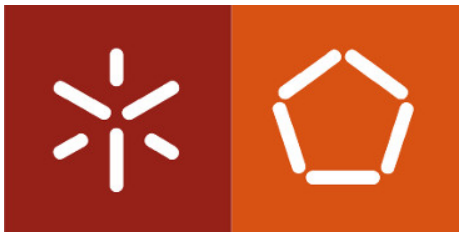
Engenharia de Segurança

23 de Março de 2021

Grupo 7

a83899	André Morais
a84485	Tiago Magalhães

Prática 1 - Aula 03



Mestrado Integrado em Engenharia Informática
Universidade do Minho

Conteúdo

1 Assinaturas cegas baseadas em Curvas Elípticas **2**
1.1 Pergunta 1.1 . . . 2

2 Protocolo SSL/TLS **2**
2.1 Pergunta 2.1 . . . 2
2.1.1 i . . . 2
2.1.2 ii . . . 2
2.1.3 iii . . . 3

3 Protocolo SSH **5**
3.1 Pergunta 3.1 . . . 5
3.1.1 1) . . . 5
3.1.2 2) . . . 7
3.1.3 3) . . . 7
3.1.4 4) . . . 8
3.1.5 5) . . . 8

1 Assinaturas cegas baseadas em Curvas Elípticas

1.1 Pergunta 1.1

O código encontra-se no repositório git.

2 Protocolo SSL/TLS

2.1 Pergunta 2.1

As Câmaras Municipais Portuguesas escolhidas foram a de Esposende e a de Amarante.

2.1.1 i

Os pdf's encontram-se no repositório git

2.1.2 ii

Ambas têm a mesma classificação, mas o da câmara municipal de Amarante apresenta um valor de *key exchange* abaixo comparado com o *website* da câmara municipal de Esposende.

O *rating* da configuração SSL do *website* da câmara municipal de Amarante, deve-se ao facto de permitir suporte aos protocolos **TLS 1.1** e **TLS 1.0**, uma vez que estes já não são mais seguros. Também este, não possui *Forward Secrecy*, isto é, não protege sessões passadas contra possíveis comprometimentos de chaves secretas no futuro. O *key exchange* tem uma classificação baixa devido ao uso de métodos de troca de chaves como *Diffie-Hellman key exchange* (DHE) e *RSA key exchange*, sendo que o primeiro é inseguro, uma vez que já são conhecidos ataques, porém existem mitigações e o segundo não fornece *Forward Secrecy*, sendo recomendável usar para troca de chaves a versão com curvas elípticas do *Diffie-Hellman* (ECDHE), uma vez que fornece *Forward Secrecy* e melhor eficiência [4].

