#### Segurança em Redes de Computadores

##### **TP5 – Práticas com firewalls (IPTables)**

##### MESTRADO INTEGRADO EM ENGenharia de Telecomunicações e informática

**Grupo 4:**

70020 – José Pedro Afonso Rocha

73232 – Luís Pedro Lobo de Araújo

Índice

[Introdução 3](#_Toc8407689)

[Conceitos Teóricos 4](#_Toc8407690)

[Parte Prática 5](#_Toc8407691)

[Tarefa 1 5](#_Toc8407692)

[Tarefa 2 8](#_Toc8407693)

[Tarefa 3 11](#_Toc8407694)

[Exercício Final 15](#_Toc8407695)

[Conclusão 18](#_Toc8407696)

# Introdução

No âmbito da Unidade Curricular de Segurança em Redes de Computadores foi-nos proposto configurar uma máquina virtual de modo a ter um funcionamento tipo servidor e outra como cliente.

Através do uso das funcionalidades do Kernel do Linux, que tem a capacidade de processar e filtrar todo o tráfego que passa na pilha de protocolos seremos capazes de instaurar numa firewall nova regras e políticas de conexão entre um cliente e servidor.

Para o sucesso deste projeto será preciso cumprir vários passos distribuídos por 3 tarefas que irão também servir de guia para a aprendizagem de vários comandos essenciais para o que é pretendido.

Também nos foi proposto realizar um exercício final em que é pretendido que se instale uma interface gráfica para configurar uma ferramenta muito importante que irá ser utilizada e uma peça central ao longo deste trabalho.

# Conceitos Teóricos

**Firewall:** Uma firewall é um dispositivo de segurança de uma rede que permite monitorizar pedidos e respostas no tráfego da rede e decide se deve permitir ou bloquear tráfego específico baseando-se em regras já definidas.

**Kernel:** É o componente central de um sistema operativo e que serve de ponte entre aplicativos e o processamento de dados feitos a nível de hardware através de mecanismos de comunicação entre processos e chamadas ao sistema.

**iptables:** Um programa que permite ao administrador de um sistema configurar as tabelas disponibilizadas pela firewall do kernel do Linux que contêm as regras e permissões de várias ligações.

**FTP (File Transfer Protocol):** O FTP é um protocolo de transferência de dados entre um cliente e servidor.

**HTTP (Hypertext Transfer Protocol):** O HTTP é um protocolo de transferência ou troca de hipertexto utilizado para sistemas de informação , distribuídos e colaborativos.

**SSH (Secure Shell):** O SSH é um protocolo de rede criptográfico que fornece um canal seguro a uma rede insegura com uma arquitetura cliente-servidor fazendo a conexão entre uma aplicação cliente SSH e uma aplicação servidor SSH que emula uma conexão de uma linha de comandos remota.

# Parte Prática

## Tarefa 1

Nesta primeira tarefa pretende-se instalar o serviço FTP, ativar e iniciar os serviços “httpd”, “sshd” e “vsftpd”, configurar a firewall da máquina virtual e verificar o resultado obtido através de comandos específicos demonstrados a seguir:

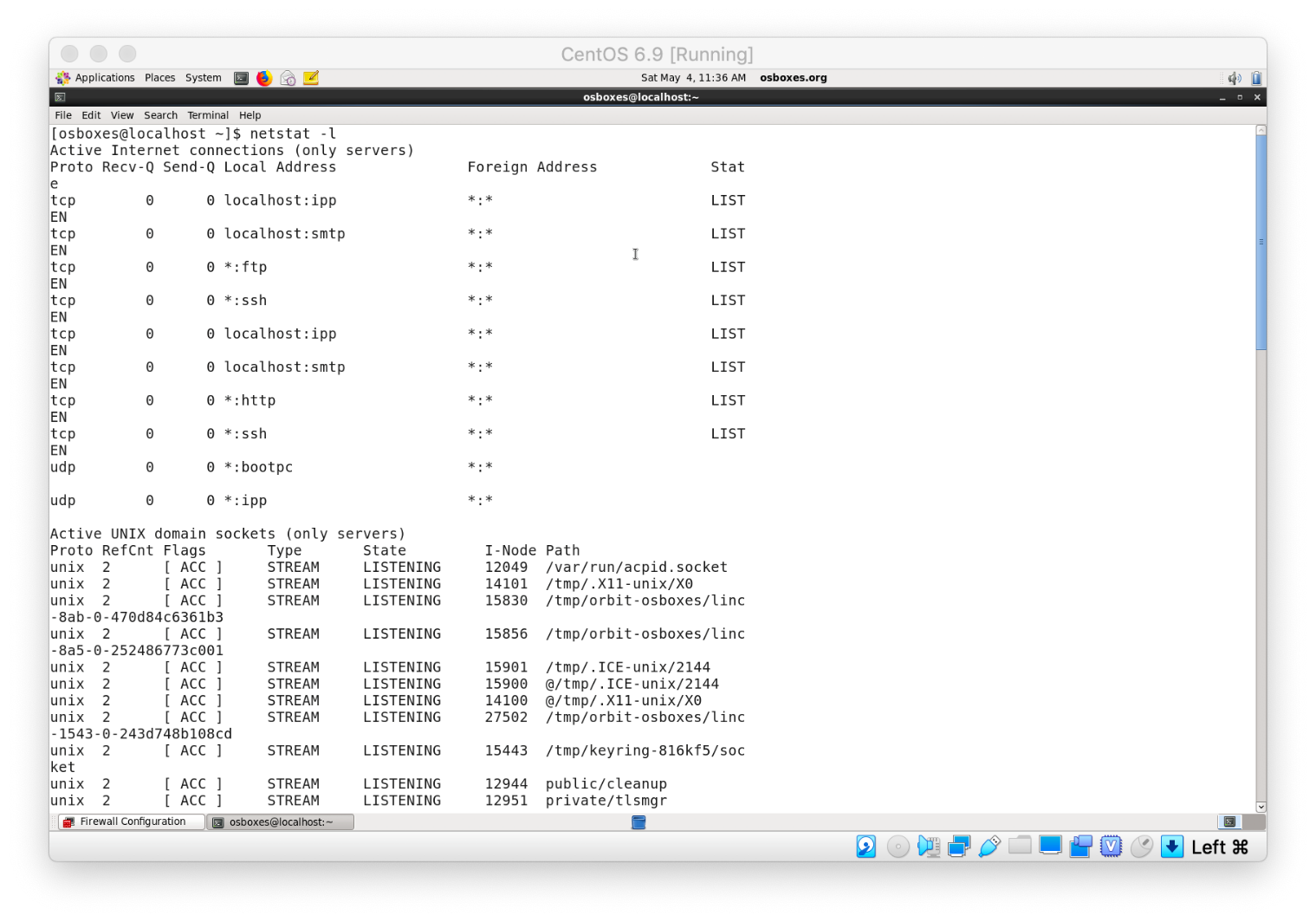


Figura - verificação dos serviços preparados.

