De Domain Name Service als Intrusion Detection System

Antoine Schonewille - talitwan@os3.nl
Dirk-Jan van Helmond - dirkjan@os3.nl

Universiteit van Amsterdam
System and Network Engineering - OS3

Agenda

- Inleiding
- Doel van het Project
- Theorie
- Werkwijze
- Resultaten
- Conclusie

Inleiding

- Research Project 1
- SURFnet
  - Behoefte aan duidelijkere netwerkmonitoring
  - Als aanvulling op IDS en NetFlow stats
  - Aan de hand van DNS informatie

Doel van het Project

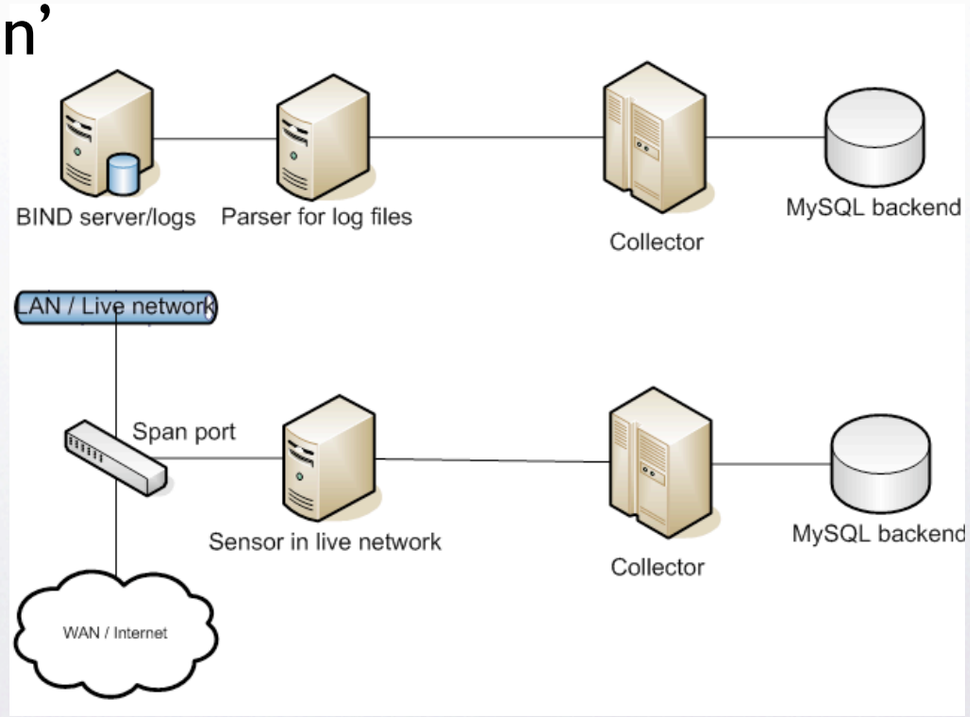
- Mogelijkheden van DNS statistieken
- Detectie
  - Vinden van geïnfecteerde computers
- Monitoren van gedrag
  - Extra (DNS) informatie over bot(net) verzamelen

Theorie

- Contact bots en controllers via domain names
- Er MOET een DNS request gedaan worden
- Afvangen en analyse DNS requests = detectie?

Werkwijze

- Live netwerk bij klant van SURFnet (ca. 6000 thuisaansluitingen)
- DNS requests verzamelen in database
  - BIND query logs parsen
  - TCP/UDP dst 53 ‘eavesdroppen’
- Data analyse
  - Statistiek
  - Correlatie
  - Baseline



Resultaten

- Triggers op bekende domain names
  (i.e. 00.devoid.us, home.played.co.uk, 00.spazbox.net etc.)
  - Direct resultaten, bijna geen false positives
  - Up-to-date domain names lijst via security mailing lists

```
+-----+--------------+-------+-------------------+
| cnt | srcip        | qtype | query             |
+-----+--------------+-------+-------------------+
| 183 | 10.10.34.59  | A     | home.played.co.uk |
| 178 | 10.10.35.118 | A     | home.played.co.uk |
| 171 | 10.10.35.44  | A     | home.played.co.uk |
| 136 | 10.10.36.53  | A     | home.played.co.uk |
| ... | ...          | ...   | ...               |
+-----+--------------+-------+-------------------+
```

Resultaten (cont'd)

- Top 10 opgevraagde domains -- opvallend:
  - Meestal verwijderde domains
  - 'Lost' bots zonder negative cache
- Top 10 clients -- opvallend:
  - +1000 queries per IP per uur

```
+------+----------------------------+
| cnt  | query                      |
+------+----------------------------+
| 5291 | mail.omgdidyougotpwned.info |
| 3474 | 46.10.239.60.in-addr.arpa  |
| 2763 | flh1adf046.kng.mesh.ad.jp  |
|  890 | 00.spazbox.net             |
|  ... | ...                        |
+------+----------------------------+
```

- Vaak overeenkomsten tussen de meeste opgevraagde domains en de clients die ze opvragen.

Resultaten (cont'd)

- Afwijkende qtype in network access layer
  - MX -- Open Relay/Spam bots
  - AXFR/IXFR -- Hacking/Hackbots

Resultaten (cont'd)

- Correlatie met NetFlow data
  - Match gebaseerd op IP én timestamp
  - Andere clients die contact hebben met dezelfde domain names

```
+---------------------+-------------+---------+-------+
| flowstart           | srcip       | packets | bytes |
+---------------------+-------------+---------+-------+
| 2006-01-27 19:06:25 | 10.10.44.142 |       1 |   140 |
+---------------------+-------------+---------+-------+

+---------------------+-------------+-------------+-------+----------------------+
| time                | srcip       | nameserver  | qtype | query                |
+---------------------+-------------+-------------+-------+----------------------+
| 2006-01-27 19:06:25 | 10.10.44.142 | 192.87.36.36 | A     | suksa.mujaskax33.com |
+---------------------+-------------+-------------+-------+----------------------+
```

Interessant

- Baselining
  - Startup van systemen
  - Gedrag van netwerken

Conclusie

- DNS als IDS bruikbaar
    - Data eenvoudig verzamelbaar
        - Analyse levert goede resultaten op
- Correlatie met verschillende bronnen
- Detectie middels DNS goede aanvulling

Future Research

- Automatisering
  - Detectie middels thresholds
  - Notificatie aan beheerders
  - Quarantaine / evt. Black holing?

Slot

- Paper: http://www.os3.nl/~dirkjan/RP1/DNS_IDS_Paper.pdf

- Presentatie: http://www.os3.nl/~dirkjan/RP1/DNS_IDS.pdf

- Vragen?