

# Objetivo

Criar um relatório técnico explicativo do uso da ferramenta (sugestões: nmap/zenmap) para coleta de informações da rede (faixa de ips, máscaras de redes, serviços e portas abertas). Neste documento deve conter: um passo a passo sobre como foi o levantamento dos dados da rede, com prints de telas. Descrição dos protocolos de redes responsáveis pelos serviços disponíveis nos servidores.

## 1. Introdução

Nmap (Network Mapper) é um software livre muito utilizado para avaliar a segurança de rede de computadores, onde o mesmo detecta computadores e serviços em uma rede, criando um “mapa” desta rede. O Nmap é um programa que é executado na linha de comando, porém dispõe de uma interface gráfica.

## 2. História

O foi originalmente desenvolvido por Gordon Lyon, conhecido por “hacker Fyodor”. Publicado em setembro de 1997 em um artigo na revista Phrack, com o código fonte incluso. Devido à ajuda da comunidade de segurança de computadores, o desenvolvimento continuou, onde o Nmap teve seu código reescrito de C para C++, dando novos recursos ao Nmap. O NmapFE (Front End) foi substituído pelo Zenmap em 11 de outubro de 2007 por ser uma versão portátil e disponibilizar uma melhor interface na execução visualização e análise dos resultados do Nmap.

## 3. Recursos

Alguns dos recursos incluídos no Nmap:

- Descoberta de hosts – identificação de hosts na rede. Ex: recebendo respostas de Ping ou de uma porta aberta.
- Scanner de portas – Mostrando as portas TCP e UDP abertas.
- Detectar versão – Interrogando serviços na rede para determinar a aplicação e o número da versão.
- Detectar sistema operacional – Remotamente determina o sistema operacional e as características de hardware do host.
- Interação com scripts com o alvo – Usando o Nmap Scripting Engine e Lua.

Além destes recursos, o Nmap pode fornecer informações furtivas do alvo, incluindo DNS reverso, tipos de dispositivos, e endereços MAC.

## 4. Usos éticos e legalidade

O Nmap é uma ferramenta que pode ser usada para identificar serviços disponíveis em sistemas conectados à internet, e que pode também ser usada para Black Hat Hacking, que é um pré-requisito para acesso não autorizado em sistemas em geral. Porém o Nmap é mais usado por administradores de sistema para identificar falhas de segurança.

## 5. Prática

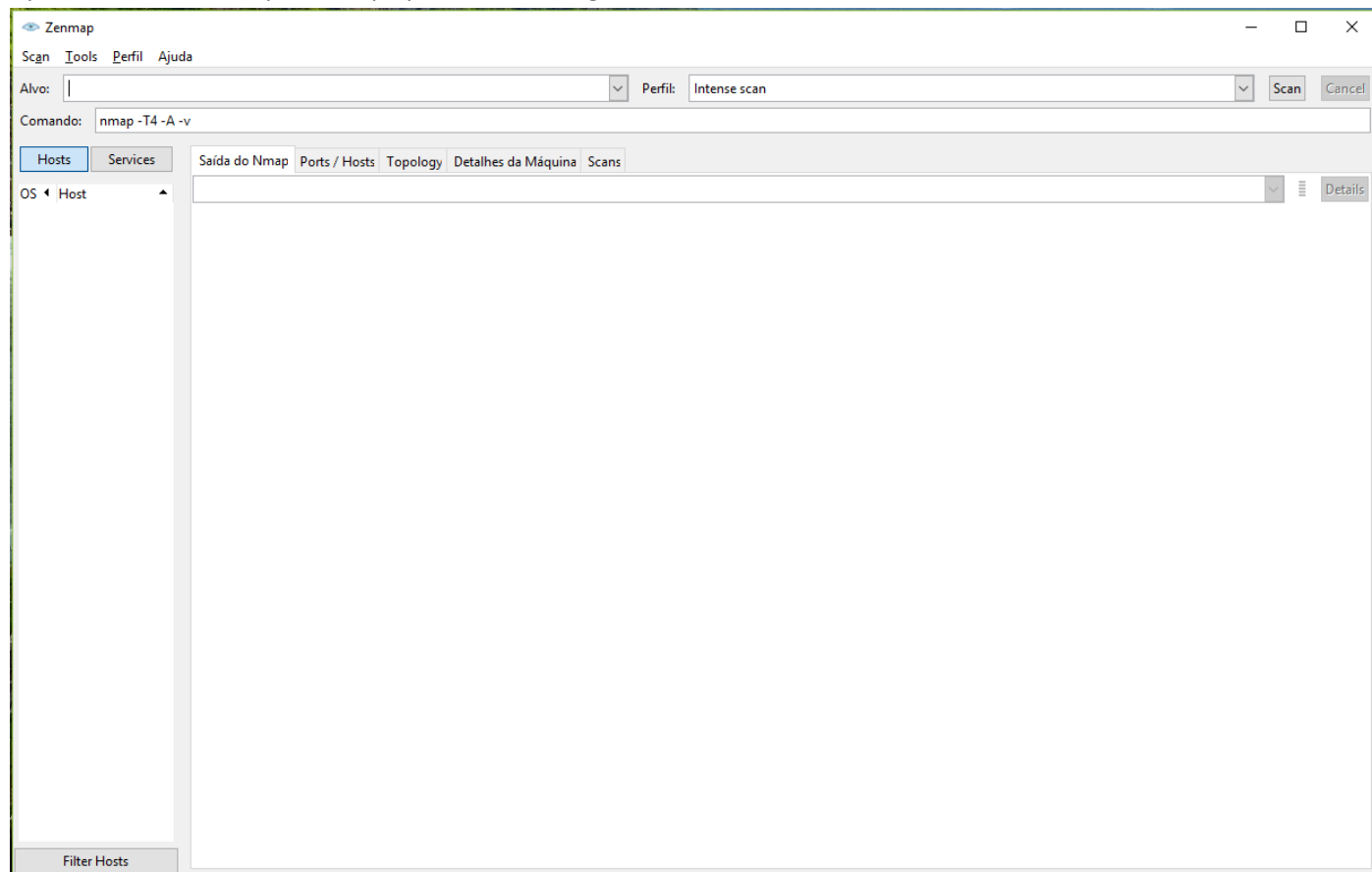
Com o objetivo de demonstrar na prática o uso da ferramenta Nmap/Zenmap, que será utilizada para a coleta de informações de redes (faixa de ips, máscaras de redes, serviços e portas abertas), iremos apresentar um relatório detalhado do uso desta ferramenta.

