POLITÉCNICO DE LEIRIA | ESCOLA SUPERIOR DE TECNOLOGIA E GESTÃO

Relatório Prático

Mestrado em Cibersegurança e Informática Forense

Teste de penetração do domínio Foradoras.pt

Filipe Henriques, 2180066

Tiago Martins, 2182716

Leiria, junho de 2019

This page was inthetionally left blank

Lista de Figuras

This page was intetionally left blank

Lista de Tabelas

This page was intetionally left blank

Índice

Introdução

No âmbito da unidade curricular de Laboratório de Testes de Penetração, do curso de Mestrado Cibersegurança e Informática Forense da Escola Superior de Tecnologia e Gestão do Instituto Politécnico de Leiria, foi elaborado o presente relatório de Teste de penetração do domínio "foradoras.pt".

Após a fase de *footprinting*, são iniciadas as fases do teste de penetração, cuja autorização deste tipo de ação, é necessária para proceder de forma legal. Desta forma, a primeira fase a efetuar é uma recolha de informação adicional sobre o *website* do domínio alvo, informação esta, que é relativa aos serviços internos usados no servidor para o *website* "foradoras.pt". Depois disto, as fases posteriores resumem-se numa fase de ataques com a finalidade de ganhar acesso ao alvo, nomeadamente, ataques às credenciais, ataques usando as vulnerabilidades. Com isto concluído, as restantes fases consistem na exploração de formas de escalonamento de privilégios no *website*, e na exploração de vulnerabilidades encontradas no *website*.

Este trabalho tem como objetivo a realização de atividades para o "*hacking* ético", que é uma generalização de modo a abranger um vasto leque de testes referentes a segurança. Estes testes passam pela análise de vulnerabilidades, intrusão, autenticação *web*, *reverse engineering*, *open source intelligence*, entre outras subcategorias e testes específicos.

O presente relatório está dividido em quatro capítulos, sendo que o primeiro consiste na fase de recolha de informação restrita, como informações sobre os serviços usados pelo website, e informações que circulação internamente na rede do domínio alvo.

No segundo capítulo, é efetuado o ganho do acesso ao *website*, usando para isto ferramentas que facilitem a execução de ataques às credenciais e acesso, e ataques por vulnerabilidades.

No terceiro capítulo, são exploradas vulnerabilidades no *website* para provocar o escalonamento de privilégios nas contas de utilizadores obtidas na fase anterior.

Por fim, o relatório termina no quarto capítulo onde é realizado um levantamento dos objetivos atingidos, a conclusão sobre o trabalho feito, e recomendações futuras.

1. *Sniffing / Scanning / Enumeration*

1.1. Scanning e Enumeration

Para esta fase do teste de penetração, utilizou-se a ferramenta *zenmap* para efetuar o *scanning* dos portos do domínio alvo. *Zenmap* é uma *interface* gráfica *open source* para a ferramenta *nmap*. Esta permite a efetuar o reconhecimento de rede e auditorias de segurança. [1] Para este trabalho, utilizou-se o *zenmap* com o intuito da descoberta de portos abertos.

Para executar o *zenmap* basta introduzir no campo "*target*" o domínio "foradoras.pt", escolhe o tipo de comando *nmap* a executar que neste caso é um comando para procurar todos os portos, tanto TCP como UDP, e o processo de *scanning* iniciou-se ao pressionar o botão de "*Scan*". Com isto, foi possivel obter a informação de vários portos abertos, nomeadamente, os portos:

- 21\tcp, serviço FTP (Pure-FTPd)
- 80\tcp, serviço HTTP (Apache httpd)
- 110\tcp, serviço POP3 (Dovecot pop3d)
- 143\tcp, serviço IMAP (Dovecot imapd)
- 443\tcp, serviço SSL/HTTP (Apache httpd)
- 465\tcp, serviço SSL/SMTP (Exim smtpd 4.92)
- 587\tcp, serviço SMTP (Exim smtpd 4.92)
- 993\tcp, serviço SSL/IMAPS
- 995\tcp, serviço SSL/POP3S
- 53\udp, serviço *Domain* (DNS)

O mesmo se pode verificar ao efetuar o mesmo processo utilizando o endereço IP do domínio como "target". Estes são os portos abertos que são normais existirem em servidores *web*, no entanto, é possivel explorar algum dos serviços nestes portos caso estes usem uma versão antiga. Infelizmente o *zenmap* não devolveu tal informação. O resultado completo dos *scannings* efetuados pelo *zenmap* podem ser visualizados em Anexo I – Resultado no *zenmap*.

Para a enumeração dos serviços, utilizou-se a ferramenta *Sparta*. Esta é uma ferramenta com *interface* gráfica desenvolvida em *python*, que permite executar as funcionalidades necessárias para a fase de *scanning* e *enumeration* em testes de penetração.

Neste caso, a ferramenta será utilizada para efeitos de enumeração. *Sparta* é uma ferramenta que integra outras ferramentas como, por exemplo, o *nmap* e *nikto*. [2] Para executar o *scanning* ou *enumeration* nesta ferramenta, é adicionado na coluna dos *hosts* o endereço IP do domínio "foradoras.pt", sendo que depois de adicionado é iniciado o processo em etapas. Com isto foi possivel obter 20 portos abertos e filtrados, sendo que dos abertos, o porto 2082 TCP não consta nos resultados do *zenmap*. Já o porto 53 UDP, que o *zenmap* encontrou aberto, o *Sparta* não encontra. Os restantes portos obtidos por esta ferramenta, são *filtered* o que significa que o servidor não respondeu ao pedido SYN do *nmap*. A lista completa de portos encontrados pela ferramenta pode ser visualizada na Tabela 1.

Tabela 1 - Lista de portos no *Sparta*

Porto	Protocolo	Estado	Nome	Versão
21	tcp	Open	FTP	Pure-FTPd
22	tcp	Filtered	SSH	
23	tcp	Filtered	TELNET	
25	tcp	Filtered	SMTP	
80	tcp	Open	HTTP	Apache HTTPd
110	tcp	Open	POP3	Dovecot POP3d
111	tcp	Filtered	RPCBind	
135	tcp	Filtered	MSRPC	
137	tcp	Filtered	Netbios-ns	
137	udp	Open | Filtered	Netbios-ns	
139	tcp	Filtered	Netbios-ssn	
143	tcp	Open	IMAP	Dovecot IMAP
161	udp	Open | Filtered	SNMP	
162	udp	Open | Filtered	SNMPtrap	
443	tcp	Open	HTTP	
445	tcp	Filtered	Microsoft-ds	
465	tcp	Open	SMTP	Exim SMTPd 4.92
500	udp	Open | Filtered	ISAKMP	
587	tcp	Open	SMTP	Exim SMTPd 4.92
993	tcp	Open	IMAPs	
995	tcp	Open	POP3s	
1433	tcp	Filtered	MS-SQL-S	
1434	udp	Open | Filtered	MS-SQL-M	
2049	tcp	Filtered	NFS	
2082	tcp	Open	Infowave	

3306	tcp	Filtered	MySQL	
3389	tcp	Filtered	MS-WBT-Server	
5060	udp	Open | Filtered	SIP	
5432	tcp	Filtered	Postgrespl	
8080	tcp	Filtered	HTTP-proxy	

1.2. Sniffing

Em termos de ferramentas para *sniffing*, aqui não foram utilizadas nenhumas diretamente na rede do alvo, sendo que o objetivo proposto para este teste de penetração, no domínio "foradoras.pt", prende-se apenas com exploração de vulnerabilidades do *website* neste domínio e não da rede. Deste modo consideramos importante demostrar, quão fácil é comprometer as credenciais enviadas em *cleartext* com um ataque passivo de *sniffing* numa rede local.

