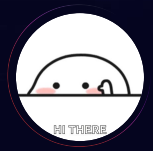
Hardly Strictly Security

Recon Round Table



Dhiyaneshwaran
AppSec Researcher
@DhiyaneshDK

Agenda

- What is Recon ?
- How to Perform Recon with PD Tools ?
- Tips & Tricks
- Live Demo
- Questionnaires

Subfinder

subfinder -d projectdiscovery.io -v -recursive -all -max-time 30 -timeout 50 -rl 1

```
enterpriseenrollment.projectdiscovery.io
blog.projectdiscovery.io
defcon.projectdiscovery.io
api.projectdiscovery.io
scheduler-prod.api.projectdiscovery.io
projectdiscovery.io
interact.projectdiscovery.io
enterpriseregistration.projectdiscovery.io
security.projectdiscovery.io
policies.projectdiscovery.io
login.projectdiscovery.io
cio83685.projectdiscovery.io
[INF] Found 62 subdomains for projectdiscovery.io in 11 seconds 364 milliseconds
```

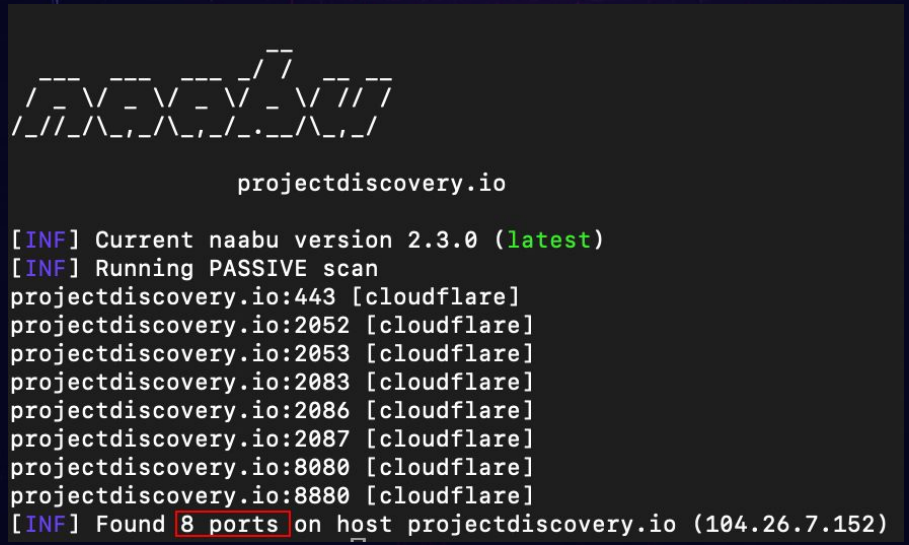
AlterX

subfinder -d projectdiscovery.io | alterx -en -silent | dnsx -t 1000

```
[INF] Enumerating subdomains for projectdiscovery.io
[INF] Found 63 subdomains for projectdiscovery.io in 3 seconds 741 milliseconds
[INF] Generated 48786 permutations in 0.0556s
api-dev.projectdiscovery.io
api.dev.projectdiscovery.io
api.projectdiscovery.io
auth.projectdiscovery.io
blog.projectdiscovery.io
chaos-data.projectdiscovery.io
chaos.projectdiscovery.io
```


Naabu

```
naabu -host projectdiscovery.io -passive -ec -cdn -c 5 -rate 500 -verify
```



