Recon Checklist for web pentesting

1.Subdomain Enumeration

1. First step is to subdomain enumeration. There are many tools and scripts to do this but today we are using Suibfinder and Assetfinder.

Subfinder

a) Subfinder is a subdomain discovery tool by Project discovery that discovers valid subdomains for websites by using passive online sources. It has a simple modular architecture and is optimized

steps to use subfinder----

i. install subfinder in your system (url-- https://github.com/projectdiscovery/subfinder)
ii. ./subfinder -h (to see the help menu)
iii. subfinder -d (somain) (you can your other option like threads etc..)

Assetfinder

b) Assetfinder--> This is a subdomain collecting tool..

steps to use subfinder----

i. install subfinder in your system (url--
https://github.com/tomnomnom/assetfinder)
ii. ./assetfinder-h (to see the help menu)
iii. assetfinder [--subs-only] <domain> (you can your other option like threads etc..)

After collecting list of subdomain of your target now its time to find live and valid subdomain from the list. for this we are using Httpx..

Httpx

Httpx is a fast and multi-purpose HTTP toolkit allow to run multiple probers using retryablehttp library, it is designed to maintain the result reliability with increased threads..

steps to use Httpx---

i. install Httpx in your system (url-- https://github.com/projectdiscovery/httpx)
ii. ./httpx -h(to see the help menu)
iii. ./httpx -l hosts.txt -silent (you can your other option like threads etc..)

Subdomain takeover

Now we will see any of the list of subdomain is vulnerable to subdomain Takeover.. So we will see some tool for subdomain Takeover….
URL--> https://github.com/EdOverflow/can-i-take-over-xyz

Here you will get all the stuffs fopr subdomain takeover

Github Recon

--> I will suggest you to do manuall github recon , its totally depends on your luck. github recon can give you Secret stuffs like secret kek, password, username, token, api etc

- You can search on default github search bar or target search bar

- The github search dorks are------

- "company" password (to find secret password) / "company" secret (to find secret secret)
- "company" credentials (to find secret crendentials) / "company" config (to find secret config file)
- “testdev.example.com” user:<username> <keytosearch> / “corps.example.com” org:<name of organization> “/admin/dashboard”
- “example.com” org:<name of organization> “next_url” / “example.com” org:<name of organization> “img_url”

(url= https://github.com/random-robbie/keywords/blob/master/keywords.txt) here yo will get some keywords for github recon.. use some creativity to use dorks, use dork based on your target etc...
if you want to remove from your search you can use "NOT" example "tesla.com" language:python password NOT owner.api.tesla.com (now the owner.api.tesla.com will not come in your search result)

To automate github recon you can use Gitgraber tool (usr = https://github.com/hisxo/gitGraber)
Steps to use--

I. Just setup the gitgraber tool in your system
ii. make token from github.com and add in gitgraber-> config file and its ready to use
iii. python3 gitGraber.py -h (to see the help menu)
Iv. python3 gitGraber.py -k keywordsfile.txt -q <target> -s
if you want top use another tool then you can use but i will suggest you do manuall github recon...

Google Dorks

Google dorks recon can help you to find hidden files, endpoints etcc… There are many dorks use can use, some common dorks are ….

- inurl: config site:<target>
- site:<target> index of : ftp

- inurl:index.php?id= / “index of” inurl:wp-content/ (Identify Wordpress Website)
- inurl:”q=user/password” (for finding drupal cms) / site:codepad.co “company”
- site:scribd.com “keyword” / site:npmjs.com “keyword”
- site:npm.runkit.com “keyword” / site:libraries.io “keyword”
- site:ycombinator.com “keyword” / inurl:wp-config.php intext:DB_PASSWORD -stackoverflow -wpbeginner -foro -forum -topic -blog -about -docs -articles

There is a automated tool you can use ----

- URL(https://github.com/Viralmaniar/BigBountyRecon) this tool is for windows dounload and install it..
- Then just add the target url and choose what you are finding , that tool use dorks and give the result
- Also you can use pentest-tools
- url (https://pentest-tools.com/information-gathering/google-hacking)
- search here .....

SSL Enumeration

Now you can scan SSL to find vulnerablities in SSL--

steps to scan --

- In kali linux you will get SSLscan pre-install
- SSlscan <target> (to scan your target, you will get version and all the information. so if there any vulnerablities in ssl like old version, you can further find exploit for that ssl vulnerablity..)