Para esta demostração, criou-se uma rede *Wi-Fi* privada, e, utilizou-se uma ferramenta de recolha de pacotes de rede, o *Wireshark* 3.0.2. [3] O cenário de demonstração, será a realização de uma tentativa de *login* na página *wp-login.php* do "foradoras.pt". Antes efetuar a tentativa de *login*, utilizou-se o *Wireshark* para ligar-se à rede *Wi-Fi* privada. Com isto, procedeu-se à tentativa de *login* com o *username* "admin" e *password* "12345", ao que foi possivel visualizar esta informação no pacote HTTP, capturado na ferramenta de *sniffing* (ver Figura 1).

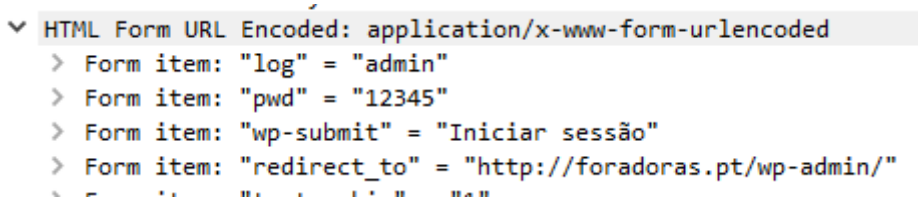

Figura 1 - Pacote HTTP com credenciais em *cleartext*

Como se pode ver com esta demonstração, é relativamente fácil descobrir as credenciais de acesso do *website*, se a rede utilizada pelo administrador estiver alvo de um ataque passivo de *sniffing*. Isto apenas é possivel devido à falta de encriptação dos dados enviados nos pacotes na rede. A solução neste cenário será em obter um certificado digital e utilizar o protocolo HTTPS para assegurar a confidencialidade dos dados enviados.

2. Ganho de Acesso

2.1. Ataque às credenciais

Para efetuar ataques de dicionário, criou-se uma lista de passwords com o auxílio de uma ferramenta CUPP (*Common User Passwords Profiler*), onde se forneceram algumas informações pessoais sobre o proprietário do domínio com o objetivo de criar uma lista de possíveis passwords. Estas informações foram recolhidas de diferentes fontes, mas maioritariamente da página de Facebook do proprietário, e de outras pessoas relacionadas com o mesmo. Quanto ao utilizador, utilizaram-se alguns nomes que foram identificados como potenciais nomes de utilizador por uma ferramenta específica para *WordPress*, *WPScan*, que vai ser abordada mais à frente.

Após a criação destas listas recorreu-se a uma ferramenta de *brute forcing*, neste caso a *patator* [4], uma pequena ferramenta desenvolvida em *python* que permite efetuar este tipo de ataques a múltiplos serviços. Fizeram-se ataques às várias páginas web encontradas, *cPanel*, *WHM*, *Webdisk*, *Wordpress Login* e também ao serviço de FTP, e ao serviço de POP3. No entanto, todos estes pontos de acesso estavam protegidos contra múltiplas tentativas de *login*, pelo que o acesso ao *host* era bloqueado após apenas algumas tentativas, forçando a utilização de vários servidores VPN para mudar o endereço IP de ataque.

Sendo o site desenvolvido em *WordPress*, fez-se uso à ferramenta *WPScan* presente no *Kali* de maneira a encontrar mais informações acerca da versão que estava instalada, dos plugins instalados e respetivas versões, e temas instalados. Com esta informação seria possível procurar vulnerabilidades específicas às versões das tecnologias instaladas. No entanto, não foi possível descobrir informações acerca dos plugins e dos temas apenas da versão do *WordPress* que era a 5.1.1, a mais recente até à data, e que segundo os *patch notes*, corrigia o CVE-2019-9787. Também com o *WPScan*, foi possível listar os utilizadores do *WordPress*, que neste caso era apenas um, "morgado".

2.2. Ataques por vulnerabilidades

De modo a explorar alguma vulnerabilidade no domínio para ganhar acesso, optou-se por utilizar duas ferramentas para ajudar a identificar possivel vulnerabilidades, o *Nessus* [5] e *Pyfuzz* [6]. Com a ferramenta *Nessus*, que é uma aplicação *web* que permite efetuar *scans* e análises para identificar vulnerabilidades e outro tipo de informações, foram executados dois *scans*: o *scan* de vulnerabilidades *web* e o *scan* avançado.

Com scan as vulnerabilidades web, a informação mais crítica que o *Nessus* encontrou foi um aviso de nível médio, no qual era relativo à potencialidade da existência de *Clickjacking*. Esta vulnerabilidade consiste basicamente na existência de um link escondido numa página alvo com o objetivo de a vítima clicar no link sem este se aperceber. Mas como o website alvo só é utilizado por um utilizador, esta vulnerabilidade não ajuda no ganho de acesso. Contudo esta vulnerabilidade pode ser resolvida, segundo o *Nessus*, devolver o HTTP *header X-Frame-Options* ou *Content-Security-Policy* com a resposta da página.

Já no scan avançado, foi possivel identificar mais avisos, sendo noves destes os maís críticos, também do nível médio. Algumas destas vulnerabilidades são:

- Possibilidade de exploração de algumas diretorias do *website*. Vulnerabilidade esta que já é explorada por ferramentas já utilizadas, e que será outra vez efetuado com o *pyfuzz*;
- Certificado SSL de não confiança. Isto deve-se ao certificado ser auto assinada, mas qualquer das formas esta é um falso positivo sendo que o website não utiliza HTTPS;
- Certificado SSL com *Hostname* errado. Isto deve-se também pelo facto dos domínios alojados no servidor onde estão, partilharem o mesmo endereço IP, o que apresenta o mesmo PTR para o domínio “flexicamais.com”;
- Outra vulnerabilidade é as passwords serem enviadas em *cleartext* entre o cliente e o servidor no serviço de POP3. O mesmo problema foi encontrado no scan anterior mas na página de *login* do *website* e *Cpanel*, que possibilita a exposição da password caso existia um ataque de *sniffing* na rede. Mas como a rede está fora dos limites deste trabalho, esta vulnerabilidade foi ignorada.

Com isto, passou-se à ferramenta *Pyfuzz*. Esta é uma ferramenta de linha de comandos em *python* que permite efetuar URL *fuzzing* que é uma técnica para descobrir diretorias e

ficheiros escondidos num servidor *web*. Nesta ferramenta foi possivel encontrar ficheiros como o *xmlprc.php*, *license.txt*; e diretorias como *wp-admin*, *wp-content*. O *Pyfuzz* tem a utilidade de apresentar os tamanhos de cada diretoria/ficheiro que encontra, desta forma são facilmente identificados ficheiros com possivel informação sensível. No total, foram encontradas 232 páginas no website "foradoras.pt", estas podem ser visualizadas em Anexo II – Resultado do *Pyfuzz*.

Também foi utilizado o *WPScan*, que é uma ferramenta de linha de comandos, própria para identificar vulnerabilidades de websites em *WordPress*. [7] Neste foi possivel encontrar páginas e ficheiros importantes, para analisar possíveis vulnerabilidades no qual poderemos explorar. Aqui foi possivel encontrar o ficheiro *robots.txt*, no qual é possivel identificar o que é permitido indexar e o que não é, pelos motores de pesquisa. Identificar que existem *must_use_plugins plugins* em uso, que significa que o *website* está a utilizar plugins que estão instalados numa diretoria especial, e por isto, estes *plugins* não existem na lista de *plugins* na página de *Plugins* do *wp-admin*. E também, tal como no *Pyfuzz*, outras páginas e ficheiros escondidos presentes em websites de *WordPress*. Por fim, como a versão do *WordPress* em uso é uma das mais recentes, e com atualizações de segurança, a versão 5.1.1., esta ferramentas não identificou nenhuma vulnerabilidade significativa.

