**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](#_Toc119421122)

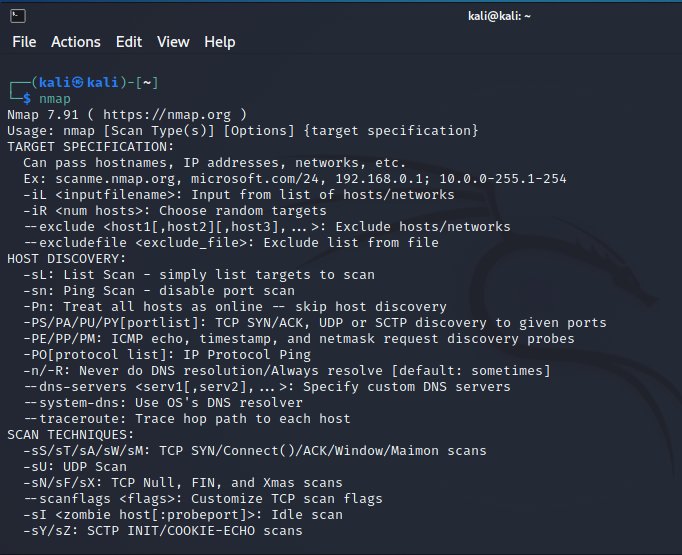
[2. COMANDOS UTILIZADOS NO LINUX? 4](#_Toc119421146)

[Bibliografia 9](#_Toc119421176)

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.



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 postas 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: Postas fechadas não possuem nenhuma aplicação “escutando” a porta.

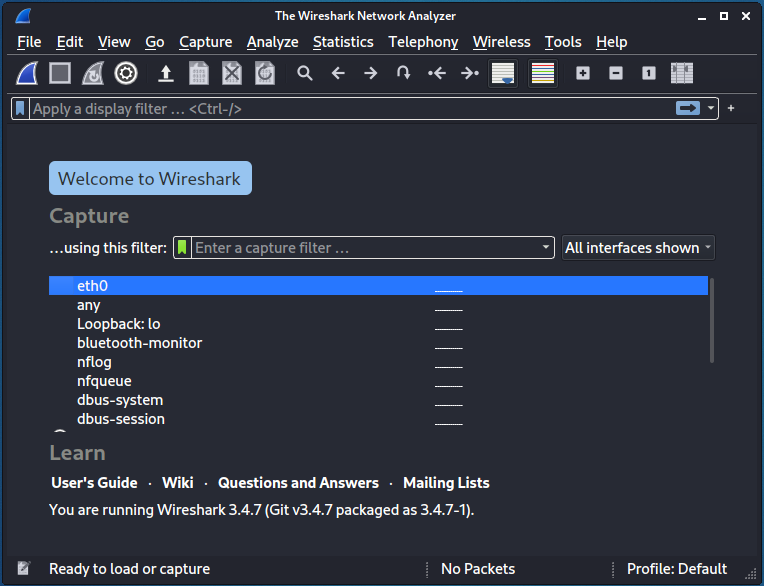
Unfiltered: Quando a porta responde ao Nmap, porém o mesmo não consegue determinar se está aberta ou fechada.

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.

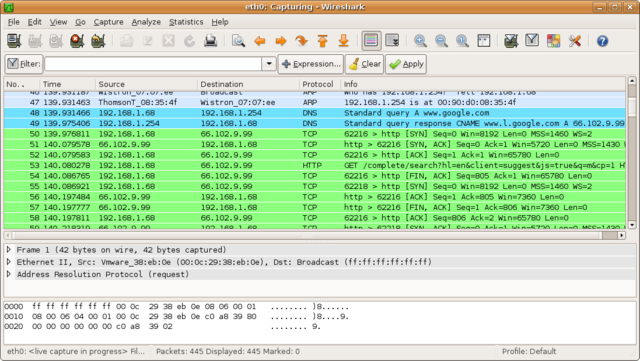
Criada em contribuição voluntária de diversas pessoas ao redor do globo a ferramenta é a continuação de um projeto iniciado por Gerald Combs em 1998.



