Initial Recon

Thursday, July 18, 2024 3:14 AM

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.

```
┌──(root💀kali)-[~]
└─# ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:50:4c:14 brd ff:ff:ff:ff:ff:ff
    inet 10.0.2.4/24 brd 10.0.2.255 scope global dynamic noprefixroute eth0
       valid_lft 526sec preferred_lft 526sec
    inet6 fe80::a00:27ff:fe50:4c14/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
```

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

Lets 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

```
┌──(root💀kali)-[~]
└─# nmap -sn -PE 10.0.2.4/24
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-17 16:24 EDT
Nmap scan report for 10.0.2.1
Host is up (0.00028s latency).
MAC Address: 52:54:00:12:35:00 (QEMU virtual NIC)
Nmap scan report for 10.0.2.2
Host is up (0.00024s latency).
MAC Address: 52:54:00:12:35:00 (QEMU virtual NIC)
Nmap scan report for 10.0.2.3
Host is up (0.00022s latency).
MAC Address: 08:00:27:2D:A6:57 (Oracle VirtualBox virtual NIC)
Nmap scan report for 10.0.2.6
Host is up (0.00032s latency).
MAC Address: 08:00:27:13:78:C3 (Oracle VirtualBox virtual NIC)
Nmap scan report for 10.0.2.7
Host is up (0.00035s latency).
MAC Address: 08:00:27:81:A3:70 (Oracle VirtualBox virtual NIC)
Nmap scan report for 10.0.2.15
Host is up (0.00034s latency).
MAC Address: 08:00:27:C5:4D:77 (Oracle VirtualBox virtual NIC)
Nmap scan report for 10.0.2.4
Host is up.
Nmap done: 256 IP addresses (7 hosts up) scanned in 2.04 seconds
```