Com isto, efetuou-se outro tipo de explorações de vulnerabilizes relativas a outros serviços. Uma destas vulnerabilidades é uma bastante recente, o CVE-2019-7524. Esta é uma vulnerabilidade entre as versões 2.2.36.3 e a anterior à 2.3.5.1 do *Dovecot* que possibilita um atacante local provocar um *buffer overflow* no processo de *indexer-worker* que pode ser utilizado para ganhar acesso ao privilégio *root*. [8] Sendo que os serviços de POP3 e IMAP no domínio, utilizam uma versão não conhecida por nós do *Dovecot*, concluímos que seria melhor evitar este ataque e focar noutros ataques.

Outra vulnerabilidade também bastante recente tinha a ver com o serviço de SMTP, neste caso mais especificamente a servidores que corressem o *Exim* de versão 4.87 até à 4.91. Esta vulnerabilidade, CVE-2019-10149, funciona através do envio de um email onde no recipiente era injetado um comando *bash* encodificado, onde esse comando era corrido no servidor como *root*. [9] A partir daqui seria possível criar um utilizador em qualquer um dos serviços disponíveis no servidor permitindo assim o acesso total à máquina. No entanto ao efetuar o *netcat* ao servidor no porto onde corria o SMTP verificou-se que a versão instalada era a 4.92, onde este *exploit* já estava corrigido.

Como este site tinha a maior parte das tecnologias atualizadas até à última versão, procedeu-se à exploração de outros domínios que estivessem no mesmo servidor e que fossem do mesmo proprietário. Neste caso explorou-se o domínio "www.myownportugal.com".

Este domínio estava muito mais negligenciado em termos de atualizações, o *WordPress* encontrava-se na versão 4.4.2 e o *WPScan* listava 56 vulnerabilidades.

A partir daqui exploraram-se as vulnerabilidades onde não fosse necessário ter credenciais. Uma destas vulnerabilidades envolvia a funcionalidade de repor a palavra passe, onde era enviado um *email* de *reset* de *password* para um endereço diferente do servidor. Era necessário injetar no POST, um *header Host* com um endereço malicioso, em que depois a função que define o endereço para onde o *email* seria enviado, procura esse *Host* injetado e envia o *email* com o link de reposição de *password* para o *email* "wordpress@<domínio-malicioso>". No entanto, após múltiplas tentativas com ferramentas distintas como o *PostMan* e a extensão para *Google Chromei - Web Spy,* não foi possível obter resultados positivos. O endereço malicioso utilizado era o "mailinator.com", um serviço de *email* público que permite colocar qualquer nome "@mailinator.com" podendo assim criar um endereço de *email* com o nome pretendido que era "wordpress".

Outra vulnerabilidade explorada era uma tentativa de *SQL Injection* via uma página onde o parâmetro GET "id" não estava devidamente "sanitizado", sendo assim possível efetuar comandos SQL não autorizados. No entanto quando se tentou utilizar a ferramenta do Kali SQLMap, após poucas tentativas, o nosso IP foi bloqueado, tendo assim que se recorrer a outro servidor de VPN.

3. Escalonamento de privilégios

Com isto, não foi possível obter nenhum tipo de acesso aos serviços *web* do domínio "foradoras.pt" devido ao facto dos serviços utilizados apresentarem as versões mais recentes o que evita a execução de *exploits* conhecidos, e também por existirem medidas contra ataques de força bruta para tentativas de *login* sucessivas. Assim sendo, neste capítulo, será exemplificada uma forma de provocar o escalonamento de privilégios através de um dos *exploits* conhecidos mais recentes, CVE-2018-20152. [10]

Este *exploit* permite a um utilizador qualquer, aceder a funcionalidades que apenas podem ser acedidas por administradores, o que permite guardar XSS e objetos de injeção no *WordPress*. Este *exploit* tira partido de da criação de *posts* do *WordPress* usados por *plugins* populares, como o *Contact Form 7*, para conseguir publicar *posts* com as credenciais da base de dados do *WordPress website*. Desta forma, a grande maioria dos *plugins* populares são vulneráveis a este *exploit*. [11]

No fundo, o importante seria encontrar uma maneira de adquirir, no melhor dos casos uma *Shell*, ou então uma maneira de alterar os ficheiros presentes no servidor, de modo a que se conseguisse de alguma forma passar a ter acesso ao *cPanel* ou ao terminal do servidor. Ao ter acesso a um destes dois, seria então possível controlar essencialmente todos os serviços presentes na máquina.

4. Conclusão

Foi possivel concluir na fase de *Sniffing / Scanning / Enumeration* que, muita da informação já recolhida na fase de *footprinting* com as ferramentas *shodan* e *censys*, é outra vez apresentada com as ferramentas utilizadas agora na fase de *Sniffing / Scanning / Enumeration*. No entanto, as ferramentas desta fase não proporcionaram devolver a todos os portos descobertos no *shodan* e *censys*. Desta forma, nada de novo se pode tirar desta fase, visto que as ferramentas no *footprinting* já mostravam toda a informação obtida nas ferramentas de *zenmap* e *Sparta*. Só o *sniffing* da rede não foi efetuado devido ao âmbito proposto para teste de penetração ao domínio "foradoras.pt".

Um ponto bastante importante que foi possível concluir na fase de Ganho de Acesso, é que não é necessário ter grandes conhecimentos de Cibersegurança para manter um simples domínio seguro, apenas basta seguir boas práticas como manter as tecnologias atualizadas sempre que possível, e utilizar *passwords* geradas aleatoriamente com um bom nível de entropia que vão dificultar bastante o trabalho de um hacker, tendo este que passar à utilização de *zero day exploits* ou a engenharia social ou *network sniffing*. No entanto, se houverem mais websites diferentes no mesmo servidor, e estes não estiverem devidamente atualizados, poderá ser possível através de *exploits* conhecidos, ganhar o acesso e escalar privilégios até ao servidor em si, tendo assim comprometido todo o sistema.

Desta forma as recomendações que deixamos ao proprietário do domínio, é que continue a manter não só o domínio principal atualizado, mas sim todos os domínios, páginas *web* e outras tecnologias e serviços a correr no servidor, de modo a dificultar bastante o uso de *exploits* conhecidos.

O servidor já aparentava ter bons mecanismos contra ataques de *bruteforcing*, pelo que apenas se refere que se devem aplicar boas práticas na criação de passwords, nunca recorrendo a informações pessoais para as mesmas pois é possível derivar possíveis *passwords* através de informação pública, diminuindo assim o número de tentativas para um ataque deste tipo.

Conclui-se assim que o processo de comprometimento de um sistema, é um processo bastante complexo, que varia bastante de caso para caso dependendo das boas práticas de cada administrador de sistema, e que está dependente da negligência dos sistemas. Este processo também requer bastantes conhecimentos nas mais diversas áreas da informática,

tendo o *pentester* que conhecer um pouco de tudo, desde construção e administração de websites, manutenção e gestão de servidores, programação nas mais diversas linguagens de programação, boas capacidades de pesquisa e recolha de informação.

Referências

[1] nmap.org, “Zenmap,” [Online]. Available: https://nmap.org/zenmap/. [Acedido em 11 6 2019].

[2] A. Quina e L. Stavliotis, “Sparta,” [Online]. Available: https://github.com/SECFORCE/sparta. [Acedido em 12 6 2019].

[3] Wireshark Foundation, “Wireshark,” [Online]. Available: https://www.wireshark.org/. [Acedido em 13 6 2019].

