

NMAP PASSO A PASSO

# VARREDURAS COMPLETA EM REDES

PARA QUEM UTILIZA *LINUX* OU *WINDOWS*



**PRÁTICO**  
MÉTODO RÁPIDO

# SUMÁRIO

## 1 Sumário

## 2 Introdução

- Direto ao ponto

## 3 Introdução básica em redes de computadores

- Lan
- Wan
- O que fazer com nmap (Exemplos)

## 8 Introdução ao NMAP

- O que é o nmap
- Estados das portas

## 13 NMAP na prática

- Download
- Grupos/Camadas

## 18 Comandos do NMAP

- TARGET SPECIFICATION
- HOST DISCOVERY
- PORT SCANNING TECHNIQUES
- SERVICE/VERSION DETECTION
- OS DETECTION
- SCRIPT SCAN (NSE)
- TIMING AND PERFORMANCE
- FIREWALL/IDS EVASION AND SPOOFING
- OUTPUT
- MISCELLANEOUS OPTIONS

# INTRODUÇÃO

## DIRETO AO PONTO

Primeiramente obrigado por confiar em meu trabalho e adquirir esse material exclusivo, **te garanto que esse material vai te ajudar a** entender como funciona uma varredura de redes em computadores.

Para estudar esse material é recomendado que você tenha conhecimento básico em redes de computadores.

Vamos direto ao ponto, não vamos ficar enrolando ou indo para outros assuntos, esse é um e-book curto e focado, para otimizar ao máximo o seu tempo (Tempo é dinheiro).

Lembre-se de me seguir no instagram.

@linux.gnu

PS: Esse material não está livre de erros de português.

**MATERIAIS  
PRODUZIDO POR  
MIM !**

saber mais



# GANHE DE R\$: 8.000 A R\$: 100.000 POR MÊS **ATRAVÉS DAS TECNOLOGIAS E PROJETOS** PRÁTICOS QUE LHE SERÃO ENSINADOS !



## QUERO APRENDER

# REDES DE COMPUTADORES

## INTRODUÇÃO BÁSICA

**Um breve lembrete,** redes de computadores são um conjunto de dispositivos e computadores conectados entre si, permitindo que os dispositivos troquem dados, compartilhem recursos e se comuniquem.

As redes são usadas para a transmissão de dados, bem como para o acesso aos serviços de rede, como o acesso à Internet, etc.

Existem vários tipos diferentes de redes, abaixo estão as mais "comuns":

- **LANs:** Redes locais
- **WANs:** Todo mundo
- **WI-FI** (wlan): Redes sem fio

Cada uma destas redes tem seu próprio conjunto de características e recursos. **Por exemplo, as LANs são utilizadas para conectar computadores dentro de uma mesma área**, enquanto as WANs são usadas para conectar computadores distantes.

## LAN

Local, por exemplo, dentro da sua casa ou empresa



192.168.1.29  
IP Local



192.168.1.2



192.168.1.25

IP Local



192.168.1.26

IP Local



**192.168.1.1** IP Local

O switch fica com 2 IPs diferentes

**1 IP Local (conexão lan)**

**1 IP Externo (conexão wan)**

**179.54.120.25**

**IP EXTERNO/PÚBLICO**

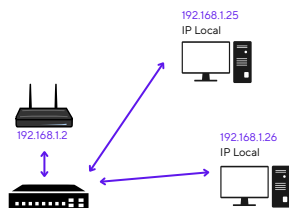
Fornecido pelo seu provedor

Cabo que vem da rua e conecta  
no seu switch, modem ou roteador

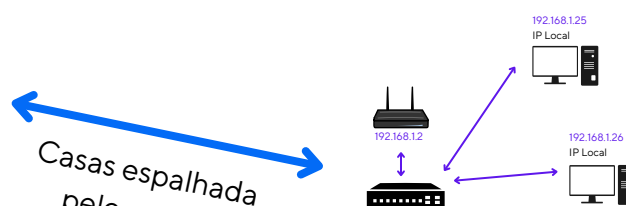


## WAN

O mundo  
rede global.



Casas espalhada  
pelo mundo

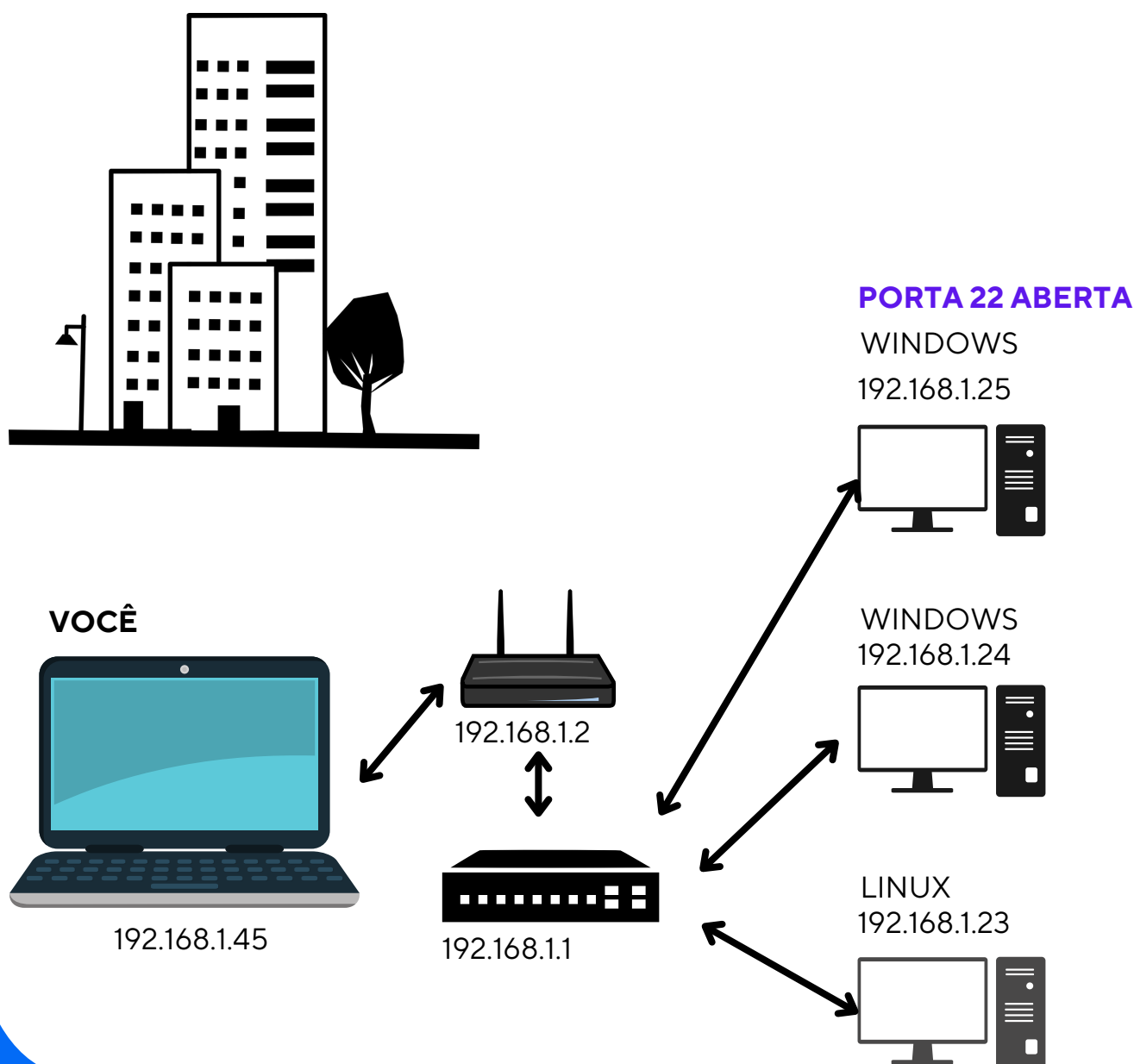


Casas espalhada  
pelo mundo

## EXEMPLO 1

Imagine que você é responsável pela rede de computadores de um call center, faculdade ou até mesmo prefeitura, são prédios com vários andares e centenas de computadores, todos estão conectados a rede, e **você precisa do inventário dessas redes e também mantê-las seguras.**

Vamos pegar o exemplo mais específico do callcenter, **você tem 120 computadores na rede** e por qualquer motivo que seja, você precisa saber quais estão "ATIVOS" na rede, seus IPs, sistema operacional ou até mesmo as portas que estão abertas, com o NMAP é possível apenas digitando um comando.



## EXEMPLO 2

Agora imagina que você é um hacker e foi contratado pela empresa XT para encontrar vulnerabilidades na infraestrutura, com o nmap você consegue fazer um scan em toda rede e entender como a infra da empresa está configurada ...

