**Nmap Basic Port Scans**

1. Introduction

This room explains:

* TCP connect port scan
* TCP SYN port scan
* UDP port scan

1. TCP and UDP ports

Để đơn giản hóa quá mức, chúng ta có thể phân loại cảng thành hai trạng thái:

* Cổng mở cho biết có một số dịch vụ đang lắng nghe trên cổng đó.
* Cổng đóng cho biết không có dịch vụ nào đang lắng nghe trên cổng đó.

Tuy nhiên, trong các tình huống thực tế, chúng ta cần xem xét tác động của tường lửa. Ví dụ, một cổng có thể mở, nhưng tường lửa có thể chặn các gói tin. Do đó, Nmap xem xét sáu trạng thái sau:

1. Open : biểu thị rằng một dịch vụ đang lắng nghe trên cổng được chỉ định.
2. Closed: chỉ ra rằng không có dịch vụ nào đang lắng nghe trên cổng được chỉ định, mặc dù cổng có thể truy cập được. Khi nói có thể truy cập được, chúng tôi muốn nói rằng nó có thể truy cập được và không bị chặn bởi tường lửa hoặc các thiết bị/chương trình bảo mật khác.
3. Filtered : có nghĩa là Nmap không thể xác định cổng mở hay đóng vì cổng không thể truy cập được. Trạng thái này thường là do tường lửa ngăn Nmap tiếp cận cổng đó. Các gói tin của Nmap có thể bị chặn không cho tiếp cận cổng; hoặc ngược lại, các phản hồi bị chặn không cho tiếp cận máy chủ của Nmap .
4. Unfiltered : có nghĩa là Nmap không thể xác định cổng đang mở hay đóng, mặc dù cổng có thể truy cập được. Trạng thái này gặp phải khi sử dụng quét ACK -sA.
5. Open | Filtered : Điều này có nghĩa là Nmap không thể xác định được cổng đang mở hay đã lọc.
6. Closed | Filtered: Điều này có nghĩa là Nmap không thể quyết định xem một cổng có bị đóng hay bị lọc hay không.
7. TCP Flags
8. TCP Connect Scan
9. TCP SYN Scan
10. UDP Scan
11. Fine-Tuning Scope and Performance
12. Summary

This room covered three types of scans.

| **Port Scan Type** | **Example Command** |
| --- | --- |
| TCP Connect Scan | **nmap -sT 10.10.164.75** |
| TCP SYN Scan | **sudo nmap -sS 10.10.164.75** |
| UDP Scan | **sudo nmap -sU 10.10.164.75** |

These scan types should get you started discovering running TCP and UDP services on a target host.

| **Option** | **Purpose** |
| --- | --- |
| **-p-** | all ports |
| **-p1-1023** | scan ports 1 to 1023 |
| **-F** | 100 most common ports |
| **-r** | scan ports in consecutive order |
| **-T<0-5>** | -T0 being the slowest and T5 the fastest |
| **--max-rate 50** | rate <= 50 packets/sec |
| **--min-rate 15** | rate >= 15 packets/sec |
| **--min-parallelism 100** | at least 100 probes in parallel |