

TeSP de Cibersegurança e Redes Informáticas



Footpriting

Disciplina: Cibersegurança Ativa

Alunos:

Diogo Garcia - 2231620

Lourenço Índio -2231606

Ivo Silva – 2231617

Zhi Ruan – 2231605

Professor: Carlos Antunes

2024/2025

## Conteúdo

[1. Quadro Recapitulativo de Informação 3](#_Toc183721089)

[2. Informação de IP e DNS 3](#_Toc183721090)

[3. Informação de Plataformas 4](#_Toc183721091)

[4. Informação Diversa Relevante 5](#_Toc183721092)

[5. Conclusão 6](#_Toc183721093)

# Quadro Recapitulativo de Informação

Neste quadro e um resumo das principais descobertas realizadas durante o Footpriting do domínio da aemgnascente.pt.

|  |  |
| --- | --- |
| Área | Descrição |
| Objetivos |  |
| Data de Começo | 20/11/2024 |
| Data de Conclusão | 29/11/2024 |
| Vulnerabilidades encontradas |  |

# Informação DNS

1. **Informação do servidor:**

Data de criação: 14/1/2015

Data de espiração: 13/1/2025

Donos: Agrupamento Escolas Marinha Grande Nascente

País: Portugal

Cidade: Marinha Grande

Localidade: Abrantes

Rua: Rua Prof.ª Amélia Cândida

Código Postal: 2430-053

Ferramentas utilizada: Whois

1. **Informações de IP:**

Endereço IP encontrados:

192.168.1.254

195.8.30.246

195.8.30.245

195.8.1.57

195.8.21.58

94.46.128.199

94.46.180.200 - IP do servidor aemgnascente.pt

Ferramentas utilizada: nslookup \ dig

1. **URL’S encontrados:**

www.aemgnascente.pt

areareservada.aemgnascente.pt

www.areareservada.aemgnascente.pt

autodiscover.aemgnascente.pt

bar.aemgnascente.pt

www.bar.aemgnascente.pt

cpanel.aemgnascente.pt

cpcalendars.aemgnascente.pt

cpcontacts.aemgnascente.pt

ferias.aemgnascente.pt

www.ferias.aemgnascente.pt

giae.aemgnascente.pt

mail.aemgnascente.pt

paa.aemgnascente.pt

www.paa.aemgnascente.pt

teste.aemgnascente.pt

www.teste.aemgnascente.pt

webdisk.aemgnascente.pt

webmail.aemgnascente.pt

wiki.aemgnascente.pt

[www.wiki.aemgnascente.pt](http://www.wiki.aemgnascente.pt)

Ferramentas utilizada: sublist3r

1. **DNS:**

Nome do domínio: aemgnascente.pt

Servidores DNS encontrados:

ns2.bdm.microsoftonline.com

ns1.bdm.microsoftonline.com

ns3.bdm.microsoftonline.com

ns4.bdm.microsoftonline.com

Ferramentas utilizada: Whois

# Informação de Plataformas

1. **Servidor web detetados:**

* **Tecnologias web utilizadas:**

CMS: Joomla

Web servers: Nginx

JavaScript frameworks: MooTools

Programmig languages: PHP

Security: Imunify360

JavaScript libraries: Spin.js, jQuery, jQuery Migarte

Miscellaneous: HTTP/2

Reverse proxies: Nginx

Ferramentas utilizada: Wappalyzer

* **Sistemas Operacionais:**

Servidor: Linux 4.4

Ferramentas utilizada: nmap

1. **Informação de Utilizadores**

* **Contas de usuário encontradas:**

Email do administrador: [registry@buydomain.pt](mailto:registry@buydomain.pt)

Emails dos donos: prof.selmaseco@gmail.com, [f976@aemgnascente.pt](mailto:f976@aemgnascente.pt)

1. **Informação Histórica**

* **Histórico de alterações de DNS:**

Mudanças recentes nos servidores de nomes.

Dados de registro histórico de domínio (via Whois).

* **Tecnologias e frameworks históricos:**

Versões antigas do WordPress, servidores anteriores (Apache vs. Nginx).

# Informação Diversa Relevante

# Conclusão

Finalize o relatório com uma breve conclusão, resumindo os principais achados do footprinting, as vulnerabilidades identificadas, e sugestões de ações a serem tomadas.