Enumerate like a Legend

w/ Nmap

The Network Mapper

0xh0russ

01

Introduction

What is Nmap?

02

Under the Hood

How does it work?

03

Scanning Hosts

Basic Usage

04

The Scripting Engine

Enumeration on steroids.

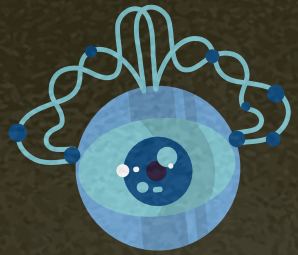
05

Further Learning

Get Good

INTRODUCTION

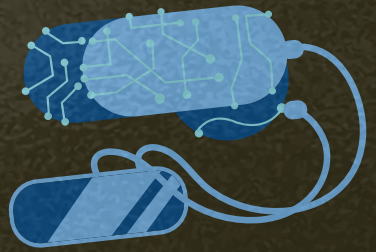
What Is Nmap?



What is Nmap?

- Open-Source tool for network exploration.
- Commonly used in Security Auditing.
- Scans ports and enumerates services.

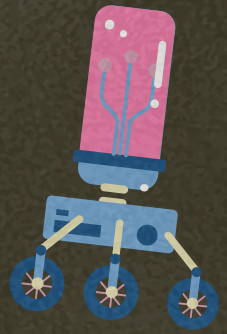
```
# nmap -A -T4 scanme.nmap.org

Nmap scan report for scanme.nmap.org (74.207.244.221)
Host is up (0.029s latency).
rDNS record for 74.207.244.221: li86-221.members.linode.com
Not shown: 995 closed ports
PORT     STATE    SERVICE     VERSION
22/tcp   open     ssh         OpenSSH 5.3p1 Debian 3ubuntu7 (protocol 2.0)
| ssh-hostkey: 1024 8d:60:f1:7c:ca:b7:3d:0a:d6:67:54:9d:69:d9:b9:dd (DSA)
|_2048 79:f8:09:ac:d4:e2:32:42:10:49:d3:bd:20:82:85:ec (RSA)
80/tcp   open     http        Apache httpd 2.2.14 ((Ubuntu))
|_http-title: Go ahead and ScanMe!
646/tcp  filtered ldp
1720/tcp filtered H.323/Q.931
9929/tcp open     nping-echo  Nping echo
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6.39
OS details: Linux 2.6.39
Network Distance: 11 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:kernel

TRACEROUTE (using port 53/tcp)
HOP RTT      ADDRESS
[Cut first 10 hops for brevity]
11  17.65 ms li86-221.members.linode.com (74.207.244.221)

Nmap done: 1 IP address (1 host up) scanned in 14.40 seconds
```



Origins of the Network Mapper

First Version

Nmap was first released on September 1st, 1997. It was written by Gordon Lyon.



Phrack Magazine

Issue 51, Article 11.

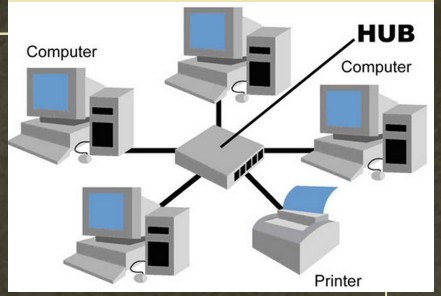
“Despite what you have heard from the media, the Internet is NOT all about TCP port 80.”

Under the Hood

How does it work?

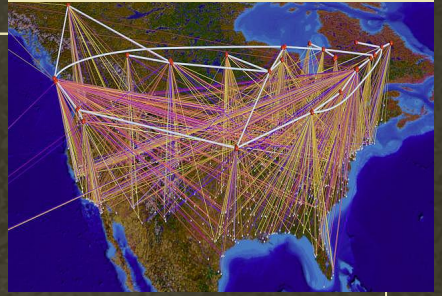
Network Topology

Typical Home Network



This is what is called a star topology. Everyone connects to a central router.

