

# GUIA HACKER

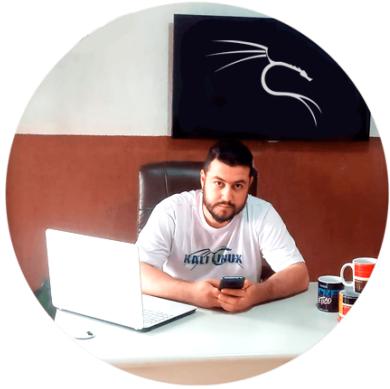
O PASSO INICIAL PARA  
COMEÇAR A SER UM HACKER



# SUMÁRIO

- 
- 01** / Sumário
  - 02** / Quem sou eu
  - 03** / Introdução
  - 05** / Hackers e Crackers
  - 06** / Tipos de chapéus
  - 07** / O que faz o Hacker ético
  - 08** / Distros Hackers
  - 10** / Como instalar o KALI linux
  - 12** / Resumo parte 1 e parte 2
  - 22** / Fase 1 – Reconhecimento e ferramentas
  - 30** / Fase 2 – Varreduras e ferramentas
  - 33** / Fase 3 – Enumeração e ferramentas
  - 36** / Fase 4 – Tipos de ataques e ferramentas
  - 43** / Fase 4.1 – Analisador de pacotes (Sniffers) e ferramentas
  - 46** / Fase 5 – Relatório final
  - 47** / Considerações finais
-

# QUEM SOU EU ?

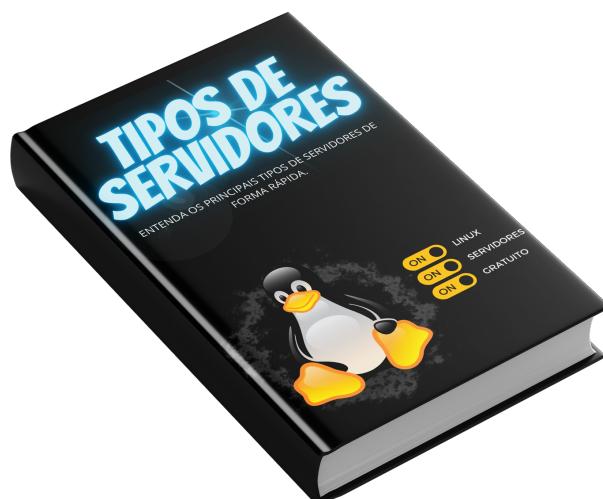
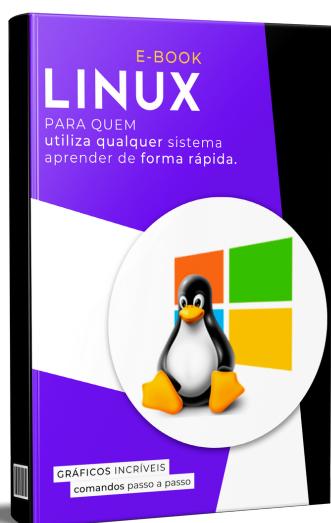


*Fernando Silva*

Olá amigos, prazer sou o **Fernando Silva** tenho 29 anos, moro em SP e sou empreendedor e hacker. A primeira vez que utilizei o **Linux** foi em 2011(Ubuntu) desde então venho estudando esse sistema incrível que proporciona milhares de oportunidades no mercado de TI.

Hoje utilizo o perfil no **instagram (@linux.gnu)** para dar dicas sobre o **Linux** e **Hacking**, hoje esse perfil conta com mais de 50.000 seguidores, sendo um dos maiores se tratando desse segmento.

## E-BOOKS ESCRITOS POR MIM.





# HACKER ÉTICO

## PASSO A PASSO

- ✓ DOMINE O LINUX
- ✓ COMO ENCONTRAR FALHAS
- ✓ HACKEANDO DO ZERO

- ✓ CRIE ROBÔS HACKING
- ✓ ACESSE REDES WI-FI
- ✓ TENHA O PODER DE ATAQUE

**QUERO SABER MAIS !**

# INTRODUÇÃO

## FERRAMENTAS QUE OS **HACKERS UTILIZAM**

Você está prestes a conhecer as principais ferramentas que **os Hackers utilizam**, ferramentas PODEROSAS que nas mãos de quem sabe utilizá-las viram **verdadeiras armas**.

A minha intenção aqui é apresentar para você um **GUIA COM** as principais ferramentas que os **HACKERS utilizam**.

A mesma ferramenta pode ser **utilizada em várias etapas do processo**, passando parâmetros diferentes.



# FASES QUE O HACKER PERCORRE

## COLETA DE INFORMAÇÕES PÚBLICAS e SIGILOSAS

## MAPEAMENTO DA REDE/VARREDURA

Descobrindo a topologia da rede, IP, sistema operacional...

## ENUMERAÇÃO DE SERVIÇOS

Entender como o sistema está configurado anotar tudo.

Como, serviços, portas, versões, usuários ...

## OBTER ACESSO E BUSCAS POR VULNERABILIDADES

Informações o suficiente para utilizar técnicas de brute force, etc.

## EXPLORAÇÃO DA VULNERABILIDADES

Parando, iniciando serviços, garantido a volta ...

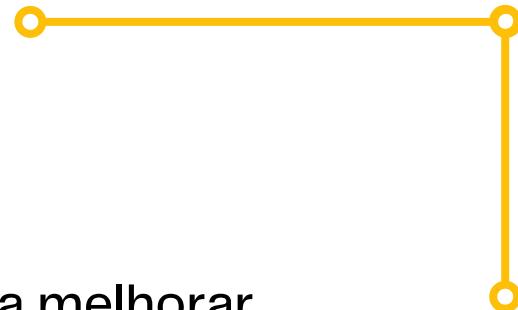
## EVIDÊNCIAS E REPORTE



# DIFERENÇAS



Hacker



Utilizam seus conhecimentos **para melhorar sistemas** e encontrar brechas de segurança para que elas possam ser corrigidas, ou melhoradas, **sem a intenção de prejudicar**.



Crackers

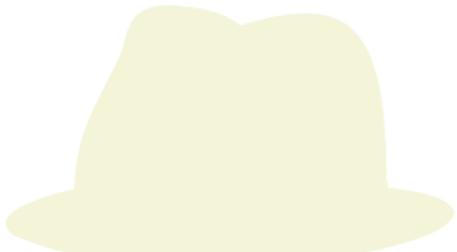


São **Cibercriminosos** que utilizam seus conhecimentos e obter algum aproveito próprio, e **prejudicar pessoas** ou empresas.

**Esse termo foi difundido pela própria comunidade hacker** para que a mídia e pessoas leigas parassem de categorizar todas as pessoas hackers como criminosas. Apesar disso, o termo ainda é muito controverso, já que, quando se trata de bem e mal, legal ou ilegal, as linhas podem ficar um pouco difusas em algum momento. Por isso, **outros termos são mais adotados pela comunidade atualmente**

# TIPOS DE CHAPÉUS

## Branco



utiliza seus **conhecimentos de forma ética**, visando antecipar os movimentos dos chapéus pretos e confrontar suas ações. Geralmente, chapéus brancos são pessoas que **trabalham em instituições** e grandes organizações, fortalecendo a segurança

## Preto



hackers que preferem utilizar seu **conhecimento de modo ilegal**, como roubos de dados e dinheiro ou tirando sistemas do ar. Suas intenções são sempre maliciosas e **suas ações são consideradas crimes**.