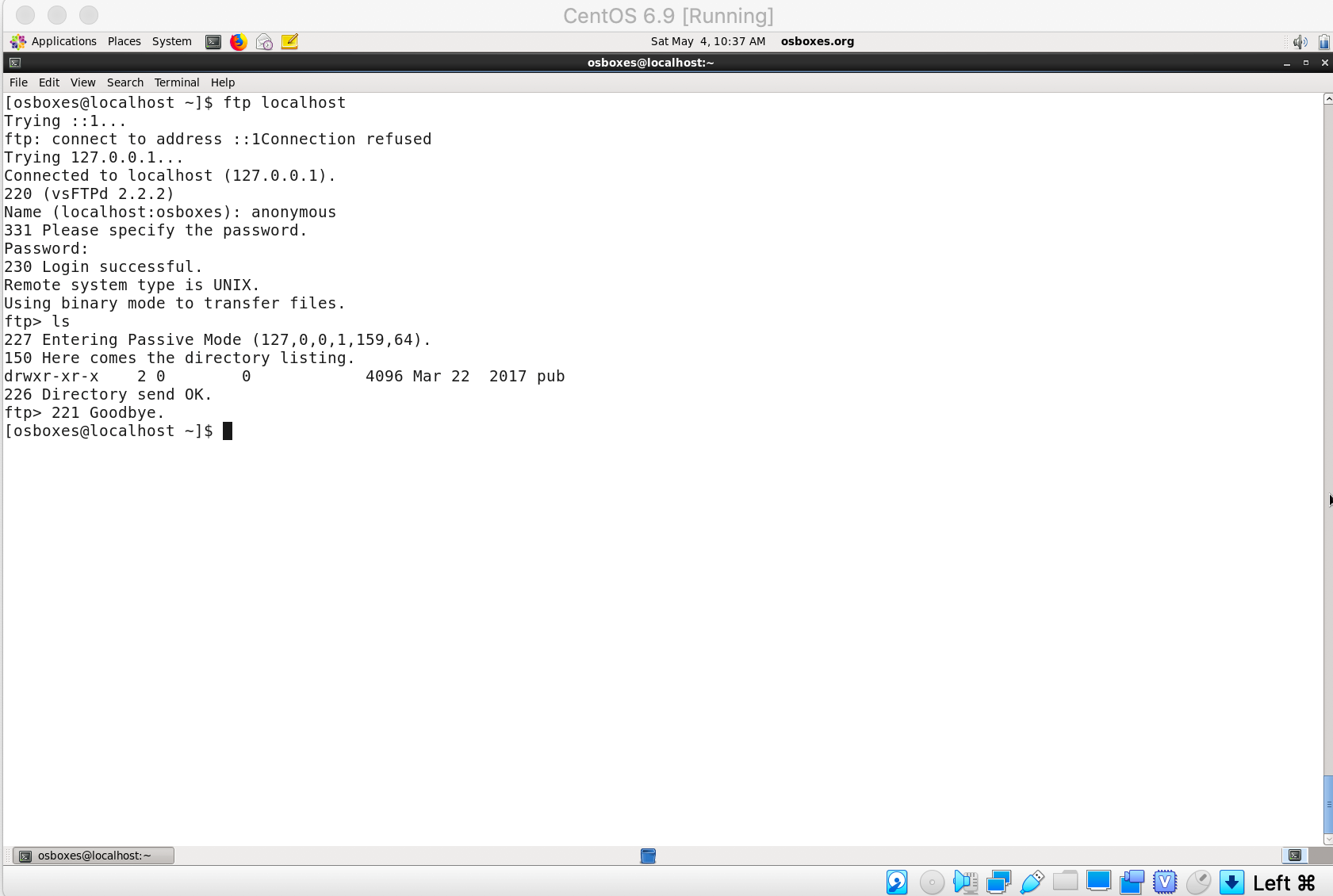


Figura - conexão ao serviço FTP.

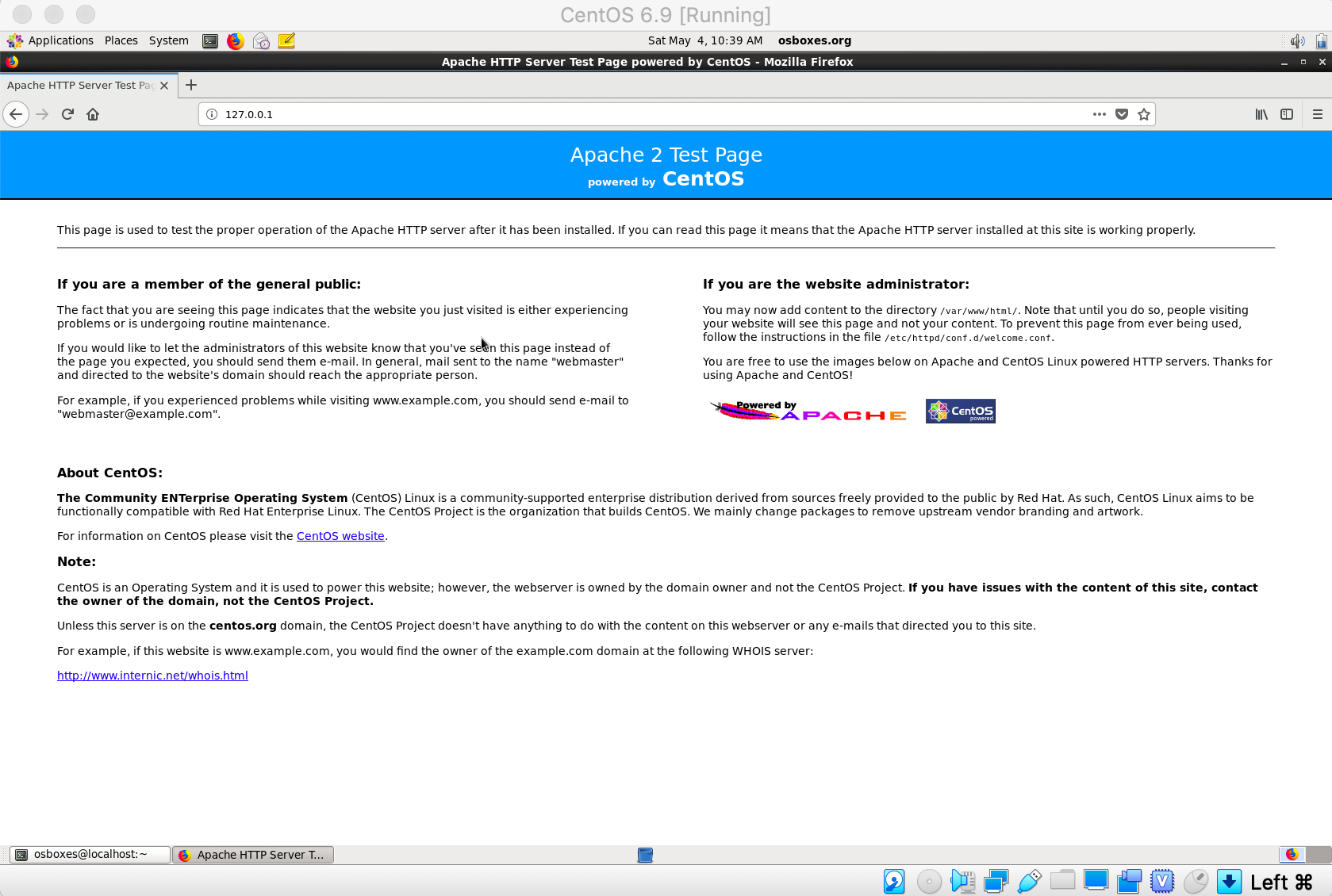


Figura – Conexão ao serviço http.

