

**ASSOCIAÇÃO EDUCACIONAL DE VITÓRIA
FACULDADES INTEGRADAS SÃO PEDRO
CURSO DE GRADUAÇÃO EM REDES DE COMPUTADORES**

MATHEUS HENRIQUE DUTRA RANGEL

TRABALHO – SISTEMAS OPERACIONAIS DE REDES ABERTAS

**VITÓRIA
2022**

MATHEUS HENRIQUE DUTRA RANGEL

TRABALHO – SISTEMAS OPERACIONAIS DE REDES ABERTAS

Trabalho acadêmico do Curso de Graduação em Redes de Computadores, apresentado às Faculdades Integradas São Pedro como parte das exigências da disciplina Sistemas operacionais de redes abertas, sob orientação do(a) professor(a) Jarbas Ferreira.

VITÓRIA

2022

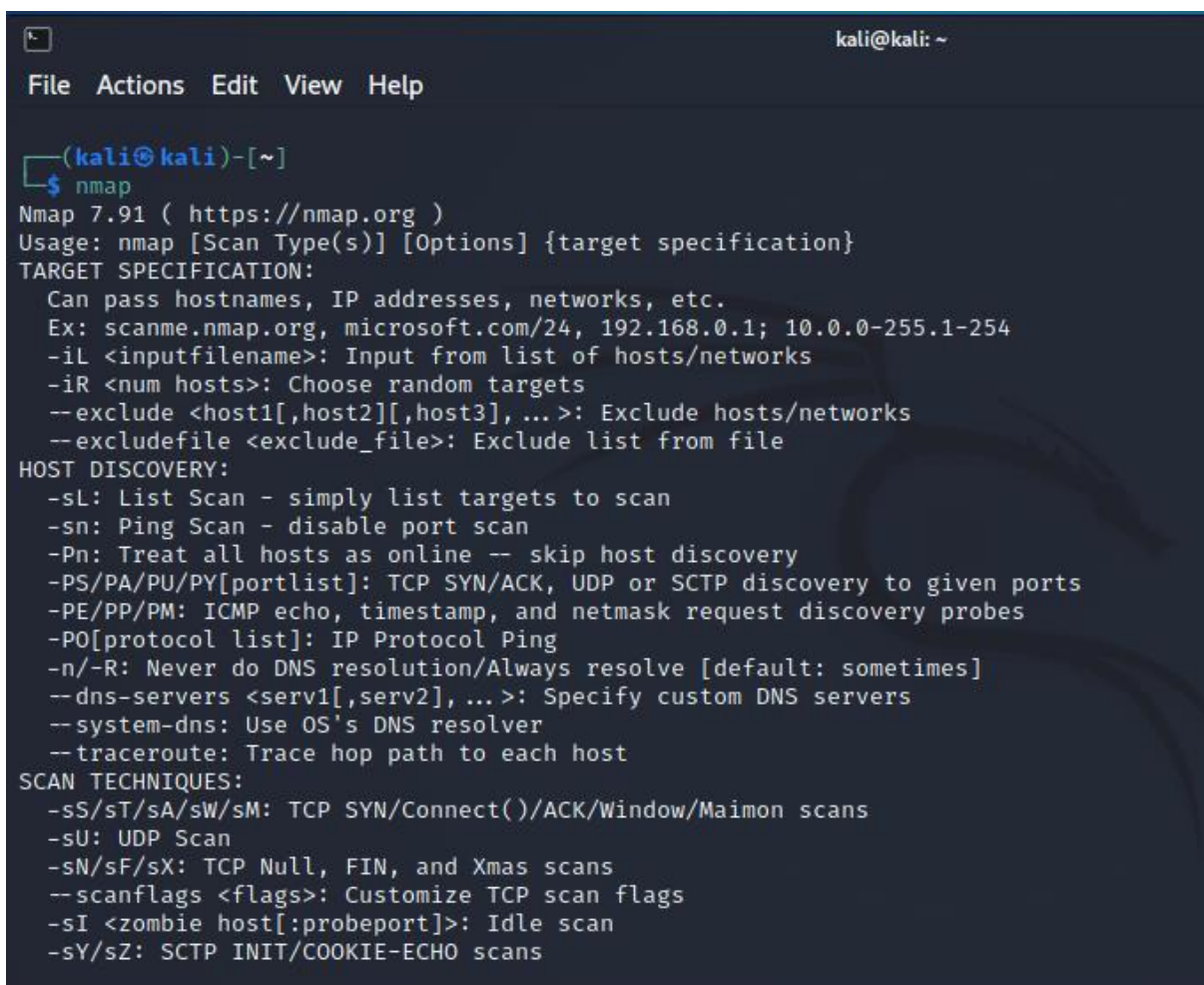
Sumário

1. FERRAMENTAS DE REDES UTILIZADAS NO KALI LINUX	1
2. COMANDOS UTILIZADOS NO LINUX?	4
Bibliografia.....	9

1. FERRAMENTAS DE REDES UTILIZADAS NO KALI LINUX

Nmap

A ferramenta Nmap abreviação de Network Mapper é uma ferramenta open source muito conhecida por fazer o reconhecimento de rede e geralmente utilizada como scanner de portas em testes de penetração em redes tanto por atores de ameaça quanto por pesquisadores, profissionais e analistas da área de segurança e redes.

A screenshot of a terminal window in Kali Linux. The window title is 'kali@kali: ~'. The menu bar shows 'File Actions Edit View Help'. The prompt is '(kali@kali)-[~]'. The command '\$ nmap' has been entered. The output shows the Nmap version (7.91) and a detailed list of usage options categorized into Target Specification, Host Discovery, and Scan Techniques.

```
kali@kali: ~  
File Actions Edit View Help  
  
(kali@kali)-[~]  
$ nmap  
Nmap 7.91 ( https://nmap.org )  
Usage: nmap [Scan Type(s)] [Options] {target specification}  
TARGET SPECIFICATION:  
  Can pass hostnames, IP addresses, networks, etc.  