## Cinza



são hackers que são mais interessados em vender suas **habilidades** para quem pagar mais, logo, a ética geralmente não vem em primeiro lugar.

# O QUE FAZ UM HACKER ÉTICO ?

Esse profissional **procura por vulnerabilidades** que possam ser exploradas por chapéus pretos, para assim **evitar prejuízos reais** onde em muitos casos são irreversíveis.

O **objetivo principal dos hackers éticos é simular ciberataques** em um ambiente controlado para evitar perdas enormes.

Recentemente a **AMERICANAS** sofreu um ataque, onde ficou fora do ar por alguns dias e teve um prejuízo de quase **R\$: 1 Bilhão de reais**.

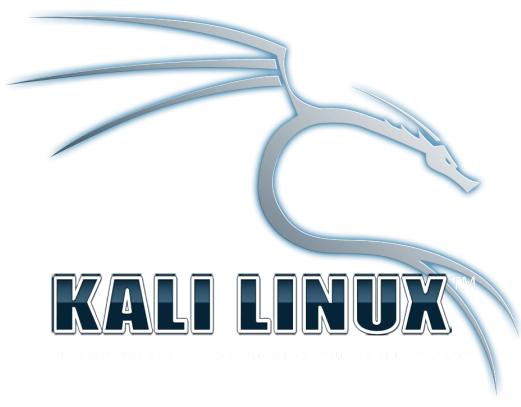


Outro caso é o **vazamento do GTA6** a empresa estava mantendo sigilo há pelo menos 8 anos, quando de repente um **hacker explora uma falha** e obtém sucesso. Casos como esses são comuns, mas exemplos é o da Uber e a RecordTV.

Por isso empresas como essas pagam **R\$: 100 mil dólares para HACKERS ÉTICOS descobrirem e corrigirem** essas falhas, pois evitam um prejuízo 10x, 20x 50x maior.

# DISTRO SISTEMA OPERACIONAL

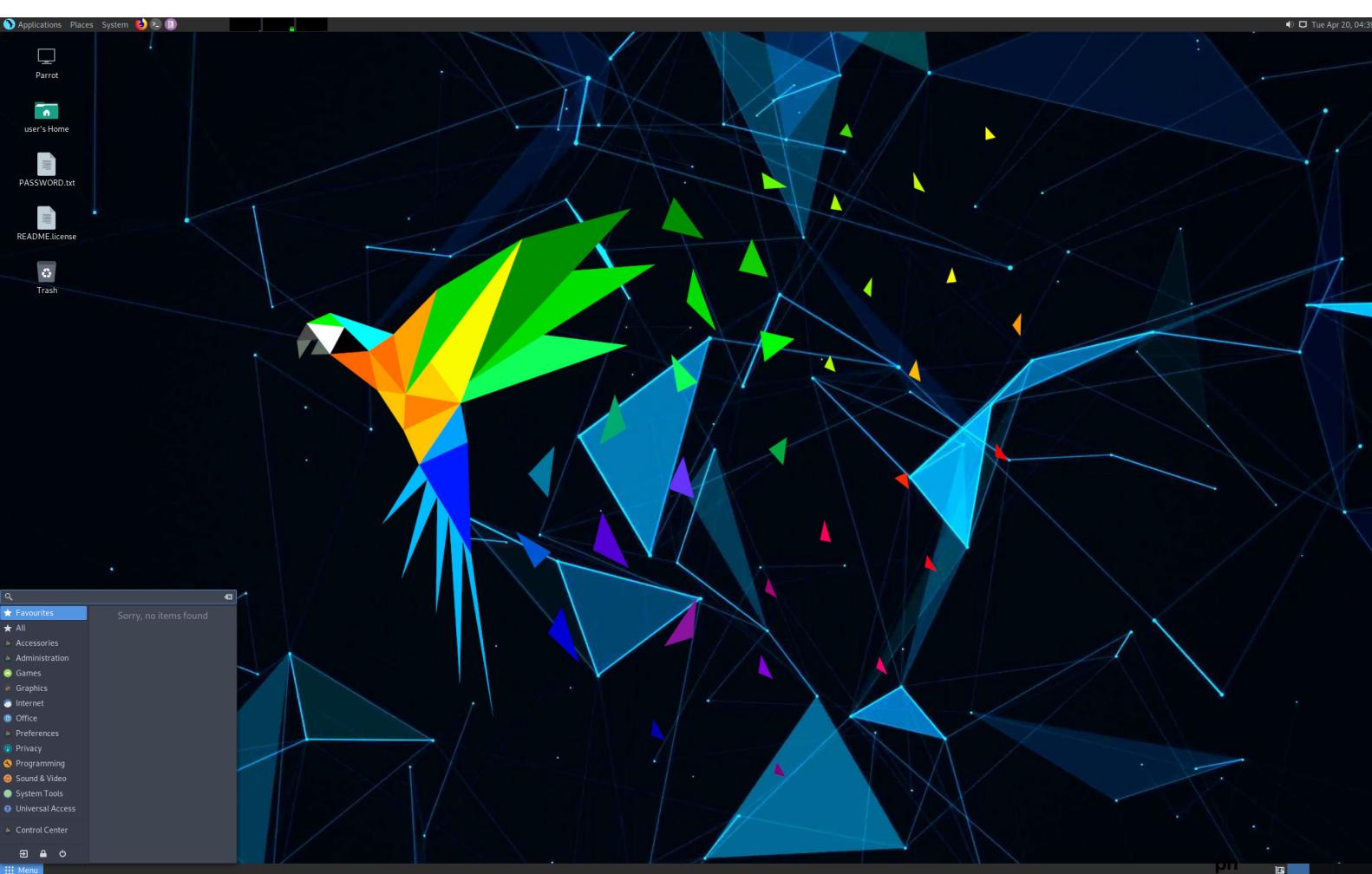
Normalmente essas são as distros utilizadas pelos Hackers, porque são **voltadas para área de segurança** e já vem com centenas de ferramentas instaladas. Você pode ter um **Debian e instalar todas ferramentas** necessárias, caso queira.



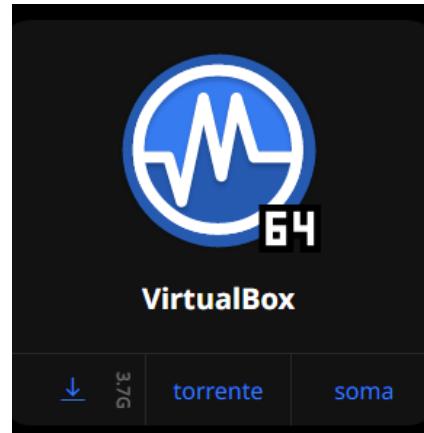
É uma distribuição Linux baseada em Debian de código aberto **voltada para várias tarefas de segurança da informação, como teste de penetração**, pesquisa de segurança, análise forense de computadores e engenharia reversa.



**Parrot OS**, o principal produto da Parrot Security, é uma distribuição GNU / Linux baseada no Debian também.



# COMO INSTALAR KALI LINUX NA VM



## PARTE 1

Baixe essa imagem, basta digitar no google kali linux download



## PARTE 3

Você terá esse arquivo salvo em seu computador



## PARTE 4

Selecione a opção importar dentro do virtualbox.

