

Relatório do Sprint 1 de Administração de Sistemas

**Membros do grupo**

1181255 Nuno Teixeira

1181498 Rafael Barbarroxa

1181500 Vítor Crista

1181529 Diogo Sousa

**Docente/Orientador:**

André Moreira (ASC)

**Unidade Curricular:**

Administração de Sistemas



Relatório entregue no dia 6 de dezembro de 2020

Índice:

[1. Introdução: 2](#_Toc57739718)

[2. US1 2](#_Toc57739719)

[3. US2 5](#_Toc57739720)

[4. US3 5](#_Toc57739721)

[5. US4 7](#_Toc57739722)

[6. US5 7](#_Toc57739723)

[7. US6 8](#_Toc57739724)

[8. US7 9](#_Toc57739725)

[9. US8 11](#_Toc57739726)

[10. Conclusão 11](#_Toc57739727)

# Introdução:

O presente relatório foi efetuado para dar resposta ao sprint efetuado na Unidade  
Curricular de ASIST. O documento escrito irá dar uma breve explicação de cada uma  
das oito **User Stories** elaboradas na execução do trabalho.

# US1

Para ser possível fornecer IPs de uma família especifica a postos de clientes, é necessário instalar e configurar um servidor **DHCP** tanto no Windows como no Linux.

Em relação ao Linux, é necessário instalar o servidor através do comando **sudo apt install isc-dhcp-server.** De seguida, editar o ficheiro **/etc/default/isc-dhcp-server** para determinar que interfaces serão usadas para processar pedidos ao servidor DHCP.

O resto da configuração é efetuada no ficheiro ***/etc/dhcp/dhcpd.conf:***

Uma imagem com texto

Descrição gerada automaticamente

Figura 1- Configuração DHCP

Uma imagem com texto

Descrição gerada automaticamente

Figura 2- Definição das interfaces DHCP

Uma imagem com texto

Descrição gerada automaticamenteÉ preciso verificar se a interface usada pelo servidor DHCP, no nosso caso a ens192, possuí um IP que pertence à subnet de DHCP, sendo então preciso aceder ao ficheiro ***/etc/netplan/50-cloud-init.yaml,*** efetuando a alteração se necessário:

Figura 3- Interfaces de rede

De seguida, liga-se o servidor DHCP com a instrução **sudo systemctl start isc-dhcp-server.service,** podendoo seu estado ser verificado com o comando **sudo systemctl status isc-dhcp-server.service:**

**Uma imagem com texto

Descrição gerada automaticamente**

Figura 4- Estado do server DHCP

Uma imagem com texto

Descrição gerada automaticamenteA lista de IPs que estão a ser disponibilizados podem ser verificados através de **dhcp-lease-list.**

Figura 5- DHCP Lease List

No **Windows** o servidor DHCP é instalado indo a Gerir > Adicionar Funções e Funcionalidades e escolher o **servidor DHCP.** Quando terminado, é feita a configuração pós-instalação, sendo depois possível configurar um âmbito. É necessário definir um intervalo de endereços a serem disponibilizados, comprimento e máscara de sub-rede, podendo ainda definir-se IPs para excluir dentro da gama, um default gateway, um servidor DNS e um WINS. Foi escolhido definir o servidor DNS como o do ISEP.

Uma imagem com texto

Descrição gerada automaticamente

Figura 6- Âmbito do servidor DHCP

# US2

O **servidor Linux** faculta endereços de 192.168.120.50 a 192.168.120.150 e o **servidor Windows** de 192.168.120.151 a 192.168.120.200. Sendo que a **interface ens192 de Linux** possuí o IP 192.168.120.1 e a **interface Ethernet1 de Windows** o 192.168.120.2.

# US3

No **servidor Windows**, para limitar o acesso por RDP a utilizadores que não sejam os administradores, é necessário alterar uma regra na **firewall.** O primeiro passo é ir a **Firewall do Windows Defender com Segurança Avançada,** escolher **Regras de Entrada** e selecionar a regra **Ambientes de Trabalho Remotos – Modo de Utilizador (Entrada de TCP)**. Seguidamente, escolher a tab de **Âmbito** e definir os endereços de **IPs remotos** do grupo: **10.8.69.22, 10.8.69.214, 10.8.69.199 e 10.8.45.114.**

