Sample: Snort rules development

The following is an effort to show how the development of exploit specific signatures can be achieved.

Reason: In the context of the diploma thesis “Conception for deployment of Intrusion Detection Systems in a corporate network” some of the goals are to examine

- how attack detection in IDS works in general
- how attack signatures can be developed
- what kind of skills are required by IDS personnel
- how various products support development of own custom signatures

Used tools:

- Tcpdump
- Ethereal
- Snort

Attack: Sub7 Gold 2.1 backdoor program

Testing environment:
Two PCs connected through a 100mbit/s hub.
Address of infected PC: 192.168.0.12
Address of attacking PC:192.168.0.11

The snort sensor has no IP address assigned for his sniffing interface, that is also connected to the hub. Snort logs its alerts to a MySQL database on a dedicated server.
ACID is used as frontend for event analysis on the database server.

Procedure:
Capturing sub7 traffic with tcpdump:
Tcpdump –s 1500 –i eth1 –w /var/sub7_x
where x is a number that is incremented with each capture.

The most relevant ethernet frames are presented in this document.
The data that was found to be typical for this kind of attack is marked in red.
This typical data was extracted in order to form a signature for sub7 connections.

 counter.spy@gmx.de

```
Frame 8 (60 on wire, 60 captured)
    Arrival Time: Mar 14, 2002 12:55:23.905415000
    Time delta from previous packet: 0.000253000 seconds
    Time relative to first packet: 0.006758000 seconds
    Frame Number: 8
    Packet Length: 60 bytes
    Capture Length: 60 bytes
Ethernet II
    Destination: 00:e0:29:3d:c5:38 (SMC_3d:c5:38)
    Source: 00:e0:29:1f:f9:f2 (SMC_1f:f9:f2)
    Type: IP (0x0800)
    Trailer: 51A551
Internet Protocol, Src Addr: 192.168.0.12 (192.168.0.12), Dst Addr:
192.168.0.11 (192.168.0.11)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 43
    Identification: 0x2c06
    Flags: 0x04
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 128
    Protocol: TCP (0x06)
    Header checksum: 0x4d5f (correct)
    Source: 192.168.0.12 (192.168.0.12)
    Destination: 192.168.0.11 (192.168.0.11)
Transmission Control Protocol, Src Port: 6666 (6666), Dst Port: 1313
(1313), Seq: 8031842, Ack: 3633166041
    Source port: 6666 (6666)
    Destination port: 1313 (1313)
    Sequence number: 8031842
    Next sequence number: 8031845
    Acknowledgement number: 3633166041
    Header length: 20 bytes
    Flags: 0x0018 (PSH, ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 1... = Push: Set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 8760
    Checksum: 0x3a63 (correct)
Data (3 bytes)

0000  50 57 44                                          PWD
```

 counter.spy@gmx.de

```
Frame 9 (60 on wire, 60 captured)
    Arrival Time: Mar 14, 2002 12:55:24.085276000
    Time delta from previous packet: 0.179861000 seconds
    Time relative to first packet: 0.186619000 seconds
    Frame Number: 9
    Packet Length: 60 bytes
    Capture Length: 60 bytes
Ethernet II
    Destination: 00:e0:29:1f:f9:f2 (SMC_1f:f9:f2)
    Source: 00:e0:29:3d:c5:38 (SMC_3d:c5:38)
    Type: IP (0x0800)
    Trailer: 000000000000
Internet Protocol, Src Addr: 192.168.0.11 (192.168.0.11), Dst Addr:
192.168.0.12 (192.168.0.12)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 40
    Identification: 0x8b50
    Flags: 0x04
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 128
    Protocol: TCP (0x06)
    Header checksum: 0xee17 (correct)
    Source: 192.168.0.11 (192.168.0.11)
    Destination: 192.168.0.12 (192.168.0.12)
Transmission Control Protocol, Src Port: 1313 (1313), Dst Port: 6666
(6666), Seq: 3633166041, Ack: 8031845
    Source port: 1313 (1313)
    Destination port: 6666 (6666)
    Sequence number: 3633166041
    Acknowledgement number: 8031845
    Header length: 20 bytes
    Flags: 0x0010 (ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 0... = Push: Not set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 17517
    Checksum: 0xac8d (correct)
```

