

Automated Recon

For Web

Agenda

- Overview
- What is Recon
- Scope based Recon
- Small Scope
- Demo
- Medium Scope
- Large Scope
- Next Steps



Overview

Phases of Attack

- 1. Scoping**
- 2. Recon & Enumeration**
- 3. Mapping & Service Identification**
4. App Analysis
5. Exploitation
6. Reporting

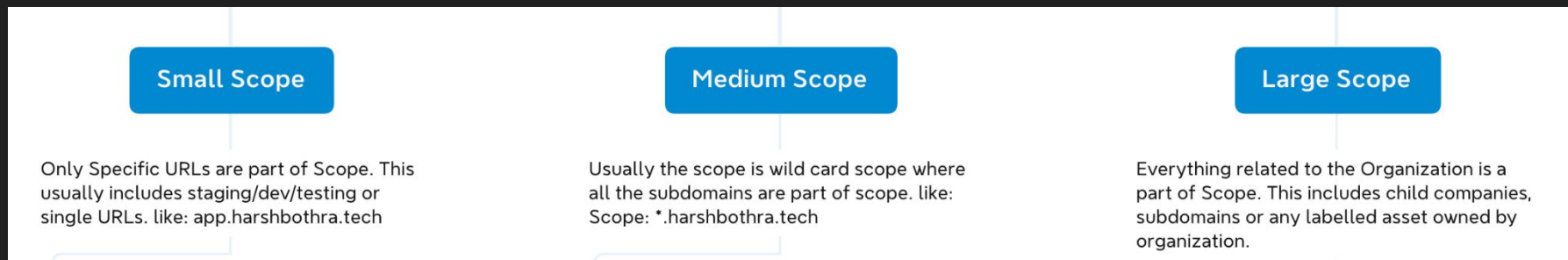
Recon?

- Map out attack surface
- Discover endpoints other are missing out
- Use hybrid approach both automated and manual
- Use automation to assist you in process of bug finding
- Recon doesn't mean bugs



Scope based recon automation

- Will save you time
- Its cost & compute effective
- Easily automate your recon workflow and combine them
- Less possibility of getting out-of-scope bugs



Small Scope

Recon automation is all about the flow of data between multiple tools to make the recon workflow smooth and fast.

- <https://null.community/>*

- **Directory Enumeration**
- **Dorking**
 - Google
 - Github
 - Shodan etc.
- **Port Scanning**
- **CVE Scanning**
- **Gf Patterns + Automation**
- **Parameter Discovery**
- **Broken Link Hijacking**

Directory Enumeration & Content discovery

Choosing right word list

- Custom wordlist
 - [Apk](#)
 - Js files
 - Assetnote techwise [wordlist](#)
 - [Robots.txt](#)
- Crawl
- waybackurls & gau
- Kiterunner for Apis



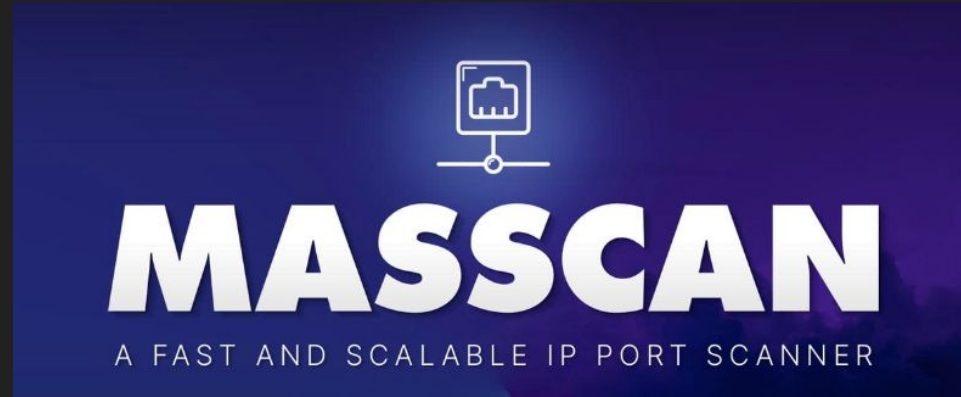
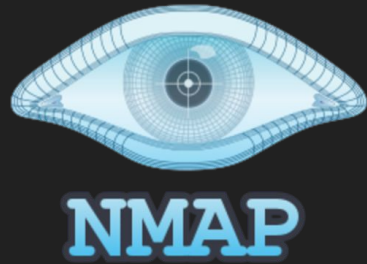
Dorking

