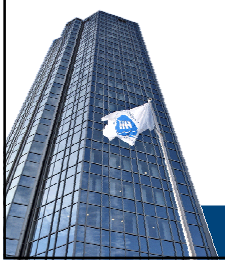
Nätverksanalys



Wecksten, Mattias
2009

Trafikanalys

- Identifiera misstänkt trafik
- Spela upp eller återskapa sessioner
- Tolka data

- (360)

Wecksten, Mattias
2009

Verktyg

- tcptrace
- snort
- tcpIflow
- Ethereal (Wireshark)

- (360)

Wecksten, Mattias
2009

Generera sessioner

- tcptrace
- Analys av datadump – generera en översikt.
- Jämför med diskavbild – Autopsy
- (362)

tcptrace

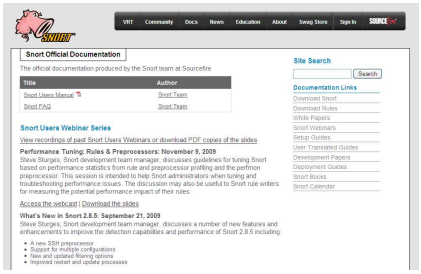
```
Beluga:/Users/mani> tcptrace tigris.dmp

1 arg remaining, starting with 'tigris.dmp'
Ostermann's tcptrace -- version 6.4.5 -- Fri Jun 13, 2003

87 packets seen, 87 TCP packets traced
elapsed wallclock time: 0:00:00.037900, 2295 pkts/sec analyzed
trace file elapsed time: 0:00:12.180796
TCP connection info:
    1: pride.cs.ohiou.edu:54735 - elephus.cs.ohiou.edu:ssh (a2b) 30> 30< (complete)
    2: pride.cs.ohiou.edu:54736 - a17-112-152-32.apple.com:http (c2d) 12> 15< (complete)
```


tcptrace (contd.)

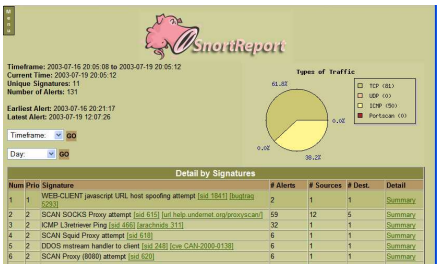
1	Session number
172.16.1.128	Source IP address, or the IP address that sent the SYN packet to begin the session
1640	Source port
172.16.1.7	Destination IP address
80	Destination port

(e2f)	Shorthand for the session, with the source referred to as e and the destination as f
62	Number of packets sent by the source computer
93	Number of packets sent by the destination computer
(reset)	How the connection was closed; complete indicates a graceful close

snort



SnortReport



FTP-analys

- (370-374)

SSH-analys

- (374-376)

Ethereal (Wireshark)

- (376-377)

Upside-Down-Ternet

- http://www.ex-parrot.com/~pete/upside-down-ternet.html