

Universidade do Minho
Escola de Engenharia

Cibersegurança
ENGENHARIA DE TELECOMUNICAÇÕES E INFORMÁTICA
2021/2022

(Docente: Henrique Santos)

21 de maio de 2022

Trabalho Prático 5
IP Tables e IDS

Inês Barreira Marques – a84913@alunos.uminho.pt

José Carlos Peixoto Ferreira – a85497@alunos.uminho.pt

Rui Filipe Ribeiro Freitas – pg47639@alunos.uminho.pt

Marcos Alexandre Ferreira Martins – a84481@alunos.uminho.pt

Tiago João Pereira Ferreira – pg47692@alunos.uminho.pt

Índice

Introdução	5
Tarefa 1 – Firewall (Básico).....	6
1. Setup inicial do servidor	6
2. Setup inicial do cliente.....	12
3. Modificação da firewall pessoal	14
4. Regras de escrita.....	18
Tarefa 2 – Firewall (Avançado)	21
1. Virtual Lab.....	21
2. Impedir o acesso a um website	25
3. Agendamento das regras.....	28
4. Web Server público	30
5. Limitar o número de conexões.....	31
Tarefa 3 – NIDS (Básico)	33
1. Configuração do Suricata.....	33
2. Testes do Suricata.....	36
Tarefa 4 – NIDS (Avançado)	38
1. Testes Suricata utilizando ferramentas de rastreamento	38
2. Utilização da ferramenta Pytbull	44
Tarefa 5 – NIDS (Complementar)	46

Índice de figuras

Figura 1 - Instalação do serviço FTP.	6
Figura 2 - Ativação e inicialização dos serviços desejados.	6
Figura 3 - Comprovativo que os serviços estão ativos.	7
Figura 4 - Página exemplo do servidor HTTP.	7
Figura 5 - Página exemplo do servidor FTP.	8
Figura 6 - Teste do serviço FTP.	8
Figura 7 - Teste do serviço SSH.	8
Figura 8 - Janela do comando "system-config-firewall-tui".	9
Figura 9 - Políticas da firewall.	9
Figura 10 - Criação do ficheiro backup da firewall.	11
Figura 11 - Realização do comando "iptables -L -v" após desativação.	11
Figura 12 - Teste de conectividade.	12
Figura 13 - Configuração da firewall.	14
Figura 14 - Realização do comando iptables.	14
Figura 15 - Teste de conectividade.	15
Figura 16 - Resultado do comando w3m.	15
Figura 17 - Resultado do comando ftp.	16
Figura 18 - Resultado do comando nmap -sS.	16
Figura 19 - Teste de conectividade.	17
Figura 20 - Resultado do comando iptables -L -v.	17
Figura 21 - Apagar e guardar as iptables.	18
Figura 22 - DROP em todas as tabelas.	18
Figura 23 - Adição das regras TCP.	19
Figura 24 - Adição da regra da interface loopback.	19
Figura 25 - Regras para o DHCP e DNS.	19
Figura 26 - Regras dos serviços fundamentais.	20
Figura 27 - Execução do iptables-restore.	20
Figura 28 - Máquina virtual com pfSense.	21
Figura 29 - Atribuição do IP do cliente 2.	21
Figura 30 - Atribuição do IP do cliente 1.	21
Figura 31 - Teste de conectividade.	22
Figura 32 - Pesquisa pelo IP da LAN no browser.	22
Figura 33 - Acesso ao pfSense através do browser.	23
Figura 34 - Regras da interface WAN.	23
Figura 35 - Regras da interface LAN.	24
Figura 36 - Regras da firewall.	24
Figura 37 - Obtenção do IP do domínio facebook.com.	25
Figura 38 - Conexão com sucesso a facebook.com.	25
Figura 39 - Acesso recusado a facebook.com.	26
Figura 40 - Regra criada e tráfego que passa.	26
Figura 41 - Regra editada e o tráfego que passa.	27

Figura 42 - Regra editada para só 1 IP.....	27
Figura 43 - Logs da firewall do sistema.	28
Figura 44 - Agendamento da regra da firewall.....	28
Figura 45 - Agendamento da regra da firewall.....	29
Figura 46 - Logs da firewall.	29
Figura 47 - Implementação da regra NAT.	30
Figura 48 - Acesso à página inicial do servidor interno.	30
Figura 49 - Realização do comando nping.....	31
Figura 50 - Análise no Wireshark.....	31
Figura 51 - Alteração da regra NAT.	32
Figura 52 - Teste de 30 conexões a 30 conexões/s.	32
Figura 53 - Instalação do pacote Suricata.	33
Figura 54 - Configuração do Suricata.	33
Figura 55 - Atualização das regras do Suricata.....	34
Figura 56 - Adição do conjunto de regras.	34
Figura 57 - Ativação das regras.....	35
Figura 58 - Ativação da monitorização das interfaces.	35
Figura 59 - Avisos do sistema.	36
Figura 60 - Operação de "name resolution".....	37
Figura 61 - Criação da lista de supressão.	37
Figura 62 - Dashboard organizado.....	38
Figura 63 - Realização do comando nmap -PS -v.....	38
Figura 64 - Dashboard momentos após o teste nmap.	39
Figura 65 - Realização do comando nmap -sS -v.	39
Figura 66 - Análise do tráfego no Wireshark.....	40
Figura 67 - Teste nmap com os argumentos -A e -v.....	40
Figura 68 - Alertas da realização do nmap.	41
Figura 69 - Teste com a ferramenta hping3.....	42
Figura 70 - Ecrã do dashboard aquando da realização do comando.	42
Figura 71 - Realização do comando hping3 -S --flood --rand-source.....	43
Figura 72 - Visualização do dashboard.	43
Figura 73 - Ficheiro de configuração do pytbull.	44
Figura 74 - Relização do comando ./pytbull -t 10.1.1.2.	45
Figura 75 - Instalação da ferramenta ELK.	46
Figura 76 - Configuração do ficheiro kibana.yml.....	46
Figura 77 - Ficheiro de configuração 01-inputs.conf.....	47
Figura 78 - Ficheiro de configuração 30-outputs.conf.	47
Figura 79 Configuração automática dos serviços.....	47
Figura 80 - Acesso aos serviços iniciados.	47

Introdução

No âmbito da realização do trabalho prático número 5, proposto na unidade curricular de Cibersegurança, serve o presente relatório para demonstrar os resultados da elaboração do mesmo. Este trabalho corresponde a uma série de passos que foram seguidos e a obtenção e documentação dos resultados obtidos da utilização de firewalls e IDSs.

Tarefa 1 – Firewall (Básico)

1. Setup inicial do servidor

Primeiro foi necessário fazer o download da imagem CentOS 6.10 e realizar a instalação na plataforma VMWare. Com a máquina virtual criada foi necessário aceder a “System -> Administration -> Add/Remove Software” de modo a instalar o serviço FTP. De seguida é demonstrado como foi realizada esta instalação.

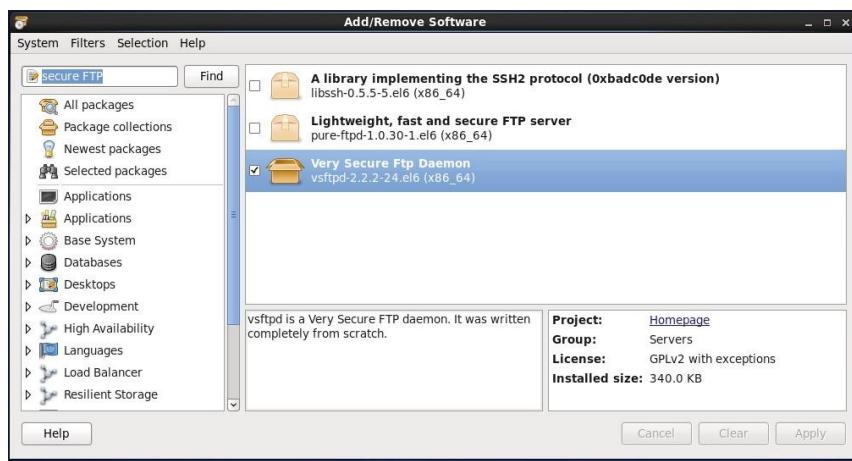


Figura 1 - Instalação do serviço FTP.

Após realizada a instalação do serviço FTP foi necessário ativar e inicializar os serviços desejados, como por exemplo o “httpd”, “sshd” e “vsftpd”. Isto foi realizado através do menu “System -> Administration -> Services”. O comprovativo de que estes serviços foram ativados e iniciados com sucesso estão representados na figura seguinte.

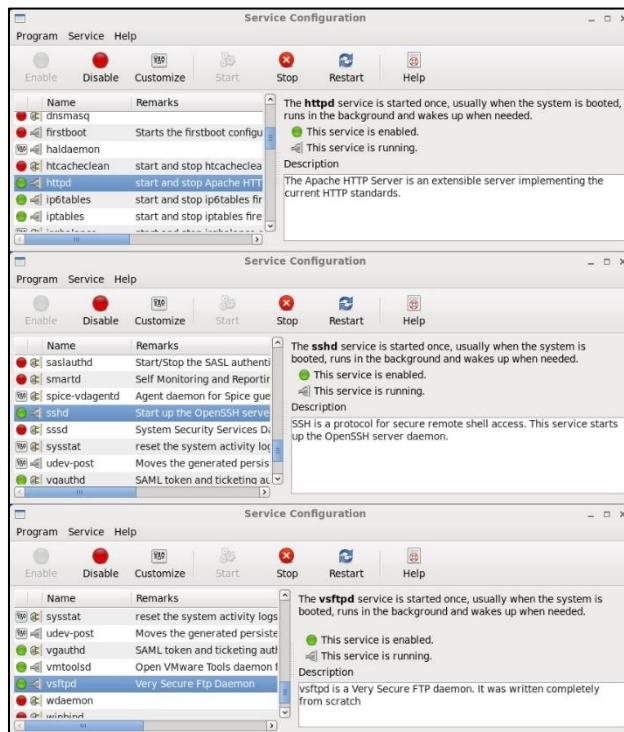


Figura 2 - Ativação e inicialização dos serviços desejados.

De modo a comprovar que os serviços estão devidamente inicializados e disponíveis foi necessário realizar o comando da imagem seguinte.

```
[centos@centos6 Desktop]$ netstat -l | grep "tcp"
tcp      0      0 *:ftp          *:*                  LISTEN
tcp      0      0 *:42933       *:*                  LISTEN
tcp      0      0 *:ssh          *:*                  LISTEN
tcp      0      0 localhost:ipp  *:*                  LISTEN
tcp      0      0 localhost:smtp *:*                  LISTEN
tcp      0      0 *:sunrpc       *:*                  LISTEN
tcp      0      0 *:http         *:*                  LISTEN
tcp      0      0 *:ssh          *:*                  LISTEN
tcp      0      0 localhost:ipp  *:*                  LISTEN
tcp      0      0 localhost:smtp *:*                  LISTEN
tcp      0      0 *:54654        *:*                  LISTEN
tcp      0      0 *:sunrpc       *:*                  LISTEN
[centos@centos6 Desktop]$
```

Figura 3 - Comprovativo que os serviços estão ativos.

Na figura acima é possível observar que os serviços estão disponíveis, pois estes estão listados como “LISTEN”. Posteriormente foi acedido ao Mozilla Firefox, uma ferramenta pré-instalada do CentOS, que nos permitiu aceder ao servidor HTTP como se pode na figura 4. Na figura abaixo está apresentada uma página HTTP exemplo definida automaticamente pelo CentOS.

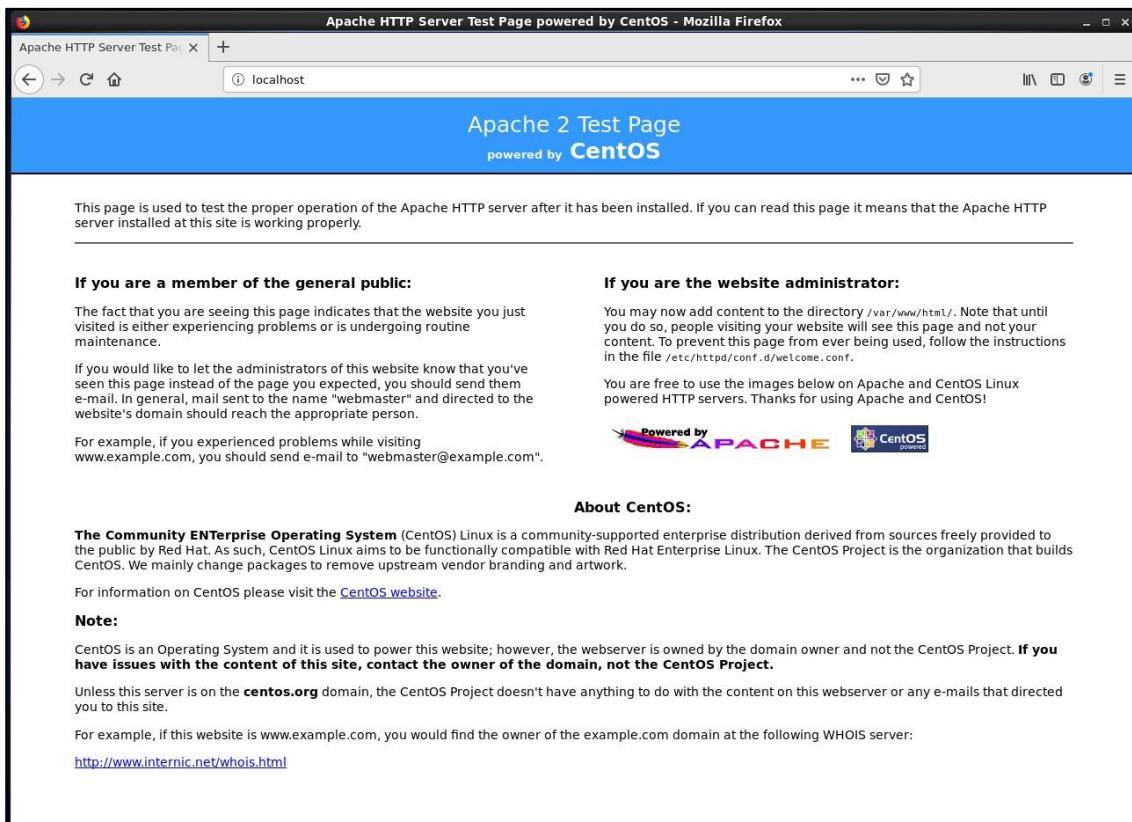


Figura 4 - Página exemplo do servidor HTTP.

Para testar o correto funcionamento do serviço FTP foi utilizado o mesmo *browser*, alterando apenas a barra de pesquisa para obter os conteúdos FTP ao invés dos conteúdos HTTP. O resultado desta pesquisa é a apresentada de seguida.



Figura 5 - Página exemplo do servidor FTP.

Por fim, foi acedido à linha de comandos para obter mais algumas informações sobre o funcionamento do servidor FTP assim como do serviço SSH. Estas informações são apresentadas a seguir.

```
root@centos6:/home/centos/Desktop
File Edit View Search Terminal Help
[root@centos6 Desktop]# ftp 127.0.0.1
Connected to 127.0.0.1 (127.0.0.1).
220 (vsFTPd 2.2.2)
Name (127.0.0.1:root): anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
227 Entering Passive Mode (127,0,0,1,184,104).
150 Here comes the directory listing.
drwxr-xr-x 2 0 0 4096 Mar 22 2017 pub
226 Directory send OK.
ftp> quit
221 Goodbye.
[root@centos6 Desktop]#
```

Figura 6 - Teste do serviço FTP.

```
root@centos6:/home/centos/Desktop
File Edit View Search Terminal Help
[root@centos6 Desktop]# ssh 127.0.0.1
The authenticity of host '127.0.0.1 (127.0.0.1)' can't be established.
RSA key fingerprint is a1:64:f6:5b:a8:ff:3b:bc:d5:f3:54:96:b6:54:dc:c6.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '127.0.0.1' (RSA) to the list of known hosts.
+-----+
L I N U X V M I M A G E S . C O M
+-----+
User Name: centos
Password: centos (sudo su -)
root@127.0.0.1's password:
Last login: Sat May 14 13:41:34 2022 from localhost
+-----+
L I N U X V M I M A G E S . C O M
+-----+
User Name: centos
Password: centos (sudo su -)
[root@centos6 ~]# ls
anaconda-ks.cfg install.log install.log.syslog
[root@centos6 ~]# exit
logout
Connection to 127.0.0.1 closed.
[root@centos6 Desktop]#
```

Figura 7 - Teste do serviço SSH.

Após realizadas as instalações e ativações dos serviços necessários foi ativada a *firewall* de uma forma simples utilizando iptables através do comando “system-config-firewall-tui”. Foi apresentada uma janela como demonstrada na figura seguinte.

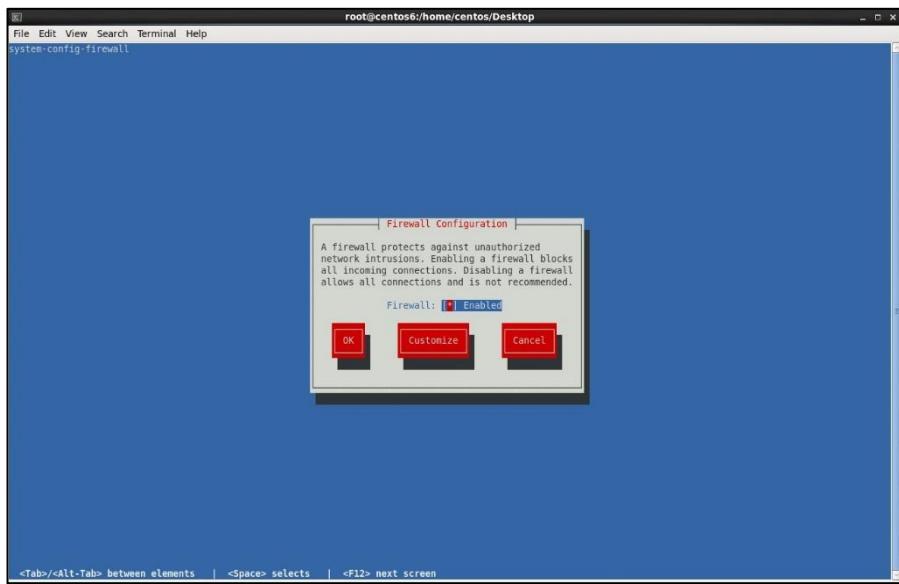


Figura 8 - Janela do comando "system-config-firewall-tui".

Da observação da figura anterior é possível observar que a *firewall* já estava ativa por *default* sendo que não foi necessário realizar qualquer configuração.

Com a firewall ativa, foi realizado o comando “iptables -L -v” cujo output foi o seguinte:

```
root@centos6:~# iptables -L -v
Chain INPUT (policy ACCEPT 0 packets, 0 bytes)
pkts bytes target  prot opt in     out    source          destination
  0   0 ACCEPT   all  --  any    any    anywhere       anywhere        state RELATED,ESTABLISHED
  0   0 ACCEPT   icmp --  any    any    anywhere       anywhere
  0   0 ACCEPT   all  --  lo     any    anywhere       anywhere
  0   0 ACCEPT   tcp  --  any    any    anywhere       anywhere        state NEW tcp dpt:ssh
  0   0 REJECT   all  --  any    any    anywhere       anywhere        reject-with icmp-host-prohibited

Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
pkts bytes target  prot opt in     out    source          destination
  0   0 REJECT   all  --  any    any    anywhere       anywhere        reject-with icmp-host-prohibited

Chain OUTPUT (policy ACCEPT 0 packets, 0 bytes)
pkts bytes target  prot opt in     out    source          destination
[root@centos6 ~]#
```

Figura 9 - Políticas da firewall.

Na figura 9 é possível observar as políticas definidas pela firewall. Através da análise da figura é possível concluir que a firewall rejeita todos os pedidos que chegam ao servidor para aceder a qualquer serviço, exceto os serviços SSH e ICMP. De seguida são apresentadas as regras para cada cadeia de uma forma mais específica.

INPUT (Tráfego destinado ao IP em questão): -

- É possível observar que o tráfego ICMP é aceite, tráfego este que corresponde aos *pings* utilizados numa rede, sendo assim é possível realizar esta troca de pacotes entre cliente e servidor;
- Para além do serviço ICMP é pode observar-se que também todo o tráfego sob o serviço SSH, através do protocolo TCP é permitido e aceite;
- Para todos os outros serviços é rejeitado qualquer tráfego, sendo enviado aquando desse pedido, uma mensagem de rejeição.

FORWARD (Tráfego que não se destina ao IP, mas que passa por ele): -

- Com a observação da figura é possível verificar que todo o tráfego que chega ao PC com o objetivo de ser reencaminhado é rejeitado não sendo então possível utilizar este PC como um elemento de um processo de *routing* visto que todo o tráfego é descartado.

OUTPUT (Tráfego proveniente do IP em questão): -

- Relativamente ao tráfego de saída do PC não é adicionado qualquer restrição em fazer pedidos de qualquer serviço.

Relativamente à complexidade desta firewall é possível dizer que se trata de uma firewall bastante básica cujas políticas são igualmente básicas, estas devem estar presentes independentemente do dispositivo. Se fosse pretendido realizar políticas mais restritas seria necessário aceder à firewall e adicionar manualmente as políticas que seriam mais adequadas.