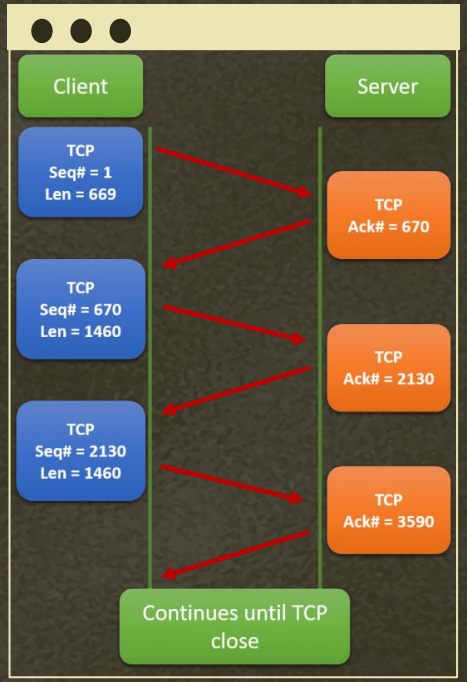
The U.S.



Shit ton of links.

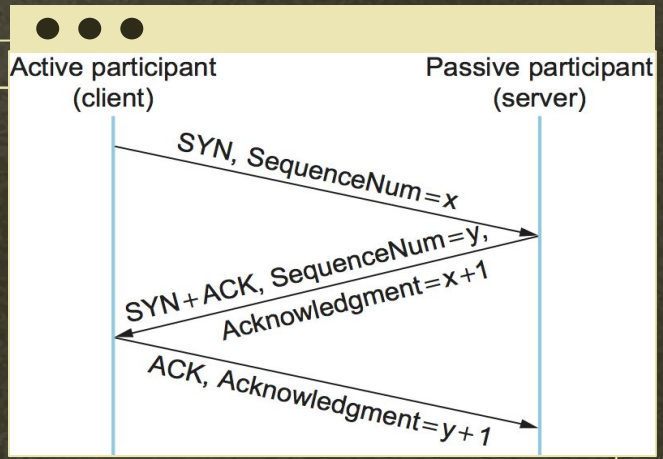
TCP Transmission Control Protocol

- Provides a reliable data stream.
  - Handles packet loss.
- Ensures in-order delivery.
  - Handles out-of order packets
  - Handles duplicates.
- Provides Congestion-Control



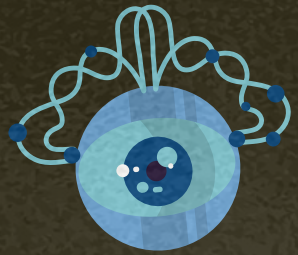
Three-way Handshake

The process of establishing a TCP connection between two hosts.



Scanning Hosts

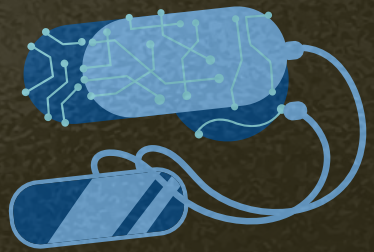
More than meets the eye



Nmap

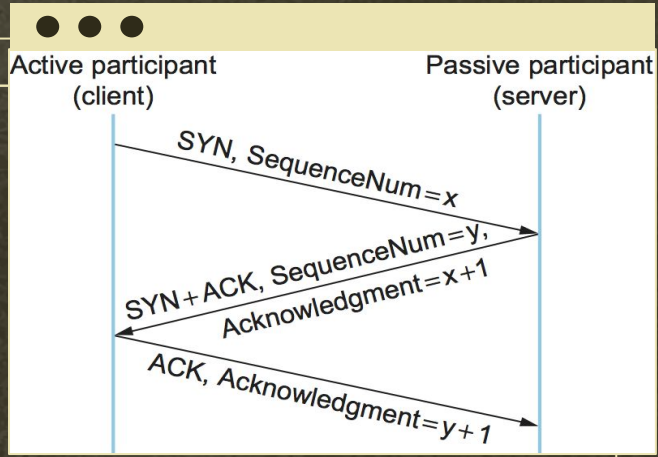
- TCP scan types
  - TCP Connect Scan (-sT)
  - TCP SYN Scan (-sS)
  - TCP FIN Scan (-sF)
- Version scan (-sV)

NMAP



TCP Connect Scan [-sT]

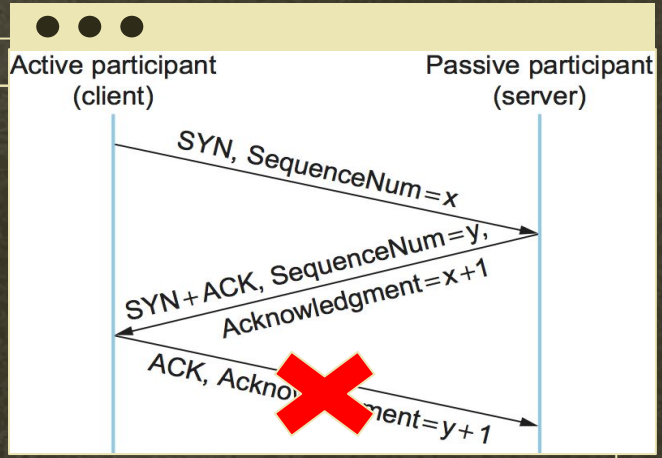
- Calls the `connect()` syscall.
- If the connection succeeds then the port is open.
- Easily detectable and filterable.



