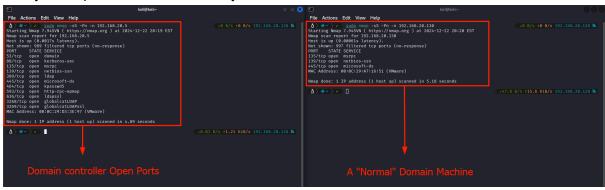


## Intro

Before using Kali Linux tools to enumerate an Active Directory, or use any other technique on those environments, we have to configure the DNS server of our Kali Linux Machine as the domain controller or Edit the file **ect/hosts** to get visibility to the Domain controller.

First we have to identify the IP address of the domain controller. We can do this using **nmap** or any other port scan tool to identify the domain controller



The second step is use tools like crackmapexec/netexec or the same nmap to get the `domain name

Third, modify the file /etc/host putting the DC IP address and the domain name

```
GNU nano 8.2

127.0.0.1 localhost

127.0.1.1 kali

::1 localhost ip6-localhost ip6-loopback

ff02::1 ip6-allnodes

ff02::2 ip6-allrouters

192.168.20.5 corp.local

Domain In

10.129.3.42 s3.thetoppers.htb

10.129.3.42 thetoppers.htb
```

And finally, make a request to the domain to see if we have a connection with it

```
Ding -c4 corp.local
PING corp.local (192.168.20.5) 56(84) bytes of data.
64 bytes from corp.local (192.168.20.5): icmp_seq=1 ttl=128 time=0.745 ms
64 bytes from corp.local (192.168.20.5): icmp_seq=2 ttl=128 time=2.27 ms
64 bytes from corp.local (192.168.20.5): icmp_seq=3 ttl=128 time=1.02 ms
64 bytes from corp.local (192.168.20.5): icmp_seq=4 ttl=128 time=2.16 ms

— corp.local ping statistics —
4 packets transmitted, 4 received, 0% packet loss, time 3006ms
rtt min/avg/max/mdev = 0.745/1.547/2.269/0.675 ms

The Doman is reacheble
```

And this is the initial configuration that we must to do to start to make a pentesting on AD environment