DEPARTAMENTO DE ENGENHARIA INFORMÁTICA

Relatório Sprint 1
ASIST

Grupo 46
José Mota (1161263)
Pedro Real (1170689)
João Flores (1171409)
Patrick Timas (1171352)

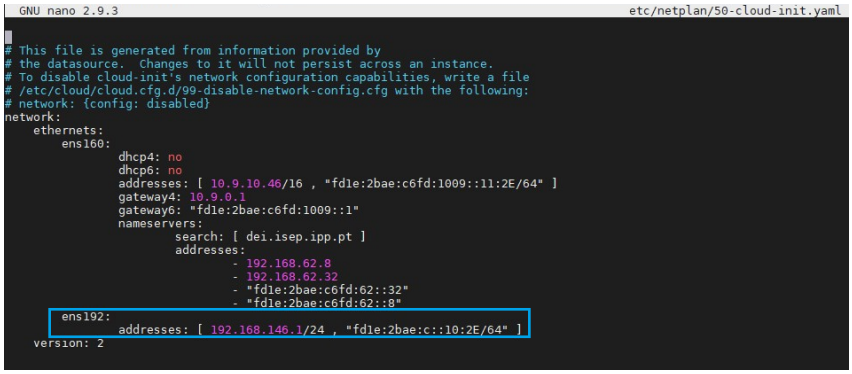
Novembro, 2019

isep Instituto Superior de Engenharia do Porto

LINUX

1/2)

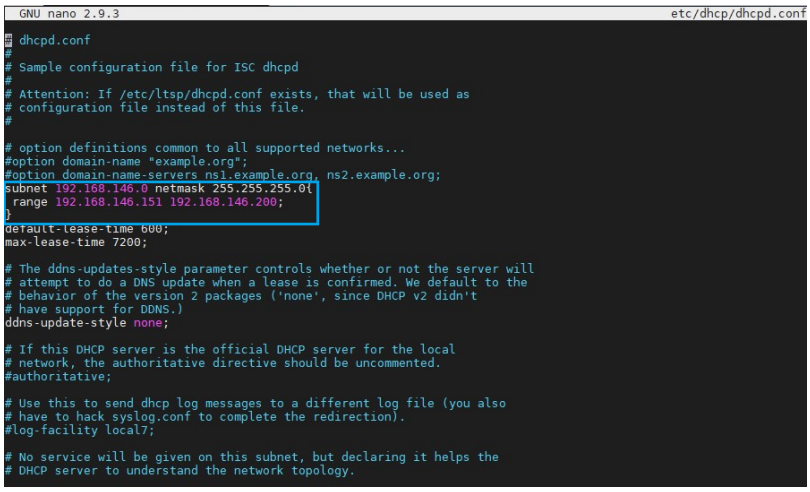
- Configurar uma interface (segunda interface) no “etc/netplan/50-cloud-init.yaml” onde o endereço deve ser estático.



A interface configurada tem que estar ativada (Up), e para isso usa-se o seguinte comando:

sudo ip link set up de ens192

- Configurar o ficheiro “etc/dhcp/dhpcd.conf” para atribuir os endereços que os clientes vão receber através do DHCP.

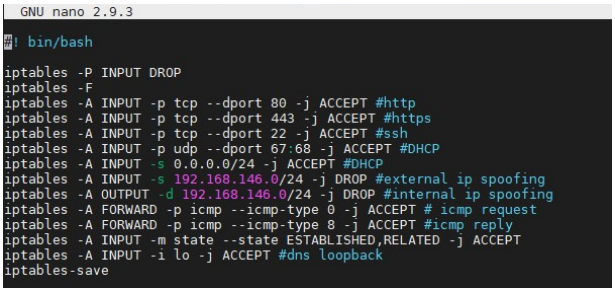


- Configurar a interface (segunda interface) que irá disponibilizar o DHCP configurado anteriormente. Para isso adiciona-se o codigo abaixo no ficheiro “/etc/default/isc-dhcp-server”

INTERFACESv4="ens192"
INTERFACESv6="ens192"

3/4/8)

- Cria-se um script “/iptables” onde através do comando “IPTABLES” adiciona-se as regras abaixo, onde o 80=HTTP,433=HTTPS,22=SSH,67:68=DCHP e por fim fazer o DROP para bloquear as outras entradas. Para o bloqueio do ip spoofing deve-se impedir toda a entrada de pacotes na rede cujo o endereço de origem é igual ao da rede local. No ICMP quando e do tipo 0=pedidos enquanto que do tipo 8=respostas.



