



Relatório Sprint 1 ASIST

Grupo 46

José Mota (1161263)

Pedro Real (1170689)

João Flores (1171409)

Patrick Timas (1171352)

Novembro, 2019

LINUX

1/2)

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

```
GNU nano 2.9.3 etc/netplan/50-cloud-init.yaml
# This file is generated from information provided by
# the datasource. Changes to it will not persist across an instance.
# To disable cloud-init's network configuration capabilities, write a file
# /etc/cloud/cloud.cfg.d/99-disable-network-config.cfg with the following:
# network: {config: disabled}
network:
  ethernets:
    ens160:
      dhcp4: no
      dhcp6: no
      addresses: [ 10.9.10.46/16 , "fd1e:2bae:c6fd:1009::11:2E/64" ]
      gateway4: 10.9.0.1
      gateway6: "fd1e:2bae:c6fd:1009::1"
      nameservers:
        search: [ dei.isep.ipp.pt ]
        addresses:
          - 192.168.62.8
          - 192.168.62.32
          - "fd1e:2bae:c6fd:62::32"
          - "fd1e:2bae:c6fd:62::8"
    ens192:
      addresses: [ 192.168.146.1/24 , "fd1e:2bae:c::10:2E/64" ]
version: 2
```

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/dhcpd.conf” para atribuir os endereços que os clientes vão receber através do DHCP.

```
GNU nano 2.9.3 etc/dhcp/dhcpd.conf
# dhcpd.conf
#
# Sample configuration file for ISC dhcpd
#
# Attention: If /etc/ltsp/dhcpd.conf exists, that will be used as
# configuration file instead of this file.
#
# option definitions common to all supported networks...
#option domain-name "example.org";
#option domain-name-servers ns1.example.org, ns2.example.org;
subnet 192.168.146.0 netmask 255.255.255.0 {
  range 192.168.146.151 192.168.146.200;
}
default-lease-time 600;
max-lease-time 7200;

# The ddns-updates-style parameter controls whether or not the server will
# attempt to do a DNS update when a lease is confirmed. We default to the
# behavior of the version 2 packages ('none', since DHCP v2 didn't
# have support for DDNS.)
# have support for DDNS.)
ddns-update-style none;

# If this DHCP server is the official DHCP server for the local
# network, the authoritative directive should be uncommented.
#authoritative;

# Use this to send dhcp log messages to a different log file (you also
# have to hack syslog.conf to complete the redirection).
#log-facility local7;

# No service will be given on this subnet, but declaring it helps the
# DHCP server to understand the network topology.
```

- Configurar a interface (segunda interface) que irá disponibilizar o DHCP configurado anteriormente. Para isso adiciona-se o código 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.

```
GNU nano 2.9.3
bin/bash

iptables -P INPUT DROP
iptables -F
iptables -A INPUT -p tcp --dport 80 -j ACCEPT #http
iptables -A INPUT -p tcp --dport 443 -j ACCEPT #https
iptables -A INPUT -p tcp --dport 22 -j ACCEPT #ssh
iptables -A INPUT -p udp --dport 67:68 -j ACCEPT #DHCP
iptables -A INPUT -s 0.0.0.0/24 -j ACCEPT #DHCP
iptables -A INPUT -s 192.168.146.0/24 -j DROP #external ip spoofing
iptables -A OUTPUT -d 192.168.146.0/24 -j DROP #internal ip spoofing
iptables -A FORWARD -p icmp --icmp-type 0 -j ACCEPT # icmp request
iptables -A FORWARD -p icmp --icmp-type 8 -j ACCEPT #icmp reply
iptables -A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
iptables -A INPUT -i lo -j ACCEPT #dns loopback
iptables-save
```

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 código abaixo no ficheiro “/etc/pam.d/sshd” para a verificação dos administradores

```
GNU nano 2.9.3 etc/pam.d/sshd
# PAM configuration for the Secure Shell service
# Standard Unix authentication.
@include common-auth

auth [success=2 auth_err=ignore] pam_succeed_if.so quiet uid < 6000
auth [success=1 auth_err=ignore] pam_succeed_if.so quiet uid > 6500
auth required pam_listfile.so onerr=fail item=rhost sense=allow file=/etc/remote-hosts

# Disallow non-root logins when /etc/nologin exists.
account required pam_nologin.so

# Uncomment and edit /etc/security/access.conf if you need to set complex
# access limits that are hard to express in sshd_config.
# account required pam_access.so

# Standard Unix authorization.
@include common-account

# SELinux needs to be the first session rule. This ensures that any
# lingering context has been cleared. Without this it is possible that a
# module could execute code in the wrong domain.
session [success=ok ignore=ignore module_unknown=ignore default=bad] pam_selinux.so close

# Set the loginuid process attribute.
session required pam_loginuid.so

# Create a new session keyring.
session optional pam_keyinit.so force revoke

# Standard Unix session setup and teardown.
@include common-session
```

6)