### Computadores ou IPs

45: Ativos

### Roteadores

tplink-XX: 192.168.1.2

vivoXX: 192.168.1.1

### Servidores

WEB Apache XX.XX

Impressão XX.XX

### Portas abertas

80: Serviço1 - Versão XX:XX

21: Serviço2 - Versão XX:XX

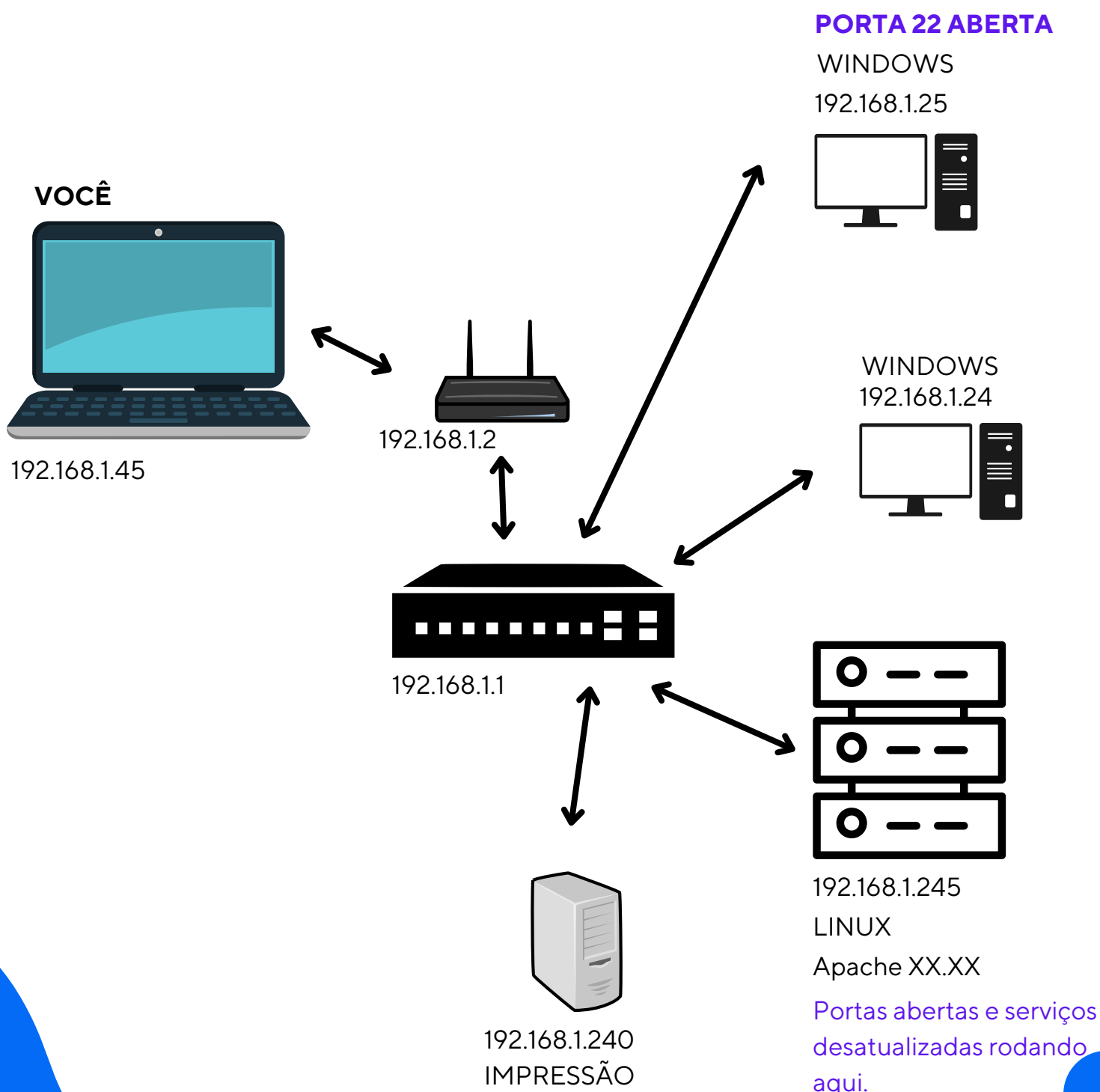
43: Serviço2 - Versão XX:XX

Vamos supor que nesse servidor WEB você descobriu que está rodando na **porta 80 uma versão de software antiga** e que essa versão possui **velhas vulnerabilidades já conhecidas** no mundo "hacker" então basta você rodar um script que já foi disponibilizado por "alguém" na internet e fazer o ataque ou atualizar o software para a nova versão, onde essas vulnerabilidades foram corrigidas.



Você como administrador de rede, hacker, analista, etc.

Precisa entender como a infra do local onde você está trabalhando está configurada, isso é praticamente obrigatório, e o nmap vai te ajudar nisso e **eu vou te mostrar exatamente como fazer.**



# INTRODUÇÃO AO NMAP

## O QUE É NMAP ?

Nmap (Network Mapper) **é uma ferramenta de scan de redes** e de código aberto, amplamente utilizada por profissionais de TI/Segurança e administradores de rede para identificar dispositivos conectados e vulnerabilidades nas redes de computadores.

Ele oferece recursos poderosos para profissionais de segurança que desejam testar a segurança de suas redes. O nmap é capaz de descobrir muitas informações, que podem ser de extrema importância, como:

- Endereços IP
- Portas abertas
- Serviços de rede e suas versões
- Sistema Operacional
- Mapeamento da topologia da rede

O Nmap também permite que os profissionais executem análises de segurança detalhadas sobre sua rede, permitindo a identificação de vulnerabilidades e a tomada de medidas corretivas.

As redes de computadores são complexas e possuem muitos pontos de vulnerabilidade.

Esses pontos de vulnerabilidade se referem ao risco de segurança que uma rede enfrenta devido a falhas nos protocolos, vulnerabilidades nos sistemas operacionais, falhas no hardware, falhas nos processos de segurança, falhas no gerenciamento de configuração ou falhas no controle de acesso.

As vulnerabilidades em redes de computadores **podem ser exploradas por cibercriminosos ou hackers para obter acesso** não autorizado a informações confidenciais ou privadas. Isso pode levar a perdas financeiras significativas, roubo de identidade, violação de privacidade e outros crimes cibernéticos.

Por isso, é importante que as empresas e usuários individuais invistam em soluções de segurança robustas para proteger seus sistemas. Isso inclui a implementação de medidas de segurança como firewalls, anti-vírus, monitoramento de rede, autenticação de usuário, criptografia e outras ferramentas de segurança.

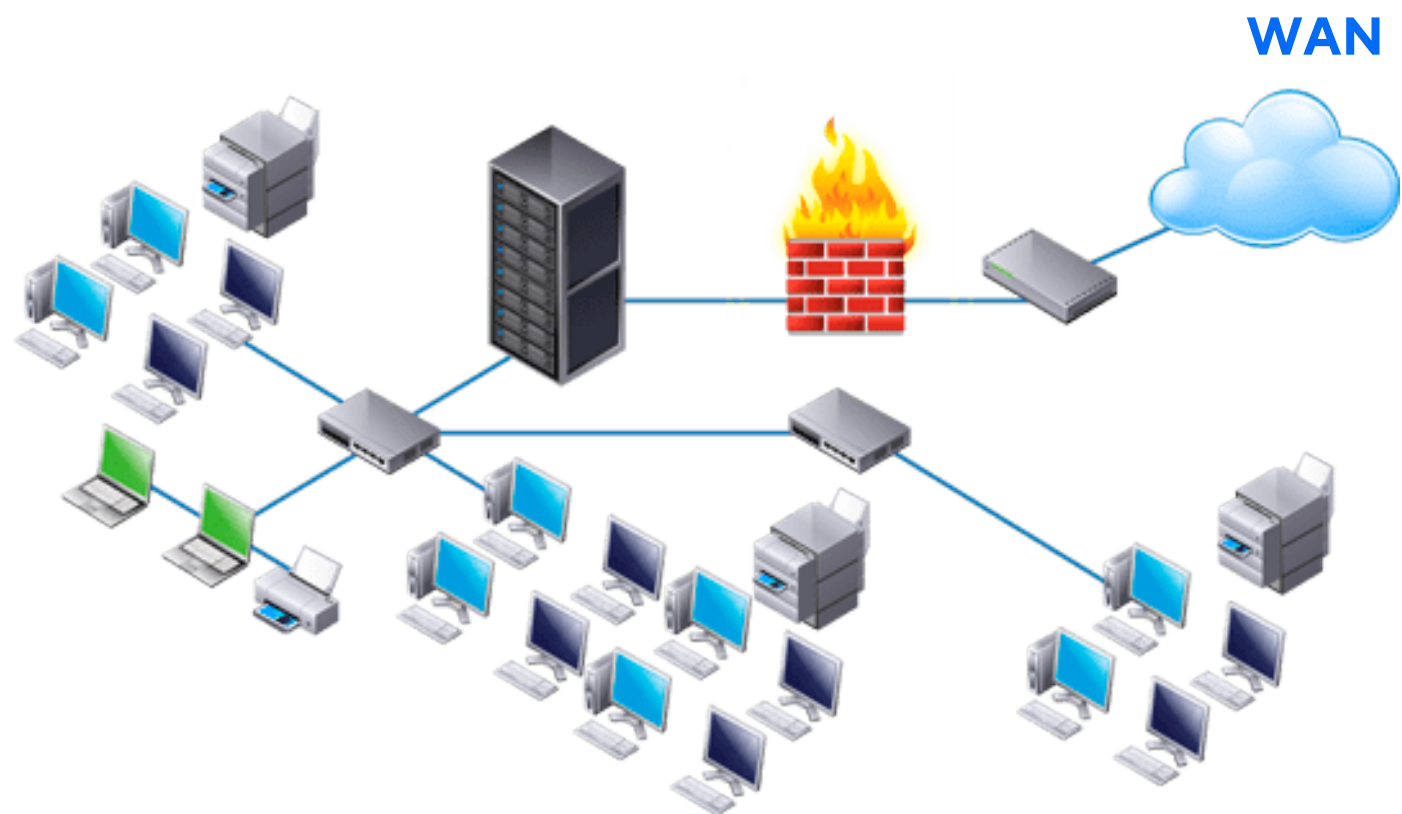
Além disso, é importante manter seus sistemas e hardware atualizados e monitorar a rede para identificar e corrigir quaisquer vulnerabilidades que possam ser exploradas. É também importante ter um plano de resposta a incidentes em caso de ataques bem definido e pronto para uso.