TCP SYN Scan [-sS]

- Does not send the final ACK in handshake.
- Half-open, incomplete connection.

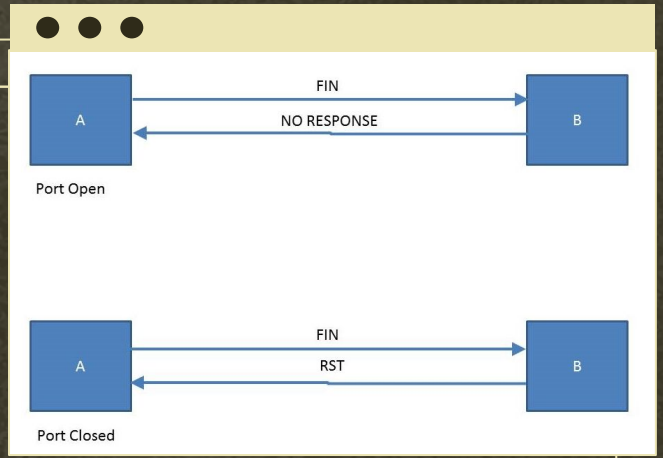
- Pro: fewer hosts will log it.
- Con: Needs root privs.



TCP FIN Scan [-sF]

- Sends a FIN packet.
- Open ports ignore FIN packets.
- You can only be sure if a port is closed.

- Pro: Fewer logs than SYN scans.
- Con: Unreliable

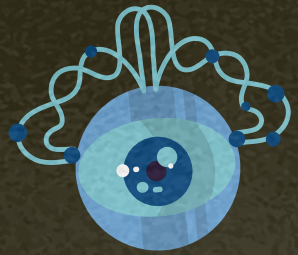


nmap Version Scan [-sV]

- Establishes a connection.
- Grabs the service banner.
- Sends specially crafted probes and analyzes response