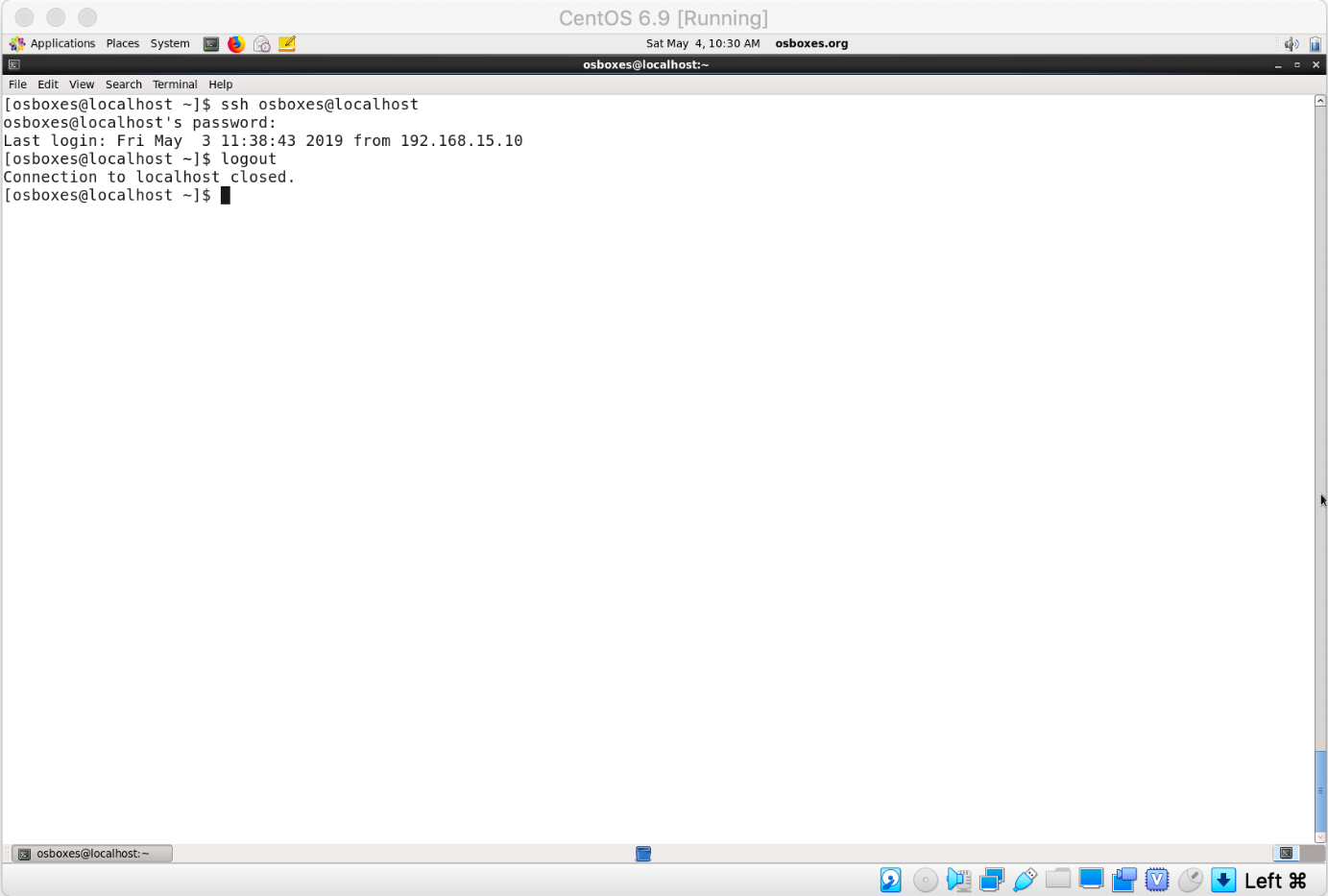


Figura – Conexão ao serviço ssh.

Uma imagem com captura de ecrã

Descrição gerada automaticamente

Figura - Ativação da firewall.

Uma imagem com captura de ecrã

Descrição gerada automaticamente

Figura – Estado de iptables após ativar Firewall.

Na Figura 6, é possível visualizar todas as regras em cadeia presentes nas iptables e verifica-se que para a cadeia INPUT as políticas implementadas por defeito são a permissão de todas as ligações com todos os protocolos, para a cadeia FORWARD são rejeitadas todas as ligações e para a cadeia OUTPUT não existe nenhuma política implementada por defeito.

Com as regras implementadas por defeito apenas é possível aceder à porta SSH.

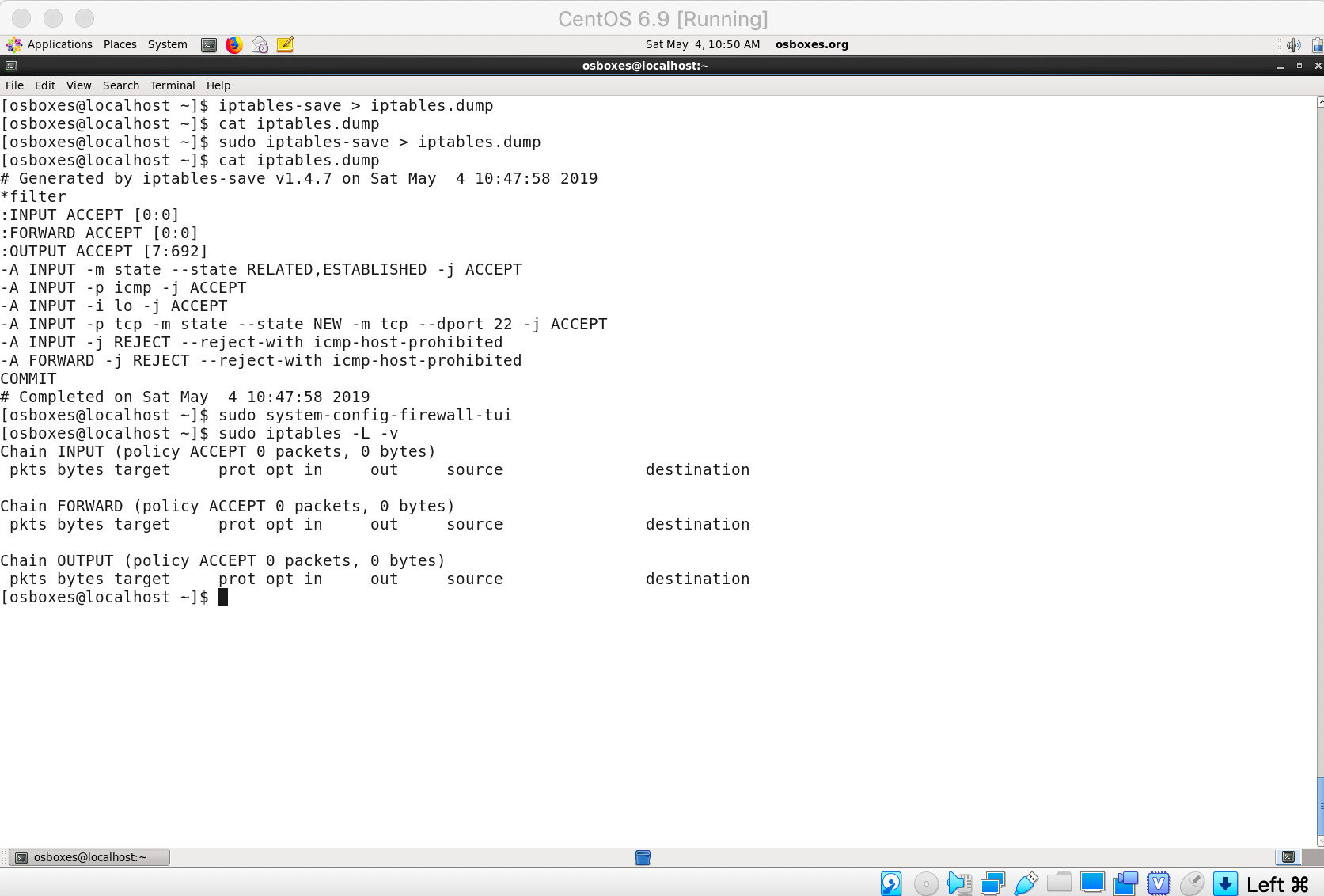


Figura - guardar as iptables num ficheiro e desativação de firewall

Na figura 7 verifica-se que ao desativar a firewall todas as regras em cadeia são removidas, logo o sistema torna-se inseguro e aberto para qualquer tipo de ligação, desejada ou indesejada.

