Forum:Hack Forums

Thread: Favourite DNS/Sub-Domain Enumeration METHOD / TOOL

Money- - *March 14, 2020, 9:27 am*

What are your favourite methods or tools you guys used to enumerate virtual hosts? Query for DNS , Sub domains etc?
You got a lot of tools available online I know Hell even web-based tools instead of the usual python coded stuff.

What's the ones you guys usually go for?

Do you guys usually use more than 1 tools to maximize the enumeration or just rely on like 1 or 2 instead of 3 to 4 tools?
Different tools queries different results by the way , so yeah I was wondering.

compalabee - *March 14, 2020, 5:14 pm*

Me, I start with Maltego first because the GUI is really user-friendly. You can just drag around.

Afterwards I just move on to aboul3la's Sublist3r. I used to be a big fan of DNSDumpster but their API has been having glitches, so I just cross it out of Sublist3r so I can get other OSINT sources from there.

ernestmiller - *March 15, 2020, 8:51 am*

Yeah I just tried to use the DNS Dumpster API myself on a website now and I got an error with connecting with it never had any issues with the API until now though, the website is still good though and gives you a nice graph as well

Money- - *March 15, 2020, 9:47 am*

(Mar 14, 2020 05:14 PM)compalabee Wrote: *[CITE]* Me, I start with Maltego first because the GUI is really user-friendly. You can just drag around.

Afterwards I just move on to aboul3la's Sublist3r. I used to be a big fan of DNSDumpster but their API has been having glitches, so I just cross it out of Sublist3r so I can get other OSINT sources from there.
I too used DNSdumpster sometimes. I just tested a site I don't see any error API or glitches as you guys mentioned.
Maltego is cool too , used it in the past but I can't be bothered with the GUI haha.

I heard Sub finder is normally used with sublister together and its faster.
https://github.com/projectdiscovery/subfinder

Normally I use more than 1 tool. Wrote a bash script to chain them together for maximum enumeration.

BigJoe7413 - *March 15, 2020, 9:57 am*

I like sublist3r for the portscan also use amass its super slow but it has great results

Money- - *March 15, 2020, 10:35 am*

(Mar 15, 2020 09:57 AM)BigJoe7413 Wrote: *[CITE]* I like sublist3r for the portscan also use amass its

super slow but it has great results
Yo man , you heard of https://www.infoblox.com
?
I never used this site before.
Someone recommend me this for sub domain enumeration lol.

POLY MATH - *March 15, 2020, 2:55 pm*
I just use Sublist3r for Subdomain Enumeration then GoBuster for Dir. Bruteforcing then Gobuster for File Bruteforcing then GoWitness(optional) for screenshotting and finish off with Somdev Parameter Bruteforcing

I mean, all of the tools out there that are up-to-date(even some out of date) are good. Just depends on preference/target(s).

I must say that this is my way doing things and I'm sure their is someone smarter then me doing it better!

Here is a good article on how deep subdomain enumeration can go.

https://0xpatrik.com/subdomain-enumeration-2019/

Money- - *March 16, 2020, 6:02 am*
(Mar 15, 2020 02:55 PM)POLY MATH Wrote: *[CITE]* I just use Sublist3r for Subdomain Enumeration then GoBuster for Dir. Bruteforcing then Gobuster for File Bruteforcing then GoWitness(optional) for screenshotting and finish off with Somdev Parameter Bruteforcing

I mean, all of the tools out there that are up-to-date(even some out of date) are good. Just depends on preference/target(s).

I must say that this is my way doing things and I'm sure their is someone smarter then me doing it better!

Here is a good article on how deep subdomain enumeration can go.

https://0xpatrik.com/subdomain-enumeration-2019/
Directory fuzzing kinda reminds me 1 time which I decided to try my luck by fuzzing back up file extensions like .bak , .bac , .old to end up finding juicy info that allows me to leverage certain vulnerabilities to exploit the target.

Guess some developers are just lazy and end up renaming files lol.

POLY MATH - *March 16, 2020, 10:46 am*
(Mar 16, 2020 06:02 AM)Money- Wrote: *[CITE]* Directory fuzzing kinda reminds me 1 time which I decided to try my luck by fuzzing back up file extensions like .bak , .bac , .old to end up finding juicy info that allows me to leverage certain vulnerabilities to exploit the target.

Guess some developers are just lazy and end up renaming files lol.
That's the idea of it :)

Squidos - *March 19, 2020, 12:46 pm*
I personally use amass and subfinder. https://www.youtube.com/watch?v=Qw1nNPiH_Go&t=1780

l4stl00k - *March 19, 2020, 2:11 pm*

thanks for the idea mate.will note this hanks