IT Security

Intrusion Detection System

Jérôme Chammartin
David Schneider

Class T3

Table of content

1 IDS

IDS or Intrusion Detection System works aside the firewall and help to eliminate attackers gaining access to the network. The IDS logs and denies unwanted traffic and send an alert message to a specified IP addresse if traffic has been detected which matches a configured signature.
We use also the term IPS or Intrusion Prevention System because the IDS reacts on suspicious activities by resetting the connection.

To verify the function of our IDS we use the linux application hping3 which is able to send custom TCP/IP packets. All the header fields can be modified.

2 Configuration

Router

```
Router> enable
Router# config term
Router(config)# ip http server
Router(config)# ip http authentication local
Router(config)# ip http secure-server

Router(config)# username sdm privilege 15 password 0 123456

Router(config)# line vty 0 4
Router(config-line)# privilege level 15
Router(config-line)# login local
Router(config-line)# transport input telnet ssh
Router(config-line)# exit

Router(config)# logging 160.98.30.82

Router(config)# interface FastEthernet0/0
Router(config-if)# ip address dhcp
Router(config-if)# no shutdown
```

After that we erased the existing OS and had put the new IOS on the Router.

Software

We are using the software SDM and Kiwi Syslogd. SDM is the Security Device Manager which checks the IPS and is able to make the modifications. Kiwi Syslogd is the server that receives the alarms/logs and represents it.

The following graphic shows the exchange between the SDM and the software Kiwi which configures the IPS using a web interface.

160.98.30.82	160.98.31.143	HTTP	POST /ios_web_exec/commandset HTTP/1.1 (application/x-www-form-urlencoded)
160.98.31.143	160.98.30.82	HTTP	HTTP/1.1 200 OK (text/plain)
160.98.30.82	160.98.31.143	HTTP	POST /ios_web_exec/commandset HTTP/1.1 (application/x-www-form-urlencoded)
160.98.31.143	160.98.30.82	HTTP	HTTP/1.1 200 OK (text/plain)
160.98.30.82	160.98.31.143	HTTP	POST /ios_web_exec/commandset HTTP/1.1 (application/x-www-form-urlencoded)
160.98.31.143	160.98.30.82	HTTP	HTTP/1.1 200 OK (text/plain)

3 Work

We installed the software SDM and Kiwi Syslogd and we configured the router as above.

The command **hping3 -a 192.168.1.1 160.98.31.143** pings the router with the public source address.

```
2008-10-07 11:05:13 Local7.Warning      160.98.31.143       713: *Oct  7 08:59:49.083:
%IPS-4-SIGNATURE: Sig:3040 Subsig:0 Sev:5 TCP NULL Packet [192.168.1.1:1285 -> 160.98.31.143:0]

2008-10-07 11:05:14 Local7.Warning      160.98.31.143       714: *Oct  7 08:59:50.087:
%IPS-4-SIGNATURE: Sig:3040 Subsig:0 Sev:5 TCP NULL Packet [192.168.1.1:1286 -> 160.98.31.143:0]

2008-10-07 11:05:15 Local7.Warning      160.98.31.143       715: *Oct  7 08:59:51.091:
%IPS-4-SIGNATURE: Sig:3040 Subsig:0 Sev:5 TCP NULL Packet [192.168.1.1:1287 -> 160.98.31.143:0]

2008-10-07 11:05:16 Local7.Warning      160.98.31.143       716: *Oct  7 08:59:52.095:
%IPS-4-SIGNATURE: Sig:3040 Subsig:0 Sev:5 TCP NULL Packet [192.168.1.1:1288 -> 160.98.31.143:0]
```

The packed had been dropped by the IPS and the warning has been logged. The signature 3040 which catches all the packets without any TCP flags set.

