

reconnaissance



context

dit document beschijft een stappenplan voor reconnaissance uitgaand van een domein ahv enkele eenvoudige basiscommando's.

belangrijker dan de tools is de methodologie: *tools zijn er om ons te helpen, niet om voor ons te denken!*

gebruikte commando's

- dig
- whois
- curl
- recon-ng

dns

- zoek de (web)server waarop je target actief is: `dig <domein> +short`
- zoek de naam van die server (vaak heb je immers met (shared) hosting te maken): `dig -x <ipadres>`
- zoek de DNS server(s) voor de server: `dig <domein> ns +short`
om de authoritative server (soa) te vinden: `dig <domein> soa +short`
- zoek de mailserver voor het domein: `dig <domein> mx +short`

whois

- zoek wanneer (en door wie) het domein geregistreerd werd: `whois <domein>`
- voor Belgische sites is het nuttig het domein op de website van dnsbelgium.be op te zoeken. Je krijgt er nl ook details ivm de registrant te zien.
- `whois --verbose <domeinnaam>` toont welke whois server gebruikt wordt.
Dit verandert naar gelang de landcode (.be, .fr, .nl, ...)
voorbeeld:

```
whois --verbose louscorner.be
Using server whois.dns.be.
Query string: "louscorner.be"
```

curl

- verbind met de server: `curl -v <domein>`
hieruit leer je onder andere:
 - ip adres
 - server software
 - of er standaard op poort 80 (of redirect naar poort 443) antwoord komt.

voorbeeld

dns

```
dig louscorner.be +short
**5.134.5.195**
dig -x 5.134.5.195 +short
**linweb486.webhosting.be.**
dig louscorner.be ns +short
**ns3.combell.net.
ns4.combell.net.**
dig louscorner.be mx +short
**50 mx.backup.mailprotect.be.
10 mx.mailprotect.be.**
```

whois

```
whois louscorner.be
**Domain: louscorner.be
Status: NOT AVAILABLE
Registered: Thu Nov 12 2020
Registrant:
    Not shown, please visit www.dnsbelgium.be for webbased whois.
Registrar Technical Contacts:
    Organisation: EasyHost®
    Language: nl
    Phone: +32.92187901
Registrar:
    Name: EasyHost®
    Website: http://www.easyhost.be
Nameservers:
    ns1.easyhost.be
    ns2.easyhost.be
    ns3.easyhost.be
Keys:
    keyTag:35940 flags:KSK protocol:3 algorithm:ECDSAP256SHA256
    pubKey:Ss8vIBIfq96pzfS/VyGgKuVpfeHl9956RrXqTN9SKWHNJ8KaFwzMeN6p3hZ+/waak+PVX
    5IqxIP07KNq/7pxdQ==
```

Flags:

Please visit www.dnsbelgium.be for more info.**

curl

```
curl -v louscorner.be
* Expire in 5 ms for 1 (transfer 0x55b673fceb0)
* Expire in 7 ms for 1 (transfer 0x55b673fceb0)
*   Trying 5.134.5.195...
* TCP_NODELAY set
* Expire in 149989 ms for 3 (transfer 0x55b673fceb0)
* Expire in 200 ms for 4 (transfer 0x55b673fceb0)
* Connected to louscorner.be (5.134.5.195) port 80 (#0)
> GET / HTTP/1.1
> Host: louscorner.be
> User-Agent: curl/7.64.0
> Accept: */*
>
< HTTP/1.1 301 Moved Permanently
< Server: nginx
< Date: Thu, 27 Jan 2022 13:26:06 GMT
< Content-Type: text/html
< Content-Length: 162
< Connection: keep-alive
< Location: https://louscorner.be/
<
<html>
<head><title>301 Moved Permanently</title></head>
<body>
<center><h1>301 Moved Permanently</h1></center>
<hr><center>nginx</center>
</body>
</html>
* Connection #0 to host louscorner.be left intact
```

meer info

[linux](#), [digital forensics](#), [dns](#), [dig](#), [curl](#), [whois](#)

From:

<https://louslab.be/> - **Lou's lab**

Permanent link:

https://louslab.be/doku.php?id=digital_forensics:reconnaissance

Last update: **2024/11/16 18:14**

