


[illegible]

<b>Name</b>	Windows Recon: Zenmap
<b>URL</b>	<a href="https://attackdefense.com/challengedetails?cid=2218">https://attackdefense.com/challengedetails?cid=2218</a>
<b>Type</b>	Windows Reconnaissance: Host Discovery

**Important Note:** This document illustrates all the important steps required to complete this lab. This is by no means a comprehensive step-by-step solution for this exercise. This is only provided as a reference to various commands needed to complete this exercise and for your further research on this topic. Also, note that the IP addresses and domain names might be different in your lab.

**Step 1:** Checking the IP address.

**Command:** ipconfig

 Administrator: Windows PowerShell

```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

PS C:\Users\Administrator> ipconfig

Windows IP Configuration

Ethernet adapter Ethernet:

    Connection-specific DNS Suffix  . : ap-southeast-1.compute.internal
    Link-local IPv6 Address . . . . . : fe80::1c7a:651c:35f4:2a45%4
    IPv4 Address. . . . . : 10.0.17.63
    Subnet Mask . . . . . : 255.255.240.0
    Default Gateway . . . . . : 10.0.16.1
PS C:\Users\Administrator>
```

**Step 2:** Run Zenmap scan against the subnet to discover the target machine's IP address.

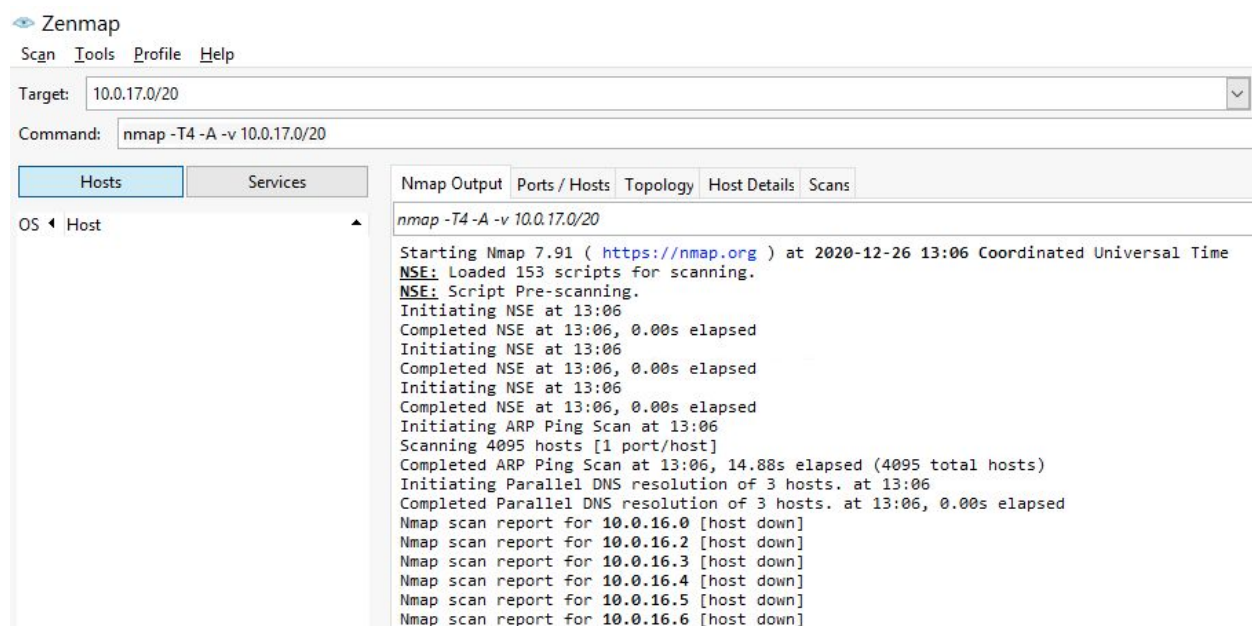
**Command:** nmap -T4 -A -v 10.0.17.0/20