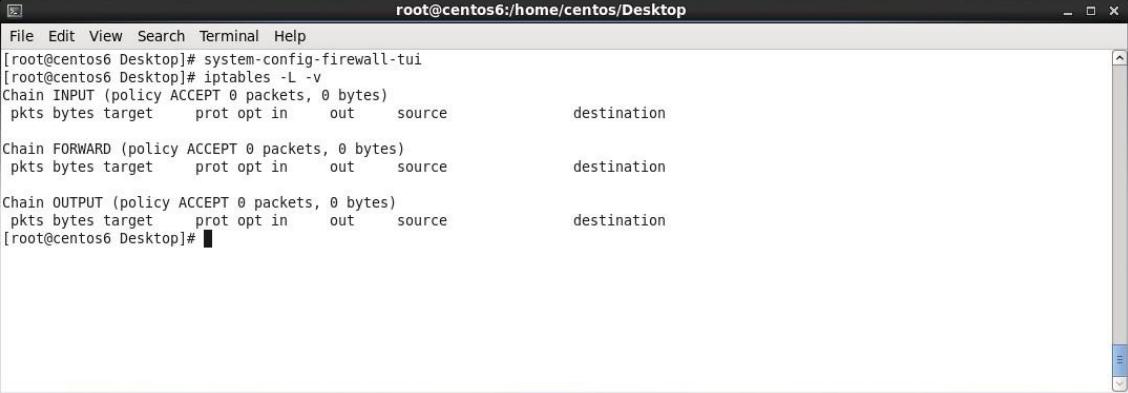
Por razões de segurança foi realizado o comando demonstrado na figura seguinte com o objetivo de na eventualidade de ocorrer um problema futuro na configuração da *firewall*, seja possível usar o ficheiro criado como *backup*.



```
root@centos6:/home/centos/Desktop
File Edit View Search Terminal Help
[root@centos6 Desktop]# iptables-save > iptables.dump
[root@centos6 Desktop]# ls
iptables.dump
[root@centos6 Desktop]# cat iptables.dump
# Generated by iptables-save v1.4.7 on Sat May 14 15:26:24 2022
*filter
:INPUT ACCEPT [0:0]
:FORWARD ACCEPT [0:0]
:OUTPUT ACCEPT [198:14834]
-A INPUT -m state --state RELATED,ESTABLISHED -j ACCEPT
-A INPUT -p icmp -j ACCEPT
-A INPUT -i lo -j ACCEPT
-A INPUT -p tcp -m state --state NEW -dport 22 -j ACCEPT
-A INPUT -j REJECT --reject-with icmp-host-prohibited
-A FORWARD -j REJECT --reject-with icmp-host-prohibited
COMMIT
# Completed on Sat May 14 15:26:24 2022
[root@centos6 Desktop]#
```

Figura 10 - Criação do ficheiro backup da firewall.

Guardada a configuração da *firewall*, foi então necessário realizar a sua desativação de modo a perceber a influência desta. O resultado é apresentado a seguir.



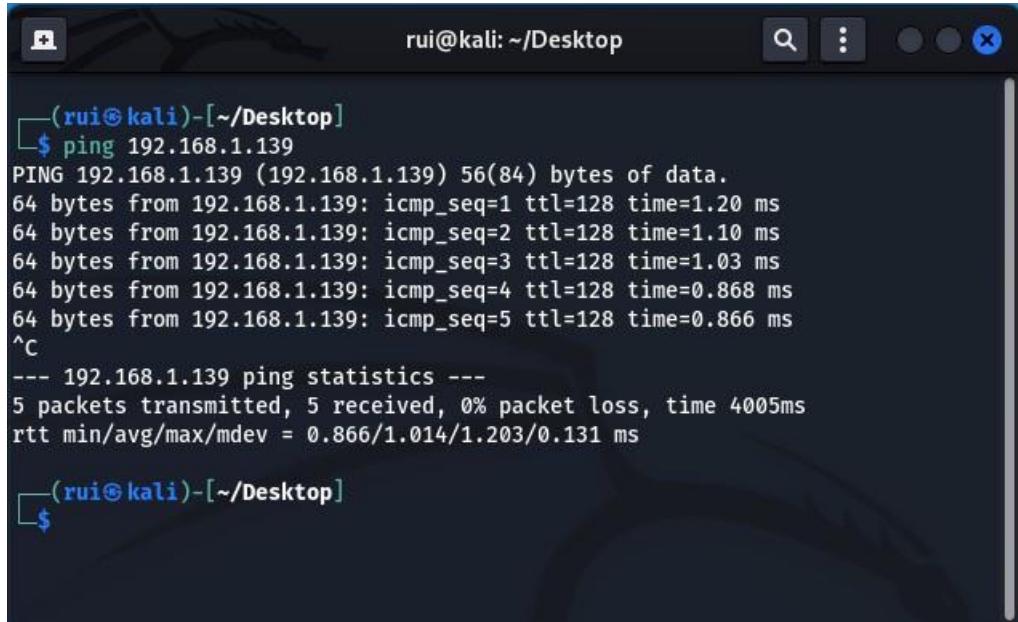
```
root@centos6:/home/centos/Desktop
File Edit View Search Terminal Help
[root@centos6 Desktop]# system-config-firewall-tui
[root@centos6 Desktop]# iptables -L -v
Chain INPUT (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination
Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination
Chain OUTPUT (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination
[root@centos6 Desktop]#
```

Figura 11 - Realização do comando "iptables -L -v" após desativação.

Após realizada a desativação das regras da *firewall* podemos ver que todo o tráfego relativo a qualquer serviço não é rejeitado sendo que a utilização destas políticas não é de todo segura. A não utilização das políticas da *firewall* implica que todo e qualquer tráfego possa entrar, passar e sair sem qualquer tipo de controlo, tornando o PC um alvo fácil a ataques informáticos. Em seguida foi realizada novamente a ativação da *firewall* com as políticas *default*.

2. Setup inicial do cliente

O grupo começou por instalar o Kali Linux no VMWare e realizou a sua configuração. Após a ativação da máquina virtual do servidor, usou-se o comando *ping* a partir do cliente para o servidor, de modo a comprovar a conectividade. O resultado do comando *ping* é apresentado na figura abaixo.



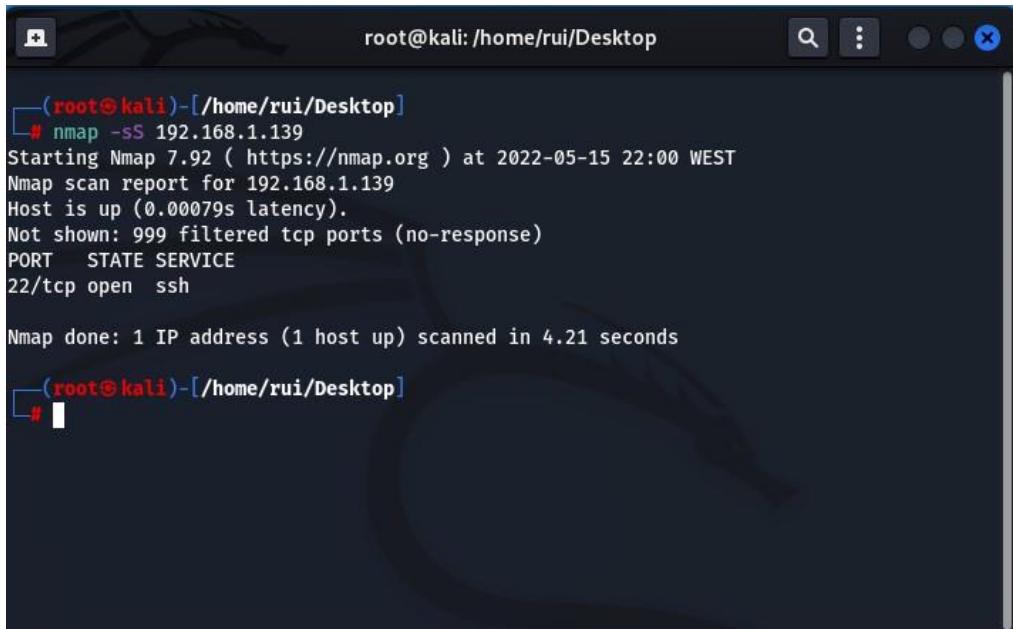
A terminal window titled "rui@kali: ~/Desktop". The user runs the command \$ ping 192.168.1.139. The output shows five successful ping requests to the IP address 192.168.1.139, with round-trip times ranging from 0.866 ms to 1.20 ms. After the pings, the user types ^C to stop the process. The terminal then displays ping statistics: 5 packets transmitted, 5 received, 0% packet loss, and a minimum/average/max/mdev of 0.866/1.014/1.203/0.131 ms.

```
(rui㉿kali)-[~/Desktop]
$ ping 192.168.1.139
PING 192.168.1.139 (192.168.1.139) 56(84) bytes of data.
64 bytes from 192.168.1.139: icmp_seq=1 ttl=128 time=1.20 ms
64 bytes from 192.168.1.139: icmp_seq=2 ttl=128 time=1.10 ms
64 bytes from 192.168.1.139: icmp_seq=3 ttl=128 time=1.03 ms
64 bytes from 192.168.1.139: icmp_seq=4 ttl=128 time=0.868 ms
64 bytes from 192.168.1.139: icmp_seq=5 ttl=128 time=0.866 ms
^C
--- 192.168.1.139 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4005ms
rtt min/avg/max/mdev = 0.866/1.014/1.203/0.131 ms

(rui㉿kali)-[~/Desktop]
```

Figura 12 - Teste de conectividade.

Ao usar o comando *nmap*, foi possível ver que o host se encontra ativo e que a porta 22/tcp se encontra aberta.



A terminal window titled "root@kali: /home/rui/Desktop". The user runs the command # nmap -sS 192.168.1.139. The output shows an Nmap scan report for the IP address 192.168.1.139. The host is found to be up with 0.00079s latency. A table lists the open ports: port 22/tcp is open and identified as ssh. The scan took 4.21 seconds.

```
(root㉿kali)-[/home/rui/Desktop]
# nmap -sS 192.168.1.139
Starting Nmap 7.92 ( https://nmap.org ) at 2022-05-15 22:00 WEST
Nmap scan report for 192.168.1.139
Host is up (0.00079s latency).
Not shown: 999 filtered tcp ports (no-response)
PORT      STATE SERVICE
22/tcp    open  ssh

Nmap done: 1 IP address (1 host up) scanned in 4.21 seconds

(root㉿kali)-[/home/rui/Desktop]
```

Figura 13 - Resultado do comando nmap -sS.

De seguida, foi pedido que fosse aplicado o comando *w3m*, no entanto, não foi possível obter uma resposta, como se pode verificar na figura abaixo.

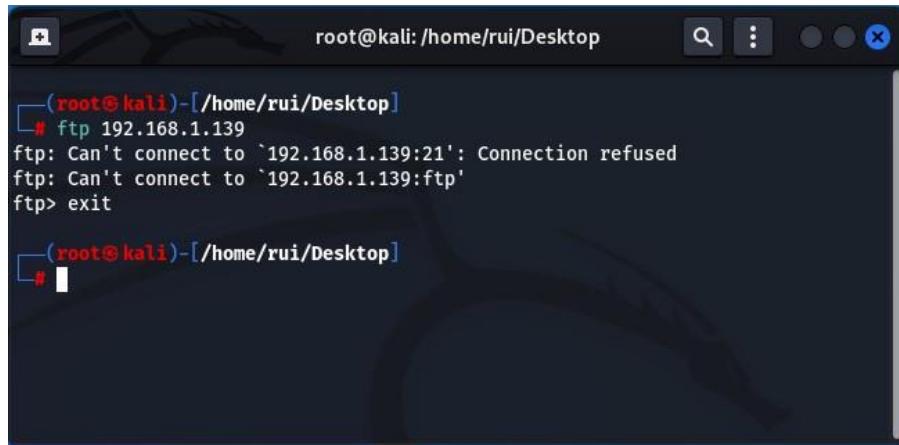


```
root@kali:~/Desktop]
# w3m http://192.168.1.139
w3m: Can't load http://192.168.1.139.

[~]
```

Figura 14 - Resultado do comando *w3m*.

Quando usado o comando *FTP*, a conexão é recusada, tal como se pode verificar na imagem abaixo.

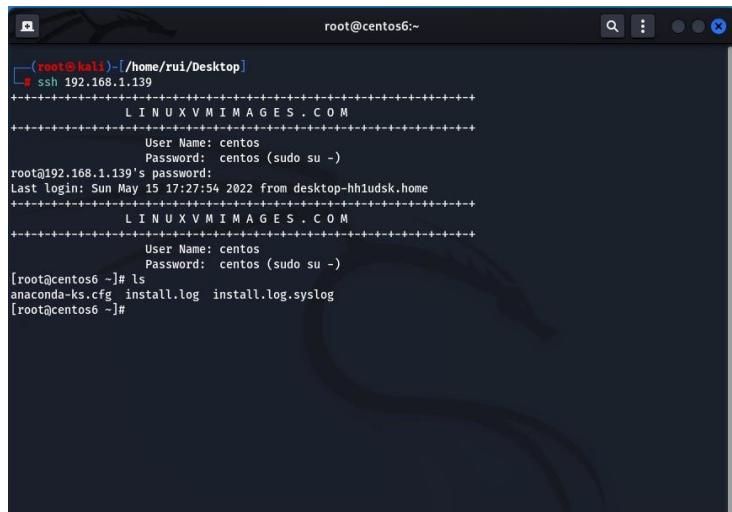


```
root@kali:~/Desktop]
# ftp 192.168.1.139
ftp: Can't connect to `192.168.1.139:21': Connection refused
ftp: Can't connect to `192.168.1.139:ftp'
ftp> exit

[~]
```

Figura 15 - Resultado do comando *ftp*.

Ao usar o comando *ssh*, verificou-se que a conexão era possível como se pode ver na figura 15.



```
root@kali:~/Desktop]
# ssh 192.168.1.139
+-----+
| L I N U X V M I M A G E S . C O M |
+-----+
User Name: centos
Password: centos (sudo su -)
root@192.168.1.139's password:
Last login: Sun May 15 17:27:54 2022 from desktop-1h1udsk.home
+-----+
| L I N U X V M I M A G E S . C O M |
+-----+
User Name: centos
Password: centos (sudo su -)
[root@centos6 ~]# ls
anaconda-ks.cfg install.log install.log.syslog
[root@centos6 ~]#
```

Figura 15 - Resultado do comando *ssh*.

3. Modificação da firewall pessoal

Voltando ao servidor foi realizada uma configuração mais profunda da firewall através do comando *system-config-firewall-tui*. De seguida é apresentada a configuração desta com a adição dos serviços confiáveis como o **FTP**, **SSH** e **HTTPS**. Para além disso é possível observar o filtro ICMP onde foi filtrado o **Echo Request (ping)**.

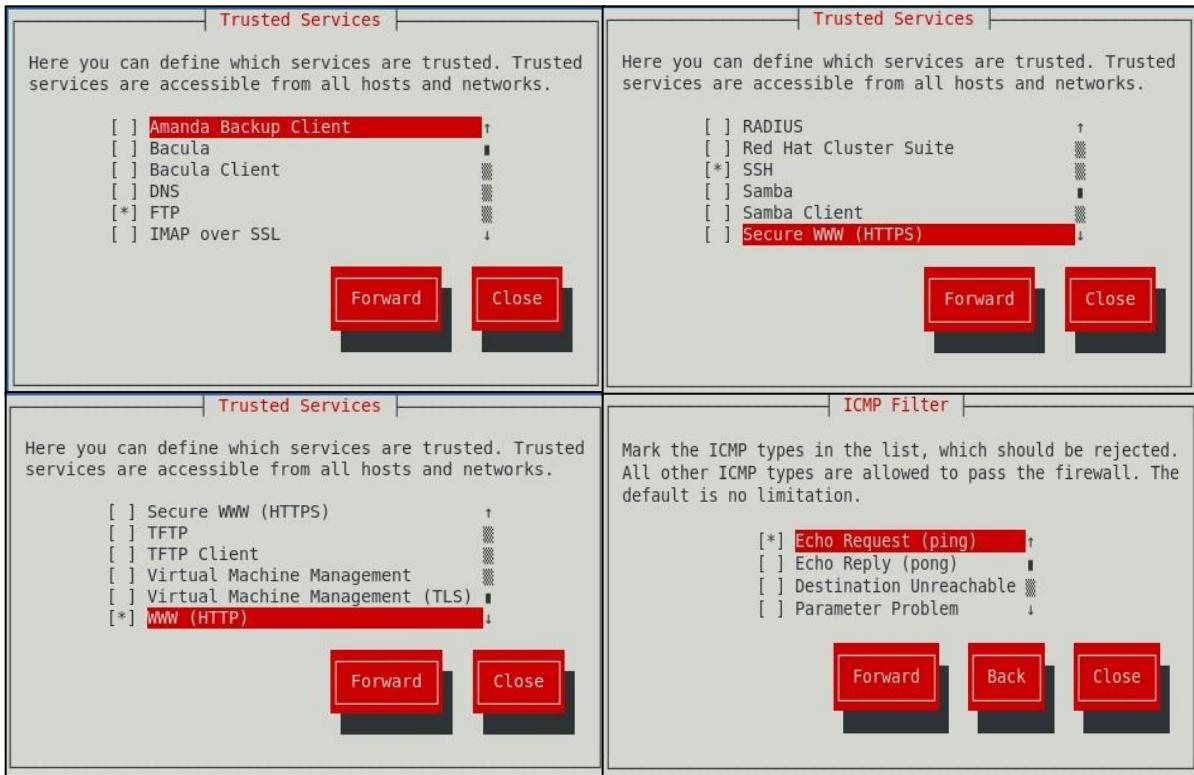


Figura 13 - Configuração da firewall.

Após a configuração da *firewall* foi realizado o comando *iptables* novamente com o resultado apresentado de seguida.

```
root@centos6:~# system-config-firewall-tui
[root@centos6 ~]# iptables -L -v
Chain INPUT (policy ACCEPT 0 packets, 0 bytes)
pkts bytes target  prot opt in  out source      destination
  2 152 ACCEPT  all --  any   any   anywhere    anywhere      state RELATED,ESTABLISHED
  2 168 REJECT  icmp --  any   any   anywhere    anywhere      icmp echo-request reject-with icmp-host-prohibited
  0  0 ACCEPT  icmp --  any   any   anywhere    anywhere
  0  0 ACCEPT  all --  lo    any   anywhere    anywhere
  0  0 ACCEPT  tcp --  any   any   anywhere    anywhere      state NEW tcp dpt:ssh
  0  0 ACCEPT  tcp --  any   any   anywhere    anywhere      state NEW tcp dpt:http
  0  0 ACCEPT  tcp --  any   any   anywhere    anywhere      state NEW tcp dpt:ftp
  1  32 REJECT  all --  any   any   anywhere    anywhere      reject-with icmp-host-prohibited

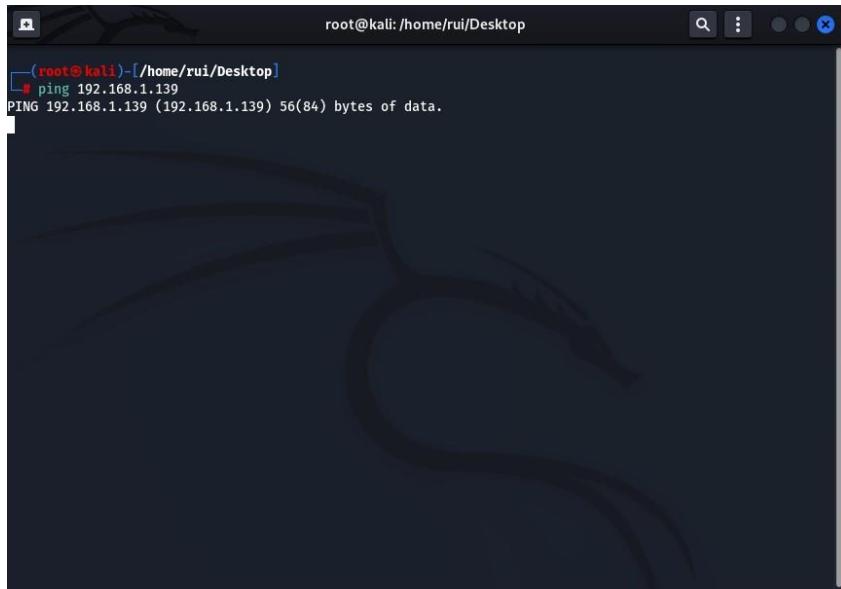
Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
pkts bytes target  prot opt in  out source      destination
  0  0 REJECT  all --  any   any   anywhere    anywhere      reject-with icmp-host-prohibited

Chain OUTPUT (policy ACCEPT 4 packets, 376 bytes)
pkts bytes target  prot opt in  out source      destination
[root@centos6 ~]#
```

Figura 14 - Realização do comando *iptables*.

É possível observar que foram adicionadas novas regras na configuração da *firewall* como pretendido, onde é possível constatar que o tráfego relativo aos serviços *ssh*, *http* e *ftp* é aceite e o tráfego *icmp host* é rejeitado.

