#### 21 - Como administrador da infraestrutura quero que o servidor Windows e Linux forneçam endereços IP (na segunda placa de rede) da família 192.168.X.0/24 aos postos clientes, onde X é obtido por 100 + número\_do\_grupo (exemplo, para o grupo 99, X=199); para o efeito devo alterar o endereço dessa placa assignado nas aulas PL

Configuramos o servidor **Linux** com ip fixo **192.168.174.1** e o servidor **Windows** com ip fixo **192.168.174.2**.

##### Linux:

Para isso, temos que editar o ficheiro **/etc/network/interfaces** com o comando **nano /etc/network/interfaces** e editar as linhas correspondente a segunda placa, no nosso caso, a placa **ens33**. Configuramos com o ip **192.168.174.1** e a respetiva mascara **255.255.255.0.**

##### Text Description automatically generated

##### Windows:

Para isso, temos que ir as definições de rede, ir as propriedades da placa pretendida (como pedido na segunda placa, no nosso servidor é a **Ethernet1**), selecionar a ligação que pretendemos, neste caso IPv4 e alterar o ip para o pretendido (**192.168.174.2**)

Graphical user interface, text, application, email

Description automatically generated > Graphical user interface, application

Description automatically generated > Graphical user interface, text, application, chat or text message

Description automatically generated > Graphical user interface, text, application

Description automatically generated

#### 22 - Como administrador da infraestrutura quero que os serviços acima referidos funcionem em failover, com um deles a facultar endereços de 192.168.X.50 a 192.168.X.150 e o outro de 192.168.X.151 a 192.168.X.200

Para os sistemas funcionarem em failover, configuramos o servidor **Linux** para atribuir ips entre **192.168.174.50 e 192.168.174.150** e o servidor **Windows** entre **192.168.174.151 e 192.168.174.200**.

##### Linux:

Para configurar o DHCP no servidor Linux, primeiro foi necessário instalar o serviço **isc-dhcp-server** com o comando **sudo apt install isc-dhcp-server.**

Após estar instalado foi necessário definir a subnet e o range pretendidos. Para isso foi necessário editar o ficheiro **dhcpd.conf** através do comando **nano /etc/dhcp/dhcpd.conf** e inserir os ips e a mascara pretendida.

Text

Description automatically generated

Depois de configuradas, foi necessário definir qual a interface que pretendiamos utilizar o DHCP, editamos o ficheiro **isc-dhcp-server** com o comando **nano /etc/default/isc-dhcp-server** e definimos a segunda placa, a ens33.

Text

Description automatically generated

No final, foi apenas necessário arrancar com o respetivo serviço com o comando **Systemctl start isc-dhcp-server.**

##### Windows:

Em primeiro lugar, é necessário instalar o servidor DHCP através da opção **Adicionar funções e funcionalidades** no gestor de servidor.

Graphical user interface

Description automatically generated > Graphical user interface, text, application

Description automatically generated

Depois de instalado, na pesquisa aparecerá a aplicação **DHCP**. Selecionando-a, a janela mostrará os servidores presentes no sistema.

Para adicionar o range na placa que pretendemos, temos que selecionar a opção **Adicionar/Remover Enlaces** e de seguida selecionar a placa que pretendemos criar o mesmo, tanto para Ipv4 como para Ipv6**.** No nosso caso na segunda placa (Ethernet1).

Shape

Description automatically generated with low confidence > Graphical user interface

Description automatically generated > Graphical user interface, text, application

Description automatically generated>Graphical user interface, text, application

Description automatically generated

Para adicionar/configurar o range de atribuição de ips, teremos que selecionar a versão de ip (IPv4) e selecionar **Novo Âmbito**.

Para finalizar a configuração basta seguir os passos e definir as configurações necessárias, tais como, **Nome** e **Descrição**, **Range** de ips e respetiva **máscara**, **duração** da concessão, ips a excluir (no nosso caso não foi necessário especificar).

Graphical user interface, text, application, email

Description automatically generated > Graphical user interface, application

Description automatically generated > Graphical user interface, application

Description automatically generated > Graphical user interface, text, application, email

Description automatically generated > Graphical user interface, text, application

Description automatically generated

#### 23 - Como administrador da infraestrutura quero os servidores Windows e Linux estejam disponíveis apenas para pedidos HTTP e HTTPS. Tal não deve impedir o acesso por SSH ou RDP aos administradores (o grupo).