Usando essas medidas, as empresas e os usuários individuais podem minimizar seu risco de segurança e proteger suas redes contra essas ameaças.

Então o Nmap é uma ferramenta útil para profissionais de segurança que desejam garantir que sua rede esteja livre de ameaças.

Com a capacidade de detectar e identificar serviços, ele pode ajudar a garantir que a rede esteja segura e livre de vírus, malware e outras ameaças. Além disso, o Nmap oferece recursos poderosos para ajudar os usuários a monitorar sua rede e garantir que esteja protegida.

**Agora que vamos entender como o nmap funciona de fato**, a forma como será explicado aqui você não vai encontrar em nenhum outro lugar, te garanto que você vai terminar esse e-book entendendo como o nmap funciona e vai saber usá-lo.



# PORTAS

Uma porta em uma rede de computadores é um mecanismo usado para controlar o tráfego de dados entre computadores.

É utilizada para identificar e direcionar o tráfego de dados entre computadores conectados à rede. **As portas são numeradas e cada porta tem um propósito específico.** Por exemplo, a porta 80 é usada para o protocolo HTTP, enquanto a porta 443 é usada para o protocolo HTTPS.

As portas também podem ser usadas para controlar o acesso à rede, permitindo que apenas certos tipos de tráfego sejam permitidos.

Existem **65.536 portas**.

## COMO O NMAP ENXERGA AS PORTAS

**Aberta:** Uma aplicação está aceitando ativamente conexões TCP ou pacotes UDP.

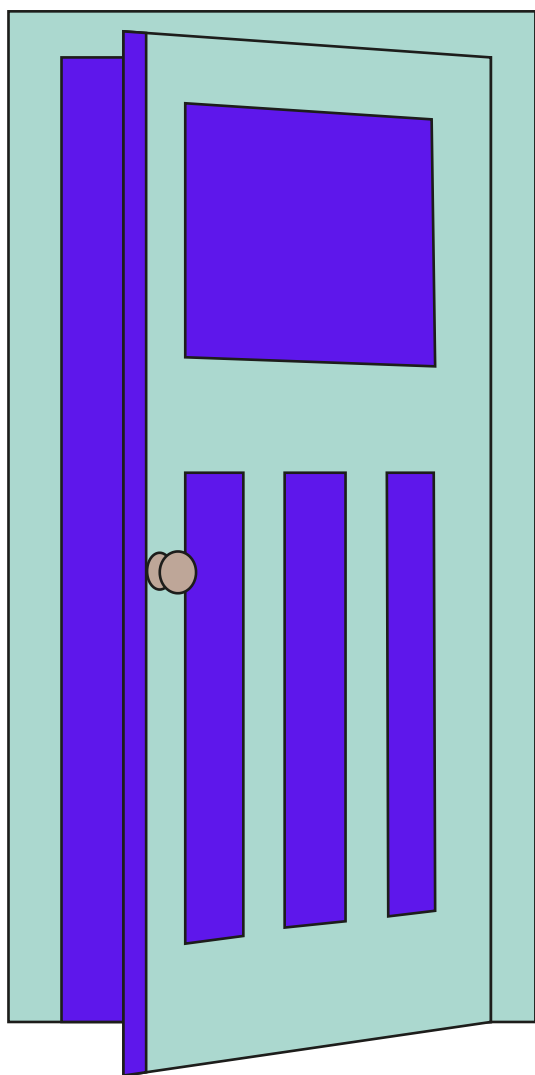
**Fechada:** Está acessível ou seja ela recebe e responde a pacotes de sondagens do Nmap, porém não há nenhuma aplicação ouvindo nela.

**Filtered:** O Nmap não consegue determinar se a porta está aberta porque uma filtragem de pacotes impede que as sondagens alcancem a porta. A filtragem poderia ser de um dispositivo firewall dedicado, regras de roteador, ou um software de firewall baseado em host.

**unfiltered:** O estado não filtrado significa que uma porta está acessível, mas que o Nmap é incapaz de determinar se ela está aberta ou fechada.

**open|filtered:** O Nmap coloca portas neste estado quando é incapaz de determinar se uma porta está aberta ou filtrada. Isso acontece para tipos de scan onde as portas abertas não dão nenhuma resposta.

Imagine as portas como portas reais, você está em um prédio e cada porta (sala) que vê é para algo específico, como advogado, RH, TI, etc. Algumas portas estão abertas outras fechadas, outras com uma brecha ou aberta sem ninguém, sem proteção.



**Aberta**

**Fechada**

**Filtered**

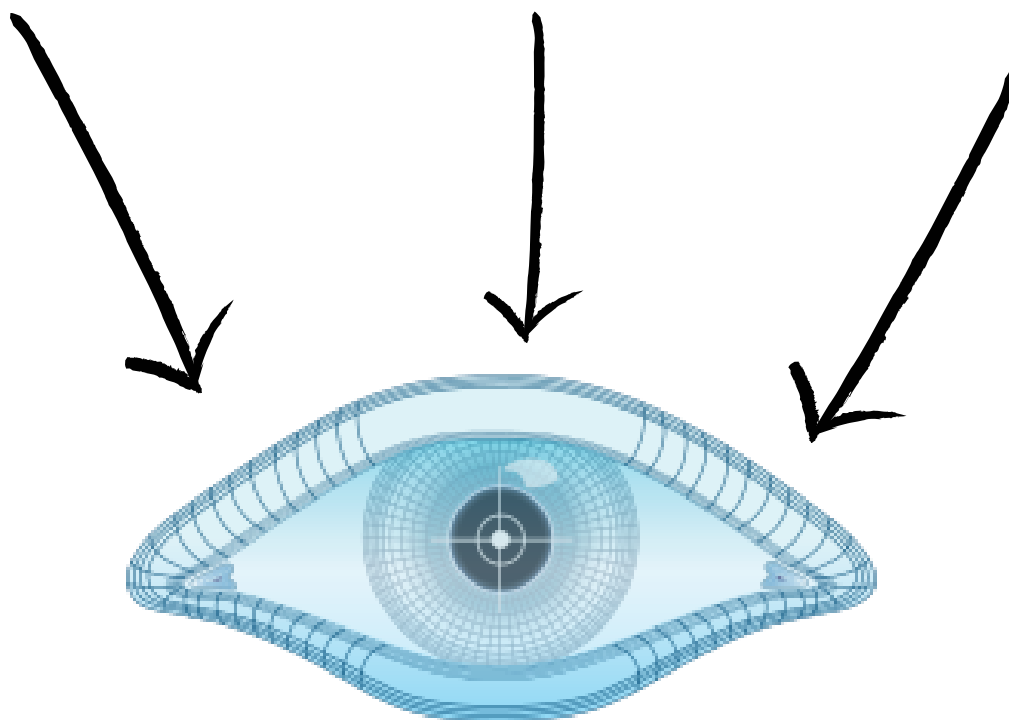
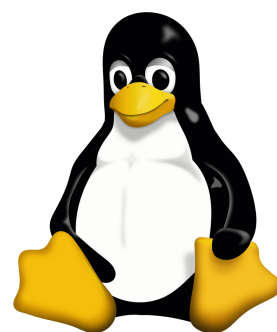
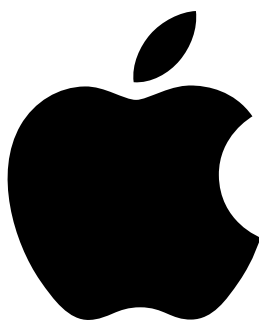
**unfiltered**

**open|filtered**

# NMAP NA PRÁTICA

## O SISTEMA

O nmap está disponível em diversos sistemas operacionais, como o Windows, MAC e claro Linux.