We tried to send a packet to the destination port 22 with the command **hping3 -p 22 -a 192.168.1.1 160.98.31.143**.

```
2008-10-07 11:01:46 Local7.Warning      160.98.31.143       708: *Oct  7 08:56:22.067:
%IPS-4-SIGNATURE: Sig:3040 Subsig:0 Sev:5 TCP NULL Packet [192.168.1.1:1888 -> 160.98.31.143:22]

2008-10-07 11:01:46 Local7.Warning      160.98.31.143       709: *Oct  7 08:56:23.063:
%IPS-4-SIGNATURE: Sig:3040 Subsig:0 Sev:5 TCP NULL Packet [192.168.1.1:1889 -> 160.98.31.143:22]

2008-10-07 11:01:48 Local7.Warning      160.98.31.143       710: *Oct  7 08:56:24.067:
%IPS-4-SIGNATURE: Sig:3040 Subsig:0 Sev:5 TCP NULL Packet [192.168.1.1:1890 -> 160.98.31.143:22]

2008-10-07 11:01:49 Local7.Warning      160.98.31.143       711: *Oct  7 08:56:25.075:
%IPS-4-SIGNATURE: Sig:3040 Subsig:0 Sev:5 TCP NULL Packet [192.168.1.1:1891 -> 160.98.31.143:22]

2008-10-07 11:01:50 Local7.Warning      160.98.31.143       712: *Oct  7 08:56:26.079:
%IPS-4-SIGNATURE: Sig:3040 Subsig:0 Sev:5 TCP NULL Packet [192.168.1.1:1892 -> 160.98.31.143:22]
```

Without any surprise the same signature had captured the packet. We can say that it didn't depend on the port at all, just on the flags.

As next step we created a new signature with the number 20000 which drops and alarms if the packet has the URG flag == 1.

The ping command **hping3 -U -a 192.168.1.1 160.98.31.143** has been used.

```
2008-10-07 11:12:41 Local7.Warning      160.98.31.143       779: *Oct  7 09:07:17.107:
%IPS-4-SIGNATURE: Sig:20000 Subsig:0 Sev:5 TCP NULL Packet private [192.168.1.1:1391 -> 160.98.31.143:0]

2008-10-07 11:12:42 Local7.Warning      160.98.31.143       780: *Oct  7 09:07:18.111:
%IPS-4-SIGNATURE: Sig:20000 Subsig:0 Sev:5 TCP NULL Packet private [192.168.1.1:1392 -> 160.98.31.143:0]

2008-10-07 11:12:43 Local7.Warning      160.98.31.143       781: *Oct  7 09:07:19.115:
%IPS-4-SIGNATURE: Sig:20000 Subsig:0 Sev:5 TCP NULL Packet private [192.168.1.1:1393 -> 160.98.31.143:0]

2008-10-07 11:12:44 Local7.Warning      160.98.31.143       782: *Oct  7 09:07:20.119:
%IPS-4-SIGNATURE: Sig:20000 Subsig:0 Sev:5 TCP NULL Packet private [192.168.1.1:1394 -> 160.98.31.143:0]

2008-10-07 11:12:45 Local7.Warning      160.98.31.143       783: *Oct  7 09:07:21.123:
%IPS-4-SIGNATURE: Sig:20000 Subsig:0 Sev:5 TCP NULL Packet private [192.168.1.1:1395 -> 160.98.31.143:0]

2008-10-07 11:12:46 Local7.Warning      160.98.31.143       784: *Oct  7 09:07:22.127:
%IPS-4-SIGNATURE: Sig:20000 Subsig:0 Sev:5 TCP NULL Packet private [192.168.1.1:1396 -> 160.98.31.143:0]

2008-10-07 11:12:47 Local7.Warning      160.98.31.143       785: *Oct  7 09:07:23.131:
%IPS-4-SIGNATURE: Sig:20000 Subsig:0 Sev:5 TCP NULL Packet private [192.168.1.1:1397 -> 160.98.31.143:0]

2008-10-07 11:12:48 Local7.Warning      160.98.31.143       786: *Oct  7 09:07:24.135:
%IPS-4-SIGNATURE: Sig:20000 Subsig:0 Sev:5 TCP NULL Packet private [192.168.1.1:1398 -> 160.98.31.143:0]
```

We can see that the signature 20000 worked well.