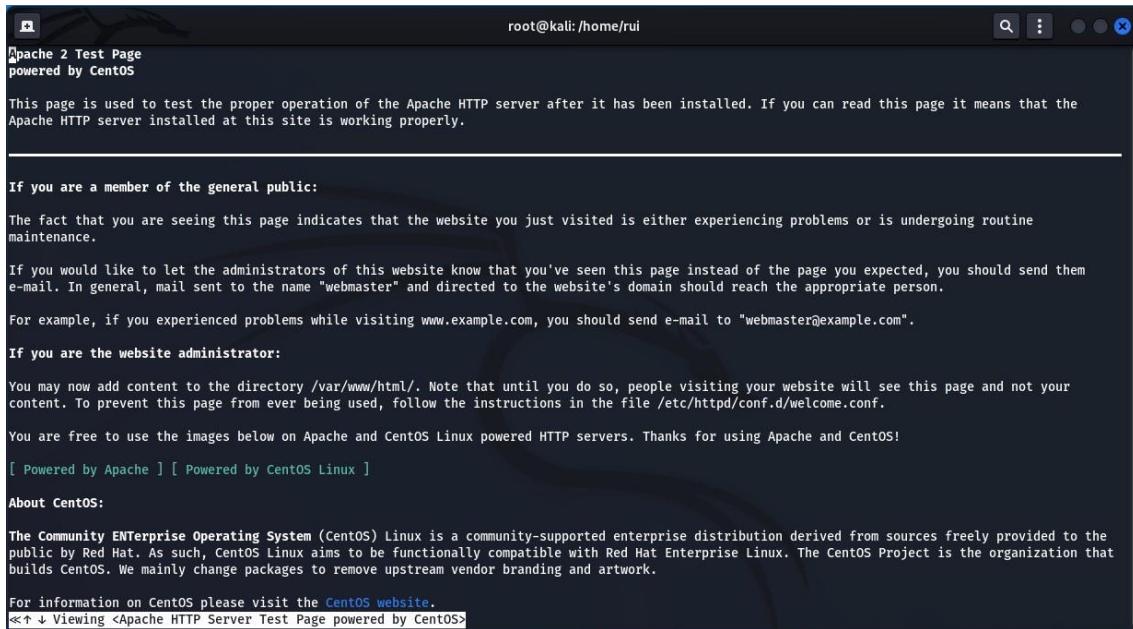
Voltando ao lado do cliente, foi realizado um teste de conectividade para o *ip* do servidor, onde não foi obtida qualquer resposta. Isto era expectável, pois o tráfego ICMP que é utilizado na realização de *pings* foi configurado para ser rejeitado.



```
root@kali:~/home/rui/Desktop
└─[root@kali]─[~/home/rui/Desktop]
# ping 192.168.1.139
PING 192.168.1.139 (192.168.1.139) 56(84) bytes of data.
```

Figura 15 - Teste de conectividade.

Realizando novamente o comando *w3m* é possível observar o conteúdo da página HTTP, isto acontece porque foi configurada a *firewall* para permitir o tráfego proveniente deste serviço.



The screenshot shows a terminal window with the title "root@kali:~/home/rui". The command "w3m" was run, and the output is a web page titled "Apache 2 Test Page powered by CentOS". The page content includes instructions for testing the Apache server's proper operation and information for website administrators. It also contains links to the Apache and CentOS websites and a brief history of CentOS.

```
root@kali:~/home/rui
Apache 2 Test Page
powered by CentOS

This page is used to test the proper operation of the Apache HTTP server after it has been installed. If you can read this page it means that the Apache HTTP server installed at this site is working properly.

If you are a member of the general public:
The fact that you are seeing this page indicates that the website you just visited is either experiencing problems or is undergoing routine maintenance.

If you would like to let the administrators of this website know that you've seen this page instead of the page you expected, you should send them e-mail. In general, mail sent to the name "webmaster" and directed to the website's domain should reach the appropriate person.

For example, if you experienced problems while visiting www.example.com, you should send e-mail to "webmaster@example.com".

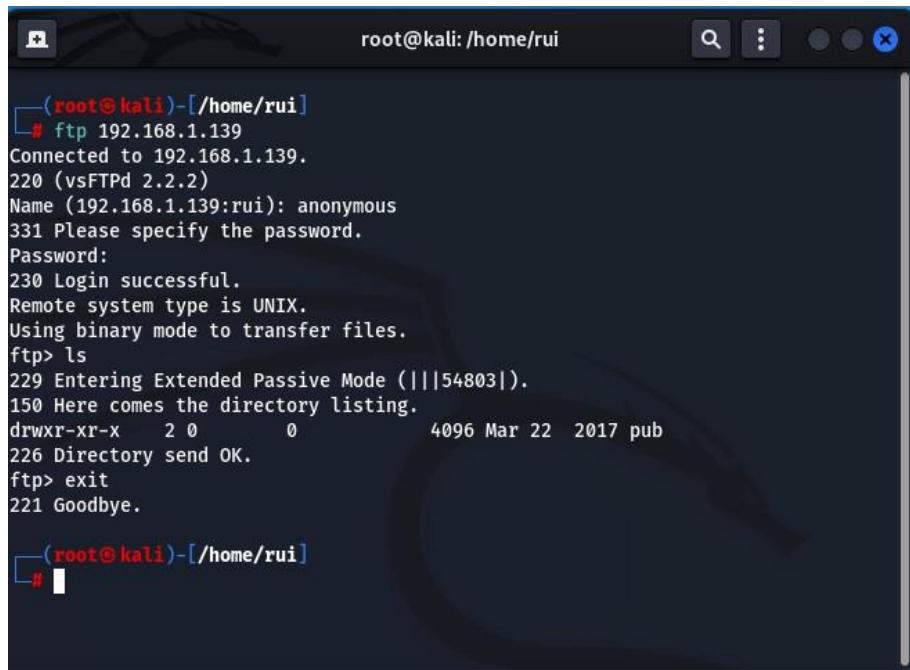
If you are the website administrator:
You may now add content to the directory /var/www/html/. Note that until you do so, people visiting your website will see this page and not your content. To prevent this page from ever being used, follow the instructions in the file /etc/httpd/conf.d/welcome.conf.

You are free to use the images below on Apache and CentOS Linux powered HTTP servers. Thanks for using Apache and CentOS!
[ Powered by Apache ] [ Powered by CentOS Linux ]
About CentOS:
The Community Enterprise Operating System (CentOS) Linux is a community-supported enterprise distribution derived from sources freely provided to the public by Red Hat. As such, CentOS Linux aims to be functionally compatible with Red Hat Enterprise Linux. The CentOS Project is the organization that builds CentOS. We mainly change packages to remove upstream vendor branding and artwork.

For information on CentOS please visit the CentOS website.
<<↑ Viewing <Apache HTTP Server Test Page powered by CentOS>
```

Figura 16 - Resultado do comando *w3m*.

Através do comando *ftp*, desta vez foi possível obter resposta, isto dado que a *firewall* foi configurada para permitir este tipo de tráfego.

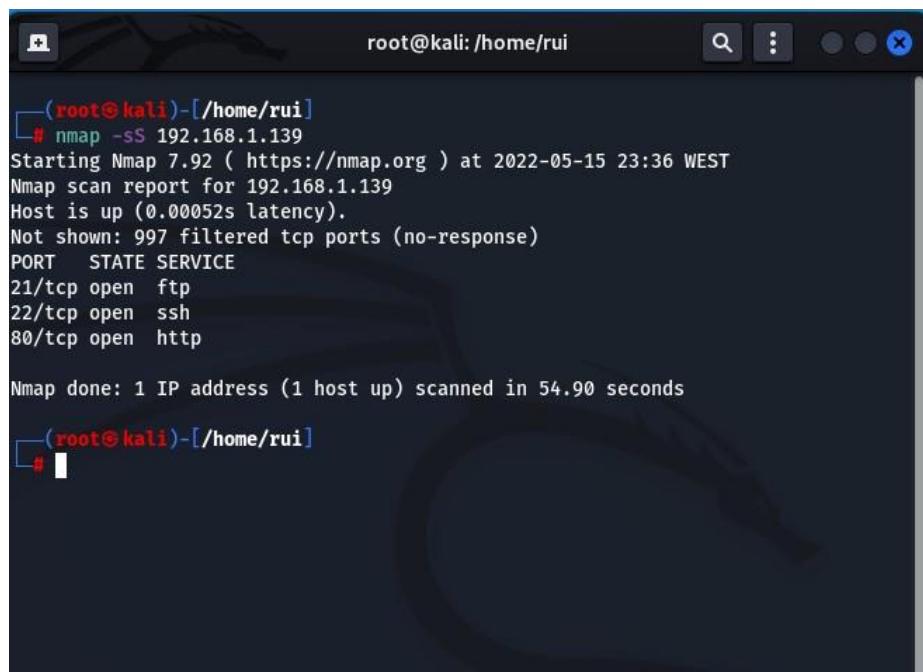


```
root@kali: /home/rui
└─# ftp 192.168.1.139
Connected to 192.168.1.139.
220 (vsFTPd 2.2.2)
Name (192.168.1.139:rui): anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
229 Entering Extended Passive Mode (|||54803|).
150 Here comes the directory listing.
drwxr-xr-x  2 0          0          4096 Mar 22  2017 pub
226 Directory send OK.
ftp> exit
221 Goodbye.

└─#
```

Figura 17 - Resultado do comando *ftp*.

Realizando novamente o comando *nmap -sS* é possível obter mais informações do que anteriormente, pois desta vez temos mais 2 portas que se encontram abertas. Estas são as portas que dizem respeito aos serviços *ftp* e *http*, serviços configurados na *firewall* para que o seu tráfego fosse permitido.



```
root@kali: /home/rui
└─# nmap -sS 192.168.1.139
Starting Nmap 7.92 ( https://nmap.org ) at 2022-05-15 23:36 WEST
Nmap scan report for 192.168.1.139
Host is up (0.00052s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
80/tcp    open  http

Nmap done: 1 IP address (1 host up) scanned in 54.90 seconds

└─#
```

Figura 18 - Resultado do comando *nmap -sS*.

Voltando ao lado do servidor foi realizado o comando ping não sendo obtida qualquer resposta, sendo que isto acontece, pois, o tráfego ICMP é rejeitado na configuração da *firewall*.

```
root@centos6:~#
File Edit View Search Terminal Help
[root@centos6 ~]# ping 192.168.232.132
PING 192.168.232.132 (192.168.232.132) 56(84) bytes of data.
```

Figura 19 - Teste de conectividade.

Voltando a realizar o comando *iptables -L -v* é obtido o seguinte resultado.

```
root@centos6:/home/centos/Desktop#
File Edit View Search Terminal Help
[root@centos6 Desktop]# iptables -L -v
Chain INPUT (policy ACCEPT 0 packets, 0 bytes)
pkts bytes target     prot opt in     out    source          destination
 227 23209 ACCEPT     all --  any   any   anywhere        anywhere      state RELATED,ESTABLISHED
    0    0 REJECT     icmp --  any   any   anywhere        anywhere      icmp echo-request reject-with icmp-host-prohibited
    0    0 ACCEPT     icmp --  any   any   anywhere        anywhere
 145 11004 ACCEPT     all --  lo    any   anywhere        anywhere
    0    0 ACCEPT     tcp  --  any   any   anywhere        anywhere      state NEW tcp dpt:ssh
    0    0 ACCEPT     tcp  --  any   any   anywhere        anywhere      state NEW tcp dpt:http
    0    0 ACCEPT     tcp  --  any   any   anywhere        anywhere      state NEW tcp dpt:ftp
    3   913 REJECT     all --  any   any   anywhere        anywhere      reject-with icmp-host-prohibited

Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
pkts bytes target     prot opt in     out    source          destination
    0    0 REJECT     all --  any   any   anywhere        anywhere      reject-with icmp-host-prohibited

Chain OUTPUT (policy ACCEPT 372 packets, 32066 bytes)
pkts bytes target     prot opt in     out    source          destination
[root@centos6 Desktop]#
```

Figura 20 - Resultado do comando *iptables -L -v*.

Ao observar a figura anterior, no campo bytes da tabela INPUT é possível observar que foram rejeitados 913 bytes tendo estes a ver com o protocolo ICMP, que corresponde aos *pings* realizados. Para além disso é possível observar que foram aceites 11004 bytes provenientes da interface *loopback* e 23209 bytes que foram aceites de qualquer interface.

4. Regras de escrita

Nesta secção é realizada a preparação de um ficheiro *iptables* com um conjunto de regras que uma *firewall* deve seguir. Primeiramente foi necessário limpar todas as tabelas e guardar num ficheiro *template* como demonstrado na figura seguinte.



```
root@centos6:/home/centos/Desktop
File Edit View Search Terminal Help
[root@centos6 Desktop]# iptables -F
[root@centos6 Desktop]# service iptables save
iptables: Saving firewall rules to /etc/sysconfig/iptables:[ OK ]
[root@centos6 Desktop]# cat /etc/sysconfig/iptables
# Generated by iptables-save v1.4.7 on Tue May 17 08:50:19 2022
*filter
:INPUT ACCEPT [0:0]
:FORWARD ACCEPT [0:0]
:OUTPUT ACCEPT [0:0]
COMMIT
# Completed on Tue May 17 08:50:19 2022
[root@centos6 Desktop]#
```

Figura 21 - Apagar e guardar as *iptables*.

Foi necessário editar o ficheiro de configuração das tabelas da firewall começando por realizar *DROP* do tráfego em todas as tabelas. Para isso foi necessário realizar os comandos apresentados de seguida.



```
root@centos6:/home/centos/Desktop
File Edit View Search Terminal Help
[root@centos6 Desktop]# iptables -P INPUT DROP
[root@centos6 Desktop]# iptables -P FORWARD DROP
[root@centos6 Desktop]# iptables -P OUTPUT DROP
[root@centos6 Desktop]# cat /etc/sysconfig/iptables
# Generated by iptables-save v1.4.7 on Tue May 17 08:50:19 2022
*filter
:INPUT ACCEPT [0:0]
:FORWARD ACCEPT [0:0]
:OUTPUT ACCEPT [0:0]
COMMIT
# Completed on Tue May 17 08:50:19 2022
[root@centos6 Desktop]# service iptables save
iptables: Saving firewall rules to /etc/sysconfig/iptables:[ OK ]
[root@centos6 Desktop]# cat /etc/sysconfig/iptables
# Generated by iptables-save v1.4.7 on Tue May 17 09:05:48 2022
*filter
:INPUT DROP [0:0]
:FORWARD DROP [0:0]
:OUTPUT DROP [11:2096]
COMMIT
# Completed on Tue May 17 09:05:48 2022
[root@centos6 Desktop]#
```

Figura 22 - *DROP* em todas as tabelas.

Foi necessário aceitar todas as conexões TCP estabelecidas, tanto nas tabelas de INPUT como de OUTPUT sendo realizado para isto os seguintes comandos.

```
root@centos6:/home/centos/Desktop
File Edit View Search Terminal Help
[root@centos6 Desktop]# iptables -A INPUT -p tcp -j ACCEPT
[root@centos6 Desktop]# iptables -A OUTPUT -p tcp -j ACCEPT
[root@centos6 Desktop]# service iptables save
iptables: Saving firewall rules to /etc/sysconfig/iptables:[ OK ]
[root@centos6 Desktop]# cat /etc/sysconfig/iptables
# Generated by iptables-save v1.4.7 on Tue May 17 09:11:26 2022
*filter
:INPUT DROP [0:0]
:FORWARD DROP [0:0]
:OUTPUT DROP [5:884]
-A INPUT -p tcp -j ACCEPT
-A OUTPUT -p tcp -j ACCEPT
-A OUTPUT -p tcp -j ACCEPT
COMMIT
# Completed on Tue May 17 09:11:26 2022
[root@centos6 Desktop]#
```

Figura 23 - Adição das regras TCP.

Todo o tráfego na interface *loopback* deve ser aceite. Isto foi obtido através do comando seguinte.

```
root@centos6:/home/centos/Desktop
File Edit View Search Terminal Help
[root@centos6 Desktop]# iptables -A INPUT -i lo -j ACCEPT
[root@centos6 Desktop]# service iptables save
iptables: Saving firewall rules to /etc/sysconfig/iptables:[ OK ]
[root@centos6 Desktop]# cat /etc/sysconfig/iptables
# Generated by iptables-save v1.4.7 on Tue May 17 09:13:44 2022
*filter
:INPUT DROP [0:0]
:FORWARD DROP [0:0]
:OUTPUT DROP [3:480]
-A INPUT -p tcp -j ACCEPT
-A INPUT -p tcp -j ACCEPT
-A INPUT -p tcp -j ACCEPT
-A INPUT -i lo -j ACCEPT
-A OUTPUT -p tcp -j ACCEPT
-A OUTPUT -p tcp -j ACCEPT
COMMIT
# Completed on Tue May 17 09:13:44 2022
[root@centos6 Desktop]#
```

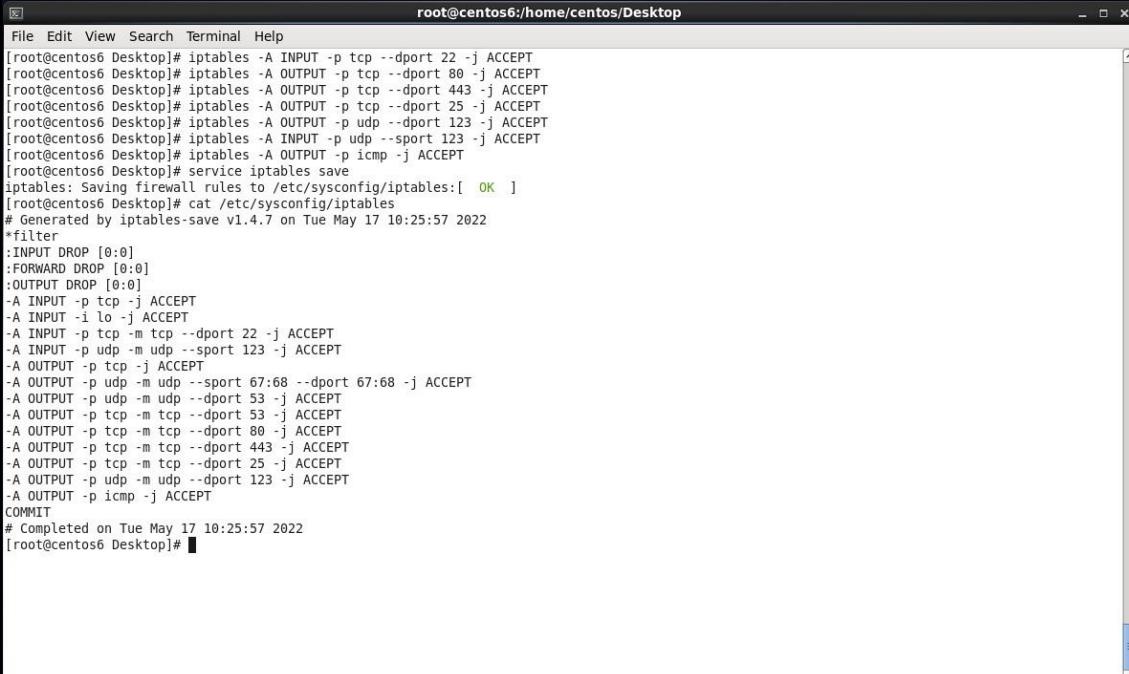
Figura 24 - Adição da regra da interface loopback.

É necessário aceitar todos os pedidos DHCP, de modo que seja possível obter um endereço IP e uma máscara. Para além disso é necessário fazer o mesmo para os pedidos DNS, sendo que isto é possível ser realizado através dos seguintes comandos.

```
root@centos6 Desktop]# iptables -A OUTPUT -p udp --dport 67:68 --sport 67:68 -j ACCEPT
[root@centos6 Desktop]# iptables -A OUTPUT -p udp -m udp --dport 53 -j ACCEPT
[root@centos6 Desktop]# service iptables save
iptables: Saving firewall rules to /etc/sysconfig/iptables:[ OK ]
[root@centos6 Desktop]# cat /etc/sysconfig/iptables
# Generated by iptables-save v1.4.7 on Tue May 17 10:05:38 2022
*filter
:INPUT DROP [0:0]
:FORWARD DROP [0:0]
:OUTPUT DROP [0:0]
-A INPUT -p tcp -j ACCEPT
-A INPUT -i lo -j ACCEPT
-A OUTPUT -p tcp -j ACCEPT
-A OUTPUT -p udp -m udp --sport 67:68 --dport 67:68 -j ACCEPT
-A OUTPUT -p udp -m udp --dport 53 -j ACCEPT
-A OUTPUT -p tcp -m tcp --dport 53 -j ACCEPT
COMMIT
# Completed on Tue May 17 10:05:38 2022
[root@centos6 Desktop]#
```

Figura 25 - Regras para o DHCP e DNS.

Outros serviços fundamentais foram necessários ser configurados, sendo aceite todo o tráfego *ssh*, *http*, *https*, *smtp*, *ntp* e *icmp*. Isto é obtido através da realização dos comandos seguintes.