# NMAP

Para fazer a instalação basta acessar o site oficial e escolha o seu sistema operacional.

<https://nmap.org/download.html>

O nmap utiliza pacotes IPs para fazer varreduras nas redes, através do envio desses pacotes é que ele consegue descobrir tais informações, o envio pode ser feito em redes grandes/enormes ou em um único alvo.

Vamos **dividir as funções do nmap por grupos** e seus respectivos comandos, vou tentar deixar fácil o entendimento para que qualquer um possa entender rápido.

# SCAN

## ALVOS

TARGET SPECIFICATION

HOST DISCOVERY

## + INVASIVO

PORT SCANNING

SERVICE/VERSION

OS DETECTION

SCRIPT SCAN

FIREWALL/IDS

## OPÇÕES

TIMING AND PERFORMANCE

OUTPUT

MISC



## **TARGET SPECIFICATION**

### **ALVO ESPECÍFICO**

Faz uma varredura em um determinado **alvo específico ou em listas** quem contenham hosts. Por exemplo, seu servidor DHCP pode exportar uma lista de 10.000 concessões atuais que você deseja verificar.

## **HOST DISCOVERY**

### **DESCOBERTA DE HOSTS**

Descobrendo os hosts que estão na rede, ele usa vários métodos para detectar hosts, incluindo ping sweeps, port scans e protocolos de descoberta de host.

## **PORT SCANNING TECHNIQUES**

### **TÉCNICAS DE VARREDURA DE PORTAS**

Descobre quais portas estão abertas e fechadas. O Nmap usa um processo chamado port scanning para descobrir quais portas estão abertas em um host específico ou em um conjunto de hosts. O port scanning envolve enviar pacotes de dados para cada porta em um host e analisar as respostas, se uma porta estiver aberta, o Nmap pode determinar qual serviço está sendo executado na porta.

## **SERVICE/VERSION DETECTION**

### **DETECÇÃO DE SERVIÇO E VERSÃO**

Vai descobrir quais serviços suas versões estão ativos em um host, isso é muito útil, pois pode analisar software e suas versões, que podem estar desatualizados e estão rodando naquela máquina.

## OS DETECTION

### DETECÇÃO DE SISTEMA OPERACIONAL

O Nmap vai descobrir qual sistema operacional o host está rodando, às vezes você precisa executar uma varredura específica para ter certeza do sistema, também pode ser usado para detectar serviços específicos, como servidores web, servidores de e-mail e outros serviços.

### SCRIPT SCAN (NSE)

Execução de scripts para automatizar varreduras de redes. Permite aos usuários executar scripts personalizados para detectar vulnerabilidades na rede.

## TIMING AND PERFORMANCE

### VELOCIDADE DA VARREDURA

Permite aos usuários ajustar o tempo de execução de seus escaneamentos, também permite que os usuários ajustem o nível de detalhamento de seus escaneamentos, desde o mais básico até o mais detalhado, você pode alterar a velocidade do scan, **indo de 0 a 5**.

## FIREWALL/IDS EVASION AND SPOOFING

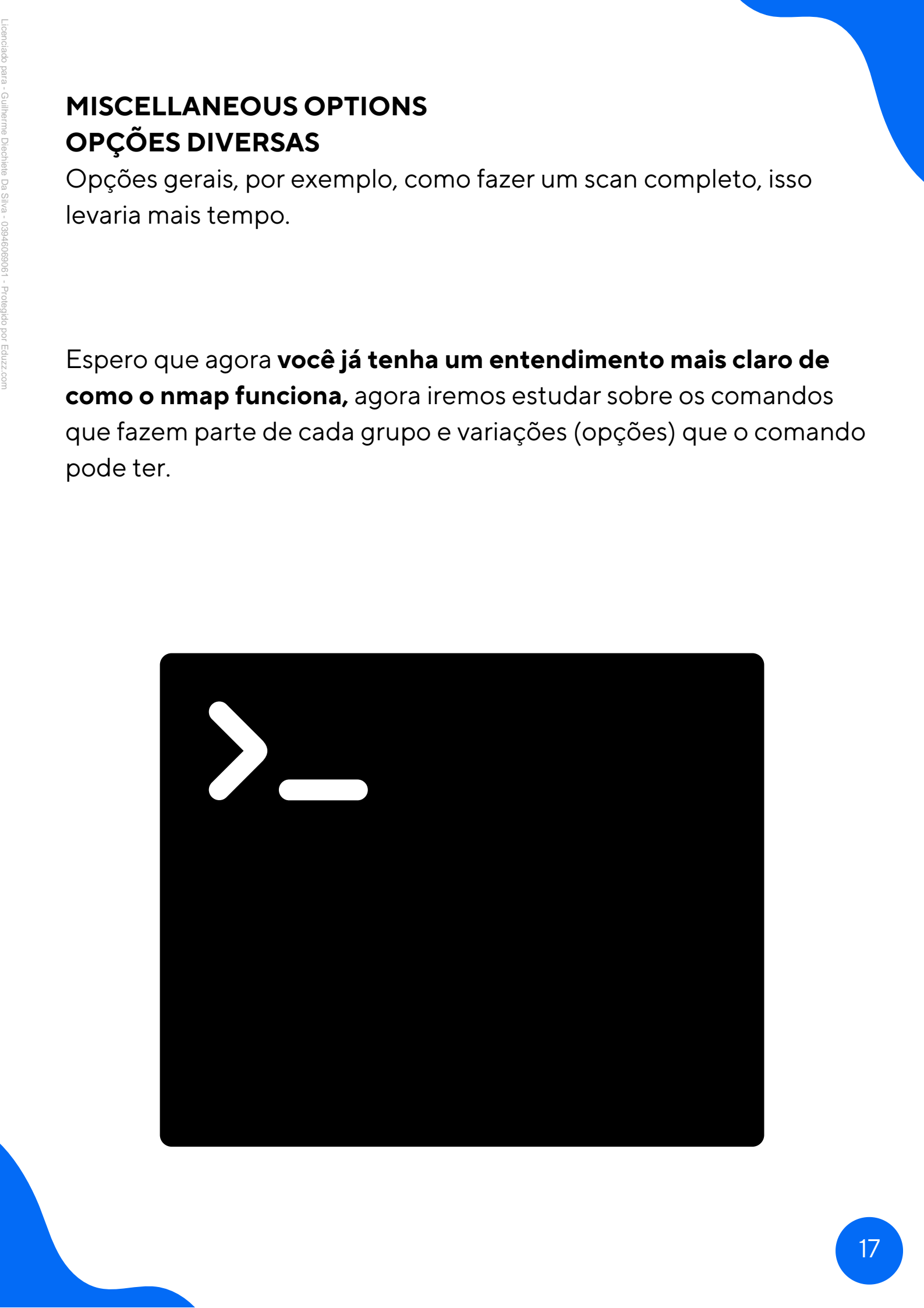
### EVASÃO E FALSIFICAÇÃO DE FIREWALL/IDS

Algumas opções para tentar burlar o firewall e IPS.

## OUTPUT

### Saída

Modos de saída, mostra os pacotes sendo enviados e recebidos, como o verbose, debugging, arquivo.txt



## MISCELLANEOUS OPTIONS

### OPÇÕES DIVERSAS

Opções gerais, por exemplo, como fazer um scan completo, isso levaria mais tempo.

Espero que agora **você já tenha um entendimento mais claro de como o nmap funciona**, agora iremos estudar sobre os comandos que fazem parte de cada grupo e variações (opções) que o comando pode ter.



# COMANDOS

Agora vamos **entender como é a estrutura dos comandos** do nmap. Letras minúsculas e maiúsculas fazem diferença.