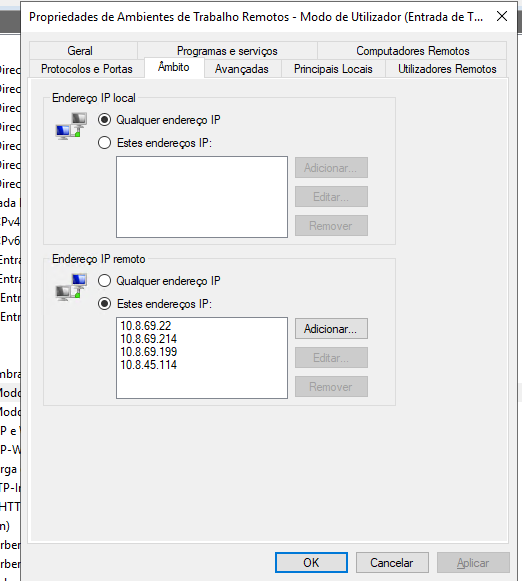
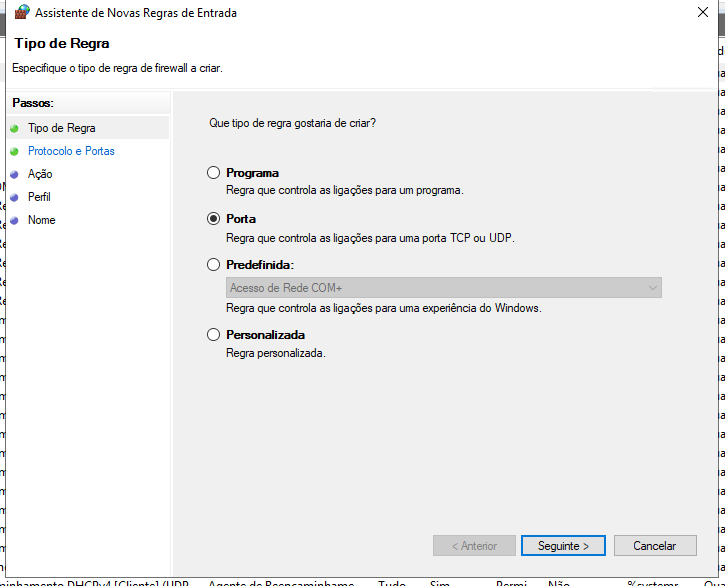


Figura 7- IPs autorizados para RDP

**** Depois, é necessário criar as regras para o acesso **HTTP e HTTPS.**  Ainda dentro de **Regras de Entrada** escolher a opção de **Nova Regra,** o **tipo de regra** deve ser **Porta**.

Em **Protocolo e Portas** deve ser escolhido o protocolo **TCP**, com a **porta 80** para **HTTP** e a **porta 443** para **HTTPS.**

Em **ação** manter o default **Permitir a ligação,** em **perfil** aplicar a regra a **Domínio, Privado e Público.**

Finalmente, escolher um **nome** para regra e, opcionalmente, uma **descrição.**

**Uma imagem com texto

Descrição gerada automaticamenteUma imagem com texto

Descrição gerada automaticamente**

Figura 8- Configuração do Protocolo HTTP e Portas

No **servidor Linux**, foi adicionado ao ficheiro ***/etc/my.firewall***as regras que permitem os pedidos **HTTP** e **HTTPS** ao servidor:



Figura 9- Regras de HTTP e HTTPS

Foram definidos também, através de regras, os IPs, nomeadamente os dos computadores do grupo, que poderiam aceder ao servidor através de **SSH**:

Uma imagem com texto

Descrição gerada automaticamente

Figura 10- Regras de SSH

Em último lugar, bloquear os outros pedidos SSH:



Figura 11- Regra de bloqueio SSH

# US4

No **Windows,** o IP Spoofing é impedido por predefinição.

No **Linux**, é necessário abrir o ficheiro **/etc/sysctl.conf** e remover os comentários das linhas:

Uma imagem com relógio, objeto, monitor, sentado

Descrição gerada automaticamente

Figura 12- Ficheiro sysctl.conf para IP SPoofing

# US5

Uma imagem com interior, sentado, laranja, escuro

Descrição gerada automaticamentePara efetuar esta verificação de UID’s no servidor Linux foi preciso alterar o ficheiro ***/etc/pam.d/sshd***

Figura 13- Ficheiro SSHD

Na primeira linha, se o UID for menor que 6000, as duas linhas a seguir são ignoradas.