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

```
┌──(root💀kali)-[~]
└─# nmap -Pn -sS -sV -O -sC -p- -T5 10.0.2.3,6,7,15
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-17 16:30 EDT
Nmap scan report for 10.0.2.3
Host is up (0.00013s latency).
All 65535 scanned ports on 10.0.2.3 are in ignored states.
Not shown: 65535 filtered tcp ports (proto-unreach)
MAC Address: 08:00:27:2D:A6:57 (Oracle VirtualBox virtual NIC)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop

Nmap scan report for 10.0.2.6
Host is up (0.00035s latency).
Not shown: 65507 closed tcp ports (reset)
PORT      STATE SERVICE       VERSION
53/tcp    open  domain        Simple DNS Plus
88/tcp    open  kerberos-sec  Microsoft Windows Kerberos (server time: 2024-07-17 20:30:44Z)
135/tcp   open  msrpc         Microsoft Windows RPC
139/tcp   open  netbios-ssn   Microsoft Windows netbios-ssn
389/tcp   open  ldap          Microsoft Windows Active Directory LDAP (Domain: BiriyaniBlend.trio0., Site: Default-First-Site-Name)
|_ssl-date: 2024-07-17T20:32:58+00:00; -46s from scanner time.
| ssl-cert: Subject: commonName=coral401-DC.BiriyaniBlend.trio
| Subject Alternative Name: othername: 1.3.6.1.4.1.311.25.1::<unsupported>, DNS:coral401-DC.BiriyaniBlend.trio
| Not valid before: 2024-06-29T19:49:38
|_Not valid after:  2025-06-29T19:49:38
445/tcp   open  microsoft-ds?
464/tcp   open  kpasswd5?
593/tcp   open  ncacn_http    Microsoft Windows RPC over HTTP 1.0
636/tcp   open  ssl/ldap      Microsoft Windows Active Directory LDAP (Domain: BiriyaniBlend.trio0., Site: Default-First-Site-Name)
|_ssl-date: 2024-07-17T20:32:58+00:00; -45s from scanner time.
| ssl-cert: Subject: commonName=coral401-DC.BiriyaniBlend.trio
```

```
49673/tcp open  msrpc         Microsoft Windows RPC
49674/tcp open  msrpc         Microsoft Windows RPC
49677/tcp open  msrpc         Microsoft Windows RPC
49687/tcp open  msrpc         Microsoft Windows RPC
49702/tcp open  msrpc         Microsoft Windows RPC
54361/tcp open  msrpc         Microsoft Windows RPC
MAC Address: 08:00:27:13:78:C3 (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Microsoft Windows 2019
OS details: Microsoft Windows Server 2019
Network Distance: 1 hop
Service Info: Host: CORAL401-DC; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_clock-skew: mean: -46s, deviation: 2s, median: -46s
| smb2-time:
|   date: 2024-07-17T20:32:37
|_  start_date: N/A
|_nbstat: NetBIOS name: CORAL401-DC, NetBIOS user: <unknown>, NetBIOS MAC: 08:00:27:13:78:c3 (Oracle VirtualBox virtual NIC)
| smb2-security-mode:
|   3:1:1:
|_    Message signing enabled and required
```

```
Nmap scan report for 10.0.2.7
Host is up (0.00032s latency).
Not shown: 65523 closed tcp ports (reset)
PORT      STATE SERVICE       VERSION
135/tcp   open  msrpc         Microsoft Windows RPC
139/tcp   open  netbios-ssn   Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds?
5040/tcp  open  unknown
49664/tcp open  msrpc         Microsoft Windows RPC
49665/tcp open  msrpc         Microsoft Windows RPC
49666/tcp open  msrpc         Microsoft Windows RPC
49667/tcp open  msrpc         Microsoft Windows RPC
49669/tcp open  msrpc         Microsoft Windows RPC
49670/tcp open  msrpc         Microsoft Windows RPC
49680/tcp open  msrpc         Microsoft Windows RPC
49689/tcp open  msrpc         Microsoft Windows RPC
MAC Address: 08:00:27:81:A3:70 (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running (JUST GUESSING): Microsoft Windows 10|2019|Longhorn|7|2008|Vista|11|8.1|XP (98%)
OS CPE: cpe:/o:microsoft:windows_10 cpe:/o:microsoft:windows cpe:/o:microsoft:windows_7::sp1 cpe:/o:microsoft:windows_server_2008:r2 cpe:/o:micro
soft:windows_8 cpe:/o:microsoft:windows_vista::sp1 cpe:/o:microsoft:windows_8.1 cpe:/o:microsoft:windows_xp::sp3
Aggressive OS guesses: Microsoft Windows 10 1709 - 1909 (98%), Microsoft Windows Server 2019 (96%), Microsoft Windows 10 1709 - 1803 (96%), Micro
soft Windows Longhorn (94%), Microsoft Windows 10 1703 (93%), Microsoft Windows 10 2004 (93%), Microsoft Windows 7 SP1 (93%), Microsoft Windows S
erver 2008 R2 (92%), Microsoft Windows 8 (92%), Microsoft Windows Vista SP1 (92%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_nbstat: NetBIOS name: BLENDTESTER, NetBIOS user: <unknown>, NetBIOS MAC: 08:00:27:81:a3:70 (Oracle VirtualBox virtual NIC)
| smb2-security-mode:
```

```
Host script results:
|_nbstat: NetBIOS name: BLENDTESTER, NetBIOS user: <unknown>, NetBIOS MAC: 08:00:27:81:a3:70 (Oracle VirtualBox virtual NIC)
| smb2-security-mode:
|   3:1:1:
|_    Message signing enabled but not required
|_clock-skew: 23s
| smb2-time:
|   date: 2024-07-17T20:33:52
|_  start_date: N/A
```

```
Nmap scan report for 10.0.2.15
Host is up (0.00030s latency).
Not shown: 65521 closed tcp ports (reset)
PORT      STATE SERVICE       VERSION
135/tcp   open  msrpc         Microsoft Windows RPC
139/tcp   open  netbios-ssn   Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds?
5040/tcp  open  unknown
5357/tcp  open  http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Service Unavailable
7680/tcp  open  pando-pub?
49664/tcp open  msrpc         Microsoft Windows RPC
49665/tcp open  msrpc         Microsoft Windows RPC
49666/tcp open  msrpc         Microsoft Windows RPC
49667/tcp open  msrpc         Microsoft Windows RPC
49670/tcp open  msrpc         Microsoft Windows RPC
49671/tcp open  msrpc         Microsoft Windows RPC
49672/tcp open  msrpc         Microsoft Windows RPC
49691/tcp open  msrpc         Microsoft Windows RPC
MAC Address: 08:00:27:C5:4D:77 (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Microsoft Windows 10
OS CPE: cpe:/o:microsoft:windows_10
OS details: Microsoft Windows 10 1709 - 1909
Network Distance: 1 hop
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
| smb2-time:
|   date: 2024-07-17T20:33:53
```

```
Host script results:
| smb2-time:
|   date: 2024-07-17T20:33:53
|_  start_date: N/A
| smb2-security-mode:
|   3:1:1:
|_    Message signing enabled but not required
|_nbstat: NetBIOS name: BLENDTS, NetBIOS user: <unknown>, NetBIOS MAC: 08:00:27:c5:4d:77 (Oracle VirtualBox virtual NIC)
|_clock-skew: 23s

Post-scan script results:
| clock-skew:
|   23s:
|     10.0.2.7
|_    10.0.2.15
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 4 IP addresses (4 hosts up) scanned in 203.51 seconds
```

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 tp fetch more information*