[4] lanjelot, “Patator,” [Online]. Available: https://github.com/lanjelot/patator. [Acedido em 12 6 2019].

[5] tenable, “Nessus,” [Online]. Available: https://www.tenable.com/products/nessus/nessus-professional. [Acedido em 12 6 2019].

[6] A. Ali, “Pyfuzz,” [Online]. Available: https://github.com/AyoobAli/pyfuzz. [Acedido em 12 6 2019].

[7] WPScan, “WPScan,” [Online]. Available: https://wpscan.org/. [Acedido em 12 6 2019].

[8] NIST, “CVE-2019-7524 Detail,” [Online]. Available: https://nvd.nist.gov/vuln/detail/CVE-2019-7524. [Acedido em 12 6 2019].

[9] SecLists.org, “CVE-2019-10149,” [Online]. Available: https://seclists.org/oss-sec/2019/q2/153. [Acedido em 12 6 2019].

[10] NIST, “CVE-2018-20152,” [Online]. Available: https://nvd.nist.gov/vuln/detail/CVE-2018-20152#vulnCurrentDescriptionTitle. [Acedido em 13 6 2019].

[11] S. Scannell, “WordPress Privilege Escalation through Post Types,” RIPSTech Blog, [Online]. Available: https://blog.ripstech.com/2018/wordpress-post-type-privilege-escalation/. [Acedido em 13 6 2019].

Anexos

Anexo I – Resultado no *zenmap*

Scan para o domínio "foradoras.pt"

Nmap scan report for foradoras.pt (185.90.56.155)
Host is up (0.0016s latency).
rDNS record for 185.90.56.155: flexicamais.com
Not shown: 999 open|filtered ports, 991 filtered ports
PORT STATE SERVICE VERSION
21/tcp open ftp Pure-FTPd
| ssl-cert: Subject: commonName=*.serverhs.org
| Subject Alternative Name: DNS:*.serverhs.org, DNS:serverhs.org
| Issuer: commonName=COMODO RSA Domain Validation Secure Server CA/organizationName=COMODO CA Limited/stateOrProvinceName=Greater Manchester/countryName=GB
| Public Key type: rsa
| Public Key bits: 4096
| Signature Algorithm: sha256WithRSAEncryption
| Not valid before: 2017-01-23T00:00:00
| Not valid after: 2020-01-23T23:59:59
| MD5: 3284 9d58 939f d7b4 f9e8 82ec 686a 30a5
|_SHA-1: 72c8 1eeb d722 8fcb 8686 6c9f b294 9cd9 bd94 b754
80/tcp open http Apache httpd
|_http-favicon: Unknown favicon MD5: D41D8CD98F00B204E9800998ECF8427E
|_http-generator: WordPress 5.1.1
| http-methods:
|_ Supported Methods: GET HEAD POST OPTIONS
|_http-server-header: Apache
110/tcp open pop3 Dovecot pop3d
|_pop3-capabilities: TOP AUTH-RESP-CODE RESP-CODES CAPA UIDL PIPELINING SASL(PLAIN LOGIN) USER STLS
|_ssl-date: TLS randomness does not represent time
143/tcp open imap Dovecot imapd
|_imap-capabilities: LOGIN-REFERRALS IMAP4rev1 LITERAL+ IDLE Pre-login ENABLE AUTH=LOGINA0001 capabilities NAMESPACE ID listed SASL-IR more OK have STARTTLS AUTH=PLAIN post-login
|_ssl-date: TLS randomness does not represent time
443/tcp open ssl/ssl Apache httpd (SSL-only mode)
| http-methods:
|_ Supported Methods: HEAD POST
|_http-title: 400 Bad Request
| ssl-cert: Subject: commonName=foradoras.pt
| Subject Alternative Name: DNS:foradoras.pt, DNS:mail.foradoras.pt, DNS:www.foradoras.pt, DNS:webmail.foradoras.pt, DNS:cpanel.foradoras.pt, DNS:webdisk.foradoras.pt, DNS:autodiscover.foradoras.pt

| Issuer: commonName=foradoras.pt
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha256WithRSAEncryption
| Not valid before: 2019-05-05T15:55:32
| Not valid after: 2020-05-04T15:55:32
| MD5: 7744 cfdb 5a23 a616 7199 f612 139d df06
|_SHA-1: 456c 76e7 3e60 5a24 a910 2de4 fd1d b308 29e4 f844
465/tcp open ssl/smtp Exim smtpd 4.92
| smtp-commands: hosting71.serverhs.org Hello foradoras.pt [194.210.216.228], SIZE 52428800, 8BITMIME, PIPELINING, AUTH PLAIN LOGIN, HELP,
|_ Commands supported: AUTH HELO EHLO MAIL RCPT DATA BDAT NOOP QUIT RSET HELP
| ssl-cert: Subject: commonName=*.serverhs.org
| Subject Alternative Name: DNS:*.serverhs.org, DNS:serverhs.org
| Issuer: commonName=COMODO RSA Domain Validation Secure Server CA/organizationName=COMODO CA Limited/stateOrProvinceName=Greater Manchester/countryName=GB
| Public Key type: rsa
| Public Key bits: 4096
| Signature Algorithm: sha256WithRSAEncryption
| Not valid before: 2017-01-23T00:00:00
| Not valid after: 2020-01-23T23:59:59
| MD5: 3284 9d58 939f d7b4 f9e8 82ec 686a 30a5
|_SHA-1: 72c8 1eeb d722 8fcb 8686 6c9f b294 9cd9 bd94 b754
|_ssl-date: TLS randomness does not represent time
587/tcp open smtp Exim smtpd 4.92
| smtp-commands: hosting71.serverhs.org Hello foradoras.pt [194.210.216.228], SIZE 52428800, 8BITMIME, PIPELINING, STARTTLS, HELP,
|_ Commands supported: AUTH STARTTLS HELO EHLO MAIL RCPT DATA BDAT NOOP QUIT RSET HELP
| ssl-cert: Subject: commonName=*.serverhs.org
| Subject Alternative Name: DNS:*.serverhs.org, DNS:serverhs.org
| Issuer: commonName=COMODO RSA Domain Validation Secure Server CA/organizationName=COMODO CA Limited/stateOrProvinceName=Greater Manchester/countryName=GB
| Public Key type: rsa
| Public Key bits: 4096
| Signature Algorithm: sha256WithRSAEncryption
| Not valid before: 2017-01-23T00:00:00
| Not valid after: 2020-01-23T23:59:59
| MD5: 3284 9d58 939f d7b4 f9e8 82ec 686a 30a5
|_SHA-1: 72c8 1eeb d722 8fcb 8686 6c9f b294 9cd9 bd94 b754
|_ssl-date: TLS randomness does not represent time
993/tcp open ssl/imaps?
|_ssl-date: TLS randomness does not represent time
995/tcp open ssl/pop3s?
|_ssl-date: TLS randomness does not represent time
53/udp open domain?
| fingerprint-strings:

| DNS-SD:
| _services
| _dns-sd
| _udp
| local
| NBTStat:
|_ CKAAAAAAAAAAAAAAAAAAAAAAAAAAAA
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port53-UDP:V=7.70%I=7%D=6/12%Time=5D010289%P=x86_64-pc-linux-gnu%r(NBTS
SF:tat,32,"\x80\xf0\x80\x15\0\x01\0\0\0\0\0\0\x20CKAAAAAAAAAAAAAAAAAAAAAA
AAA
SF:AAAAAAA\0\0!\0\x01")%r(DNS-SD,2E,"\0\0\x80\x05\0\x01\0\0\0\0\0\0\t_serv
SF:ices\x07_dns-sd\x04_udp\x05local\0\0\x0c\0\x01");
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: WAP|general purpose
Running: Actiontec embedded, Linux 3.X, Microsoft Windows XP|7|2012
OS CPE: cpe:/h:actiontec:mi424wr-gen3i cpe:/o:linux:linux_kernel cpe:/o:linux:linux_kernel:3.2 cpe:/o:microsoft:windows_xp::sp3 cpe:/o:microsoft:windows_7 cpe:/o:microsoft:windows_server_2012
OS details: Actiontec MI424WR-GEN3I WAP, Linux 3.2, Microsoft Windows XP SP3, Microsoft Windows XP SP3 or Windows 7 or Windows Server 2012
Network Distance: 2 hops
TCP Sequence Prediction: Difficulty=256 (Good luck!)
IP ID Sequence Generation: Incremental
Service Info: Host: hosting71.serverhs.org

