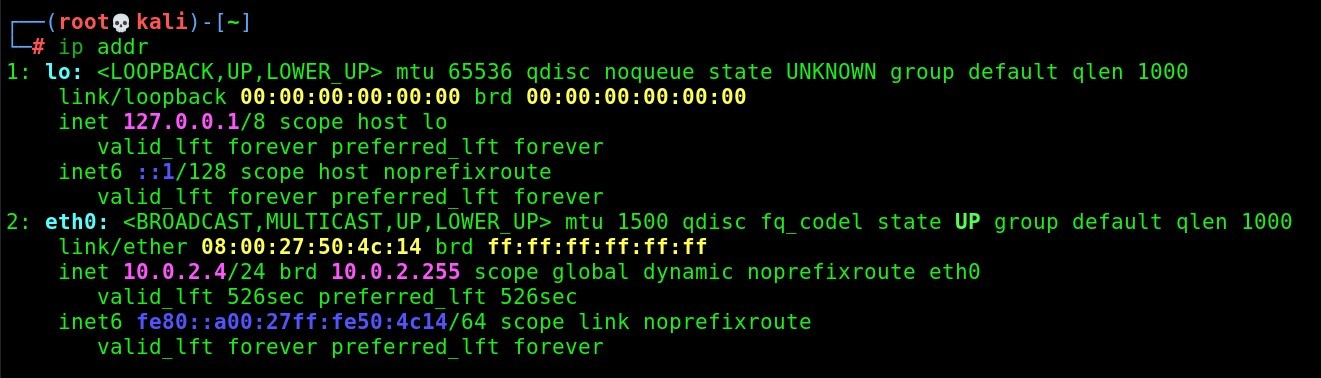
**Network Mapping:**

Imitating the internal pentest environment, we are thrown into a local area network on an organization named as BiriyaniBlend.trio. Hence our primary objective is to map the network.

We will move ahead using 'nmap'.

Firstly let us grab some info regarding our IP and network CIDR.

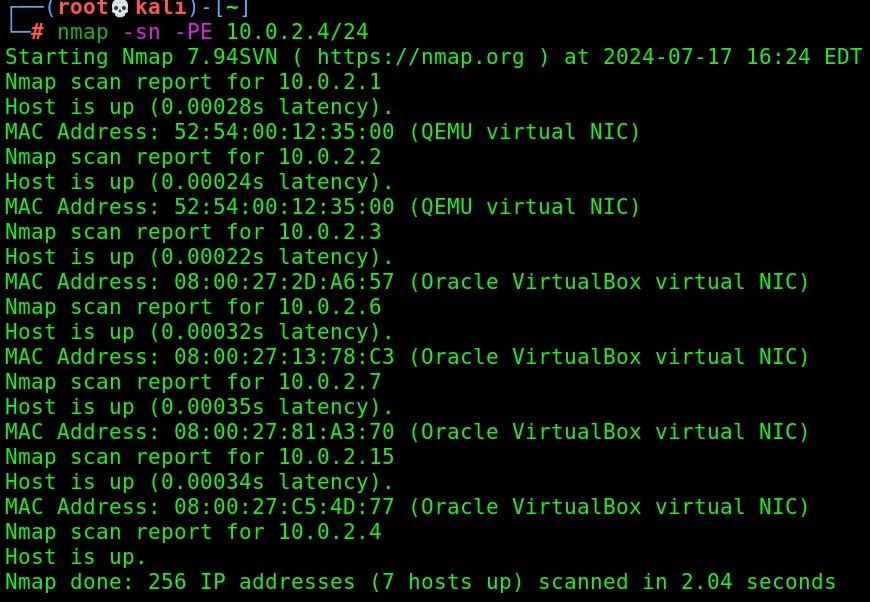


Interface is eth0 and CIDR is 10.0.2.0/24 and we are at 10.0.2.4

Let proceed with nmap.

-sn: for no port scanning as we are only intended in finding the active devices on the network.

-PE: for ping icmp echo scan



we can see that 10.0.2.6,7,15 is active and now we will move ahead to exfiltrate some more information regarding them.