O download do Nmap pode ser feito em: <https://nmap.org/download.html>

Onde as versões para: Windows, Linux, Mac OS X entre outros sistemas operacionais e também é disponibilizado seu código fonte.

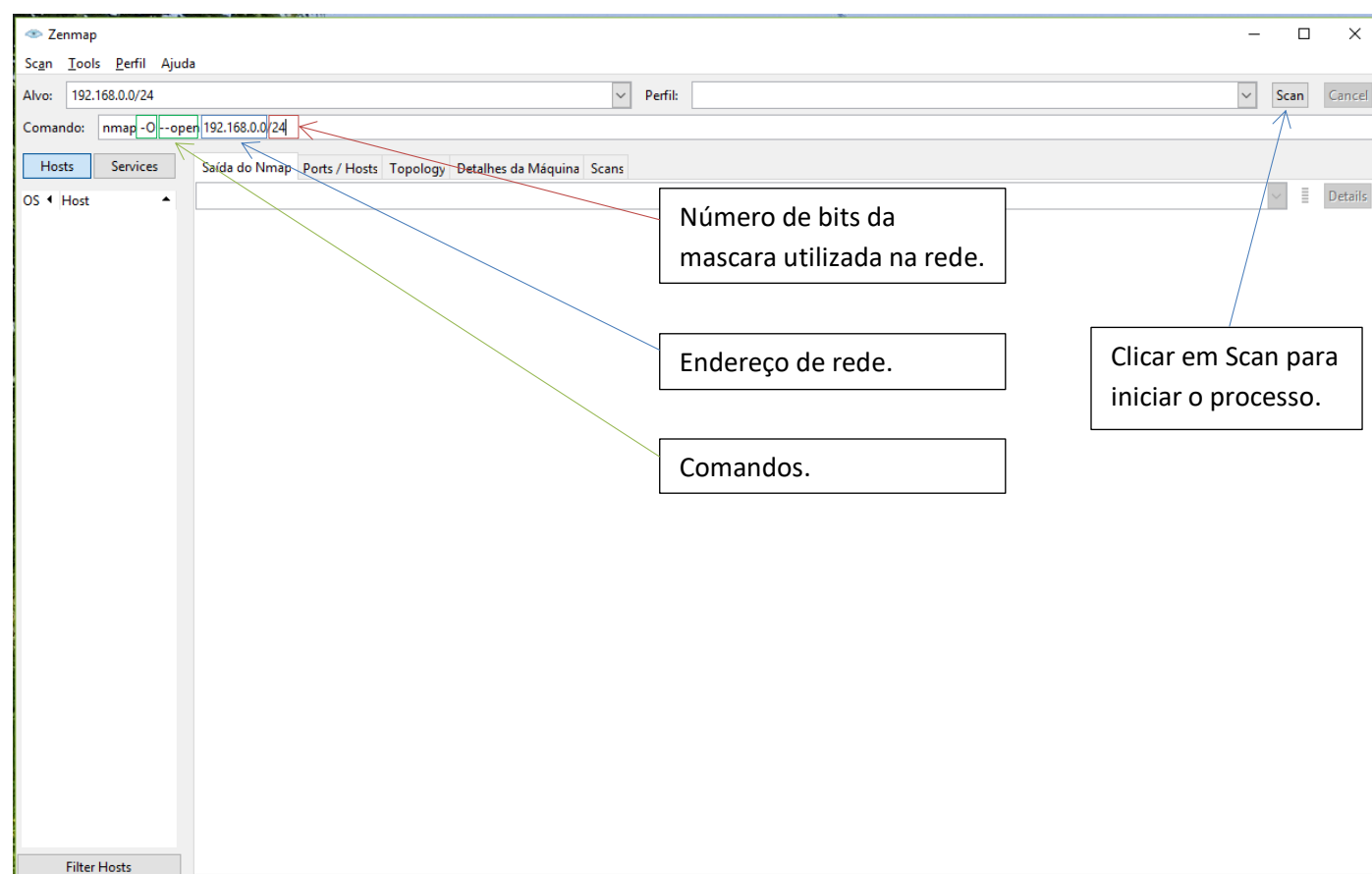
Utilizaremos a versão Windows na demonstração.

