



UNIVERSITY  
OF TASMANIA

Faculty of Commerce

School of Information Systems



# Intrusion Detection: Forensic Computing Insights from a Case Study on SNORT

Vlasti Broucek & Paul Turner



# Disclaimer

- It is not the intention of this paper to evaluate the SNORT IDS. No comparisons are being made concerning the relative merits of SNORT against any other free or commercially available IDS systems and all the conclusions made in this paper would apply to IDS in general.
- This case study is based on the data collected by running SNORT as a part of “normal” business operations, although some adjustments have been made to ensure consistent data.



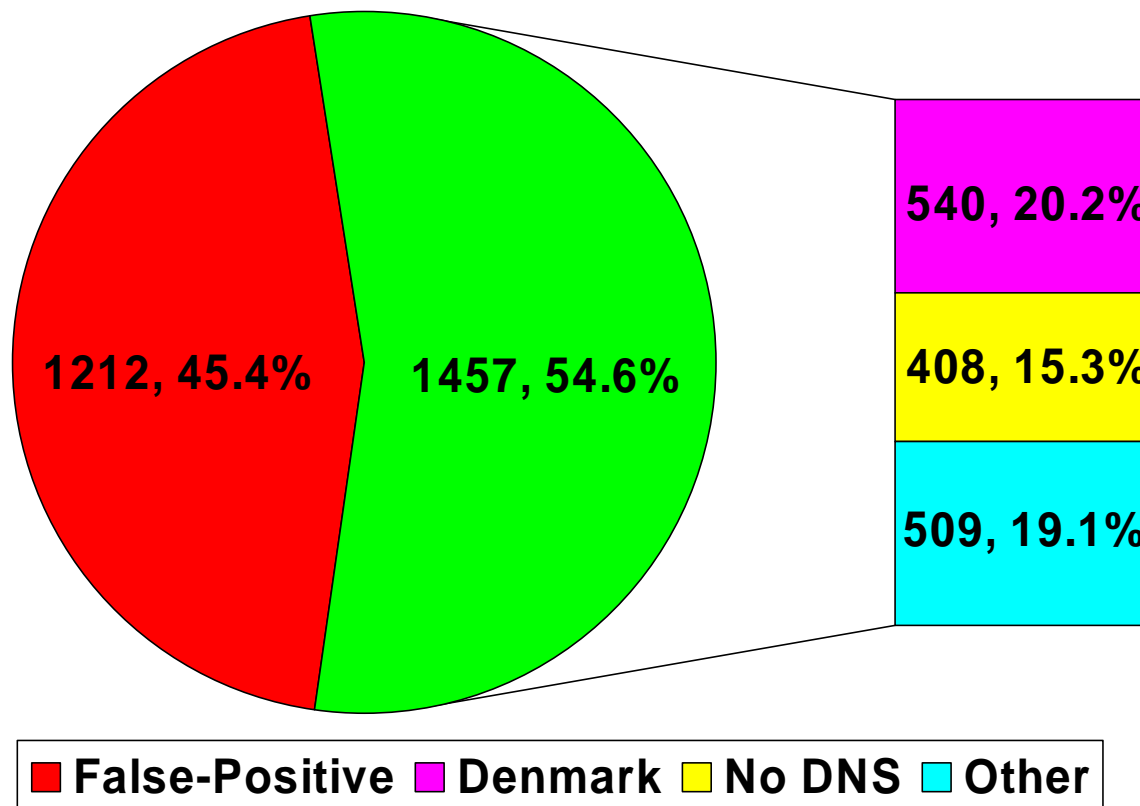
# ARE IDS (and alerts they generate) GOOD FOR ANYTHING?