## Tarefa 2

Esta segunda tarefa serve para verificar a conetividade da máquina virtual configurada ao servidor inicializado através dos seguintes comandos abaixo representados:

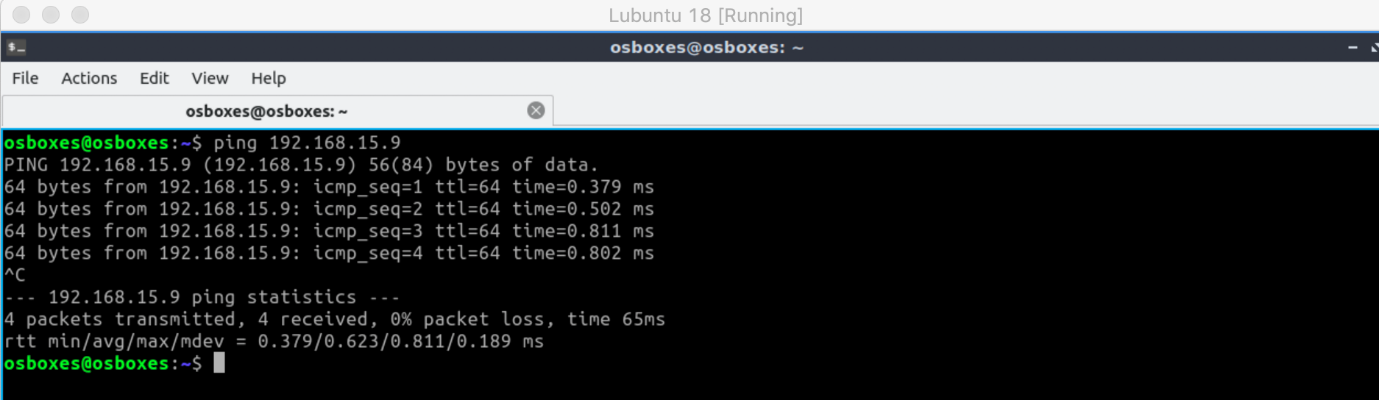


Figura - verificação de conetividade via ping.

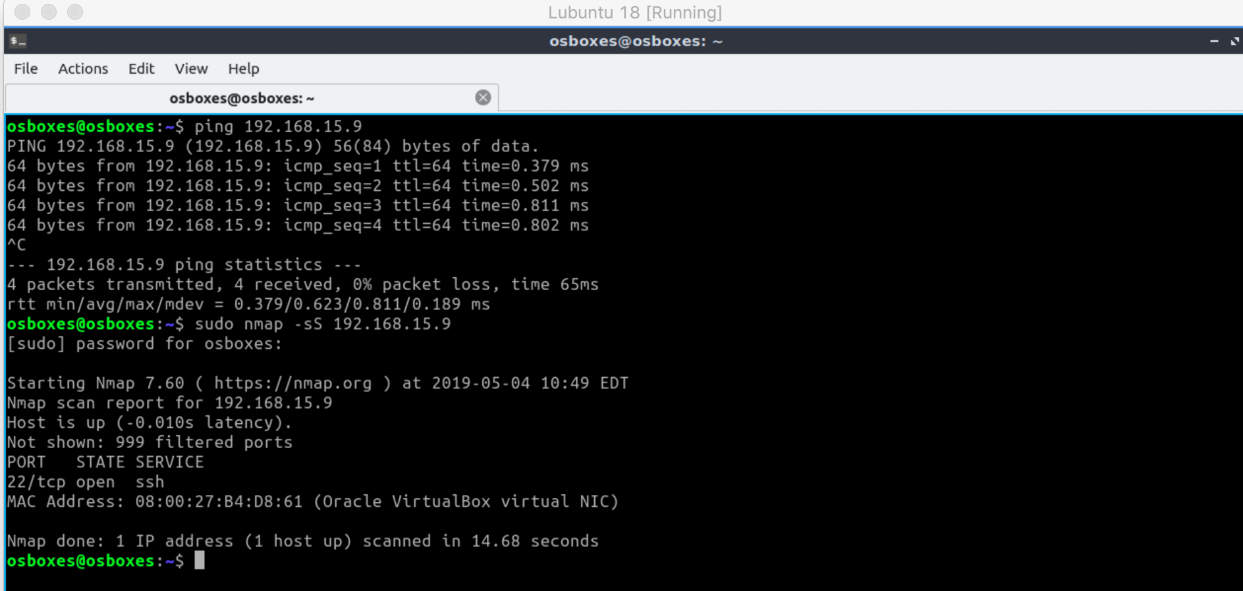


Figura - execução do comando nmap

A figura acima mostra a execução do comando “nmap” que nos fornece informação do host que se pretende analisar, informa-nos da disponibilidade do host , do número de portas filtradas, das portas disponíveis e do estado e do serviço das mesmas.

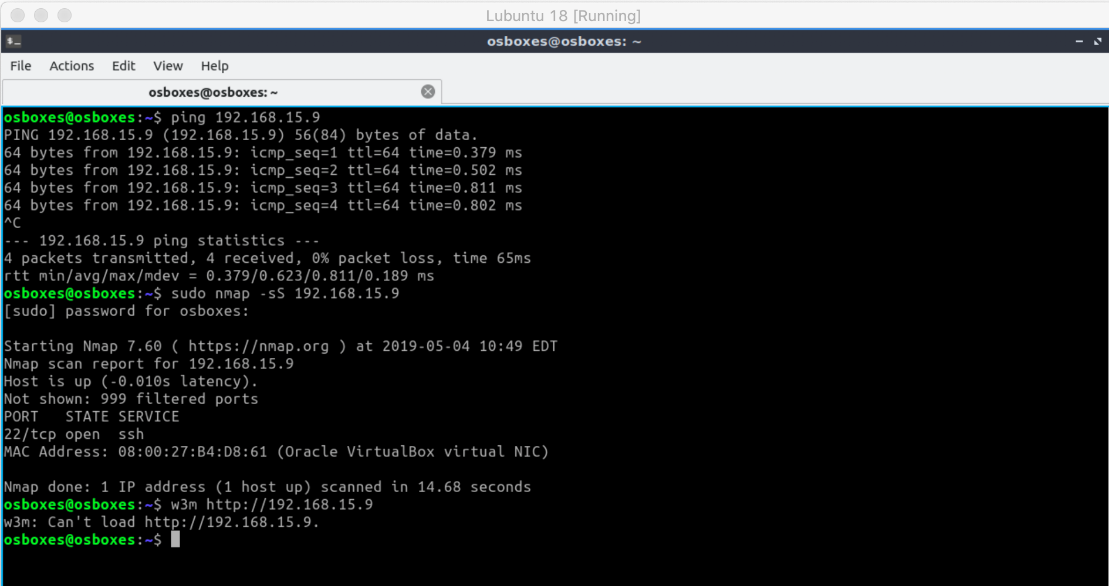


Figura - execução do comando w3m

Na figura acima podemos verificar que não é possível aceder ao servidor http.

