

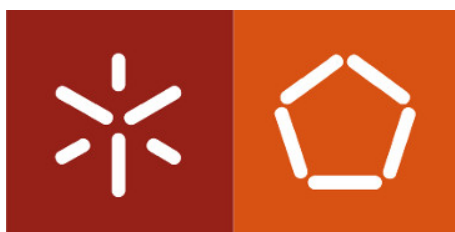
Engenharia de Segurança

23 de Março de 2021

Grupo 7

a83899	André Moraes
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].

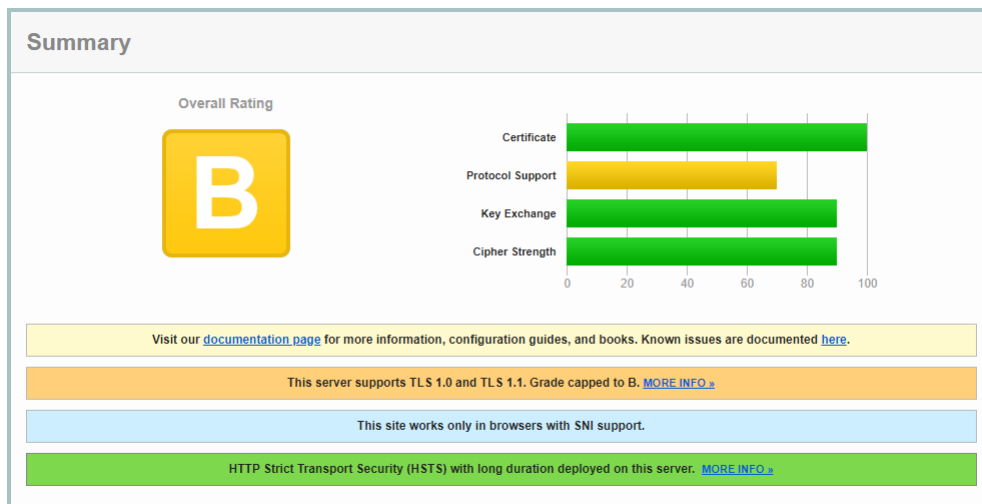


Figura 1: Rating Overall do Website da CM de Esposende

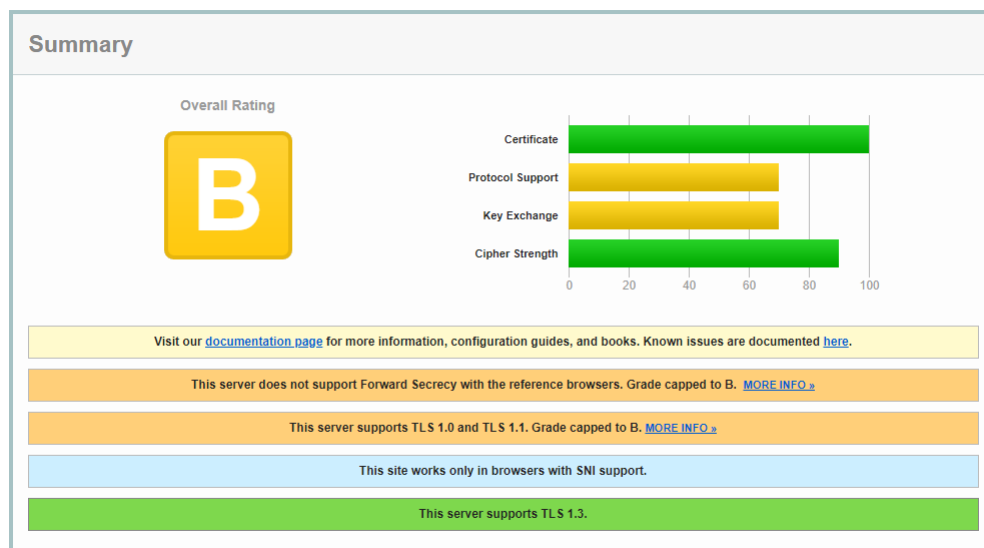


Figura 2: Rating Overall do Website da CM de Amarante

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)

```
morais@DESKTOP-OR2ENHF:/mnt/c/Users/andre/Downloads/ssh-audit-master$ python3 ssh-audit.py 174.red-88-23-75.staticip.rima-tde.net
# general
(gen) banner: SSH-2.0-dropbear_0.46
(gen) software: Dropbear SSH 0.46
(gen) compatibility: OpenSSH 2.5.0-6.6, Dropbear SSH 0.28+
(gen) compression: disabled

# security
(cve) CVE-2016-3116 -- (5.5) bypass command restrictions via xauth command injection
(cve) CVE-2013-4434 -- (5.0) discover valid usernames through different time delays
(cve) CVE-2013-4421 -- (5.0) cause DoS (memory consumption) via a compressed packet
(cve) CVE-2007-1099 -- (7.5) conduct a MitM attack (no warning for hostkey mismatch)
(cve) CVE-2006-1206 -- (7.5) cause DoS (slot exhaustion) via large number of connections
(cve) CVE-2006-0225 -- (4.6) execute arbitrary commands via scp with crafted filenames
(cve) CVE-2005-4178 -- (6.5) execute arbitrary code via buffer overflow vulnerability

# key exchange algorithms
(key) diffie-hellman-group1-sha1 -- [fail] removed (in server) since OpenSSH 6.7, unsafe algorithm
-- [fail] disabled (in client) since OpenSSH 7.0, logjam attack
-- [warn] using small 1024-bit modulus
-- [warn] using weak hashing algorithm
-- [info] available since OpenSSH 2.3.0, Dropbear SSH 0.28

# host-key algorithms
(key) ssh-rsa -- [info] available since OpenSSH 2.5.0, Dropbear SSH 0.28

# encryption algorithms (ciphers)
(enc) 3des-cbc -- [fail] removed (in server) since OpenSSH 6.7, unsafe algorithm
-- [warn] using weak cipher
-- [warn] using weak cipher mode
-- [warn] using small 64-bit block size
-- [info] available since OpenSSH 1.2.2, Dropbear SSH 0.28

# message authentication code algorithms
(mac) hmac-sha1 -- [warn] using encrypt-and-MAC mode
-- [warn] using weak hashing algorithm
-- [info] available since OpenSSH 2.1.0, Dropbear SSH 0.28
(mac) hmac-md5 -- [fail] removed (in server) since OpenSSH 6.7, unsafe algorithm
-- [warn] disabled (in client) since OpenSSH 7.2, legacy algorithm
-- [warn] using encrypt-and-MAC mode
-- [warn] using weak hashing algorithm
-- [info] available since OpenSSH 2.1.0, Dropbear SSH 0.28

# algorithm recommendations (for Dropbear SSH 0.46)
(rec) -hmac-md5 -- mac algorithm to remove
```

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

```

morais@DESKTOP-OR2ENMF:/mnt/c/Users/andre/Downloads/ssh-audit-master$ python3 ssh-audit.py static-232-11-24-46.ipcom.comunitel.net
# general
(gen) banner: SSH-2.0-OpenSSH_5.3p1 Debian-3ubuntu4
(gen) software: OpenSSH 5.3p1
(gen) compatibility: OpenSSH 4.7-6.6, Dropbear SSH 0.53+ (some functionality from 0.52)
(gen) compression: enabled (zlib@openssh.com)

# key exchange algorithms
(kex) diffie-hellman-group-exchange-sha256 -- [warn] using custom size modulus (possibly weak)
      -- [info] available since OpenSSH 4.4
(kex) diffie-hellman-group-exchange-sha1 -- [fail] removed (in server) since OpenSSH 6.7, unsafe algorithm