Após instalado o Nmap/Zenmap apresentará a seguinte tela:

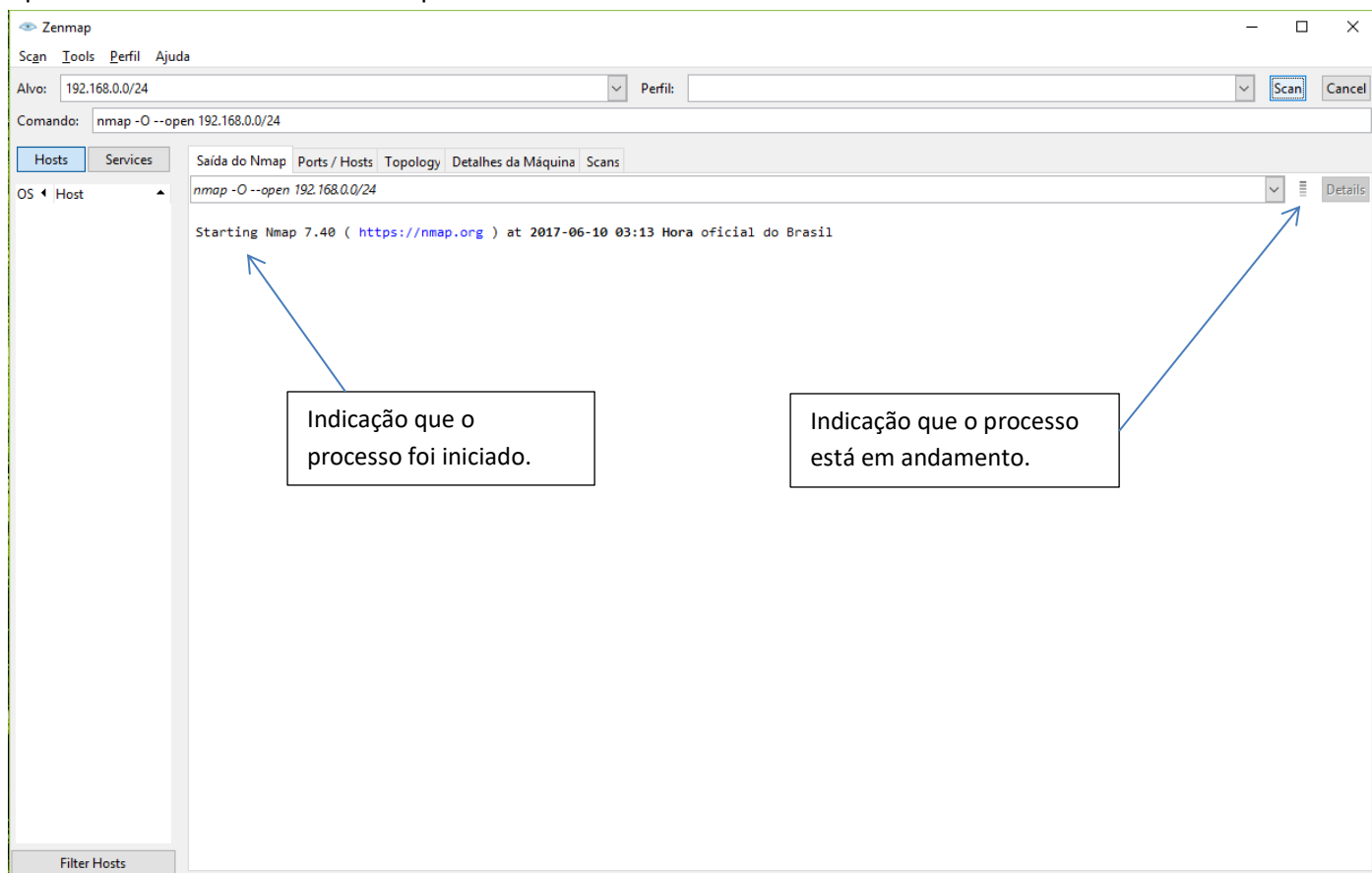


Antes de iniciar o processo de escaneamento das portas e serviços alguns dados ao programa que são:

