tcpdump DNS Filter Rules for Fun and Profit

Shane Kerr <shane@ca.afilias.info>
Afilias Limited

Contents

- Why? What?
- DNS tools
- Captured Packets
- DNS Packet
- QNAME/QTYPE/QCLASS Matching
- Example Rule
- Other Notes

Why? What?

- We get lots of traffic
  - Impractical to store all queries
  - Difficult to look at that much data
  - Special case for us: NAT into cluster
- Use a pcap filter to capture DNS packets for:
  - A specific query ID
  - A specific QNAME/QTYPE/QCLASS (such as "ID.SERVER/TXT/CH")

DNS Tools

- Tools do exist to filter and capture DNS
- dnscap
  - No filtering based on type/class
  - Failed me once... ;)
- tshark
  - Part of Wireshark
  - Not installed everywhere
- Others?

Captured Packets

- pcap files store:
  - capture information (such as time)
  - Ethernet packet
- Ethernet packets for DNS have:
  - Ethernet header
  - IP header
  - UDP header (we're only looking at UDP)
  - DNS packet

DNS Packet

- 2 bytes: query ID
- 2 bytes: QR, OPCODE, AA, TC, RD, RA, Z, RCODE
- 2 bytes: QDCOUNT (query count)
- 2 bytes: ANCOUNT (answer count)
- 2 bytes: NSCOUNT (authority count)
- 2 bytes: ARCOUNT (additional count)
- N bytes: queries, answers, authority, additional records
- *Note:* IPv4 header lengths vary, but tcpdump gives a udp array. So, udp[8] and udp[9] are the query id of a DNS packet.

QNAME/QTYPE/ QCLASS Matching

- Each query is variable length:
  - QNAME/QTYPE/QCLASS is N/2/2 bytes
    - To match QTYPE or QLCASS, you must match a specific name, like “hostname.bind”
- QNAME is an encoded version of the name:

  “foo.bar.example”

  0x03 “foo” 0x03 “bar” 0x07 “example” 0x00
- DNS is case-insensitive, tcpdump cannot be

Example Rule

```
(udp[20] == 2) and
  ((udp[21] == 105) or (udp[21] == 73)) and
  ((udp[22] == 100) or (udp[22] == 68)) and
(udp[23] == 6) and
  ((udp[24] == 115) or (udp[24] == 83)) and
  ((udp[25] == 101) or (udp[25] == 69)) and
  ((udp[26] == 114) or (udp[26] == 82)) and
  ((udp[27] == 118) or (udp[27] == 86)) and
  ((udp[28] == 101) or (udp[28] == 69)) and
  ((udp[29] == 114) or (udp[29] == 82)) and
(udp[30] == 0) and
(udp[31] == 0) and (udp[32] == 16) and
(udp[33] == 0) and (udp[34] == 3)
```

“id”

“server”

Type: TXT (16)

Class: CH (3)

Other Notes I

- Answers copy the query section, so filtering on question also gets associated reply (but be careful when mixing with rules for specific source/destination IP and port)

- Using udp[] does not work with IPv6, and there is no udp6[] rule.
  - IPv6 headers are fixed length, so ip6[40] is the same as udp[0] in IPv6

Other Notes II

- Looking at EDNS0 is tricky
  - In additional section of query, which means offset depends on query contents
  - Can't write a simple rule to look at DO bit

Final Page

- You can build your own rules at:

  http://www.time-travellers.org/dns-tcpdump/

- Questions/Comments?