CURSO: Tecnologo em Sistemas para Internet - 4º período – Noturno

UNIDADE CURRICULAR: Sistemas Operacionais I - TURMA:

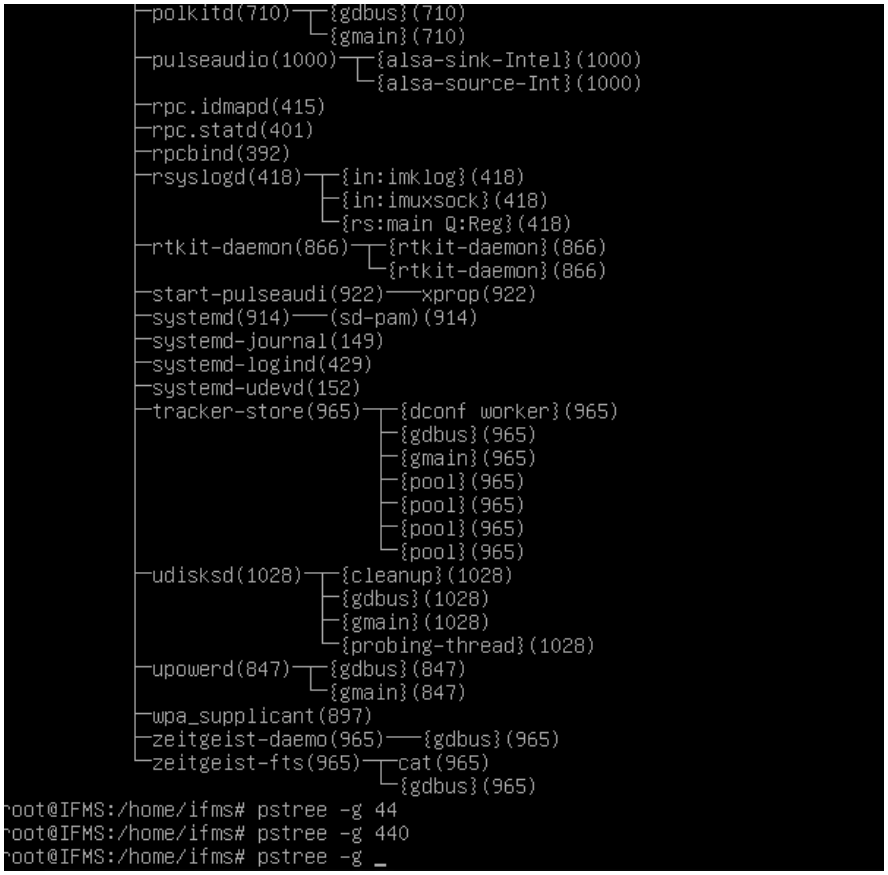
PROFESSOR: Genair C. Viana

Aula prática:

- Visualização do PID do sistema.
- Configuração do apt listas.
- Habilitação de roteamento e proteções do sistema.
- Configurando a rede com o Firewalls em ambientes Linux..

18/04/2023

Depois que o sistema Debian estiver instalado, para entender o que foi instalado e saber a estrutura dos processos digite **pstree -g** com os números do **(PID)** que ira mostrar a estrutura do Debian.



Configuração do apt listas

#vim /etc/apt/source.list

```
#

# deb cdrom:[Debian GNU/Linux 8.3.0 _Jessie_ - Official amd64 DVD Binary-1 20160123-19:03]/ jessie c
ontrib main

deb cdrom:[Debian GNU/Linux 8.3.0 _Jessie_ - Official amd64 DVD Binary-1 20160123-19:03]/ jessie con
trib main

deb http://security.debian.org/ jessie/updates main contrib
deb-src http://security.debian.org/ jessie/updates main contrib

# jessie-updates, previously known as 'volatile'
# A network mirror was not selected during install.  The following entries
# are provided as examples, but you should amend them as appropriate
# for your mirror of choice.
#
deb http://ftp.debian.org/debian/ jessie-updates main contrib
deb-src http://ftp.debian.org/debian/ jessie-updates main contrib
```

Atualizando o sistema

apt-get update

apt-get upgrade

Vamos começar a configurar o iptables, mas antes iremos habilitar roteamento e proteções do sistema Debian:

1- habilita roteamento no kernel

#echo 1 >/proc/sys/net/ipv4/ip_forward

2- protecao contra spoofing

#echo "1” >/proc/sys/net/ipv4/conf/all/rp_filter

3 - proteçao contra spoofing

echo 0 >/proc/sys/net/ipv4/conf/all/accept_source_route

echo 1 >/proc/sys/net/ipv4/tcp_syncookies

echo 1 >/proc/sys/net/ipv4/icmp_echo_ignore_broadcasts

echo 1 >/proc/sys/net/ipv4/icmp_ignore_bogus_error_responses

limpeza das tabelas do Iptables existentes

Vamos fazer uma limpeza nas tabelas do firewall para garantir que não fique nenhuma regras de **iptables**.