Importar Appliance Virtual

Appliance para importar

Especifique a origem de onde o appliance será importado. A origem pode ser um sistema de arquivos local para importar o arquivo OVF, ou um dos provedores de nuvens conectados para importar a VM.

Origem (S): Sistemas de Arquivos Local

Selecione um arquivo de onde será importado o appliance virtual. O VirtualBox atualmente suporta importar appliances salvos no formato Open Virtualization Format (OVF). Para continuar, selecione o arquivo a importar da lista abaixo.

Arquivo (F): C:\Users\fernanda\Downloads\kali-linux-2022.2-virtualbox-amd64.ovf\kali-linux-2022.2-virtualbox-amd64.ovf



## PARTE 5

Selecione o arquivo OVA que você baixou e importe.

## PARTE 6

Iniciar



PRONTO

LOGIN: **kali**

SENHA: **kali**

# RECAPITULANDO

## O BÁSICO DE LINUX



# ARQUITETURA

## EQUIPAMENTO FÍSICO

Parte física do computador como placa de memória RAM, disco



## HARDWARE

## KERNEL



## CORAÇÃO DO SISTEMA

É basicamente o coração do sistema, no Kernel está escrita todas as instruções de gerenciamento do Sistema e do Hardware.

## BIBLIOTECA DE FUNÇÕES PADRÃO

É a camada que permite o acesso a recursos através da execução de chamadas feitas por processos, como Habilitar



## BIBLIOTECA

## SHELL



## INTERPRETA COMANDOS

interpretador de comandos, um entre os diversos tradutores entre o usuário e o sistema operacional conhecidos como shell.

## PROGRAMAS UTILIZADOS

Softwares utilizados pelo usuário como browsers, editores de texto, editores de imagens etc.

Uma DISTRIBUIÇÃO Linux já vem com alguns softwares específicos instalados.



## APLICAÇÕES

# DERIVADOS

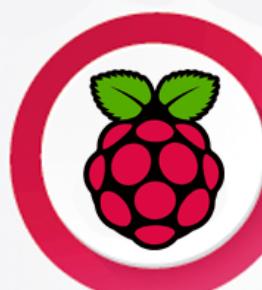
## UBUNTU

POPULARIZADO  
LANÇADO EM 2004



## RASPBIAN

MAIS DE 35.000 PACOTES DEB PARA  
COMPUTADORES RASPBERRY PI



## MINT

LINUX MINT É UMA DISTRIBUIÇÃO LINUX IRLANDESA.  
POSSUI DUAS VERSÕES: UMA BASEADA EM UBUNTU E  
OUTRA VERSÃO BASEADA EM DEBIAN

## DEEPIN

DEEPIN USA SEU PRÓPRIO AMBIENTE DE DESKTOP  
QUE É INTEGRADO COM OUTRAS APLICAÇÕES PRÓPRIAS



## LITE

O PROPÓSITO DO LINUX LITE É A  
INTRODUÇÃO DO LINUX  
AOS USUÁRIOS DE WINDOWS.



## DERIVADOS



## debian

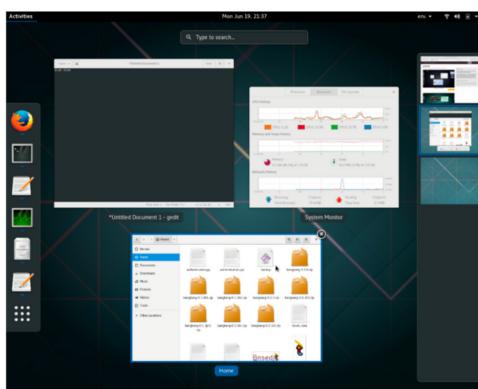


## KALI

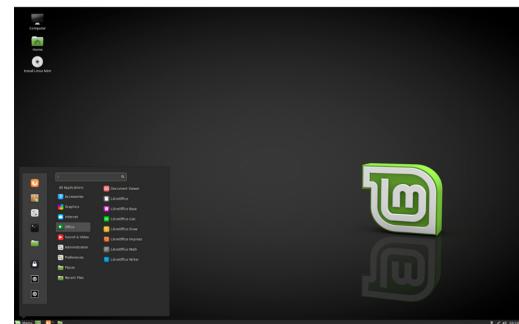
AUDITORIAS DE SEGURANÇA E  
TESTES DE PENETRAÇÃO

