



INSTITUTO POLITÉCNICO DE BEJA
Escola Superior de Tecnologia e Gestão
Licenciatura em Engenharia Informática
Tópicos de Engenharia Informática

WAF – Web Application Firewall

Martinho José Novo Caeiro - 23917
Paulo António Tavares Abade - 23919



Beja, março de 2025

INSTITUTO POLITÉCNICO DE BEJA
Escola Superior de Tecnologia e Gestão
Licenciatura em Engenharia Informática
Tópicos de Engenharia Informática

WAF – Web Application Firewall

Martinho José Novo Caeiro - 23917
Paulo António Tavares Abade - 23919

Orientador: Professor Armando Ventura

Beja, março de 2025

Resumo

Neste relatório será abordado o processo de instalação da máquina Servidor com o uso do AlmaLinux, os pacotes instalados e a configuração de DNS, Virtual Hosts e WAF para a realização do Projeto. Este relatório foi realizado no âmbito da Unidade Curricular de Tópicos de Engenharia Informática (IPBeja, 2025).

Keywords: almalinux, putty, dns, virtual hosts, waf

Abstract

In this report, we will address the installation process of the Server machine using AlmaLinux, the installed packages and the configuration of DNS, Virtual Hosts and WAF for the completion of the Project.

Keywords: almalinux, putty, dns, virtual hosts, waf

Índice

1	Introdução	1
2	Introdução Teórica	2
2.1	DNS	2
2.2	Virtual Hosts	2
2.3	WAF	2
3	Configuração de Máquinas	3
4	Instalação de Pacotes	4
5	Configuração de Serviços	5
5.1	DNS	5
5.2	Virtual Hosts	9
6	WAF	14
7	Testes com o Kali Linux	19
8	Conclusão	20
	Bibliografia	21

Índice de Figuras

1	Exemplo de Máquina Utilizada	3
2	Demonstração de funcionamento do DNS	8
3	Demonstração dos Virtual Hosts	13
4	Ecrã de login da WAF	15
5	Atribuição de Nome ao Serviço	16
6	Atribuição de Servidor Host	16
7	Bloqueio de IPs	17
8	Aplicação do Recaptcha	18
9	Bloqueio de Países	18

1 Introdução

Para a realização do projeto é necessária a configuração de duas máquina AlmaLinux, Servidor e WAF. Em seguida são configurados os serviços DNS, Virtual Hosts e WAF. Para a configuração de todos estes serviços foi utilizado o Putty (Putty, 2025) que permitiu inserir comandos mais rapidamente.

2 Introdução Teórica

2.1 DNS

O DNS (Domain Name System) é um sistema hierárquico e distribuído que permite a resolução de nomes de domínio em endereços IP, permitindo que os utilizadores acessem a sites e serviços na Internet de forma mais fácil.

2.2 Virtual Hosts

Os Virtual Hosts permitem que um único servidor Apache hospede múltiplos sites ou aplicações web, cada um com o seu próprio nome de domínio e configuração. Isto é feito através da criação de entradas de configuração específicas para cada domínio.

2.3 WAF

O WAF (Web Application Firewall) é uma solução de segurança que protege aplicações web contra ataques e vulnerabilidades. Ele atua como uma camada adicional de defesa, analisando as requisições e respostas entre o cliente e o servidor, bloqueando atividades maliciosas e garantindo a integridade e confidencialidade dos dados.

3 Configuração de Máquinas

A instalação AlmaLinux (AlmaLinux, 2025) , foi feita na máquina Servidor com o uso de um .iso fornecido pelo docente da UC. Para a instalação foi necessário a criação de um disco de 8GB de espaço com três partições cujas quais são:

- Partição /boot - 500MB em ext4
- Partição swap - 1000MB
- Partição / - Resto do Disco em ext4

Informações adicionais incluem 1MB de RAM e dois processadores de CPU e a rede está em modo 'bridge'. No instalador foi definida a palavra-passe do 'root' como '1234', KDUMP desativado e nomes de rede 'server.tei.pt' e 'waf.tei.pt' para o Servidor e WAF respetivamente.

