

# Manual de Operações Linux & Windows

## Usando NMAP com Windows e Linux

### ### No Windows:

#### 1. \*\*Instalação:\*\*

- Baixe o instalador do Nmap do site oficial [nmap.org](https://nmap.org/download.html).
- Execute o instalador e siga as instruções na tela para instalar o Nmap.

#### 2. \*\*Executando o Nmap:\*\*

- Abra o Command Prompt (cmd).
- Digite `nmap` seguido do endereço IP que você deseja escanear. Exemplo:

```
...\n\nnmap 192.168.1.1\n\n
```

#### 3. \*\*Interpretando os Resultados:\*\*

- O Nmap exibirá uma lista de portas abertas e o respectivo serviço associado a cada porta.
- Por exemplo, se uma porta 80 estiver aberta, pode indicar um servidor web em execução.

### ### No Linux:

#### 1. \*\*Instalação:\*\*

- Abra o terminal.
- Dependendo da sua distribuição, use um dos seguintes comandos:
- Debian/Ubuntu: `sudo apt-get install nmap`
- Fedora: `sudo dnf install nmap`
- Arch: `sudo pacman -S nmap`

#### 2. \*\*Executando o Nmap:\*\*

- No terminal, digite `nmap` seguido do endereço IP. Exemplo:

```
...\n\nnmap 192.168.1.1\n\n
```

#### 3. \*\*Interpretando os Resultados:\*\*

- Assim como no Windows, o Nmap mostrará as portas abertas e os serviços correspondentes.

### ### Leitura dos Resultados:

- **Porta/Estado/Serviço:** Para cada porta, o Nmap informará o estado (aberto, fechado, filtrado) e o serviço

padrão associado a essa porta (por exemplo, HTTP para a porta 80).

- **Versões de Serviços:** Alguns comandos do Nmap podem detectar versões de serviços rodando nas portas abertas, fornecendo informações detalhadas sobre o software e a versão do serviço.

- **Hosts e IPs:** O Nmap também exibe informações sobre o host, incluindo o endereço IP e, às vezes, o nome do host.

- **Outras Informações:** Dependendo das opções usadas, o Nmap pode fornecer informações adicionais, como sistemas operacionais suspeitos e serviços rodando em portas incomuns, o que pode indicar configurações personalizadas ou mesmo vulnerabilidades.

### ### Exemplo de Saída do Nmap:

```
...
```

Nmap scan report for 192.168.1.1 Página 1 / 2

# Manual de Operações Linux & Windows

Host is up (0.00080s latency).

```
PORT STATE SERVICE
```

```
21/tcp open ftp
```

```
22/tcp open ssh
```

```
80/tcp open http
```

```
443/tcp open https
```

```
```\n
```

Neste exemplo, o Nmap encontrou quatro portas abertas: FTP (21), SSH (22), HTTP (80) e HTTPS (443). Cada uma destas portas está associada a um serviço de rede comum.

### Dicas Adicionais:

- **Use com Permissão:** Sempre tenha permissão explícita para escanear uma rede ou um endereço IP.
- **Opções Avançadas:** O Nmap tem muitas opções avançadas, incluindo detecção de versão de serviço (`-sV`), detecção de sistema operacional (`-O`), e muito mais.
- **Documentação:** Consulte a documentação oficial do Nmap para mais informações e opções avançadas.

Lembrando que este é um guia básico, e o Nmap é uma ferramenta muito poderosa com muitas opções e capacidades avançadas. É recomendável consultar a documentação oficial do Nmap para um entendimento mais profundo e para aprender sobre as práticas recomendadas de uso.

ID de solução único: #1020

Autor:: Admin

Última atualização: 2024-01-15 10:27