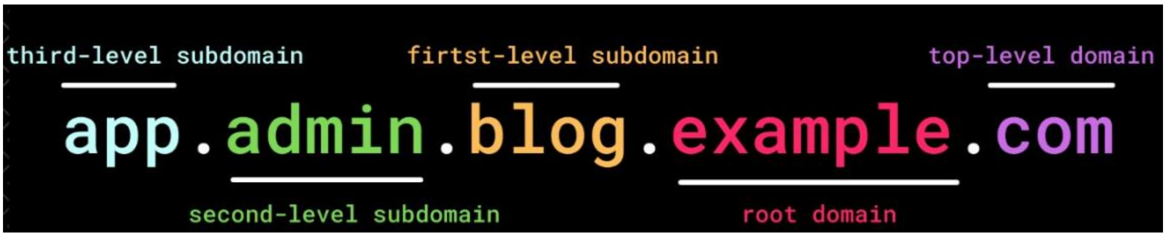
SUBDOMAIN ENUMERATION

What is Subdomain?



- A subdomain is a second-level domain that is part of a larger domain.
- Subdomains can be used for a variety of purposes, such as to host a blog, an e-commerce site, or even an entirely different website from the root domain.
- Subdomains are often used to segregate different services or functionalities within an organization.

What do you mean by SubdomainEnumeration?

- It is the process of finding as many
- subdomains as possible and expanding our attack surface by finding any hiddenweb applications or forgotten subdomains.
- There are many great tools for enumerating subdomains for one or moredomains.
- These tools are crucial in a penetration testing environment, to find subdomainsand test on all the targets for finding anybugs.
- Tools for subdomain enumeration includeamass, subfinder, pdlist, turbolist3r, etc.

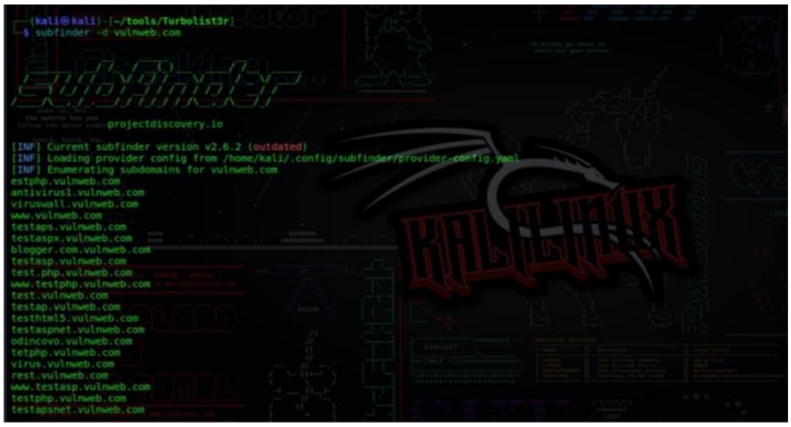
- All these tools are fast and efficient and have their own unique features.
- Let's see some of the tools and their usage.

Why sub-domain enumeration is important?

- Sub-domain enumeration can reveal a lot of domains/sub-domains that are in scope of a security assessment which in turn increases the chances of finding vulnerabilities.
- By enumerating all subdomains, you may be able to find subdomains that are less well- protected than the root domain or the target organization, making them more vulnerable to attack.
- Finding applications running on hidden, forgotten sub-domains may lead to uncovering critical vulnerabilities.
- Often times the same vulnerabilities tend to be present across different domains/applications of the same organization.
- In some cases, organizations may have misconfigured DNS entries that reveal sensitive information, such as internal IP addresses.

1) Subfinder (by Project Discovery)

- Target tested on: http://www.vulnweb.com
- GitHub Link:
  https://github.com/projectdiscovery/subfinder
- Tool Example POC on target:

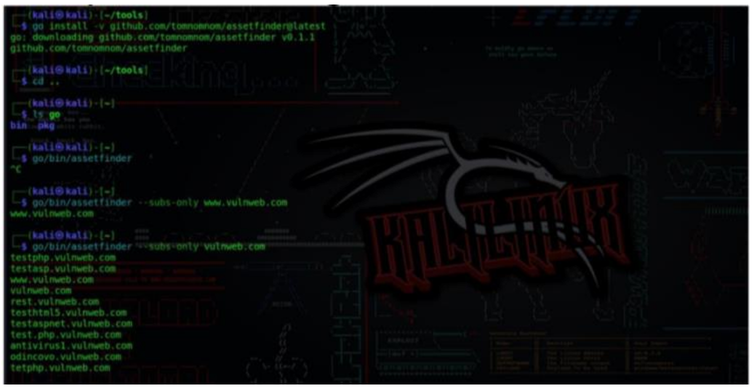


```
┌──(kali㉿kali)-[~/tools/Turbolist3r]
└─$ subfinder -d vulnweb.com

                projectdiscovery.io

[INF] Current subfinder version v2.6.2 (outdated)
[INF] Loading provider config from /home/kali/.config/subfinder/provider-config.yaml
[INF] Enumerating subdomains for vulnweb.com
estphp.vulnweb.com
antivirus1.vulnweb.com
viruswall.vulnweb.com
www.vulnweb.com
testaps.vulnweb.com
testaspx.vulnweb.com
blogger.com.vulnweb.com
testasp.vulnweb.com
test.php.vulnweb.com
www.testphp.vulnweb.com
test.vulnweb.com
testap.vulnweb.com
testhtml5.vulnweb.com
testaspnet.vulnweb.com
odincovo.vulnweb.com
tetphp.vulnweb.com
virus.vulnweb.com
rest.vulnweb.com
www.testasp.vulnweb.com
testphp.vulnweb.com
testapsnet.vulnweb.com
```

- Usage: subfinder -d <target.com>

2) Assetfinder (by tomnomnom)

- Target tested on: http://www.vulweb.com
- GitHub Link:
  https://github.com/tomnomnom/assetfinder
- Tool Example POC on target:



```
┌──(kali㉿kali)-[~/tools]
└─$ go install -v github.com/tomnomnom/assetfinder@latest
go: downloading github.com/tomnomnom/assetfinder v0.1.1
github.com/tomnomnom/assetfinder

┌──(kali㉿kali)-[~/tools]
└─$ cd ..

┌──(kali㉿kali)-[~]
└─$ ls go
bin  pkg

┌──(kali㉿kali)-[~]
└─$ go/bin/assetfinder
^C

┌──(kali㉿kali)-[~]
└─$ go/bin/assetfinder --subs-only www.vulnweb.com
www.vulnweb.com

┌──(kali㉿kali)-[~]
└─$ go/bin/assetfinder --subs-only vulnweb.com
testphp.vulnweb.com
testasp.vulnweb.com
www.vulnweb.com
vulnweb.com
rest.vulnweb.com
testhtml5.vulnweb.com
testaspnet.vulnweb.com
test.php.vulnweb.com
antivirus1.vulnweb.com
odincovo.vulnweb.com
tetphp.vulnweb.com
```

- Usage: assetfinder –subs-only <target.com>

References

1. Vulnweb: http://www.vulnweb.com
2. Assetfinder:
https://github.com/tomnomnom/assetfinder
3. Subfinder:
https://github.com/projectdiscovery/subfind er

Done by:

Naveenkumar.v

Intern at Cyber Sapiens