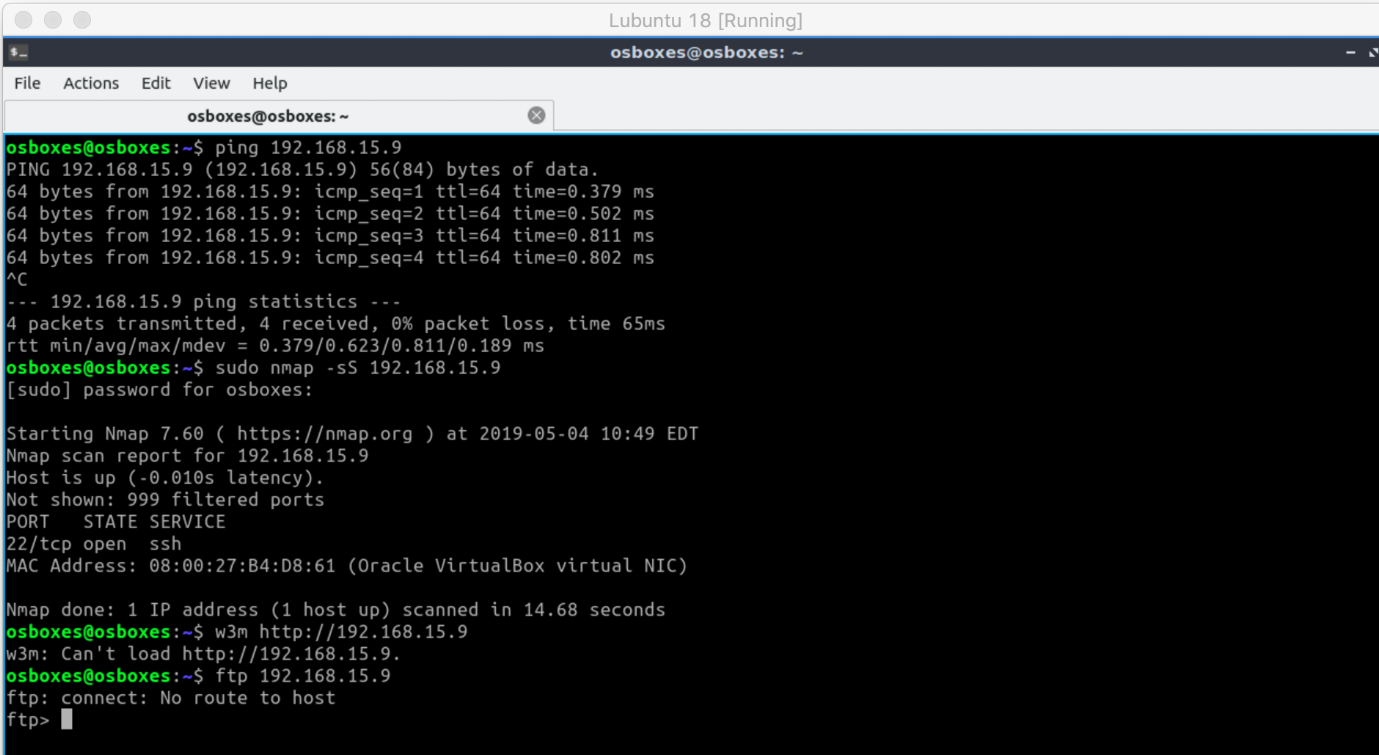


Figura - Execução do comando ftp

Também para o FTP, o cliente não tem acesso à porta FTP, como podemos ver na figura acima.

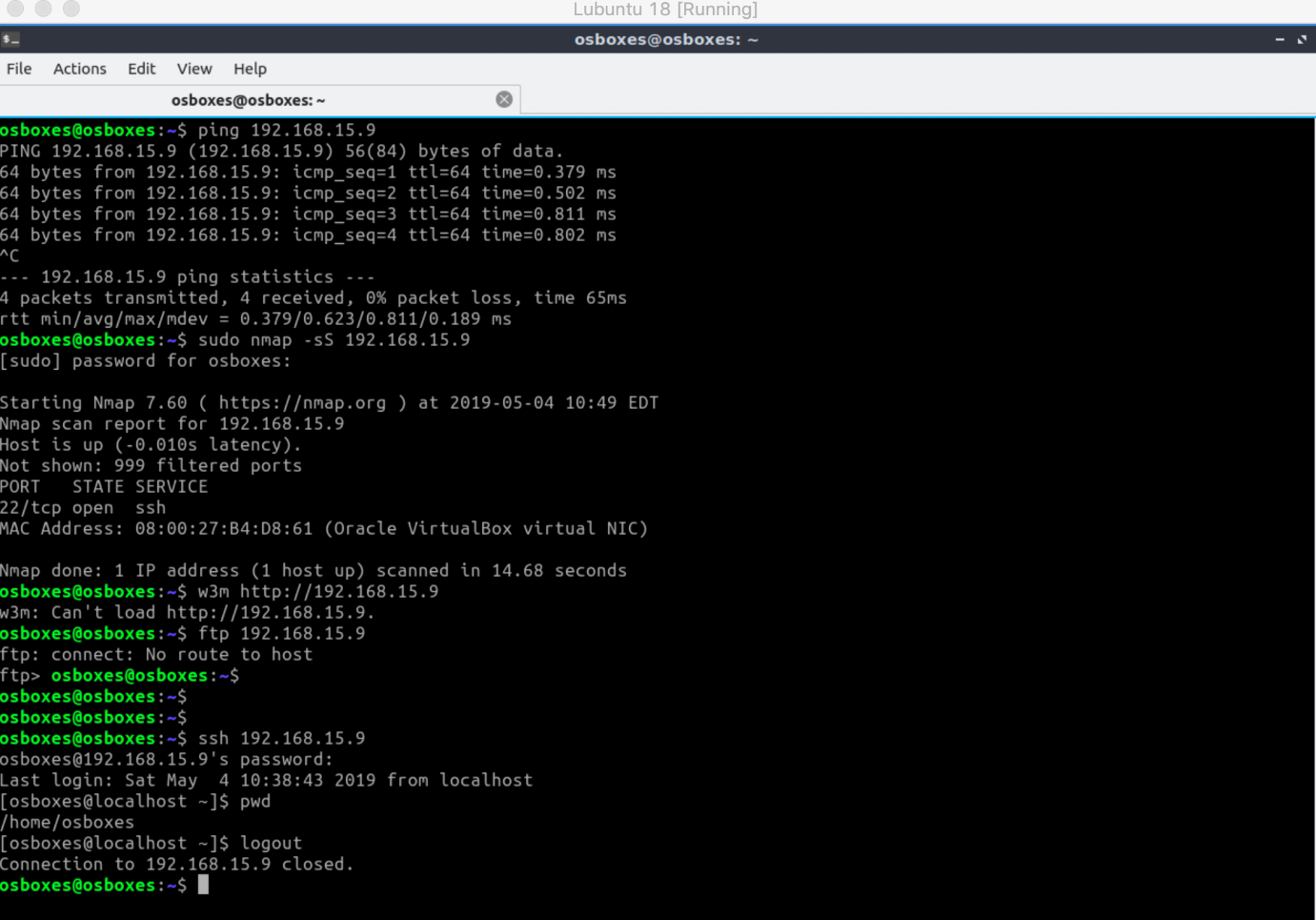


Figura - Execução do comando ssh

Como podemos verificar na figura acima, com a configuração por defeito apenas é possível aceder ao servidor de SSH, e todas as outras portas estão inacessíveis.

## Tarefa 3

Nesta terceira e última tarefa pretende-se que os serviços FTP, SSH e HTTP(WWW) estejam acessíveis aos clientes, abrindo portas para as interfaces de rede que se irão conectar e que terão acesso completo, ativar a função port forwarding e um filtro para o protocolo ICMP.