- Awesome Shodan [dorks](#)
- Awesome Github [dorks](#)
- Awesome Google [dorks](#)







```
## Login pages
lpadmin="inurl:admin"
lplogin="inurl:login"
lpadminlogin="inurl:adminlogin"
lpcplogin="inurl:cplogin"
lpweblogin="inurl:weblogin"
lpquicklogin="inurl:quicklogin"
lpwp1="inurl:wp-admin"
lpwp2="inurl:wp-login"
lpportal="inurl:portal"
lpuserportal="inurl:userportal"
lploginpanel="inurl:loginpanel"
lpmemberlogin="inurl:memberlogin"
lpremote="inurl:remote"
lpdashboard="inurl:dashboard"
lpauth="inurl:auth"
lpexc="inurl:exchange"
lpfp="inurl:ForgotPassword"
lpptest="inurl:test"
```


Port Scanning



Medium Scope

- *.defcon.org
- (*) Wild card domains
- Specific list of “*.target.com”

Scopes			
In Scope			
Domain	*.lacity.org	 Critical	 Ineligible
Domain	*.lacity.gov	 Critical	 Ineligible
Download Burp Suite Project Configuration File (4 URLs) View changes Last updated on March 7, 2023.			

- Subdomain Enumeration
 - Passive
 - Active
- Subdomain Takeovers
- Screenshotting
- Vhost Probing
- Bucket Brute Forcing

Demo time

```
➤ app_analysis.sh
➤ autorecon.sh
➤ Bucket_Enum.sh
🔗 crtsh_enum_psql.py
➤ Domain_Recon.sh
➤ JS_wayback.sh
➤ narrow_recon.sh
➤ Port_scanning.sh
➤ recon_analysis.sh
➤ Screenshot_Recon.sh
➤ single_wildcard_recon.sh
➤ Subdomain_Recon.sh
➤ Subdomain_Takeover.sh
➤ tlsScrape.sh
```

```
http://epc.
http://
http://www.
https://3.
https://auth.
https://cdn-design.
https://cx-apac.
https://engage.
https://epc.
https://feedback.
https://inside.
https://ir.
https://livestream.
https://mfa.
https://profile.
https://service.
https://shop.
https://static-assets-pay.
https://static-assets.
https://static.
https://www.
```

Large Scope

Complete Online Presence of org

CIDR's / ASN's

- 172.200.0.0/16
- 2001:db8::/48
- AS4755

Dorking with @copyright

OSINT

Discovering file Metadata

- Acquisitions(Max-depth)
- CIDR
- ASN
- Reverse Whois
- Reverse DNS
- Favicon hash
 - murmurhash to get hash
 - shodan : http.favicon.hash

Few People you should follow for cool stuff in Bug Bounty

- **Jason Haddix** ([TBHM](#))
- Shubs_shah
- **Tomnomnom**
- Katie Paxton-Fear
- Naffy
- Sean Wright
- Th3g3nt3lman
- **Todayisnew**

Little bit about me ;)

<https://github.com/jdranpariya>

<https://twitter.com/JDRanpariya>

<https://www.linkedin.com/in/jdranpariya/>

<https://jdranpariya.vercel.app/>

For Any queries regarding Bug Bounties Dm's are open. Feel Free to ping me on either Twitter or LinkedIn

Thank you!

Q/A