

DNS Bruteforcing

@mmar



DNS Bruteforcing

DNS Bruteforcing is a technique where an attacker systematically generates and tries a large number of DNS queries in an attempt to discover valid subdomains or hostnames associated with a target domain. The advantages of DNS bruteforcing include identifying hidden or forgotten subdomains, uncovering potential entry points for further attacks, and gaining insights into the target's DNS infrastructure. It can help in reconnaissance, mapping the target's network, and identifying potential vulnerabilities or misconfigurations

Wordlists

- ❖ Brute forcing requires good wordlists. Seclists provide very good wordlists for any brute-forcing task

```
>sudo apt install seclists
```

```
(kali㉿kali)-[~]
└─$ sudo apt install seclists
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following packages were automatically installed and are no longer required:
  libpython3.10-dev python3-alabaster python3-imagesize python3.10-minimal sphinx-common
Use 'sudo apt autoremove' to remove them.
The following NEW packages will be installed:
  seclists
```

Nmap

Nmap

- ❖ Nmap provides a handy script for DNS bruteforcing

```
>nmap -p 53 --script dns-brute zonetransfer.me
```

```
(kali㉿kali)-[~]
└─$ nmap -p 53 --script dns-brute zonetransfer.me
Starting Nmap 7.93 ( https://nmap.org ) at 2023-06-12 02:30 EDT
Nmap scan report for zonetransfer.me (5.196.105.14)
Host is up (0.22s latency).

PORT      STATE SERVICE
53/tcp    closed domain

Host script results:
| dns-brute:
|   DNS Brute-force hostnames:
|     testing.zonetransfer.me - 5.196.105.14
|     vpn.zonetransfer.me - 174.36.59.154
|     owa.zonetransfer.me - 207.46.197.32
|     www.zonetransfer.me - 5.196.105.14
|     _
|     home.zonetransfer.me - 127.0.0.1
└─

Nmap done: 1 IP address (1 host up) scanned in 15.40 seconds
```

DNSMAP

dnsmap

- ❖ Dnsmap is a DNS bruteforcer with very easy to use syntax

```
>dnsmap zonetransfer.me -w  
/usr/share/seclists/discovery/DNS/fierce-hostlists.txt
```

```
(kali㉿kali)-[~]  
└─$ dnsmap zonetransfer.me -w /usr/share/seclists/Discovery/DNS/fierce-hostlist.txt  
  
dnsmap 0.36 - DNS Network Mapper  
  
[+] searching (sub)domains for zonetransfer.me using /usr/share/seclists/Discovery/DNS/fierce-hostlist.txt  
[+] using maximum random delay of 10 millisecond(s) between requests  
  
email.zonetransfer.me  
IP address #1: 74.125.206.26  
  
home.zonetransfer.me  
IP address #1: 127.0.0.1  
[+] warning: domain might be vulnerable to "same site" scripting (https://seclists.org/bugtraq/2008/Jan/270)  
  
office.zonetransfer.me  
IP address #1: 4.23.39.254
```

Fierce

Fierce

- ❖ Fierce can also be used to bruteforce DNS and is the favourite tool for pentesters

```
>fierce --domain zonetransfer.me --subdomain-file  
/usr/share/seclists/Discovery/DNS/fierce-hostlist.txt
```

```
(kali@kali)-[~]  
└─$ fierce --domain zonetransfer.me --subdomain-file /usr/share/seclists/Discovery/DNS/fierce-hostlist.txt  
NS: nsztl2.digi.ninja. nsztl1.digi.ninja.  
SOA: nsztl1.digi.ninja. (81.4.108.41)  
Zone: success  
{<DNS name @>: '@ 7200 IN SOA nsztl1.digi.ninja. robin.digi.ninja. 2019100801 '  
'172800 900 1209600 3600\n'  
'@ 300 IN HINFO "Casio fx-700G" "Windows XP"\n'  
'@ 301 IN TXT '  
'"google-site-verification=tyP28J7JAUHA9fw2sHXMGcCC0I6XBmmoVi04VlMewxA"\n'  
'@ 7200 IN MX 0 ASPMX.L.GOOGLE.COM.\n'  
'@ 7200 IN MX 10 ALT1.ASPMX.L.GOOGLE.COM.\n'  
'@ 7200 IN MX 10 ALT2.ASPMX.L.GOOGLE.COM.\n'  
'@ 7200 IN MX 20 ASPMX2.GOOGLEMAIL.COM.\n'
```



THANKS