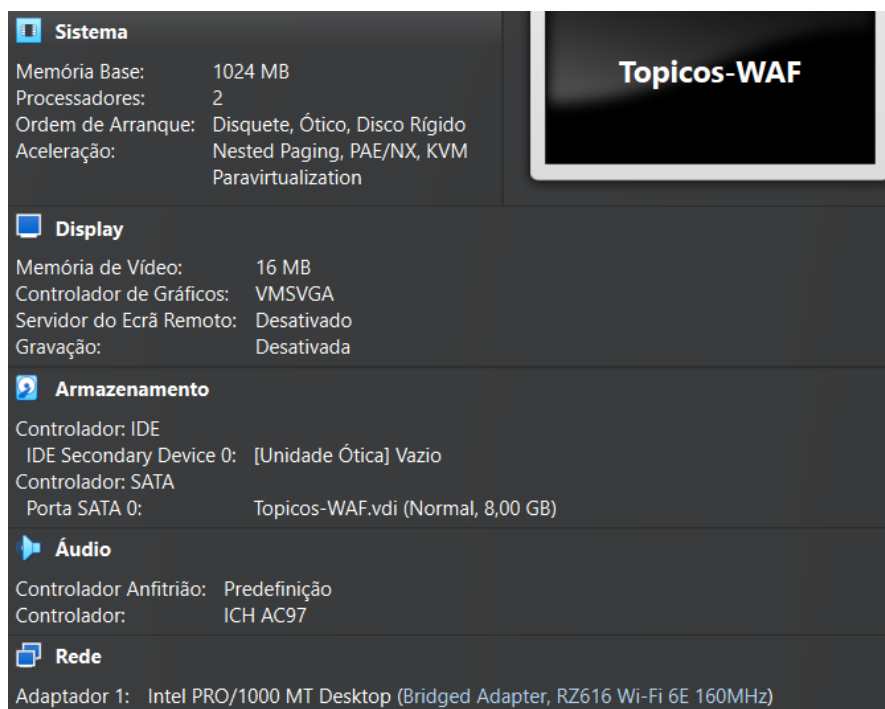


Figura 1: Exemplo de Máquina Utilizada

4 Instalação de Pacotes

A firewall foi desativada com o comando **systemctl disable --now firewalld** e desativado o SELinux, necessitando a edição do ficheiro **/etc/selinux/config** e alteração da linha **SELINUX=enforcing** para **SELINUX=disabled**. Adicionalmente, foi necessário instalar os seguintes pacotes para a configuração dos serviços:

Servidor:

- **nano** - Para a edição de ficheiros
- **whois** - Para verificar o IP da máquina
- **bind** - Para o DNS
- **bind-utils** - Para o DNS
- **httpd** - Para as Virtual Hosts

WAF:

- **nano** - Para a edição de ficheiros
- **nginx** - Para a WAF
- **epel-release** - Para a WAF
- **bunkerweb** - Para a WAF

5 Configuração de Serviços

5.1 DNS

Primeiramente é inicializado o DNS com o comando **systemctl enable --now named**. Em seguida, para a configuração do DNS, foram feitas as seguintes alterações no ficheiro **/etc/named.conf** com o uso do Putty:

- Adicionado *"any;"* nas linhas de *listen-on port 53* e *allow-query;*
- Adicionadas as zonas forward.

Zonas Forward

```
zone "trinta.org" {
    type master;
    file "/var/named/trinta.org.hosts";
};

zone "3emfrente.eu" {
    type master;
    file "/var/named/3emfrente.eu.hosts";
};

zone "the.com" {
    type master;
    file "/var/named/the.com.hosts";
};

zone "tei.pt" {
    type master;
    file "/var/named/tei.pt.hosts";
};
```

Também necessitamos criar um ficheiro de configuração com caminho dado anteriormente em cada zona, cujos quais são:

Zonas Forward

```
nano /var/named/trinta.org.hosts

$TTL 86400

@ IN SOA server.tei.pt. admin.tei.pt. (
2024051701 ; Serial
3600      ; Refresh
1800      ; Retry
604800    ; Expire
86400 )    ; Minimum TTL

IN NS server.tei.pt.

IN A 192.168.1.100

www IN A 192.168.1.100
```

```
nano /var/named/3emfrente.eu.hosts

$TTL 86400

@ IN SOA server.tei.pt. admin.tei.pt. (
2024051701 ; Serial
3600      ; Refresh
1800      ; Retry
604800    ; Expire
86400 )    ; Minimum TTL

IN NS server.tei.pt.

IN A 192.168.1.100

www IN A 192.168.1.100
```

```

nano /var/named/the.com.hosts

$TTL 86400

@ IN SOA server.tei.pt. admin.tei.pt. (
2024051701 ; Serial
3600      ; Refresh
1800      ; Retry
604800    ; Expire
86400 )    ; Minimum TTL

IN NS server.tei.pt.

IN A 192.168.1.100

www IN A 192.168.1.100