      -- [warn] using weak hashing algorithm
      -- [info] available since OpenSSH 2.3.0
(kex) diffie-hellman-group14-sha1 -- [warn] using weak hashing algorithm
      -- [info] available since OpenSSH 3.9, Dropbear SSH 0.53
(kex) diffie-hellman-group1-sha1 -- [fail] removed (in server) since OpenSSH 6.7, unsafe algorithm
      -- [fail] disabled (in client) since OpenSSH 7.0, logjam attack
      -- [warn] using small 1024-bit modulus
      -- [warn] using weak hashing algorithm
      -- [info] available since OpenSSH 2.3.0, Dropbear SSH 0.28

# host-key algorithms
(key) ssh-rsa -- [info] available since OpenSSH 2.5.0, Dropbear SSH 0.28
      -- [fail] removed (in server) and disabled (in client) since OpenSSH 7.0, weak algorithm
      -- [warn] using small 1024-bit modulus
      -- [warn] using weak random number generator could reveal the key
      -- [info] available since OpenSSH 2.1.0, Dropbear SSH 0.28
(key) ssh-dss

# encryption algorithms (ciphers)
(enc) aes128-ctr -- [info] available since OpenSSH 3.7, Dropbear SSH 0.52
      -- [info] available since OpenSSH 3.7
(enc) aes192-ctr -- [info] available since OpenSSH 3.7, Dropbear SSH 0.52
(enc) aes256-ctr -- [fail] removed (in server) since OpenSSH 6.7, unsafe algorithm
      -- [warn] disabled (in client) since OpenSSH 7.2, legacy algorithm
      -- [warn] using weak cipher
(enc) arcfour256 -- [info] available since OpenSSH 4.2
      -- [fail] removed (in server) since OpenSSH 6.7, unsafe algorithm
      -- [warn] disabled (in client) since OpenSSH 7.2, legacy algorithm
      -- [warn] using weak cipher
(enc) arcfour128 -- [info] available since OpenSSH 4.2
      -- [fail] removed (in server) since OpenSSH 6.7, unsafe algorithm
      -- [warn] disabled (in client) since OpenSSH 7.2, legacy algorithm
      -- [warn] using weak cipher
(enc) aes128-cbc -- [info] available since OpenSSH 2.3.0, Dropbear SSH 0.28
      -- [fail] removed (in server) since OpenSSH 6.7, unsafe algorithm
      -- [warn] using weak cipher mode
      -- [warn] using small 64-bit block size
(enc) blowfish-cbc -- [info] available since OpenSSH 1.2.2, Dropbear SSH 0.28
      -- [fail] removed (in server) since OpenSSH 6.7, unsafe algorithm
      -- [fail] disabled since Dropbear SSH 0.53
      -- [warn] disabled (in client) since OpenSSH 7.2, legacy algorithm
      -- [warn] using weak cipher mode
      -- [warn] using small 64-bit block size
(enc) cast128-cbc -- [info] available since OpenSSH 1.2.2, Dropbear SSH 0.28
      -- [fail] removed (in server) since OpenSSH 6.7, unsafe algorithm
      -- [warn] disabled (in client) since OpenSSH 7.2, legacy algorithm
      -- [warn] using weak cipher mode
      -- [warn] using small 64-bit block size
(enc) aes192-cbc -- [info] available since OpenSSH 2.1.0
      -- [fail] removed (in server) since OpenSSH 6.7, unsafe algorithm
      -- [warn] using weak cipher mode
      -- [info] available since OpenSSH 2.3.0
(enc) aes256-cbc -- [fail] removed (in server) since OpenSSH 6.7, unsafe algorithm
      -- [warn] using weak cipher mode
      -- [info] available since OpenSSH 2.3.0, Dropbear SSH 0.47
(enc) arcfour -- [fail] removed (in server) since OpenSSH 6.7, unsafe algorithm

