



Universidade do Minho

UNIVERSIDADE DO MINHO
MESTRADO EM CIBERSEGURANÇA
2025/2026

TCP/IP Attack Lab

PG59783 - Carlos Daniel Silva Fernandes - Mestrado em Cibersegurança
PG59790 - Luís Filipe Pinheiro Silva - Mestrado em Cibersegurança
PG59791 - Pedro Augusto Ennes de Martino Camargo - Mestrado em
Cibersegurança

Ao longo do trabalho prático **TCP/IP Attack Lab** foram desenvolvidos e executados vários scripts que implementam as técnicas e os testes propostos no guião. Cada script encontra-se devidamente identificado.

Questão 1.1

Após reduzirmos significativamente o tamanho da fila de conexões pendentes (**backlog queue**) e aumentarmos o número de retransmissões de pacotes SYN que o TCP efetua durante o processo de estabelecimento da ligação, conseguimos executar com sucesso o ataque de **DoS**.

```
root@ec0753a4fa82:/# telnet 10.9.0.5 -l seed
Trying 10.9.0.5...
```

Figura 1: Tentar entrar no container da vítima

Questão 1.2

Ao implementar este tipo de ataque em C, constatamos que a queue enche mais rapidamente. Devido ao desempenho superior do C em relação ao Python, o código consegue gerar um número de pacotes por unidade de tempo mais elevado, o que torna mais fácil saturar os recursos da vítima.

```
root@c69f75d8a7d6:/# ss -n state syn-recv sport = :23 | wc -l
130
```

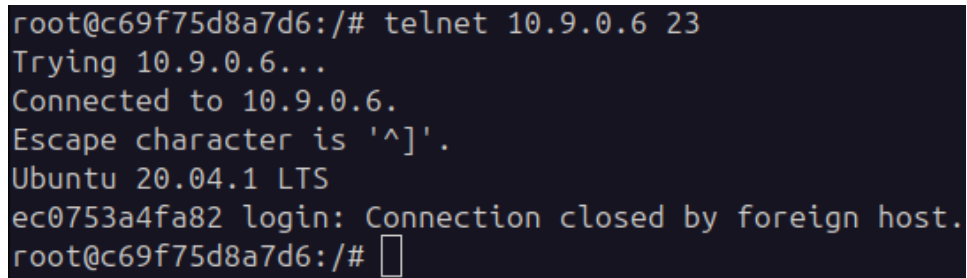
Figura 2: Espaço usado na queue da vítima

Questão 1.3

Ao ativar a opção `net.ipv4.tcp_syncookies=1`, o kernel passa a utilizar **SYN cookies**, criando a conexão apenas após receber um **ACK** válido. Desta forma, evita-se o esgotamento da fila de **backlog**, o que impede que ataques do tipo **SYN Flooding** sejam eficazes.

Questão 2

Para realizar o ataque **TCP RST**, começámos por fazer sniffing do tráfego da máquina 10.9.0.5. Sempre que detetamos um pacote TCP dirigido à porta 23 com origem em 10.9.0.5, enviávamos um pacote para encerrar a ligação. O resultado pode ser visto na imagem seguinte.

A terminal window with a dark background and light-colored text. The text shows a telnet session attempt. The prompt is root@c69f75d8a7d6:/. The user enters telnet 10.9.0.6 23. The output shows 'Trying 10.9.0.6...', 'Connected to 10.9.0.6.', 'Escape character is '^]'.', 'Ubuntu 20.04.1 LTS', and 'ec0753a4fa82 login: Connection closed by foreign host.' followed by the root prompt again with a cursor.

```
root@c69f75d8a7d6:/# telnet 10.9.0.6 23
Trying 10.9.0.6...
Connected to 10.9.0.6.
Escape character is '^]'.
Ubuntu 20.04.1 LTS
ec0753a4fa82 login: Connection closed by foreign host.
root@c69f75d8a7d6:/#
```

Figura 3: Conexão falhada