Para o sucesso desta tarefa foram executados os seguintes comandos:

Uma imagem com captura de ecrã

Descrição gerada automaticamente

Figura - Filtro icmp: Ativação do filtro echo requestUma imagem com captura de ecrã

Descrição gerada automaticamente

Figura - ativar servico www (http), FTP e SSH.

Uma imagem com captura de ecrã

Descrição gerada automaticamente

Figura - iptables alteradas no servidor com acesso SSH, HTTP e FTP.

A figura acima mostra o resultado da escolha da opção FORWARD no processo de configuração da firewall, onde se colocou também os serviços FTP, SSH e WWW acessíveis e estes passos fizeram com com que seja acrescentada à cadeia INPUT quatro novas políticas, uma para cada serviço agora acessível e a política existente na cadeia FORWARD.

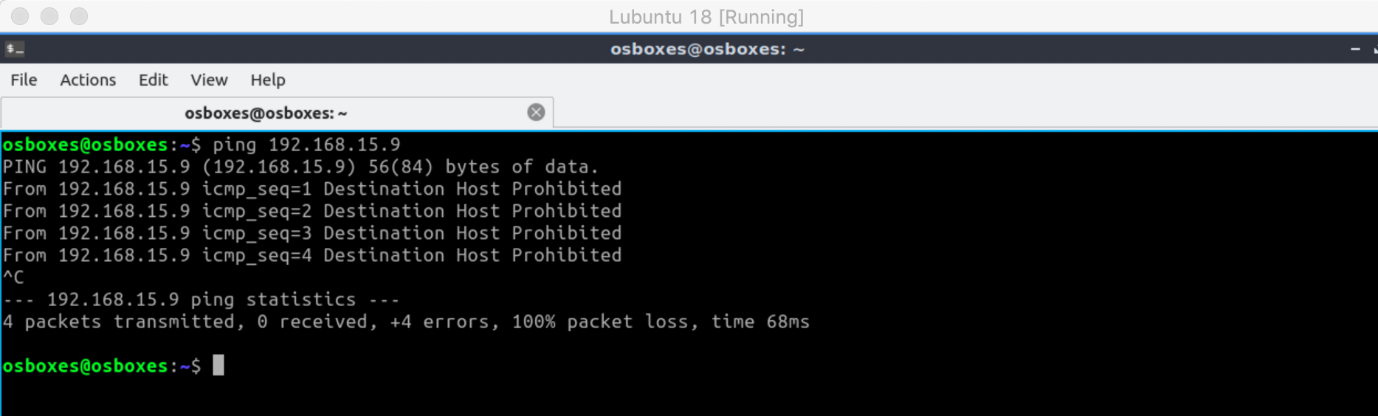


Figura - Comando ping no cliente.

Como podemos verificar na figura acima, as alterações realizadas na Firewall do servidor surtiram efeito e os pacotes de ping são rejeitados. No lado do cliente foi utilizado o sistema operativo Lubuntu 18.

Uma imagem com captura de ecrã

Descrição gerada automaticamente

Figura - Comando w3m: Página visualizada.

Uma imagem com captura de ecrã, monitor

Descrição gerada automaticamente

Figura - Comando ftp: ligação com utilizador "anonymous".

Nas figuras 17 e 18, podemos ver que já é possível aceder aos servidores FTP e HTTP, uma vez alteradas as regras da Firewall no servidor.

Uma imagem com captura de ecrã

Descrição gerada automaticamente

Figura - comando nmap: estado das portas dos serviços ativos.

Na imagem acima conseguimos demonstrar que foram abertas 3 portas de protocolo TCP/IP, uma para cada seu respetivo serviço, neste caso, para os serviços FTP, SSH e HTTP.

Uma imagem com captura de ecrã

Descrição gerada automaticamente

Figura - iptables do servidor

## Exercício Final

Para a realização do exercício final, o grupo necessitou de instalar o software Firewall Builder, que permite alterar as regras da firewall (via iptables) através de uma interface gráfica.

Para obter as alterações realizadas anteriormente o grupo guardou o estado das regras via iptables-save. De seguida foram carregadas para o Firewall Builder como podemos verificar na imagem seguinte:

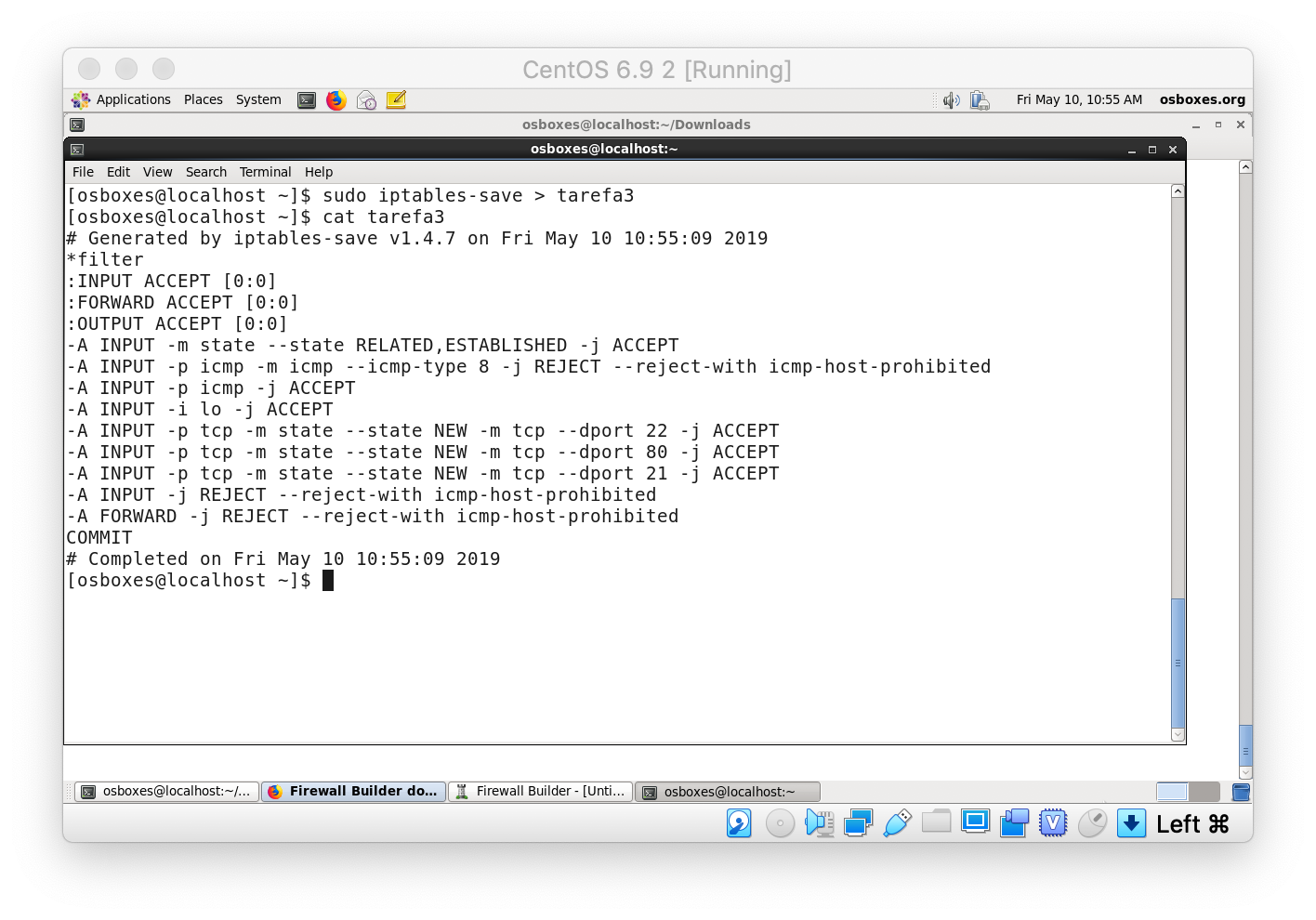


Figura - iptables-save.