# INTERFACES

GNOME



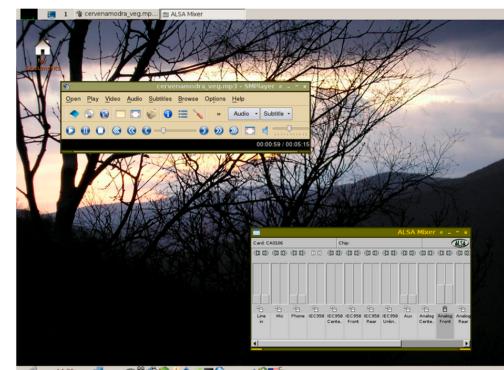
CINNAMON



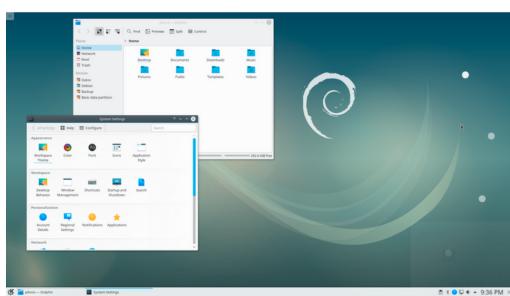
XFCE



LXDE



KDE  
PLASMA



MATE



# DIRETÓRIOS

## ESTRUTURA



# COMANDOS



**\$:** usuário comum (sem privilégios)  
**#:** super usuários (**root**/administrador)



**ls:** listar  
**ls -l:** listar detalhes



**cd:** navega entre os diretórios  
**cd ~ :** ir para diretório /home  
**cd .. :** voltar para uma diretório acima



**touch:** criar arquivo  
**> :** criar arquivo  
**cat:** exibe o conteúdo de um arquivo



**mkdir:** criar pastas  
**rm:** excluir (diretórios/arquivos)  
**rmdir:** excluir diretórios **vazios**

**rm -f:** força excluir arquivos  
**rm -rf:** força excluir pastas



**mv:** mover ou renomear  
**cp:** copiar arquivos ou diretórios



**pwd:** onde estou? diretório atual  
**clear:** limpa tela do terminal



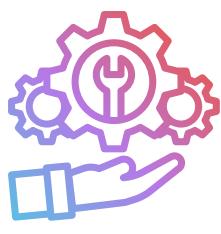
**df:** espaço em disco

**df -h:** espaço em disco com leitura legível para humanos



**free:** espaço de memória

**free -h:** espaço de memória de forma mais legível



**apt-get install** nomedopacote

**apt-get remove** nomedopacote

**apt-get update:** atualizar repositórios

**apt-get upgrade:** atualizar sistema



**dpkg -i:** nomedopacote.deb

**dpkg -l:** listar pacotes instalados



**uname -a:** informações do Kernel

**uptime:** há quanto tempo o sistema está ativo

**who:** quem está conectado na máquina



**adduser:** cria usuários ou grupos (-group) no sistema

**userdel:** remove usuário

**groupdel:** remove um grupo



**passwd:** mudar senha do usuário atual



**passwd username:** mudar a senha do usuário especificado



**ifconfig:** seu endereço IP e informações de rede

**route:** tabela de rotas IP

**iwlist scan:** exibe as redes sem fio



**lspci:** o que está conectado no **barramento PCI**

**lsusb:** o que está conectados nas **saídas USB**



**tar -cvzf Arquivos.tar.gz:** Compressão **gz**

**tar -cvjf Arquivos.tar.bz2:** Compressão **bz2**

**z:** Tipo gz

**j:** Tipo bz2



**tar -xvf Arquivos.tar.gz:** Descompactado **.gz**

**tar -xvf Arquivos.tar.bz2:** Descompactado **.bz2**

**x:** Extrai



**ps:** visualizar processos atuais do usuário

**ps aux:** exibe todos os processos de todos os usuários



**halt:** desligar o computador

**reboot:** reiniciar o computador

**systemctl start httpd.service:** Inicia um serviço

**systemctl stop httpd.service:** Para um serviço

**systemctl restart httpd.service:** Reinicia um serviço

**systemctl status httpd.service:** Estado de um serviço

**systemctl enable httpd.service:** Inicia o serviço no Boot

**systemctl disable httpd.service:** Remove o serviço do Boot



# PERMISSÕES



- **rwx rwx rwx**

permissões do arquivo dividido em  
**3 grupos** (comando ls-l)

- tipo de arquivo (comum)

**Grupo1** **rwx**: permissões do **proprietário** e/ou usuário

**Grupo2** **rwx**: permissões para usuários do **grupo**

**Grupo3** **rwx**: permissões para **todos** usuário (qualquer um)



**r**: read (permissão de leitura)

**w**: write (permissão de escrita)

**x**: execute (permissão de execução)

**Todos os grupos**

tem todas permissões

## Permissões em valores decimais

**0**: --- (nenhuma permissão)

**1**: --x (somente execução)

**2**: -w- (somente escrita)

**3**: -wx (escrita e execução)

**4**: r-- (somente leitura)

**5**: r-x (leitura e execução)

**6**: rw- (leitura e escrita)

**7**: rwx (leitura, escrita e execução)

comando chmod  
para **alterar as  
permissões**



# RESUMO PARTE 1

## O QUE VOCÊ APRENDEU...

- DIFERENÇAS HACKER E CRACKER
- TIPOS DE **CHAPÉUS**
- COMO UM **HACKER ÉTICO** TRABALHA
- **DISTROS** HACKERS
- COMO INSTALAR O **KALI LINUX** NA VM
- O BÁSICO DE **LINUX**

# RESUMO PARTE 2

## O QUE VOCÊ VAI APRENDER...

- FASES QUE O HACKER PERCORRE
- FASE 1 - **RECONHECIMENTO**
- FASE 2 - **VARREDURA**
- FASE 3 - **ENUMERAÇÃO**
- FASE 4 - **ATAQUES**
- FASE 5 - **RELATÓRIO**

## FASE 1

# RECONHECIMENTO FOOTPRINTING

O termo "Footprinting" geralmente se refere a uma das fases de pré-ataque, que são tarefas executadas antes de se fazer o ataque real.

Metodologia utilizada para **obter informações do ALVO**, muitas informações importantes podem estar disponíveis para todos na internet, por exemplo **GOOGLE** mesmo.

Essas informações é útil **para um HACKER que está tentando quebrar todo o sistema.**

**Algumas informações que devem ser obtidas nessa fase:**

- E-mails
- Telefones
- Datas
- Nomes dos Funcionários, Chefes, etc.
- Nome de domínios, sites e subdomínios
- Informações sobre DNS

# FERRAMENTAS UTILIZADAS PARA RECONHECIMENTO

## GOOGLE HACKING

Encontra **brechas de segurança nas configurações** ou nos códigos utilizados pelos website e outras aplicações.

Se utiliza de operadores de busca avançados para localizar erros específicos e explorar vulnerabilidades.

Muitos CRACKERS manipulam esses operadores para encontrar dados sensíveis, como:

- Configurações
- Cartões de créditos
- Senhas
- Erros, falhas

e muitas outras possibilidades

Esse conhecimento pode ser utilizado para o bem ou para o mal.

# OPERADORES UTILIZADOS

**site:** Pesquisa dentro de um site específico

**intitle:** Pesquisa o título de uma página

**inurl:** Busca termos na URL

**intext:** Resultados no texto do texto

**filetype:** Formatos de arquivos (txt, doc, pdf...)

## Fazendo buscas por telefones

site:uol.com.br intext:telefone

## Busca por arquivos txt contendo senhas nos domínios .com.br

site:com.br filetype:txt intext:senhas

## Busca arquivos de banco de dados sql, palavra chave "senha" nos sites do governo do Brasil

site:gov.br filetype:sql intext:senha

# SHODAN GOOGLE DOS HACKERS

Já imaginou um mecanismo de busca **capaz de rastrear qualquer aparelho conectado à internet**, fornecendo detalhes que podem permitir o acesso por hackers a milhões de dispositivos. Ele existe, e se chama Shodan.

Essa ferramenta permite fazer buscas de dispositivos conectados à internet.

Como roteadores, webcams smartphones, tablets, computadores, servidores, sistemas de videoconferência, sistema de refrigeração, etc.

O Shodan funciona vasculhando servidores de internet como HTTP/HTTPS, FTP, SSH, Telnet, SNMP, SIP, UPnP com objetivo de encontrar dispositivos conectados à rede.

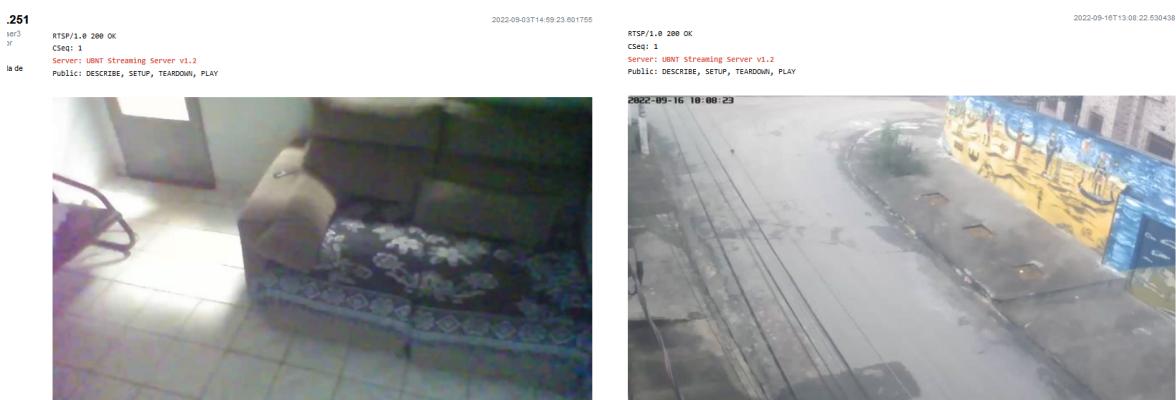
**Você consegue saber quantos Windows xp estão rodando em um estado.**

# UTILIZANDO NA PRÁTICA SHODAN

The screenshot shows the Shodan Explore interface. At the top, there are links for 'SHODAN', 'Explore', 'Pricing', and a search bar. Below the search bar is a red search button. The main area is titled 'Explore' and includes sections for 'CATEGORIES' (Industrial Control Systems, Databases, Network Infrastructure, Video Games), 'RESEARCH' (Shodan 2000, featuring an 80's retro-futuristic interface to synthwave music), 'BROWSE SEARCH DIRECTORY' (with a search bar for shared queries), 'Popular Tags' (listing terms like webcam, cam, camera, ip, router, scada, ftp, server, http, io, test, password, cisco, web, default, login, ssh, i, nes, ipcam), 'Job Board' (listing websites that advertise jobs via HTTP), and 'Ethereum Miners' (listing devices that mine Ethereum, with tags for cryptocurrency and ethereum).

