

# COMO INVADIR REDES WI-FI UTILIZANDO APENAS 1 COMANDO E 1 VULNERABILIDADE

# Wifi

liberado



**Senha:**  
259637



Senha do  
WIFI



1234567890

# 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.



**QUERO LER AGORA !**



# DISTRO

Criados para atender uma **necessidade específica**, uma distribuição derivada já vem com ferramentas específicas para atender um determinado objetivo.

Por exemplo, **o KALI LINUX já vem com diversas ferramentas hacking**, assim o profissional de cibersegurança não perde tempo instalando essas ferramentas uma a uma. Todo o sistema já vem personalizado e preparado para cumprir as necessidades de um **profissional de cibersegurança**.

Muitas distribuições usam o Debian como base, pois o Debian está consolidado há muito tempo.

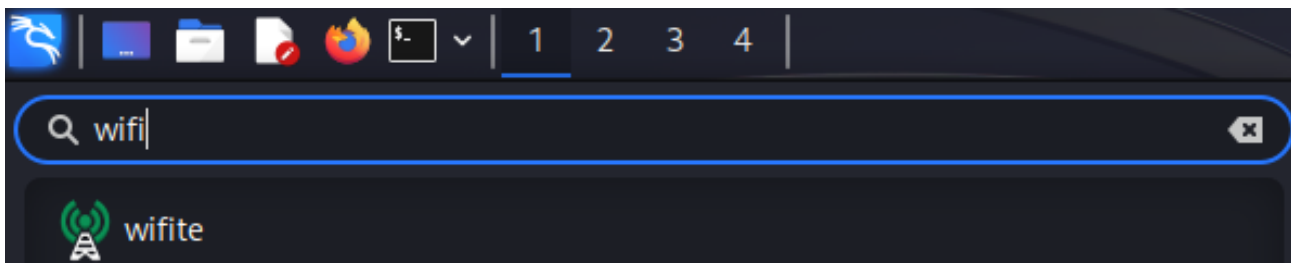


# INVASÃO

O Wifite é uma ferramenta disponível no sistema operacional Kali Linux, que é uma distribuição de Linux especializada em testes de penetração e segurança.

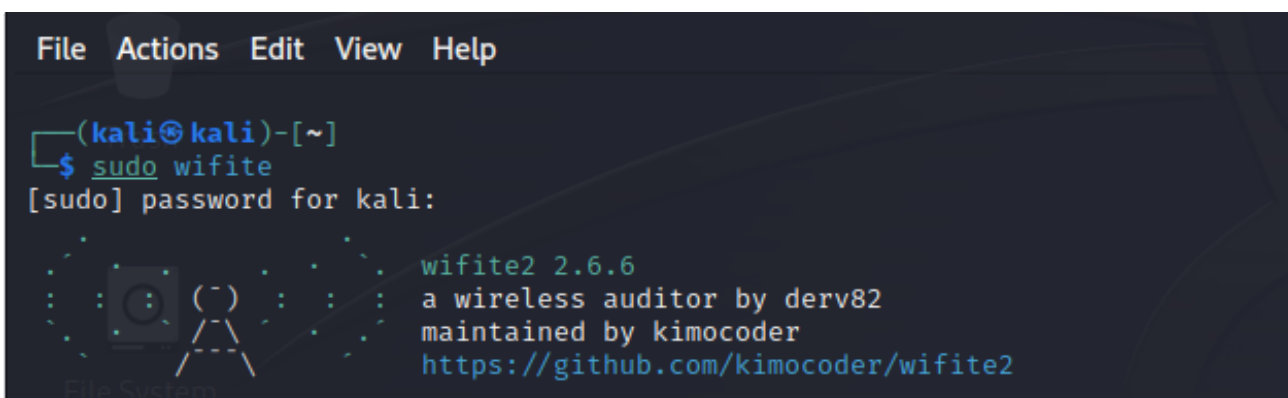
O Wifite é projetado para **automatizar o processo de ataque a redes sem fio**, especificamente redes Wi-Fi protegidas por criptografia WEP, WPA e WPS.

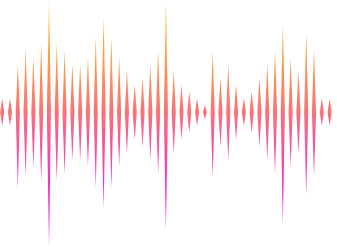
Para abrir o programa basta pesquisar o nome no kali linux e clicar nele, ou digitar o comando no terminal.



## wifite

Digite o comando wifite e o programa irá abrir.

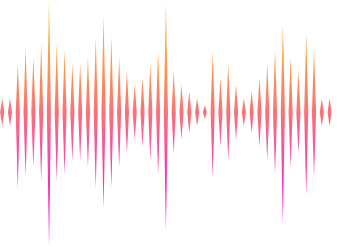




## WIFITE

Essa ferramenta é extremamente poderosa e fácil de ser utilizada, vou te mostrar passo a passo como utilizá-la agora. Mas antes vamos ver alguns pontos importantes sobre ela.

