NMAP

Nmap (“Network Mapper“) é um software livre que realiza port scan desenvolvido pelo Gordon Lyon, autoproclamado hacker "Fyodor".

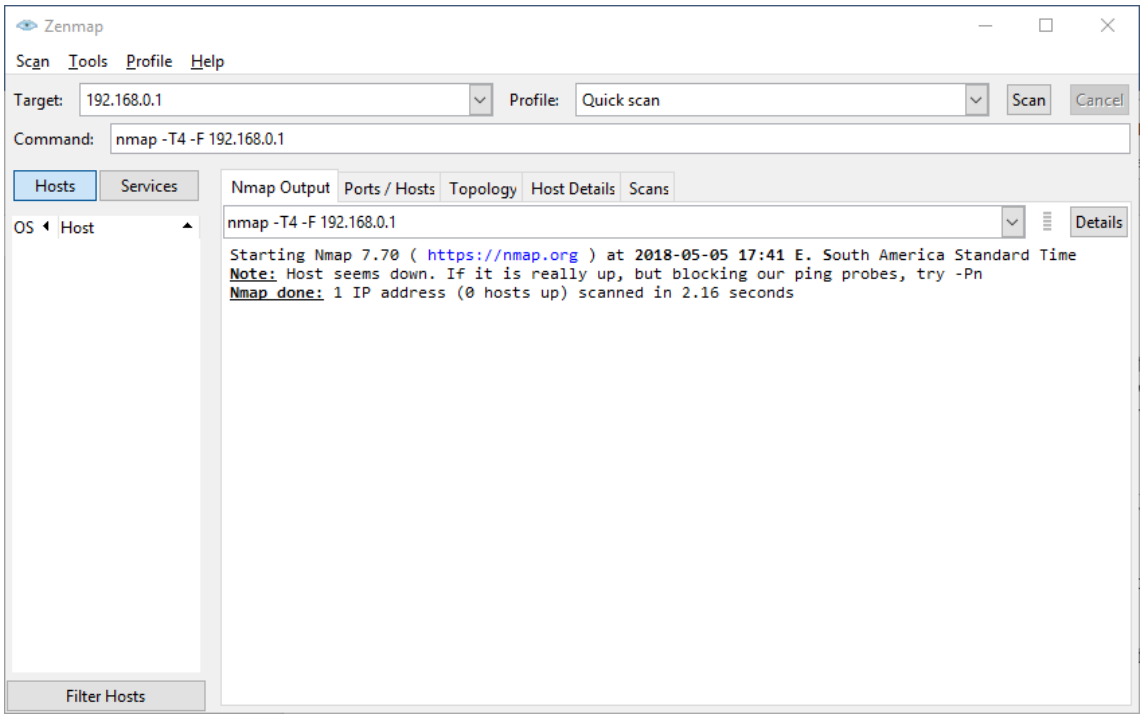
O NMAP é um utilitário de exploração e auditoria de segurança. geralmente é utilizado na linha comando, porem você fazer o uso do ZenMap que é uma interface gráfica amigável onde os comandos podem ser executados e interpretados.

Esse é um dos mais conhecidos softwares utilizados para scan de portas, detecção de SO e muito mais.

É possível baixar o nmap no site https://nmap.org/. Nas aulas do treinamento eu uso o nmap no Windows e no Kali Linux no qual já vem com o nmap instalado.

A instalação completa da ferramenta para Windows também faz a instalação do

- **NPCap** – Biblioteca de captura
- **Zenmap** – Que é um frontEnd do Nmap
- **Ncat** – Implementação do NetCat para nmap
- **Ndiff** – Usado para comparação do XML do nmap
- **Nping** – gerador de pacotes



Principais parâmetros do NMAP

Parametro Nmap	Tipo de escaneamento
-sn	PING Scan
-sO	IP Scan
-sV	Tenta identificar serviço/versões das porta
-sT	TCP connect scan
-sS	SYN scan
-sF	FIN scan
-sX	XMAS tree scan
-sN	Null scan
-sP	Ping scan
-sU	UDP scan
-sO	Protocol scan
-sA	ACK scan
-sW	Windows scan
-sR	RPC scan
-sL	List / DNS scan
-sI	Idle scan
-Po	Don’t ping
-PT	TCP ping
-PS	SYN ping
-PI	ICMP ping
-PB	TCP and ICMP ping
-PB	ICMP timestamp
-PM	ICMP netmask
-oN	Normal output
-oX	XML output
-oG	Greppable output
-oA	All output
-T Paranoid	Serial scan; 300 sec entre os scans
-T Sneaky	Serial scan; 15 sec entre os scans
-T Polite	Serial scan; .4 sec entre os scans
-T Normal	Parallel scan
-T Aggressive	Parallel scan, 300 sec timeout, e 1.25 sec/probe
-T Insane	Parallel scan, 75 sec timeout, e .3 sec/probe

Exemplos de comandos

Escaneamento rápido de um host
nmap -F 192.168.0.1

Escaneamento rápido de uma rede
nmap -F 192.168.0.0/24

Escaneamento de duas redes com detalhes e ping usando o Ping scan
nmap -v -sn 192.168.0.0/16 10.0.0.0/8

Analisar porta 80
nmap -p 80 192.168.0.1

Analisar porta 53 UDP
nmap -p U:53 192.168.0.1

Exibir programas e versões
map -sv 192.168.0.1

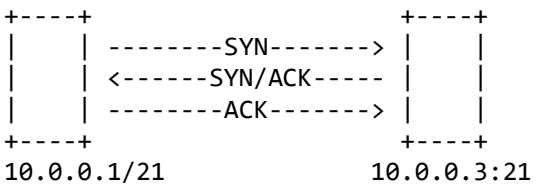
Analisar firewall (Pacotes Fragmentados)
nmap -f 192.168.2.2

Scan com MAC Spoofing
nmap -v -sT -PN --spoof-mac 0 192.168.0.1.