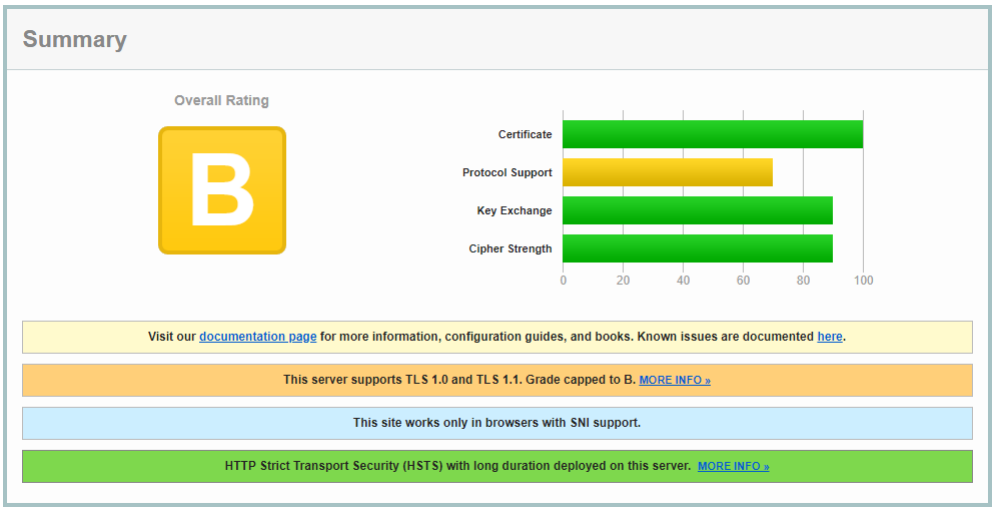


Figura 1: Rating Overall do Website da CM de Esposende

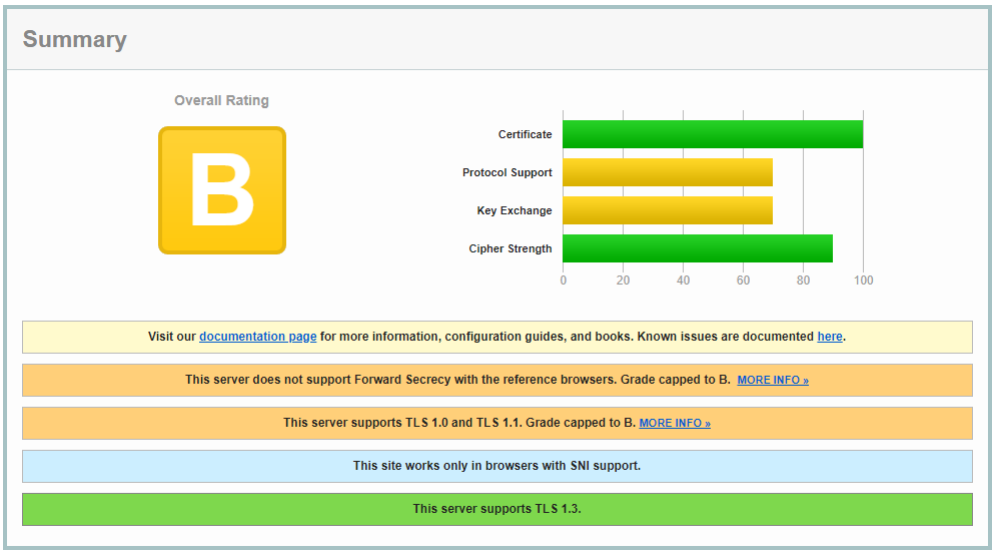


Figura 2: Rating Overall do Website da CM de Amarante

2.1.3 iii

O **POODLE** é um ataque conhecido, direcionado ao protocolo SSL 3. Algumas implementações TLS também são vulneráveis a este ataque.

Se o atacante consegue explorar com sucesso esta vulnerabilidade, ele apenas precisa de fazer, em média, 256 SSL 3.0 requests para revelar 1 byte da mensagem cifrada.

Assim sendo o *SSL Server test* passou a incluir nestes testes, informação acerca se o site avaliado encontra-se exposto por esta vulnerabilidade, visto que este exploit "matou"o SSL 3 e portanto este protocolo não deve ser mais usado.

3 Protocolo SSH

3.1 Pergunta 3.1

3.1.1 1)