Hervé Debar

(IBM IDS research Labs, France Télécom R&D, NESS, CAMDIER)

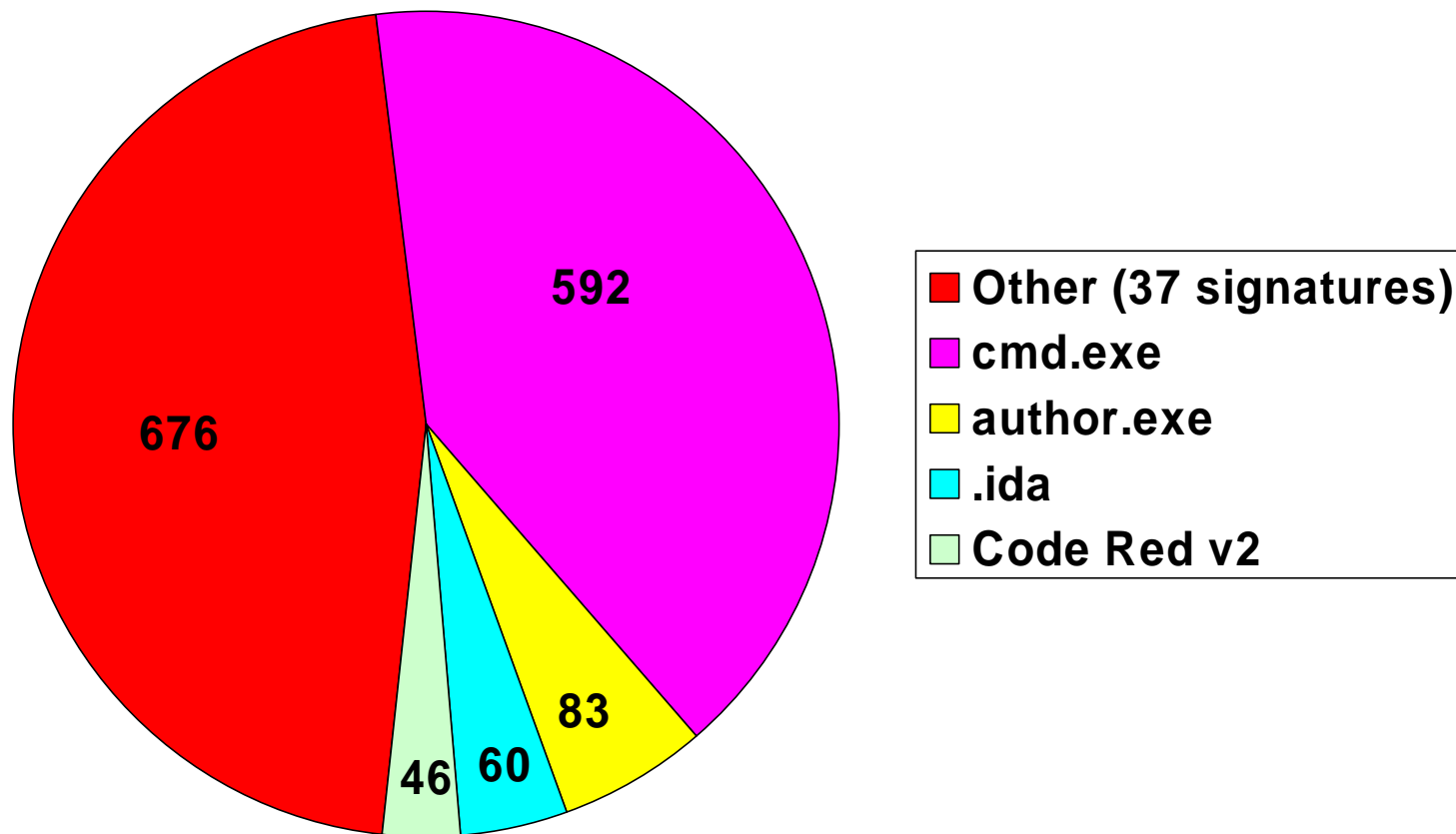


# Statistics – False Positive v Positive





# Statistics – Signatures





# Problems with Alerts – Too Many

- Positives
- False-positives
  - Set-up – location, configuration etc
  - Rules tuning
    - Trusted systems
    - Two rules with different priorities?
  - Remove irrelevant rules?
    - Is alert about IIS attack on Apache based server really positive?