Entre no site shodan.io e acesse Explorar, será mostrado várias categorias.

Veja algumas imagens de câmeras que estão abertas e provavelmente não deveriam



# UTILIZANDO FILTROS NO SHODAN

Você pode utilizar diversos filtros para encontrar dispositivos específicos. **Veja alguns exemplos.**

**City:** Limita o resultado da busca a dispositivos localizados na cidade. Por exemplo: "city:miami".

**Country:** Limita o resultado da busca a dispositivos localizados no país utilizando o respectivo código de dois dígitos. Por exemplo, "country:US".

**Hostname:** Limita o resultado da busca a dispositivos com o respectivo nome de host. Por exemplo, "hostname:facebook.com".

**Operating system:** Limita o resultado da busca a dispositivos que utilizem determinado dispositivo. Por exemplo, "microsoft os:windows".

# + FERRAMENTAS UTILIZADAS PARA RECONHECIMENTO

## Have I Been Pwned

Nesse site você pode verificar se já houve vazamento de dados de um determinado e-mail ou telefone, essas informações podem ser úteis nas próximas etapas.

## Wappalyzer

Essa é **uma extensão** que você adicionar em seu navegador para **visualizar as tecnologias/plataformas** utilizadas em um determinado site. Essas informações podem ser muito úteis para descobrir falhas/bugs em determinadas versões de software que estão rodando.

## Whois

Um site que você pode **visualizar informações de um domínio** (uol.com.br) exemplo ...

- Servidor DNS
- Titular
- Data de criação
- Status
- Contato
- E-mail

## hunter.io

Nesse site você consegue E-mails de uma empresa através do domínio.

## ping

Utilizado para descobrir se um host está ativo (online).

## fping

Uma lista de IPs para serem "**testado**" descobrindo assim quem dessa lista está online na rede.

Ex: #fping -f ips.txt

ou

Você pode usar a **opção -g** para verificar um intervalo grande como todos os **255 hosts**

Ex: fping -g 192.168.1.0/24



### ips.txt

192.168.0.1  
192.168.0.2  
192.168.0.3  
192.168.0.4  
192.168.0.5

## genlist

Praticamente a mesma coisa. Faz **ping em todos os hosts** de uma rede e exibir os IPs que responderam, ou seja os "ativos".

Ex: #genlist -s 192.168.16.\*

## FASE 2

# VARREDURAS SCANNING

O objetivo é realizar um **port scan** e identificar portas e serviços ativos no ALVO.

## 3 tipos de Scanning

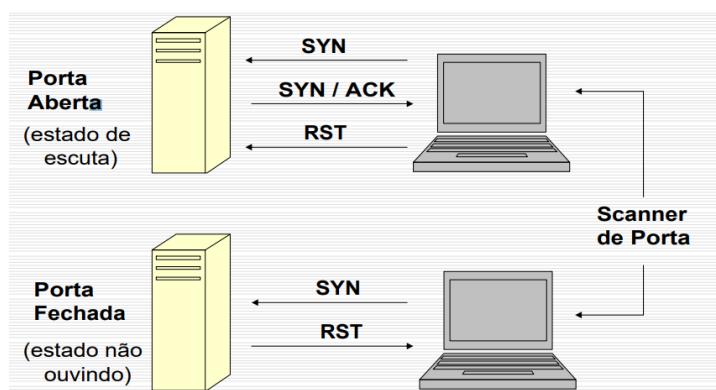
- Hosts ativos na rede
- Portas ativas e serviços
- Vulnerabilidades do sistema, é um scan mais avançado.

## Técnica TCP SYN

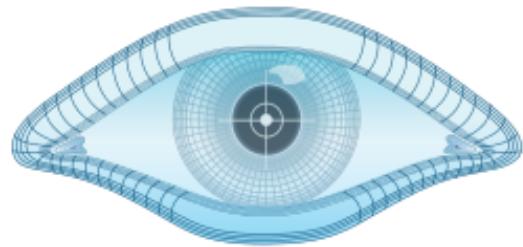
O scanner **envia um a mensagem SYN**, como se estivesse pedindo conexão.

O alvo **envia uma resposta** com SYN/ ACK indica que a porta está ouvindo, através de um serviço.

Um RST indica que a porta não está ouvindo.



# FERRAMENTAS UTILIZADAS PARA VARREDURAS



**NMAP**

Nmap é um **software livre que realiza port scan** desenvolvido pelo Gordon Lyon. Muito utilizado para avaliar a segurança, e para descobrir serviços ou servidores em uma rede. O Zenmap uma "versão" gráfica do Nmap, **está disponível para Windows**.

Essa ferramenta pode ser utilizada em **várias etapas do processo** de "hackear"

## Recursos

- Descoberta de hosts
- Scanner de portas: Mostrando as portas TCP e UDP abertas.
- Detecção de versão: Exibe os softwares do ALVO e as versões.
- Detecção do sistema operacional: Exibe o SO que está rodando no ALVO.
- Execução de scripts: Fase mais avançada.

**#nmap 192.168.1.12**

Retorna informações importantes, como portas **abertas**, **serviços**, e **endereços MAC**.

**#nmap -sn 192.168.1.0/24**

Envia ping para esse **range de IPs** e retorna somente os dispositivos que responderam. (**IPs e Endereços MACs**)

**#nmap -Pn 192.168.1.12**

Faz a varredura **sem usar o PING**, isso faz com que passe "despercebido" do firewall.

# Nessus

O Nessus é uma ferramenta de verificação de segurança remota, que verifica um computador e emite um alerta se descobrir alguma vulnerabilidade que **Hackers ou Crackers possam usar para obter acesso** a qualquer computador conectado a rede.

Se você puder fazer uma varredura de vulnerabilidade em uma rede interna, você terá um banco de dados de todas as vulnerabilidades potenciais na rede.

É uma ótima ferramenta para ajudar administradores de redes a manter seus domínios livres das **vulnerabilidades fáceis que hackers e vírus costumam explorar**.

The screenshot shows the Nessus web interface. On the left, there's a sidebar with 'Folders' (My Scans, All Scans, Trash) and 'Resources' (Policies, Plugin Rules, Customized Reports, Scanners). The main area is titled 'Live Results Scan' and shows a table of vulnerabilities. The table has columns for 'Hosts' (1), 'Vulnerabilities' (45), and 'History' (1). A filter bar allows searching for vulnerabilities. To the right of the table, a message box says: 'Notice: This scan has been updated with Live Results. Launch a new scan to confirm these findings or remove them.' Below this is a 'Scan Details' section with fields: Name (Live Results Scan), Status (Completed), Policy (Advanced Scan), Scanner (Local Scanner), and Modified (Today at 6:03 PM (Live Results)). At the bottom right is a 'Vulnerabilities' chart showing the distribution of severity levels: Critical (red), High (orange), Medium (yellow), Low (green), and Info (blue).