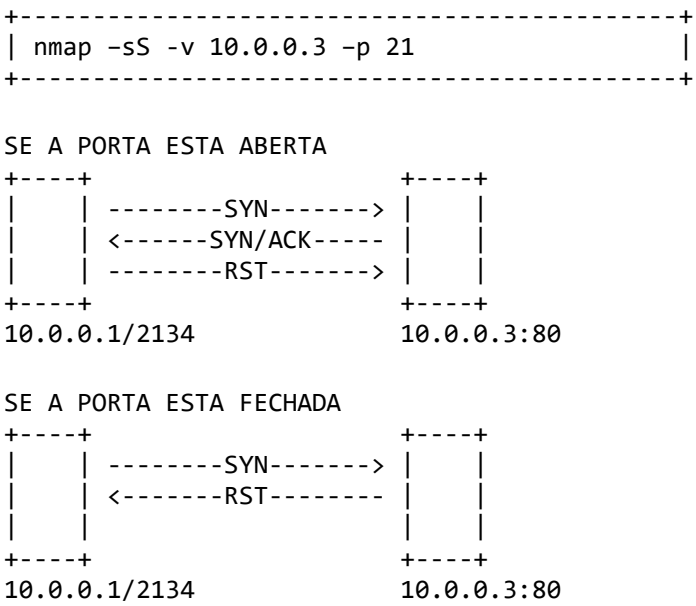
HALF/SYN/XMAS/FIN/NULL Scans com Nmap

Para entender bem esses tipos de escaneamento e seu resultado é importante que conheça bem o 3handshake, utilizado na comunicação do TCP/IP.

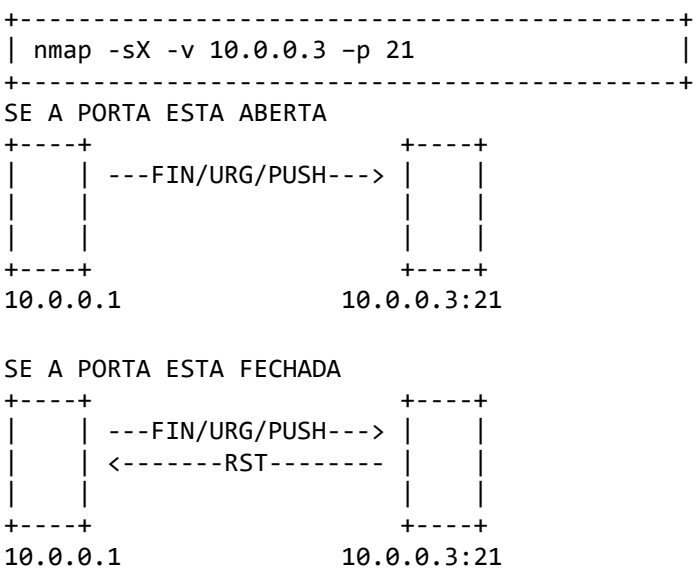
Three-way handshake



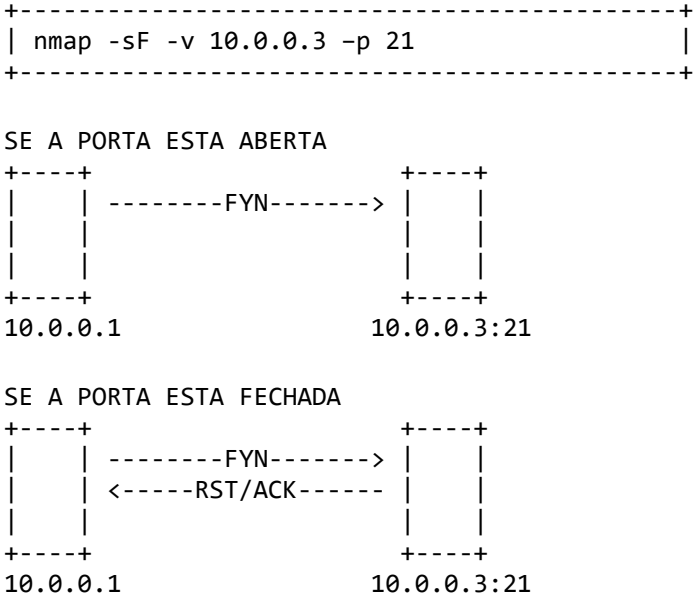
Stealth Scan (half-open scan)



Xmas Scan (Não funciona no Windows) RFC 793



FIN Scan (Não funciona no Windows) RFC 793



NULL Scan (Não funciona no Windows) RFC 793