DnsX

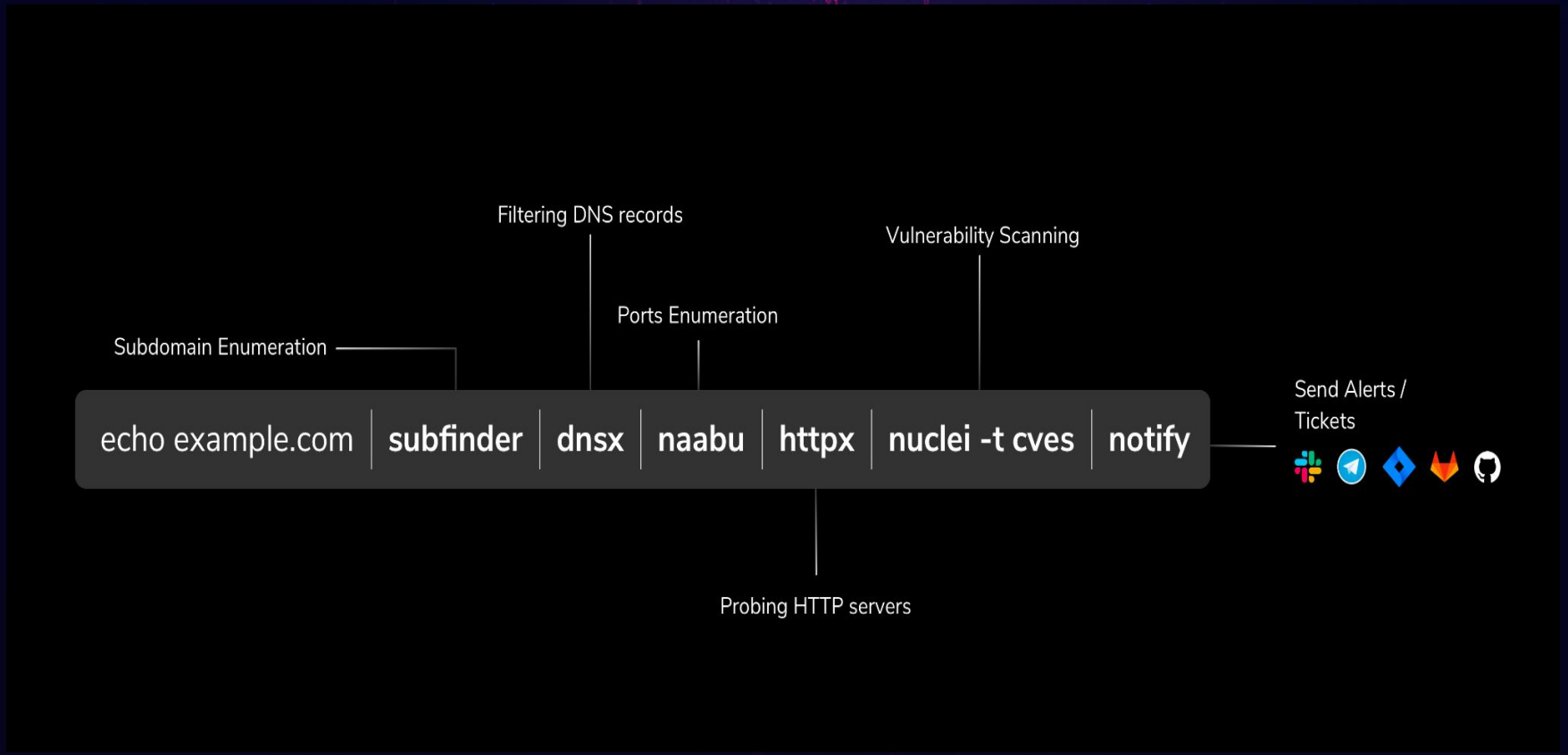
echo projectdiscovery.io | dnsx -recon -asn -cdn -t 20

```
projectdiscovery.io [AAAA] [2606:4700:20::ac43:4ad6]  [AS13335, cloudflarenet, US]
projectdiscovery.io [AAAA] [2606:4700:20::681a:698]  [AS13335, cloudflarenet, US]
projectdiscovery.io [MX] [aspmx.l.google.com]  [AS13335, cloudflarenet, US]
projectdiscovery.io [MX] [alt1.aspmx.l.google.com]  [AS13335, cloudflarenet, US]
projectdiscovery.io [MX] [alt2.aspmx.l.google.com]  [AS13335, cloudflarenet, US]
projectdiscovery.io [MX] [alt3.aspmx.l.google.com]  [AS13335, cloudflarenet, US]
projectdiscovery.io [MX] [alt4.aspmx.l.google.com]  [AS13335, cloudflarenet, US]
projectdiscovery.io [NS] [alexandra.ns.cloudflare.com]  [AS13335, cloudflarenet, US]
projectdiscovery.io [NS] [otto.ns.cloudflare.com]  [AS13335, cloudflarenet, US]
projectdiscovery.io [SOA] [alexandra.ns.cloudflare.com]  [AS13335, cloudflarenet, US]
projectdiscovery.io [SOA] [dns.cloudflare.com]  [AS13335, cloudflarenet, US]
```


