



DNS Based OSINT Techniques for Product and Service Discovery

Speaker: Rishi (@rxerium)

Date: 23rd April 2026

Event: BSides Prague

2026



whoami



Senior Security Researcher based in London specialising in vulnerability research, attack surface management, threat intelligence, OSINT and risk management, dedicated to strengthening cyber resilience through proactive discovery and defence.

Rishi

Senior Security Researcher
@ KYND



LinkedIn



Twitter / X

The Realm of DNS Records

Act as the
"address book" of
the internet

DNS

Maps domain names to
IP addresses

A DNS record type for storing
text data

TXT

Email security
(SPF, DKIM,
DMARC)

CNAME

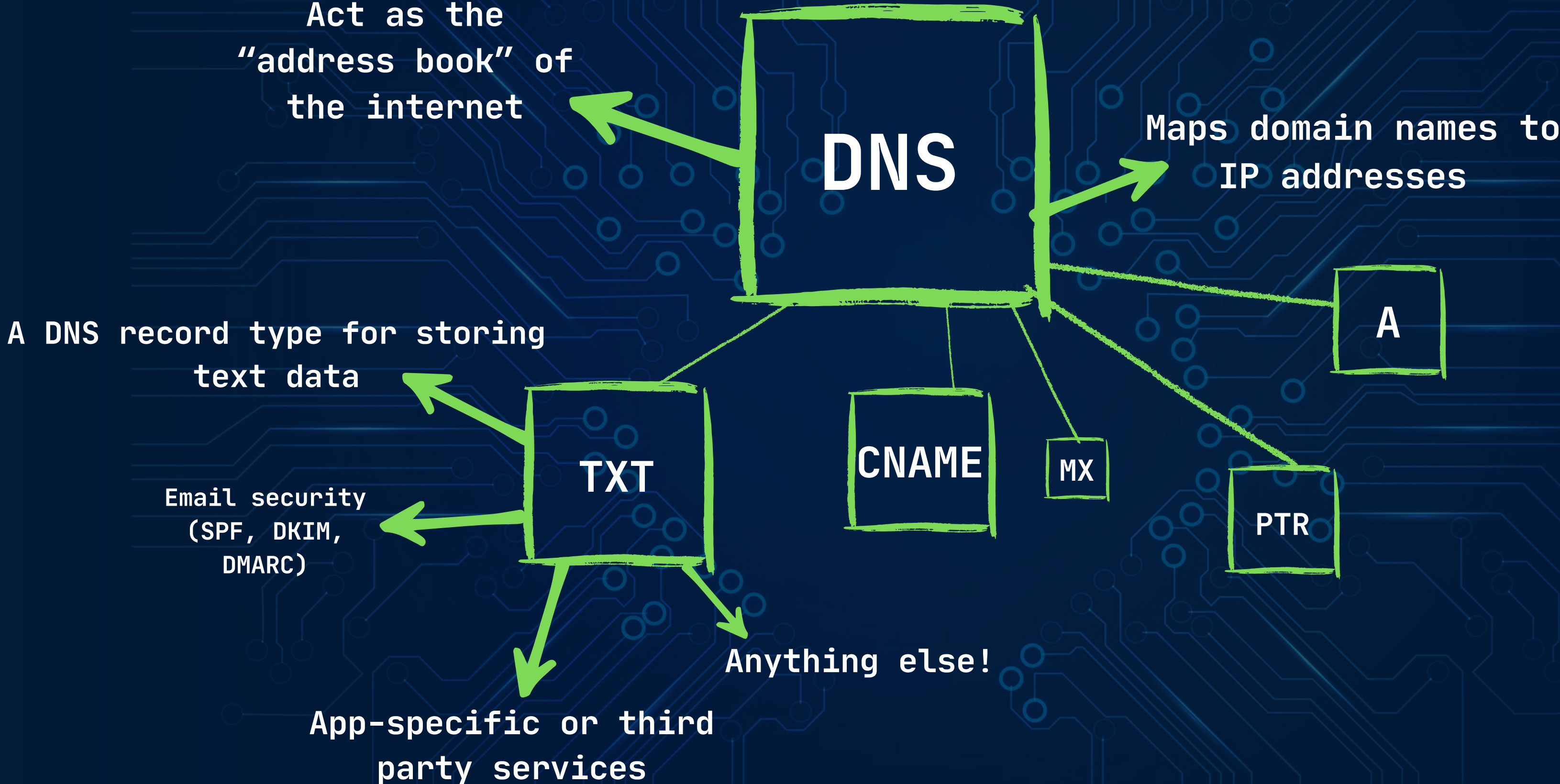
MX

A

PTR

Anything else!

App-specific or third
party services



Example TXT Records

```
> echo adobe.com | dnsx -txt -re -silent
```

```
adobe.com [TXT] [openai-domain-verification=dv-xsmu3zewiau4l5v23bd1l0ts]  
adobe.com [TXT] [_globalsign-domain-verification=lnj0izgjup0bosg7lasjuwlkcoksamz2emkst9_cus]  
adobe.com [TXT] [atlassian-domain-verification=9uyxhbbyogbk9b1ain6fhelo/cg08ihvd7rwduadq8ivehyffecc6gtaxw3kwshw]  
adobe.com [TXT] [google-site-verification=iwlts5bv60rglzcktgxcltsunlb9ct_09-pevxid2o8]  
adobe.com [TXT] [cisco-ci-domain-verification=6e22d6f101dd96dc12fabfe843ff4e6748b9f7a89af1ff342476b923f01e4292]  
adobe.com [TXT] [drift-domain-verification=502160a86dc2f7411dec54f019b785a7010eb9f38a6152011c1be40b89f68e9b]
```

Domain

Record
Type

Service / Product

Verification String

Salesloft Drift Supply Chain Attack

- Salesloft Drift was breached in August / September 2025
- Exploited stolen OAuth tokens from Salesloft's Drift app were used to access and steal Salesloft data
- Over 700 companies were breached (Cloudflare, Workday, Elastic)

Salesloft Drift Detection via TXT Records



```
~ → cat input.txt | dnsx -silent -txt -re | grep "drift"  
adobe.com [TXT] [drift-domain-verification=ce77053dc2d9b73c71437d5afda3b6d06fbc34a1b0e4527fe81c55e0d99ca4b4]  
workday.com [TXT] [drift-domain-verification=c27c30cb5d3220cb0eb600eb65e1e6cec4f6d879afcce75a77d530854d500d00]  
cloudflare.com [TXT] [drift-domain-verification=f037808a26ae8b25bc13b1f1f2b4c3e0f78c03e67f24cefdd4ec520efa8e719f]  
netapp.com [TXT] [drift-domain-verification=52b9f655153f557dfa494e77ee44158246fd173da5fe107a371597dfafa3de06a]
```

Why is this important?

- Prioritise threat hunting
- Assess third-party risk by understanding shared supply chain exposure
- Accelerate incident response through proactive detection

How do I run this myself?

Amass

An OWASP flagship project -
In-depth attack surface
mapping and asset discovery
framework

Amass
OWASP®

Nuclei

Fast, community-driven
vulnerability scanning tool





Demo