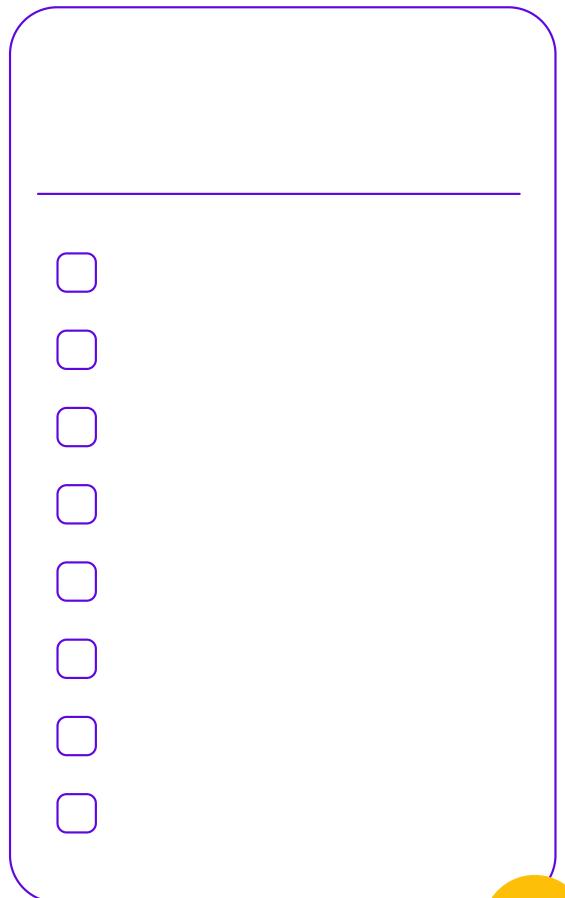
Hosts	Vulnerabilities	History			
1	45	1			
<input type="button" value="Filter"/> <input type="text" value="Search Vulnerabilities"/> <input type="button" value="Search"/>					
45 Vulnerabilities					
	Sev	Name	Family	Count	
<input type="checkbox"/>	Critical	LIVE Mozilla Foundation Unsupported Application ...	MacOS X Local Security Checks	1	<input type="radio"/> <input type="checkbox"/>
<input type="checkbox"/>	High	LIVE Mozilla Firefox < 59 Multiple Vulnerabilitie... (m...)	MacOS X Local Security Checks	1	<input type="radio"/> <input type="checkbox"/>
<input type="checkbox"/>	High	LIVE Mozilla Firefox < 59.0.1 Multiple Code Executi... (m...)	MacOS X Local Security Checks	1	<input type="radio"/> <input type="checkbox"/>
<input type="checkbox"/>	High	LIVE Mozilla Firefox < 59.0.2 Denial of Service Vuln... (m...)	MacOS X Local Security Checks	1	<input type="radio"/> <input type="checkbox"/>
<input type="checkbox"/>	High	LIVE Mozilla Firefox < 60 Multiple Critical Vulnerabil... (m...)	MacOS X Local Security Checks	1	<input type="radio"/> <input type="checkbox"/>
<input type="checkbox"/>	High	LIVE Mozilla Firefox < 61 Multiple Critical Vulnerabil... (m...)	MacOS X Local Security Checks	1	<input type="radio"/> <input type="checkbox"/>
<input type="checkbox"/>	High	LIVE Mozilla Firefox < 62 Multiple Critical Vulnerabil... (m...)	MacOS X Local Security Checks	1	<input type="radio"/> <input type="checkbox"/>
<input type="checkbox"/>	Medium	SSL Certificate Cannot Be Trusted	General	1	<input type="radio"/> <input type="checkbox"/>
<input type="checkbox"/>	Info	Netstat Portscanner (SSH)	Port scanners	16	<input type="radio"/> <input type="checkbox"/>
<input type="checkbox"/>	Info	Service Detection	Service detection	4	<input type="radio"/> <input type="checkbox"/>
<input type="checkbox"/>	Info	HTTP Server Type and Version	Web Servers	2	<input type="radio"/> <input type="checkbox"/>
<input type="checkbox"/>	Info	Additional DNS Hostnames	General	1	<input type="radio"/> <input type="checkbox"/>

## FASE 3

# ENUMERAÇÃO INFORMAÇÕES

Enumeração é o processo de extrair informações de um sistema alvo **para entender melhor suas configurações**, essa fase já é mais invasiva, utiliza-se de **ferramentas e parâmetros mais agressivos** e é importante adquirir informações como ...

- Nomes das máquinas
- Hardware, memória total.
- uptime do sistema
- Usuários e grupos
- Servidores, Serviços e versões
- Compartilhamentos
- Tabela de roteamento
- Aplicações e banners
- Endereço MAC
- Detalhes de SNMP E DNS, Registro MX ,etc.



# FERRAMENTAS UTILIZADAS PARA FASE DE ENUMERAÇÃO

## Nmap

Essa ferramenta é utilizada para vários objetivos, ela pode ser utilizada de forma mais agressiva, dependendo do grau e do objetivo.

## NBTscan

NBTscan é um programa para varredura de redes IP para informações de NetBIOS.

Para cada host respondido, ele lista o endereço IP, o nome do computador NetBIOS, o nome de usuário conectado e o endereço MAC.

**EX: nbtscan -v 192.168.11-159**

```
# nbtscan --help
```

## Snmpcheck

Enumerador de SNMP (É o protocolo padrão para monitoramento e gerenciamento de redes). É possível se obter informações, como, hostsnames, interfaces de redes, serviços, processos, uptime do sistema, memória, hardware entre outras informações.

```
# snmp-check -h
```

# Netcat

O Netcat é uma ferramenta de rede, que permite **abrir portas TCP/UDP**.

**Permite forçar conexões UDP/TCP** utilizado para uma série de tarefas de manutenção, desenvolvimento, levantamento e troubleshooting de rede.

# nslookup

Utilizado para se obter informações sobre DNS de um determinado domínio

<https://www.nslookup.io/>

# dnsenum

script multithread para **enumerar informações** em um domínio como, endereço do host , registro MX, registro A, nomes de servidores.

`# dnsenum -h`

# dnsrecon

É um script Python que oferece a capacidade de realizar pesquisas de, registros NS, registro SOA, registros mx, transferências de zona e enumeração de serviços.

`# dnsrecon -h`

## FASE 4

# TIPOS DE ATAQUES EXPLORAÇÃO

Através das fases anteriores **RECONHECIMENTO**, **VARREDURA** e **ENUMERAÇÃO** o Hacker já possui diversas informações em mãos, como **portas abertas**, **serviços** (versões) e **vulnerabilidades**, onde o ataque poderá ser feito.

Agora irei te apresentar ferramentas de ataques, não faça isso, pois rastros serão deixados e você será encontrado facilmente.