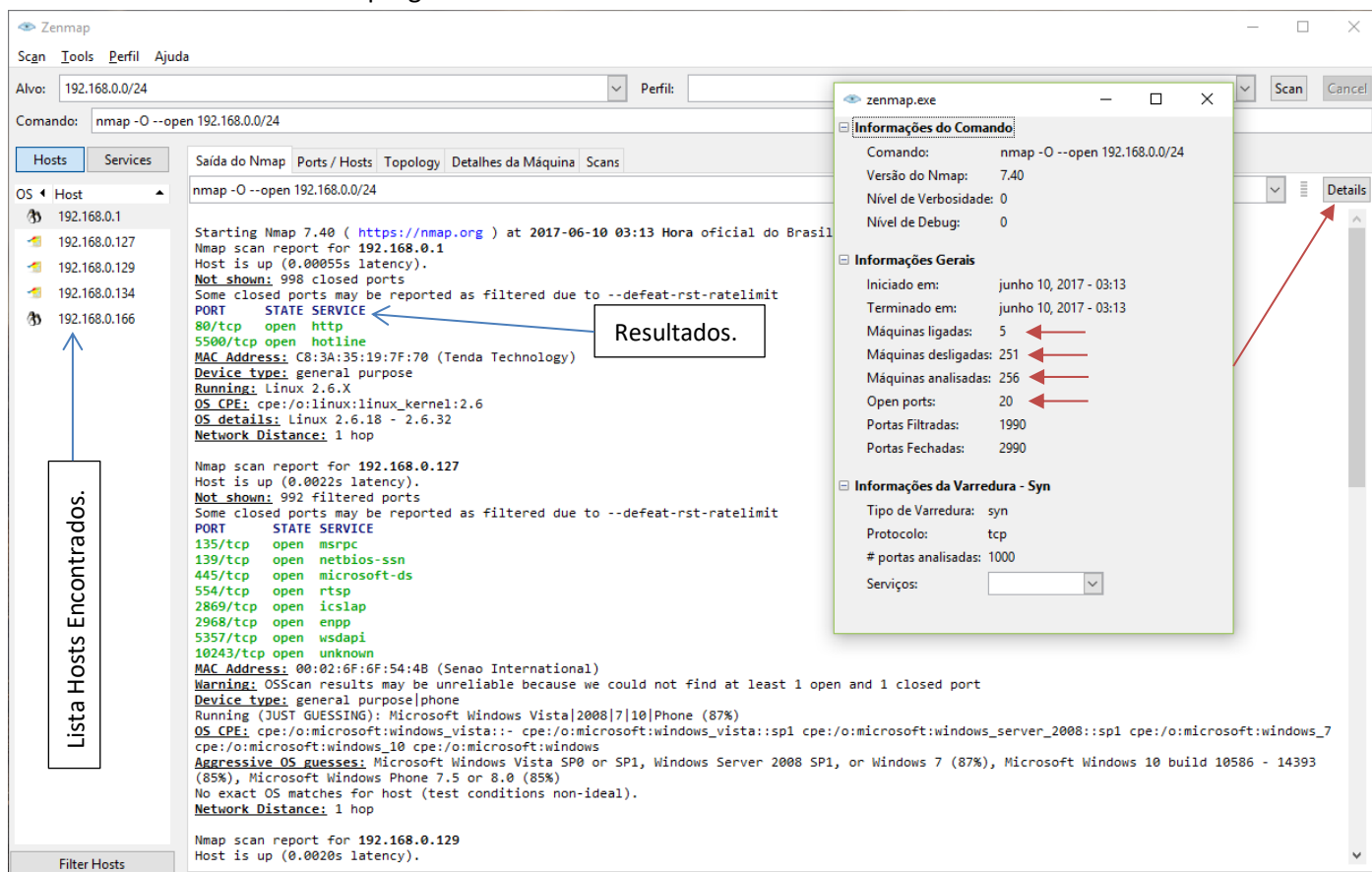
1. Comando
2. Endereço de rede.
3. Número de bits da mascara utilizada na rede a ser escaneada.