  Ex: scanme.nmap.org, microsoft.com/24, 192.168.0.1; 10.0.0-255.1-254  
  -iL <inputfilename>: Input from list of hosts/networks  
  -iR <num hosts>: Choose random targets  
  --exclude <host1[,host2][,host3], ...>: Exclude hosts/networks  
  --excludefile <exclude_file>: Exclude list from file  
HOST DISCOVERY:  
  -sL: List Scan - simply list targets to scan  
  -sn: Ping Scan - disable port scan  
  -Pn: Treat all hosts as online -- skip host discovery  
  -PS/PA/PY/PY[portlist]: TCP SYN/ACK, UDP or SCTP discovery to given ports  
  -PE/PP/PM: ICMP echo, timestamp, and netmask request discovery probes  
  -PO[protocol list]: IP Protocol Ping  
  -n/-R: Never do DNS resolution/Always resolve [default: sometimes]  
  --dns-servers <serv1[,serv2], ...>: Specify custom DNS servers  
  --system-dns: Use OS's DNS resolver  
  --traceroute: Trace hop path to each host  
SCAN TECHNIQUES:  
  -sS/sT/sA/sW/sM: TCP SYN/Connect()/ACK/Window/Maimon scans  
  -sU: UDP Scan  
  -sN/sF/sX: TCP Null, FIN, and Xmas scans  
  --scanflags <flags>: Customize TCP scan flags  
  -sI <zombie host[:probeport]>: Idle scan  
  -sY/sZ: SCTP INIT/COOKIE-ECHO scans
```

Tela do terminal após execução do comando Nmap.

O Nmap funciona enviando pacotes brutos com o intuito de determinar quais hosts estão disponíveis na rede, quais serviços, as versões dos sistemas operacionais além do tipo de filtro/firewall que estejam em uso. Outros usos que podem ser feitos com o Nmap são: auditorias de segurança, utilizado por administradores de rede em tarefas de rotina como inventário de rede, gerenciamento do agendamento de atualizações, além de ser possível monitorar a atividade e disponibilidade de hosts e serviços.