- **Ataques automatizados:** É uma ferramenta de ataque automatizada, o que significa que pode realizar uma série de ações automaticamente, como escanear redes sem fio disponíveis, capturar pacotes de dados, quebrar senhas de redes protegidas e obter acesso à rede.
- **Suporte a múltiplas criptografias:** Suporta a quebra de redes sem fio protegidas por várias criptografias, incluindo WEP (Wired Equivalent Privacy), WPA (Wi-Fi Protected Access) e WPS (Wi-Fi Protected Setup).
- **Interface de linha de comando:** É executado na linha de comando do terminal do Kali Linux, o que significa que é uma ferramenta de linha de comando e não possui uma interface gráfica de usuário. Isso pode exigir um conhecimento básico de comandos de terminal do Linux para usá-lo efetivamente.



- **Personalização de ataques:** O Wifite permite personalizar o tipo de ataque que você deseja executar em uma rede sem fio. Por exemplo, você pode especificar o tipo de criptografia que deseja atacar, o tempo máximo de execução do ataque, o número máximo de tentativas de senha, entre outras opções.
- **Uso ético:** É importante ressaltar que o uso do Wifite ou de qualquer outra ferramenta de teste de penetração em redes sem fio deve ser realizado de forma ética e legal, com permissão explícita do proprietário da rede. O uso não autorizado de ferramentas de hacking é ilegal e pode resultar em consequências legais graves.

É fundamental ter conhecimentos e compreensão adequada sobre as leis locais, ética e responsabilidade antes de usar o Wifite ou qualquer outra ferramenta de teste de penetração em redes sem fio. Sempre obtenha permissão por escrito do proprietário da rede antes de realizar qualquer teste de penetração ou atividade de hacking.

## # wifite

### \$ sudo 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 hcxpcapngtool
[!] Conflicting processes: NetworkManager (PID 1244), wpa_supplicant (PID 1283)
[!] If you have problems: kill -9 PID or re-run wifite with --kill

Interface  PHY  Driver  Chipset
-----
1. wlan0    phy0  rtl818x_pci  Realtek Semiconductor Co., Ltd. RTL8187SE (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  1
3    VIRUS_2G  13  WPA-P  17db  yes
```

**CTRL + C**

Para o comando parar.

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.**

```
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.**





# E AGORA ?

Espero que você tenha aprendido a utilizar essa ferramenta, tentei ir direto ao ponto sem muita enrolação, para que você já coloque a mão na massa.

É possível que o seu adaptador, placa ou notebook **não tenha suporte ao modo monitor, esse modo é 'obrigatório'** para que você possa monitorar as redes WI-FI que estão ao seu alcance.

No **COMBO de E-books Linux e Hacking** eu mostro passo a passo como dominar o Linux de forma super rápida através de gráficos incríveis **mesmo que você utilize Windows**.

Você também vai descobrir diversas ferramentas utilizadas por hackers do mundo todo e como utilizá-las, **e terá acesso ao e-book completo "Monitoramento e invasão de redes WI-FI"** onde você será capaz de entender os tipos de antenas, ver se o adaptador possui o modo monitoramento e fazer ataques manualmente.

**GARANTA AGORA SUPER PROMOÇÃO DO COMBO DE E-BOOKS LINUX E HACKING.**



**QUERO LER AGORA !**



# ALGUMAS PÁGINAS



## ARQUITETURA DO LINUX



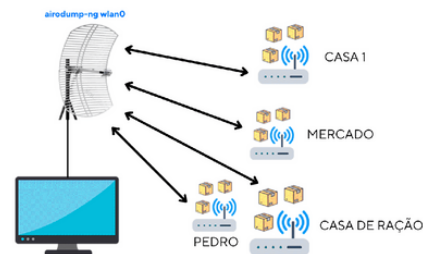
14



## 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 isso você precisa **ativar o MODO monitoramento** da sua interface de rede Wi-Fi.

# airmo-ng check [Para ver processos em execução que podem entrar em algum conflito]  
# airmo-ng check kill



19

## FERRAMENTAS UTILIZADAS PARA FORÇA BRUTA

28



### 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



padro  
joao  
fernando  
maysara  
rh  
admin



105969  
2525  
123456  
00001  
56565  
admin

### DERIVADOS

Criados para atender uma **necessidade específica**, uma distribuição derivada já vem com ferramentas específicas para atender um determinado objetivo.

Por exemplo, o **KALI LINUX** já vem com diversas ferramentas hacking, assim o profissional de cibersegurança não perde tempo instalando essas ferramentas uma a uma. Todo o sistema já vem personalizado e preparado para cumprir as necessidades de um **profissional de cibersegurança**.

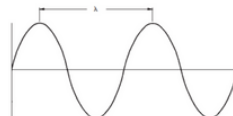
Muitas distribuições usam o Debian como base, pois o Debian está consolidado há muito tempo.



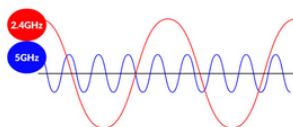
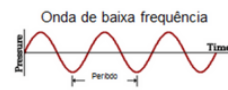
16



### Comprimento de onda



### Frequência



13

## FASES QUE O HACKER PERCORRE

3

### COLETA DE INFORMAÇÕES

PÚBLICAS e SIGILOSAS

### MAPEAMENTO DA REDE/VARREDURA

Descobrir 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, parando e volta...

### EVIDÊNCIAS E REPORTE



8

**QUERO LER AGORA !**