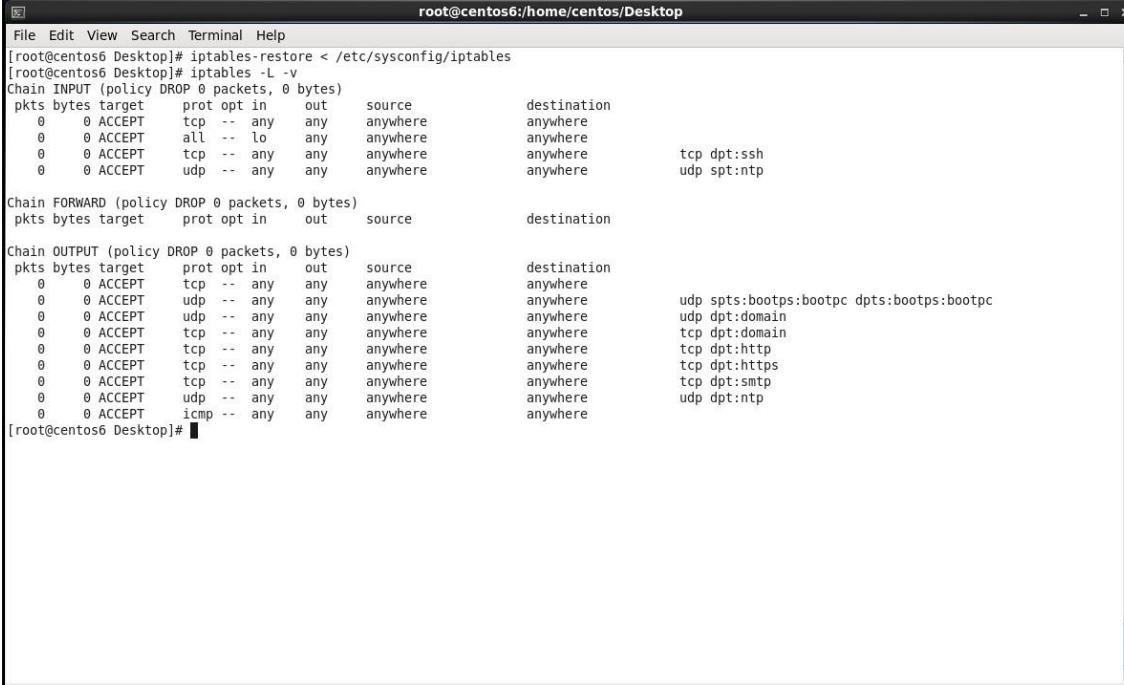
```

root@centos6:/home/centos/Desktop
File Edit View Search Terminal Help
[root@centos6 Desktop]# iptables -A INPUT -p tcp --dport 22 -j ACCEPT
[root@centos6 Desktop]# iptables -A OUTPUT -p tcp --sport 80 -j ACCEPT
[root@centos6 Desktop]# iptables -A OUTPUT -p tcp --dport 443 -j ACCEPT
[root@centos6 Desktop]# iptables -A OUTPUT -p tcp --dport 25 -j ACCEPT
[root@centos6 Desktop]# iptables -A OUTPUT -p udp --sport 123 -j ACCEPT
[root@centos6 Desktop]# iptables -A INPUT -p udp --dport 123 -j ACCEPT
[root@centos6 Desktop]# iptables -A OUTPUT -p icmp -j ACCEPT
[root@centos6 Desktop]# service iptables save
iptables: Saving firewall rules to /etc/sysconfig/iptables:[ OK ]
[root@centos6 Desktop]# cat /etc/sysconfig/iptables
# Generated by iptables-save v1.4.7 on Tue May 17 10:25:57 2022
*filter
:INPUT DROP [0:0]
:FORWARD DROP [0:0]
:OUTPUT DROP [0:0]
-A INPUT -p tcp -j ACCEPT
-A INPUT -i lo -j ACCEPT
-A INPUT -p tcp --dport 22 -j ACCEPT
-A INPUT -p udp -m udp --sport 123 -j ACCEPT
-A OUTPUT -p tcp -j ACCEPT
-A OUTPUT -p udp -m udp --sport 67:68 --dport 67:68 -j ACCEPT
-A OUTPUT -p udp -m udp --dport 53 -j ACCEPT
-A OUTPUT -p tcp -m tcp --dport 53 -j ACCEPT
-A OUTPUT -p tcp -m tcp --dport 80 -j ACCEPT
-A OUTPUT -p tcp -m tcp --dport 443 -j ACCEPT
-A OUTPUT -p tcp -m tcp --dport 25 -j ACCEPT
-A OUTPUT -p udp -m udp --dport 123 -j ACCEPT
-A OUTPUT -p icmp -j ACCEPT
COMMIT
# Completed on Tue May 17 10:25:57 2022
[root@centos6 Desktop]#

```

Figura 26 - Regras dos serviços fundamentais.

Por último, foi necessário testar o ficheiro realizando o comando apresentado de seguida. Após isso, ao aceder às *iptables* criadas é possível verificar que não ocorreram erros e que as regras estavam bem implementadas.



```

root@centos6:/home/centos/Desktop
File Edit View Search Terminal Help
[root@centos6 Desktop]# iptables-restore < /etc/sysconfig/iptables
[root@centos6 Desktop]# iptables -L -v
Chain INPUT (policy DROP 0 packets, 0 bytes)
pkts bytes target prot opt in  out source      destination
  0   0 ACCEPT  tcp  --  any   any anywhere   anywhere
  0   0 ACCEPT  all  --  lo    any anywhere   anywhere
  0   0 ACCEPT  tcp  --  any   any anywhere   anywhere      tcp dpt:ssh
  0   0 ACCEPT  udp  --  any   any anywhere   anywhere      udp spt:ntp

Chain FORWARD (policy DROP 0 packets, 0 bytes)
pkts bytes target prot opt in  out source      destination

Chain OUTPUT (policy DROP 0 packets, 0 bytes)
pkts bytes target prot opt in  out source      destination
  0   0 ACCEPT  tcp  --  any   any anywhere   anywhere
  0   0 ACCEPT  udp  --  any   any anywhere   anywhere      udp spts:bootps:bootpc dpts:bootps:bootpc
  0   0 ACCEPT  udp  --  any   any anywhere   anywhere      udp dpt:domain
  0   0 ACCEPT  tcp  --  any   any anywhere   anywhere      tcp dpt:domain
  0   0 ACCEPT  tcp  --  any   any anywhere   anywhere      tcp dpt:http
  0   0 ACCEPT  tcp  --  any   any anywhere   anywhere      tcp dpt:https
  0   0 ACCEPT  tcp  --  any   any anywhere   anywhere      tcp dpt:smtp
  0   0 ACCEPT  udp  --  any   any anywhere   anywhere      udp dpt:ntp
  0   0 ACCEPT  icmp --  any   any anywhere   anywhere

[root@centos6 Desktop]#

```

Figura 27 - Execução do *iptables-restore*.

Tarefa 2 – Firewall (Avançado)

Na realização desta tarefa foi necessária a criação de 3 máquinas virtuais, sendo que 1 corre o software *pfSense*, cujo objetivo foi servir de router a outras 2 máquinas virtuais. Estas 2 máquinas foram criadas com imagens Xubuntu.

1. Virtual Lab

Foi realizada a configuração da máquina virtual com *pfSense* seguindo o tutorial do enunciado. Foi necessário realizar o menu 2 para atribuir um endereço IP diferente à LAN visto que esta era da mesma sub-rede da WAN.

```
8) Shell
Enter an option: ^C
FreeBSD/amd64 (pfSense.home.arpa) (ttyv0)

VirtualBox Virtual Machine - Netgate Device ID: bd1ec30622d63c1922f7

*** Welcome to pfSense 2.6.0-RELEASE (amd64) on pfSense ***

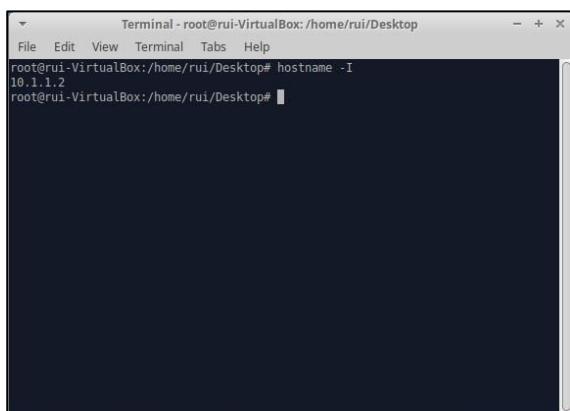
WAN (wan)      -> vtne0      -> v4/DHCP4: 192.168.1.140/24
                           v6: 2001:8a0:f595:9800:a00:27ff:fe25:50e9/64
LAN (lan)      -> vtne1      -> v4: 10.1.1.1/24

0) Logout (SSH only)          9) pfTop
1) Assign Interfaces           10) Filter Logs
2) Set interface(s) IP address 11) Restart webConfigurator
3) Reset webConfigurator password 12) PHP shell + pfSense tools
4) Reset to factory defaults   13) Update from console
5) Reboot system               14) Enable Secure Shell (sshd)
6) Halt system                 15) Restore recent configuration
7) Ping host                   16) Restart PHP-FPM

Enter an option: ■
```

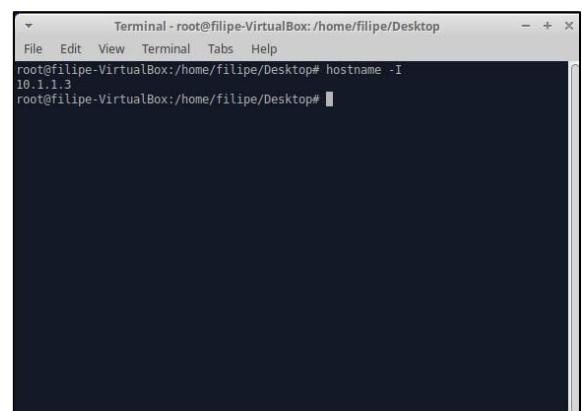
Figura 28 - Máquina virtual com *pfSense*.

Nas outras máquinas virtuais é possível verificar o IP atribuído como demonstrado nas 2 figuras seguintes.



```
Terminal - root@rui-VirtualBox:/home/rui/Desktop
File Edit View Terminal Tabs Help
root@rui-VirtualBox:/home/rui/Desktop# hostname -I
10.1.1.2
root@rui-VirtualBox:/home/rui/Desktop#
```

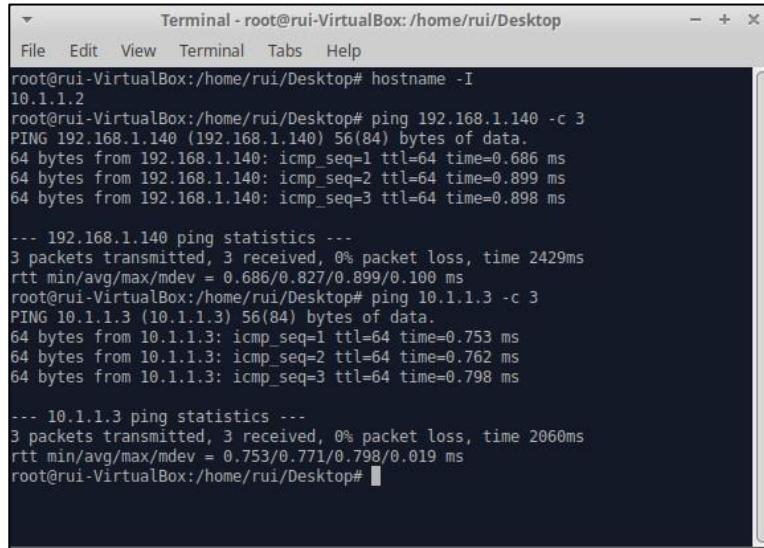
Figura 30 - Atribuição do IP do cliente 1.



```
Terminal - root@filipe-VirtualBox:/home/filipe/Desktop
File Edit View Terminal Tabs Help
root@filipe-VirtualBox:/home/filipe/Desktop# hostname -I
10.1.1.3
root@filipe-VirtualBox:/home/filipe/Desktop#
```

Figura 29 - Atribuição do IP do cliente 2.

De seguida foram realizados alguns testes de conectividade, como o exemplo seguinte, em que foi efetuado um *ping* entre a VM1 e a VM0 e entre a VM1 e a VM2, ambos com sucesso.



```
Terminal - root@rui-VirtualBox:/home/rui/Desktop
File Edit View Terminal Tabs Help
root@rui-VirtualBox:/home/rui/Desktop# hostname -I
10.1.1.2
root@rui-VirtualBox:/home/rui/Desktop# ping 192.168.1.140 -c 3
PING 192.168.1.140 (192.168.1.140) 56(84) bytes of data.
64 bytes from 192.168.1.140: icmp_seq=1 ttl=64 time=0.686 ms
64 bytes from 192.168.1.140: icmp_seq=2 ttl=64 time=0.899 ms
64 bytes from 192.168.1.140: icmp_seq=3 ttl=64 time=0.898 ms

--- 192.168.1.140 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2429ms
rtt min/avg/max/mdev = 0.686/0.827/0.899/0.100 ms
root@rui-VirtualBox:/home/rui/Desktop# ping 10.1.1.3 -c 3
PING 10.1.1.3 (10.1.1.3) 56(84) bytes of data.
64 bytes from 10.1.1.3: icmp_seq=1 ttl=64 time=0.753 ms
64 bytes from 10.1.1.3: icmp_seq=2 ttl=64 time=0.762 ms
64 bytes from 10.1.1.3: icmp_seq=3 ttl=64 time=0.798 ms

--- 10.1.1.3 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2060ms
rtt min/avg/max/mdev = 0.753/0.771/0.798/0.019 ms
root@rui-VirtualBox:/home/rui/Desktop#
```

Figura 31 - Teste de conectividade.

Após comprovada a conectividade foi acedido ao *browser* e colocado o IP da LAN do router virtual que no nosso caso era 10.1.1.1. O resultado foi o seguinte.

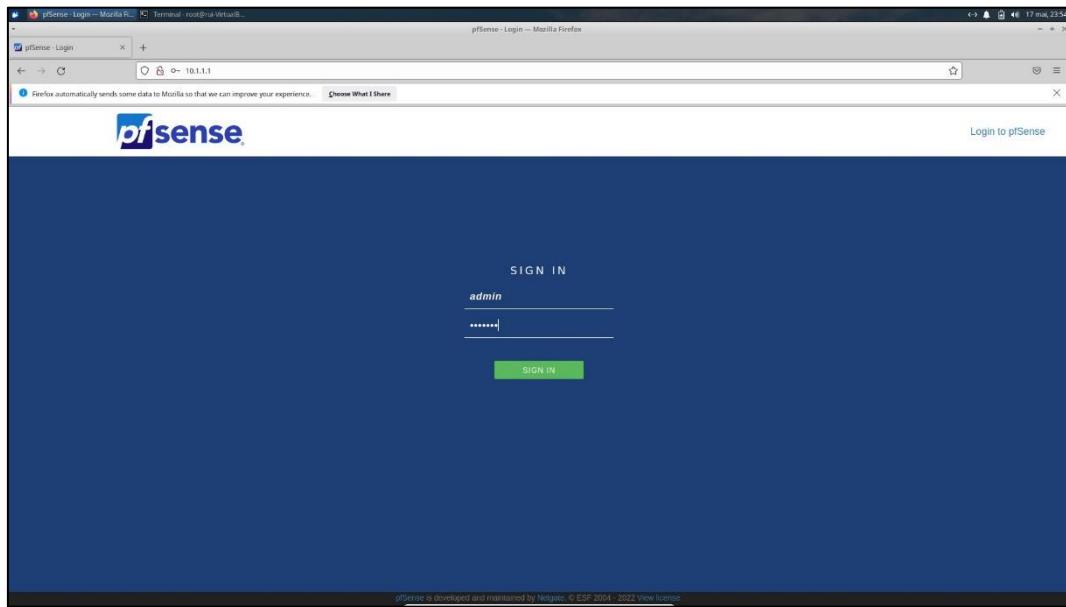


Figura 32 - Pesquisa pelo IP da LAN no browser.

Realizando o login de modo a aceder à interface gráfica do *pfSense*, o grupo deparou-se com o seguinte ecrã.

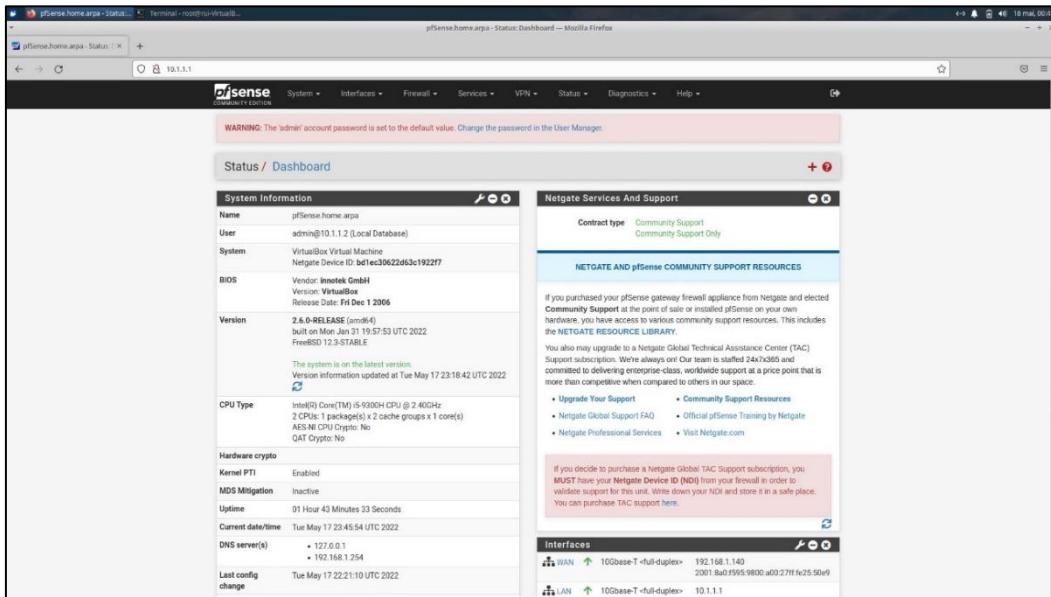


Figura 33 - Acesso ao *pfSense* através do browser.

Através da observação do menu Interfaces é possível observar as regras *default* do *pfSense* para a rede WAN e LAN. Na rede WAN é possível observar os tipos de configuração de ambos os IPV4 e IPV6 e que esta interface se encontra ativa. Para além disso, todos os restantes campos estão com as configurações *default* e é possível também observar 2 regras relativas às redes reservadas. A primeira bloqueia tráfego proveniente de redes privadas e endereços *loopback* e a segunda bloqueia redes falsas. Apesar de apresentar estas 2 regras, apresenta um baixo nível de segurança.

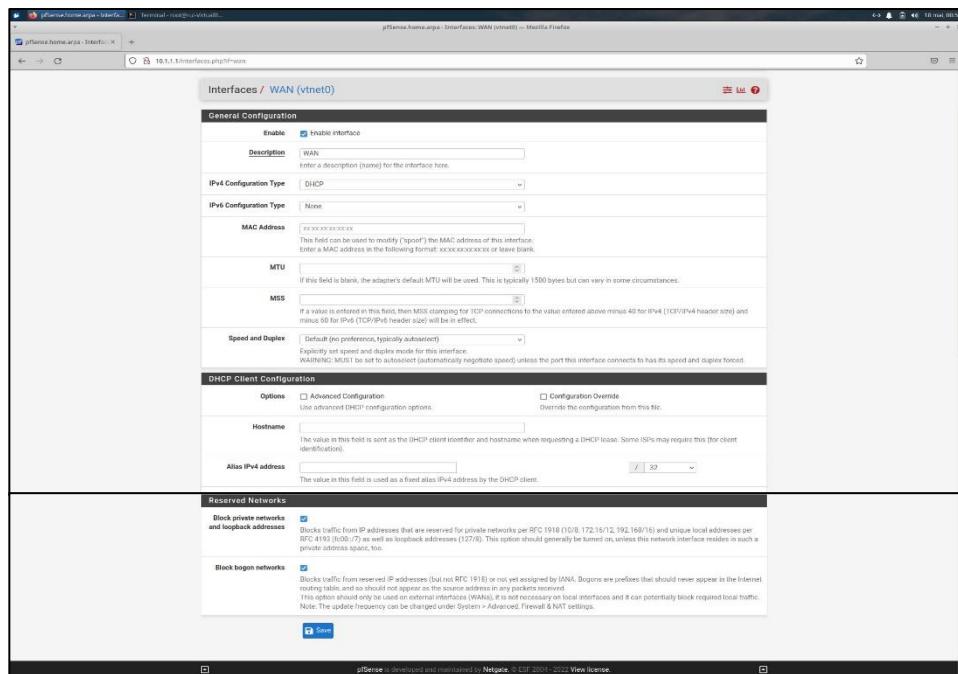


Figura 34 - Regras da interface WAN.

Quanto à rede LAN, nesta também é possível observar os tipos de configuração realizados. Quanto ao endereço IPV4, este é realizado estaticamente como foi previamente demonstrado onde adicionamos o IP 10.1.1.1 na VM0. Relativamente aos outros campos de configuração, também se encontram vazios não havendo quaisquer regras na realização do controlo.

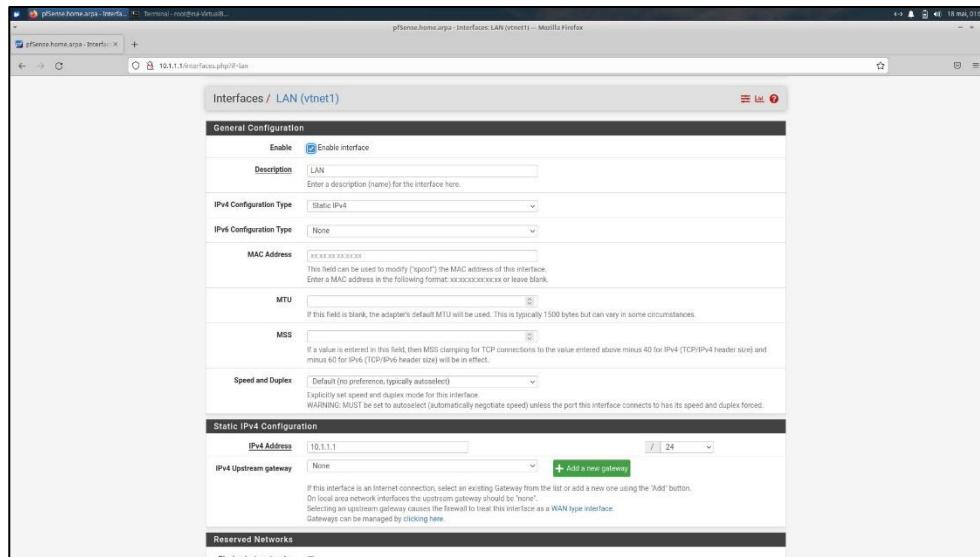


Figura 35 - Regras da interface LAN.