Na segunda linha, se o UID for maior que 6500, a próxima linha é ignorada. Isto ocorre devido ao parâmetro **success** que determina o número de linhas, ser ignorado se a condição suceder.

A terceira linha vai verificar se o **remote host** que está a tentar aceder via SSH, está indicado no ficheiro ***/etc/remote-hosts,*** se estiver, permite o login, senão, é impedido.

Uma imagem com texto

Descrição gerada automaticamente Exemplo de funcionamento (é usado o luser3, visto ele possuir um UID de 6002, e não se encontrando no ficheiro ***/etc/remote-hosts***):

Figura 14- Exemplo de funcionamento do remote host bloqueado

# US6

Numa primeira tentativa, foi criado um script em ***/etc/lockbadguys.sh***que vai ler o ficheiro ***/etc/bad-guys*** e bloquear os utilizadores que nesse ficheiro tentem aceder ao sistema, através do comando **passwd -l.** Contudo este método não é suficiente porque o script teria de ser percorrido manualmente ou periodicamente, e como tal não seria possível ao utilizador fazer login após o seu nome ter sido removido da lista.

Uma imagem com texto

Descrição gerada automaticamente

Figura 15- Script lockbadguys.sh

Exemplo de utilização:

Uma imagem com texto

Descrição gerada automaticamente

Figura 16- Resultado do script

Na segunda tentativa, foi adicionada a seguinte linha para o ficheiro ***/etc/pam.d/common-auth*** :



Figura 17- Ficheiro common-auth

Através desta linha é analisado o ficheiro (**pam\_listfile.so**) /***etc/bad-guys***, como indicado no parâmetro **file**, os utilizadores(**item=user**) que lá se encontram são inibidos de entrar no sistema (**sense=deny**).

# US7

No **servidor Linux**, para criar a mensagem de pré-login, foi criado um script no ficheiro ***/etc/prelogin.sh*** e a mensagem gerada é guardada no ficheiro ***/etc/ssh/sshd-banner***

Uma imagem com texto

Descrição gerada automaticamente

Figura 18- Script do ficheiro prelogin.sh para mensagem de pré login

Foi preciso também editar o ficheiro ***/etc/ssh/sshd\_config*** e adicionar uma linha relativamente ao **Banner** a ser atualizado:

Uma imagem com texto

Descrição gerada automaticamente

Figura 19- Ficheiro sshd\_config

Para a automatização do processo, foram procurados e experimentados vários métodos, incluindo o uso do ficheiro ***/etc/rc.local*** e a criação de um serviço tal como exemplificado em **https://medium.com/@kevintimotius/banner-before-login-with-dynamic-hostname-debian-9-b5cefebaaa62**, contudo, não obtivemos nenhum sucesso. Optamos então por usar o **cron.** Através do ***/etc/crontab***, o script é corrido de 5 em 5 minutos, atualizando o ficheiro com a hora certa e a mensagem dinâmica que depende da altura do dia.

Uma imagem com texto

Descrição gerada automaticamente

Figura 20- Ficheiro crontab

Em relação à mensagem pós-login, foi criado um script parecido ao anterior, mas este encontra-se em ***/etc/profile.d/welcome.sh.*** Após o utilizador tiver efetuado o login, o script é corrido automaticamente.

Uma imagem com texto

Descrição gerada automaticamente

Figura 21- Script welcome.sh gerador da mensagem pós login

# US8

Para esta user storie, adicionamos ao ficheiro ***/etc/my.firewall*** as seguintes linhas que contêm

os IPs do grupo (**10.8.69.22, 10.8.69.214, 10.8.69.199, 10.8.45.114).**

Uma imagem com relógio, cidade, sentado, monitor

Descrição gerada automaticamente

Figura 22- Regras do ficheiro my. firewall

Depois são adicionadas as seguintes linhas, em várias combinações das mesmas, para tentar bloquear pedidos ICMP de outras máquinas que não as do grupo:

Uma imagem com texto

Descrição gerada automaticamente

Figura 23- Regras de pedidos ICMP

Contudo, depois de várias tentativas com diferentes linhas na firewall, acabamos por não conseguir alcançar o resultado pretendido, visto que **todos** os pings ao server são bloqueados.

# Conclusão

Com a realização deste trabalho, o grupo conseguiu interiorizar os tópicos lecionados nas aulas, aumentando o nosso conhecimento sobre os mesmo ao ter que pôr o que aprendemos e o que pesquisamos em prática.