TRACEROUTE (using port 80/tcp)
HOP RTT ADDRESS
1 0.14 ms 192.168.174.2
2 0.17 ms flexicamais.com (185.90.56.155)

Scan para o IP 185.90.56.155

Nmap scan report for flexicamais.com (185.90.56.155)
Host is up (0.0015s latency).
Not shown: 999 open|filtered ports, 991 filtered ports
PORT STATE SERVICE VERSION
21/tcp open ftp Pure-FTPd
| ssl-cert: Subject: commonName=*.serverhs.org
| Subject Alternative Name: DNS:*.serverhs.org, DNS:serverhs.org
| Issuer: commonName=COMODO RSA Domain Validation Secure Server CA/organizationName=COMODO CA Limited/stateOrProvinceName=Greater Manchester/countryName=GB
| Public Key type: rsa
| Public Key bits: 4096
| Signature Algorithm: sha256WithRSAEncryption

| Not valid before: 2017-01-23T00:00:00
| Not valid after: 2020-01-23T23:59:59
| MD5:   3284 9d58 939f d7b4 f9e8 82ec 686a 30a5
|_SHA-1: 72c8 1eeb d722 8fcb 8686 6c9f b294 9cd9 bd94 b754
|_ssl-date: TLS randomness does not represent time
80/tcp open http   Apache httpd
| http-methods:
|_ Supported Methods: POST OPTIONS HEAD GET
|_http-server-header: Apache
|_http-title: Flexica+
110/tcp open pop3   Dovecot pop3d
|_pop3-capabilities: AUTH-RESP-CODE USER UIDL RESP-CODES PIPELINING TOP CAPA STLS SASL(PLAIN LOGIN)
|_ssl-date: TLS randomness does not represent time
143/tcp open imap   Dovecot imapd
|_imap-capabilities: ENABLE SASL-IR have IMAP4rev1 LOGIN-REFERRALS Pre-login post-login NAMESPACE LITERAL+ IDLE more ID OK AUTH=PLAIN AUTH=LOGINA0001 STARTTLS listed capabilities
|_ssl-date: TLS randomness does not represent time
443/tcp open ssl/http   Apache httpd
| http-methods:
|_ Supported Methods: POST OPTIONS HEAD GET
|_http-server-header: Apache
|_http-title: Flexica+
| ssl-cert: Subject: commonName=www.arena-sa.pt
| Subject Alternative Name: DNS:www.arena-sa.pt, DNS:arena-sa.pt
| Issuer: commonName=Sectigo RSA Domain Validation Secure Server CA/organizationName=Sectigo Limited/stateOrProvinceName=Greater Manchester/countryName=GB
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha256WithRSAEncryption
| Not valid before: 2019-04-22T00:00:00
| Not valid after: 2020-04-22T23:59:59
| MD5:   8db9 704b 4dd1 ad8e c5c6 336e 5113 0958
|_SHA-1: a399 4a9e e032 c466 40af 6ffa b09b 9d10 b007 3bff
465/tcp open ssl/smtp   Exim smtpd 4.92
| smtp-commands: hosting71.serverhs.org Hello flexicamais.com [194.210.216.228], SIZE 52428800, 8BITMIME, PIPELINING, AUTH PLAIN LOGIN, HELP,
|_ Commands supported: AUTH HELO EHLO MAIL RCPT DATA BDAT NOOP QUIT RSET HELP
| ssl-cert: Subject: commonName=*.serverhs.org
| Subject Alternative Name: DNS:*.serverhs.org, DNS:serverhs.org
| Issuer: commonName=COMODO RSA Domain Validation Secure Server CA/organizationName=COMODO CA Limited/stateOrProvinceName=Greater Manchester/countryName=GB
| Public Key type: rsa
| Public Key bits: 4096
| Signature Algorithm: sha256WithRSAEncryption
| Not valid before: 2017-01-23T00:00:00

| Not valid after: 2020-01-23T23:59:59
| MD5:   3284 9d58 939f d7b4 f9e8 82ec 686a 30a5
|_SHA-1: 72c8 1eeb d722 8fcb 8686 6c9f b294 9cd9 bd94 b754
|_ssl-date: TLS randomness does not represent time
587/tcp open smtp   Exim smtpd 4.92
| smtp-commands: hosting71.serverhs.org Hello flexicamais.com [194.210.216.228], SIZE 52428800, 8BITMIME, PIPELINING, STARTTLS, HELP,
|_ Commands supported: AUTH STARTTLS HELO EHLO MAIL RCPT DATA BDAT NOOP QUIT RSET HELP
| ssl-cert: Subject: commonName=*.serverhs.org
| Subject Alternative Name: DNS:*.serverhs.org, DNS:serverhs.org
| Issuer: commonName=COMODO RSA Domain Validation Secure Server CA/organizationName=COMODO CA Limited/stateOrProvinceName=Greater Manchester/countryName=GB
| Public Key type: rsa
| Public Key bits: 4096
| Signature Algorithm: sha256WithRSAEncryption
| Not valid before: 2017-01-23T00:00:00
| Not valid after: 2020-01-23T23:59:59
| MD5:   3284 9d58 939f d7b4 f9e8 82ec 686a 30a5
|_SHA-1: 72c8 1eeb d722 8fcb 8686 6c9f b294 9cd9 bd94 b754
|_ssl-date: TLS randomness does not represent time
993/tcp open ssl/imaps?
|_ssl-date: TLS randomness does not represent time
995/tcp open ssl/pop3s?
|_ssl-date: TLS randomness does not represent time
53/udp open domain?
| fingerprint-strings:
| DNS-SD:
| _services
| _dns-sd
| _udp
| local
| NBTStat:
|_   CKAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port53-UDP:V=7.70%I=7%D=6/12%Time=5D00EF3D%P=x86_64-pc-linux-gnu%r(NBTS
SF:tat,32,"\x80\xf0\x80\x15\0\x01\0\0\0\0\0\0\x20CKAAAAAAAAAAAAAAAAAAAAAA
SF:AAAAA\0\0!\0\x01")%r(DNS-SD,2E,"\0\0\x80\x05\0\x01\0\0\0\0\0\0\t_serv
SF:ices\x07_dns-sd\x04_udp\x05local\0\0\x0c\0\x01");
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: WAP|general purpose
Running: Actiontec embedded, Linux 3.X, Microsoft Windows XP|7|2012
OS CPE: cpe:/h:actiontec:mi424wr-gen3i cpe:/o:linux:linux_kernel cpe:/o:linux:linux_kernel:3.2 cpe:/o:microsoft:windows_xp::sp3 cpe:/o:microsoft:windows_7 cpe:/o:microsoft:windows_server_2012