De seguida foi necessário desmarcar a primeira regra da interface WAN visto que esta impedia o tráfego proveniente de redes privadas e como na realização da nossa simulação estamos a utilizar uma rede privada, caso não desmarcássemos esta opção não seria possível aceder à rede WAN das VMs.

Como comprovado pela imagem seguinte foi aplicada a alteração anterior com sucesso pois esta não está presente nas regras da *firewall* da WAN.

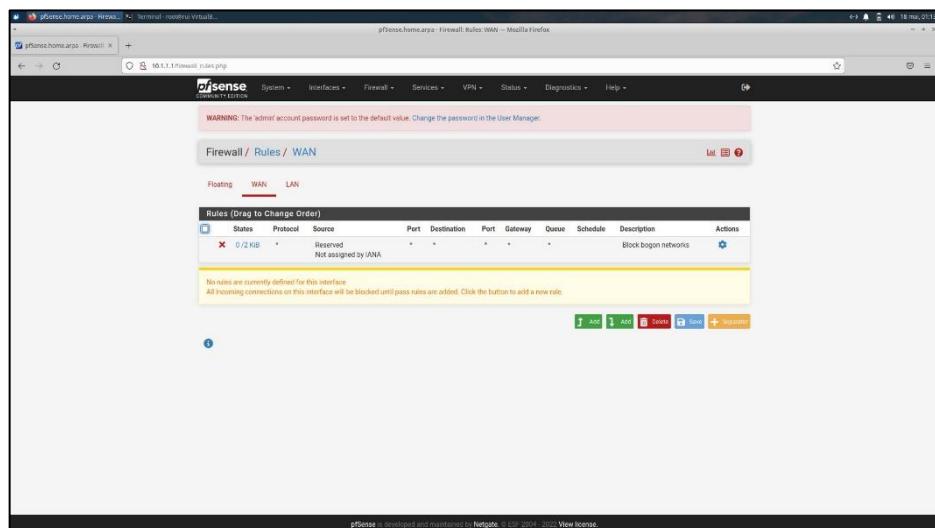


Figura 36 - Regras da firewall.

2. Impedir o acesso a um website

Neste capítulo do trabalho é necessário bloquear o acesso ao Facebook dos trabalhadores de uma empresa. Primeiro foi então necessário obter o IP que era utilizado no acesso. Na figura seguinte é demonstrado como é que este é obtido.

```
Terminal - root@rui-VirtualBox: /home/rui/Desktop
File Edit View Terminal Tabs Help
root@rui-VirtualBox:/home/rui/Desktop# host -t a www.facebook.com
www.facebook.com is an alias for star-mini.c10r.facebook.com.
star-mini.c10r.facebook.com has address 157.240.212.35
root@rui-VirtualBox:/home/rui/Desktop# whois 157.240.212.35 | grep NetRange
NetRange:      157.240.0.0 - 157.240.255.255
root@rui-VirtualBox:/home/rui/Desktop#
```

Figura 37 - Obtenção do IP do domínio facebook.com.

Através do comando *host* é possível obter o alias do domínio *facebook.com*, assim como o endereço IP. Com o comando *whois* foi possível obter a gama de valores correspondente ao IP.

Para comprovar o acesso ao *facebook.com* através das VM1 e VM2 foi realizada uma pesquisa no browser com sucesso como demonstrado na figura seguinte.

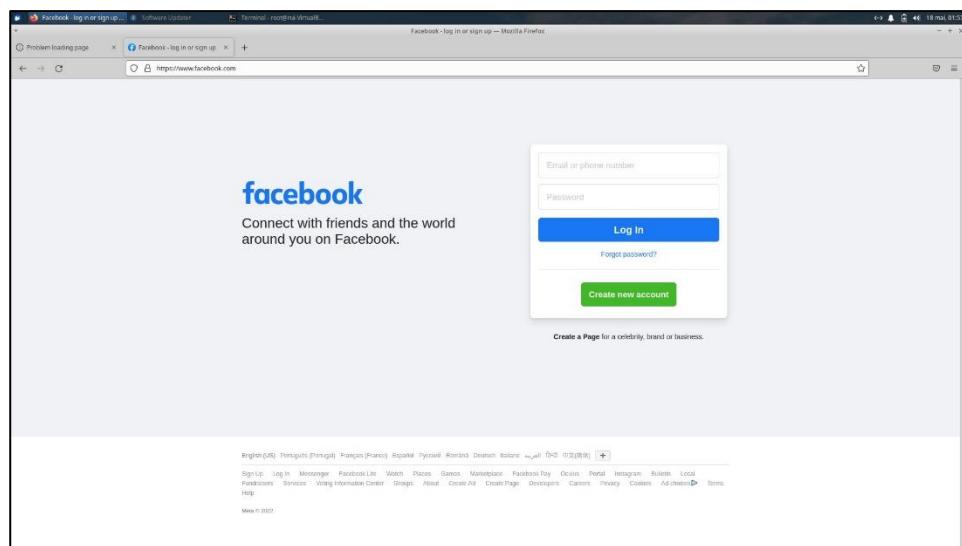


Figura 38 - Conexão com sucesso a facebook.com.

De modo a rejeitar o tráfego com origem na rede LAN e destino o facebook.com, foi realizada uma regra no *pfSense* que não permitisse este tráfego. Após guardarmos a regra e a termos enviado para o *pfSense*, voltamos a aceder ao website para ver se o tráfego era rejeitado como desejado. Na figura seguinte é apresentado o resultado obtido.

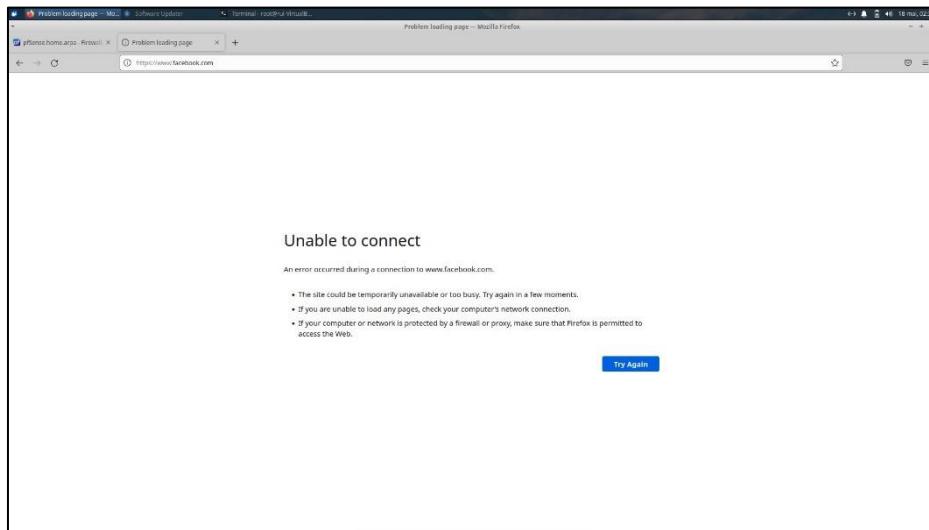


Figura 39 - Acesso recusado a facebook.com.

O acesso foi então rejeitado e é possível comprovar que foi graças à regra criada pois como demonstrado na figura seguinte houve 6 tentativas de conexão ao Facebook em que todas foram rejeitadas visto terem satisfeito a regra criada.

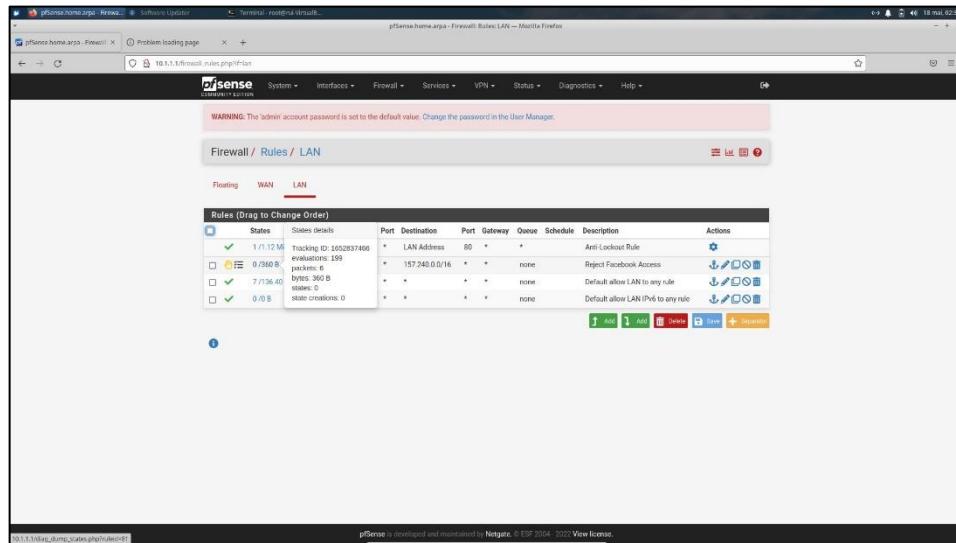


Figura 40 - Regra criada e tráfego que passa.

Após realizar a mudança de rejeitar os pacotes para bloquear foi possível observar que não era obtida resposta do *facebook.com*, no entanto, o pedido de conexão é realizado constantemente sendo que é possível observar a página a recarregar sem parar. Na figura seguinte é possível observar o número de pacotes que foram enviados aquando da tentativa de conexão, substancialmente maior que quando era utilizado a rejeição de pacotes.

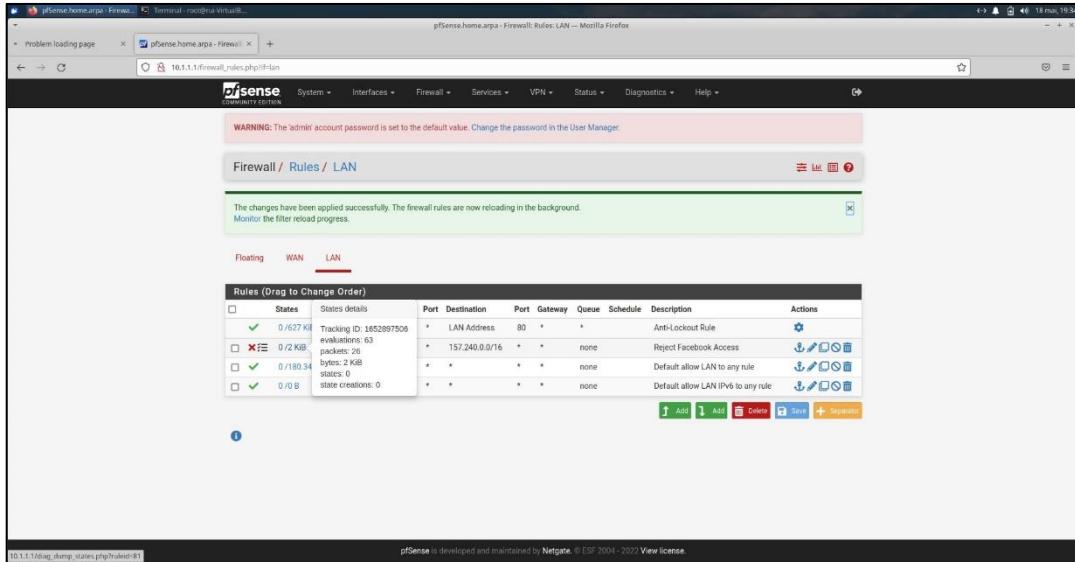


Figura 41 - Regra editada e o tráfego que passa.

É possível realizar o controlo do tráfego a um IP em específico em vez de controlar a rede toda. De seguida é demonstrado que desta forma também é possível realizar o controlo a um só IP, no entanto, esta não será a forma mais adequada de o fazer, visto que como o domínio Facebook utiliza a rede 157.240.0.0/16, esta poderá indicar a presença de outros servidores. Caso ocorra a mudança de servidor utilizado na realização da conexão, com as novas regras este tráfego não vai ser detetado, não sendo realizado o descarte dos pacotes.

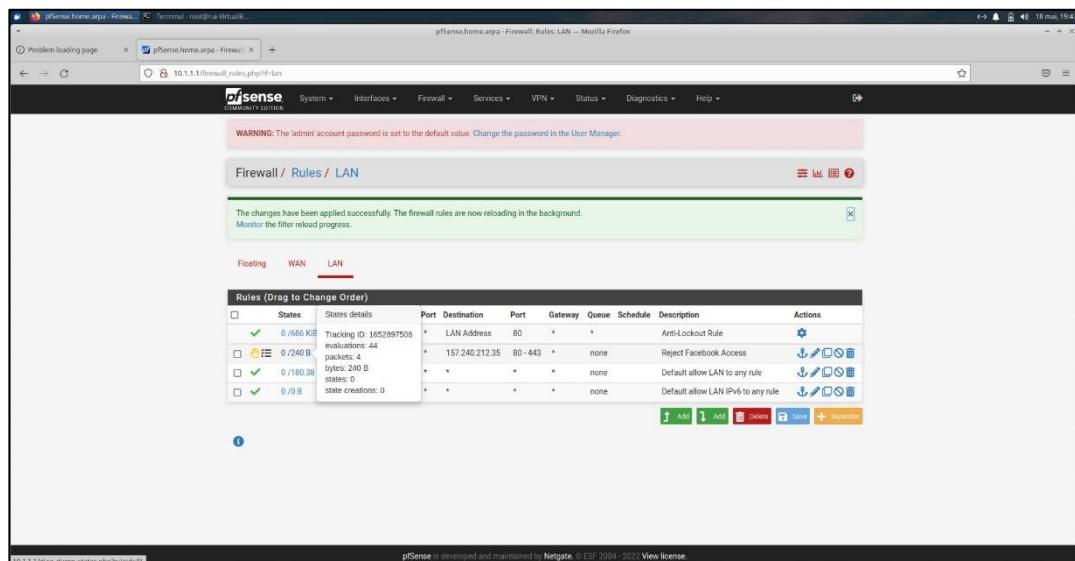
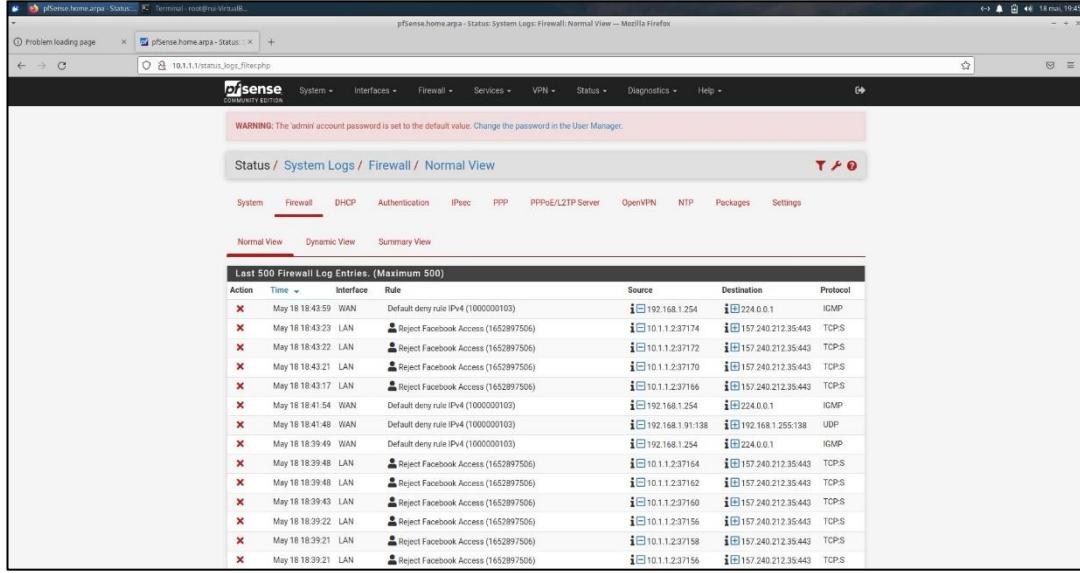


Figura 42 - Regra editada para só 1 IP.

Acedendo aos *logs* da *firewall* do sistema é possível obter informação dos pacotes que foram rejeitados em que na imagem seguinte podemos ver que estes sofreram essa ação devido à regra previamente criada cujo nome dos *logs* é “Reject Facebook Access”.



The screenshot shows the pfSense firewall log interface. At the top, there's a warning message: "WARNING: The 'admin' account password is set to the default value. Change the password in the User Manager." Below this, the navigation bar includes System, Firewall, DHCP, Authentication, IPsec, PPP, PPPoE/L2TP Server, OpenVPN, NTP, Packages, and Settings. Under Firewall, Normal View is selected. The main content area displays the "Last 500 Firewall Log Entries (Maximum 500)". The table has columns for Action, Time, Interface, Rule, Source, Destination, and Protocol. Most entries show a reject action against Facebook access from various LAN and WAN interfaces, with source addresses like 192.168.1.254 and destination addresses like 157.240.212.35:443. The protocol is TCP:S in most cases, except for some UDP and ICMP entries.

Action	Time	Interface	Rule	Source	Destination	Protocol
✗	May 18 18:43:59	WAN	Default deny rule IPv4 (10000000103)	192.168.1.254	72.0.0.1	ICMP
✗	May 18 18:43:23	LAN	Reject Facebook Access (1652897506)	10.1.2.37174	157.240.212.35:443	TCP:S
✗	May 18 18:43:22	LAN	Reject Facebook Access (1652897506)	10.1.2.37172	157.240.212.35:443	TCP:S
✗	May 18 18:43:21	LAN	Reject Facebook Access (1652897506)	10.1.2.37170	157.240.212.35:443	TCP:S
✗	May 18 18:43:17	LAN	Reject Facebook Access (1652897506)	10.1.2.37166	157.240.212.35:443	TCP:S
✗	May 18 18:41:54	WAN	Default deny rule IPv4 (10000000103)	192.168.1.254	224.0.0.1	ICMP
✗	May 18 18:41:48	WAN	Default deny rule IPv4 (10000000103)	192.168.1.91:19	192.168.1.255:19	UDP
✗	May 18 18:39:49	WAN	Default deny rule IPv4 (10000000103)	192.168.1.254	224.0.0.1	ICMP
✗	May 18 18:39:48	LAN	Reject Facebook Access (1652897506)	10.1.2.37164	157.240.212.35:443	TCP:S
✗	May 18 18:39:48	LAN	Reject Facebook Access (1652897506)	10.1.2.37162	157.240.212.35:443	TCP:S
✗	May 18 18:39:43	LAN	Reject Facebook Access (1652897506)	10.1.2.37160	157.240.212.35:443	TCP:S
✗	May 18 18:39:22	LAN	Reject Facebook Access (1652897506)	10.1.2.37156	157.240.212.35:443	TCP:S
✗	May 18 18:39:21	LAN	Reject Facebook Access (1652897506)	10.1.2.37158	157.240.212.35:443	TCP:S
✗	May 18 18:39:21	LAN	Reject Facebook Access (1652897506)	10.1.2.37156	157.240.212.35:443	TCP:S

Figura 43 - Logs da firewall do sistema.

3. Agendamento das regras

De modo que os colaboradores da empresa fiquem contentes e possam aceder a conteúdos do Facebook foi necessário permitir o seu acesso num dado intervalo de tempo. Esta medida acaba por ser benéfica para ambas as partes, visto que os colaboradores continuam a ter grande parte do tempo impossibilitados de aceder ao Facebook, mas têm uma pequena janela de tempo onde podem navegar livremente. Foi necessário então realizar um agendamento de quando a regra criada anteriormente tomava efeito. Este agendamento foi realizado da maneira representada a seguir com os colaboradores a não poderem aceder durante os dias de trabalho entre as 10 da manhã e as 4 da tarde.

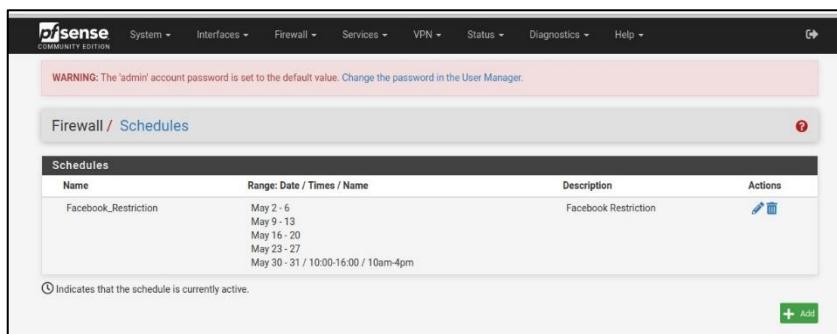


Figura 44 - Agendamento da regra da firewall.

De modo a incluir este agendamento na regra antes criada foi necessário aceder ao menu *Edit* na regra e em *Schedule* colocar o agendamento criado. Na próxima figura é possível observar o agendamento já realizado sendo que como já passou da hora limite o ícone aparece a amarelo. Caso se encontrasse dentro do limite este ícone apareceria a vermelho.