 counter.spy@gmx.de

```
Frame 10 (61 on wire, 61 captured)
    Arrival Time: Mar 14, 2002 12:55:26.235819000
    Time delta from previous packet: 2.150543000 seconds
    Time relative to first packet: 2.337162000 seconds
    Frame Number: 10
    Packet Length: 61 bytes
    Capture Length: 61 bytes
Ethernet II
    Destination: 00:e0:29:1f:f9:f2 (SMC_1f:f9:f2)
    Source: 00:e0:29:3d:c5:38 (SMC_3d:c5:38)
    Type: IP (0x0800)
Internet Protocol, Src Addr: 192.168.0.11 (192.168.0.11), Dst Addr:
192.168.0.12 (192.168.0.12)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 47
    Identification: 0x8b51
    Flags: 0x04
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 128
    Protocol: TCP (0x06)
    Header checksum: 0xee0f (correct)
    Source: 192.168.0.11 (192.168.0.11)
    Destination: 192.168.0.12 (192.168.0.12)
Transmission Control Protocol, Src Port: 1313 (1313), Dst Port: 6666
(6666), Seq: 3633166041, Ack: 8031845
    Source port: 1313 (1313)
    Destination port: 6666 (6666)
    Sequence number: 3633166041
    Next sequence number: 3633166048
    Acknowledgement number: 8031845
    Header length: 20 bytes
    Flags: 0x0018 (PSH, ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 1... = Push: Set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 17517
    Checksum: 0x6b51 (correct)
Data (7 bytes)

0000  50 57 44 73 75 62 37                                PWDsub7
```

```
Frame 11 (115 on wire, 115 captured)
    Arrival Time: Mar 14, 2002 12:55:26.236402000
    Time delta from previous packet: 0.000583000 seconds
    Time relative to first packet: 2.337745000 seconds
    Frame Number: 11
    Packet Length: 115 bytes
    Capture Length: 115 bytes
Ethernet II
    Destination: 00:e0:29:3d:c5:38 (SMC_3d:c5:38)
    Source: 00:e0:29:1f:f9:f2 (SMC_1f:f9:f2)
    Type: IP (0x0800)
Internet Protocol, Src Addr: 192.168.0.12 (192.168.0.12), Dst Addr:
192.168.0.11 (192.168.0.11)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 101
    Identification: 0x2d06
    Flags: 0x04
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 128
    Protocol: TCP (0x06)
    Header checksum: 0x4c25 (correct)
    Source: 192.168.0.12 (192.168.0.12)
    Destination: 192.168.0.11 (192.168.0.11)
Transmission Control Protocol, Src Port: 6666 (6666), Dst Port: 1313
(1313), Seq: 8031845, Ack: 3633166048
    Source port: 6666 (6666)
    Destination port: 1313 (1313)
    Sequence number: 8031845
    Next sequence number: 8031906
    Acknowledgement number: 3633166048
    Header length: 20 bytes
    Flags: 0x0018 (PSH, ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 1... = Push: Set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 8753
    Checksum: 0xba26 (correct)
Data (61 bytes)

0000  63 6f 6e 6e 65 63 74 65 64 2e 20 31 32 3a 35 30   connected. 12:50
0010  2e 33 38 20 2d 20 4d e4 72 7a 20 31 34 2c 20 32   .38 - M.rz 14, 2
0020  30 30 32 2c 20 44 6f 6e 6e 65 72 73 74 61 67 2c   002, Donnerstag,
0030  20 76 65 72 73 69 6f 6e 3a 20 32 2e 31              version: 2.1
```

 counter.spy@gmx.de

Suggested Snort Rules:

```
alert tcp $HOME_NET any -> $EXTERNAL_NET any \
      (msg:"Possible BACKDOOR Sub7 21 traffic"; fragbits: D+; flags: AP; \
      content: "PWD"; offset: 0; depth: 10; nocase; \
      classtype: misc-activity;)

alert tcp $EXTERNAL_NET any -> $HOME_NET any \
      msg:"Possible BACKDOOR Sub7 21 traffic"; fragbits: D+; flags: AP; \
      content: "PWD"; offset: 0; depth: 10; nocase; \
      classtype: misc-activity;)

alert tcp $HOME_NET any -> $EXTERNAL_NET any \
      msg:"Possible BACKDOOR Sub7 21 traffic"; fragbits: D+; flags: AP; \
      content: "|76 65 72 73 69 6f 6e 3a 20 32 2e 31|"; \
      offset: 40; depth: 40; nocase; classtype: misc-activity;)
```

These rules have been tested successfully in a testing environment.
All three rules matched every time when a sub7 connection was initiated.
In order to minimize false positives you could add typical portnumbers to the rules,
such as 27374, but be aware that the sub7 server port can be customized, as you can see in the example.

The next step is to let snort run with these rules on a production network in order to see if it generates many false positives.

 counter.spy@gmx.de