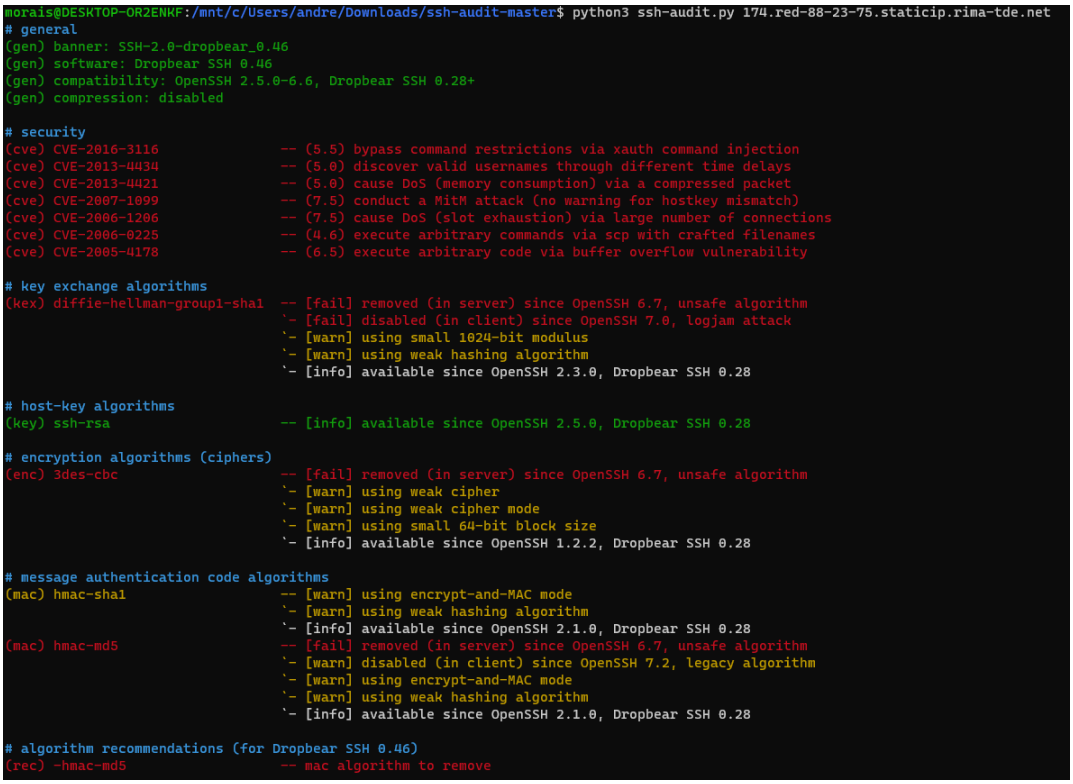


Figura 3: python3 ssh-audit.py 174.red-88-23-75.staticip.rima-tde.net

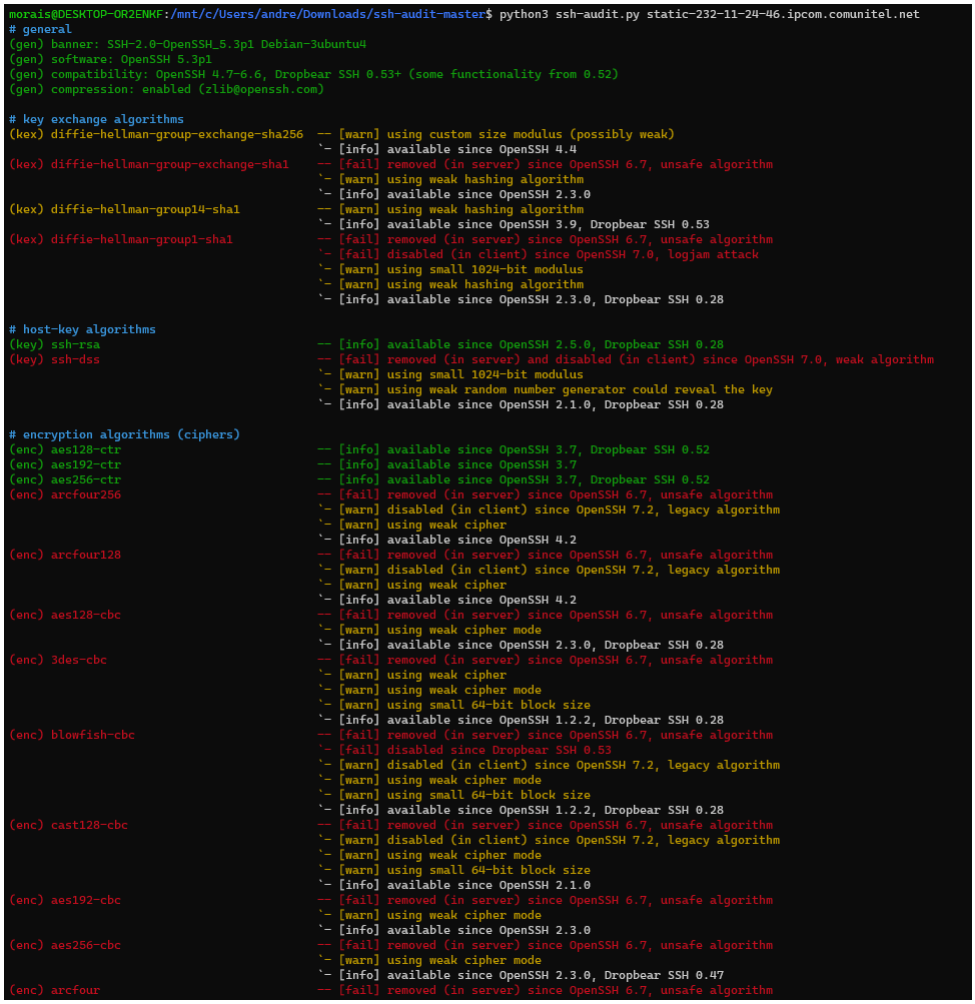


Figura 4: python3 ssh-audit.py static-232-11-24-46.ipcom.comunitel.net

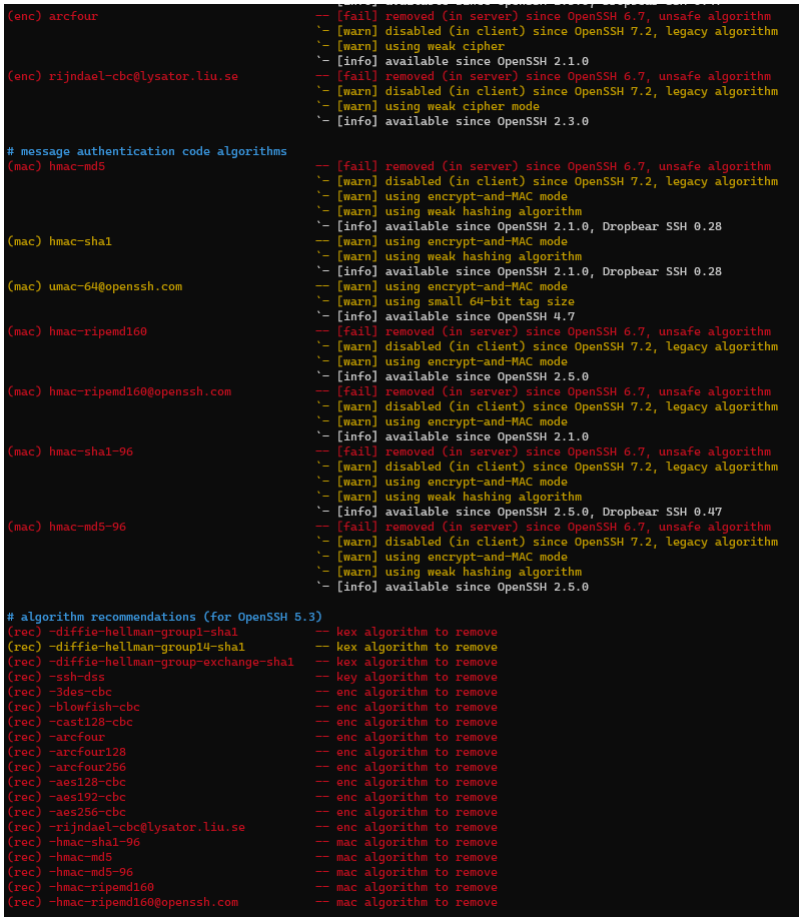


Figura 5: python3 ssh-audit.py static-232-11-24-46.ipcom.comunitel.net

3.1.2 2)

Telefonica de Espana Static IP

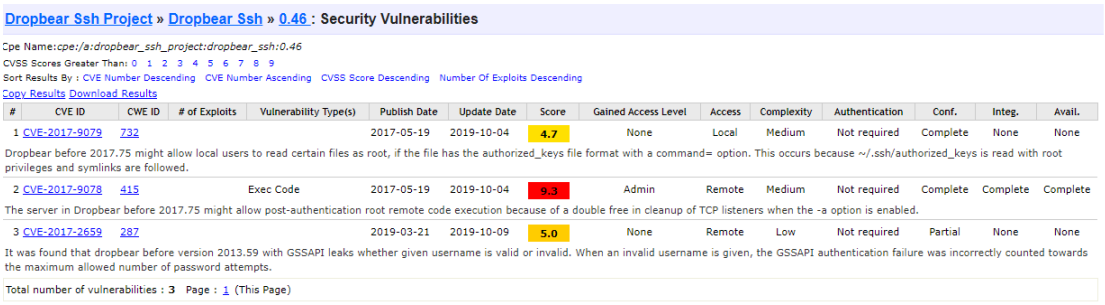
- **Software & Versão do SSH**: Dropbear SSH 0.46

Vodafone

- **Software & Versão do SSH**: OpenSSH 5.3p1

3.1.3 3)

Ambos os softwares apresentam 3 vulnerabilidades, como se pode observar nas imagens que se seguem:



Dropbear Ssh Project » Dropbear Ssh » 0.46 : Security Vulnerabilities

Cpe Name:*cpe:/a:dropbear_ssh_project:dropbear_ssh:0.46*

CVSS Scores Greater Than: 0 1 2 3 4 5 6 7 8 9

Sort Results By : CVE Number Descending CVE Number Ascending CVSS Score Descending Number Of Exploits Descending

Copy Results Download Results

#	CVE ID	CWE ID	# of Exploits	Vulnerability Type(s)	Publish Date	Update Date	Score	Gained Access Level	Access	Complexity	Authentication	Conf.	Integ.	Avail.
1	CVE-2017-9079	732			2017-05-19	2019-10-04	4.7	None	Local	Medium	Not required	Complete	None	None

Dropbear before 2017.75 might allow local users to read certain files as root, if the file has the authorized_keys file format with a command= option. This occurs because ~/.ssh/authorized_keys is read with root privileges and symlinks are followed.