# FERRAMENTA UTILIZADAS PARA NEGAÇÃO - SYN FLOOD

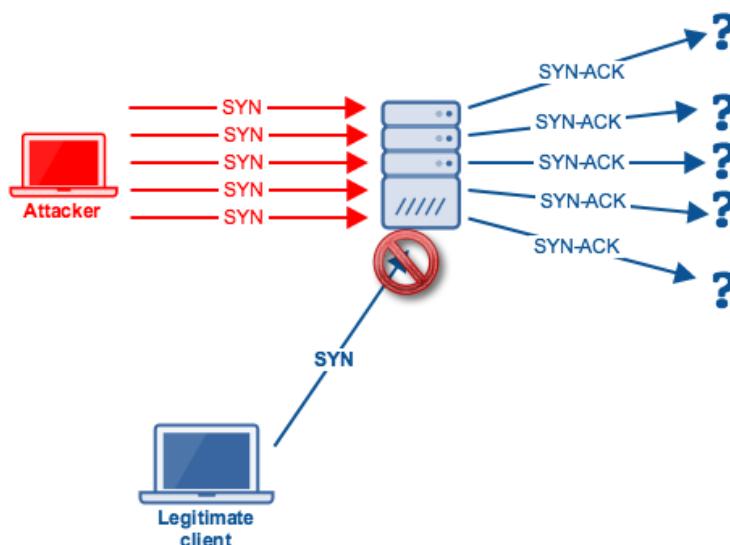
## hping3

Você pode usar essa ferramenta para esse tipo de ataque, mas **atenção não faça isso, seu rastro irá ficar registrado nos LOGs do sistema da "Vítima" e você será encontrado.**

Faça isso em algum servidor seu, **por exemplo em máquinas virtuais.** Esse ataque fará a máquina "travar" negação de serviços.

# hping3 -c 20 -S 192.168.1.1 -a 192.168.1.58 -p 80 --flood

Esse comando irá enviar 20 pacotes por várias vezes no ip 192.168.1.1 o **seu IP será mascarado no caminho** para 192.168.1.58 (falsificado) e o ataque será na porta 80



São **várias requisições SYN** para o servidor.

Ele não tem como responder, pois o **seu endereço IP foi alterado**, então ele fica aguardando, porém não para de **chegar requisições** para ele responder.

# FERRAMENTAS UTILIZADAS PARA FORÇA BRUTA



## Hydra

Resumidamente o **Hydra** descobre **senha** através de Brute Force (tentativa e erro), ele busca em wordlists prováveis usuários/senhas e vai testando as combinações, uma a uma.

O **Hydra** possui suporte aos serviços Telnet, Formulário HTTP/HTTPS, SSH, MySQL, PostgreSQL, MSSQL, SMB, LDAP2 e LDAP3, FTP, SNMP, CVS, VNC, entre outros.

## wordlists

É um arquivo contendo "palavras" ou seja um arquivo.txt contendo possíveis Logins ou Senhas.

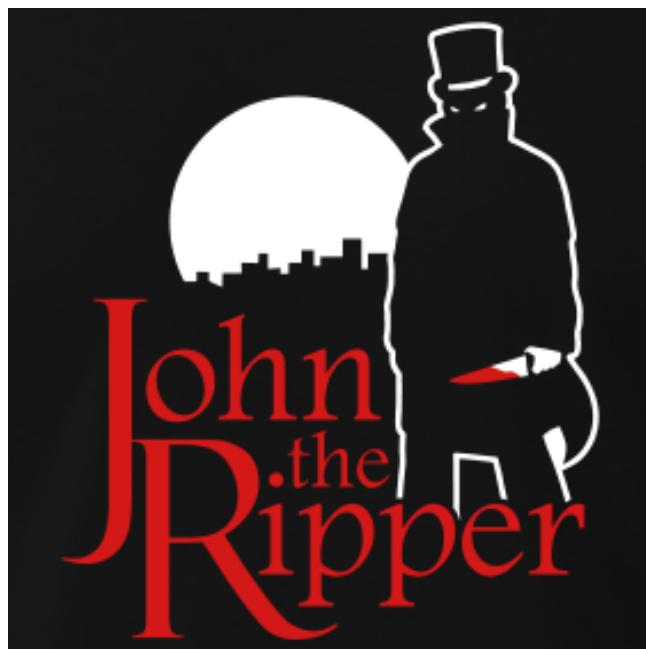
Exemplo: users.txt e senhas.txt



pedro  
joao  
fernando  
mayara  
rh  
admin



105969  
2525  
123456  
00001  
56565  
admin



É um software para quebra de senhas.

John the Ripper é capaz fazer força bruta em senhas cifradas em **DES, MD4 e MD5 entre outras.**

O John possui alguns modos de operação:

- **Dicionário (Wordlist):** sendo o modo mais simples suportado pelo programa, este é o conhecido ataque de dicionário, que lê as palavras de um arquivo e verifica se são correspondentes entre si.
- **Quebra Simples (Single Crack):** mais indicado para início de uma quebra e mais rápido que o wordlist, este modo usa técnicas de mangling e mais informações do usuário pelo nome completo e diretório /home em combinação, para achar a senha mais rapidamente.
- **Incremental:** sendo o modo mais robusto no John the Ripper, ele tentará cada caractere possível até achar a senha correta, e por esse motivo é indicado o uso de parâmetros com o intuito de reduzir o tempo de quebra.
- **Externo (External):** o modo mais complexo do programa que faz a quebra a partir de regras definidas em programação no arquivo de configuração do programa, que irá pré-processar as funções no arquivo no ato da quebra quando usar o programa na linha de comando e executá-las. Este modo é mais completo e necessita de tempo para aprender e acostumar-se.

# wordlists

É um arquivo contendo "palavras" ou seja um arquivo.txt contendo possíveis Logins ou Senhas.

É possível obter wordlists em diversos sites, que disponibilizam para download, essas wordlists possuem possíveis senhas, senhas já vazadas ou que grande parte dos usuários utilizam, como ..

- amor
- 123
- 123456
- 123456789
- Brasil
- senha123



## Sites para wordlists

<https://pastebin.com/>

<http://project-rainbowcrack.com/>

<https://crackstation.net/>



# Medusa

Medusa é programa de **brute-forcer de login rápido**, massivamente paralelo e modular.

O objetivo é oferecer suporte ao maior número possível de serviços que permitem **autenticação remota**.

Para listar os módulos disponíveis  
COMANDO: **#medusa -h**

# FERRAMENTA UTILIZADAS PARA EXPLORAÇÃO DE FALHAS



## Metasploit

É um projeto de segurança que fornece informações **sobre vulnerabilidades de segurança já descobertas**. Por exemplo um serviço apache rodando em um servidor, você pode verificar **se já foi descoberta uma falha para aquela versão** e executa um exploit.

## Exploit

Este é um trecho de código que, quando executado, irá explorar a vulnerabilidade no alvo.

## Payload

Este é um trecho de código executado no destino após uma exploração bem-sucedida. Ele define o tipo de acesso e ações que precisamos obter no sistema de destino.

## FASE 4.1

# ANALISADOR DE PACOTES SNIFFER

É um software ou hardware que **pode interceptar e registrar o tráfego** que passa sobre uma rede ou placa de rede específica.



O sniffer **captura cada pacote** e, se necessário, **decodifica os dados brutos** do pacote, mostrando os valores de vários campos no pacote, e analisa seus conteúdos.