*Os print desses comando foram rodados em WINDOWS para você ver como é simples, no Linux é a mesma coisa.*

## NMAP [TIPO DE SCAN] [OPÇÕES] [ALVO OU LISTA]

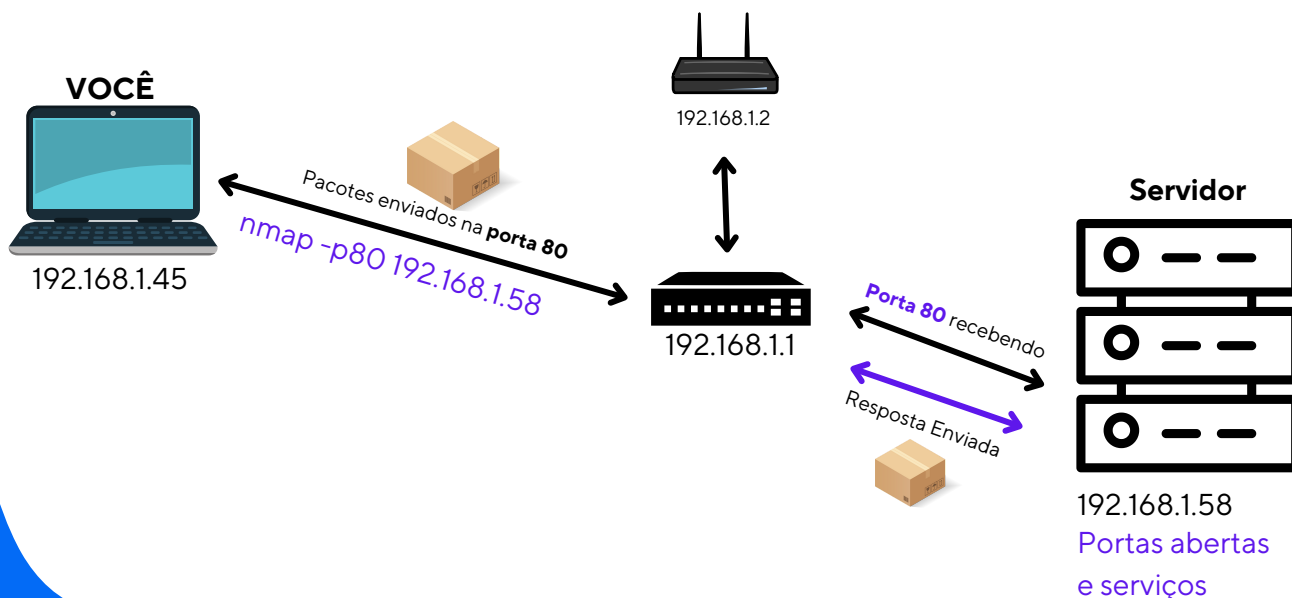
### TARGET SPECIFICATION

**#nmap -p80 192.168.1.58**

**-p80:** Scan padrão na porta 80 com *ping scan* em um determinado

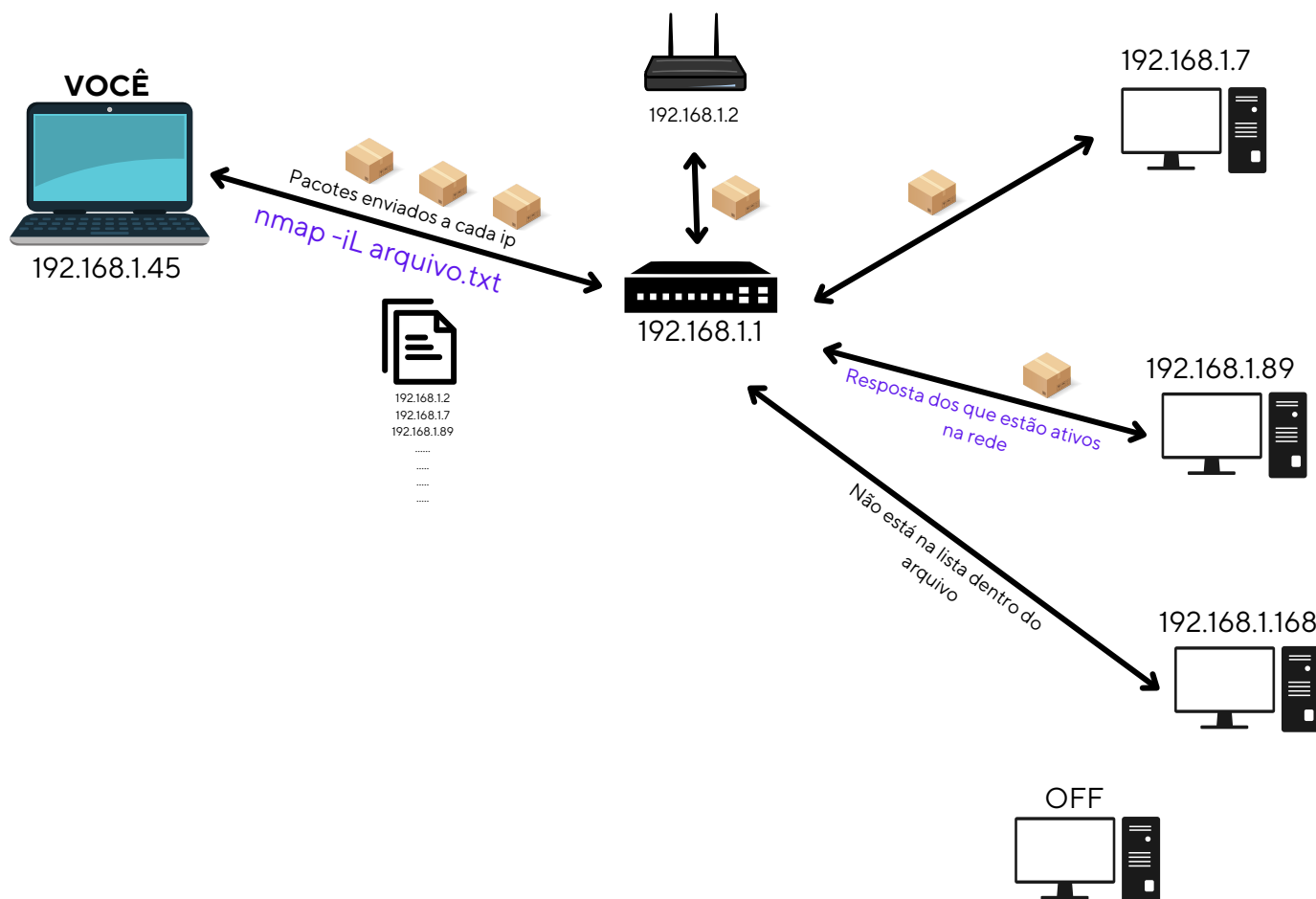
```
C:\Users\ferna>nmap 192.168.15.58
Starting Nmap 7.93 ( https://nmap.org ) at 2023-01-30 18:57 Hora oficial do Brasil
Nmap scan report for fernando-mkt (192.168.15.58)
Host is up (0.00095s latency).
Not shown: 996 closed tcp ports (reset)
PORT      STATE SERVICE
135/tcp    open  msrpc
139/tcp    open  netbios-ssn
445/tcp    open  microsoft-ds
5357/tcp   open  wsapi
Nmap done: 1 IP address (1 host up) scanned in 0.37 seconds
```

Veja como já mostrou algumas informações como portas abertas(não especifiquei a porta 80), protocolos e serviços rodando no host.



## #nmap -iL hosts.txt

**-iL (inputfilename):** Passar uma lista enorme de hosts , Por exemplo, seu servidor DHCP pode exportar uma lista de 10.000 concessões atuais que você deseja verificar.



## #nmap -iL hosts.txt --excludefile hosts2.txt

**--excludefile:** Não faz Scan em nos hosts que estão no arquivo chamado hosts2.txt ou seja você poderia especificar uma lista de hosts para não receberem os pacotes. Pacotes podem "alarmar" um firewall por exemplo.

