DnsÜberNOOBer – DNS enumeration on steroids!

Presented by Jaco van Heerden, Ruxcon, 21 November 2010

whoami

- 12 Years in IT Security
- Started IT sec via company firewall
- Moved on to IT Sec consulting
- Focused on security testing

DNS footprint

The crux of it…

DNS Enumeration is:

- Exploring a DNS domain
- Discovering as much information as possible

Discover = Enumerate

DNS footprint

Why???

DNS information represents:

- Who
- What
- Relationships and context

Hacker + DNS info = **Uncovering Targets**

Pentester + DNS info = **Informed, Productive testing**

DNS footprint

Why I (have to) do it…

- Back in 5 BDC

- Client gets “Internet”

- ISP very happy; provides large netblock

- Client worried about getting hacked

- Buys super expensive firewall

- Client wants a pentest

- Pentester armed with:
  - No info
  - Dial-up modem
  - Cheap and nasty coffee

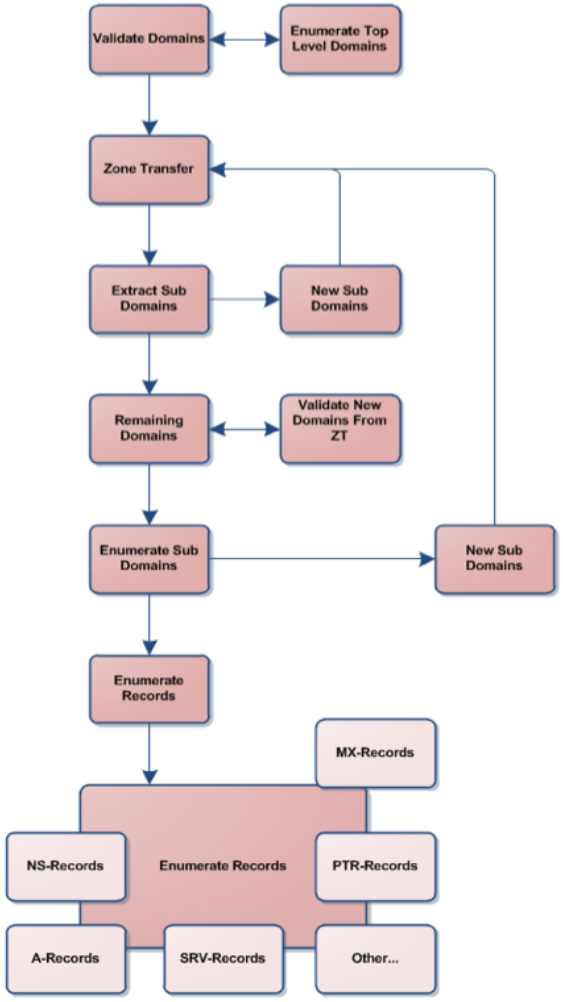
- Large attack surface

= **SHORTCUT**
(targeted approach)

DNS footprint

How?

DNS footprint



- Validate domains
  - Top level domain enumeration
- Zone transfer
  - Extract sub domains
    - Zone transfer
    - Rinse & repeat
- Remaining domains
  - Validate any new domains
  - Enumerate:
    - New sub domains
      - Rinse & repeat
    - Record types of interest
      - NS, MX, A, PTR etc.

Overview

DNS footprint

Ingredients

- Accuracy
- Speed
- Automate
- Which questions to ask
- When to ask them
- Next step/decision

Encapsulates DNS enumeration methodology

Console based tool

- .Net 2.0 / Mono 1.2.3 or higher
- Great for running in virtual console (headless)
- Disclaimer: May induce childbirth – consult physician

Super duper threading

Progress bar

Pet friendly

Work in Progress

DOWNLOAD HERE

www.dnsfootprint.com

Video

My Cousin Thready Kruger

Tools

(Learning to Bake Code)

My experiences with:

- Perl
- .Net / Mono
- Python
- Other…

- Alphons van der Heijden
  Kick Ass DNS resolver for .NET
  http://www.codeproject.com/KB/IP/DNS_NET_Resolver.aspx

DNS footprint

STEP 1: Validate

What?

