP que tiene origen cualquier puerto UDP de una máquina de una de una red externa y tiene como destino el puerto 69 de una máquina de la red local, y cuyo contenido sea “|00 00|” en hexadecimal.

Creación del paquete 3:

```
>>> ip2=IP()
>>> ip2.src="10.10.10.0"
>>> ip2.dst="192.168.100.11"
>>> udp2=UDP()
>>> udp2.sport=3344
>>> udp2.dport=69
>>> payload2="\x00\x00"
>>> paquete2=ip2/udp2/payload2


>>> send(paquete3)


>>> paquete3.show()

###[ IP ]###
  version= 4
  ihl= None
  tos= 0x0
  len= None
  id= 1
  flags=
  frag= 0
  ttl= 64
  proto= udp
  chksum= None
  src= 10.10.10.0
  dst= 192.168.100.11
  \options\
###[ UDP ]###
     sport= netbios_ns
     dport= tftp
     len= None
     chksum= None
###[ Raw ]###
```

load= '\x00\x00'

Comprobaciones: