Beginner's Guide to recon automation.

Ashish Jha Follow
Jun 30, 2019 · 5 min read

RECON LIKE A PRO!

Hello hackers, I am ashish jha yet again with all of you , It's been a long time since i wrote, So i had some interesting finding all these time, But today i am going to share you my automated recon process , Though i'll not be sharing my **secret receipe** anyway, But i'll share you the surface level recon which every hacker does!

Prerequisite:

1. Python
2. Grep with basic regex knowledge

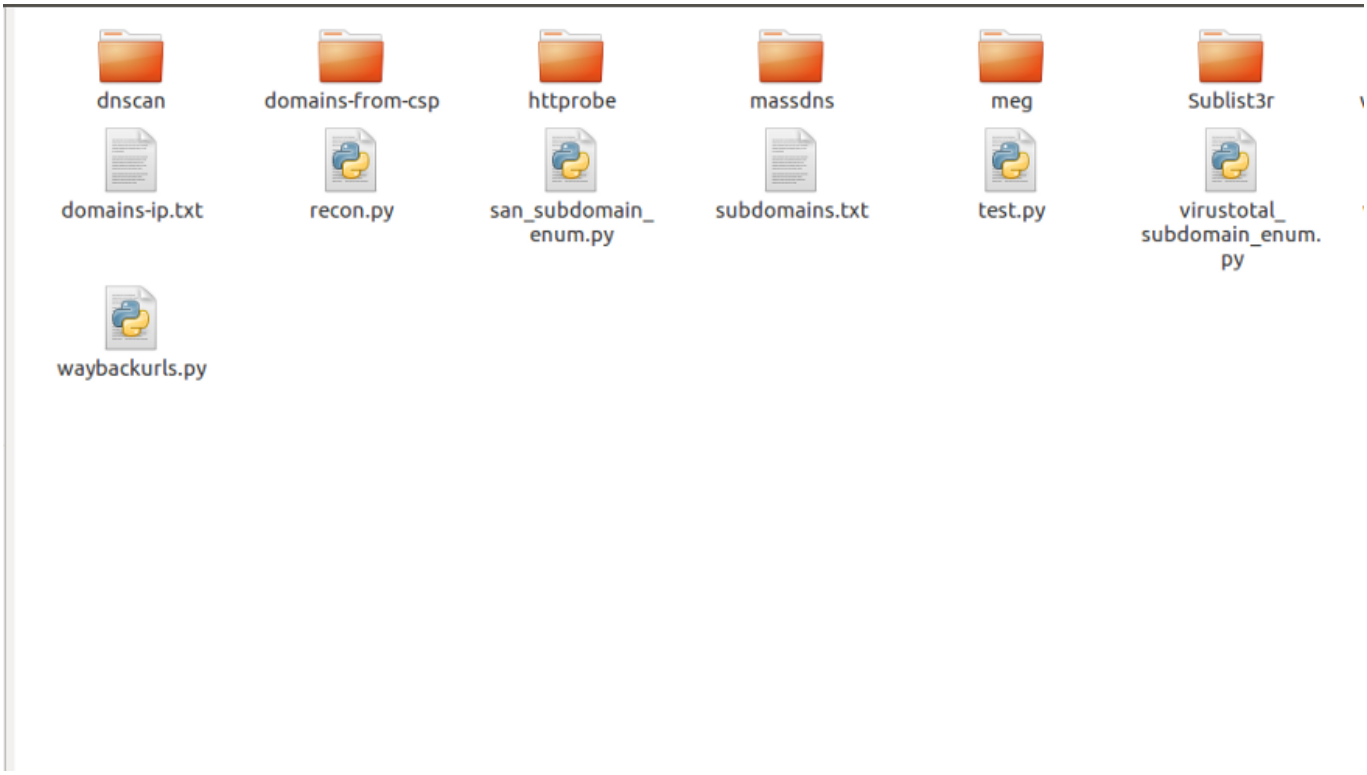
Let's start:

1. First off get ready with all your sub-domain enumeration tools.

I use: massdns's scripts (subrute and cert), sublister, dnsscan , virustotal's subdomain enum, domain's from csp , By using all these i gather almost all subdomains and by using cert script (certificate transparency logs) in massdns it even provides level 2 and more level up domains!