- If (exist) {…}
  - ✓ Collect name server data
  - ○ Wildcard?

How to:

- Check for NS records
- Is domain a wildcard?

E.g. does <someRandomNo>unique text.domain (X 2) resolve to the same IP?

- Collect, expand (process), store
  - ○ NS IP's & associated domains

DNS footprint

STEP 1.666: Enumerate Top Level Domains

What?

- Seek target domain in:
  - cTLD & gTLD's
- Confirm relationship
  - Wait a minute!
  - Other related domains…?
- Recommendation:
  - Separate from DNS Enum

How to:

- Compile TLD list
- Add target domain
- Use techniques from validation
- Validate relationship to target domain

DNS footprint

TOP LEVEL DOMAINS: Flies in the Soup

Watch Out!

- Relationship frequently not obvious
- Exceptions = very difficult automation
  - False positives
- Reliable methods are limited
  - E.g. whois
- No silver bullet (at the moment)

STEP 2: Zone Transfer

What?

- NS data (Step 1)
- Attempt zone transfer
- Reverse zones anyone?
- Decision:
  Continue ZT's for remaining NS?

How to:

- Basic rocket science…
- Try AXFR for every NS!

DNS footprint

ZONE TRANSFER: Flies in the Soup

Watch Out!

- Dodgy DNS servers vs. DNS clients
- Dodgy DNS servers vs. programming libraries / API's
- Dodgy DNS servers vs. dnsfootprint

Video

DOWNLOAD HERE

www.dnsfootprint.com

Slipping your DNS client a Roofy

THANK YOU

- Red Wine
- Chris Bradley, Wynand Viljoen & Jarrod Loidl
- Red Wine & Wines with a reddish colour

DNS footprint

STEP 3: Process Zone Transfer Data

What?

- Expand records
  - NS, MX, MB,
  - MG, MR, AFSDB
  - Collect records of interest
- Massage data
  - Pick output format

How to:

- BFF = threading
- Expand records so that you can:
  - Keep state
  - Use data later during if/else
- However get rid of the rest
  - Send to output, free memory (Willy)
- Format NOW!

DNS footprint

```
NA;HINFO;cat1924-west.hubs.[redacted];NA;CPU=CISCO OS=1924EN
NA;HINFO;cat5505-east.hubs.[redacted];NA;CPU=CISCO OS=5505
NA;HINFO;cat5509-west.hubs.[redacted];NA;CPU=CISCO OS=5509
NA;HINFO;eastups.hubs.[redacted];NA;CPU=APC OS=UPS
NA;HINFO;westups.hubs.[redacted];NA;CPU=APC OS=UPS
NA;HINFO;abiseq.[redacted];NA;CPU=Mac OS=MacOS
NA;HINFO;abiseqpr.[redacted];NA;CPU=HP OS=1600CM
NA;HINFO;accfx980.[redacted];NA;CPU=Epson OS=FX980
NA;HINFO;acclaser4m.[redacted];NA;CPU=HP OS=HP4M
NA;HINFO;accsq2550.[redacted];NA;CPU=Epson OS=LQ2550
NA;HINFO;acomm.[redacted];NA;CPU=DEC OS=DECUNIX
NA;HINFO;allenmac.[redacted];NA;CPU=Mac OS=MacOS
NA;HINFO;ashton.[redacted];NA;CPU=MAC OS=MACOS
NA;HINFO;asio.[redacted];NA;CPU=PC OS=SunOS
NA;HINFO;batyocatyo.[redacted];NA;CPU=PC OS=Debian
NA;HINFO;biomatters.[redacted];NA;CPU=PC OS=WinXP
NA;HINFO;biospec.[redacted];NA;CPU=SGI OS=IRIX
NA;HINFO;biosym.[redacted];NA;CPU=SUN OS=BLADE
NA;HINFO;blake.[redacted];NA;CPU=PC OS=WIN95
NA;HINFO;bradley.[redacted];NA;CPU=PC OS=NTWKS
NA;HINFO;brind.[redacted];NA;CPU=PC OS=NTWKS
:
```

DNS footprint

STEP 4: Extract Sub Domains

What?

- From ZT
  - Analyze NS records
  - Look for sub domains
- ZT sub domains!
- Rinse & repeat
- Validate remaining!