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 analise mais intuitiva.

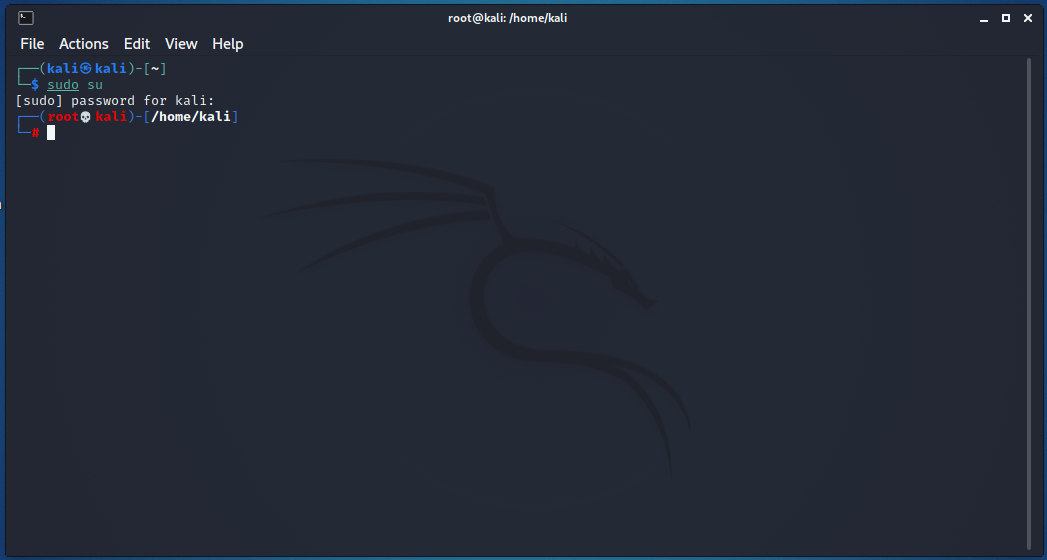


Wireshark analisando uma rede e mostrando os pacotes capturados

1. COMANDOS UTILIZADOS NO LINUX?

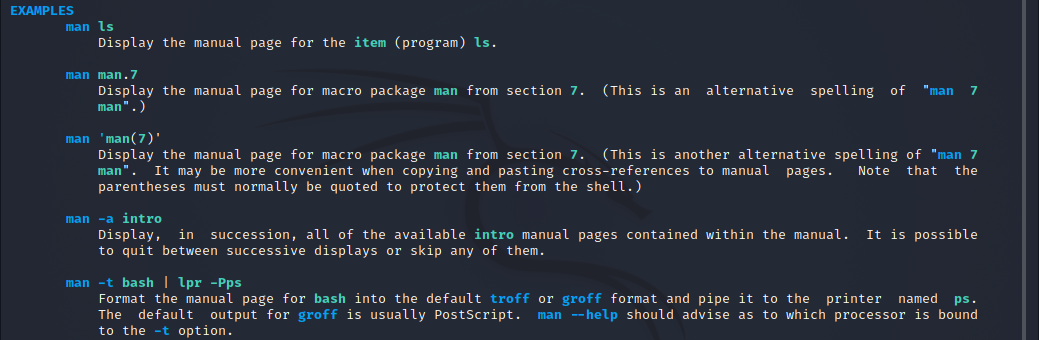
$ sudo su

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



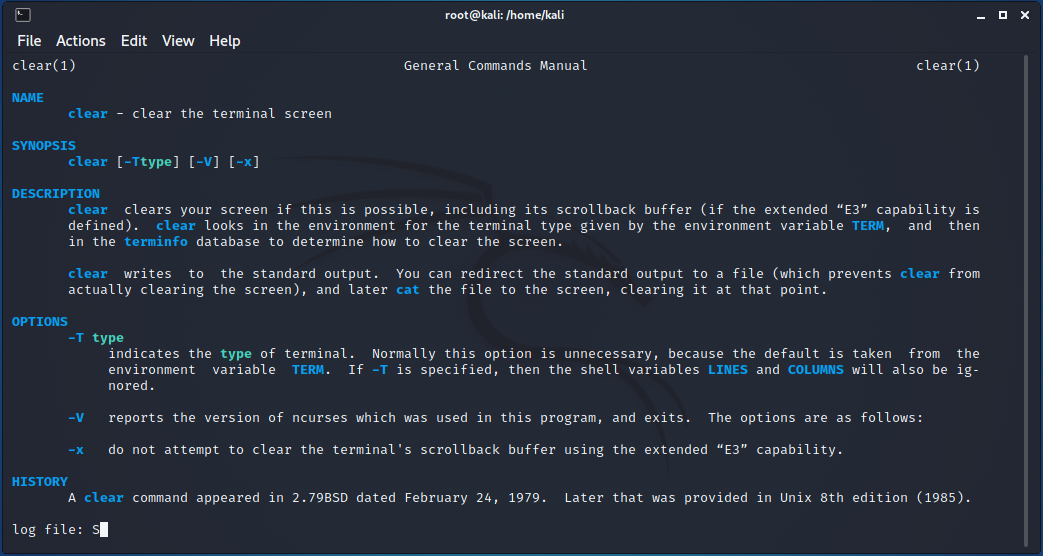
$ man (alguma interface do sistema)