# More Problems with Alerts

- Incorrect information
  - Bugs, decoy methods
- Not enough information
  - Log all packets?
    - Size
    - Noise
- Knowledge, tools & time



# BUGS

```
[**] [1:485:2] ICMP Destination Unreachable (Communication  
Administratively Prohibited) [**]  
[Classification: Misc activity] [Priority: 3]  
08/17-05:15:22.029533 XXX.XXX.XXX.XXX -> YYY.YYY.YYY.YYY  
ICMP TTL:242 TOS:0x0 ID:54572 IpLen:20 DgmLen:56  
Type:3 Code:13 DESTINATION UNREACHABLE: ADMINISTRATIVELY  
PROHIBITED,PACKET FILTERED_  
** ORIGINAL DATAGRAM DUMP:  
YYY.YYY.YYY.YYY:0 -> ZZZ.ZZZ.ZZZ.ZZZ:0  
UDP TTL:126 TOS:0x0 ID:7936 IpLen:20 DgmLen:71  
Len: 51  
** END OF DUMP
```

**BUG in SNORT – should be :137 -> :53**



```

232161 2002-08-17 05:15:22.029533000 198.110.188.1 131.217.35.6 ICMP Destination unreachable
#Ethernet II, Src: 00:04:9b:2f:e3:fc, Dst: 00:30:c1:0a:82:6b
  Destination: 00:30:c1:0a:82:6b [Hewlett-0a:82:6b]
  Source: 00:04:9b:2f:e3:fc [Cisco_2F:e3:fc]
  Type: IP (0x0800)
  Trailer: 93A64071
#Internet Protocol, Src Addr: 198.110.188.1 (198.110.188.1), Dst Addr: 131.217.35.6 (131.217.35.6)
  Version: 4
  Header length: 20 bytes
  #Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
    0000 00.. = Differentiated Services Codepoint: Default (0x00)
    .... 00.. = ECN-Capable Transport (ECT): 0
    .... 00.. = ECN-CE: 0
  Total Length: 56
  Identification: 0xd52c
  #Flags: 0x00
    .0.. = Don't fragment: Not set
    ..0. = More fragments: Not set
  Fragment offset: 0
  Time to live: 242
  Protocol: ICMP (0x01)
  Header checksum: 0xca48 (correct)
  Source: 198.110.188.1 (198.110.188.1)
  Destination: 131.217.35.6 (131.217.35.6)
#Internet Control Message Protocol
  Type: 3 (Destination unreachable)
  Code: 13 (Communication administratively filtered)
  Checksum: 0x556e (correct)
#Internet Protocol, Src Addr: 131.217.35.6 (131.217.35.6), Dst Addr: 148.61.1.10 (148.61.1.10)
  Version: 4
  Header length: 20 bytes
  #Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
    0000 00.. = Differentiated Services Codepoint: Default (0x00)
    .... 00.. = ECN-Capable Transport (ECT): 0
    .... 00.. = ECN-CE: 0
  Total Length: 71
  Identification: 0x1f00
  #Flags: 0x00
    .0.. = Don't fragment: Not set
    ..0. = More fragments: Not set
  Fragment offset: 0
  Time to live: 126
  Protocol: UDP (0x11)
  Header checksum: 0xa17f (correct)
  Source: 131.217.35.6 (131.217.35.6)
  Destination: 148.61.1.10 (148.61.1.10)
#User Datagram Protocol, Src Port: netbios-ns (137), Dst Port: domain (53)
  Source port: netbios-ns (137)
  Destination port: domain (53)
  Length: 51
  Checksum: 0xa693
0000 00 35 c1 0a 82 6b 05 24 9b 2f e3 fc 08 00 45 00  .0...k.../....6.
0010 00 38 05 2c 00 00 f3 81 ca 48 09 6e bc 01 83 d9  .8.....H.n...
0020 23 05 03 00 55 6e 00 00 00 00 45 00 00 47 1e 00  #.....E..0..
0030 00 00 fe 11 e1 7f 81 09 23 06 94 1d 01 0a 00 89  #..0..#.E...
0040 00 35 00 33 a6 93 93 a6 4b 71                    -.5.....Hq