HttpX

httpx -sc -location -title -server -td -method -cdn -t 5 -rl 10 -http2 -vhost

```
https://api-dev.projectdiscovery.io [404] [] [GET] [404 Not Found] [] [http2] [google] [HSTS]
https://api.dev.projectdiscovery.io [200] [] [GET] [] [cloudflare] [vhost] [http2] [cloudflare] [Cloudflare,HSTS]
https://asn.projectdiscovery.io [404] [] [GET] [] [] [vhost] [http2] [google] [HSTS]
https://auth.projectdiscovery.io [404] [] [GET] [] [cloudflare] [vhost] [http2] [cloudflare] [Cloudflare,HSTS]
https://blog.projectdiscovery.io [200] [] [GET] [ProjectDiscovery.io | Blog] [openresty] [vhost] [http2] [fastly] [Ghost:5.8
https://431pxcngpdba88wc4r46.projectdiscovery.io [404] [] [GET] [Squarespace - Domain Not Claimed] [Squarespace] [http2] [Sq
https://api.projectdiscovery.io [200] [] [GET] [] [cloudflare] [vhost] [http2] [cloudflare] [Cloudflare,HSTS]
https://clerk.projectdiscovery.io [200] [] [GET] [] [cloudflare] [vhost] [http2] [cloudflare] [Cloudflare,Cloudflare Bot Man
https://cloud.projectdiscovery.io [200] [] [GET] [] [Vercel] [vhost] [http2] [HSTS,Vercel]
https://chaos.projectdiscovery.io [200] [] [GET] [Projectdiscovery.io | Chaos] [cloudflare] [vhost] [http2] [cloudflare] [Cl
https://chaos-data.projectdiscovery.io [403] [] [GET] [] [cloudflare] [vhost] [http2] [cloudflare] [Amazon Web Services,Clou
https://docs.projectdiscovery.io [308] [/introduction] [GET] [] [Vercel] [vhost] [http2] [HSTS,Vercel]
https://cloud-dev.projectdiscovery.io [401] [] [GET] [Authentication Required] [cloudflare] [vhost] [http2] [cloudflare] [Cl
https://cve.projectdiscovery.io [404] [] [GET] [] [] [vhost] [http2] [google] [HSTS]
https://enterpriseregistration.projectdiscovery.io [404] [] [GET] [] []
https://enterpriseenrollment.projectdiscovery.io [302] [https://intune.microsoft.com/] [GET] [] [] [HSTS]
https://email.gh-mail.projectdiscovery.io [404] [] [GET] [] [] [http2] [google]
https://dns.projectdiscovery.io [404] [] [GET] [] [cloudflare] [vhost] [http2] [cloudflare] [Cloudflare,HSTS]
https://nuclei.projectdiscovery.io [302] [https://docs.nuclei.sh] [GET] [302 Found] [cloudflare] [vhost] [http2] [cloudflare
https://login.projectdiscovery.io [302] [https://projectdiscovery.io/] [GET] [] [cloudflare] [vhost] [http2] [cloudflare] [A
https://scheduler-dev.api.projectdiscovery.io [530] [] [GET] [] [cloudflare] [vhost] [http2] [cloudflare] [Cloudflare,HSTS]
```



Reference

- Subfinder Unleashed – Geek Freak
- Recon with Me !!! – Geek Freak
- Reconnaissance – Geek Freak
- Reconnaissance - The way it should be
- Hack with Automation !!! – Geek Freak

Thank You

Dhiyaneshwaran
AppSec Researcher
@DhiyaneshDK