Rest all machines are default gateway and network DNS with our virtual environment

Hence,

-Pn: no ping scan directly move for the port scanning part

-sS: Use stealth scanning

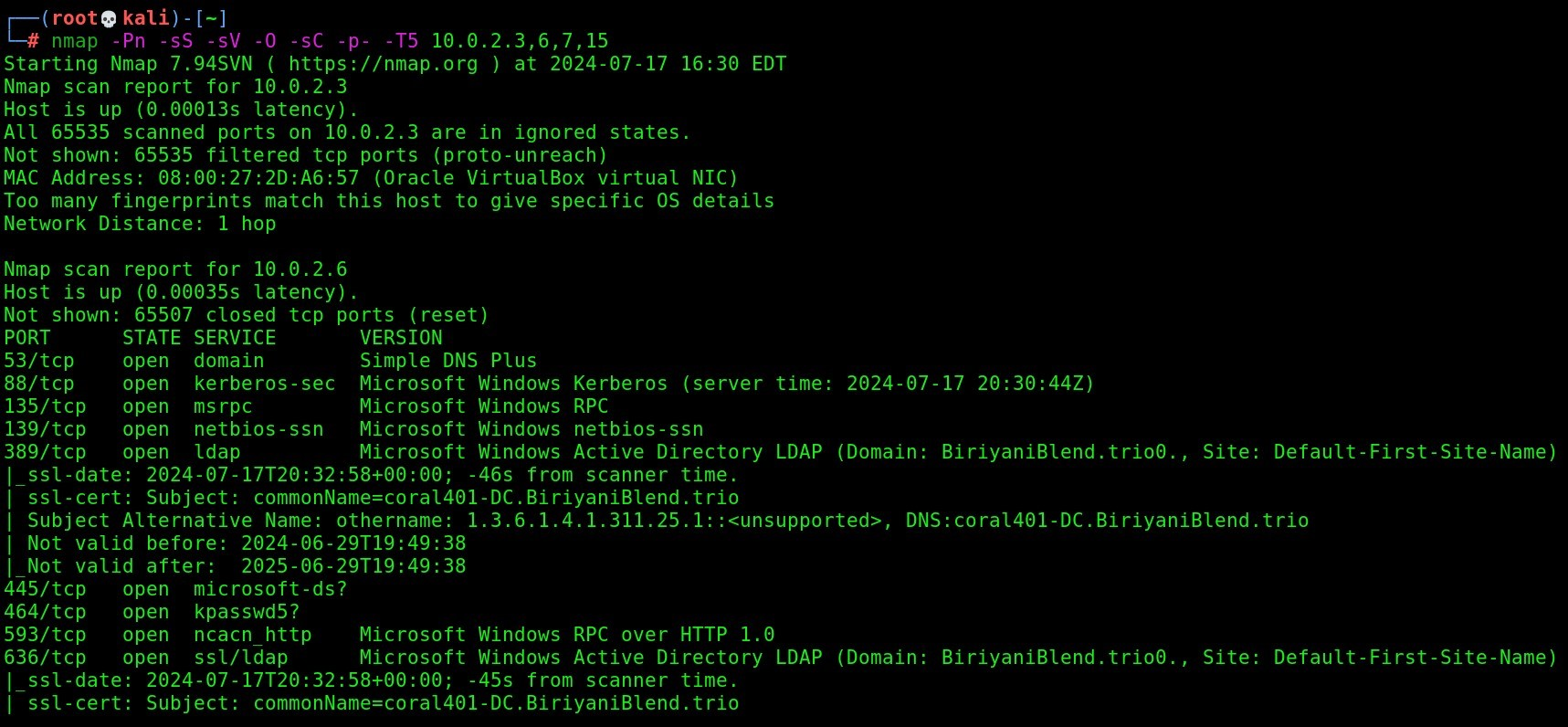
-sV: Version detection

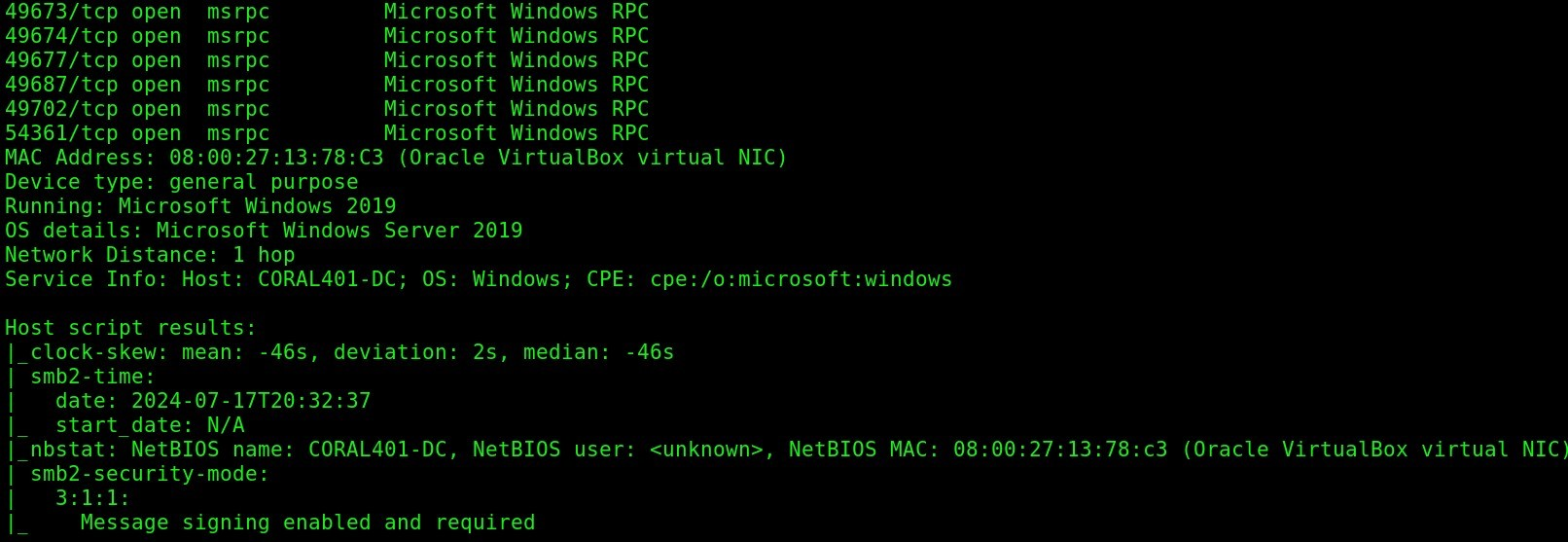
-O: OS detection

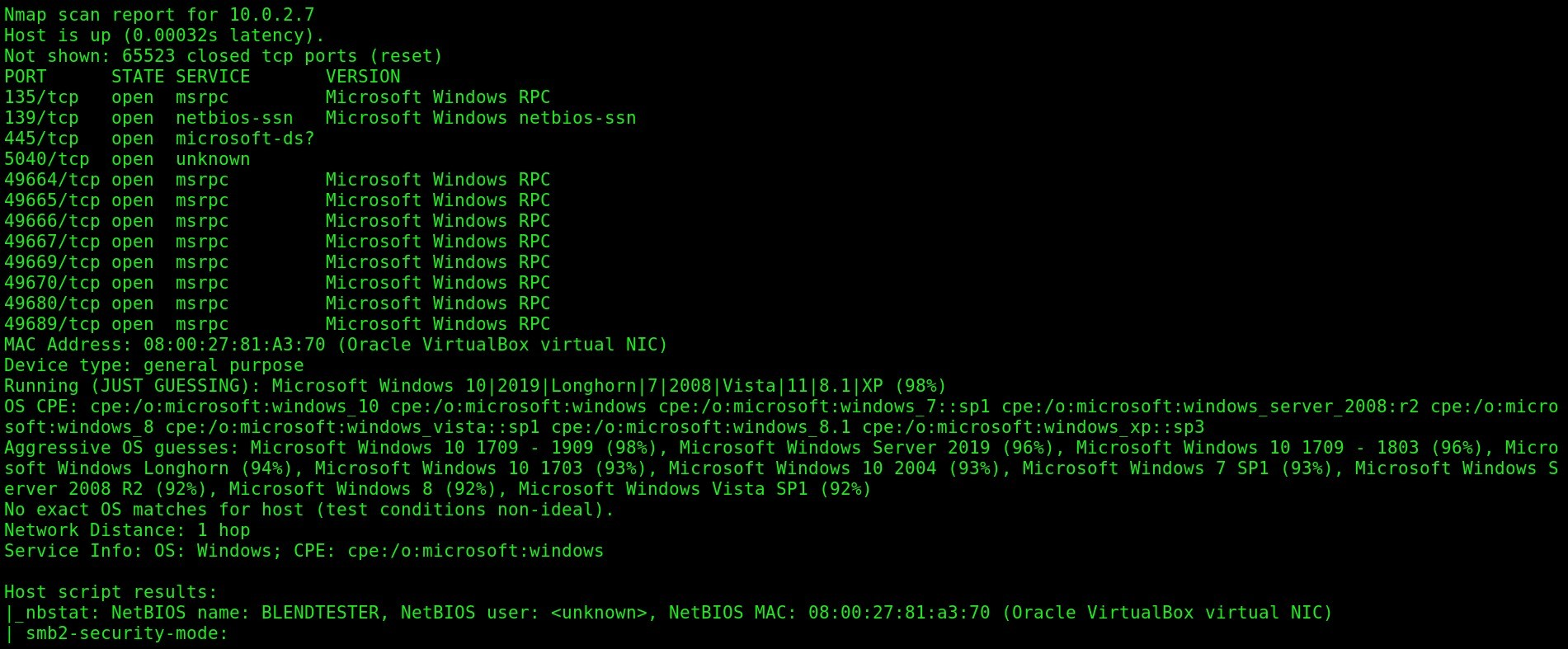
-sC: use --script=default

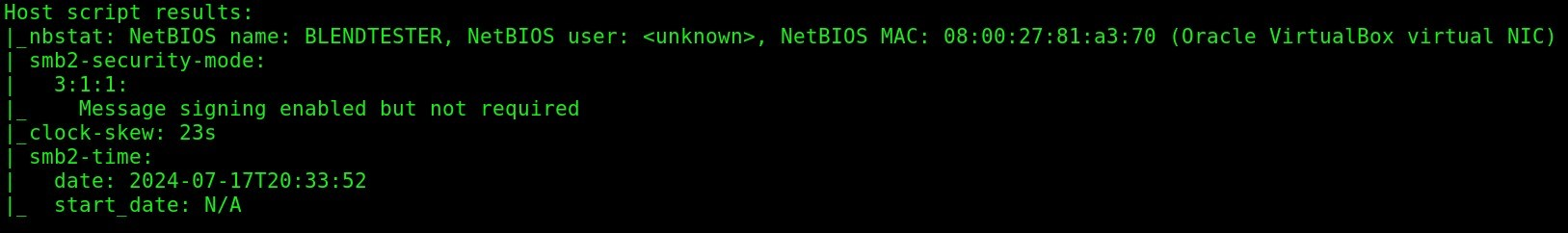
-T5: scan at an insane rate

and our targets are 10.0.2.6,7,15

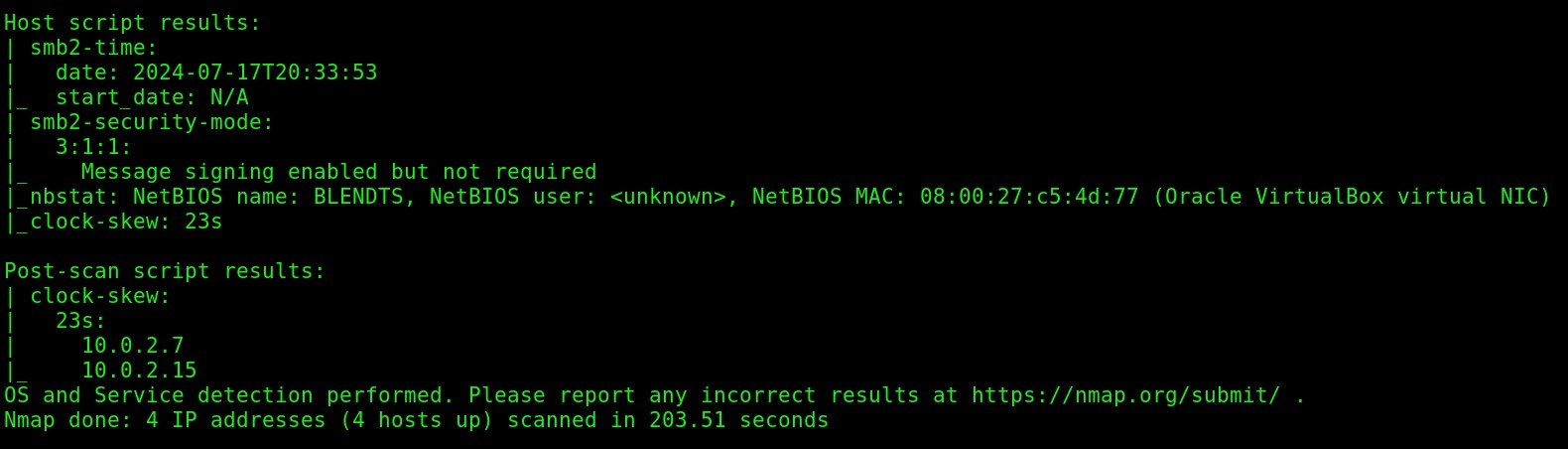












After examining the above output of our nmap command we can conclude that:

***Domain***

BiriyaniBlend.trio

***Domain Controller***

**name:** coral401-DC

**commonName=**coral401-DC.BiriyaniBlend.trio

**IP:** 10.0.2.6

**OS:** Windows 2019 Server

**Important Services:** DNS:53, ldap/(s):389,636, SMB:445(Signing enabled and required)

***Workstations***

**name:** BLENDTESTER

**commonName=**BLENDTESTER.BiriyaniBlend.trio

**IP:** 10.0.2.7

**OS:** Windows 10

**Important Services:** SMB:455(Signing disabled and required)

**name:** BLENDTS

**commonName=**BLENDTS.BiriyaniBlend.trio

**IP:** 10.0.2.15

**OS:** Windows 10

**Important Services:** SMB:455(Signing disabled and required)

**As we are in an Active Directory environment**

**We can proceed with three attacks:**

1) LLMNR Poisoning and SMB relay(as SMB signing is disabled on both workstation in the domain)

2) Compromise the ipv4 network using ipv6(mitm6)

3) Try to enumerate services like SMB and LDAP to fetch more information\*