Nmap

O Nmap é uma ferramenta de port-scan muito poderosa, com ele nós podemos encontrar portas abertas rodando diferentes serviços a fim de encontrar algum serviço vulnerável ou brecha no sistema, os diferentes parâmetros do Nmap nos permite ver quais serviços certa porta está rodando e algumas vezes até qual sistema operacional está sendo usado, vamos ver alguns desses parâmetros agora.

Para utilizar o Nmap em algum alvo específico em primeiro momento você pode apenas utilizar o ip ou nome de domínio desse alvo, por exemplo:

```
nmap 192.168.0.1

ou

nmap siteteste.com
```

Além disso você pode colocar quantos números de ip ou domínios você quiser, não precisa necessariamente fazer um de cada vez, uma jeito simples de usar o nmap em vários ips é fazendo um scanner por bloco, por exemplo:

```
nmap 192.168.0.1-20
```

Esse comando irá escanear todos os ips de 192.168.0.1 até 192.168.0.20.

Caso você queira fazer uma analise rápida você pode utilizar a flag -F, por exemplo:

```
nmap 192.168.0.1 -F
```

Utilizando a flag -p você define o número da porta que quer fazer um scanner, exemplo:

```
nmap -p 23 192.168.0.1
```

Se quiser você pode também usar mais de uma porta, basta adicionar uma vírgula:

```
nmap -p 22,23,80 192.168.0.1
```

Você pode procurar pelo sistema operacional que está rodando o serviço com a flag -O:

```
nmap 192.168.0.1 -O
```

Você pode utilizar a flag -sS para fazer um scan muito rápido que é também mais difícil de ser detectado, pois é um scan feito de forma camuflada:

```
nmap -sS 192.168.0.1
```

A flag -D permite que você envie pacotes através de um ip falso caso durante seus testes permitidos de forma legal seu ip seja bloqueado:

```
nmap -D 192.168.0.1
```

Essas foram algumas flags para você testar com o seu nmap, caso queira aprender mais sobre ele você pode visitar o site https://nmap.org/

jcesar_n

JulioCesarNSM

Obrigado!