Some more tools: knockpy , aquatone,subfinder and the list goes on and on …..

Wordlists: jasson hadix's all.txt and built in massdns wordlists, Now you can combine any such wordlist and grow your results accordingly!



My directory of tools

2. After collecting your favourite tools ,Let's get our hand's dirty with python

i.) First off you'll be importing the os library and thereby using the system function for executing the scripts.

In the above directory you can see the recon.py script this is the scripts which does all the automation, whether that's extraction of domains, extraction of ip !

ii.) Secondly execute the scripts by using the system function.

Build a directory called recon -> system('mkdir recon')

secondly while executing the script make sure to add your subdomain.txt files in this directory.

example: system('python massdns/scripts/subbrute.py domain.com | massdns/bin/massdns -r /lists/resolver.txt -t A -o S -w **recon/subdomain.txt**')

Go ahead and add all your scripts for execution by the same above function

Now after getting your domains from specifically massdns scripts , you'll find domains and A record (or up to you which record you specify)together so in order to separate all of this you'll need to learn grep!

example : **domain.com A xxx.xxx.xxx.xxx**

3. Let's learn some grep and regex

Grep is a built in linux tools which is damn usefull for almost everyone who uses linux and working with files!

Grep basically searches and filters out data according to your regular-expression pattern. I cannot cover the entire regex here as it need another write-up , we'll only be discussing what i used in this basic recon script!

I'll soon be posting for Regular expressions too!

Here' you'll have your subdomain.txt file which you've got from your massdns script subbrute , cert and it has both the dns record and the domain name with it.

example : **domain.com A xxx.xxx.xxx.xxx**

Now here you can use grep for extracting the ip's only as you have to scan those in scope for open ports and services using **masscan.**

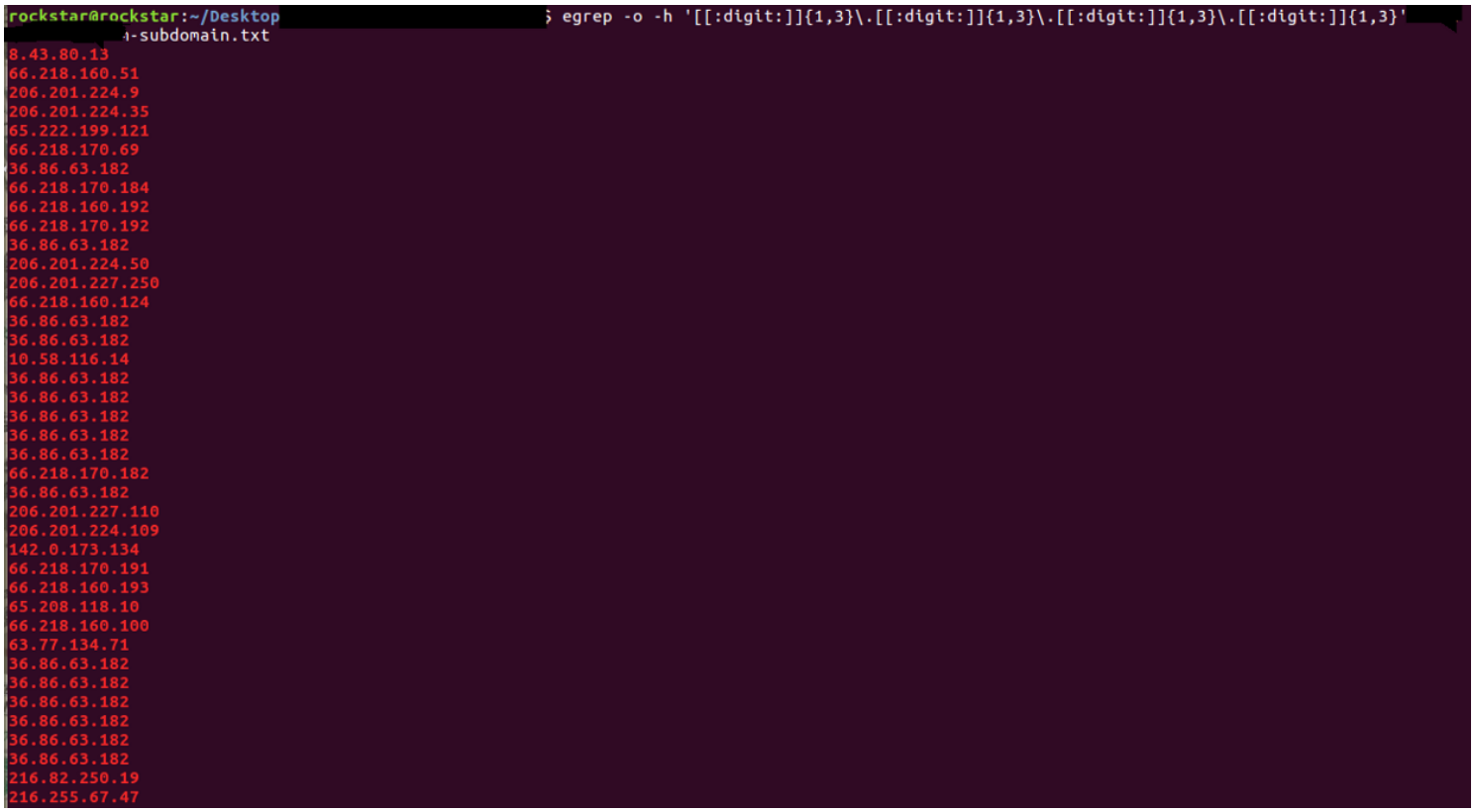
Command: egrep -o -h '[[:digit:]]{1,3}\.[[:digit:]]{1,3}\.[[:digit:]]{1,3}\.[[:digit:]]{1,3}' recon/subdomain.txt recon.subdomain-cert.txt | sort -u > ips.txt