Após clicar em Scan será iniciado o processo de escaneamento.



Após finalizar o escaneamento o programa retornará os resultados de acordo com os comandos utilizados.



O Zenmap possui uma série de comandos que pode ser usado de acordo com a necessidade, os comandos também podem ser combinados obtendo-se resultados simultâneos. Abaixo alguns comandos e exemplo de combinação.

**-O:** habilita a detecção do sistema operacional.

**-A:** Permite detecção de sistema operacional e detecção de versão

**--open:** Mostrar apenas portas abertas (ou possivelmente abertas).

**-O --open:** habilita a detecção do sistema operacional e mostra apenas portas abertas(ou possivelmente abertas).

Há uma lista de comandos completa no site oficial: [https://nmap.org/man/pt\\_BR/man-briefoptions.html](https://nmap.org/man/pt_BR/man-briefoptions.html)

Existem **65.536** portas TCP, numeradas de **0** a **65535**. Cada porta pode ser usada por um programa ou serviço diferente, de forma que em teoria poderíamos ter até 65536 serviços diferentes ativos simultaneamente em um mesmo servidor, com um único endereço IP válido, o Zenmap pode escanar todas as portas, porem este processo seria muito demorado, por padrão Zenmap verifica 1000 portas por host, mas dependendo o tamanho da sua rede se possuir muitos hosts disponíveis faram que o processo ainda assim ficar lento. Por exemplo, em uma rede com o prefixo /21 temos um total de 65.536 hosts disponíveis multiplicado pelo número de portas verificadas pelo Zenmap seriam verificadas 65.536.000 verificações.

Para contornar este problema será necessário fazer o escaneamento por sub-redes com menor quantidade de hosts. No nosso exemplo de verificação iremos utilizar faixas com menores quantidades de hosts.

**Exemplo 1:** Rede Wi-Fi da faculdade SENAC Goiás.

**Endereço de Rede:** 192.168.40.0

**Endereço de Broadcast:** 192.168.106.255

**Mascara de Rede:** 255.255.248.0 /21

**Total de Hosts:** 2048

**Total de verificações:** 2.048.000

Como o número de hosts é muito grande iremos utilizar uma das 8 Sub-redes disponíveis:

**Endereço de Rede:** 192.168.40.0 /24

**Endereço de Broadcast:** 192.168.106.255


**Mascara de Rede:** 255.255.255.0 /24

**Total de Hosts:** 255

**Total de verificações:** 255.000

**Comando utilizado:** nmap --open

Impressões de tela usando as configurações acima descritas:

 Zenmap

ScanToolsPerfilAjuda

Alvo:192.168.40.0/24

Comando:nmap --open 192.168.40.0/24

HostsServices

OS ▾ Host ▾

192.168.41.52

192.168.41.129

192.168.41.134

192.168.41.162

192.168.41.180

192.168.41.186

192.168.41.212

192.168.40.162

192.168.40.230

192.168.40.232

192.168.40.136

192.168.40.144

192.168.40.172

192.168.40.195

192.168.40.206

Saída do NmapPorts / HostsTopologyDetalhes da MáquinaScans

nmap --open 192.168.40.0/24

Nmap scan report for 192.168.40.172

Host is up (0.0059s latency).

Not shown: 994 filtered ports

Some closed ports may be reported as filtered due to --defeat-rst-ratelimit

PORTSTATESERVICE

80/tcpopenhttp

135/tcpopenmsrpc

139/tcpopennetbios-ssn

443/tcpopenhttps

445/tcpopenmicrosoft-ds

7070/tcpopenrealserver

MAC Address: 20:16:D8:44:76:A2 (Liteon Technology)

Nmap scan report for 192.168.40.195

Host is up (0.0066s latency).

Not shown: 999 filtered ports

Some closed ports may be reported as filtered due to --defeat-rst-ratelimit

PORTSTATESERVICE

22/tcpopenssh

MAC Address: A4:17:31:FE:99:FF (Hon Hai Precision Ind.)

Nmap scan report for 192.168.40.206

Host is up (0.085s latency).

Not shown: 994 filtered ports

Some closed ports may be reported as filtered due to --defeat-rst-ratelimit

PORTSTATESERVICE

80/tcpopenhttp

135/tcpopenmsrpc

139/tcpopennetbios-ssn

443/tcpopenhttps

445/tcpopenmicrosoft-ds

8888/tcpopensun-answerbook

MAC Address: A0:A8:CD:ED:DD:DE (Intel Corporate)

Nmap scan report for 192.168.40.230

Host is up (0.015s latency).