A nossa solução passou por bloquear todas as portas e apenas libertar as que pretendíamos. Para isso as regras de permissão foram inseridas antes da regra de bloqueio, de forma a analisar o tráfego primeiro e só depois bloquear, se for o caso.

Para isso foi criado um ficheiro para as iptables com o nome **iptables.sh** criado em **/etc/save** com o comando **nano /etc/save/iptables.sh.**

Graphical user interface

Description automatically generated with medium confidence

Para memorizar permanentemente as configurações das iptables, foi executado o comando **iptables-save > /etc/save/iptables.sh**.



De forma a carregar as iptables quando o servidor é desligado ou reiniciado, foi necessário adicionar o comando **iptables-restore > /etc/save/iptables.sh** ao ficheiro **crontab**.

O ficheiro **crontab** no Linux é um daemon que executa tarefas editadas pelo usuário em horários e eventos específicos. Neste caso, não temos horário definido é apenas no arranque da máquina.

Alteramos o ficheiro e colocamos o comando.

**Text

Description automatically generated**

**FALTA TESTAR E PERGUNTAR AO PROF PARA TER 100% certeza**

##### Windows:

No sistema Windows não há ordem de execução de regras na firewall, ou seja, estando a Firewall ativa, é permitido apenas o tráfego indicado nas regras sendo o restante bloqueado por defeito.

Para isso, para o servidor ficar apenas disponível para pedidos HTTP e HTTPs, foi necessário aceder as definições avançadas da Firewall.

Graphical user interface, text, application, email

Description automatically generated > Graphical user interface, text, application

Description automatically generated

Dentro da Firewall foi necessário criar as regras de entrada. Criamos duas regras, uma para permitir pedidos HTTP e HTTPs, nas portas correspondentes 80 e 443, para o protocolo TCP e uma com as mesmas configurações para o protocolo UDP.

Exemplo para protocolo TCP:

Graphical user interface, text, application

Description automatically generated > Graphical user interface, application, Teams

Description automatically generated > Graphical user interface, text, application

Description automatically generated > Graphical user interface, text, application, Teams

Description automatically generated > Graphical user interface, text, application, Teams

Description automatically generated > Graphical user interface, application

Description automatically generated

Por fim, regras criadas:

Graphical user interface, text, application

Description automatically generated

#### 24 - Como administrador da infraestrutura quero impedir o IP spoofing na minha rede

##### Windows:

Para impedir o IP spoofing no servidor Windows, foi necessário criar regras de entrada e de saída.

Para as regras de entrada, foi necessário criar uma para aceitar entrada de IPs na nossa gama de IPs **192.168.174.0/24** e uma para bloquear as várias gamas, tais como, **0.0.0.0/8** - Rede atual (válido apenas como endereço de origem), **127.0.0.0/8** – ip privado, **10.0.0.0/8** – ip privado, **172.16.0.0/12** – ip privado, **192.168.0.0/16**, **224.0.0.0/3**, **192.168.174.2/24** (IP do próprio servidor).

Exemplo de criação de regra de entrada para impedir acesso:

Graphical user interface, text, application

Description automatically generated > Graphical user interface, text, application, email

Description automatically generated > Graphical user interface, text, application, email

Description automatically generated > Graphical user interface, application

Description automatically generated > Graphical user interface

Description automatically generated > Graphical user interface, text, application, Teams

Description automatically generated

Regra de entrada para permitir acesso a gama de IPs **192.168.174.0/24**:

Graphical user interface, text, application, email

Description automatically generated > Graphical user interface

Description automatically generated

Resultado das regras de entrada:

Graphical user interface, application

Description automatically generated

Para as regras de saída, foram criadas as regras com as mesmas configurações:

Graphical user interface, application

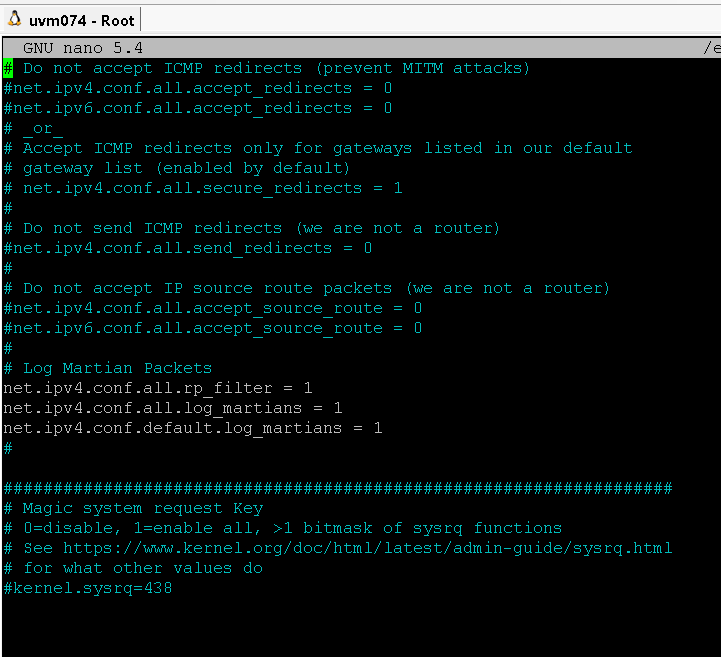
Description automatically generated

##### Linux:

Text

Description automatically generated

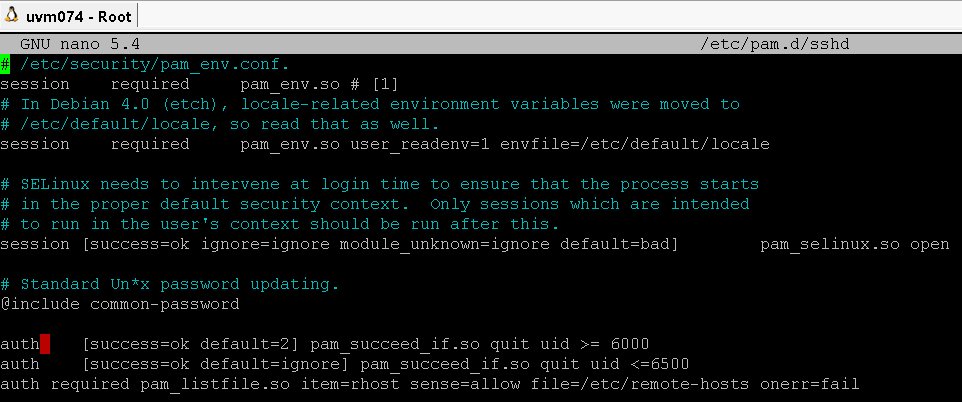
nano /etc/sysctl.conf



#### 25 - Como administrador da infraestrutura quero que os utilizadores registados no Linux com UID entre 6000 e 6500 só consigam aceder via SSH se esse acesso for a partir de uma máquina listada em /etc/remote-hosts

Solução proposta:

O módulo PAM pam\_limits define os limites dos recursos do sistema que podem ser obtidos em uma sessão do utilizador ou seja PAM é o modulo que nega sempre os acessos, salvo indicação em contrário. Tendo isto em mente, abrimos o ficheiro /etc/pam.d/sshd e inserimos no final das mesmo três linhas de código como demonstra a imagem, a primeira ira testar se o UID do user em questão é igual ou superior, caso não seja, por defeito, ira salvar duas linhas, descartando assim a necessidade de verificar se o IP esta na lista de IPs autorizados. Caso seja superior a 6000, ira verificar na segunda linha se o UID é igual ou inferior a 6500, o que caso não seja ira ignorar e tentar a terceira linha, a terceira linha ira verificar o ficheiro /etc/remote-hosts para ver se o IP da sessão que esta a ser testada percente a lista de IPs aceites.



Apos definir este ficheiro, criamos então o ficheiro /etc/remote-hosts e inserimos um IP de uma das nossas máquinas para testarmos.



Uma imagem com texto, relógio

Descrição gerada automaticamente

#### 26 - Como administrador da infraestrutura quero que o acesso ao sistema seja inibido aos utilizadores listados em /etc/bad-guys

Antes de mais criamos o ficheiro bad-guys com os users que pretendíamos inibir o acesso.

A picture containing graphical user interface

Description automatically generated > Text

Description automatically generated

Para configurar e inibir o respetivo acesso, foi necessário editar o ficheiro **common-auth** com o comando **nano /etc/pam.d/common-auth** e adicionar a linha que pretendíamos.