```



# Not Enough Information

```
[**] [1:485:2] ICMP Destination Unreachable (Communication  
Administratively Prohibited) [**]  
[Classification: Misc activity] [Priority: 3]  
08/17-05:15:22.029533 XXX.XXX.XXX.XXX -> 131.217.35.6  
ICMP TTL:242 TOS:0x0 ID:54572 IpLen:20 DgmLen:56  
Type:3 Code:13 DESTINATION UNREACHABLE: ADMINISTRATIVELY  
PROHIBITED,PACKET FILTERED_
```

```
** ORIGINAL DATAGRAM DUMP:
```

```
131.217.35.6:137 -> ZZZ.ZZZ.ZZZ.ZZZ:53  
UDP TTL:126 TOS:0x0 ID:7936 IpLen:20 DgmLen:71  
Len: 51  
** END OF DUMP
```



# Not Enough Information

- NOP86 on antivirus update downloads
- Reverse NDS look-up not working
- Collected Data Not Enough to Identify Intruder/Activity



# Knowledge and Tools

## tethereal

```

Frame 226 2002-08-17 05:15:22.0295 XXX.XXX.XXX.XXX -> YYY.YYY.YYY.YYY ICMP Destination
unreachable
0000 00 30 c1 0a 82 6b 00 04 9b 2f e3 fc 08 00 45 00 .0...k.../....E.
0010 00 38 d5 2c 00 00 f2 01 ca 48 XX XX XX XX YY YY .8.,.....H.n....
0020 YY YY 03 0d 55 6e 00 00 00 00 45 00 00 47 1f 00 #...Un....E..G..
0030 00 00 7e 11 e1 7f 83 d9 23 06 ZZ ZZ ZZ ZZ 00 89 ..~.....#..=....
0040 00 35 00 33 a6 93 93 a6 4b 71 .5.3....Kq

```

## tcpdump

```

05:15:22.029533 0:4:9b:2f:e3:fc 0:30:c1:a:82:6b 0800 74: XXX.XXX.XXX.XXX > YYY.YYY.YYY.YYY:
icmp: host ZZZ.ZZZ.ZZZ.ZZZ unreachable - admin prohibited filter
0x0000 4500 0038 d52c 0000 f201 ca48 XXXX XXXX E..8.,.....H.n..
0x0010 YYY YYY 030d 556e 0000 0000 4500 0047 ..#...Un....E..G
0x0020 1f00 0000 7e11 e17f 83d9 2306 ZZZZ ZZZZ .....~.....#..=..
0x0030 0089 0035 0033 a693 93a6 4b71 ...5.3....Kq

05:15:22.029533 XXX.XXX.XXX.XXX > YYY.YYY.YYY.YYY: icmp: host ZZZ.ZZZ.ZZZ.ZZZ unreachable -
admin prohibited filter for YYY.YYY.YYY.YYY 137 > ZZZ.ZZZ.ZZZ.ZZZ 53: 37798 updataA+$
[b2&3=0x4b71] [1537a] [1579q] [513n] [11013au][domain] (ttl 126, id 7936, len 71) (ttl 242,
id 54572, len 56)

```



# ARE IDS (and alerts they generate) GOOD FOR ANYTHING?



# Forensic Computing Perspective

- Previous research claims/hypotheses
  - ✓ The data sets collected may be flawed, erroneous or already have been tampered with
  - ✓ IDS may collect only partial data sets
    - IDS deployment subject to privacy regulations
- Inconsistent results from different tools



# Privacy Issues

- Collect Everything Approach?
  - All the time - **YES**
  - When needed – it is late to start collecting after something has already started
- Collected Data May Violate Privacy Laws
  - regular traffic (http, telnet, ftp, SMTP etc)



# Encryption

- NIDS cannot detect malicious traffic that is encrypted
  - Store keys on IDS machine?
- HIDS or AIDS need to be deployed



# Conclusion

- Previous Claims/Hypotheses Confirmed
- Shown Need for
  - Set-up, tuning
  - Monitoring
    - Console
    - Log file rotation system
  - Knowledge, Training



# Conclusion

- Side effects
  - Traffic that was not supposed to be seen on switched network
    - Overflow in CISCO tables
  - Noise traffic – IPX, AppleTalk broadcasts, CiscoWorks, HP JetAdmin, Novell NDPS and much more



UNIVERSITY  
OF TASMANIA

Faculty of Commerce

School of Information Systems



# SPONSORSHIP ANYONE?