Not shown: 997 filtered ports

Some closed ports may be reported as filtered due to --defeat-rst-ratelimit

PORTSTATESERVICE

135/tcpopenmsrpc

139/tcpopennetbios-ssn

445/tcpopenmicrosoft-ds

MAC Address: 50:B7:C3:C9:BD:0E (Samsung Electronics)

Nmap scan report for 192.168.40.232

Host is up (0.033s latency).

Not shown: 993 filtered ports

Some closed ports may be reported as filtered due to --defeat-rst-ratelimit

PORTSTATESERVICE

135/tcpopenmsrpc

139/tcpopennetbios-ssn

445/tcpopenmicrosoft-ds

1801/tcpopenmsmq

2103/tcpopenzephyr-clt

2105/tcpopeneklogin

2107/tcpopenmsmq-mgmt

MAC Address: 20:7C:8F:4B:F8:5F (Quanta Microsystems)

Nmap done: 256 IP addresses (40 hosts up) scanned in 908.03 seconds

Filter Hosts

Alvo: 192.168.40.0/24

Comando: nmap --open 192.168.40.0/24

Hosts

Services

Saída do Nmap

Ports / Hosts

Topology

Detalhes da Máquina

Scans

OS ▾ Host

192.168.41.52

192.168.41.129

192.168.41.134

192.168.41.162

192.168.41.180

192.168.41.186

192.168.41.212

192.168.40.162

192.168.40.230

192.168.40.232

192.168.40.136

192.168.40.144

192.168.40.172

192.168.40.195

192.168.40.206

nmap --open 192.168.40.0/24

Starting Nmap 7.40 ( <https://nmap.org> ) at 2017-06-07 19:55 Hora oficial do Brasil  
Nmap scan report for 192.168.40.136

RTTVAR has grown to over 2.3 seconds, decreasing to 2.0

RTTVAR has grown to over 2.3 seconds, decreasing to 2.0

RTTVAR has grown to over 2.3 seconds, decreasing to 2.0

RTTVAR has grown to over 2.3 seconds, decreasing to 2.0

Host is up (0.035s latency).

Not shown: 999 closed ports

Some closed ports may be reported as filtered due to --defeat-rst-ratelimit

PORT STATE SERVICE

631/tcp open ipp

MAC Address: E0:F8:47:38:D9:34 (Apple)

Nmap scan report for 192.168.40.144

Host is up (0.16s latency).

Not shown: 998 filtered ports

Some closed ports may be reported as filtered due to --defeat-rst-ratelimit

PORT STATE SERVICE

135/tcp open msrpc

139/tcp open netbios-ssn

MAC Address: 74:29:AF:A5:CB:F3 (Hon Hai Precision Ind.)

Nmap scan report for 192.168.40.162

Host is up (0.079s latency).

Not shown: 988 closed ports, 2 filtered ports

Some closed ports may be reported as filtered due to --defeat-rst-ratelimit

PORT STATE SERVICE

80/tcp open http

135/tcp open msrpc

139/tcp open netbios-ssn

443/tcp open https

445/tcp open microsoft-ds

2968/tcp open enpp

49152/tcp open unknown

49153/tcp open unknown

49154/tcp open unknown

49155/tcp open unknown

MAC Address: F8:16:54:FE:04:1B (Intel Corporate)

Nmap scan report for 192.168.40.172

Host is up (0.0059s latency).

Not shown: 994 filtered ports

Some closed ports may be reported as filtered due to --defeat-rst-ratelimit

PORT STATE SERVICE

80/tcp open http

135/tcp open msrpc

139/tcp open netbios-ssn

443/tcp open https

445/tcp open microsoft-ds

7070/tcp open realserver

MAC Address: 20:16:D8:44:76:A2 (Liteon Technology)

Nmap scan report for 192.168.40.195

Host is up (0.0066s latency).

Not shown: 999 filtered ports

Some closed ports may be reported as filtered due to --defeat-rst-ratelimit

PORT STATE SERVICE

22/tcp open ssh

MAC Address: A4:17:31:FE:99:FF (Hon Hai Precision Ind.)

Filter Hosts

A tabela abaixo demonstra descrição de portas e serviços escaneados pela ferramenta Zenmap.