- Pro: Unreliable
- Con: Fewer logs than SYN scans.

```
oxdf@hacky$ nmap -p 22,80 -sCV 10.10.11.156
Starting Nmap 7.80 ( https://nmap.org ) at 2022-07-25 15:49 UTC
Nmap scan report for 10.10.11.156
Host is up (0.090s latency).

PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.6p1 Ubuntu 4ubuntu0.6 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 02:5e:29:0e:a3:af:4e:72:9d:a4:fe:0d:cb:5d:83:07 (RSA)
|   256 41:e1:fe:03:a5:c7:97:c4:d5:16:77:f3:41:0c:e9:fb (ECDSA)
|_  256 28:39:46:98:17:1e:46:1a:1e:a1:ab:3b:9a:57:70:48 (ED25519)
80/tcp open  http    nginx 1.14.0 (Ubuntu)
|_http-server-header: nginx/1.14.0 (Ubuntu)
|_http-title: Late - Best online image tools
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

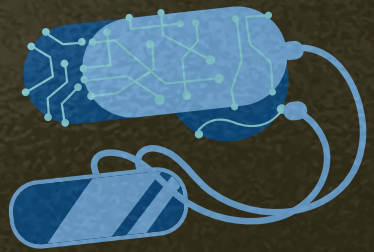


Recap

- TCP scan types
  - TCP Connect Scan (-sT)
  - TCP SYN Scan (-sS)
  - TCP FIN Scan (-sF)
- Version scan (-sV)

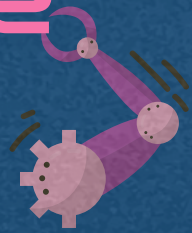
- `nmap <options> -p <ports> <target-ip>`
- `nmap -sS -sV -p- 127.0.0.1`

NMAP



Nmap Scripting Engine

Enumeration on Steroids

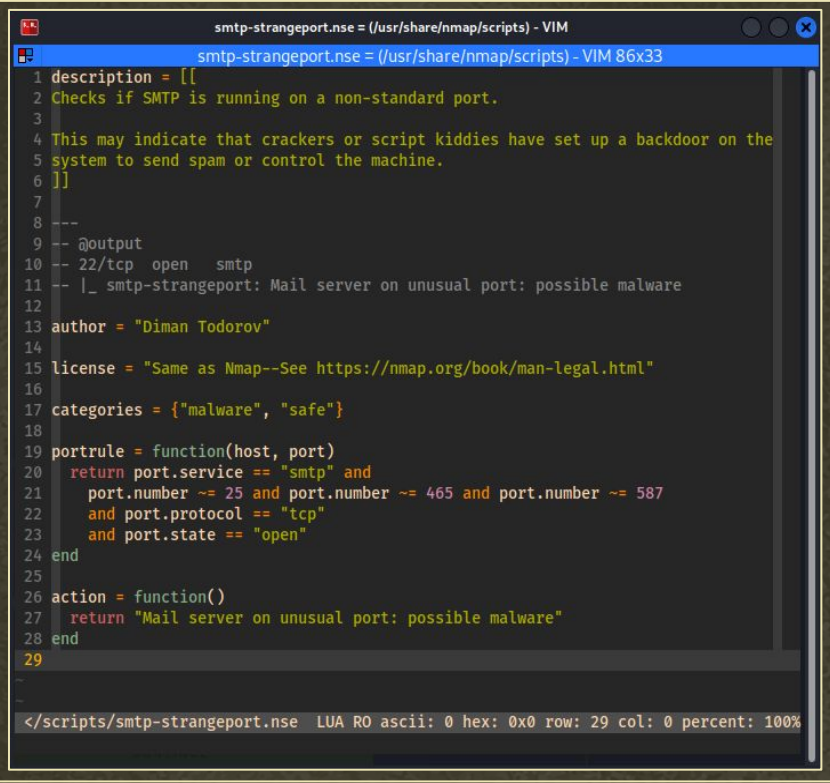


nmap Scripting Engine

- Makes nmap versatile and extensible.
- Scripts written Lua + nmap library (API)
- Scripts are organized into 13 categories:
  - `brute`, `default`. `discovery`, `dos`, `fuzzer`...
- Automates finding and exploiting vulns.

```
oxdf@hacky$ nmap -p 22,80 -sCV 10.10.11.156
Starting Nmap 7.80 ( https://nmap.org ) at 2022-07-25 15:49 UTC
Nmap scan report for 10.10.11.156
Host is up (0.090s latency).

PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.6p1 Ubuntu 4ubuntu0.6 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 02:5e:29:0e:a3:af:4e:72:9d:a4:fe:0d:cb:5d:83:07 (RSA)
|   256 41:e1:fe:03:a5:c7:97:c4:d5:16:77:f3:41:0c:e9:fb (ECDSA)
|_  256 28:39:46:98:17:1e:46:1a:1e:a1:ab:3b:9a:57:70:48 (ED25519)
80/tcp open  http    nginx 1.14.0 (Ubuntu)
|_http-server-header: nginx/1.14.0 (Ubuntu)
|_http-title: Late - Best online image tools
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

Nmap Script Format



smtp-strangeport.nse

Checks if SMTP is running on a non-standard port.

Standard Fields

Description, author, license, categories, portrule, action

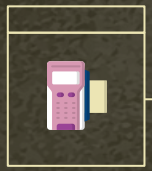
Further Learning

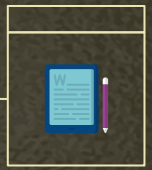
What now?

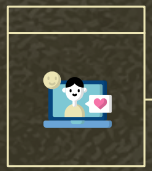
Learning Resources

Nmap Book

(Power User Level)
https://nmap.org/book/toc.html







man Page

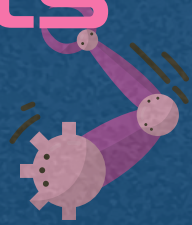
(Regular User Level)
Simply RTFM

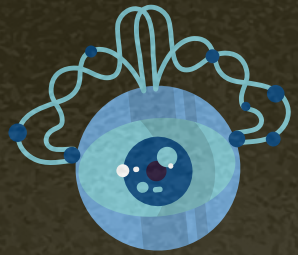
Github Src

(Developer Level)
https://github.com/nmap/nmap

Maximizing Your Results

Get the most for your work





Tips

- Curb your perfectionism
- Invest in your people-skills
- Burn yourself out occasionally.

NMAP