# DNS Bruteforcing

@mmar

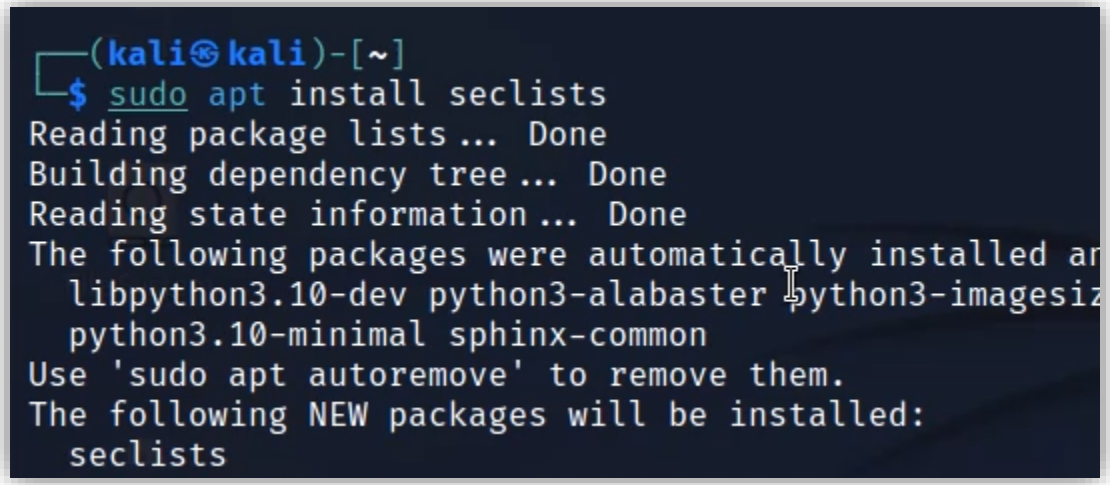
# DNS Bruteforcing

**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

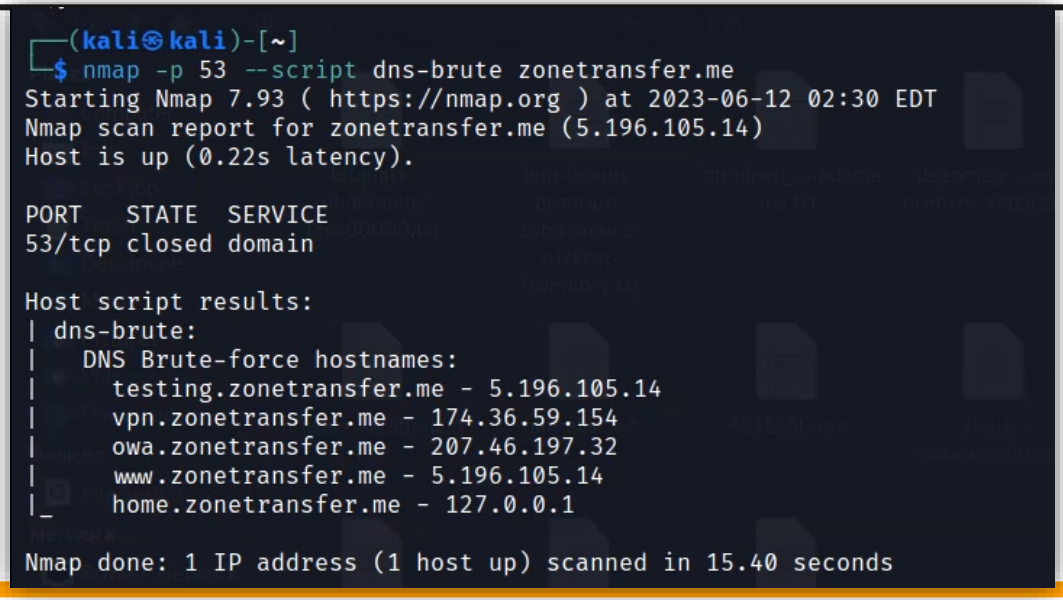


# Nmap

# Nmap

- Nmap provides a handy script for DNS bruteforcing

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

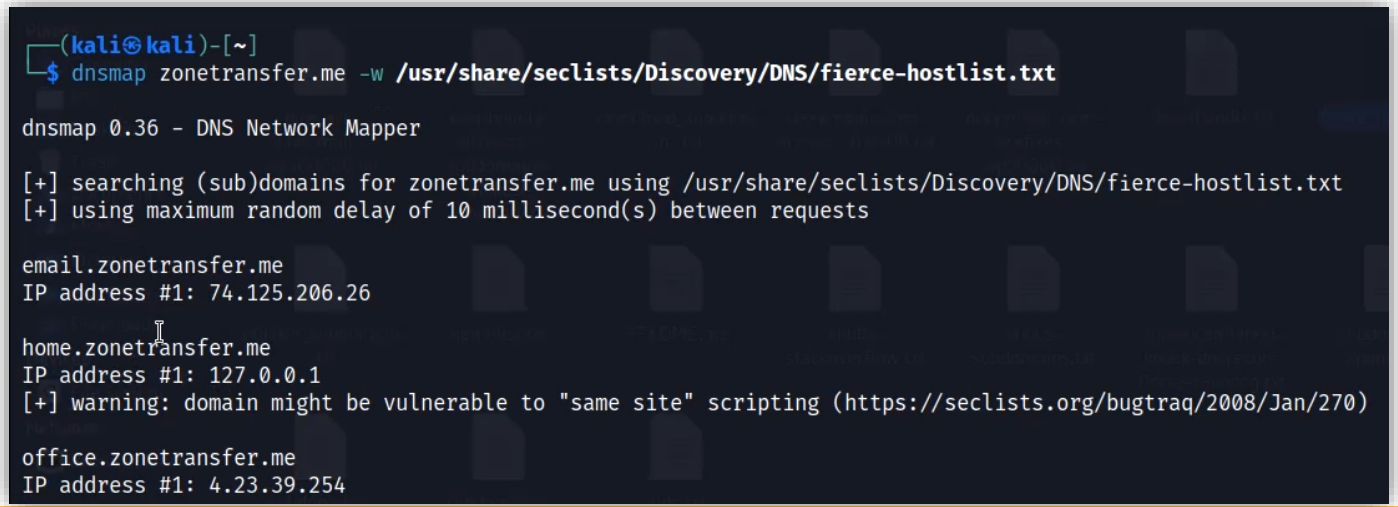


# DNSMAP

# dnsmap

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

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



# 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: nsztm2.digi.ninja. nsztm1.digi.ninja.
SOA: nsztm1.digi.ninja. (81.4.108.41)
Zone: success
{<DNS name @>: '@ 7200 IN SOA nsztm1.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