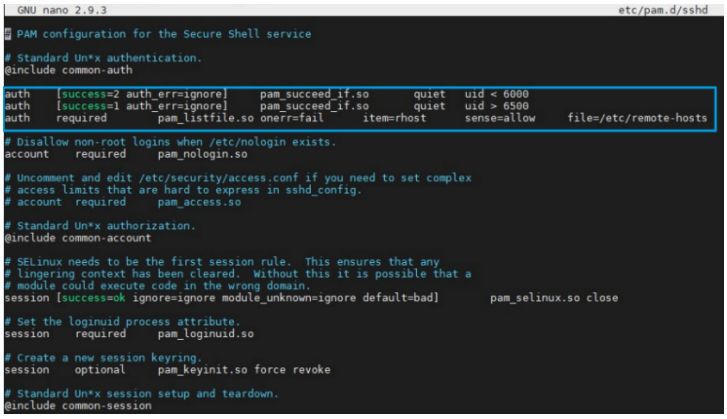
5)

- No ficheiro “etc/remote-hosts” deve ser colocado os Ips dos administradores que podem entrar com os USERs de UID entre 6000 e 6500.

  10.8.2.3

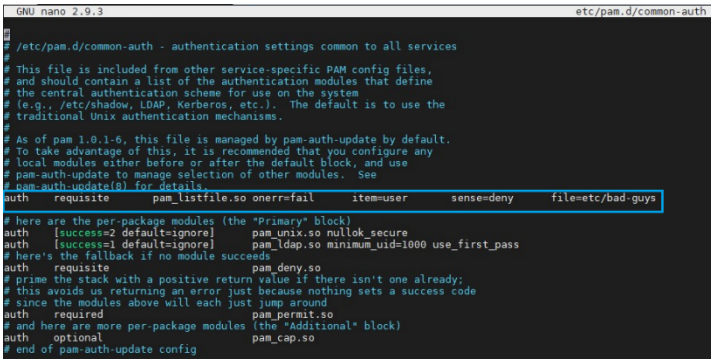
  10.8.106.228

- Agora tem que se adicionar o codigo abaixo no ficheiro “/etc/pam.d/sshd” para a verificação dos administradores



6)

- Para rejeitar o acesso de determinados USERs, aplica-se o codigo abaixo no ficheiro “etc/pam.d/common-auth”



- De seguida cria-se o ficheiro “etc/bad-guys” onde adiciona-se os USERs que vão ficar sem acesso a máquina.

  luser1

  luser2

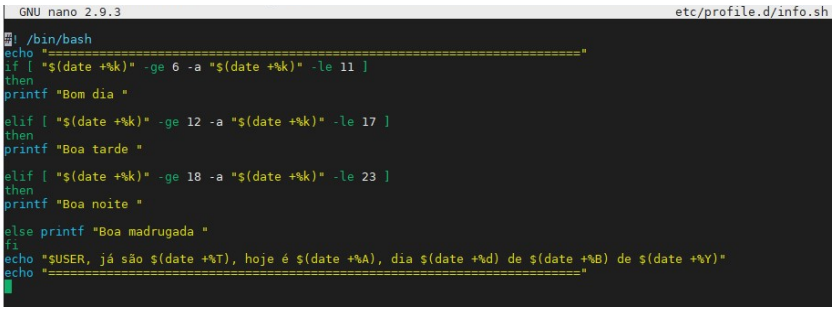
7)

- Para adicionar textos pré-login, é necessário configurar o ficheiro “etc/issue” para o acesso local ou “etc/issue.net” para o acesso remoto e edita-los conforme pretendido. De seguida para que o texto no “etc/issue.net” apareça deve-se ativar o “Banner” que se encontra no ficheiro “etc/ssh/sshd_config” colocando o seguinte codigo:

  Banner /etc/issue.net

  Depois deve-se reiniciar o “ssh” com o seguinte comando “etc/init.d/ssh restart”.