PORTAS	PROTOCOLO / DESCRIÇÃO		SERVIÇO	DESCRIÇÃO
80	TCP	O TCP (Transmission Control Protocol - Protocolo de Controle de Transmissão) é um dos principais protocolos da camada de transporte do modelo TCP/IP	http	(HyperText Transfer Protocol)(Procolo de transferência de HiperTexto) - usada para transferir páginas WWW.
135	TCP		msrpc	Microsoft RPC ( Microsoft Remote Procedure Call ) é uma versão modificada do DCE / RPC . As adições incluem suporte parcial para cadeias UCS-2 (mas não Unicode ), identificadores implícitos e cálculos complexos nos paradigmas de cadeias e estrutura de comprimento variável já presentes no DCE / RPC.
139	TCP		netbios-ssn	NetBIOS Session Service (Serviço de sessão NetBios).
443	TCP		https	Protocol over TLS/SSL (transmissão segura)(Camada de transporte seguro).
445	TCP		microsoft-ds	Microsoft-DS SMB (Bloco de mensagem de servidor) file sharing.
7070	TCP		realserver	Serviço de Streaming de áudio e vídeo RealPlayer/QuickTime.
22	TCP		ssh	(Secure Shell - Shell seguro) - Usada para logins seguros, transferência de arquivos e redirecionamento de porta.
8888	TCP		Sun-Answerbook	Servidor Dwhttpd (definido como obsoleto por docs.sun.com).
1801	TCP		msmq	Microsoft Message Queuing ou o MSMQ é uma implementação de fila de mensagens desenvolvida pela Microsoft.
2103	TCP		Zephyr-Clt	Criado no MIT , como parte do Projeto Athena , o Zephyr foi projetado como um protocolo de mensagens instantâneas e uma suite de aplicativos com um fundo Unix pesado.
2105	TCP		eklogin	Eklogin Kerberos login criptografado remoto (rlogin).
2107	TCP		msmq-mgmt	MSMQ-Mgmt - Enfileiramento de mensagens.
631	TCP		ipp	(Internet Printing Protocol) (Protocolo de impressão na internet).
2968	TCP		enpp	Rtvscan (Symantec Antivirus) para servidores Novell NetWare,Trojans que podem usar esta porta: SDBot .
49152	TCP		unknown	Por definição, não pode haver registro de portas no intervalo dinâmico de 49152 à 65535.
49153	TCP		unknown	Por definição, não pode haver registro de portas no intervalo dinâmico de 49152 à 65535.
49154	TCP		unknown	Por definição, não pode haver registro de portas no intervalo dinâmico de 49152 à 65535.
49155	TCP		unknown	Por definição, não pode haver registro de portas no intervalo dinâmico de 49152 à 65535.

## Exemplo 2: Rede Cabeada da faculdade SENAC Goiás.

**Endereço de Rede:** 192.168.106.0

**Endereço de Broadcast:** 192.168.106.255

**Mascara de Rede:** 255.255.255.0 /24

**Total de Hosts:** 255

**Total de verificações:** 255.000

Impressões de tela usando as configurações acima descritas:

The screenshot shows the Zenmap application window. At the top, there are tabs for 'Scan', 'Tools', 'Perfil', and 'Ajuda'. Below these, the 'Alvo:' field is set to '192.168.106.0/24' and the 'Comando:' field contains 'nmap --open 192.168.106.0/24'. The main interface is divided into two panes. The left pane, titled 'Hosts', shows a list of IP addresses from 192.168.106.18 to 192.168.106.225. The right pane, titled 'Saída do Nmap', displays the output of the Nmap scan. The output includes the Nmap version (7.40), the scan time (2017-06-07 19:47), and the scan report for the target network. The report shows that the host is up and lists several open ports and services, including vnc-http, vnc, msrpc, netbios-ssn, microsoft-ds, iss-realsecure, apex-mesh, and unknown. The MAC address for the host is also displayed.

**Hosts List:**

- 192.168.106.18
- 192.168.106.19
- 192.168.106.21
- 192.168.106.24
- 192.168.106.32
- 192.168.106.33
- 192.168.106.40
- 192.168.106.70
- 192.168.106.79
- 192.168.106.81
- 192.168.106.183
- 192.168.106.197
- 192.168.106.225

**Nmap Scan Report:**

```
Starting Nmap 7.40 ( https://nmap.org ) at 2017-06-07 19:47 Hora oficial do Brasil
Nmap scan report for 192.168.106.18
Host is up (0.0016s latency).
Not shown: 998 filtered ports
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT      STATE SERVICE
5800/tcp  open  vnc-http
5900/tcp  open  vnc
MAC Address: 50:E5:49:FA:EF:82 (Giga-byte Technology)

Nmap scan report for 192.168.106.19
Host is up (0.00070s latency).
Not shown: 992 filtered ports
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
902/tcp   open  iss-realsecure
912/tcp   open  apex-mesh
5800/tcp  open  vnc-http
5900/tcp  open  vnc
50001/tcp open  unknown
MAC Address: 50:E5:49:F6:FF:B4 (Giga-byte Technology)

Nmap scan report for 192.168.106.21
Host is up (0.0025s latency).
Not shown: 992 filtered ports
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT      STATE SERVICE
```



Zenmap

ScanToolsPerfilAjuda

Alvo: 192.168.106.0/24Perfil: ScanCancel

Comando: nmap --open 192.168.106.0/24

HostsServices

Saída do NmapPorts / HostsTopologyDetalhes da MáquinaScans

OS Host

192.168.106.18

192.168.106.19

192.168.106.21

192.168.106.24

192.168.106.32

192.168.106.33

192.168.106.40

192.168.106.70

192.168.106.79

192.168.106.81

192.168.106.183

192.168.106.197

192.168.106.225

nmap --open 192.168.106.0/24

5900/tcp open vnc

50001/tcp open unknown

MAC Address: 50:E5:49:F7:10:8B (Giga-byte Technology)

Nmap scan report for 192.168.106.225

Host is up (0.0022s latency).