A saída do Nmap gera um relatório de portas escaneadas e uma lista suplementar de informações que pode variar conforme as opções disponíveis em seu menu. Neste relatório contém o status das portas escaneadas, sendo eles: Open, filtered, closed ou unfiltered.

Open: Quer dizer que a aplicação na máquina alvo está esperando por conexões e pacotes naquela porta.

Filtered: Significa que um firewall, filtro ou algum tipo de bloqueio na rede está impedindo de se comunicar naquela porta, impossibilitando o Nmap de dizer se a porta está aberta ou fechada.

Closed: Portas fechadas não possuem nenhuma aplicação “escutando” a porta.

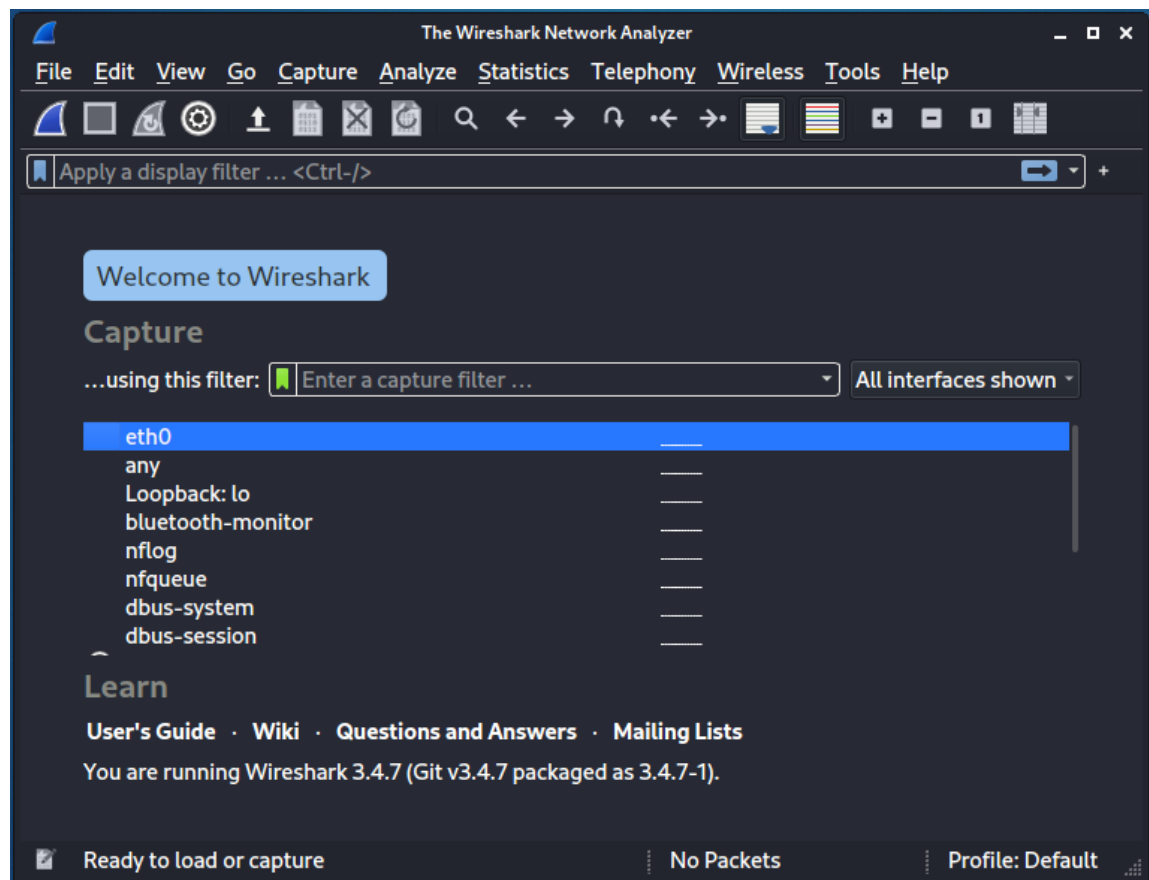
Unfiltered: Quando a porta responde ao Nmap, porém o mesmo não consegue determinar se está aberta ou fechada.