OS details: Actiontec MI424WR-GEN3I WAP, Linux 3.2, Microsoft Windows XP SP3, Microsoft Windows XP SP3 or Windows 7 or Windows Server 2012
Network Distance: 2 hops
TCP Sequence Prediction: Difficulty=257 (Good luck!)
IP ID Sequence Generation: Incremental
Service Info: Host: hosting71.serverhs.org

TRACEROUTE (using port 80/tcp)
HOP RTT ADDRESS
1 0.18 ms 192.168.174.2
2 0.21 ms flexicamais.com (185.90.56.155)

Anexo II – Resultado do *Pyfuzz*

```
./pyfuzz.py -u http://foradoras.pt -l lists/wordpress.fuzz.txt
Target       : foradoras.pt
Path         : /
Method       : GET
Header       : {}
Body         :
Timeout      : 15
Scanning ( 876 ) files...
Code 200 : http://foradoras.pt/license.txt (19935 Byte)
Code 200 : http://foradoras.pt/readme.html (7978 Byte)
Code 200 : http://foradoras.pt/wp-admin/admin-footer.php (2 Byte)
Code 200 : http://foradoras.pt/wp-admin/admin-post.php (0 Byte)
Code 200 : http://foradoras.pt/wp-admin/css/ (19333 Byte)
Code 200 : http://foradoras.pt/wp-admin/css/dashboard.css (24528 Byte)
Code 200 : http://foradoras.pt/wp-admin/css/dashboard-rtl.css (24525 Byte)
Code 200 : http://foradoras.pt/wp-admin/css/farbtastic.css (611 Byte)
Code 200 : http://foradoras.pt/wp-admin/css/farbtastic-rtl.css (612 Byte)
Code 200 : http://foradoras.pt/wp-admin/css/ie.css (11998 Byte)
Code 200 : http://foradoras.pt/wp-admin/css/ie-rtl.css (12005 Byte)
Code 200 : http://foradoras.pt/wp-admin/css/install.css (6982 Byte)
Code 200 : http://foradoras.pt/wp-admin/css/install-rtl.css (6983 Byte)
Code 200 : http://foradoras.pt/wp-admin/css/login.css (4212 Byte)
Code 200 : http://foradoras.pt/wp-admin/css/login-rtl.css (4225 Byte)
Code 200 : http://foradoras.pt/wp-admin/css/media.css (23974 Byte)
Code 200 : http://foradoras.pt/wp-admin/css/media-rtl.css (23986 Byte)
Code 200 : http://foradoras.pt/wp-admin/css/widgets.css (16173 Byte)
Code 200 : http://foradoras.pt/wp-admin/css/widgets-rtl.css (16171 Byte)
Code 200 : http://foradoras.pt/wp-admin/css/wp-admin.css (365 Byte)
Code 200 : http://foradoras.pt/wp-admin/css/wp-admin-rtl.css (421 Byte)
Code 200 : http://foradoras.pt/wp-admin/custom-background.php (0 Byte)
Code 200 : http://foradoras.pt/wp-admin/custom-header.php (0 Byte)
Code 200 : http://foradoras.pt/wp-admin/edit-form-advanced.php (2 Byte)
Code 200 : http://foradoras.pt/wp-admin/edit-form-comment.php (2 Byte)
Code 200 : http://foradoras.pt/wp-admin/edit-link-form.php (2 Byte)
Code 200 : http://foradoras.pt/wp-admin/edit-tag-form.php (2 Byte)
Code 200 : http://foradoras.pt/wp-admin/images/ (12864 Byte)
Code 200 : http://foradoras.pt/wp-admin/includes/ (18744 Byte)
Code 200 : http://foradoras.pt/wp-admin/includes/bookmark.php (0 Byte)
Code 200 : http://foradoras.pt/wp-admin/includes/class-ftp.php (0 Byte)
Code 200 : http://foradoras.pt/wp-admin/includes/class-pclzip.php (0 Byte)
Code 200 : http://foradoras.pt/wp-admin/includes/class-wp-filesystem-base.php (0 Byte)
Code 200 : http://foradoras.pt/wp-admin/includes/class-wp-importer.php (0 Byte)
Code 200 : http://foradoras.pt/wp-admin/includes/comment.php (0 Byte)
Code 200 : http://foradoras.pt/wp-admin/includes/dashboard.php (0 Byte)
Code 200 : http://foradoras.pt/wp-admin/includes/deprecated.php (0 Byte)
Code 200 : http://foradoras.pt/wp-admin/includes/export.php (0 Byte)
Code 200 : http://foradoras.pt/wp-admin/includes/image-edit.php (0 Byte)
```

Code 200 : http://foradoras.pt/wp-admin/includes/image.php (0 Byte)
Code 200 : http://foradoras.pt/wp-admin/includes/import.php (0 Byte)
Code 200 : http://foradoras.pt/wp-admin/includes/media.php (0 Byte)
Code 200 : http://foradoras.pt/wp-admin/includes/meta-boxes.php (0 Byte)
Code 200 : http://foradoras.pt/wp-admin/includes/misc.php (0 Byte)
Code 200 : http://foradoras.pt/wp-admin/includes/ms-deprecated.php (0 Byte)
Code 200 : http://foradoras.pt/wp-admin/includes/ms.php (0 Byte)
Code 200 : http://foradoras.pt/wp-admin/includes/plugin-install.php (0 Byte)
Code 200 : http://foradoras.pt/wp-admin/includes/plugin.php (0 Byte)
Code 200 : http://foradoras.pt/wp-admin/includes/post.php (0 Byte)
Code 200 : http://foradoras.pt/wp-admin/includes/taxonomy.php (0 Byte)
Code 200 : http://foradoras.pt/wp-admin/includes/theme-install.php (0 Byte)
Code 200 : http://foradoras.pt/wp-admin/includes/theme.php (0 Byte)
Code 200 : http://foradoras.pt/wp-admin/includes/update-core.php (0 Byte)
Code 200 : http://foradoras.pt/wp-admin/includes/update.php (0 Byte)
Code 200 : http://foradoras.pt/wp-admin/includes/widgets.php (0 Byte)
Code 200 : http://foradoras.pt/wp-admin/install-helper.php (0 Byte)
Code 200 : http://foradoras.pt/wp-admin/install.php (1084 Byte)
Code 200 : http://foradoras.pt/wp-admin/js/ (16832 Byte)
Code 200 : http://foradoras.pt/wp-admin/js/comment.js (2795 Byte)
Code 200 : http://foradoras.pt/wp-admin/js/common.js (42764 Byte)
Code 200 : http://foradoras.pt/wp-admin/js/custom-background.js (3345 Byte)
Code 200 : http://foradoras.pt/wp-admin/js/dashboard.js (19605 Byte)
Code 200 : http://foradoras.pt/wp-admin/js/edit-comments.js (28554 Byte)
Code 200 : http://foradoras.pt/wp-admin/js/editor.js (45313 Byte)
Code 200 : http://foradoras.pt/wp-admin/js/farbtastic.js (7689 Byte)
Code 200 : http://foradoras.pt/wp-admin/js/gallery.js (5638 Byte)
Code 200 : http://foradoras.pt/wp-admin/js/image-edit.js (29294 Byte)
Code 200 : http://foradoras.pt/wp-admin/js/inline-edit-post.js (16307 Byte)
Code 200 : http://foradoras.pt/wp-admin/js/inline-edit-tax.js (7701 Byte)
Code 200 : http://foradoras.pt/wp-admin/js/link.js (3875 Byte)
Code 200 : http://foradoras.pt/wp-admin/js/media.js (5227 Byte)
Code 200 : http://foradoras.pt/wp-admin/js/media-upload.js (3463 Byte)
Code 200 : http://foradoras.pt/wp-admin/js/nav-menu.js (42475 Byte)
Code 200 : http://foradoras.pt/wp-admin/js/password-strength-meter.js (3173 Byte)
Code 200 : http://foradoras.pt/wp-admin/js/plugin-install.js (7017 Byte)
Code 200 : http://foradoras.pt/wp-admin/js/postbox.js (11765 Byte)
Code 200 : http://foradoras.pt/wp-admin/js/post.js (37355 Byte)
Code 200 : http://foradoras.pt/wp-admin/js/set-post-thumbnail.js (841 Byte)
Code 200 : http://foradoras.pt/wp-admin/js/tags.js (4346 Byte)
Code 200 : http://foradoras.pt/wp-admin/js/user-profile.js (12244 Byte)
Code 200 : http://foradoras.pt/wp-admin/js/widgets.js (22876 Byte)
Code 200 : http://foradoras.pt/wp-admin/js/word-count.js (7690 Byte)
Code 200 : http://foradoras.pt/wp-admin/js/xfn.js (7710 Byte)
Code 200 : http://foradoras.pt/wp-admin/link-parse-opml.php (0 Byte)
Code 200 : http://foradoras.pt/wp-admin/load-scripts.php (0 Byte)
Code 200 : http://foradoras.pt/wp-admin/load-styles.php (0 Byte)
Code 200 : http://foradoras.pt/wp-admin/maint/ (805 Byte)
Code 200 : http://foradoras.pt/wp-admin/maint/repair.php (1066 Byte)
Code 200 : http://foradoras.pt/wp-admin/upgrade.php (1061 Byte)

