Relatório de ASIST

Turma 3DF_ 032
1181616 _ Tiago Oliveira
1180604 _ Vasco Silva
1190881 _ Matheus Figueira
1190835 _ Luís Teixeira

Data: 05/12/2021

Índice

Parte I – Introdução e estrutura do trabalho

Este relatório visa expor e explicar o processo de administração de sistemas relativa ao módulo de Desenho e Operação de Sistemas, no âmbito da Unidade Curricular de Administração de Sistemas (ASIST), lecionada (Aulas Pratico-Laboratoriais) pelo professor Joaquim Santos (JPE). Este módulo será parte integrante do projeto integrador do 5º semestre da Licenciatura de Engenharia Informática do ISEP, no ano curricular 21/22.

O relatório está dividido em três partes:

- Parte 1 – Introdução e estrutura do relatório;
- Parte 2 – Desenvolvimento;
- Parte 3 – Conclusão.

No final, encontram-se as referências utilizadas para o desenvolvimento do trabalho.

Parte II – Desenvolvimento

II.1 Use Cases – Casos de Uso (UC)

Nesta secção iremos expor os casos de uso requisitados.

- UC21 - 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;
- UC22 - 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;
- UC23 - 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) ;
- UC24 - Como administrador da infraestrutura quero impedir o IP spoofing na minha rede;
- UC25 - 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;
- UC26 - Como administrador da infraestrutura quero que o acesso ao sistema seja inibido aos utilizadores listados em /etc/bad-guys;
- UC27 - 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.) ;
- UC28 - 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.

II.2 Implementação das UC

Nesta secção iremos falar sobre cada um dos casos de uso.

II:2.1 UC21

Neste caso de uso, era pretendido que se instalasse DHCP nos servidores LINUX e WINDOWS. Fomos bem sucedidos na implementação de DHCP em Linux, no entanto, tal não foi possível em WINDOWS devido a falta de espaço.

- LINUX – Começamos por alterar o endereço IP da interface ens33, no ficheiro /etc/network/interfaces para 192.168.132.10. De seguida, acedemos ao ficheiro /etc/default/isc-dhcp-server e fizemos a respetiva configuração. Seguem imagens ilustrativas.

```
# The secondary network interface
auto ens33
iface ens33 inet static
        address 192.168.132.10
        netmask 255.255.255.0
# This is a static IPV6 interface
iface ens33 inet6 static
        address ::ffff:c0a8:840a
        prefix 64
```

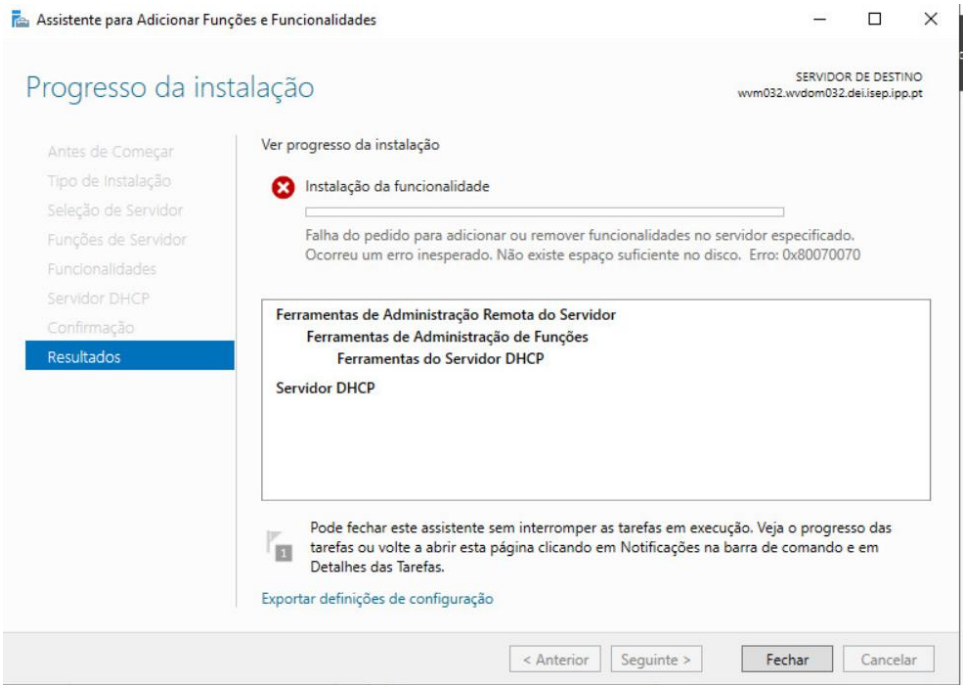
Figura 1 - Configuração interface ens33.