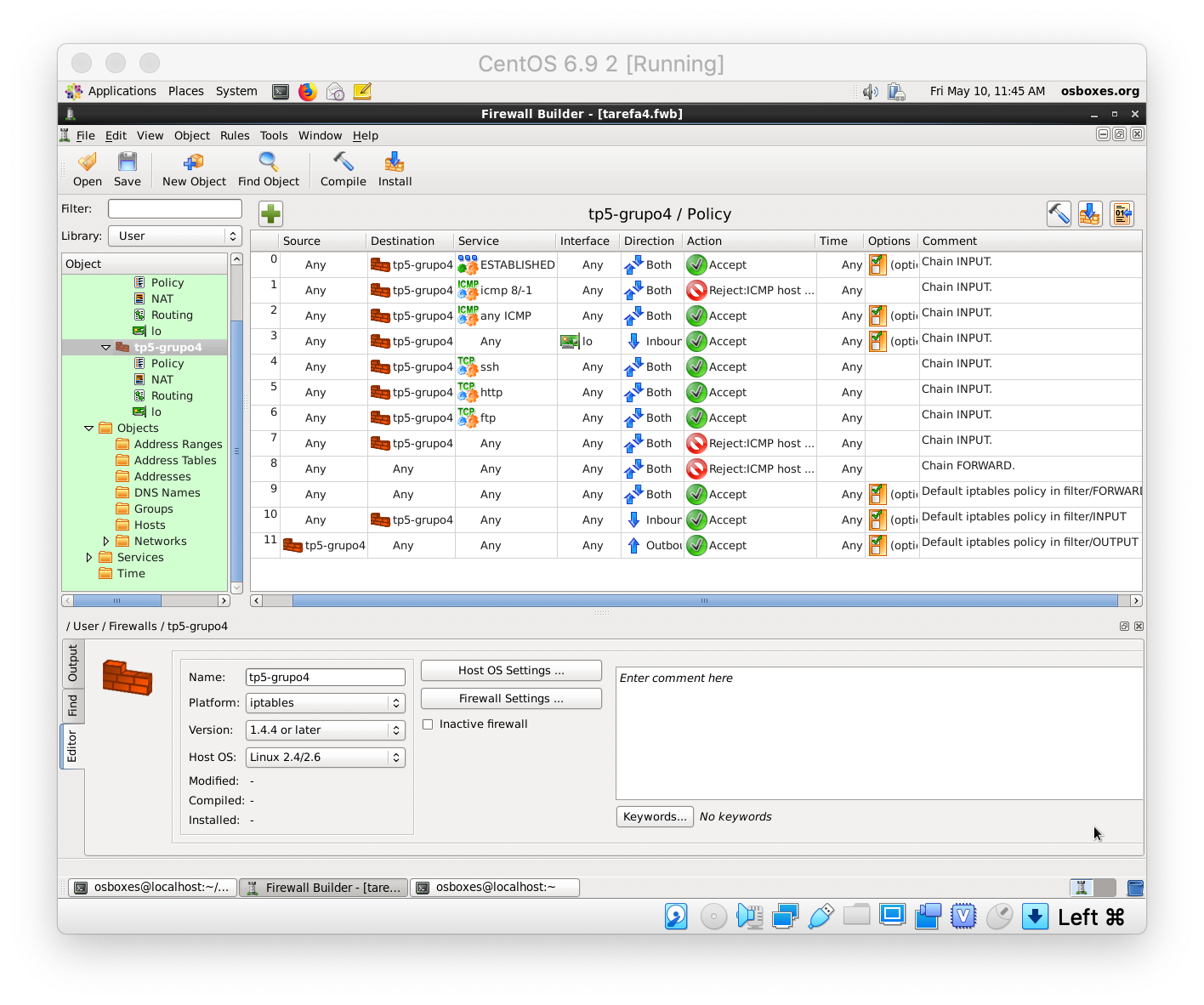


Figura - Regras importadas do iptables-save.

De seguida foram alteradas as regras de forma a limitar o acesso apenas a endereços locais, e ativados os logs para as diferentes regras.

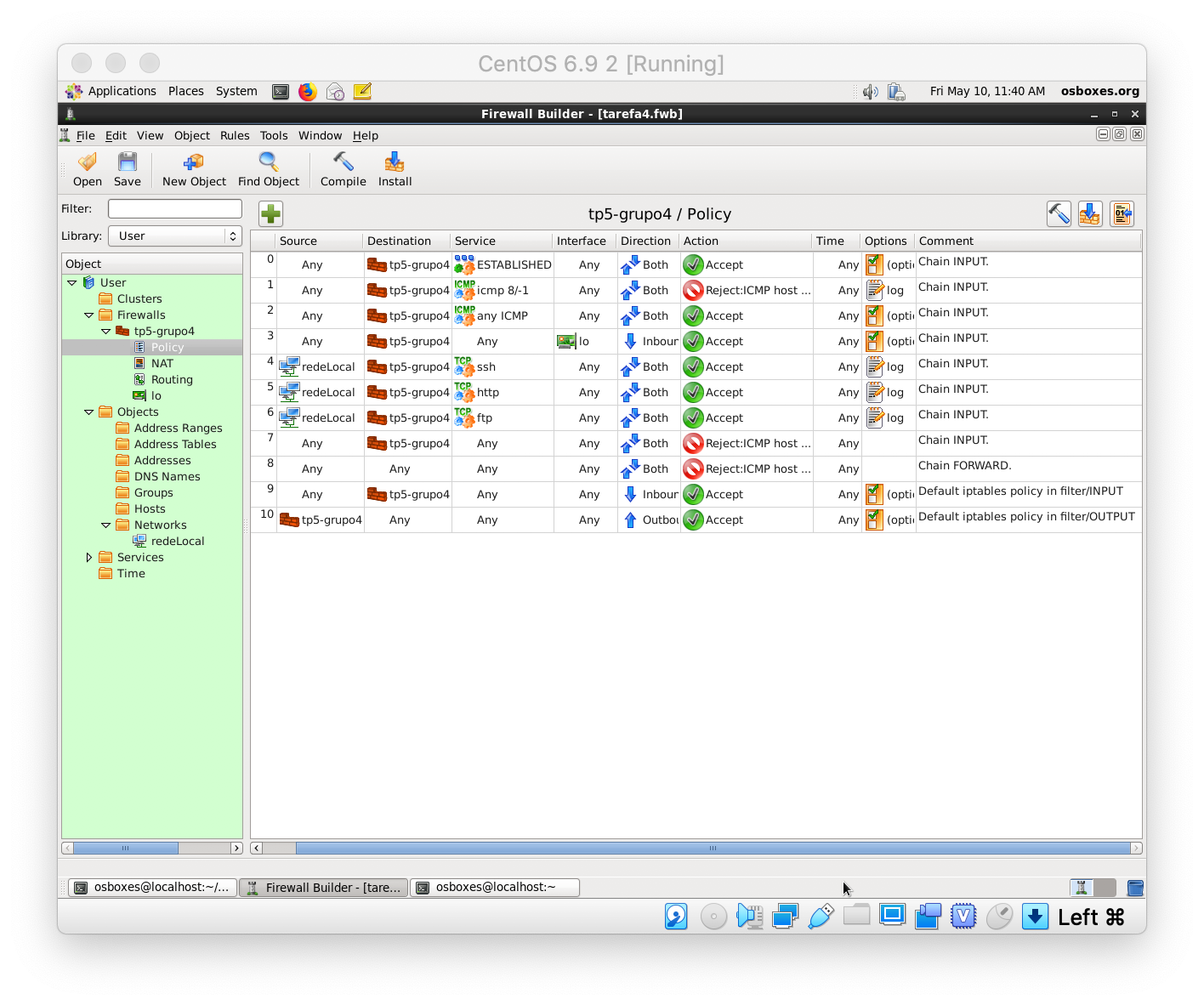


Figura - Firewall builder com novas regras.