## Zenmap:

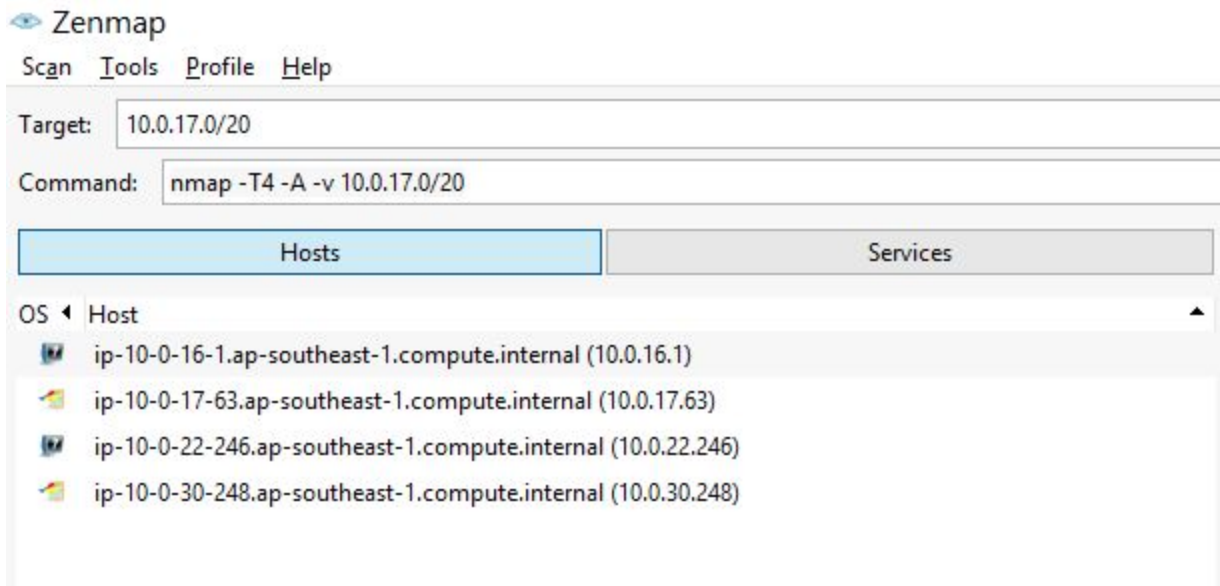
“Zenmap is the official Nmap Security Scanner GUI. It is a multi-platform (Linux, Windows, Mac OS X, BSD, etc.) free and open-source application that aims to make Nmap easy for beginners to use while providing advanced features for experienced Nmap users. Frequently used scans can be saved as profiles to make them easy to run repeatedly. A command creator allows the interactive creation of Nmap command lines. Scan results can be saved and viewed later. Saved scan results can be compared with one another to see how they differ. The results of recent scans are stored in a searchable database.”

**Source:** <https://nmap.org/zenmap/>

We will be scanning the target using default Zenmap options.

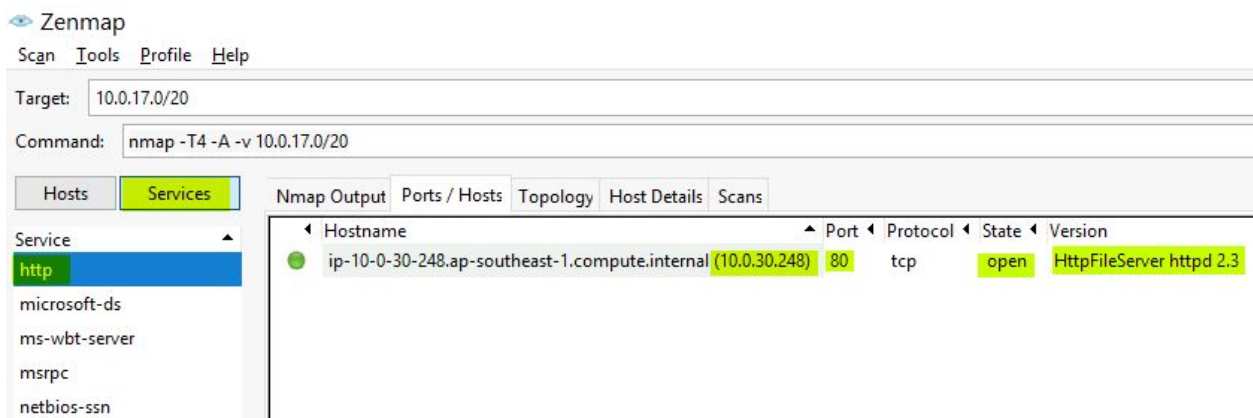


**Note:** The scan would take 3-5 minutes. Also, the output of live hosts would be different and that is completely normal.