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



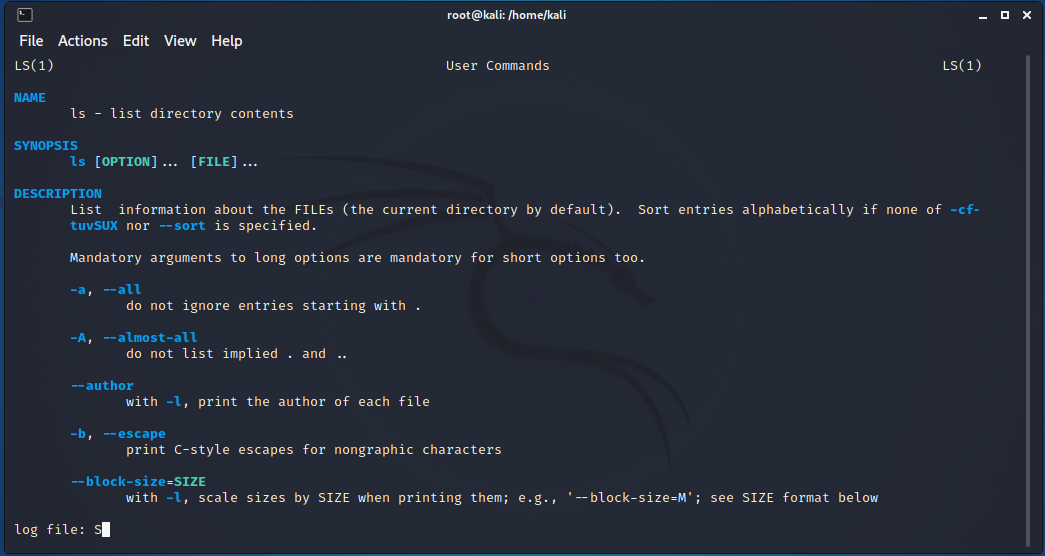
$ clear

Utilizado para limpar a tela do terminal



$ ls

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



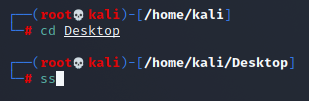
$ chmod

Permite alterar as configurações de permissão de arquivos e diretórios



$ cd

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



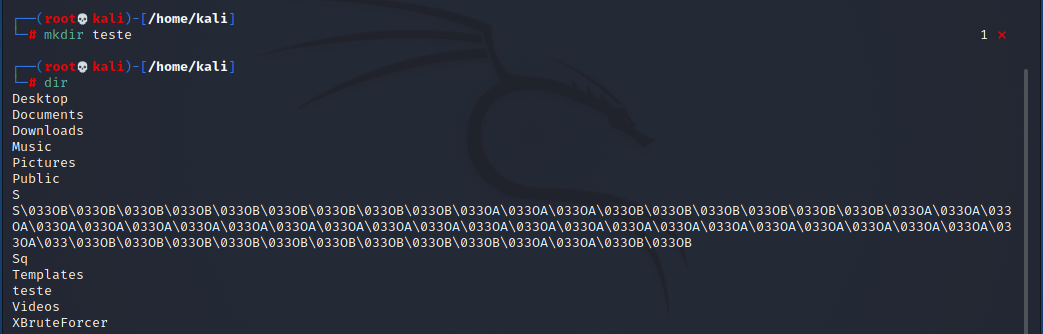