Após a instalação das novas regras, foram realizados os seguintes comandos:

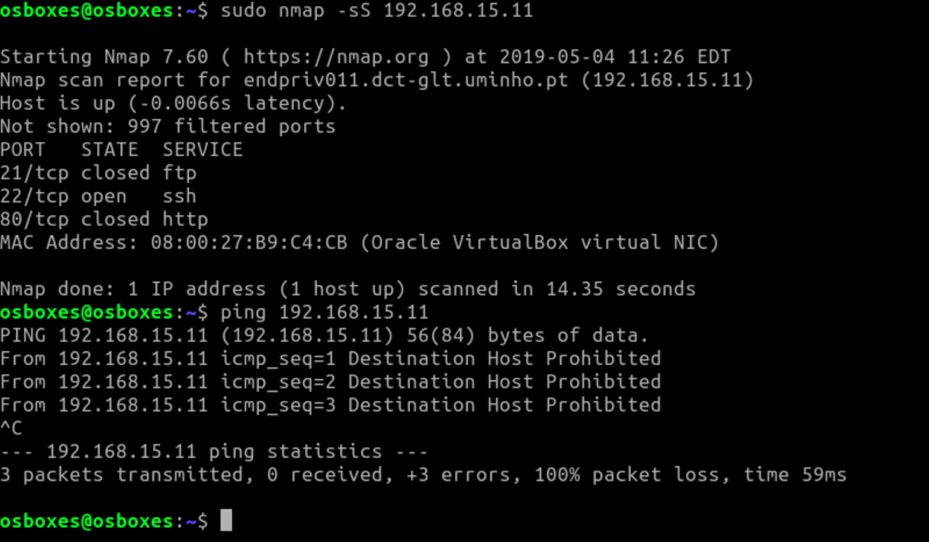


Figura - Execução de NMAP e Ping no cliente.

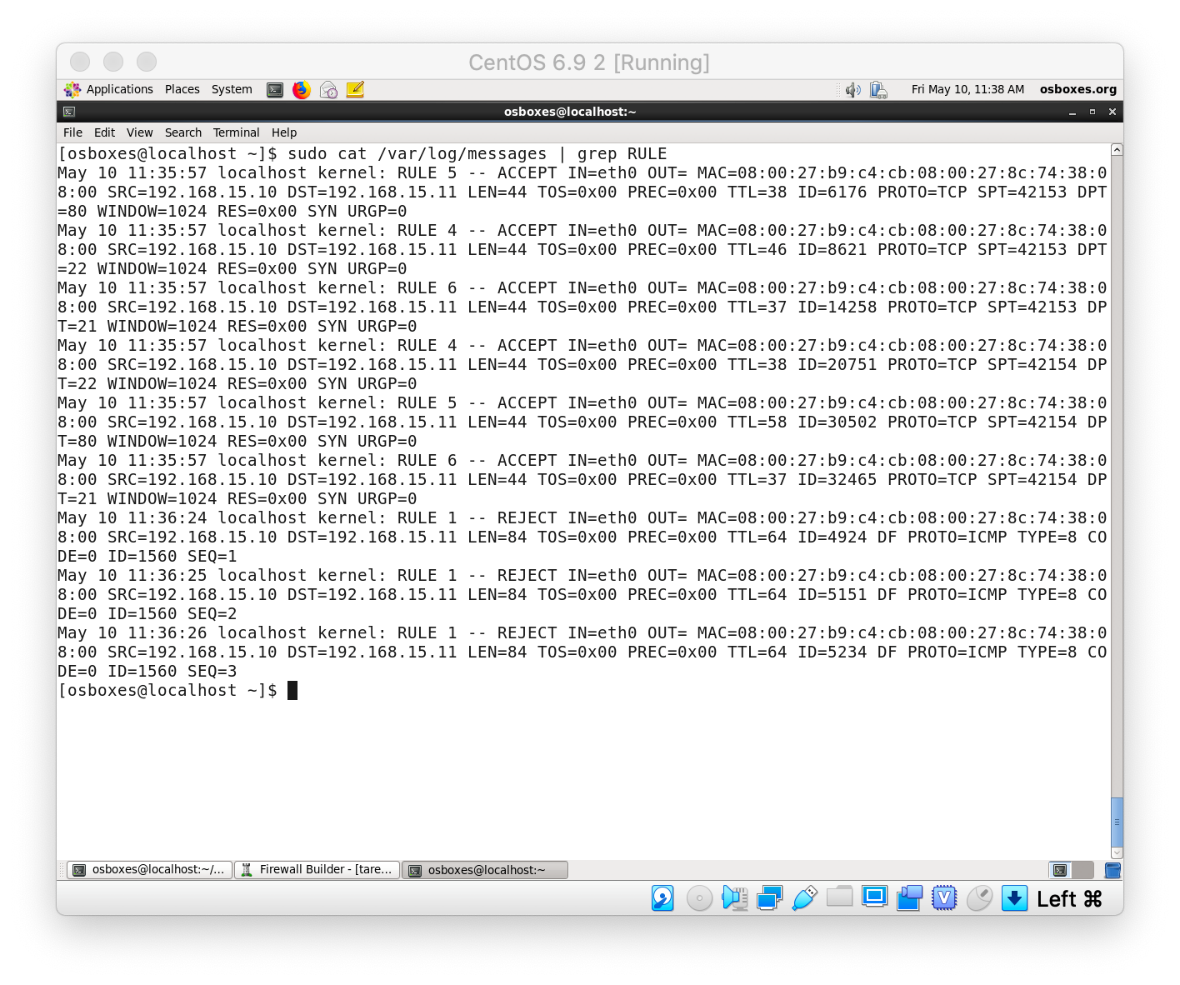


Figura - Logs no Servidor após Ping e Nmap do cliente.

# Conclusão

Após realização deste trabalho o grupo fica satisfeito com o cumprimento de todos os objetivos propostos, sendo agora capaz de entender o funcionamento de uma firewall ao nível de uma rede e numa máquina com sistema operativo.

Foram consolidados vários aspetos que são precisos para a correta configuração de uma firewall tais como o uso de vários comandos e serviços em ambiente Linux e as regras e políticas de segurança.

De modo a aprofundar e obter ainda mais informação acerca da ferramenta mais importante que foi utilizada, a **iptables**, foi ainda utilizada uma interface gráfica que faz uso da mesma ferramenta. A instalação do Firewall Builder foi um processo complicado, visto não existir muita documentação para este efeito.

Por fim, consideramos os objetivos do trabalho cumpridos com sucesso e conseguimos perceber a importância de uma boa configuração da firewall nos tempos atuais, pois o mundo tecnológico atual torna-se cada vez mais composto por dispositivos conectados entre si e a segurança e controlo das ligações entre eles são absolutamente cruciais.