#iptables -F

#iptables -t mangle -F

#iptables -t nat -F

#iptables -X

Para ver as configurações do iptables digite:

#iptables -L

Vamos começar a configurar nossas regras de firewall

1 - Configuração da politica padrão do iptables

#iptables -P INPUT DROP

#iptables -P OUTPUT ACCEPT

#iptables -P FORWARD DROP

2 - Configuração das conexões preestabelecidas

#iptables -A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT

#iptables -A OUTPUT -m state --state ESTABLISHED,RELATED,NEW -j ACCEPT

#iptables -A FORWARD -m state --state ESTABLISHED,RELATED,NEW -j ACCEPT

3 – Configuração da liberação da interface loopback

#iptables -A INPUT -i lo -j ACCEPT

4 - Configuração do registro de logs

#iptables -A INPUT -p tcp --dport 333 --syn -j LOG --log-prefix="[TENTATIVA ACESSO FWLOGWATCH]"

#iptables -A INPUT -p tcp --dport 23 --syn -j LOG --log-prefix="[TENTATIVA ACESSO TELNET]"

#iptables -A INPUT -p tcp --dport 10000 --syn -j LOG --log-prefix="[TENTATIVA ACESSO WEBMIN]"

#iptables -A FORWARD -m multiport -p tcp --dport 5800,5900,6000 -j LOG --log-prefix="[ACESSO VNC]"

#iptables -A INPUT -p tcp --dport 22 --syn -j LOG --log-prefix="[TENTATIVA ACESSO SSH]"

#iptables -A INPUT -p tcp --dport 2222 --syn -j LOG --log-prefix="[TENTATIVA ACESSO SSH]"

#iptables -A INPUT -p tcp --dport 21 --syn -j LOG --log-prefix="[TENTATIVA ACESSO FTP]"

Configuração das regras de segurança

1 - Protege contra port scanners

#iptables -A INPUT -p tcp --tcp-flags SYN,ACK,FIN,RST RST -m limit --limit 5/s -j ACCEPT

2 - proteção contra traceroute "Vai depender das placas de rede e da configuração do SW"

#iptables -A INPUT -p udp -s 0/0 -i eth3 --dport 33435:33525 -j REJECT

3 - Protecoes contra pacotes inválidos

#iptables -A INPUT -m state --state INVALID -j REJECT

Configuração das regras de entrada(INPUT)

1 - liberando Servidor DNS

#iptables -A INPUT -p tcp --dport 53 -j ACCEPT

#iptables -A INPUT -p udp --dport 53 -j ACCEPT

2 - libera proxy squid pelo navegador

#iptables -A INPUT -s 192.168.0.0/24 -p tcp --dport 3128 -j ACCEPT

#iptables -A INPUT -s 192.168.1.0/24 -p tcp --dport 3128 -j ACCEPT

#iptables -A INPUT -s 192.168.2.0/24 -p tcp --dport 3128 -j ACCEPT

#iptables -A INPUT -s 192.168.3.0/24 -p tcp --dport 3128 -j ACCEPT

#iptables -A INPUT -s 192.168.4.0/24 -p tcp --dport 3128 -j ACCEPT

3 - libera ping para rede do Administrador do sistema

#iptables -A INPUT -s 192.168.1.0/24 -p icmp --icmp-type 8 -j ACCEPT

4 - libera ssh para o administrado e bloqueia todo o resto

#iptables -A INPUT -s 192.168.1.0/24 -p tcp --dport 22 -j ACCEPT

5 - libera ssh externamente para o administrador

#iptables -A INPUT -p tcp --dport 22 -j ACCEPT

6 - libera acesso ao WEBMIN para o administrador

#iptables -A INPUT -p tcp --dport 10000 -j ACCEPT

7 - libera acesso ao fwlogwatch para o administrador

#iptables -A INPUT -s 192.168.1.0/24 -p tcp --dport 333 -j ACCEPT

8 - bloqueia todo o resto

#iptables -A INPUT -p tcp --syn -j DROP

#iptables -A INPUT -p tcp -j DROP

Configuração das regras de VLANS e DMZ (FORWARD)