Furthermore we tried a ping with the destination address as source address.

```
2008-10-07 11:15:32 Local7.Warning      160.98.31.143       787: *Oct  7 09:10:07.927:
%IPS-4-SIGNATURE: Sig:1102 Subsig:0 Sev:5 Impossible IP packet [160.98.31.143:1927 -> 160.98.31.143:0]

2008-10-07 11:15:32 Local7.Warning      160.98.31.143       788: *Oct  7 09:10:07.931:
%IPS-4-SIGNATURE: Sig:3040 Subsig:0 Sev:5 TCP NULL Packet [160.98.31.143:1927 -> 160.98.31.143:0]

2008-10-07 11:15:33 Local7.Warning      160.98.31.143       789: *Oct  7 09:10:08.931:
%IPS-4-SIGNATURE: Sig:1102 Subsig:0 Sev:5 Impossible IP packet [160.98.31.143:1928 -> 160.98.31.143:0]

2008-10-07 11:15:33 Local7.Warning      160.98.31.143       790: *Oct  7 09:10:08.931:
%IPS-4-SIGNATURE: Sig:3040 Subsig:0 Sev:5 TCP NULL Packet [160.98.31.143:1928 -> 160.98.31.143:0]

2008-10-07 11:15:34 Local7.Warning      160.98.31.143       791: *Oct  7 09:10:09.935:
%IPS-4-SIGNATURE: Sig:1102 Subsig:0 Sev:5 Impossible IP packet [160.98.31.143:1929 -> 160.98.31.143:0]

2008-10-07 11:15:34 Local7.Warning      160.98.31.143       792: *Oct  7 09:10:09.935:
%IPS-4-SIGNATURE: Sig:3040 Subsig:0 Sev:5 TCP NULL Packet [160.98.31.143:1929 -> 160.98.31.143:0]

2008-10-07 11:15:35 Local7.Warning      160.98.31.143       793: *Oct  7 09:10:10.939:
%IPS-4-SIGNATURE: Sig:1102 Subsig:0 Sev:5 Impossible IP packet [160.98.31.143:1930 -> 160.98.31.143:0]

2008-10-07 11:15:35 Local7.Warning      160.98.31.143       794: *Oct  7 09:10:10.939:
%IPS-4-SIGNATURE: Sig:3040 Subsig:0 Sev:5 TCP NULL Packet [160.98.31.143:1930 -> 160.98.31.143:0]

2008-10-07 11:15:36 Local7.Warning      160.98.31.143       795: *Oct  7 09:10:11.943:
%IPS-4-SIGNATURE: Sig:1102 Subsig:0 Sev:5 Impossible IP packet [160.98.31.143:1931 -> 160.98.31.143:0]

2008-10-07 11:15:36 Local7.Warning      160.98.31.143       796: *Oct  7 09:10:11.943:
%IPS-4-SIGNATURE: Sig:3040 Subsig:0 Sev:5 TCP NULL Packet [160.98.31.143:1931 -> 160.98.31.143:0]
```

This was a very interesting experiment because we had two signatures which captured this packet. The signature 3040 we already saw before (no flags set) and the signature 1102 which indicates a „Impossible IP packet".

We had to find out the used port by the syslog server. Therefore we had different possibilities, the netstat command, into the Kiwi software preferencies, or by capturing the packet with wireshark.

```
 6393 388.652378  160.98.31.143    160.98.30.82     Syslog   LOCAL7.WARNING: 710: *Oct  7 08:56:24.067:

Frame 6375 (170 bytes on wire, 170 bytes captured)
Ethernet II, Src: Cisco_3d:fb:3c (00:1a:e2:3d:fb:3c), Dst: IntelCor_56:2d:b6 (00:13:20:56:2d:b6)
Internet Protocol, Src: 160.98.31.143 (160.98.31.143), Dst: 160.98.30.82 (160.98.30.82)
User Datagram Protocol, Src Port: 49867 (49867), Dst Port: syslog (514)
Syslog message: LOCAL7.WARNING: 709: *Oct  7 08:56:23.063: %IPS-4-SIGNATURE: Sig:3040 Subsig:0 Sev:5 TCP
```

We can see here that the UDP port 514 (syslog) is used.