Let’s break this down

egrep is basically extended grep, You can also use **grep -E** instead, the -o is foronly showing matching result , In this case which is the ip’s we need and the -h is used to not show the file names and lastly by piping the output of the regex to sort -u you are sorting the unique ip’s and avoiding duplications!

Now the regex: [[:digit:]]{1,3}\. → This is basically the first part of the ip adddress example: **192**.xxx.xxx.xx and now as it has 3 numbers we are using **{1,3}** and as we have 4 parts in an ip we do the same for the remaining parts. Example: **216.168.1.101** -> i don’t know what this resolves to :)

The Most important in this regex is **escaping the dot by using \.**



Now After you have your ip’s extracted, Let’s even extract the subdomains

Command: egrep -o -h ‘(.+)\.domain.com’ subdomain.txt subdomain-cert.txt | sort -u > alldomain.txt

Lets break it down: **‘(.+)\.domain.com’** What this regex means is basically extract the subdomains (.+) -> means get me everything before the domain.com and \. again escaping the dot!

```
rockstar@rockstar:~/Desktop/1                    m$ egrep -o  '(.+)\          com'                cert-subdomain.txt
taiopos              com
wupostabletperf                .com
sandbox.token-ci                .com
geo-corp.fi                .com
ca.globalpay                .com
```

4. After you have all the domains and ip address extracted from your massdns scans go ahead and append the results of sublister and other domain enum tools to this alldomain.txt file by using the system function again

example: system(‘cat subdomain-sublister.txt >> alldomain.txt’) don’t forget the >> means append and not to overwrite

After getting your domains together run another system function for sorting and only keeping the unique domains!

example: system(‘sort -u alldomain.txt > finaldomains.txt’)

Here’s How the complete script looks like :

recon.py

Note: Here you can also use argv[1] for the domain as argument , But i personally like argparser for this stuff again it is up to you!

After all these i found 781 subdomains for a program , that too sorted!!

781 sub-domains

After you have your **alldomain.txt** and **domainips.txt** go head and check whether those domains are running a http or https server and also go and check for open ports and services using masscan!

Again recon can never have an end, it's about how creative you are at your recon and how efficient too, This script can become more tiny and sophisticated , But as this is a beginners guide it's good for you and i still use this beast!

Get ready for the advanced guide to recon very soon, Untill next time, Happy Hacking!

Our team: bluefire-redteam Checkout for any cyber security services!

Command Line Hacking Hacking Tools Bug Bounty Penetration Testing

About Help Legal

Get the Medium app