```

```

nano /var/named/tei.pt.hosts

$TTL 86400

@ IN SOA server.tei.pt. admin.tei.pt. (
2024051701 ; Serial
3600      ; Refresh
1800      ; Retry
604800    ; Expire
86400 )    ; Minimum TTL

IN NS server.tei.pt.

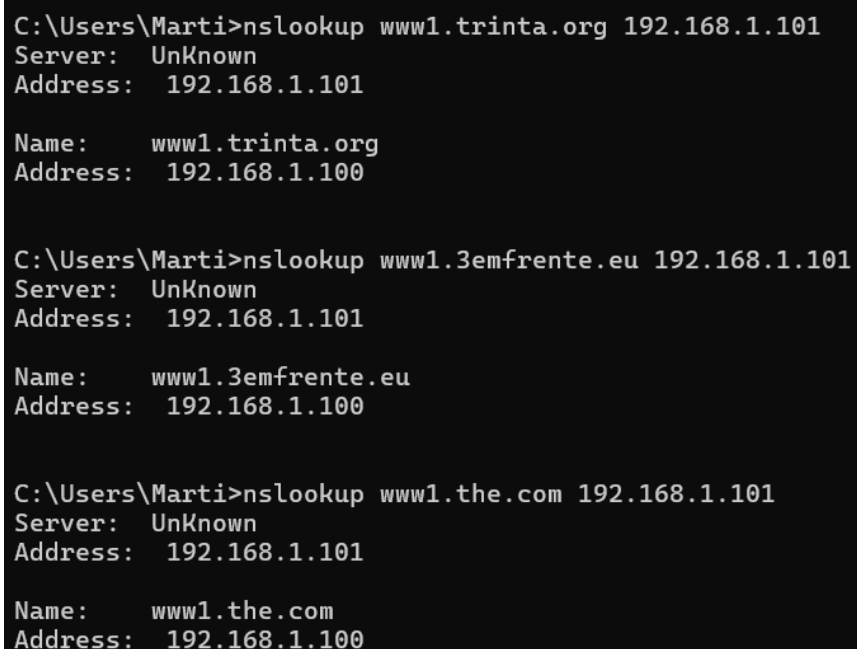
IN A 192.168.1.100

waf IN A 192.168.1.100

server IN A 192.168.1.100

```

Após serem configurados os ficheiros, é necessário reiniciar o serviço DNS com o comando `systemctl restart named`.



```
C:\Users\Marti>nslookup www1.trinta.org 192.168.1.101
Server:  UnKnown
Address:  192.168.1.101

Name:     www1.trinta.org
Address:  192.168.1.100

C:\Users\Marti>nslookup www1.3emfrente.eu 192.168.1.101
Server:  UnKnown
Address:  192.168.1.101

Name:     www1.3emfrente.eu
Address:  192.168.1.100

C:\Users\Marti>nslookup www1.the.com 192.168.1.101
Server:  UnKnown
Address:  192.168.1.101

Name:     www1.the.com
Address:  192.168.1.100
```

Figura 2: Demonstração de funcionamento do DNS

Como podemos verificar, o DNS está a funcionar corretamente.

5.2 Virtual Hosts

Primeiramente é necessária a criação de três utilizadores **trinta.org**, **3emfrente.eu** e **the.com** com a palavra-passe **1234**. É em seguida, é necessário criar o ficheiro `/etc/httpd/conf/httpd.conf` com o seguinte conteúdo:

```
NameVirtualHost 192.168.30.10:80
<VirtualHost 192.168.30.10:80>
DocumentRoot "/home/trinta.org/"
ServerName www.trinta.org
ServerAlias trinta.org
<Directory "/home/trinta.org">
Options Indexes FollowSymLinks
AllowOverride All
Order allow,deny
Allow from all
Require method GET POST OPTIONS
</Directory>
</VirtualHost>
```

```

NameVirtualHost 192.168.30.10:443

<VirtualHost 192.168.30.10:443>
    DocumentRoot "/home/trinta.org/"
    ServerName www.trinta.org
    ServerAlias trinta.org
    <Directory "/home/trinta.org">
        Options Indexes FollowSymLinks
        AllowOverride All
        Order allow,deny
        Allow from all
        Require method GET POST OPTIONS
    </Directory>
</VirtualHost>

NameVirtualHost 192.168.30.10:80

<VirtualHost 192.168.30.10:80>
    DocumentRoot "/home/3emfrente.eu/"
    ServerName www.3emfrente.eu
    ServerAlias 3emfrente.eu
    <Directory "/home/3emfrente.eu">
        Options Indexes FollowSymLinks
        AllowOverride All
        Order allow,deny
        Allow from all
        Require method GET POST OPTIONS
    </Directory>
</VirtualHost>