Nmap pode reportar uma combinação de status, sendo eles: open | filtered e closed | filtered quando não consegue determinar quais dos dois status descreve a porta.

Wireshark

A ferramenta de código aberto Wireshark é uma das mais famosas e mais utilizadas no âmbito de análise detalhada de pacotes de rede, ela permite visualizar de forma “microscópica” o que acontece em sua rede, sendo usada por pesquisadores, estudantes e agências do governo.

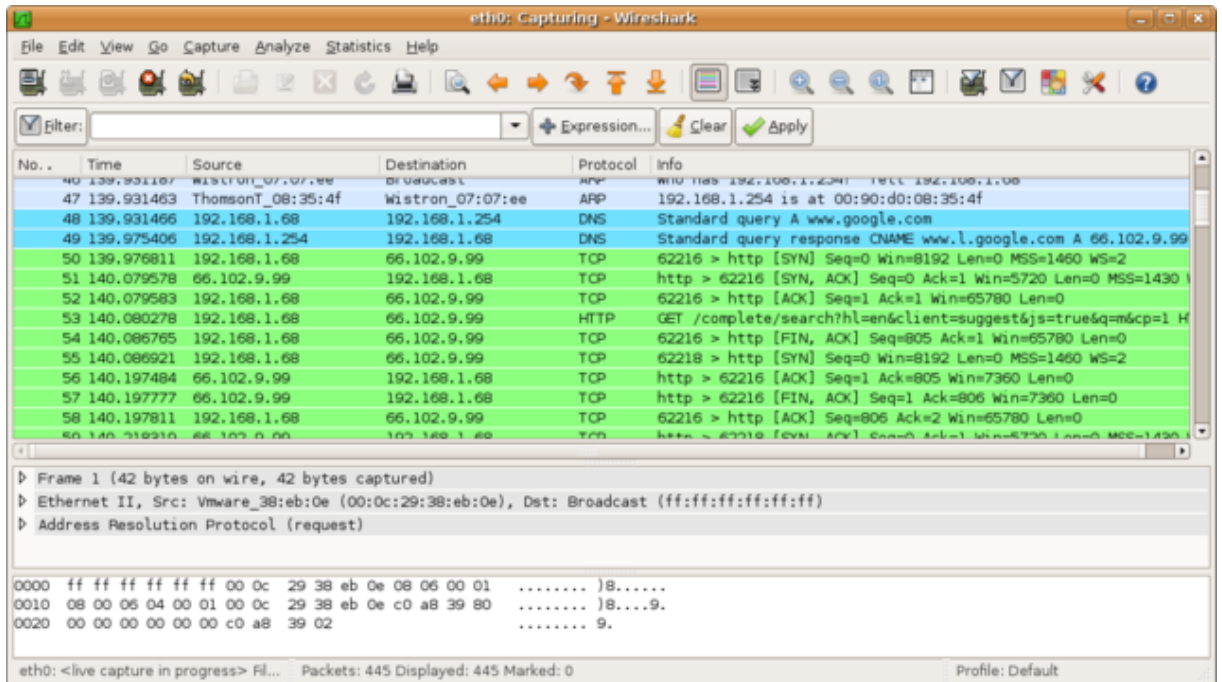
Criada em contribuição voluntária de diversas pessoas ao redor do globo a ferramenta é a continuação de um projeto iniciado por Gerald Combs em 1998.