1 - libera portas ctvoicer

#iptables -A FORWARD -d 192.168.0.8/24 -p tcp -m multiport --dport 3050,10014,10010 -j ACCEPT

2 - liberado ping para rede ADM (qualquer destino)

#iptables -A FORWARD -s 192.168.1.0/24 -p icmp --icmp-type echo-request -j ACCEPT

#iptables -A FORWARD -s 192.168.1.0/24 -p icmp --icmp-type echo-reply -j ACCEPT

3 - libera portas rede para ADM

#iptables -A FORWARD -i eth0.10 -p tcp -m multiport --dport 53,137,138,139,110,25,22,2222,995,465,5800,5900,6000 -j ACCEPT

#iptables -A FORWARD -i eth0.10 -p udp -m multiport --dport 53,137,138,139,110,25,22,995,465 -j ACCEPT

4 - regras para o webserver

#iptables -A FORWARD -d 192.168.0.253/24 -p tcp -m multiport --dport 80,8080 -j ACCEPT

#iptables -A FORWARD -d 192.168.0.253/24 -p udp -m multiport --dport 80,8080 -j ACCEPT

#iptables -A FORWARD -s 192.168.1.0/24 -d 192.168.1.0/24 -p tcp -m multiport --dport 137,138,139 -j ACCEPT

#iptables -A FORWARD -s 192.168.1.0/24 -d 192.168.1.0/24 -p udp -m multiport --dport 137,138,139 -j ACCEPT

5 - regras para servidor de email

#iptables -A FORWARD -d 192.168.0.254/24 -p tcp -m multiport --dport 995,465,110,25,143 -j ACCEPT

#iptables -A FORWARD -d 192.168.0.254/24 -p udp -m multiport --dport 995,465,110,25,143 -j ACCEPT

6 - regras para o asterisk

#iptables -A FORWARD -d 192.168.0.250/24 -p tcp --dport 5060 -j ACCEPT

#iptables -A FORWARD -d 192.168.0.250/24 -p udp --dport 5060 -j ACCEPT

i#ptables -A FORWARD -d 192.168.0.250/24 -p udp --dport 10000:20000 -j ACCEPT

7 - regras para servidor samba

#iptables -A FORWARD -i eth0 -d 192.168.0.127/24 -p tcp -m multiport --dport 137,138,139 -j ACCEPT

#iptables -A FORWARD -i eth0 -d 192.168.0.127/24 -p udp -m multiport --dport 137,138,139 -j ACCEPT

8 - regras para serv-adm2

#iptables -A FORWARD -d 192.168.0.252/24 -p tcp --dport 3389 -j ACCEPT

#iptables -A FORWARD -d 192.168.0.252/24 -p udp --dport 3389 -j ACCEPT

9 - regras de forward para vnc para o administrador

#iptables -A FORWARD -s 192.168.1.0/24 -p tcp -m multiport --dport 5800,5900,6000 -j ACCEPT

Configuração das regras para redes NAT

1 - redirecionando acesso ao servidor VOIP

#iptables -t nat -A PREROUTING -d 200.195.YYY.YYY -j DNAT --to 192.168.0.250

2 - redirecionado pop e smtp

#iptables -t nat -A PREROUTING -d 200.195.ZZZ.ZZZ -p tcp -m tcp --dport 110 -j DNAT --to-destination 192.168.0.254:110

#iptables -t nat -A PREROUTING -d 200.195.ZZZ.ZZZ -p tcp -m tcp --dport 25 -j DNAT --to-destination 192.168.0.254:25

3 - redirecionando acesso ao servidor web via rede local e internet

#iptables -t nat -A PREROUTING -s 200.195.KKK.KKK -p tcp --dport 80 -j DNAT --to 192.168.0.253

4 - redireciona acesso terminal service para serv-adm

#iptables -t nat -A PREROUTING -d 200.195.ZZZ.ZZZ -p tcp --dport 3389 -j DNAT --to 192.168.0.252

5 - redireciona acesso vnc

#iptables -t nat -A PREROUTING -d 200.139.XXX.XXX -p tcp --dport 5900 -j DNAT --to 192.168.0.8

6 - acesso vnc Genair_IFMS

#iptables -t nat -A PREROUTING -d 200.139.XXX.XXX -p tcp --dport 6000 -j DNAT --to 192.168.1.2

