**Configuração:**

**PC REAL: IP: 192.168.56.1**

Para rodar o llama, entrar no diretório:

C:\Users\pedro\AppData\Local\Programs\Ollama  
ollama app.exe

Ollama run llama3

Computador real usando Windows, rodando llama no endereço padrão: <http://127.0.0.1:11434/api/generate>

**Vm Servidor: Nome da VM: Servidor – TCC**

Configurações de rede:

1. Interface em NAT para instalação das dependências.
2. Também em Host Only

Softwares utilizados e configurações:

1. **Tshark** para a captura dos pacotes usando o comando:   
    **sudo tshark -i enp0s8 -w teste.pcap**

Está capturando os pacotes e jogando no endereço /home/tcc

1. **Apache** instalado e rodando na porta 80

**sudo systemctl status apache2**

1. **Python** instalado para ler o conteúdo desse arquivo pcap e processar para que o llama possa entender.
2. **Insomnia** instalado para testar conexão com o pc real.
3. **Ngrok** para fazer conexão com o PC real... não estava conseguindo fazer posts para o pc real, mesmo com o firewall do Windows desativado. ( Solução temporária )

**IP: 192.168.56.3**

**VM Atacante: Nome da VM: Atacante - TCC**

Configurações de rede:

1. Interface em NAT para instalação das dependências.
2. Em modo Host Only para que as vms se conversem e também converse com o Windows, que é o host das vms.

Softwares utilizados e configurações:

1. **Ettercap** para simular o ataque DoS
2. **GoldenEye**

Os **agentes** no GoldenEye são **processos que simulam múltimos usuários atacando o servidor ao mesmo tempo**.  
Cada agente age como se fosse um navegador diferente, enviando múltiplas requisições HTTP.

**GoldenEye sozinho NÃO muda o IP** → ele apenas usa múltiplas conexões (threads).

**"Agentes" são os processos que simulam acessos simultâneos**.

Para **simular múltiplos IPs**, combine com **proxies, Tor ou rode em várias máquinas**.

**Para instalar:**

git clone <https://github.com/jseidl/GoldenEye.git>

cd GoldenEye

chmod +x goldeneye.py

sudo apt update && sudo apt install python3

**Para usar:**

**python3 goldeneye.py http://alvo.com -w 50 -s 100**

1. **Torshammer**

sudo apt install python2

git clone <https://github.com/dotfighter/torshammer.git>

cd torshammer

python2 torshammer.py -t 192.168.56.3 -r 10

IP: **192.168.56.2**

**Medir consumo de memória e processamento:**

**Para cada vez medir o tempo de detecção**

**Testar 20 a 30 rodadas para usar intervalo de confiança, testando cada ferramenta de ataque (Pro llama)**

**Ettercap**

**Golden Eye**

**Torshammer**