$ dir

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



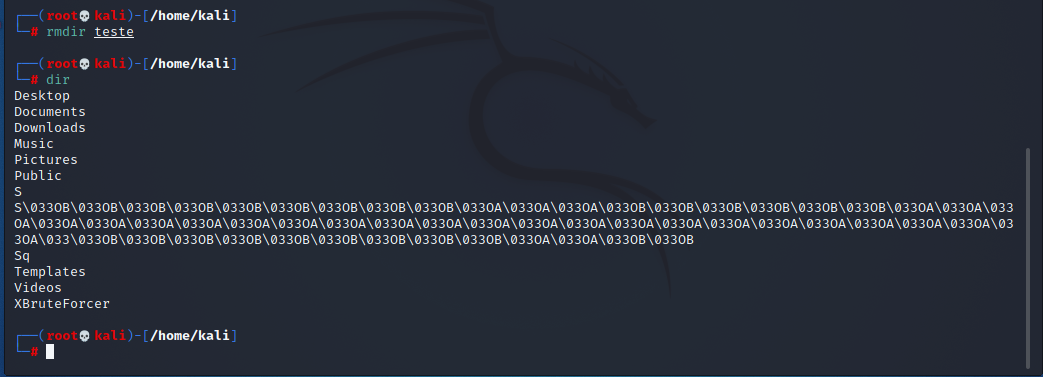
$ mkdir

Comando utilizado para criação de um novo diretório

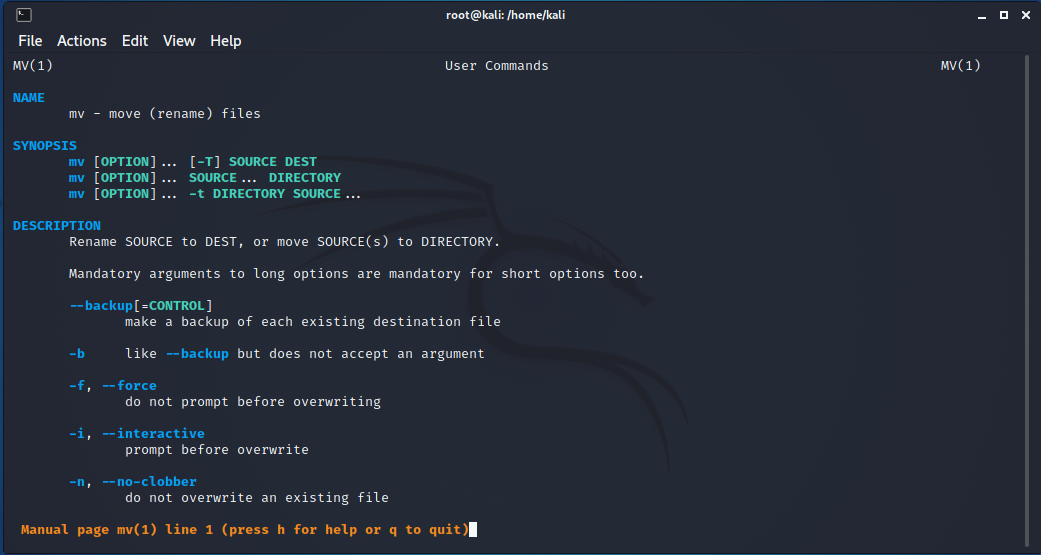


$ rmdir

Utilizado para remoção de diretórios (devem estar vazios)



$ mv

Comando utilizado para mover pastas e arquivos para outro diretório e também para os renomear

# 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/