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

```
GNU nano 2.9.3 etc/pam.d/common-auth
#
# /etc/pam.d/common-auth - authentication settings common to all services
#
# This file is included from other service-specific PAM config files,
# and should contain a list of the authentication modules that define
# the central authentication scheme for use on the system
# (e.g., /etc/shadow, LDAP, Kerberos, etc.). The default is to use the
# traditional Unix authentication mechanisms.
#
# As of pam 1.0.1-6, this file is managed by pam-auth-update by default.
# To take advantage of this, it is recommended that you configure any
# local modules either before or after the default block, and use
# pam-auth-update to manage selection of other modules. See
# pam-auth-update(8) for details.
auth requisite pam_listfile.so onerr=fail item=user sense=deny file=etc/bad-guys
# here are the per-package modules (the "Primary" block)
auth [success=2 default=ignore] pam_unix.so nullok secure
auth [success=1 default=ignore] pam_ldap.so minimum_uid=1000 use_first_pass
# here's the fallback if no module succeeds
auth requisite pam_deny.so
# prime the stack with a positive return value if there isn't one already;
# this avoids us returning an error just because nothing sets a success code
# since the modules above will each just jump around
auth required pam_permit.so
# and here are more per-package modules (the "Additional" block)
auth optional pam_cap.so
# end of pam-auth-update config
```

- 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 editá-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 código:

Banner /etc/issue.net

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

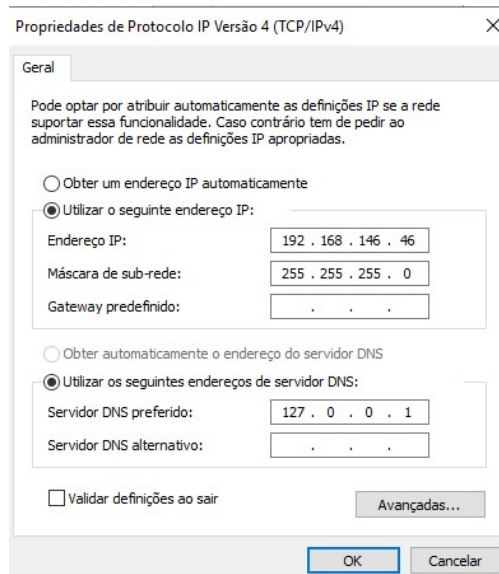
- Para adicionar textos pós-login, é necessário criar um ficheiro em “etc/profile.d/” e desenvolver o script com outputs pretendidos.

```
GNU nano 2.9.3 etc/profile.d/info.sh
#!/bin/bash
echo "=====
if [ "$(date +%k)" -ge 6 -a "$(date +%k)" -le 11 ]
then
printf "Bom dia "
elif [ "$(date +%k)" -ge 12 -a "$(date +%k)" -le 17 ]
then
printf "Boa tarde "
elif [ "$(date +%k)" -ge 18 -a "$(date +%k)" -le 23 ]
then
printf "Boa noite "
else printf "Boa madrugada "
fi
echo "$USER, já são $(date +%T), hoje é $(date +%A), dia $(date +%d) de $(date +%B) de $(date +%Y)"
echo "=====
"
```

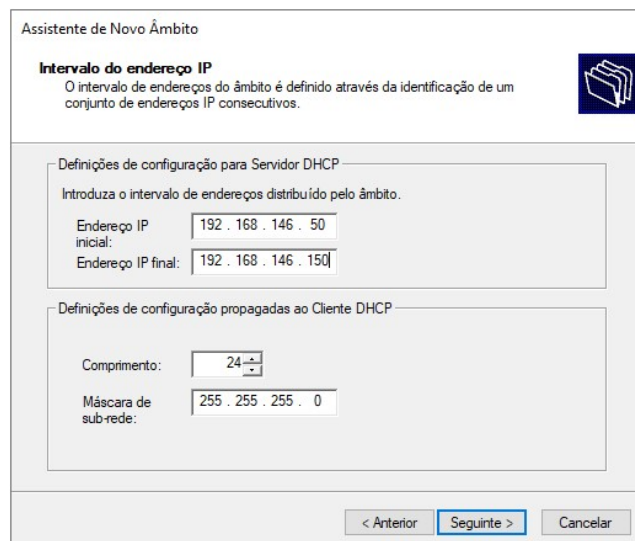
WINDOWS

1/2)

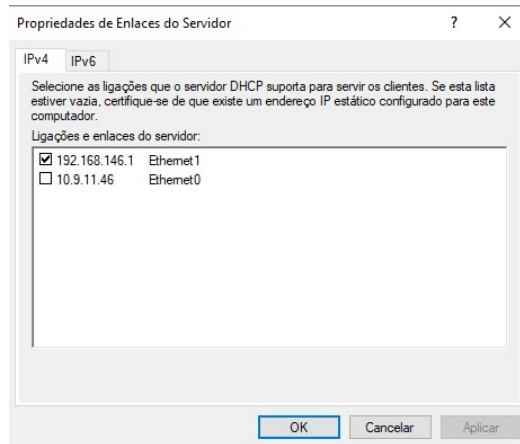
- Atribuir um IPv4 estático a interface “Ethernet1” (segunda interface) e o DNS que se encontra no “Centro de Rede e Partilha”.



- 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 UDP (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

