--- More Targets -- More Options -- More Opportunities ---

Agenda::

* Increase your Attack Area
* Determine Techlogies used by Website
* Amazon Web Service(AWS) recon and Hacking
* Github Recon
* Content Discovery

1. Go to WayBackMachine : https://archive.org/web/
2. Use waybackurls and waybacorobots
3. Now Find Subdomains:: Knockpy , subliat3r , Amaass , SubBrute

By Dorking :: site:*.google.com

```
knockpy target.com
python sublist3r.py -d target.com
python sublist3r.py -d target.com -p 80,443
subrute.py target.com
```

https://searchdns.netcraft.com/
https://crt.sh/
https://dnsdumpster.com/
https://subdomainfinder.c99.nl/
https://www.criminalip.io/en
https://www.nmmapper.com/sys/tools/subdomainfinder/

4. Find Subdomains of the subdomains this is called reverse subdomain :: altdns

https://github.com/infosec-au/altdns

```
altdns.py -i subdomains.txt -o data_output -w words.txt -r -s output.txt
```

Find Subdomain of Subsomain:

```
subbrute.py target.com > subdomains.txt
subbrute.py -t subdomains.txt
```

5. SubDomain Valudation :: EyeWitness

```
EyeWitness.py -f subdomains.txt
```

https://www.yougetsignal.com/

6. Make your IP range :: https://whois.arin.net/ui

```
#!/bin/bash
for ipa in 98.13{6..9}.{0..255}.{0..255}; do
wget -t 1 -T 5 http://${ipa}/phpinfo.php; done&
```

7. Now find the endpoints js files by Burpsuite in Zscanner and JS-Scan

8. Github Recon ::

“target.com” “dev”
“dev.target.com”
“target.com” API_key
“target.com” password
“api.target.com”

site: “github.com” + “Target” + password

9. Content Discovery::

site:target.com filetype:php
site:target.com filetype:aspx
site:target.com filetype:swf (Shockwave Flash)
site:target.com filetype:wsdl

site: target.com inurl:.php?id=
site: target.com inurl:.php?user=
site: target.com inurl:.php?book=

site: target.com inurl:login.php
site: target.com intext: “login”
site: target.com inurl:portal.php
site: target.com inurl:register.php

site: target.com intext: “index of /”

site: target.com filetype:txt
site: target.com inurl:.php.txt
site: target.com ext:txt

```
gobuster –w wordlist.txt –u http://trgt.com
```