```

```
NameVirtualHost 192.168.30.10:443
<VirtualHost 192.168.30.10:443>
DocumentRoot "/home/3emfrente.eu/"
ServerName www.3emfrente.eu
ServerAlias 3emfrente.eu
<Directory "/home/3emfrente.eu">
Options Indexes FollowSymLinks
AllowOverride All
Order allow,deny
Allow from all
Require method GET POST OPTIONS
</Directory>
</VirtualHost>
```

```
NameVirtualHost 192.168.30.10:80
<VirtualHost 192.168.30.10:80>
DocumentRoot "/home/the.com/"
ServerName www.the.com
ServerAlias the.com
<Directory "/home/the.com">
Options Indexes FollowSymLinks
AllowOverride All
Order allow,deny
Allow from all
Require method GET POST OPTIONS
</Directory>
</VirtualHost>
```

```
NameVirtualHost 192.168.30.10:443

<VirtualHost 192.168.30.10:443>

DocumentRoot "/home/the.com/"

ServerName www.the.com

ServerAlias the.com

<Directory "/home/the.com">

Options Indexes FollowSymLinks

AllowOverride All

Order allow,deny

Allow from all

Require method GET POST OPTIONS

</Directory>

</VirtualHost>
```

Finalmente, é necessário criar as diretorias para cada um dos sites, com os seguintes comandos:

```
mkdir /home/trinta.org/public_html  
mkdir /home/3emfrente.eu/public_html  
mkdir /home/the.com/public_html
```

Após a criação das diretorias, é necessário criar um ficheiro **index.html** em cada um dos diretórios com o seguinte conteúdo:

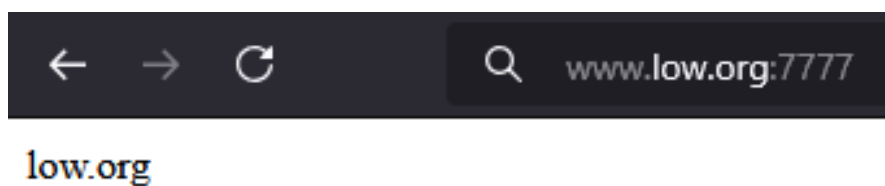


Figura 3: Demonstração dos Virtual Hosts

Como podemos verificar, após realizar os comandos **systemctl restart named** e **systemctl restart httpd** os sites já se encontram funcionais.

6 WAF

Para a configuração do WAF foi seguido o guia que está no site do BunkerWeb (BunkerWeb, 2025), e foram feitas as seguintes alterações no ficheiro `/etc/yum.repos.d/nginx.repo`:

```
[nginx-stable]
name=nginx stable repo
baseurl=http://nginx.org/packages/centos/$releasever/$basearch/
gpgcheck=1
enabled=1
gpgkey=https://nginx.org/keys/nginx_signing.key
module_hotfixes=true

[nginx-mainline]
name=nginx mainline repo
baseurl=http://nginx.org/packages/mainline/centos/$releasever/$basearch/
gpgcheck=1
enabled=0
gpgkey=https://nginx.org/keys/nginx_signing.key
module_hotfixes=true
```

Em seguida fazemos os seguintes comandos para a instalação dos pacotes já mencionados:

```
yum install nginx-1.26.3 -y
yum install epel-release -y
curl -s https://repo.bunkerweb.io/install/script.rpm.sh | sudo bash
yum check-update
yum install bunkerweb-1.6.1 -y
```

Para evitar que o Nginx e BunkerWeb atualizem automaticamente, foram feitos os comando `yum versionlock add nginx` e `yum versionlock add bunkerweb`.

Agora é possível configurar a WAF através do browser, acedendo ao endereço **https://192.168.1.100/setup**. Iremos dar ao utilizador **root** a palavra-passe **Tei1234.** e para aceder à WAF a qualquer outra altura é apenas necessário aceder ao endereço **https://192.168.1.100/login**.