How to:

- Simple quantum physics ☺
- If (current record = NS)
  - Compare domain data with current domain
  - If (same as current domain)
    - IGNORE
  - Else (subdomain)

DNS footprint

Video

The Missing Link

STEP 5: Enumerate Sub Domains

What?

- Want wordlist or two
  - Some light fuzzing
- Watch out for wildcards
- Initial domain validation now **mandatory**

How to:

- You're doing…
  - Domain validation
- Input = wordlist
  - And using list to create variations
- Still look out for (new) wildcards!

DNS footprint

STEP 6: New Sub Domains?

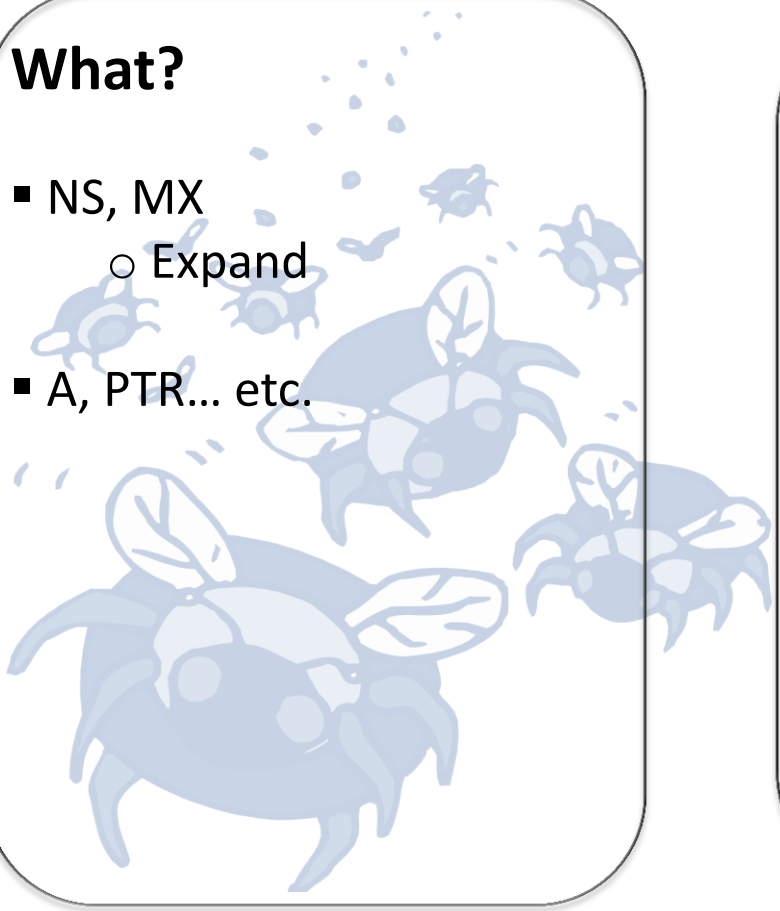
What?

- Add it back to mixture
  - Zone transfer
    - Enum more sub domains
- Decision:
  - *Continue enumerating sub domains?*

STEP 7: Enumerate Records

What?

- NS, MX
  - Expand
- A, PTR… etc.



How to:

- Again: Threading = BFF
- The usual records:
  - NS, MX = Expand
  - A = wordlist + variations
- *Wildcard domains still a pain in the butt*
- PTR
  - Start, stop numeric values

THANK YOU

- Charles Gillman
- + Charles's Red wine & cigars ☺

DNS footprint

ENUMERATE RECORDS: Flies in the Soup

Watch Out!

- Wildcard domains (A-Records)
  - Round robin responses from DNS server

Video

Putting it all together

Video

Zone transfer with feeling

Questions?

References

- http://everything2.com/title/CPU+history%253A+A+timeline+of+microprocessors
- http://www.iana.org
- http://www.codeproject.com/KB/IP/DNS_NET_Resolver.aspx
- http://www.darkoperator.com/blog/2009/4/3/dns-recon-tool-written-in-ruby.html
- http://code.google.com/p/dnsenum/
- http://ha.ckers.org/fierce/

DNS footprint