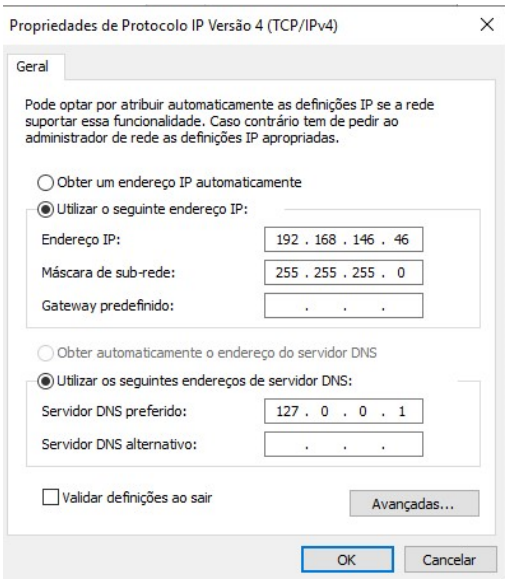
- Para adicionar textos pós-login, e necessários criar um ficheiro em “etc/profile.d/” e desenvolver o script com outputs pretendidos.



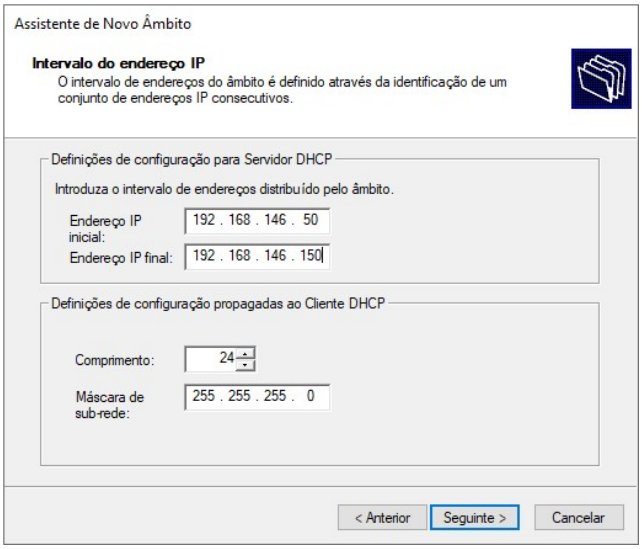
WINDOWS

1/2)

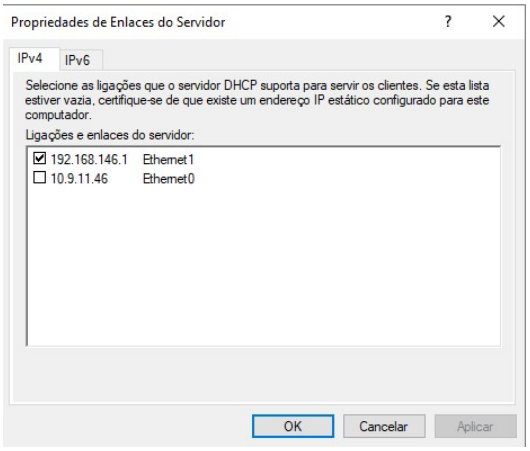
- Atribuir um IPv4 estático a interface “Ethernet1” (segunda interface) e o DNS que se encontra no “Centro de Rede e Partilha”.



- Através da funcionalidade DHCP no “gestor de servidor” configura-se o DHCP. Para isso tem que se criar um novo âmbito no IPv4 onde definimos o intervalo de IPs que serão atribuídos aos clientes dhcp.

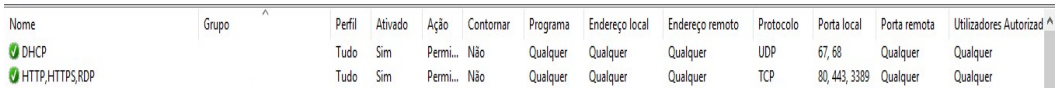


- Ativar o dhcp apenas para a segunda interface



3/4)

- Através da Firewall do Windows adiciona-se novas regras de entrada, onde deve-se permitir a entrada de tráfegos para as seguintes portas UPD (67:68), TCP (80,443,3389).



Nome	Grupo	Perfil	Ativado	Ação	Contornar	Programa	Endereço local	Endereço remoto	Protocolo	Porta local	Porta remota	Utilizadores Autorizad
DHCP		Tudo	Sim	Permi...	Não	Qualquer	Qualquer	Qualquer	UDP	67, 68	Qualquer	Qualquer
HTTP,HTTPS,RDP		Tudo	Sim	Permi...	Não	Qualquer	Qualquer	Qualquer	TCP	80, 443, 3389	Qualquer	Qualquer

- Para o IP spoofing, é impedir a entrada de dados cujo o endereço de origem dos ips que pertencem a rede 192.168.146.0/24