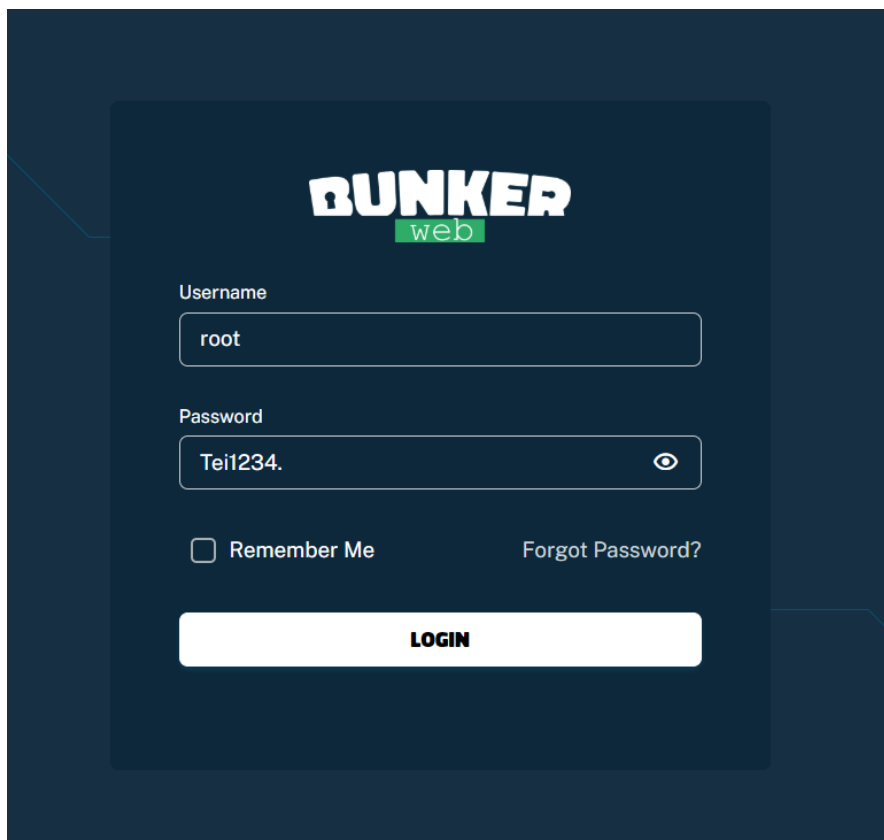
The image shows a login page for 'BUNKER web'. The background is dark blue with a lighter blue square in the center containing the login form. At the top of the form is the 'BUNKER web' logo, with 'BUNKER' in white and 'web' in a green box. Below the logo are two input fields: 'Username' with the value 'root' and 'Password' with the value 'Tei1234.'. To the right of the password field is an eye icon. Below the password field are two links: 'Remember Me' with an unchecked checkbox and 'Forgot Password?'. At the bottom of the form is a white 'LOGIN' button.

Figura 4: Ecrã de login da WAF

Para a criação de regras, iremos à aba **Services** e clicamos em **New Service**. Iremos dar o nome correto ao serviço na secção 1, no nosso caso iremos ter três serviços:

- **www1.trinta.org**
- **www1.3emfrente.eu**
- **www1.the.com**

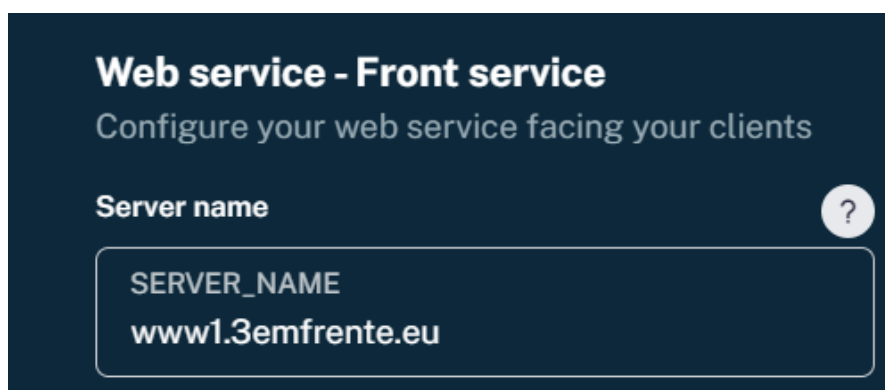


Figura 5: Atribuição de Nome ao Serviço

Na secção 2, iremos escolher o servidor host, cujo qual vai ser o endereço de cada um dos sites:

- **http://www1.trinta.org**
- **http://www1.3emfrente.eu**
- **http://www1.the.com**

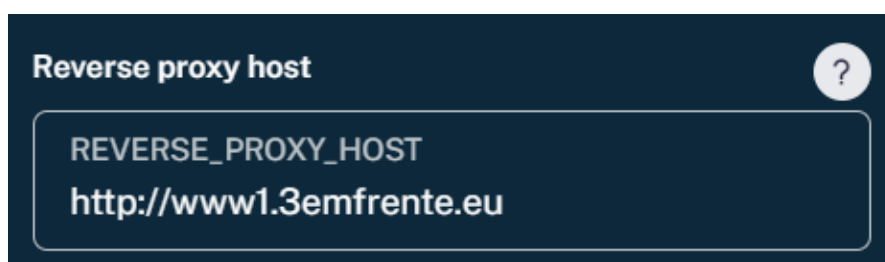


Figura 6: Atribuição de Servidor Host

Na secção 6 iremos adicionar IPs à nossa Blacklist, no nosso caso iremos adicionar o IP **...adicionar ip...** que é proveniente da maquina Kali Linux.

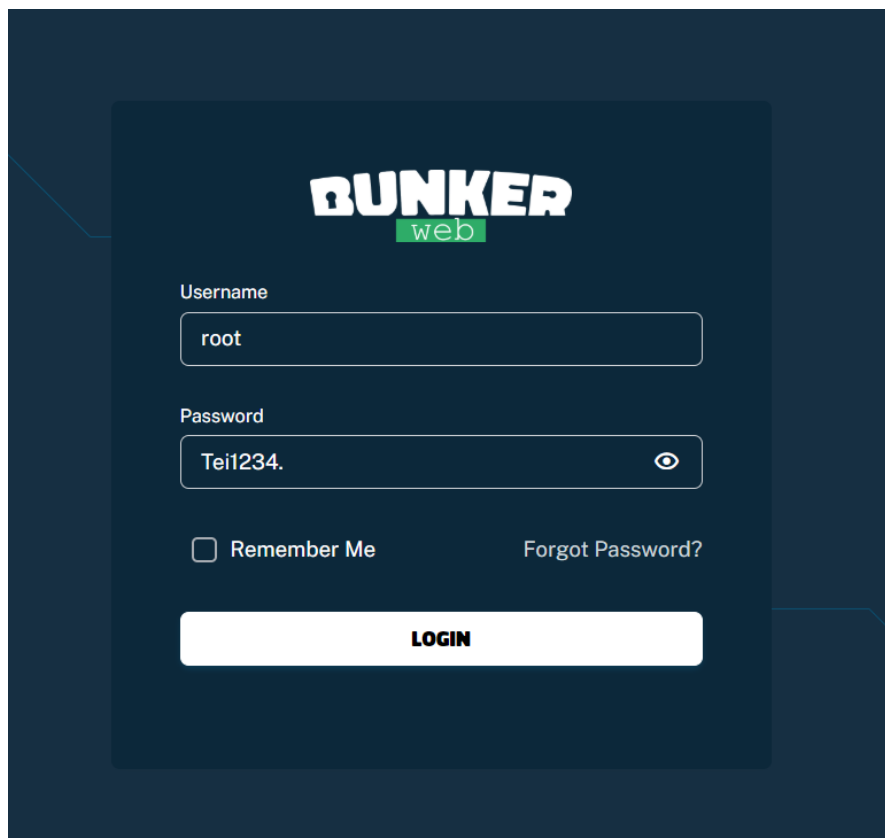
The image shows a login page for 'BUNKER web'. The page has a dark blue background with a central white login form. The form contains the following elements: a 'Username' label above a text input field containing 'root'; a 'Password' label above a text input field containing 'Tei1234.' with a toggle eye icon on the right; a checkbox labeled 'Remember Me'; a link labeled 'Forgot Password?'; and a large white 'LOGIN' button at the bottom. The 'BUNKER web' logo is at the top of the form, with 'BUNKER' in white and 'web' in white text on a green rectangular background.