7 - acesso vnc IFMS

#iptables -t nat -A PREROUTING -d 200.139.XXX.XXX -p tcp --dport 6001 -j DNAT --to 192.168.1.3

8 - ativando proxy transparente

#iptables -t nat -A PREROUTING -p tcp -s 192.168.0.0/24 --dport 80 -j REDIRECT --to-ports 3128

9 - ativando masquerade

#iptables -t nat -A POSTROUTING -p all -s 192.168.1.2 -o eth3 -j SNAT --to-source 200.139.XXX.XXX

10 - ativando SNAT

#iptables -t nat -A POSTROUTING -s 192.168.1.0/24 -m multiport -p tcp --dport 53,110,25,22,2222,995,465,5800, 5900,6000 -o eth3 -j SNAT --to-source 200.139.XXX.XXX

#iptables -t nat -A POSTROUTING -s 192.168.1.0/24 -m multiport -p udp --dport 53,110,25,22,995,465 -j SNAT --to-source 200.139.XXX.XXX

iptables -t nat -A POSTROUTING -s 192.168.1.0/24 -p icmp -o eth3 -j SNAT --to-source 200.139.XXX.XXX

Criando prioridades de pacotes na rede

#iptables -t mangle -A PREROUTING -p tcp --dport 5060 -j TOS --set-tos 16

#iptables -t mangle -A PREROUTING -p udp --dport 1000:20000 -j TOS --set-tos 8

#iptables -t mangle -A PREROUTING -p tcp --dport 80 -j TOS --set-tos 8

#iptables -t mangle -A PREROUTING -p udp --dport 80 -j TOS --set-tos 8

#iptables -t mangle -A OUTPUT -o eth3 -p tcp --dport 5060 -j TOS --set-tos 16

#iptables -t mangle -A OUTPUT -o eth3 -p udp --dport 10000:20000 -j TOS --set-tos 8

#iptables -t mangle -A OUTPUT -o eth3 -p tcp --dport 80 -j TOS --set-tos 8

#iptables -t mangle -A OUTPUT -o eth3 -p udp --dport 80 -j TOS --set-tos 8

Configuração e balanceamento dos links tipo o da “OI” e “gvt” realizado por serviços de internet

1 - link1 OI 120mb
2 - link2 gvt 200mb

#echo 10 link1 >>/etc/iproute2/rt_tables **“CRIA A PRIMEIRA TABELA”**

#echo 20 link2 >>/etc/iproute2/rt_tables **“CRIA SEGUNDA TABELA”**

#iptables -t mangle -A PREROUTING -p tcp --dport 443 -j MARK --set-mark 3

#iptables -t mangle -A PREROUTING -p tcp --dport 80 -j MARK --set-mark 3

#iptables -t mangle -A PREROUTING -p tcp --dport 5060 -j MARK --set-mark 3

#iptables -t mangle -A PREROUTING -p tcp --dport 21 -j MARK --set-mark 4

#iptables -t mangle -A PREROUTING -p tcp --dport 25 -j MARK --set-mark 4

#iptables -t mangle -A PREROUTING -p tcp --dport 110 -j MARK --set-mark 4

#iptables -t mangle -A PREROUTING -p tcp --dport 5800:6000 -j MARK --set-mark 4

#iptables -t mangle -A PREROUTING -p tcp --dport 3306 -j MARK --set-mark 4

#ip rule add fwmark 3 table link1 **“COPIA PARA TABELA 1 TODAS AS CONFIGURAÇOES TERMINADA EM 3”**

#ip rule add fwmark 4 table link2 **“COPIA PARA TABELA 2 TODAS AS CONFIGURAÇOES TERMINADA EM 4”**

#ip route add default via 200.195.XXX.XXX table link1 **“VOCÊ DETERMINA O IP”**

#ip route add default via 200.139.XXX.XXX table link2 **“VOCÊ DETERMINA O IP”**

Para ver as configurações do iptables digite:
#iptables -L

Salve com o comando **iptables-save > nome-do-arquivo**
Ex:
#iptables-save > tabela-de-regras

Você ira salvar essas configuração em um arquivo que você nomeou, e toda vez que o sistema for iniciado faça o seguinte **iptables-restore < nome-do-arquivo**
Ex:
iptables-restore < tabela-de-regras

Assim você ira carregar todas as configuração do iptables que foram feitas, ou pode ser instalado o pacote **iptables-persistente.**