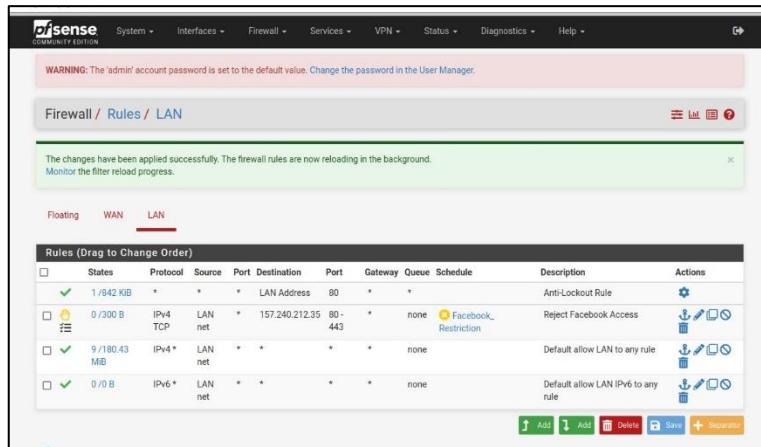


Figura 45 - Agendamento da regra da firewall.

Relativamente aos ficheiros *logs* é possível observar o seguinte, sendo que ao contrário de anteriormente, onde aparecia a descrição da regra, agora aparece um ID que corresponde à regra com o agendamento efetuado.

Action	Time	Interface	Rule	Source	Destination	Protocol
✗	May 18 19:52:30	LAN	s:62854d1f40bcb (1652897506)	10.1.1.2:37192	157.240.212.35:443	TCP:S
✗	May 18 19:52:29	LAN	s:62854d1f40bcb (1652897506)	10.1.1.2:37190	157.240.212.35:443	TCP:S
✗	May 18 19:52:28	LAN	s:62854d1f40bcb (1652897506)	10.1.1.2:37188	157.240.212.35:443	TCP:S
✗	May 18 19:52:28	LAN	s:62854d1f40bcb (1652897506)	10.1.1.2:37186	157.240.212.35:443	TCP:S
✗	May 18 19:52:27	LAN	s:62854d1f40bcb (1652897506)	10.1.1.2:37184	157.240.212.35:443	TCP:S
✗	May 18 19:52:18	WAN	Default deny rule IPv4 (1000000103)	192.168.1.86:9999	192.168.1.255:9999	UDP
✗	May 18 19:52:17	WAN	Default deny rule IPv4 (1000000103)	192.168.1.86:9999	192.168.1.255:9999	UDP

Figura 46 - Logs da firewall.

4. Web Server público

De modo a criar um servidor HTTP interno foi necessário implementar uma regra NAT, demonstrada de seguida. Esta regra faz com que todo o tráfego TCP na porta 80 seja encaminhado para a VM2, servindo esta como um servidor HTTP.

Figura 47 - Implementação da regra NAT.

Acedendo ao browser com o endereço da rede WAN é possível obter a página principal do servidor interno como demonstrado de seguida.

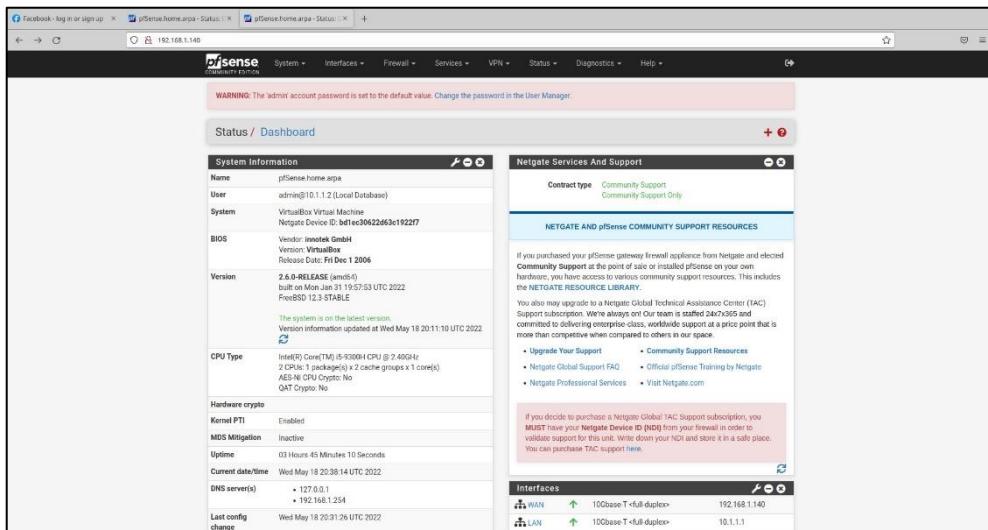


Figura 48 - Acesso à página inicial do servidor interno.

5. Limitar o número de conexões

De modo a nos prevenirmos de um ataque DDOS, cujo conceito passa por inundar a rede de tráfego levando a que o servidor não seja capaz de conseguir lidar com os pedidos de conexão, foi necessário realizar uma limitação de 20 pedidos de conexão por segundo. Para isso foi necessário implementar uma regra dentro da *firewall* para que este valor não fosse ultrapassado.

Primeiro foi realizado com o auxílio do *nping* um teste de um ataque DDOS ao servidor de modo a perceber como este reagia.

```
Max rtt: 7.230ms | Min rtt: 0.071ms | Avg rtt: 1.825ms
TCP connection attempts: 40 | Successful connections: 40 | Failed: 0 (0.00%)
Nping done: 1 IP address pinged in 2.07 seconds
root@rui-VirtualBox:/home/rui/Desktop#
```

Figura 49 - Realização do comando *nping*.

Da figura anterior podemos retirar que foram aceites 40 conexões das 40 tentadas e o tempo máximo, mínimo e médio que leva a enviar um pacote e receber uma resposta. De seguida foi procedido à análise do tráfego no Wireshark como demonstrado de seguida, onde é possível observar os pacotes trocados correspondentes ao processo de *three-way handshake*.

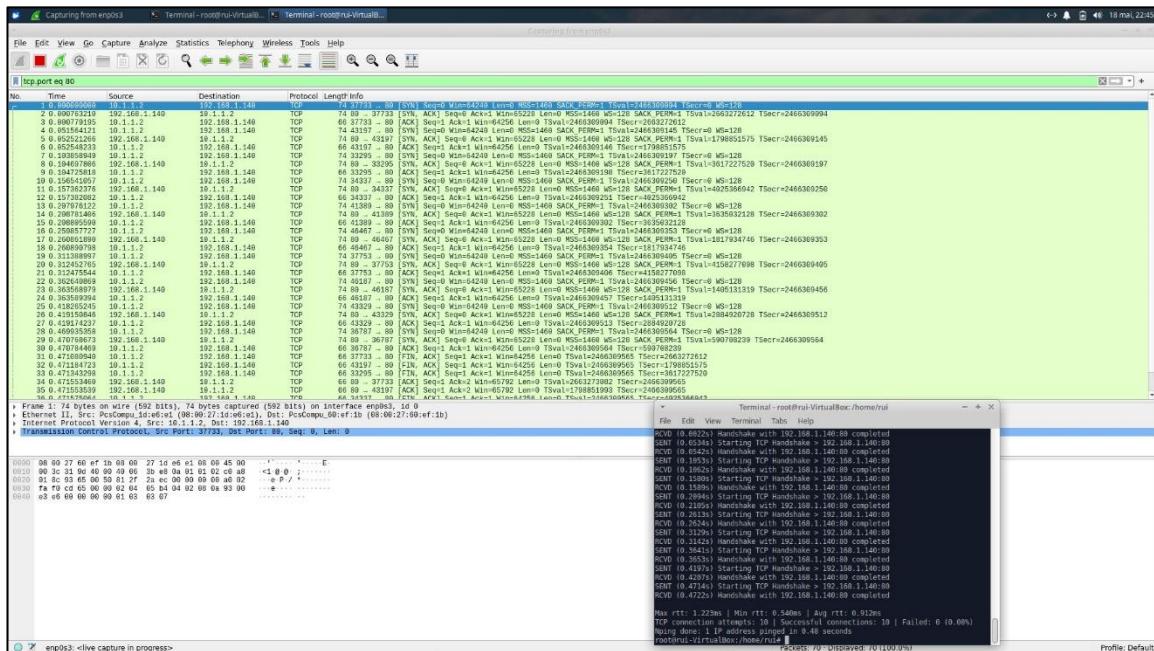


Figura 50 - Análise no Wireshark.

Foram ainda realizados alguns testes para ver o número de conexões por segundo obtidos e ao introduzir um rate de 1000 tentativas/s em 5000 tentativas foram obtidos 0.44% de erros e demorou 10.82 segundos, indicando que é possível realizar uma simulação de um ataque DDOS a esta rede visto estar a realizar cerca de 462 conexões por segundo.

De modo a limitarmos o número de conexões foi então necessário editar a regra da rede WAN, que encaminha o tráfego para o servidor interno e editá-la de modo que passasse a aceitar um máximo de 20 conexões por segundo. Na imagem seguinte é possível observar isto realizado com sucesso.

Figura 51 - Alteração da regra NAT.

Ao realizar um novo teste e inserindo um rate de 30 conexões/s era de esperar que fosse apresentado algum erro visto que o máximo aceitável era de 20, no entanto não houve qualquer regra a ser utilizada visto que ao realizar as 30 conexões a 30 conexões/s estas foram realizadas em aproximadamente 1 segundo, que não era o desejado.

```

SENT (0.7180s) Starting TCP Handshake > 192.168.1.140:80
RCVD (0.7195s) Handshake with 192.168.1.140:80 completed
SENT (0.7698s) Starting TCP Handshake > 192.168.1.140:80
RCVD (0.7711s) Handshake with 192.168.1.140:80 completed
SENT (0.8064s) Starting TCP Handshake > 192.168.1.140:80
RCVD (0.8076s) Handshake with 192.168.1.140:80 completed
SENT (0.8405s) Starting TCP Handshake > 192.168.1.140:80
RCVD (0.8421s) Handshake with 192.168.1.140:80 completed
SENT (0.8761s) Starting TCP Handshake > 192.168.1.140:80
RCVD (0.8769s) Handshake with 192.168.1.140:80 completed
SENT (0.9108s) Starting TCP Handshake > 192.168.1.140:80
RCVD (0.9118s) Handshake with 192.168.1.140:80 completed
SENT (0.9449s) Starting TCP Handshake > 192.168.1.140:80
RCVD (0.9466s) Handshake with 192.168.1.140:80 completed
SENT (0.9784s) Starting TCP Handshake > 192.168.1.140:80
RCVD (0.9791s) Handshake with 192.168.1.140:80 completed
SENT (1.0135s) Starting TCP Handshake > 192.168.1.140:80
RCVD (1.0148s) Handshake with 192.168.1.140:80 completed
SENT (1.0480s) Starting TCP Handshake > 192.168.1.140:80
RCVD (1.0488s) Handshake with 192.168.1.140:80 completed
SENT (1.0826s) Starting TCP Handshake > 192.168.1.140:80
RCVD (1.0835s) Handshake with 192.168.1.140:80 completed

Max rtt: 8.473ms | Min rtt: 0.715ms | Avg rtt: 1.644ms
TCP connection attempts: 30 | Successful connections: 30 | Failed: 0 (0.00%)
Nping done: 1 IP address pinged in 1.09 seconds
root@rui-VirtualBox:/home/rui#

```

Figura 52 - Teste de 30 conexões a 30 conexões/s.

Tarefa 3 – NIDS (Básico)

1. Configuração do Suricata

Foi necessário proceder à instalação do pacote Suricata através da interface gráfica do *pfSense*. De modo a comprovar a realização desta instalação com sucesso é apresentada a figura seguinte.

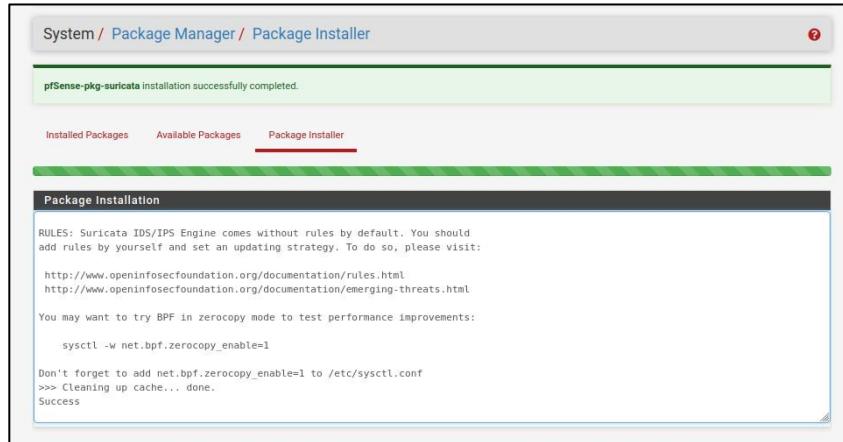


Figura 53 - Instalação do pacote Suricata.

Após isto foi necessário realizar a configuração do Suricata acedendo ao menu “Services -> Suricata” como demonstrado de seguida.

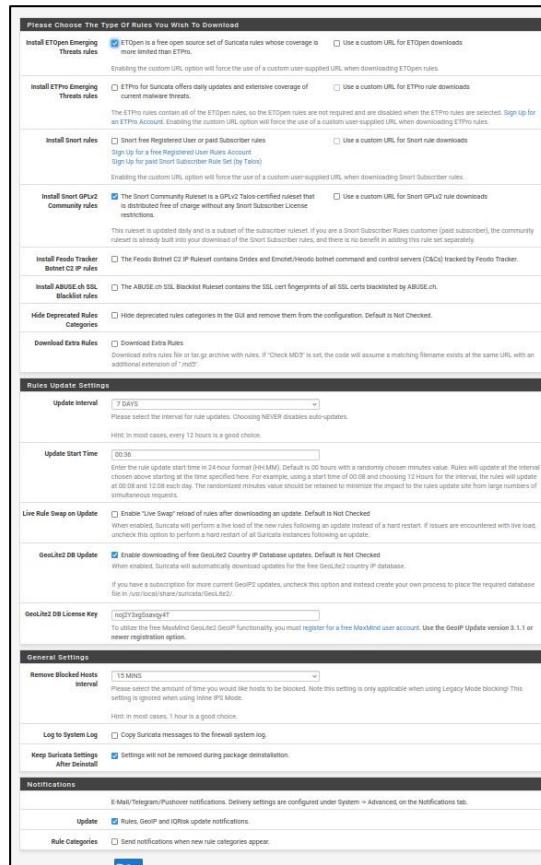


Figura 54 - Configuração do Suricata.

Após a realização da configuração é necessário atualizar as regras guardadas localmente carregando no botão Upload. Após visitarmos a página com os logs realizados é possível obter a seguinte informação.

The screenshot shows a web-based interface for managing rule sets. At the top, there's a header 'UPDATE YOUR RULE SET' with a timestamp 'Last Update: May-19 2022 15:10' and a message 'Result: success'. Below this are two buttons: a blue 'Update' button with a checkmark icon and an orange 'Force' button with a download icon. The main area is titled 'MANAGE RULE SET LOG' and contains a 'Hide' button (with a close icon) and a 'Clear' button (with a trash bin icon). A note states: 'The log file is limited to 1024K in size and automatically clears when the limit is exceeded.' Below this is a section titled 'RULE SET UPDATE LOG' which displays the log file content:

```

Starting rules update... Time: 2022-05-19 15:10:28
  Downloading Emerging Threats Open rules md5 file...
  Checking Emerging Threats Open rules md5 file...
  There is a new set of Emerging Threats Open rules posted.
  Downloading file 'emerging.rules.tar.gz'...
  Done downloading rules file.
  Downloading Snort GPLv2 Community Rules md5 file...
  Checking Snort GPLv2 Community Rules md5 file...
  There is a new set of Snort GPLv2 Community Rules posted.
  Downloading file 'community.rules.tar.gz'...
  Done downloading rules file.
  Extracting and installing Emerging Threats Open rules...
  Installation of Emerging Threats Open rules completed.
  Extracting and installing Snort GPLv2 Community Rules...
  Installation of Snort GPLv2 Community Rules completed.
  Copying new config and map files...
  Warning: No interfaces configured for Suricata were found...
The Rules update has finished. Time: 2022-05-19 15:10:26

```

Figura 55 - Atualização das regras do Suricata.

Acedendo ao separador *Categories* foi possível adicionar o conjunto de regras desejadas onde foram selecionadas todas como demonstrado de seguida.

The screenshot shows the 'WAN Categories' configuration page. At the top, there are tabs: WAN Settings, WAN Categories (which is active), WAN Rules, WAN Flow/Stream, WAN App Parsers, WAN Variables, and WAN IP Rep. Below the tabs, there's a section titled 'Automatic flowbit resolution' with a 'Resolve Flowbits' checkbox (which is checked) and a note: 'Default is Checked. Suricata will examine the enabled rules in your chosen rule categories for checked flowbits. Any rules that set these dependent flowbits will be automatically enabled and added to the list of files in the interface rules directory.' There's also a 'View rules' button with a 'View' icon. A note below it says: 'Click to view auto-enabled rules required to satisfy flowbit dependencies'. Another note at the bottom says: 'Note: Auto-enabled rules generating unwanted alerts should have their GID:SID added to the Suppression List for the interface.' Below this is a section titled 'Select the rulesets (Categories) Suricata will load at startup'. It shows a legend: a green circle for 'Category is auto-enabled by SID Mgmt conf files' and a red circle for 'Category is auto-disabled by SID Mgmt conf files'. There are three buttons at the top right: 'Select All' (blue), 'Unselect All' (orange), and a 'Save' button with a disk icon. The main area lists rule sets under 'Enabled' and 'Ruleset':

Enabled	Ruleset:	
<input checked="" type="checkbox"/>	Snort GPLv2 Community Rules (Talos-certified)	
<input checked="" type="checkbox"/>	Ruleset: ET Open Rules	Snort Rules are not enabled.
<input checked="" type="checkbox"/>	emerging-3coresc.rules	
<input checked="" type="checkbox"/>	emerging-activex.rules	
<input checked="" type="checkbox"/>	emerging-adware_pup.rules	
<input checked="" type="checkbox"/>	emerging-attack_response.rules	
<input checked="" type="checkbox"/>	emerging-botcc.portgrouped.rules	
<input checked="" type="checkbox"/>	emerging-botcc.rules	
<input checked="" type="checkbox"/>	emerging-chat.rules	
<input checked="" type="checkbox"/>	emerging-clarmy.rules	
<input checked="" type="checkbox"/>	emerging-coinminer.rules	
<input checked="" type="checkbox"/>	emerging-compromised.rules	
<input checked="" type="checkbox"/>	emerging-current_events.rules	
<input checked="" type="checkbox"/>	emerging-deleted.rules	
<input checked="" type="checkbox"/>	emergenc...	

Figura 56 - Adição do conjunto de regras.

Após isso foi necessário proceder à ativação das regras criadas como demonstrado a seguir.

State	Action	GID	SID	Proto	Source	Sport	Destination	DPort	Message
✓	▲	1	2419	tcp	\$HOME_NET	any	\$EXTERNAL_NET	\$HTTP_PORTS	FILE-IDENTIFY RealNetworks Realplayer .ram playlist file download request
✓	⚠	1	2420	tcp	\$HOME_NET	any	\$EXTERNAL_NET	\$HTTP_PORTS	FILE-IDENTIFY RealNetworks Realplayer .mp3 playlist file download request
✓	⚠	1	2422	tcp	\$HOME_NET	any	\$EXTERNAL_NET	\$HTTP_PORTS	FILE-IDENTIFY RealNetworks Realplayer .rt playlist file download request
✓	▲	1	2423	tcp	\$HOME_NET	any	\$EXTERNAL_NET	\$HTTP_PORTS	FILE-IDENTIFY RealNetworks Realplayer .rp playlist file download request

Figura 57 - Ativação das regras.

Com a configuração finalizada foi necessário iniciar a monitorização da interface WAN clicando o ícone da seta presente na página de configuração da interface. Copiando os ficheiros de configuração foi também iniciada a monitorização da interface LAN como demonstrado a seguir.

Interface Settings Overview					
Interface	Suricata Status	Pattern Match	Blocking Mode	Description	Actions
WAN (vtnet0)	✓	AUTO	DISABLED	WAN	
LAN (vtnet1)	✓	AUTO	DISABLED	LAN	

Figura 58 - Ativação da monitorização das interfaces.

2. Testes do Suricata

Acedendo ao separador *Alerts*, é possível observar os vários alertas obtidos relativamente a ambas as interfaces. Tendo em conta a rede WAN, que lida com o acesso à internet e realizando um comando para realizar “update” dos pacotes do sistema é possível observar alguns alertas que correspondem a falsos positivos visto que como é possível constatar pela figura, dizem respeito provavelmente a gestão de pacotes.

The screenshot shows the 'Alert Log View Settings' and 'Alert Log View Filter' sections of the Suricata interface. The settings section includes fields for 'Instance to View' (WAN), 'Save or Remove Logs' (with 'Download' and 'Clear' buttons), 'Save Settings' (with 'Save' and 'Refresh' checkboxes), and a 'Number of alerts to display' set to 250. The filter section displays a table of 'Last 250 Alert Entries'. The table has columns: Date, Action, Pri, Proto, Class, Src, SPort, Dst, DPort, GID:SID, and Description. The data shows multiple entries from May 19, 2022, at 19:15:15, all categorized as 'Not Suspicious Traffic' with an 'ET POLICY' action and 'Outbound likely related to package management' description. The IP addresses involved are 192.168.1.140, 193.136.212.166, and 185.125.190.36.

