Active Information Gathering

DNS Enumeration

Host Command:

```
kali@kali:~$ host www.megacorpone.com
www.megacorpone.com has address 38.100.193.76

kali@kali:~$ host -t mx megacorpone.com
megacorpone.com mail is handled by 10 fb.mail.gandi.net.

kali@kali:~$ host -t txt megacorpone.com
megacorpone.com descriptive text "Try Harder"
```

Host Brute Force:

```
kali@kali:~$ cat list.txt
www
ftp
mail
owa
proxy
router

kali@kali:~$ for ip in $(cat list.txt); do host $ip.megacorpone.com; done
www.megacorpone.com has address 38.100.193.76
Host ftp.megacorpone.com not found: 3(NXDOMAIN)
mail.megacorpone.com has address 38.100.193.84
Host owa.megacorpone.com not found: 3(NXDOMAIN)
Host proxy.megacorpone.com not found: 3(NXDOMAIN)
router.megacorpone.com has address 38.100.193.71
```

If you have an approximate ip range you can do a reverse dns bruteforce:

```
kali@kali:~$ for ip in $(seq 50 100); do host 38.100.193.$ip; done | grep -v "not
found"
69.193.100.38.in-addr.arpa domain name pointer beta.megacorpone.com.
70.193.100.38.in-addr.arpa domain name pointer ns1.megacorpone.com.
72.193.100.38.in-addr.arpa domain name pointer admin.megacorpone.com.
73.193.100.38.in-addr.arpa domain name pointer mail2.megacorpone.com.
76.193.100.38.in-addr.arpa domain name pointer www.megacorpone.com.
77.193.100.38.in-addr.arpa domain name pointer vpn.megacorpone.com.
```

If a dns server is misconfigured you can attempt a zone transfer. If they have multiple dns server (ie ns1, ns2) you should try multiple as maybe only one of them is misconfigured:

```
host -t ns megacorpone.com | cut -d " " -f 4
ns1.megacorpone.com.
ns2.megacorpone.com.
ns3.megacorpone.com.

host -l <domain name> <dns server address>
host -l megacorpone.com ns1.megacorpone.com
dnsrecon -d megacorpone.com -t axfr
```

Some useful automated tools for this are DNSrecon and DNSenum.

Port Scanning