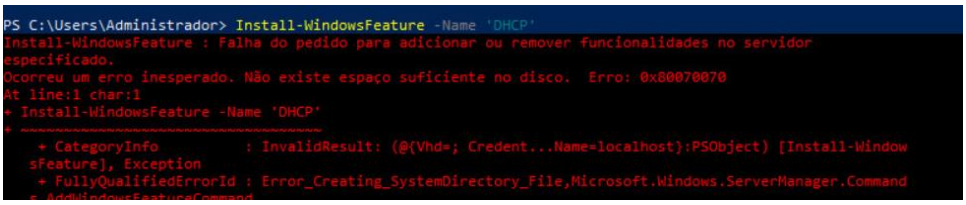
```
  GNU nano 5.4                          etc/default/isc-dhcp-server
# Defaults for isc-dhcp-server (sourced by /etc/init.d/isc-dhcp-server)

# Path to dhcpd's config file (default: /etc/dhcp/dhcpd.conf).
#DHCPDv4_CONF=/etc/dhcp/dhcpd.conf
#DHCPDv6_CONF=/etc/dhcp/dhcpd6.conf

# Path to dhcpd's PID file (default: /var/run/dhcpd.pid).
#DHCPDv4_PID=/var/run/dhcpd.pid
#DHCPDv6_PID=/var/run/dhcpd6.pid

# Additional options to start dhcpd with.
#       Don't use options -cf or -pf here; use DHCPD_CONF/ DHCPD_PID instead
#OPTIONS=""

# On what interfaces should the DHCP server (dhcpd) serve DHCP requests?
#       Separate multiple interfaces with spaces, e.g. "eth0 eth1".
INTERFACES="ens33"
```

Figura 2- Configuração ficheiro isc-dhcp-server

- WINDOWS

Neste Use Case, para a máquina Windows não foi possível fazer a configuração do DHCP pois a máquina virtual das aulas PL não suporta a instalação e também não tínhamos créditos suficientes para uma outra máquina Windows no servidor do DEI. Abaixo temos os prints do erro ao tentar a instalação por meio do assistente do servidor e do powershell:





II.2.2 UC22

II:2.3 UC23

II.2.4 UC24

II:2.5 UC25

II.2.6 UC26

O objetivo deste caso de uso é que os utilizadores listados em /etc/bad-guys estejam inibidos de entrar no sistema. Para tal criamos o ficheiro bad-guys em /etc onde serão colocados os ips dos utilizadores que não podem aceder ao sistema. De seguida criamos um script que corre quando um utilizador dá login e verifica se o ip dele não está no ficheiro.

Segue-se imagem ilustrativa do script criado.

```
 GNU nano 5.4                                rules_iptables.sh
#INIBIR ACESSO AO SISTEMA
iptables -P FORWARD DROP
for mac in $(cat /etc/badguys); do
iptables -A INPUT -m mac --mac-source $mac -j DROP
done
```

II:2.7 UC27

O objetivo deste caso de uso é que o utilizador ao conectar-se seja recebido com mensagens dinâmicas. Conseguimos implementar tais mensagens para o pós-login, mas não para o pré-login.

Para o pós-login, implementamos um script (/etc/login_greet.sh) que corre quando o utilizador consegue efetuar login na máquina, tal conseguimos, executando o script no ficheiro ~/.bash_profile. Seguem imagens ilustrativas.

```
 GNU nano 5.4                              /etc/login_greet.sh *
hour=$(date +"%H")
if [ $hour -gt 0 -a $hour -le 12 ]
then
        greet="Bom dia, $USER"
elif [ $hour -gt 12 -a $hour -le 18 ]
then
        greet="Boa tarde, $USER"
else
        greet="Boa noite, $USER"
fi


echo $greet
```

Figura 3- Script de boas-vindas após login

```
  GNU nano 5.4                                    .bash_profile
../etc/login_greet.sh
```

Figura 4-Ficheiro ~/.bash_profile

II.2.8 UC28

Para a realização deste caso de uso foi criado um script que especifica ao sistema para aceitar comunicação através do protocolo ICMP. Este é o mesmo script usado em outros UCs referentes à firewall do servidor Linux.

```
  GNU nano 5.4                              rules_iptables.sh
#INIBIR ACESSO AO SISTEMA
iptables -P FORWARD DROP
for mac in $(cat /etc/badguys); do
iptables -A INPUT -m mac --mac-source $mac -j DROP
done

#Accept icmp
iptables -A INPUT -p icmp -J ACCEPT
#ACCEPT HTTP
iptables -A INPUT -p tcp --dport 80 -m conntrack --ctstate NEW,ESTABLISHED -j ACCEPT
iptables -A OUTPUT -p tcp --sport 80 -m conntrack --ctstate ESTABLISHED -j ACCEPT
```

Parte III – Conclusão

III.1 Conclusão

Alguns dos casos de uso que não foram implementados, tais não o foram devido a problemas na instalação de packages necessários à sua implementação, como por exemplo no caso do comando iptables.

Referências