Figura 7: Bloqueio de IPs

Na secção 8 iremos ativar o Aimbot através de Recaptcha e na secção 10 iremos adicionar Portugal à lista de países bloqueados.

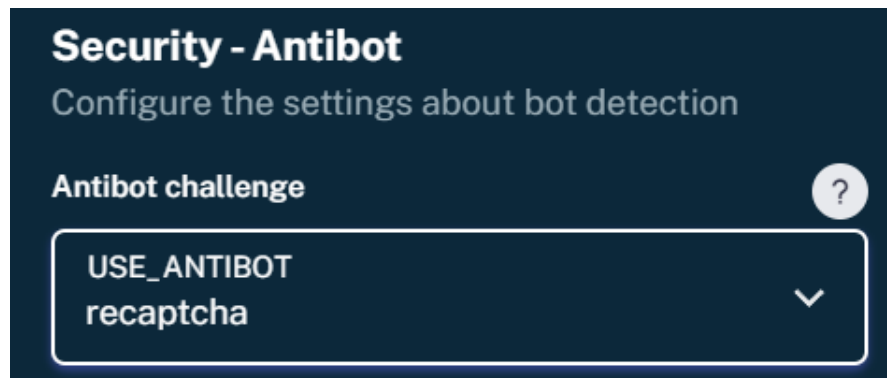


Figura 8: Aplicação do Recaptcha

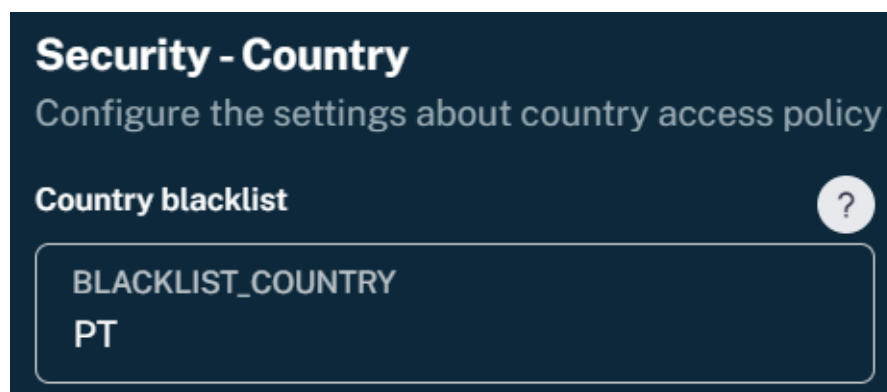


Figura 9: Bloqueio de Países

7 Testes com o Kali Linux

Para testar a WAF, foi utilizado o Kali Linux (Kali Linux, 2025) com o uso da ferramenta **Nikto**.

Estes foram os resultados obtidos:

8 Conclusão

Todos os serviços foram implementados com sucesso, dado que a sua maioria foi semelhante ao Laboratório 2 da Unidade Curricular de Administração de Sistemas. Apenas não foram utilizados os IP pedidos dado que o importante era a configuração dos serviços e não o IP em si. Este projeto permitiu adquirir conhecimentos sobre este Tópico e as diferentes possibilidades de manter os serviços seguros. Além disso, a configuração de WAF é essencial para garantir a segurança das aplicações web, protegendo-as contra ataques e vulnerabilidades.

Bibliografia

- AlmaLinux. (2025). *Repositorio AlmaLinux* [Instalador AlmaLinux]. Obtido maio 29, 2025, de https://repo.almalinux.org/almalinux/8.10/isos/x86_64/AlmaLinux-8.10-x86_64-minimal.iso
- BunkerWeb. (2025). *Quickstart guide - BunkerWeb documentation* [Guia BunkerWeb]. Obtido maio 29, 2025, de <https://docs.bunkerweb.io/latest/quickstart-guide/#basic-setup>
- IPBeja. (2025). *Disciplina: Tópicos de Engenharia Informatica / IPBeja* [Página TEI]. Obtido maio 29, 2025, de <https://cms.ipbeja.pt/course/view.php?id=2775>
- Kali Linux. (2025). *Get Kali / Kali Linux* [Instalador Kali Linux]. Obtido maio 29, 2025, de <https://www.kali.org/get-kali/>
- Putty. (2025). *Download PuTTY: latest release (0.83)* [Instalador Putty]. Obtido maio 29, 2025, de <https://www.chiark.greenend.org.uk/~sgtatham/putty/latest.html>