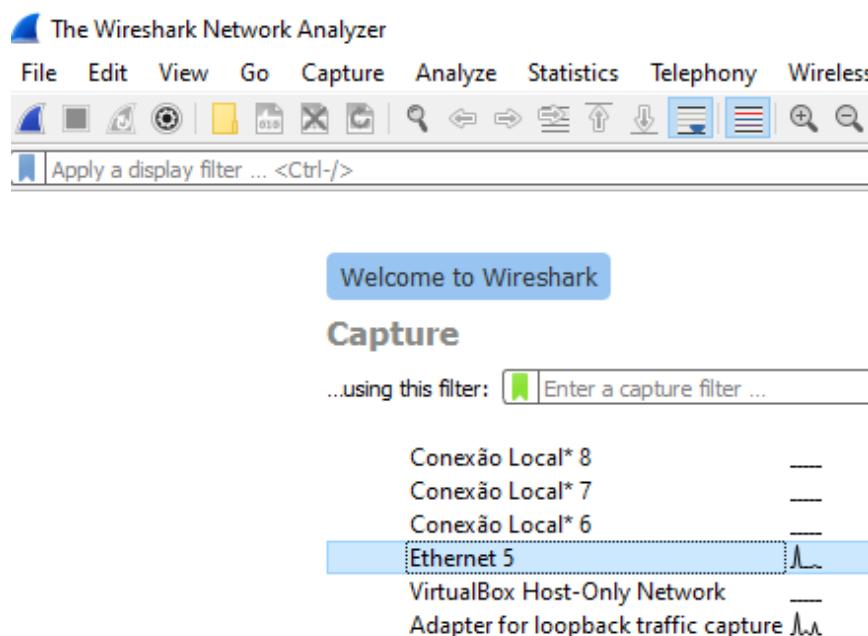
Por exemplo você fica **visualizando os sites que a vítima está acessando**, e sendo possível capturar senhas, quando for efetuado login em algum site.

# FERRAMENTAS UTILIZADAS PARA ANALISAR PACOTES

## WIRESHARK

É um analisador de protocolo de rede mais importante e amplamente usado do mundo.

Ele permite que você **veja o que está acontecendo em sua rede** em um nível microscópico e tem sido padrão de fato em muitas empresas comerciais e agências governamentais.



Escolha **quais das interfaces de redes** de sua máquina/servidor você deseja **monitorar o tráfego**, e ele mostrará tudo, inclusive **quais site estão sendo acessados** em tempo real.

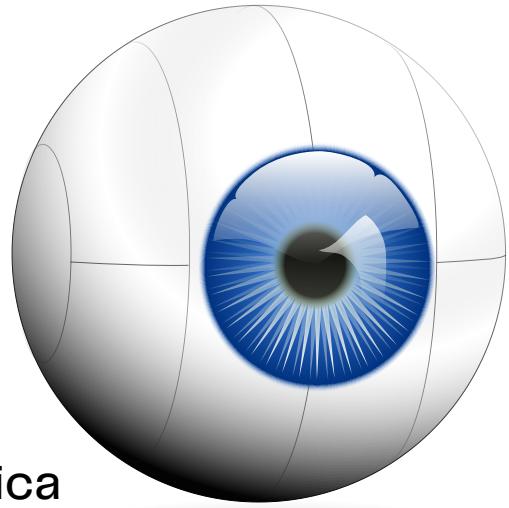
# TCPDUMP

É uma ferramenta de **linha de comando**, também utilizada para **capturar ou filtrar pacotes TCP/IP** que são recebidos ou transferidos por uma rede em uma interface específica.

LisLis

**#tcpdump -D**

Lista interfaces de redes disponíveis



**#tcpdump -i eth0**

Captura os pacotes da **interface eth0**

**#tcpdump -i eth0 port 22**

Captura os pacotes de uma **porta específica**

LisLis

## FASE 5

# REPORT RELATÓRIO FINAL

Um relatório detalhado que **aponte as vulnerabilidades encontradas** na empresa que contratou o hacker, e **as medidas de correções** a serem tomadas, como atualizações a serem feitas, treinamentos de funcionários, configurações, etc.



# RESUMO

## RECONHECIMENTO

- Goole Hacking
- Shodan
- Have I Been Pwned
- Wappalyzer
- Whois
- hunter.io
- fping
- genlist

## VARREDURA

- Nmap
- Nessus

## ENUMERAÇÃO

- Nmap
- NBTscan
- Snmpcheck
- Netcat
- nslookup
- dnsenum
- dnsrecon

## ATAQUE

- hping3
- Hydra
- Wordlists
- John the Ripper
- Medusa
- Metasploit
- Exploit
- Payload
- WireShark
- TCPDUMP

# E AGORA ?

Sua jornada chegou ao fim, agora você já conhece as principais **ferramentas utilizadas pelos HACKERS e as fases de RECONHECIMENTO, VARREDURA, ENUMERAÇÃO, TIPOS DE ATAQUES e SNIFFERs**, também conheceu alguns "termos" que talvez antes eram totalmente desconhecidos.

Existem diversas ferramentas que **podem ser utilizada para o mesmo objetivo**, por exemplo uma furadeira, existem várias marcas e modelos, porém todas **servem para fazer um buraco**.

Claro que existem muitas outras coisas que não foram abordadas nesse material, **porque seria inviável** tentar demonstrar por aqui.

Como mencionado no começo desse material, **a minha intenção aqui foi te apresentar um GUIA** com as principais ferramentas dos HACKERS, espero que esse material tenha te ajudado de alguma forma.

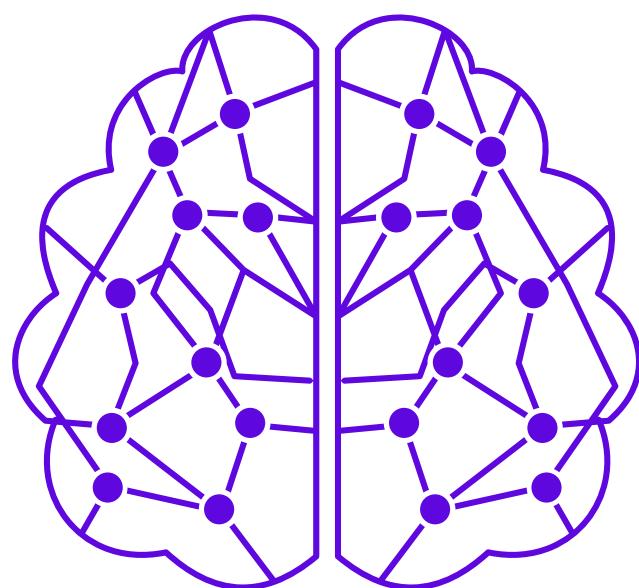
Versão 4.0 em breve.

# NOVA FASE DA SUA VIDA DESBLOQUEANDO SUA MENTE

Só você tem o **PODER de obter novos conhecimentos e evoluir na carreira** e na vida financeira, transformando a sua vida e a de todos em sua volta, é isso que acontece quando você ganha muito mais dinheiro, você tem o poder de dar segurança e conforto para todos que dependem de você.

Garanta agora a sua transformação de vida com o curso **HACKER ÉTICO**.

O CURSO HACKER ÉTICO **sozinho já tem a capacidade de mudar sua vida** profissionalmente, e te trazer grandes oportunidades de ouro, pensa em tudo o que você aprendeu somente nesse GUIA.





# HACKER ÉTICO

## PASSO A PASSO

- ✓ DOMINE O LINUX
- ✓ COMO ENCONTRAR FALHAS
- ✓ HACKEANDO DO ZERO

- ✓ CRIE ROBÔS HACKING
- ✓ ACESSE REDES WI-FI
- ✓ TENHA O PODER DE ATAQUE

**QUERO SABER MAIS !**