Code 200 : http://foradoras.pt/wp-content/ (0 Byte)
Code 200 : http://foradoras.pt/wp-content/index.php (0 Byte)
Code 200 : http://foradoras.pt/wp-content/plugins/ (0 Byte)
Code 200 : http://foradoras.pt/wp-content/plugins/index.php (0 Byte)
Code 200 : http://foradoras.pt/wp-content/themes/ (0 Byte)
Code 200 : http://foradoras.pt/wp-content/themes/index.php (0 Byte)
Code 200 : http://foradoras.pt/wp-cron.php (0 Byte)
Code 200 : http://foradoras.pt/wp-includes/ (36986 Byte)
Code 200 : http://foradoras.pt/wp-includes/atomlib.php (0 Byte)
Code 200 : http://foradoras.pt/wp-includes/author-template.php (0 Byte)
Code 200 : http://foradoras.pt/wp-includes/bookmark.php (0 Byte)
Code 200 : http://foradoras.pt/wp-includes/bookmark-template.php (0 Byte)
Code 200 : http://foradoras.pt/wp-includes/cache.php (0 Byte)
Code 200 : http://foradoras.pt/wp-includes/canonical.php (0 Byte)
Code 200 : http://foradoras.pt/wp-includes/capabilities.php (0 Byte)
Code 200 : http://foradoras.pt/wp-includes/category.php (0 Byte)
Code 200 : http://foradoras.pt/wp-includes/category-template.php (0 Byte)
Code 200 : http://foradoras.pt/wp-includes/class-json.php (0 Byte)
Code 200 : http://foradoras.pt/wp-includes/class-oembed.php (0 Byte)
Code 200 : http://foradoras.pt/wp-includes/class-phpass.php (0 Byte)
Code 200 : http://foradoras.pt/wp-includes/class-phpmailer.php (0 Byte)
Code 200 : http://foradoras.pt/wp-includes/class-pop3.php (0 Byte)
Code 200 : http://foradoras.pt/wp-includes/class-smtp.php (0 Byte)
Code 200 : http://foradoras.pt/wp-includes/class.wp-dependencies.php (0 Byte)
Code 200 : http://foradoras.pt/wp-includes/comment.php (0 Byte)
Code 200 : http://foradoras.pt/wp-includes/comment-template.php (0 Byte)
Code 200 : http://foradoras.pt/wp-includes/cron.php (0 Byte)
Code 200 : http://foradoras.pt/wp-includes/default-constants.php (0 Byte)
Code 200 : http://foradoras.pt/wp-includes/deprecated.php (0 Byte)
Code 200 : http://foradoras.pt/wp-includes/feed.php (0 Byte)
Code 200 : http://foradoras.pt/wp-includes/formatting.php (0 Byte)
Code 200 : http://foradoras.pt/wp-includes/functions.wp-scripts.php (0 Byte)
Code 200 : http://foradoras.pt/wp-includes/functions.wp-styles.php (0 Byte)
Code 200 : http://foradoras.pt/wp-includes/general-template.php (0 Byte)
Code 200 : http://foradoras.pt/wp-includes/http.php (0 Byte)
Code 200 : http://foradoras.pt/wp-includes/images/ (5745 Byte)
Code 200 : http://foradoras.pt/wp-includes/images/crystal/ (2450 Byte)
Code 200 : http://foradoras.pt/wp-includes/images/crystal/license.txt (149 Byte)
Code 200 : http://foradoras.pt/wp-includes/images/smilies/ (5397 Byte)
Code 200 : http://foradoras.pt/wp-includes/images/wlw/ (1199 Byte)
Code 200 : http://foradoras.pt/wp-includes/js/ (20893 Byte)
Code 200 : http://foradoras.pt/wp-includes/js/autosave.js (21338 Byte)
Code 200 : http://foradoras.pt/wp-includes/js/colorpicker.js (29083 Byte)
Code 200 : http://foradoras.pt/wp-includes/js/comment-reply.js (10076 Byte)
Code 200 : http://foradoras.pt/wp-includes/js/crop/ (1367 Byte)
Code 200 : http://foradoras.pt/wp-includes/js/crop/cropper.css (2949 Byte)
Code 200 : http://foradoras.pt/wp-includes/js/crop/cropper.js (16485 Byte)
Code 200 : http://foradoras.pt/wp-includes/js/hoverIntent.js (4950 Byte)
Code 200 : http://foradoras.pt/wp-includes/js/imgareaselect/ (1605 Byte)
Code 200 : http://foradoras.pt/wp-includes/js/imgareaselect/imgareaselect.css (790 Byte)