2	CVE-2017-9078	415		Exec Code	2017-05-19	2019-10-04	9.3	Admin	Remote	Medium	Not required	Complete	Complete	Complete

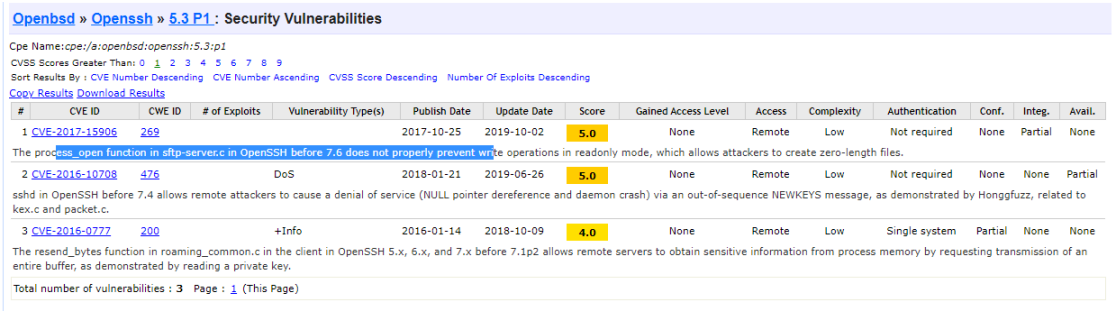
The server in Dropbear before 2017.75 might allow post-authentication root remote code execution because of a double free in cleanup of TCP listeners when the -a option is enabled.

3	CVE-2017-2659	287			2019-03-21	2019-10-09	5.0	None	Remote	Low	Not required	Partial	None	None

It was found that dropbear before version 2013.59 with GSSAPI leaks whether given username is valid or invalid. When an invalid username is given, the GSSAPI authentication failure was incorrectly counted towards the maximum allowed number of password attempts.

Total number of vulnerabilities : **3** Page : 1 (This Page)

Figura 6: Vulnerabilidades do Dropbear SSH 0.46



Openbsd » Openssh » 5.3 P1 : Security Vulnerabilities

Cpe Name:*cpe:/a:openbsd:openssh:5.3:p1*

CVSS Scores Greater Than: 0 1 2 3 4 5 6 7 8 9

Sort Results By : CVE Number Descending CVE Number Ascending CVSS Score Descending Number Of Exploits Descending

Copy Results Download Results

#	CVE ID	CWE ID	# of Exploits	Vulnerability Type(s)	Publish Date	Update Date	Score	Gained Access Level	Access	Complexity	Authentication	Conf.	Integ.	Avail.
1	CVE-2017-15906	269			2017-10-25	2019-10-02	5.0	None	Remote	Low	Not required	None	Partial	None

The process_open function in sftp-server.c in OpenSSH before 7.6 does not properly prevent write operations in readonly mode, which allows attackers to create zero-length files.

2	CVE-2016-10708	476		DoS	2018-01-21	2019-06-26	5.0	None	Remote	Low	Not required	None	None	Partial

sshd in OpenSSH before 7.4 allows remote attackers to cause a denial of service (NULL pointer dereference and daemon crash) via an out-of-sequence NEWKEYS message, as demonstrated by Honggfuzz, related to kex.c and packet.c.

3	CVE-2016-0777	200		+Info	2016-01-14	2018-10-09	4.0	None	Remote	Low	Single system	Partial	None	None

The resend_bytes function in roaming_common.c in the client in OpenSSH 5.x, 6.x, and 7.x before 7.1p2 allows remote servers to obtain sensitive information from process memory by requesting transmission of an entire buffer, as demonstrated by reading a private key.

Total number of vulnerabilities : **3** Page : 1 (This Page)

Figura 7: Vulnerabilidades do OpenSSH 5.3p1

3.1.4 4)

De acordo com as imagens anteriores, podemos verificar que a vulnerabilidade mais grave encontra-se no *Dropbear SSH 0.46* com um *score* de **9.3** de acordo com o CVE Details (CVE-2017-9078).

3.1.5 5)

A gravidade desta vulnerabilidade é crítica de acordo com as métricas CVSS. Esta vulnerabilidade compromete completamente a confidencialidade, integridade e a disponibilidade do serviço, que são propriedades esperadas num protocolo que se espera seguro, como o ssh.

Referências

[1] https://www.ssllabs.com/ssltest/

[2] https://www.shodan.io/

[3] https://www.cvedetails.com/version-search.php

[4] https://github.com/ssllabs/research/wiki/SSL-and-TLS-Deployment-Best-Practices25-use-forward-secrecy