## HOST DISCOVERY

### #nmap -sL 192.168.1.0/24

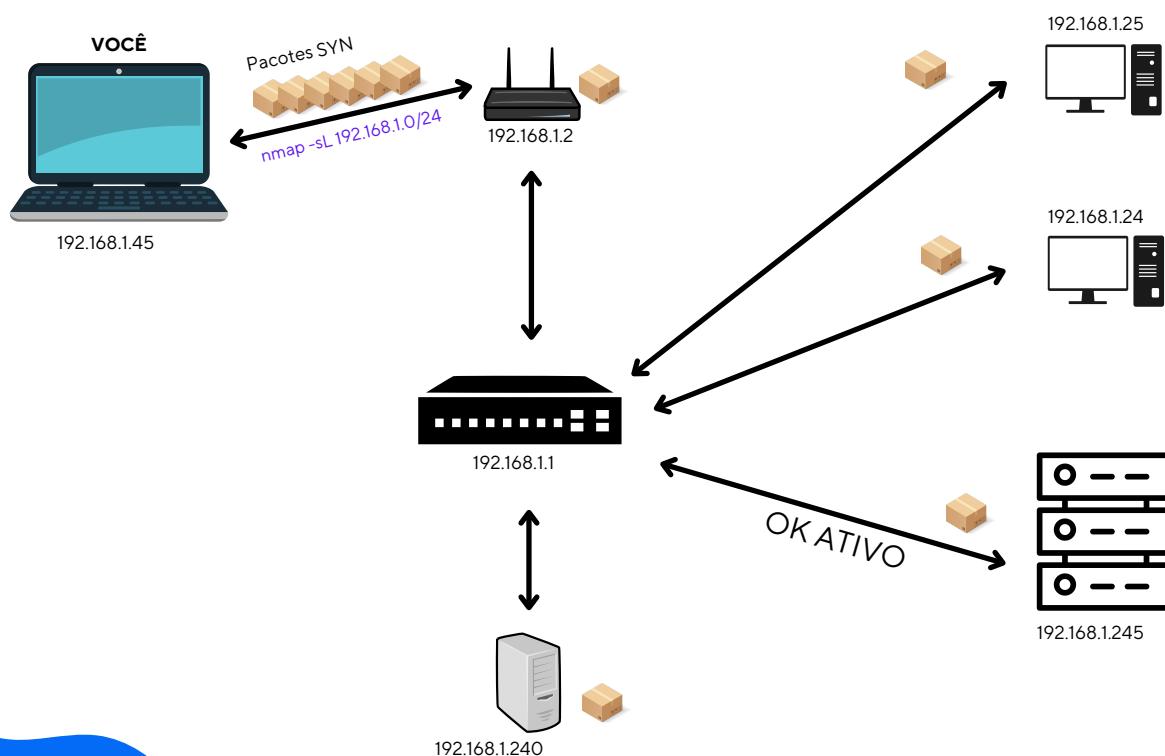
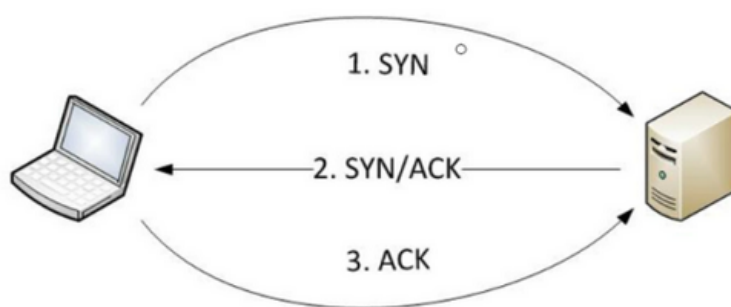
**-sL (List Scan):** É uma forma de descobrir os hosts que estão ativos na rede toda, ele envia um **pacote SYN**. Ele não realiza varredura de portas ou serviços, mas simplesmente lista os endereços IP ativos

```
Nmap scan report for dudu-mint (192.168.15.50)
Nmap scan report for 192.168.15.51
Nmap scan report for M2006C3MG-Redmi9C (192.168.15.52)
Nmap scan report for 192.168.15.53
Nmap scan report for 192.168.15.54
Nmap scan report for 192.168.15.55
```

No exemplo acima, eu fiz um scan em minha rede **192.168.15.0/24**

Note os dispositivos ATIVOS e seus IPs foram identificados.

### PACOTE SYN



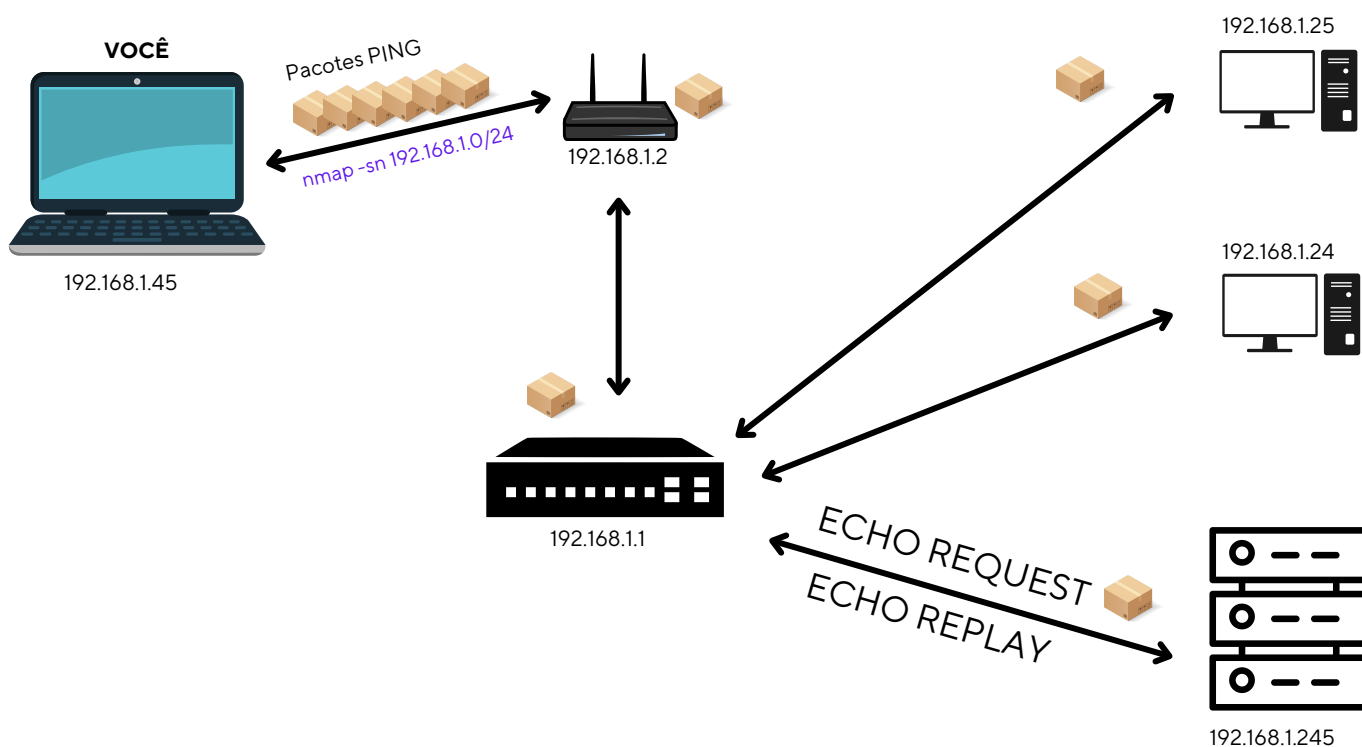
## #nmap -sn 192.168.1.0/24

**-sn: (Ping Scan):** Ele envia **pacotes de ping** para todos os endereços IP em uma rede específica e, em seguida, analisa as respostas para determinar quais hosts estão ativos na rede. Esse scan é útil para descobrir **quais hosts estão retornando os ping**.

Administradores de sistemas frequentemente acham esta opção valiosa. Ela pode ser facilmente utilizada para contar o número de máquinas disponíveis em uma rede ou monitorar a disponibilidade dos servidores.


```
C:\Users\ferna>nmap -sn 192.168.15.0/24
Starting Nmap 7.93 ( https://nmap.org ) at 2023-02-01 10:04 Hora oficial do Brasil
Nmap scan report for 192.168.15.24
Host is up (0.0010s latency).
MAC Address: C8:22:02:2C:CD:F8 (Unknown)
Nmap scan report for M2006C3MG-Redmi9C (192.168.15.52)
Host is up (0.083s latency).
MAC Address: AC:1E:9E:C1:A1:C8 (Xiaomi Communications)
Nmap scan report for 192.168.15.59
```

No exemplo acima, são enviados "pacotes de ping/ICMP Echo Request"



## #nmap -Pn 192.168.1.0/24

**-Pn (Sem Ping Scan):** É usado para realizar um escaneamento de portas **sem enviar pacotes de ping**. Isso significa que o nmap não tentará determinar se o alvo está ativo ou não, mas simplesmente começará a escanear as portas. Isso pode ser útil em situações em que o alvo está bloqueado para ping ou quando você deseja escanear um alvo sem alertá-lo.

 Prompt de Comando

```
C:\Users\ferna>nmap -Pn 192.168.15.0/24
Starting Nmap 7.93 ( https://nmap.org ) at 2023-01-29 15:06 Hora oficial do Brasil
Nmap scan report for 192.168.15.24
Host is up (0.0011s latency).
Not shown: 997 closed tcp ports (reset)
PORT      STATE SERVICE
80/tcp    open  http
554/tcp   open  rtsp
5800/tcp  open  vnc-http
MAC Address: C8:22:02:2C:CD:F8 (Unknown)
```

Veja que ele me trouxe as portas abertas os serviços e o endereço MAC.

## #nmap -n 192.168.1.0/24

**-n:** Para nunca fazer uma resolução DNS reversa nos endereços IP ativos que ele encontrar. Uma vez que o DNS é normalmente lento, isso acelera as coisas.

