THM{Nmap Live Host Discovery} - Severity: Medium

Gravite & guyizdez

1 Introduction

We're two friends who share a passion for cybersecurity and solving challenges, so we team up to tackle TryHackMe and Hackthebox boxes. Whether it's cracking codes, exploiting vulnerabilities, or learning new skills, we do it for the thrill of the challenge and the fun of problem-solving together. This time we picked the Nmap Live Host Discovery room from THM.

2 Task 3

To determine the IP-Range that is defined by the Classless Inter-Domain Routing (CIDR) we can use the Subnet-Calculator.

However we can also calculate it by hand as follows:
When scanning the network `10.10.12.13/29`, Nmap determines the subnet based on the provided CIDR notation.

Step 1: Understanding CIDR /29

CIDR `/29` means the subnet mask is 29 bits long:

- Subnet mask in binary: `11111111.11111111.11111111.11111000`
- Subnet mask in decimal: `255.255.255.248`

Network size:

- A `/29` subnet has $2^{(32-29)} = 8$ total IP addresses.

Step 2: Identify the Subnet Range

The subnet range is determined by aligning the given IP address (`10.10.12.13`) to the nearest multiple of the subnet size.

- **Subnet increment:**
  - Increment size is $256 - 248 = 8$. Each `/29` subnet has blocks of 8 IPs.
- **Find the base network address:**
  - Divide the last octet of the IP (`13`) by the increment (`8`) and round down:

$$13 \div 8 = 1 \quad \text{(remainder 5, discard the remainder)}$$

  - Multiply the result (`1`) by `8` to find the base network address:

$$\text{Base address} = 10.10.12.(1 \times 8) = 10.10.12.8$$

- **Calculate the range:**
  - Starting address (network address): `10.10.12.8`
  - Broadcast address: `10.10.12.(8 + 8 - 1)` = `10.10.12.15`
  - Usable range for hosts in this subnet: `10.10.12.9` to `10.10.12.14`.

Step 3: Determine the First Scanned IP

Nmap starts scanning from the first usable host IP, which is:

10.10.12.9

The first IP address Nmap would scan in the `10.10.12.13/29` subnet is: `10.10.12.9`.

How Many IPs Nmap Will Scan for a Range?

To calculate the total number of IP addresses Nmap will scan for the range `10.10.0-255.101-125`, we need to break it down systematically.

Step 1

- `10.10.0-255`:
  - Represents all possible values in the third octet, i.e., from `0` to `255`.
  - Total values = `256`.
- `101-125`:
  - Represents all possible values in the fourth octet, i.e., from `101` to `125`.
  - Total values = $125 - 101 + 1 = 25$.

Step 2

For each of the `256` values in the third octet (`0` to `255`), there are `25` values in the fourth octet (`101` to `125`). The total number of IPs is the product of these two ranges:

$$256 \times 25 = 6400 \text{ IP addresses.}$$

Nmap will scan **6,400 IP addresses** for the range `10.10.0-255.101-125`. We can also just use the following command: nmap -sL -n 10.10.12.13/29 to see how many devices are being scanned.

3 Summary

What we learned is the *nmap* usage, and we can define the cheat sheet as the key takeaway from this room like Comparitech-NMAP-CheatSheet or Stationx-NMAP-CheatSheet