Enumerate Http methods

You can cheak what are the Http methods allowing like PUT,DELETE etc.. To cheak Http methods there are nmap script, metasploit, Curl

- [Metasploit] --> start metasploit--->use scanner/http/options--->set RHOST <target IP or domain name>--->exploit
- nmap --script http-methods --script-args http-methods.url-path='/website' <target>
- curl -v -X OPTIONS <target>
- nc <ip> <port>---> OPTIONS <ip>/ HTTP/1.0--> host:<ip>

Enumerate web technologies

Enumerating web technologies plays a imp role bcox of this we will set our payload, attack etc.
Methods to enum web technologies--->

i. Wappalyzer extention to see technologies
ii. whatweb <target> (whatweb comes pre install in Kali linux)
iii. https://whatcms.org/ (This will give CMS Info of your Target)

Javascript Recon

Sometimes you will get some hidden endpoints, api, key etc.. in javascript you can search that in javascript. not to see whole javascript but only intresting endpoints . You can use automation tool like jsparser

steps to use jsparser

- URL (https://github.com/nahamsec/JSParser) setup on your system
- It will give gui in your browser , just copy all javascript url and past in the tool It will automatically filter endpoints ...
- There are othere tool also you can use..

Directory Fuzzing

There are several tools to do this like FFuf, dirbuster, dirsearch, gobuster etc etc.. (FFuF is geting so popular)
Today we will use Dirsearch

steps to use

- git clone https://github.com/maurosoria/dirsearch.git
- cd dirsearch
- pip3 install -r requirements.txt
- python3 dirsearch.py -u <URL> -e <EXTENSIONS>
  other options you can use....

Fuzzing Parameters

There are many tools like Arjun, ffuf, etc
Today we are using ffuf

steps to use ffuf

- git clone https://github.com/ffuf/ffuf --> cd ffuf --> go get --> go build
- ./ffuf -u <Target>
- Read all the options to use all the options

Enumerate open ports

Enumerate open port and see vulnerable port to exploit them

steps to find open ports

- nmap -h (to see help menu)
- nmap -sv(service version) -t (threads) -O (OS version) -o (output) . there are other many option you can use
- After finding open ports cheak and finf exploit and try to exploit them ..

Bypass 4xx

If you get any 4xx like 403 page you can try to bypass by this tool "byp4xx"

Byp4xx - steps to use

- git clone https://github.com/lobuhi/byp4xx.git
- cd byp4xx
- chmod u+x byp4xx.sh
- ./byp4xx.sh [OPTIONS] http(s)://url/path

Cloudflare Bypass

CloudFail - If the target is behind Cloudflare , you can try to bypass and find the real ip by is tool

steps to use

- url (https://github.com/m0rtem/CloudFail) setup the tool
- python3 cloudfail.py --target <target> --tor

4-ZERO-3→

Tool to bypass 403/401. This script contain all the possible techniques to do the same.

steps to use

i. setup the tool in linux
ii. bash 403-bypass.sh <target/dir>

Tips and Reference -- >

- Always see robots.txt
- Always go for outdated and open ports vulnerablity t then automation then manuall hunting
- https://notifybugme.medium.com/how-github-recon-help-me-to-find-nine-full-ssrf-vulnerability-with-aws-metadata-access-531d931413a5
- If it is wordpress then use wpscan
- Get ASN Number:(– Autonomous System Number (ASN) -> http://bgp.he.net -> check for example tesla.com and checkin Prefixes V4 to get the IP range
- large-words.txt, https://github.com/danielmiessler/SecLists
- PayloadAllTheThings — https://github.com/swisskyrepo/PayloadsAllTheThings
- https://infosecwriteups.com/recon-everything-48aafbb8987
- https://orwaatyat.medium.com/your-full-map-to-github-recon-and-leaks-exposure-860c37ca2c82
- https://blog.appsecco.com/static-analysis-of-client-side-javascript-for-pen-testers-and-bug-bounty-hunters-f1cb1a5d5288
- https://github.com/m0rtem/CloudFail

Tips and Reference -- >

- https://blog.appsecco.com/static-analysis-of-client-side-javascript-for-pen-testers-and-bug-bounty-hunters-f1cb1a5d5288
- https://github.com/m0rtem/CloudFail
- https://github.com/0xghostwriter/public/blob/master/recon%20cheatsheet
- https://github.com/iamthefrogy/frogy
- https://github.com/darklotuskdb/sd-goo
- https://github.com/0xdekster/deksterecon

Thanks for ...Share and support.... Other Checklist is coming ..