## #nmap -R 192.168.1.1

**-R:** Sempre fazer uma resolução DNS reversa nos endereços IP-alvos.

## #nmap --traceroute 192.168.1.1

**--traceroute:** Quantidade de saltos até o host alvo.



# PORT SCANNING TECHNIQUES

## #nmap -F 192.168.1.0/24

**-F (Fast Mode):** Realiza a verificação rápida apenas nas portas comuns de serviços. Significa que ele não verificará todas as portas disponíveis.

Cmd. Prompt de Comando

```
C:\Users\ferna>nmap -F 192.168.15.0/24
Starting Nmap 7.93 ( https://nmap.org ) at 2023-01-29 15:49 Hora oficial do Brasil
Nmap scan report for 192.168.15.24
Host is up (0.0011s latency).
Not shown: 97 closed tcp ports (reset)
PORT      STATE SERVICE
80/tcp    open  http
554/tcp   open  rtsp
5800/tcp  open  vnc-http
MAC Address: C8:22:02:2C:CD:F8 (Unknown)

Nmap scan report for 192.168.15.53
Host is up (0.047s latency).
All 100 scanned ports on 192.168.15.53 are in ignored states.
Not shown: 100 closed tcp ports (reset)
MAC Address: 02:E0:20:00:9B:81 (Unknown)

Nmap scan report for 192.168.15.56
Host is up (0.0048s latency).
All 100 scanned ports on 192.168.15.56 are in ignored states.
Not shown: 100 closed tcp ports (reset)
MAC Address: EE:0F:95:E4:B8:C4 (Unknown)
```

É útil para verificar rapidamente se há alguma porta aberta

## #nmap -sS 192.168.1.0/24

**-sS:** (TCP SYN Scan): O scan SYN é uma opção de scan padrão e mais popular. Pode ser executado rapidamente, escaneando milhares de portas por segundo em uma rede rápida, não bloqueada por firewalls intrusivos. O scan SYN é relativamente não obstrutivo e camuflado, uma vez que ele nunca completa uma conexão TCP.

```
C:\Users\ferna>nmap -sS 192.168.15.58
Starting Nmap 7.93 ( https://nmap.org ) at 2023-01-29 15:56 Hora oficial do Brasil
Nmap scan report for fernando-mkt (192.168.15.58)
Host is up (0.0012s latency).
Not shown: 996 closed tcp ports (reset)
PORT      STATE SERVICE
135/tcp    open  msrpc
139/tcp    open  netbios-ssn
445/tcp    open  microsoft-ds
5357/tcp   open  wsdaapi

Nmap done: 1 IP address (1 host up) scanned in 0.36 seconds
```

Nesse caso escolhe um alvo específico.

## #nmap -sO 192.168.1.1

**-sO (Scans do protocolo IP):** Esta análise permite detectar quais são os protocolos (TCP, ICMP, IGMP etc) que o alvo suporta.

```
C:\Users\ferna>nmap -sO 192.168.15.58
Starting Nmap 7.93 ( https://nmap.org ) at 2023-01-29 19:51 Hora oficial do Brasil
Nmap scan report for fernando-mkt (192.168.15.58)
Host is up (0.0021s latency).
Not shown: 249 closed n/a protocols (proto-unreach)
PROTOCOL STATE      SERVICE
1         open          icmp
2         open|filtered igmp
6         open          tcp
17        open          udp
50        open|filtered esp
51        open|filtered ah
58        open|filtered ipv6-icmp

Nmap done: 1 IP address (1 host up) scanned in 2.52 seconds
```

## #nmap -sU 192.168.1.1

**-sU(UDP):** Scan em portas UDP no alvo. O scan UDP é usado para verificar se um serviço específico está sendo executado em um determinado endereço IP ou faixa de IP.

Ele envia pacotes UDP para cada porta especificada e analisa as respostas. É útil para detectar serviços que usam o protocolo UDP, como o DNS, DHCP, SNMP e outros. Ele também pode ser usado para detectar serviços que estão escondidos ou não documentados.

```
C:\Users\ferna>nmap -sU 192.168.15.58
Starting Nmap 7.93 ( https://nmap.org ) at 2023-01-29 16:21 Hora oficial do Brasil
Nmap scan report for fernando-mkt (192.168.15.58)
Host is up (0.00073s latency).
Not shown: 991 closed udp ports (port-unreach)
PORT      STATE      SERVICE
137/udp    open|filtered netbios-ns
138/udp    open|filtered netbios-dgm
500/udp    open|filtered isakmp
1900/udp   open|filtered upnp
3702/udp   open|filtered ws-discovery
4500/udp   open|filtered nat-t-ike
5050/udp   open|filtered mmcc
5353/udp   open|filtered zeroconf
5355/udp   open|filtered llmnr

Nmap done: 1 IP address (1 host up) scanned in 49.06 seconds
```

O scan UDP funciona enviando um cabeçalho UDP vazio (sem dados) para cada porta

## SERVICE/VERSION DETECTION

**#nmap -sV 192.168.1.1**

**-sV:** É usado para verificar o **serviço e a versão** do serviço em um host remoto. Executa uma varredura de porta TCP para identificar quais portas estão abertas e, em seguida, tenta determinar qual **serviço está sendo executado na porta**.

```

Nmap scan report for fernando-mkt (192.168.15.58)
Host is up (0.0016s latency).
Not shown: 996 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
135/tcp    open  msrpc        Microsoft Windows RPC
139/tcp    open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp    open  microsoft-ds?
5357/tcp   open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows
  
```

```

Nmap scan report for 192.168.15.24
Host is up (0.00099s latency).
Not shown: 997 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
80/tcp    open  http         uc-httpd/1.0.0
554/tcp   open  rtsp
5800/tcp  open  vnc-http?
  
```

## OS DETECTION

**#nmap -O 192.168.1.0/24**

**#nmap -O 192.168.1.10**

**-O (Enable OS detection):** Executa o scan e tenta descobrir qual o sistema operacional do alvo.

```

C:\Users\ferna>nmap -O 192.168.15.58
Starting Nmap 7.93 ( https://nmap.org ) at 2023-01-29 20:02 Hora oficial do Brasil
Nmap scan report for fernando-mkt (192.168.15.58)
Host is up (0.00063s latency).
Not shown: 996 closed tcp ports (reset)
PORT      STATE SERVICE
135/tcp    open  msrpc
139/tcp    open  netbios-ssn
445/tcp    open  microsoft-ds
5357/tcp   open  wsddapi
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
  
```

## SCRIPT SCAN (NSE)

Nmap Scripting Engine (NSE) é um dos recursos mais poderosos e flexíveis do Nmap. Ele permite que os usuários escrevam (e compartilhem) scripts simples (usando a linguagem de programação Lua ) para **automatizar uma ampla variedade de tarefas de rede**.

Os usuários podem contar com o crescente e diversificado conjunto de scripts distribuídos com o Nmap ou escrever seus próprios para atender às necessidades personalizadas.

Na pasta de instalação do Nmap você encontra os scripts, eles são classificados por categorias. O NSE pode até ser usado para exploração de vulnerabilidades.

### #nmap -sC 192.168.1.1

-sC: Executar um scan de portas usando o script padrão do Nmap.

```
Nmap scan report for fernando-mkt (192.168.15.58)
Host is up (0.0017s latency).
Not shown: 996 closed tcp ports (reset)
PORT      STATE SERVICE
135/tcp    open  msrpc
139/tcp    open  netbios-ssn
445/tcp    open  microsoft-ds
5357/tcp   open  wsapi

Host script results:
| smb2-security-mode:
|   311:
|_    Message signing enabled but not required
| smb2-time:
|   date: 2023-01-29T23:10:49
|_  start_date: N/A
```

Alguns dos scripts nesta categoria são considerados intrusivos e não devem ser executados em uma rede de destino sem permissão.

## CATEGORIAS

- **auth:** Relacionados a mecanismos de autenticação e credenciais de acesso.
- **broadcast:** Fazem descoberta de hosts não listados como alvos através do envio de pacotes broadcast.
- **brute:** Visam descobrir credenciais de acesso através de ataques de dicionário.
- **default:** É a categoria padrão, em que os scripts devem fornecer respostas rápidas, concisas e confiáveis, além de serem pouco intrusivos, de fornecerem informações úteis para a maior parte dos usuários e de não estressarem o alvo a ponto de ser detectado por seus administradores como um ataque.
- **discovery:** Visam descobrir ativamente mais informações sobre o alvo.
- **dos:** Tentam causar indisponibilidade do alvo, ao provocar erros no lado do servidor.
- **exploit:** Exploram uma dada vulnerabilidade conhecida.
- **external:** Fazem consultas legítimas a recursos de terceiros, não listados como alvos.