Date	Action	Pri	Proto	Class	Src	SPort	Dst	DPort	GID:SID	Description
05/19/2022 19:15:15	⚠️	3	TCP	Not Suspicious Traffic	192.168.1.140	50342	193.136.212.166	80	1:2013504	ET POLICY GNU/Linux APT User-Agent Outbound likely related to package management
05/19/2022 19:15:15	⚠️	3	TCP	Not Suspicious Traffic	192.168.1.140	50342	193.136.212.166	80	1:2013504	ET POLICY GNU/Linux APT User-Agent Outbound likely related to package management
05/19/2022 19:15:15	⚠️	3	TCP	Not Suspicious Traffic	192.168.1.140	50342	193.136.212.166	80	1:2013504	ET POLICY GNU/Linux APT User-Agent Outbound likely related to package management
05/19/2022 19:15:15	⚠️	3	TCP	Not Suspicious Traffic	192.168.1.140	50342	193.136.212.166	80	1:2013504	ET POLICY GNU/Linux APT User-Agent Outbound likely related to package management
05/19/2022 19:15:15	⚠️	3	TCP	Not Suspicious Traffic	192.168.1.140	50342	193.136.212.166	80	1:2013504	ET POLICY GNU/Linux APT User-Agent Outbound likely related to package management
05/19/2022 19:15:15	⚠️	3	TCP	Not Suspicious Traffic	192.168.1.140	50342	193.136.212.166	80	1:2013504	ET POLICY GNU/Linux APT User-Agent Outbound likely related to package management
05/19/2022 19:15:15	⚠️	3	TCP	Not Suspicious Traffic	192.168.1.140	53721	185.125.190.36	80	1:2013504	ET POLICY GNU/Linux APT User-Agent Outbound likely related to package management
05/19/2022 19:15:14	⚠️	3	TCP	Not Suspicious Traffic	192.168.1.140	53721	185.125.190.36	80	1:2013504	ET POLICY GNU/Linux APT User-Agent Outbound likely related to package management

Figura 59 - Avisos do sistema.

Realizando uma pequena pesquisa no Google com as descrições obtidas é possível concluir que estes alertas podem indicar ameaças reais visto que a gestão de pacotes do Linux contém algumas vulnerabilidades que dependendo do dispositivo e da versão podem ser prejudiciais.

Com a pesquisa realizada anteriormente é possível verificar que a quantidade de alertas sem quaisquer filtros tende a aumentar substancialmente podendo tornar-se uma dor de cabeça realizar a análise a todas as ameaças detetadas. Sendo assim é necessário realizar um ajuste no Suricata de modo a melhorar a sua análise e controlo de ameaças.

Primeiro é necessário aprender a navegar na página de alertas, sendo que clicando no botão com uma lupa é possível realizar uma operação de “name resolution” a ambos os IPs de origem e destino sendo que só é possível realizar esta operação em redes públicas. Realizando a operação no IP de destino é possível obter a informação a seguir apresentada.

The screenshot shows the 'Alert Log View Settings' interface. In the center, a modal dialog box displays the result of a name resolution for the IP address 10.1.1.1, which resolves to the host 'aerodent.canonical.com'. There is an 'OK' button at the bottom right of the dialog. Below the dialog, the main table shows the 'Last 250 Alert Entries' with three entries related to TCP traffic from 192.168.1.140 to 185.125.190.39, all labeled as 'ET POLICY GNU/Linux APT User-Agent' and 'Outbound likely related to package management'.

Figura 60 - Operação de "name resolution".

Clicando no símbolo é possível adicionar a regra a uma lista de supressão. Foi então realizada esta ação no símbolo do IP de origem sendo então criada uma lista de supressão tendo em conta aquele IP. De seguida é possível observar a lista criada acedendo ao menu “Services -> Suricata -> Suppress”.

The screenshot shows the 'Services / Suricata / Suppression List / Edit' page. The 'Suppress' tab is selected. A new suppression list named 'suppresslist' has been created. The 'General Information' section shows the name 'suppresslist' and a description 'Auto-generated list for Alert suppression'. The 'Suppression List Content' section contains several suppression rules, each starting with '#ET POLICY GNU/Linux APT User-Agent Outbound likely related to package management' followed by 'suppress gen_id 1, sig_id 2013504, track by_src, ip 192.168.1.140'. Below the rules, there is a note about valid keywords: 'Valid keywords are suppress', 'event_filter' and 'threshold'. Examples of usage are provided: 'Example 1: suppress gen_id 1, sig_id 1852, track_by_src, ip 10.1.1.54', 'Example 2: event_filter gen_id 1, sig_id 1851, type limit, track_by_src, count 1, seconds 60', and 'Example 3: threshold gen_id 135, sig_id 1, type threshold, track_by_src, count 100, seconds 1'.

Figura 61 - Criação da lista de supressão.

Tarefa 4 – NIDS (Avançado)

1. Testes Suricata utilizando ferramentas de rastreamento

De modo a ser mais prática a observação do que acontece no sistema foi necessário organizar o *dashboard*, sendo que ficou da maneira demonstrada de seguida.

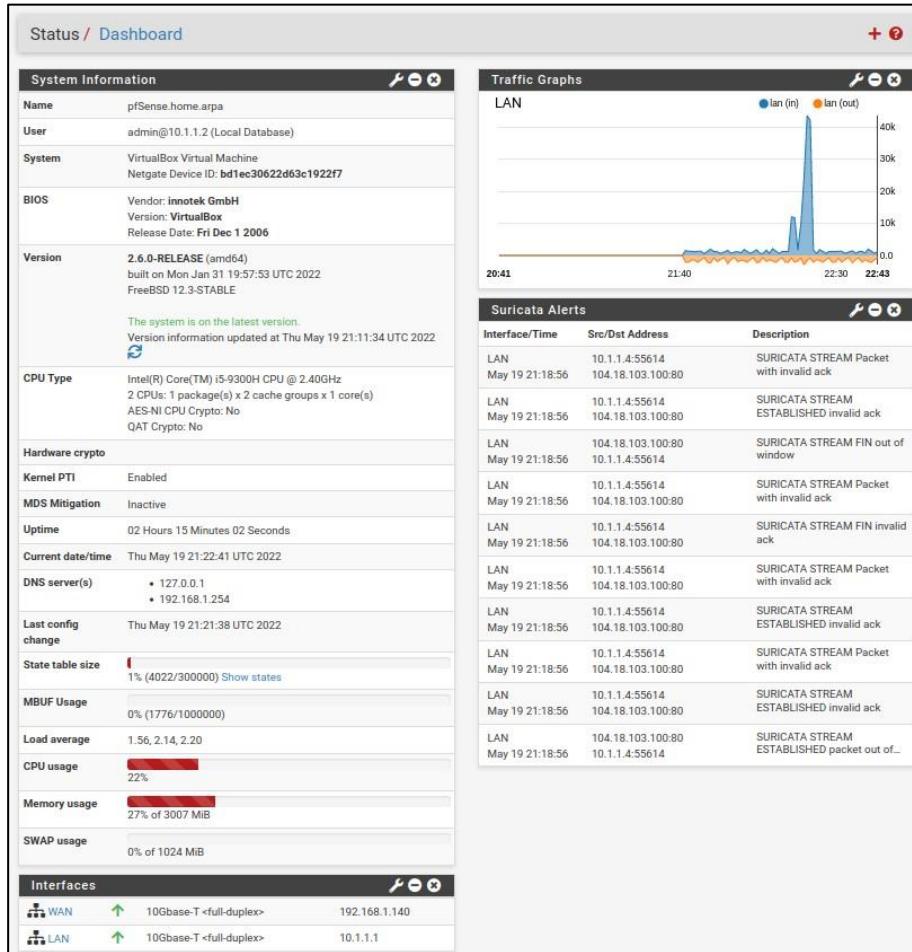


Figura 62 - Dashboard organizado.

Após isso foi realizado o comando apresentado na figura seguinte numa máquina virtual a correr o Kali.

```
(root㉿kali)-[~/home/kali]
# nmap -PS -v 10.1.1.0/24
Starting Nmap 7.92 ( https://nmap.org ) at 2022-05-19 17:23 EDT
Initiating ARP Ping Scan at 17:23
Scanning 255 hosts [1 port/host]
```

Figura 63 - Realização do comando nmap -PS -v.

Acedendo ao *dashboard* logo após a realização do comando do *nmap* é possível observar um pico grande de tráfego na altura do teste como demonstrado na próxima figura. É possível também constatar que não houve qualquer alerta ocorrido na rede LAN, o que era de esperar visto que o *nmap* apenas realiza *pings* através das portas mais usuais não sendo detetado como tráfego suspeito.

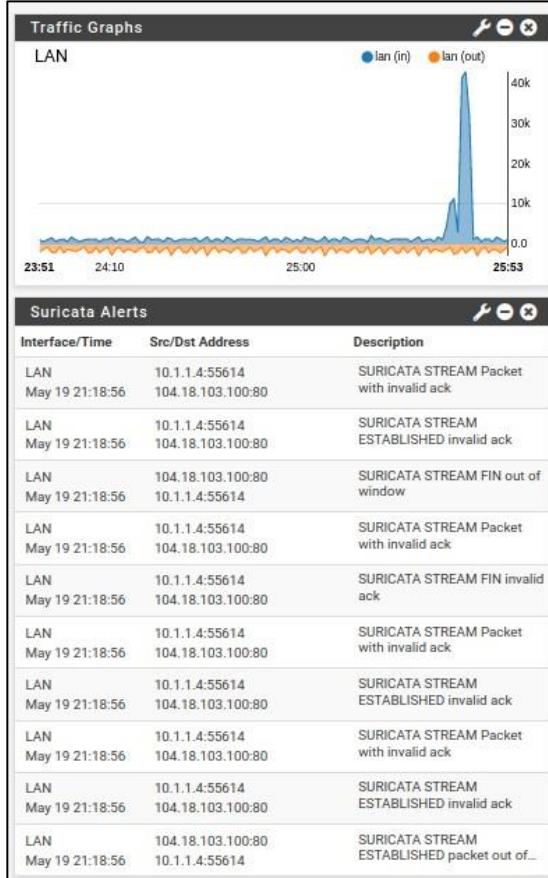


Figura 64 - Dashboard momentos após o teste nmap.

Foram realizados mais alguns testes alterando o parâmetro *-P* do comando do *nmap*, não sendo notada qualquer alteração relativamente à deteção de ameaças pois não foram acionados quaisquer alertas.

Após isso foi então realizado outro teste com um comando diferente, o comando apresentado na próxima figura.

```
(root㉿kali)-[~/home/kali]
└─# nmap -sS -v 10.1.1.1
Starting Nmap 7.92 ( https://nmap.org ) at 2022-05-19 17:47 EDT
Initiating ARP Ping Scan at 17:47
Scanning 10.1.1.1 [1 port]
Completed ARP Ping Scan at 17:47, 0.05s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 17:47
Completed Parallel DNS resolution of 1 host. at 17:47, 0.00s elapsed
Initiating SYN Stealth Scan at 17:47
Scanning pfSense.home.arpa (10.1.1.1) [1000 ports]
Discovered open port 53/tcp on 10.1.1.1
Discovered open port 80/tcp on 10.1.1.1
Completed SYN Stealth Scan at 17:47, 4.58s elapsed (1000 total ports)
Nmap scan report for pfSense.home.arpa (10.1.1.1)
Host is up (0.0010s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT      STATE SERVICE
53/tcp    open  domain
80/tcp    open  http
MAC Address: 08:00:27:60:EF:1B (Oracle VirtualBox virtual NIC)

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 4.76 seconds
Raw packets sent: 2001 (88.028KB) | Rcvd: 5 (204B)
```

Figura 65 - Realização do comando nmap -sS -v.

Mais uma vez não houve qualquer alerta por parte do Suricata utilizando o comando anterior. Alternado o parâmetro “-sS” para “-sX”, apesar de não ser possível detetar qualquer alerta, foi possível observar no *dashboard* uma grande quantidade de informação que foi enviada. Acedendo ao Wireshark de modo a ser possível retirar melhores ilações acerca do tráfego, foi possível observar o conteúdo presente na próxima figura em que é possível ver que foram enviados 2000 pacotes TCP para diferentes portas com as *flags* FIN, PSH e URG indicando que o pacote correspondia a uma conclusão de conexão (FIN), que os dados devem ser enviados diretamente para a aplicação e não colocados num buffer (PSH) e que os dados devem ser processados urgentemente (URG).

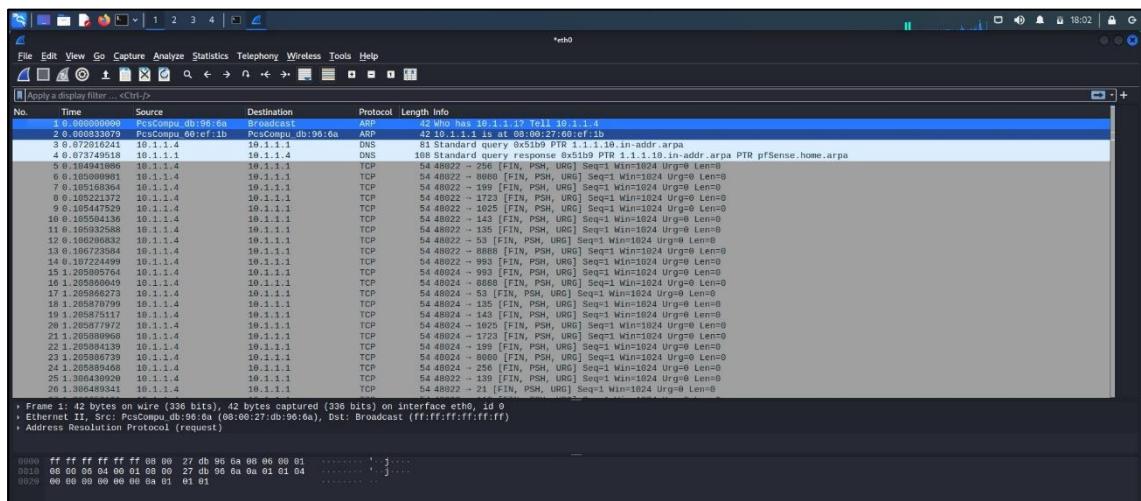


Figura 66 - Análise do tráfego no Wireshark.

Continuando sem receber qualquer tipo de alerta por parte do Suricata foi então realizado um novo comando do *nmap*, em que este é bastante mais intrusivo que os anteriores, pois efetua um rastreamento completo do alvo, incluindo serviços e as versões. O comando utilizado é o apresentado de seguida.

```
(root㉿kali)-[~/home/kali]
# nmap -A -v 10.1.1.1
Starting Nmap 7.92 ( https://nmap.org ) at 2022-05-19 18:06 EDT
NSE: Loaded 155 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 18:06
Completed NSE at 18:06, 0.00s elapsed
Initiating NSE at 18:06
Completed NSE at 18:06, 0.00s elapsed
Initiating NSE at 18:06
Completed NSE at 18:06, 0.00s elapsed
Initiating ARP Ping Scan at 18:06
Scanning 10.1.1.1 [1 port]
```

Figura 67 - Teste nmap com os argumentos -A e -v.

Realizando este último teste já foi possível obter alguns alertas apresentados de seguida como demonstrados no *dashboard* do servidor.

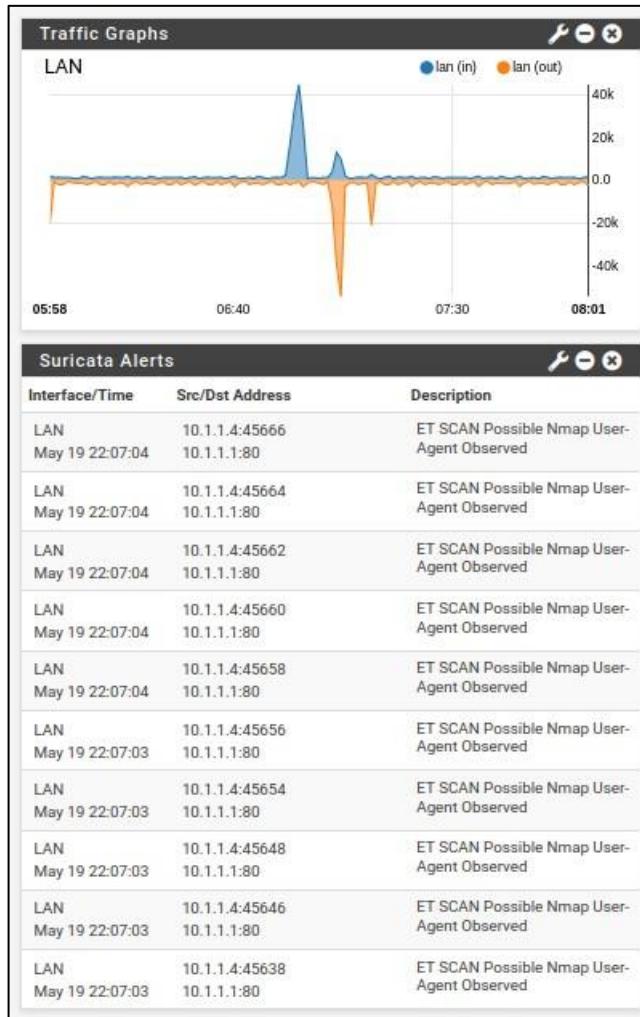


Figura 68 - Alertas da realização do nmap.

Para além dos alertas é também possível observar que a quantidade de tráfego foi bem maior do que a que era realizada nos testes anteriores, devido a uma pesquisa mais intrusiva do sistema. Quanto aos alertas, todos contêm a mesma descrição. Esta avisa o observador que há a possibilidade de este estar a ser vigiado por um agente *nmap*. Este alerta aparece, pois, ao realizar o comando “*nmap -A -v*” é possível retirar informações pessoais e que não devia ser partilhada com o exterior como os serviços que um sistema está a utilizar assim como o sistema operativo usado, pois através da obtenção destas informações é possível tirar partido das vulnerabilidades que possam existir de versões mais antigas ou até vulnerabilidades desconhecidas.

Realizando outro teste com a ferramenta *hping3* foi executado na máquina virtual a correr o Kali o comando seguinte.

```
(root@kali)-[~/home/kali]
# hping3 -S --flood 10.1.1.1
HPING 10.1.1.1 (eth0 10.1.1.1): S set, 40 headers + 0 data bytes
hping in flood mode, no replies will be shown
^C
— 10.1.1.1 hping statistic —
1308690 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
```

Figura 69 - Teste com a ferramenta *hping3*.

Acedendo ao *dashboard* enquanto o comando estava a correr é possível observar que a utilização do CPU se encontrava a 100% o que é um mau indicador visto que este teste estava a congestionar o sistema. Para além disso, ao observar o gráfico do tráfego é possível observar que estava a ser gerado uma enorme quantidade de transferência de dados tendo em conta que a escala do gráfico atinge os 1 Mbps. Tomando atenção à área dos alertas é possível reparar num novo alerta que apareceu aquando da realização do comando, em que este tem como descrição “SURICATA STREAM 3way handshake wrong seq wrong ack” sendo que a regra era “alert tcp any any -> any any”. De seguida é apresentado a imagem do *dashboard* obtido.

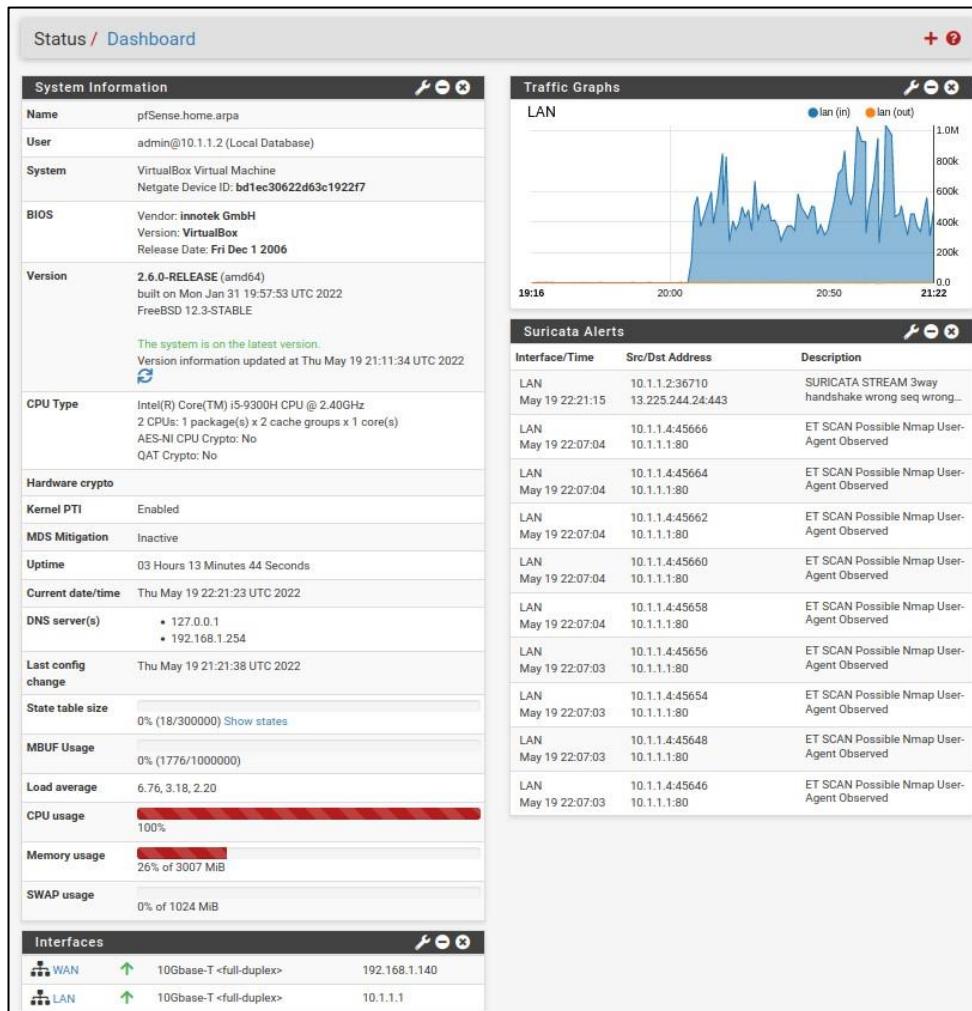


Figura 70 - Ecrã do dashboard aquando da realização do comando.