We have discovered four hosts using Zenmap. We can switch the tab to “**Services**” and we can observe that when we select the “Services” tab, it filters the output of all host machines by open ports.

Zenmap has discovered port 80 on only one host i.e 10.0.30.248.



We have also discovered that port 80 is running HFS 2.3.

Select “**msrpc**” service and we can observe that two machines are exposed to RPC ports.



Zenmap

Scan Tools Profile Help

Target: 10.0.17.0/20

Command: nmap -T4 -A -v 10.0.17.0/20

Hosts Services

Service

- http
- microsoft-ds
- ms-wbt-server
- msrpc**
- netbios-ssn

Nmap Output Ports / Hosts Topology Host Details Scans

Hostname	Port	Protocol	State	Version
ip-10-0-17-63.ap-southeast-1.compute.internal (10.0.17.63)	135	tcp	open	Microsoft Windows RPC
ip-10-0-30-248.ap-southeast-1.compute.internal (10.0.30.248)	135	tcp	open	Microsoft Windows RPC
ip-10-0-30-248.ap-southeast-1.compute.internal (10.0.30.248)	49154	tcp	open	Microsoft Windows RPC
ip-10-0-30-248.ap-southeast-1.compute.internal (10.0.30.248)	49155	tcp	open	Microsoft Windows RPC
ip-10-0-30-248.ap-southeast-1.compute.internal (10.0.30.248)	49175	tcp	open	Microsoft Windows RPC

We can also plot the alive hosts diagram using Topology → Fisheye

Zenmap

Scan Tools Profile Help

Target: 10.0.17.0/20

Command: nmap -T4 -A -v 10.0.17.0/20

Hosts Services

Service

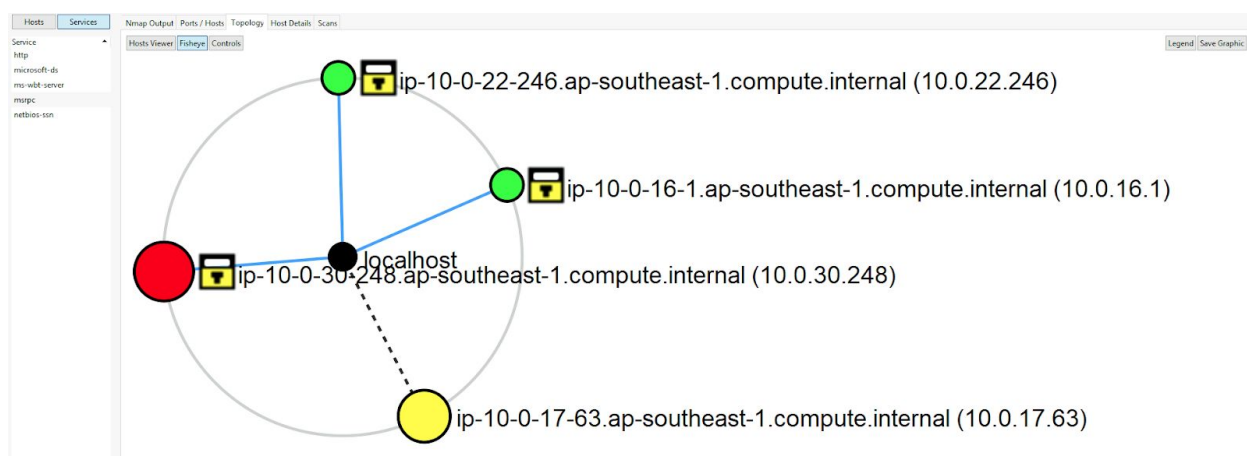
- http
- microsoft-ds
- ms-wbt-server
- msrpc
- netbios-ssn


Nmap Output Ports / Hosts **Topology** Host Details Scans

Hosts Viewer **Fisheye** Controls

1

2





In the plotted diagram we can see that the “Yellow” colored one is the machine i.e 10.0.17.63 where we have launched the scan (that is, the attacker machine) and it has plotted the other hosts connection with hostname and IP addresses to localhost.

Color “Green” means the machine is accessible. Color “Red” means the machine is alive but not responding or not directly accessible.

### References:

1. Zenmap (<https://nmap.org/zenmap/>)
2. Nmap (<https://nmap.org/>)