- **afuzzer:** Enviam pacotes contendo aleatórios ou inesperados pela aplicação servidor visando descobrir bugs e vulnerabilidades.
- **intrusive:** Representam considerável risco de provocar erros no lado do servidor, utilizar uma quantidade significativa de recursos ou estressar o alvo a ponto de ser detectado por seus administradores como um ataque.
- **malware:** Detectam remotamente se o alvo está infectado com um dado malware.
- **safe:** Representam pouco risco e não devem causar erros no lado do servidor, utilizar muitos recursos ou explorar brechas de segurança.
- **version:** Estendem a funcionalidade de detecção de versão do Nmap.
- **vuln:** Verificam se há uma dada vulnerabilidade conhecida no alvo.

**nmap --script whois-domain.nse google.com**

**whois-domain.nse:** Busca o Whois de um site.

**nmap -p80,443 --script http-methods site.com**

**-p:** Especifica as portas

**http-methods:** Busca os métodos de autenticação HTTP em uma página (GET, POST, etc) nas portas **80** e **443**, esse filtro refina a busca.

**nmap --script dns-brute.nse site.com**

**dns-brute.nse:** Esse script busca por subdomínios que podem ser novos alvos.

**nmap --script mysql-enum IP/SITE**

**mysql-enum:** Tenta descobrir usuários do MySQL

**nmap -sV --script http-apache-server-status IP/SITE**

**http-apache-server-status:** Exibe o status do servidor Apache

## Pasta dos scripts windows

> Disco Local (C:) > Arquivos de Programas (x86) > Nmap > scripts				
Nome	Data de modificação		Tipo	Tamanho
acarsd-info.nse	01/09/2022 19:24		Arquivo NSE	4 KB
address-info.nse	01/09/2022 19:24		Arquivo NSE	9 KB
...	...		...	...

## Scripts no Linux

Digite o comando abaixo

locate \*.nse



## TIMING AND PERFORMANCE

### #nmap -T5 192.168.1.1

Alterando a velocidade, muito rápido vai interferir no scan, algumas informações poderão ser deixadas de lado.

- T1: Ajuste de timing lento
- T2: Ajuste de timing padrão.
- T3: Ajuste de timing rápido
- T4: Ajuste de timing muito rápido.
- T5: Ajuste de timing extremamente rápido.

## FIREWALL/IDS EVASION AND SPOOFING

Técnicas usadas por hackers para burlar sistemas de segurança. Estas técnicas permitem aos hackers acessar redes e computadores protegidos por firewalls e sistemas de detecção de intrusão (IDS).

**Firewall/IDS Evasion** é o processo de contornar as regras de segurança de um firewall ou IDS. Os hackers podem usar várias técnicas para contornar os firewalls e IDS, incluindo o uso de protocolos de rede não suportados, o uso de portas não padrão, o uso de criptografia para ocultar o tráfego e o uso de pacotes maliciosos para enganar os sistemas de segurança.

**Spoofing** é outra técnica usada por hackers para burlar sistemas de segurança. Esta técnica envolve o uso de informações falsas para enganar os sistemas de segurança. Por exemplo, um hacker pode usar um endereço IP falso para se conectar a uma rede protegida.

## #nmap -f 4047

**-f:** Fragmenta o pacote, então vários pequenos pacotes são enviados assim fica mais difícil para os filtros de pacotes identificar o scan e barra-lo.

## nmap -e enp0s -Pn -S 192.168.1.25 192.168.1.1

**-e enp0s:** Interface de rede de saída

**-S:** Para realizar o Spoof

**192.168.1.25:** IP origem (falsificado)

**192.168.1.1:** IP alvo

É usado para enviar pacotes de rede com um endereço IP falso. Isso é útil para testar a segurança de um sistema, pois permite que o usuário simule um ataque de spoofing.

## nmap --spoof-mac 00:00:00:00:00:00 192.168.1.1

**--spoof-mac:** Falsifica em endereço MAC da sua "escolha" pode usar sites que geram endereços MAC

## nmap -D 192.168.1.15, 192.168.1.28, 192.168.1.154 192.168.1.1

**-D:** Envia endereços de ips falsos, é como se fosse iscas para dificultar o seus que está por ali.

## # nmap --source-port 53 192.168.1.1

**--source-port:** Especifica manualmente o número da porta de origem de um scan. Por padrão, o Nmap irá escolher aleatoriamente uma porta de origem de saída.

## #nmap --data-length 30 192.168.1.1

--data-length: Acrescenta dados aleatórios nos pacotes enviados, por exemplo 30 bytes em cada pacote.

## OUTPUT

### #nmap -v 192.168.1.1

-v ou -vv: Ativa o modo verbose (Modo detalhado) mostra na tela os detalhes que estão acontecendo enquanto o comando roda, dois v significa que aumenta o "nível de detalhes".

### #nmap -d 192.168.1.1

-d ou -dd: Modo debugging (Muito mais detalhes), essa opção é mais utilizadas por desenvolvedores.

### #nmap 192.168.1.1 > arquivo.txt

> arquivo.txt: Salvando as informações em um arquivo.txt

### #nmap --packet-trace 192.168.1.1

--packet-trace: Exibe na tela os bastidores, todo um resumo de cada pacote enviado ou recebido.

### #nmap --iflist 192.168.1.1

--iflist: Exibe IP, interface e gateway local

## MISCELLANEOUS OPTIONS

-6: Força o uso do protocolo IPv6.

-A: Ativa o modo agressivo (Ativa todas opções de scan)

## RESUMO

Você viu os principais comandos do nmap e como ele funciona, dezenas de comandos foram listados e explicado, espero que você tenha entendido a importância e o perigo de fazer varreduras em redes de computadores, **faça testes somente em redes que você tenha autorização, caso ao contrário é por sua conta e risco.**

# SCAN

## ALVOS

### TARGET SPECIFICATION

ALVO ESPECÍFICO OU EM LISTAS

### HOST DISCOVERY

DESCOBERTA DE HOSTS NA REDE

## + INVASIVO

### PORT SCANNING

PORTAS ABERTAS/FECHADAS

### SERVICE/VERSION

SERVIÇOS SUAS VERSÕES

### OS DETECTION

SISTEMA OPERACIONAL

### SCRIPT SCAN

EXECUÇÃO DE SCRIPTS

### FIREWALL/IDS

BURLAR O FIREWALL E IPS

## OPÇÕES

### TIMING AND PERFORMANCE

VELOCIDADE

### OUTPUT

MODOS DE SAÍDA

### MISC

OPÇÕES GERAIS

## + EXEMPLOS

### EXTRA

**nmap -p80 192.168.1.1**

Scan padrão na porta 80

**nmap -v 192.168.1.1 192.168.1.2**

Scan em modo verbose(-v) mais de um host

**nmap -v 192.168.1.1-50**

Scan em intervalo de hosts do 1 ao 50

**nmap -v -A 192.168.1.1**

Detecção do sistema operacional

**nmap -sA 192.168.1.2**

Descobrimos se o alvo tem algum firewall

**nmap --open 192.168.1.1**

Exibir apenas portas abertas

**nmap -p T:80 192.168.1.1**

Scan TCP na porta 80

**nmap -p U:53 192.168.1.1**

Scan UDP na porta 53

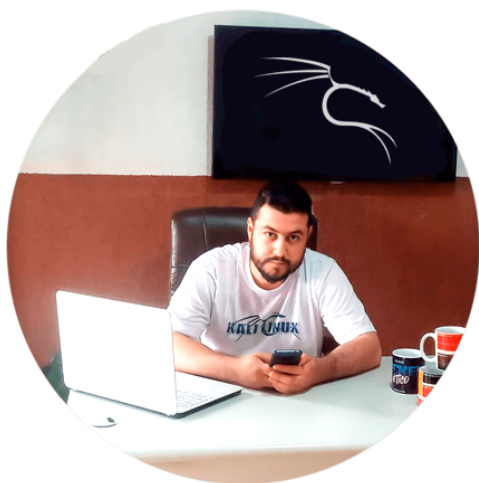
## CONSIDERAÇÕES FINAIS

### OBRIGADO !

Espero que esse material tenha te ajudado a entender como funciona varreduras em redes de computadores e que você possa utilizar esse conhecimento a seu favor, como por exemplo melhorar a segurança em redes que você administra ou venha administrar no futuro.

Obrigado novamente por adquirir esse material e confiar no meu trabalho, **se possível me envie um feedback** do que você achou desse material, pode ser no instagram @linux ou em meu whatsapp 11 974128091.

Até mais ;)



**GANHE DE R\$: 8.000 A R\$: 100.000 POR MÊS ATRAVÉS  
DAS TECNOLOGIAS E PROJETOS PRÁTICOS QUE LHE  
SERÃO ENSINADOS !**



**QUERO APRENDER**