Code 200 : http://foradoras.pt/wp-includes/js/imgareaselect/jquery.imgareaselect.js (38132 Byte)
Code 200 : http://foradoras.pt/wp-includes/js/jcrop/ (1197 Byte)
Code 200 : http://foradoras.pt/wp-includes/js/jquery/ (3997 Byte)
Code 200 : http://foradoras.pt/wp-includes/js/jquery/jquery.form.js (41023 Byte)
Code 200 : http://foradoras.pt/wp-includes/js/jquery/jquery.hotkeys.js (5612 Byte)
Code 200 : http://foradoras.pt/wp-includes/js/jquery/jquery.js (97183 Byte)
Code 200 : http://foradoras.pt/wp-includes/js/jquery/jquery.schedule.js (3457 Byte)
Code 200 : http://foradoras.pt/wp-includes/js/jquery/jquery.table-hotkeys.js (3730 Byte)
Code 200 : http://foradoras.pt/wp-includes/js/jquery/suggest.js (6991 Byte)
Code 200 : http://foradoras.pt/wp-includes/js/json2.js (18422 Byte)
Code 200 : http://foradoras.pt/wp-includes/js/quicktags.js (22582 Byte)
Code 200 : http://foradoras.pt/wp-includes/js/swfobject.js (10231 Byte)
Code 200 : http://foradoras.pt/wp-includes/js/swfupload/ (1374 Byte)
Code 200 : http://foradoras.pt/wp-includes/js/swfupload/handlers.js (1460 Byte)
Code 200 : http://foradoras.pt/wp-includes/js/swfupload/swfupload.js (4439 Byte)
Code 200 : http://foradoras.pt/wp-includes/js/thickbox/ (1381 Byte)
Code 200 : http://foradoras.pt/wp-includes/js/thickbox/thickbox.css (2658 Byte)
Code 200 : http://foradoras.pt/wp-includes/js/thickbox/thickbox.js (13163 Byte)
Code 200 : http://foradoras.pt/wp-includes/js/tinymce/ (2431 Byte)
Code 200 : http://foradoras.pt/wp-includes/js/tinymce/langs/ (851 Byte)
Code 200 : http://foradoras.pt/wp-includes/js/tinymce/langs/wp-langs-en.js (15599 Byte)
Code 200 : http://foradoras.pt/wp-includes/js/tinymce/license.txt (26441 Byte)
Code 200 : http://foradoras.pt/wp-includes/js/tinymce/plugins/ (4566 Byte)
Code 200 : http://foradoras.pt/wp-includes/js/tinymce/plugins/directionality/ (1069 Byte)
Code 200 : http://foradoras.pt/wp-includes/js/tinymce/plugins/fullscreen/ (1061 Byte)
Code 200 : http://foradoras.pt/wp-includes/js/tinymce/plugins/media/ (1051 Byte)
Code 200 : http://foradoras.pt/wp-includes/js/tinymce/plugins/paste/ (1051 Byte)
Code 200 : http://foradoras.pt/wp-includes/js/tinymce/plugins/tabfocus/ (1057 Byte)
Code 200 : http://foradoras.pt/wp-includes/js/tinymce/plugins/wordpress/ (1059 Byte)
Code 200 : http://foradoras.pt/wp-includes/js/tinymce/plugins/wpeditimage/ (1063 Byte)
Code 200 : http://foradoras.pt/wp-includes/js/tinymce/plugins/wpgallery/ (1059 Byte)
Code 200 : http://foradoras.pt/wp-includes/js/tinymce/themes/ (1021 Byte)
Code 200 : http://foradoras.pt/wp-includes/js/tinymce/tiny_mce_popup.js (15988 Byte)
Code 200 : http://foradoras.pt/wp-includes/js/tinymce/utils/ (1393 Byte)
Code 200 : http://foradoras.pt/wp-includes/js/tinymce/utils/editable_selects.js (2125 Byte)
Code 200 : http://foradoras.pt/wp-includes/js/tinymce/utils/form_utils.js (6071 Byte)
Code 200 : http://foradoras.pt/wp-includes/js/tinymce/utils/mctabs.js (4160 Byte)
Code 200 : http://foradoras.pt/wp-includes/js/tinymce/utils/validate.js (6466 Byte)
Code 200 : http://foradoras.pt/wp-includes/js/tinymce/wp-tinymce.php (357327 Byte)
Code 200 : http://foradoras.pt/wp-includes/js/wp-ajax-response.js (3201 Byte)
Code 200 : http://foradoras.pt/wp-includes/js/wp-list-revisions.js (970 Byte)
Code 200 : http://foradoras.pt/wp-includes/js/wp-lists.js (25282 Byte)
Code 200 : http://foradoras.pt/wp-includes/kses.php (0 Byte)
Code 200 : http://foradoras.pt/wp-includes/l10n.php (0 Byte)
Code 200 : http://foradoras.pt/wp-includes/link-template.php (0 Byte)
Code 200 : http://foradoras.pt/wp-includes/load.php (0 Byte)
Code 200 : http://foradoras.pt/wp-includes/meta.php (0 Byte)
Code 200 : http://foradoras.pt/wp-includes/ms-default-constants.php (0 Byte)
Code 200 : http://foradoras.pt/wp-includes/ms-deprecated.php (0 Byte)

Code 200 : http://foradoras.pt/wp-includes/ms-files.php (29 Byte)
Code 200 : http://foradoras.pt/wp-includes/ms-functions.php (0 Byte)
Code 200 : http://foradoras.pt/wp-includes/ms-load.php (0 Byte)
Code 200 : http://foradoras.pt/wp-includes/nav-menu.php (0 Byte)
Code 200 : http://foradoras.pt/wp-includes/pluggable-deprecated.php (0 Byte)
Code 200 : http://foradoras.pt/wp-includes/pluggable.php (0 Byte)
Code 200 : http://foradoras.pt/wp-includes/plugin.php (0 Byte)
Code 200 : http://foradoras.pt/wp-includes/pomo/ (1706 Byte)
Code 200 : http://foradoras.pt/wp-includes/pomo/entry.php (0 Byte)
Code 200 : http://foradoras.pt/wp-includes/pomo/mo.php (0 Byte)
Code 200 : http://foradoras.pt/wp-includes/pomo/po.php (0 Byte)
Code 200 : http://foradoras.pt/wp-includes/pomo/streams.php (0 Byte)
Code 200 : http://foradoras.pt/wp-includes/pomo/translations.php (0 Byte)
Code 200 : http://foradoras.pt/wp-includes/post.php (0 Byte)
Code 200 : http://foradoras.pt/wp-includes/post-template.php (0 Byte)
Code 200 : http://foradoras.pt/wp-includes/post-thumbnail-template.php (0 Byte)
Code 200 : http://foradoras.pt/wp-includes/query.php (0 Byte)
Code 200 : http://foradoras.pt/wp-includes/rewrite.php (0 Byte)
Code 200 : http://foradoras.pt/wp-includes/shortcodes.php (0 Byte)
Code 200 : http://foradoras.pt/wp-includes/taxonomy.php (0 Byte)
Code 200 : http://foradoras.pt/wp-includes/Text/ (983 Byte)
Code 200 : http://foradoras.pt/wp-includes/Text/Diff/ (1181 Byte)
Code 200 : http://foradoras.pt/wp-includes/Text/Diff/Engine/ (1378 Byte)
Code 200 : http://foradoras.pt/wp-includes/Text/Diff/Engine/native.php (0 Byte)
Code 200 : http://foradoras.pt/wp-includes/Text/Diff/Engine/shell.php (0 Byte)
Code 200 : http://foradoras.pt/wp-includes/Text/Diff/Engine/string.php (0 Byte)
Code 200 : http://foradoras.pt/wp-includes/Text/Diff/Engine/xdiff.php (0 Byte)
Code 200 : http://foradoras.pt/wp-includes/Text/Diff.php (0 Byte)
Code 200 : http://foradoras.pt/wp-includes/Text/Diff/Renderer/ (850 Byte)
Code 200 : http://foradoras.pt/wp-includes/Text/Diff/Renderer/inline.php (0 Byte)
Code 200 : http://foradoras.pt/wp-includes/Text/Diff/Renderer.php (0 Byte)
Code 200 : http://foradoras.pt/wp-includes/theme-compat/ (2276 Byte)
Code 200 : http://foradoras.pt/wp-includes/theme.php (0 Byte)
Code 200 : http://foradoras.pt/wp-includes/user.php (0 Byte)
Code 200 : http://foradoras.pt/wp-includes/version.php (0 Byte)
Code 200 : http://foradoras.pt/wp-includes/widgets.php (0 Byte)
Code 200 : http://foradoras.pt/wp-includes/wlwmanifest.xml (1045 Byte)
Code 200 : http://foradoras.pt/wp-includes/wp-db.php (0 Byte)
Code 200 : http://foradoras.pt/wp-json/ (101263 Byte)
Code 200 : http://foradoras.pt/wp-json/wp/v2/posts (1726 Byte)
Code 200 : http://foradoras.pt/wp-json/wp/v2/users (559 Byte)
Code 200 : http://foradoras.pt/wp-links-opml.php (253 Byte)
Code 200 : http://foradoras.pt/wp-load.php (0 Byte)
Code 200 : http://foradoras.pt/wp-login.php (3742 Byte)
Total Pages found: 232