Finalmente foi realizado um último comando com o objetivo de obter mais alguns alertas do que anteriormente de modo a realizar uma melhor análise destes. O comando é o apresentado de seguida e foi realizado na VM a correr o Kali.

```
(root@kali)-[~/home/kali]
# hping3 -S --flood --rand-source 10.1.1.1
HPING 10.1.1.1 (eth0 10.1.1.1): S set, 40 headers + 0 data bytes
hping in flood mode, no replies will be shown
^C
-- 10.1.1.1 hping statistic --
344842 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
```

Figura 71 - Realização do comando `hping3 -S --flood --rand-source`.

Observando o *dashboard* do utilizador é possível verificar que mais uma vez a utilização do CPU do sistema atingiu os 100% e que a quantidade de informação transmitida é enorme, pois o gráfico de tráfego chega a atingir taxas de transmissão a rondar os 800Kbps. Quanto às regras, surgiu um número elevado em que todas tinham a mesma descrição (“ET DROP Spamhaus DROP Listed Traffic Inbound group X”) alterando apenas o número do grupo (X). Este comando despoletou alertas baseados nas listas anti-spam, pois foram encontrados IPs cujo tráfego tinha origem em IPs pertencentes a estas listas. Isto pode não significar diretamente que se trata de um ataque DoS, no entanto, como foram muitos os avisos que surgiram e a quantidade enorme de tráfego transmitido, pode ter sido esta a causa do aparecimento dos avisos.

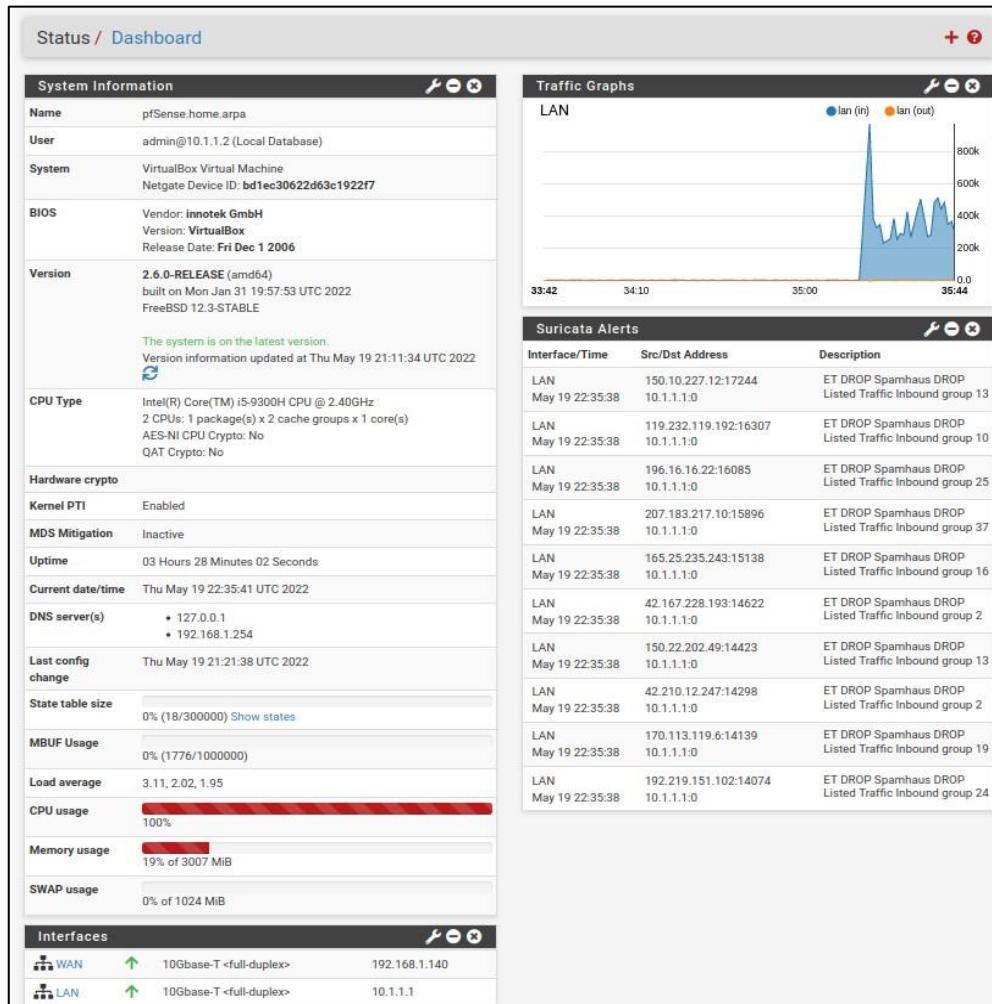


Figura 72 - Visualização do dashboard.

2. Utilização da ferramenta Pytbull

Primeiramente foi necessário realizar a instalação da ferramenta Pytbull realizando o download do ficheiro, descompactando-o e movendo este para a pasta *opt* do sistema operativo.

Após esta instalação foi necessário aceder ao ficheiro *config.cfg* e realizar algumas alterações ficando o ficheiro como demonstrado de seguida.

```
GNU nano 6.2
[CLIENT]
ipaddr          = 10.1.1.4
iface            = eth0
useproxy         = 0
proxyhost        =
proxyport        =
proxyuser        =
proxypass        =

[PATHS]
db               = data/pytbull.db
urlpdf           = https://github.com/sebastiendamaye/public/raw/master/infected/
pdfdir           = pdf/malicious
pcapdir          = pcap
tempfile         = /tmp/pytbull.tmp
#alertsfile      = /var/log/snort/alert
#alertsfile      = /var/log/suricata/fast.log
alertsfile       = /home/rui/Desktop/Ciber/alertsfile.log

[ENV]
sudo             = /usr/bin/sudo
nmap             = /usr/bin/nmap
nikto            = /usr/bin/nikto
niktoconf        = /etc/nikto.conf
hping3           = /usr/sbin/hping3
tcpreplay        = /usr/bin/tcpreplay
ab               = /usr/bin/ab
ping             = /usr/bin/ping
ncrack           = /usr/bin/ncrack
ncrackusers     = data/ncrack-users.txt
ncrackpasswords = data/ncrack-passwords.txt
localhost        = 127.0.0.1

[FTP]
ftpproto        = sftp
ftpport          = 22
ftpuser          = root
ftppasswd        =

[TIMING]
sleepbeforegetalerts = 2
sleepbeforenexttest = 2
sleepbeforetwoftp   = 2
urlltimeout        = 10

[SERVER]
reverseshellport  = 12345

[TESTS]
clientSideAttacks = 1
testRules          = 1
badTraffic         = 1
fragmentedPackets = 1
bruteForce         = 1
evasionTechniques = 1
shellCodes         = 1
denialOfService    = 1
pcapReplay         = 1
normalUsage        = 1
ipReputation       = 1

[TESTS_PARAMS]
ipreputationnbttests = 10
```

Figura 73 - Ficheiro de configuração do pytbull.

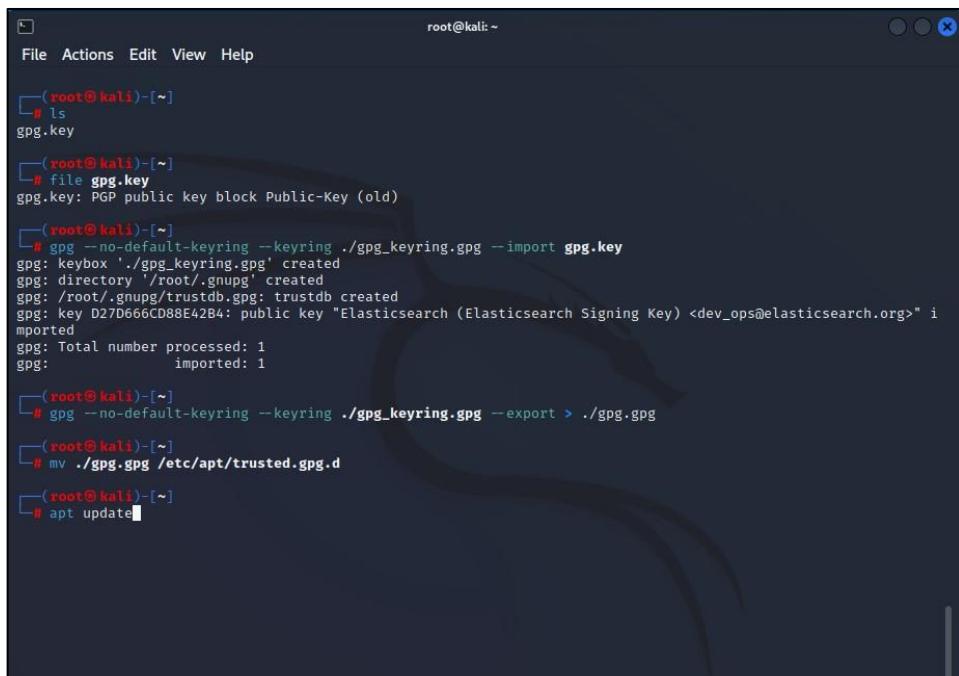
O primeiro conjunto de testes que foi realizado foi os testes **ShellCode**, através da realização do comando demonstrado de seguida na VM com o Kali.

Figura 74 - Execução do comando ./pytbyll -t 10.1.1.2.

Apesar de no enunciado pedir que fosse observado os alertas que apareciam aquando da realização do comando anterior, ao observar o *dashboard* não foi possível detetar qualquer alerta. De modo a comprovar que realmente o comando funcionou e os testes estavam a ser executados foi acedido ao *Wireshark* onde foi possível ver a troca de pacotes entre as 2 máquinas com uma quantidade de tráfego razoável.

Tarefa 5 – NIDS (Complementar)

Primeiro foi necessário realizar a instalação da ferramenta **ELK** (Elasticsearch, Longstash e Kibana) realizando os comandos demonstrados de seguida. Para além destes, de modo a concluir a instalação foi necessário realizar também os comandos *apt install elasticsearch/longstash/kibana*.



```
root@kali: ~
File Actions Edit View Help
└─(root㉿kali)-[~]
    └─# ls
        gpg.key

    └─(root㉿kali)-[~]
        └─# file gpg.key
            gpg.key: PGP public key block Public-Key (old)

    └─(root㉿kali)-[~]
        └─# gpg --no-default-keyring --keyring ./gpg_keyring.gpg --import gpg.key
            gpg: keybox './gpg_keyring.gpg' created
            gpg: directory '/root/.gnupg' created
            gpg: /root/.gnupg/trustdb.gpg: trustdb created
            gpg: key D27D666CD88E42B4: public key "Elasticsearch (Elasticsearch Signing Key) <dev_ops@elasticsearch.org>" imported
            gpg: Total number processed: 1
            gpg: imported: 1

    └─(root㉿kali)-[~]
        └─# gpg --no-default-keyring --keyring ./gpg_keyring.gpg --export > ./gpg.gpg

    └─(root㉿kali)-[~]
        └─# mv ./gpg.gpg /etc/apt/trusted.gpg.d

    └─(root㉿kali)-[~]
        └─# apt update
```

Figura 75 - Instalação da ferramenta ELK.

Com a ferramenta instalada foi necessário proceder a algumas configurações iniciais. Relativamente ao *Kibana* foi necessário realizar uma pequena alteração no ficheiro de configuração “*kibana.yml*”, como demonstrado de seguida.



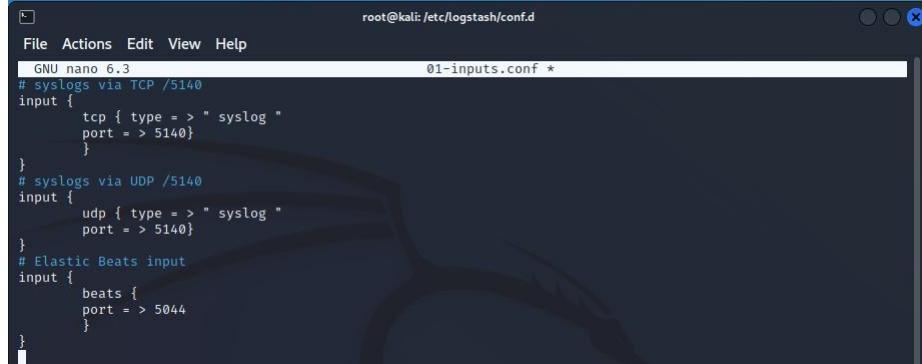
```
root@kali: /etc/kibana
File Actions Edit View Help
GNU nano 6.3                                     kibana.yml *
# Kibana is served by a back end server. This setting specifies the port to use.
server.port: 5601

# Specifies the address to which the Kibana server will bind. IP addresses and host names are both valid values.
# The default is 'localhost', which usually means remote machines will not be able to connect.
# To allow connections from remote users, set this parameter to a non-loopback address.
server.host: "0.0.0.0"

# Enables you to specify a path to mount Kibana at if you are running behind a proxy.
# Use the 'server.rewriteBasePath' setting to tell Kibana if it should remove the basePath
# from requests it receives, and to prevent a deprecation warning at startup.
# This setting cannot end in a slash.
#server.basePath: ""
```

Figura 76 - Configuração do ficheiro *kibana.yml*.

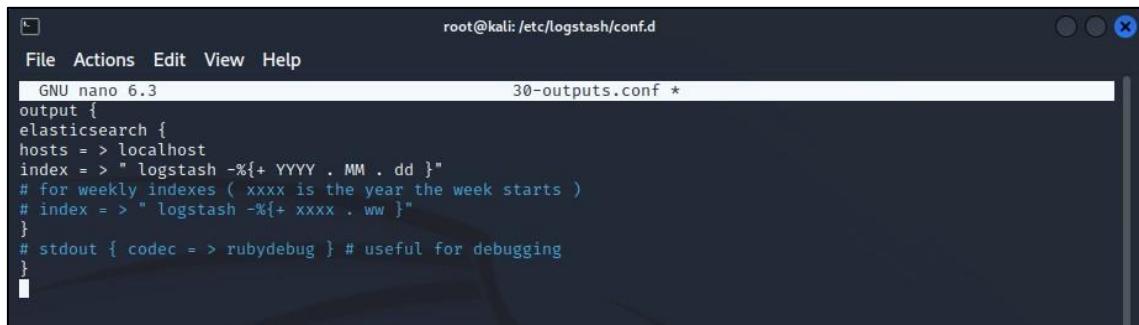
Relativamente ao *Logstash*, foi necessário criar 2 ficheiros de configuração em que o primeiro, *01-inputs.conf*, foi criado para permitir aceitar entradas da porta 5140 através de TCP e UDP e da porta 5044 através de TCP. O ficheiro criado para as entradas foi configurado como demonstrado a seguir.



```
root@kali: /etc/logstash/conf.d
GNU nano 6.3                                     01-inputs.conf *
# syslogs via TCP /5140
input {
    tcp { type => "syslog"
        port => 5140}
}
# syslogs via UDP /5140
input {
    udp { type => "syslog"
        port => 5140}
}
# Elastic Beats input
input {
    beats {
        port => 5044
    }
}
```

Figura 77 - Ficheiro de configuração *01-inputs.conf*.

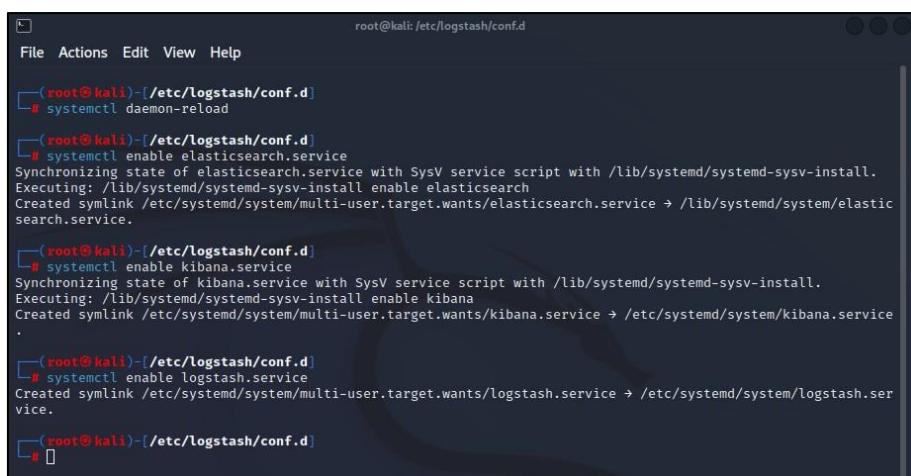
Outro ficheiro que teve de ser criado foi o ficheiro *30-outputs.conf*, correspondente às saídas do *Logstash* com o objetivo de encaminhar os dados para o módulo *Elasticsearch*. O ficheiro foi configurado da seguinte maneira.



```
root@kali: /etc/logstash/conf.d
GNU nano 6.3                                     30-outputs.conf *
output {
    elasticsearch {
        hosts => localhost
        index = > "logstash-%{+ YYYY . MM . dd }"
        # for weekly indexes ( xxxx is the year the week starts )
        # index = > "logstash-%{+ xxxx . ww }"
    }
    # stdout { codec => rubydebug } # useful for debugging
}
```

Figura 78 - Ficheiro de configuração *30-outputs.conf*.

Foram também realizados os seguintes comandos com o objetivo de configurar os serviços para que estes iniciem automaticamente quando for realizado o *boot* do sistema.



```
(root@kali)-[ /etc/logstash/conf.d ]
# systemctl daemon-reload

(root@kali)-[ /etc/logstash/conf.d ]
# systemctl enable elasticsearch.service
Synchronizing state of elasticsearch.service with SysV service script with /lib/systemd/systemd-sysv-install.
Executing: /lib/systemd/systemd-sysv-install enable elasticsearch
Created symlink /etc/systemd/system/multi-user.target.wants/elasticsearch.service → /lib/systemd/system/elasticsearch.service.

(root@kali)-[ /etc/logstash/conf.d ]
# systemctl enable kibana.service
Synchronizing state of kibana.service with SysV service script with /lib/systemd/systemd-sysv-install.
Executing: /lib/systemd/systemd-sysv-install enable kibana
Created symlink /etc/systemd/system/multi-user.target.wants/kibana.service → /etc/systemd/system/kibana.service.

(root@kali)-[ /etc/logstash/conf.d ]
# systemctl enable logstash.service
Created symlink /etc/systemd/system/multi-user.target.wants/logstash.service → /etc/systemd/system/logstash.service.

(root@kali)-[ /etc/logstash/conf.d ]
#
```

Figura 79 Configuração automática dos serviços.

Como demonstração do funcionamento dos sistemas devidamente instalados foi acedido num browser aos endereços *localhost:5601* (para o *Kibana*) e *localhost:9200* (para o *Elasticsearch*). De seguida é demonstrado o seu correto funcionamento com o aparecimento de duas janelas indicativas dos sistemas.

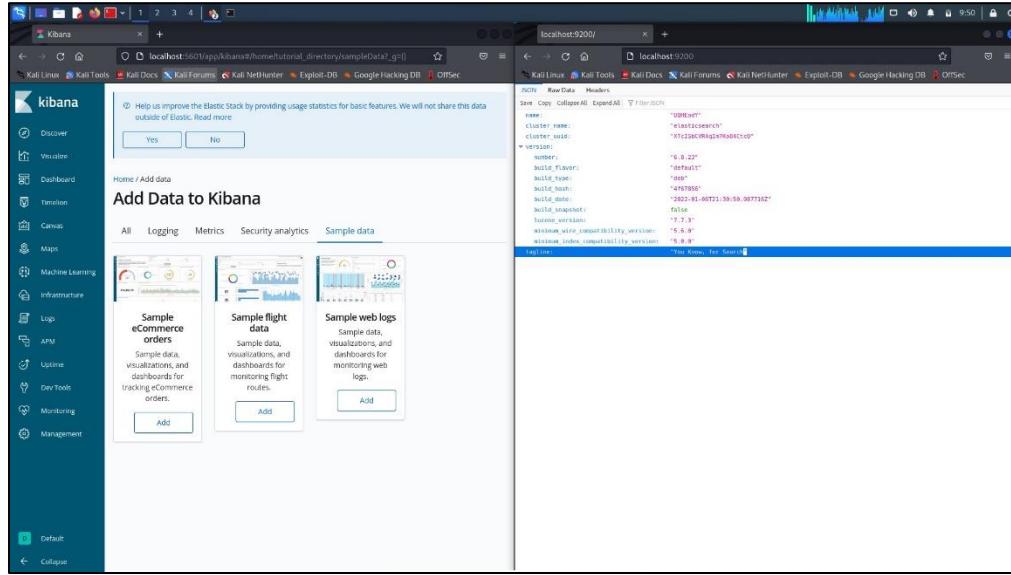


Figura 80 - Acesso aos serviços iniciados.