Tela inicial do Wireshark

Algumas das principais funções do Wireshark são:

- Captura de pacotes em atividade e posterior análise de forma offline.
- Inspeção profunda de centenas de protocolos, sendo adicionados novos a todo instante.
- Saída pode ser exportada para XML, CSV, entre outros.
- Seu filtro pode ser utilizado com regras de cores, para uma análise mais intuitiva.

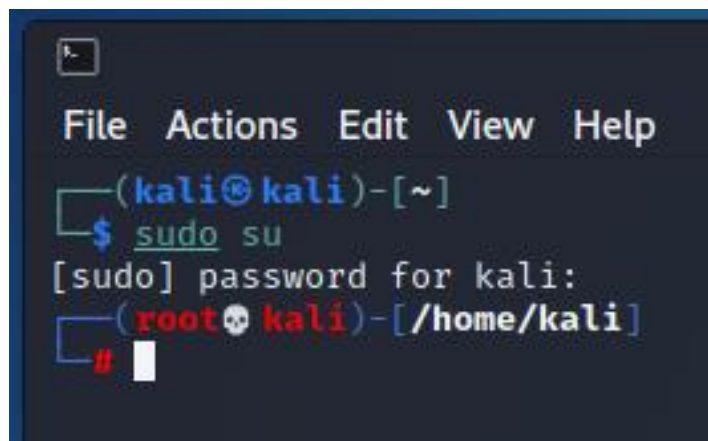


Wireshark analisando uma rede e mostrando os pacotes capturados

2. COMANDOS UTILIZADOS NO LINUX?

\$ sudo su

Este comando tem por função tornar elevar o privilégio de execução do usuário para administrador.



\$ man (alguma interface do sistema)

Tal comando utilizado em combinação com mais um implemento mostra o manual de utilização da aplicação. Exemplo

```

EXAMPLES
man ls
    Display the manual page for the item (program) ls.

man man.7
    Display the manual page for macro package man from section 7. (This is an alternative spelling of "man 7 man".)

man 'man(7)'
    Display the manual page for macro package man from section 7. (This is another alternative spelling of "man 7 man". It may be more convenient when copying and pasting cross-references to manual pages. Note that the parentheses must normally be quoted to protect them from the shell.)

man -a intro
    Display, in succession, all of the available intro manual pages contained within the manual. It is possible to quit between successive displays or skip any of them.

man -t bash | lpr -Pps
    Format the manual page for bash into the default troff or groff format and pipe it to the printer named ps. The default output for groff is usually PostScript. man --help should advise as to which processor is bound to the -t option.

```

\$ clear

Utilizado para limpar a tela do terminal

```

root@kali: /home/kali
File Actions Edit View Help
clear(1)                                General Commands Manual                                clear(1)

NAME
    clear - clear the terminal screen

SYNOPSIS
    clear [-Ttype] [-V] [-x]

DESCRIPTION
    clear clears your screen if this is possible, including its scrollback buffer (if the extended "E3" capability is defined). clear looks in the environment for the terminal type given by the environment variable TERM, and then in the terminfo database to determine how to clear the screen.

    clear writes to the standard output. You can redirect the standard output to a file (which prevents clear from actually clearing the screen), and later cat the file to the screen, clearing it at that point.

OPTIONS
    -T type
        indicates the type of terminal. Normally this option is unnecessary, because the default is taken from the environment variable TERM. If -T is specified, then the shell variables LINES and COLUMNS will also be ignored.

    -V
        reports the version of ncurses which was used in this program, and exits. The options are as follows:

    -x
        do not attempt to clear the terminal's scrollback buffer using the extended "E3" capability.

HISTORY
    A clear command appeared in 2.79BSD dated February 24, 1979. Later that was provided in Unix 8th edition (1985).

log file: $