Not shown: 992 filtered ports

Some closed ports may be reported as filtered due to --defeat-rst-ratelimit

PORT	STATE	SERVICE
135/tcp	open	msrpc
139/tcp	open	netbios-ssn
445/tcp	open	microsoft-ds
902/tcp	open	iss-realsecure
912/tcp	open	apex-mesh
5800/tcp	open	vnc-http
5900/tcp	open	vnc
50001/tcp	open	unknown

MAC Address: 50:E5:49:F8:3A:C0 (Giga-byte Technology)

Nmap scan report for 192.168.106.79

Host is up (0.010s latency).

Not shown: 980 closed ports, 16 filtered ports

Some closed ports may be reported as filtered due to --defeat-rst-ratelimit

PORT	STATE	SERVICE
135/tcp	open	msrpc
139/tcp	open	netbios-ssn
445/tcp	open	microsoft-ds
1688/tcp	open	nsjtp-data

Nmap done: 256 IP addresses (17 hosts up) scanned in 28.26 seconds

Filter Hosts

A tabela abaixo demonstra descrição de portas e serviços escaneados pela ferramenta Zenmap.

PORTAS	PROTOCOLO / DESCRIÇÃO		SERVIÇO	DESCRIÇÃO
5800	TCP	O TCP (Transmission Control Protocol - Protocolo de Controle de Transmissão) é um dos principais protocolos da camada de transporte do modelo TCP/IP	vnc-http	Protocolo remoto de desktop VNC - para uso em HTTP
5900	TCP		vnc	Protocolo remoto VNC de desktop (usado pela ARD)
135	TCP		msrpc	Microsoft RPC ( Microsoft Remote Procedure Call ) é uma versão modificada do DCE / RPC . As adições incluem suporte parcial para cadeias UCS-2 (mas não Unicode ), identificadores implícitos e cálculos complexos nos paradigmas de cadeias e estrutura de comprimento variável já presentes no DCE / RPC.
139	TCP		netbios-ssn	NetBIOS Session Service (Serviço de sessão NetBios).
445	TCP		microsoft-ds	Microsoft-DS SMB (Bloco de mensagem de servidor) file sharing.
902	TCP		iss-realsecure	ISS RealSecure Sensor
912	TCP		apex-mesh	APEX relay-relay service
50001	TCP		unknown	Por definição, não pode haver registro de portas no intervalo dinâmico de 49152 à 65535.
554	TCP		rtsp	RTSP (Real Time Streaming Protocol) (Protocolo de transmissão em tempo real)
2869	TCP		icslap	Microsoft Internet Connection Firewall (ICF), Internet Connection Sharing (ICS), SSDP Discover Service, Microsoft Universal Plug and Play (UPnP), Microsoft Event Notification
5357	TCP		wsdapi	Usado pela Microsoft Network Discovery, deve ser filtrado para redes públicas. Desativar a descoberta de rede para qualquer perfil de rede pública deve fechar a porta, a menos que esteja sendo usado por outro serviço potencialmente mal-intencionado.
10243	TCP		unknown	Windows Media Player Network Sharing Service
22	TCP		ssh	(Secure Shell - Shell seguro) - Usada para logins seguros, transferência de arquivos e redirecionamento de porta.
111	TCP		rpcbind	portmapper, rpcbind
1688	TCP		nsjtp-data	IANA registered for: nsjtp-data NSJTP stands for HP's Network ScanJet Transfer Protocol. Port 1688 TCP is also used for Microsoft's KMS Traffic.

#### Fontes

[https://pt.wikipedia.org/wiki/Lista\\_de\\_portas\\_de\\_protocolos#Portas\\_49152\\_to\\_65535](https://pt.wikipedia.org/wiki/Lista_de_portas_de_protocolos#Portas_49152_to_65535)  
<http://admredesifpe.blogspot.com.br/2010/06/principais-portas-e-protocolos-usadas.html>  
[https://nmap.org/man/pt\\_BR/man-briefoptions.html](https://nmap.org/man/pt_BR/man-briefoptions.html)  
<https://pt.wikipedia.org/wiki/Nmap>  
<https://nmap.org/>  
<https://nmap.org/book/man.html>