Adicionamos a seguinte linha:  
**auth required pam\_listfile.so item=user sense=deny file=/etc/bad-guys onerr=succeed**

Text

Description automatically generated

O **pam\_listfile** é um módulo **PAM** que dá a possibilidade de negar ou permitir serviços baseados num ficheiro arbitrário.

Nessa mesma configuração, o argumento **item** **= user** indica a **pam\_listfile** que este deve encontrar nomes de utilizadores em **//etc/bad-guys**.

O argumento **sense = deny** indica a **pam\_listfile** que o ficheiro **bad-guys**,em **file=//etc/bad-guys** é uma lista de negação, ou seja, qualquer utilizador nesse ficheiro faz com que o **pam\_listfile** falhe, fazendo com que a autenticação falhe.

O argumento **onerr=succeed** indica que a condição de sucesso é erro.

Por último, foi necessário reiniciar os serviços através dos comandos **sudo service ssh restart** e **sudo service sshd restart.**



Como podemos ver, ao utilizador luser2 que estava presente na lista, não é permitido iniciar sessão.

A screenshot of a computer

Description automatically generated with medium confidence

#### 27 - Como administrador da infraestrutura quero que as mensagens pré-login e pós-login bem-sucedido sejam dinâmicas (por exemplo, “[Bom dia] | [Boa tarde] username”, etc.)

##### Linux:

Para resolvermos esta user case, vamos dividir a questão em duas partes.

A primeira parte será definir a mensagem pré login (mensagem apresentada aos utilizadores que estão prestes a entrar efectuar o login), para isso criamos um ficheiro no directorio /etc/ssh/ com o nome “ssh\_banner\_pre\_login”.

Uma imagem com texto

Descrição gerada automaticamente

Neste ficheiro colocamos a mensagem que gostaríamos de ver ao inicializarmos a maquina.

Uma imagem com texto

Descrição gerada automaticamente

Depois da criação e edição do ficheiro, vamos ao ficheiro sshd\_config localizado no diretório /etc/ssh/ e descomentamos a linha que indica o banner (posteriormente estava a banner none) e inserimos o banner definido anteriormente



Uma imagem com texto

Descrição gerada automaticamente

Com disto, damos concluído a criação do banner de pre login e para testarmos, reiniciamos a maquina com o comando init 6 e podemos comprovar o resultado.



Uma imagem com texto

Descrição gerada automaticamente

Para realizar a segunda etapa desta user case, a definição customizada do pos login, vamos ao ficheiro /etc/profile e inserimos um script que ira verificar as horas atuais e consoante essas horas ira dar as boas-vindas dizendo bom dia, boa tarde ou boa noite ao utilizador logado.

Uma imagem com texto

Descrição gerada automaticamente

Uma imagem com texto

Descrição gerada automaticamente

Por fim, ao fazermos o login podemos comprovar que já temos a mensagem pos login a funcionar.

Uma imagem com texto

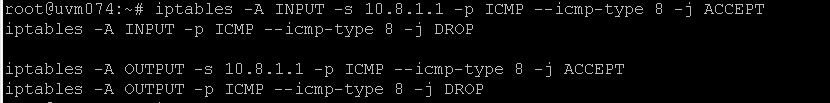
Descrição gerada automaticamente

#### 28 - Como administrador da infraestrutura quero que o servidor Linux responda e envie pedidos ICMP para teste de conectividade apenas e só aos computadores dos elementos do grupo

Resolução proposta:

Para permitimos envios de ping de determinadas máquinas podemos usar o comando iptables.

Este comando funciona de forma ordenada, ou seja, o primeiro comando tem prioridade pelos demais. Com isto em mente, colocamos a aceitação dos IPs das nossas máquinas nas primeiras linhas tanto para input como para output. Nas linhas imediatamente a seguir colocamos o drop de qualquer IP tanto para input como para output. Ao fazermos um ping ao nossa máquina em Linux através de uma das nossas maquinas iremos conseguir obter uma resposta do ping porque os nossos IPs estão na primeira linha da iptables, caso não seja o IP autorizado, automaticamente passaria para a segunda linha (o que nesta demostração apenas esta um IP, mas no servidor temos 5 IPs seguidos de uma iptable para DROP).



Text

Description automatically generated