```


\$ ls

Este comando é utilizado quando precisa ser visualizado o conteúdo em determinado diretório, possuindo diversos complementos, como segue no exemplo abaixo.

```

root@kali: /home/kali
File Actions Edit View Help
LS(1) User Commands LS(1)

NAME
    ls - list directory contents

SYNOPSIS
    ls [OPTION]... [FILE]...

DESCRIPTION
    List information about the FILES (the current directory by default). Sort entries alphabetically if none of -cf-
    tuvsUX nor --sort is specified.

    Mandatory arguments to long options are mandatory for short options too.

    -a, --all
        do not ignore entries starting with .

    -A, --almost-all
        do not list implied . and ..

    --author
        with -l, print the author of each file

    -b, --escape
        print C-style escapes for nongraphic characters

    --block-size=SIZE
        with -l, scale sizes by SIZE when printing them; e.g., '--block-size=M'; see SIZE format below

log file: $

```

\$ chmod

Permite alterar as configurações de permissão de arquivos e diretórios

```

root@kali: /home/kali
File Actions Edit View Help
CHMOD(1) User Commands CHMOD(1)

NAME
    chmod - change file mode bits

SYNOPSIS
    chmod [OPTION]... MODE[,MODE]... FILE...
    chmod [OPTION]... OCTAL-MODE FILE...
    chmod [OPTION]... --reference=RFILE FILE...

DESCRIPTION
    This manual page documents the GNU version of chmod. chmod changes the file mode bits of each given file according to mode, which can be either a symbolic representation of changes to make, or an octal number representing the bit pattern for the new mode bits.

    The format of a symbolic mode is [ugoa...][[-+=][perms...]]..., where perms is either zero or more letters from the set rwXst, or a single letter from the set ugo. Multiple symbolic modes can be given, separated by commas.

    A combination of the letters ugoa controls which users' access to the file will be changed: the user who owns it (u), other users in the file's group (g), other users not in the file's group (o), or all users (a). If none of these are given, the effect is as if (a) were given, but bits that are set in the umask are not affected.

    The operator + causes the selected file mode bits to be added to the existing file mode bits of each file; - causes them to be removed; and = causes them to be added and causes unmentioned bits to be removed except that a directory's unmentioned set user and group ID bits are not affected.

    The letters rwXst select file mode bits for the affected users: read (r), write (w), execute (or search for directories) (x), execute/search only if the file is a directory or already has execute permission for some user (X), set user or group ID on execution (s), restricted deletion flag or sticky bit (t). Instead of one or more of

Manual page chmod(1) line 1/113 30% (press h for help or q to quit)

```

\$ cd

O comando cd permite se movimentar para algum diretório específico como podemos ver no exemplo abaixo.

```
(root@kali)-[/home/kali]
# cd Desktop

(root@kali)-[/home/kali/Desktop]
# ss
```

\$ dir

Quando em um novo diretório e for preciso saber qual o seu conteúdo o comando dir pode ser usado para mostra-lo.

```
root@kali: /home/kali

File Actions Edit View Help

(root@kali)-[/home/kali]
# dir
Desktop
Documents
Downloads
Music
Pictures
Public
S
S\0330B\0330B\0330B\0330B\0330B\0330B\0330B\0330B\0330A\0330A\0330A\0330B\0330B\0330B\0
0A\0330A\0330A\0330A\0330A\0330A\0330A\0330A\0330A\0330A\0330A\0330A\0330A\0330A\0330A\
30A\033\0330B\0330B\0330B\0330B\0330B\0330B\0330B\0330B\0330A\0330A\0330B\0330B
Sq
Templates
Videos
XBruteForcer

(root@kali)-[/home/kali]
#
```


Bibliografia

Computer Hope. (2022, Novembro 15). *Linux chmod command*. Retrieved from Site da Computer hope: <https://www.computerhope.com/unix/uchmod.htm>

Nmap.org. (2022, Novembro 15). *Chapter 15. Nmap Reference Guide*. Retrieved from Site da Nmap.org: <https://nmap.org/book/man.html#man-description>

Wireshark.org. (2022, Novembro 22). *About Wireshark*. Retrieved from Site do wireshark.org: <https://www.wireshark.org/>