```

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

```

(enc) arcfour -- [fail] removed (in server) since OpenSSH 6.7, unsafe algorithm
               ^- [warn] disabled (in client) since OpenSSH 7.2, legacy algorithm
               ^- [warn] using weak cipher
(enc) rijndael-cbc@lysator.liu.se -- [info] available since OpenSSH 2.1.0
               ^- [fail] removed (in server) since OpenSSH 6.7, unsafe algorithm
               ^- [warn] disabled (in client) since OpenSSH 7.2, legacy algorithm
               ^- [warn] using weak cipher mode
               ^- [info] available since OpenSSH 2.3.0

# message authentication code algorithms
(mac) hmac-md5 -- [fail] removed (in server) since OpenSSH 6.7, unsafe algorithm
                ^- [warn] disabled (in client) since OpenSSH 7.2, legacy algorithm
                ^- [warn] using encrypt-and-MAC mode
                ^- [warn] using weak hashing algorithm
                ^- [info] available since OpenSSH 2.1.0, Dropbear SSH 0.28
(mac) hmac-sha1 -- [warn] using encrypt-and-MAC mode
                 ^- [warn] using weak hashing algorithm
                 ^- [info] available since OpenSSH 2.1.0, Dropbear SSH 0.28
(mac) umac-64@openssh.com -- [warn] using encrypt-and-MAC mode
                          ^- [warn] using small 64-bit tag size
                          ^- [info] available since OpenSSH 4.7
(mac) hmac-ripemd160 -- [fail] removed (in server) since OpenSSH 6.7, unsafe algorithm
                      ^- [warn] disabled (in client) since OpenSSH 7.2, legacy algorithm
                      ^- [warn] using encrypt-and-MAC mode
                      ^- [info] available since OpenSSH 2.5.0
(mac) hmac-ripemd160@openssh.com -- [fail] removed (in server) since OpenSSH 6.7, unsafe algorithm
                                  ^- [warn] disabled (in client) since OpenSSH 7.2, legacy algorithm
                                  ^- [warn] using encrypt-and-MAC mode
                                  ^- [info] available since OpenSSH 2.1.0
(mac) hmac-sha1-96 -- [fail] removed (in server) since OpenSSH 6.7, unsafe algorithm
                    ^- [warn] disabled (in client) since OpenSSH 7.2, legacy algorithm
                    ^- [warn] using encrypt-and-MAC mode
                    ^- [warn] using weak hashing algorithm
                    ^- [info] available since OpenSSH 2.5.0, Dropbear SSH 0.47
(mac) hmac-md5-96 -- [fail] removed (in server) since OpenSSH 6.7, unsafe algorithm
                    ^- [warn] disabled (in client) since OpenSSH 7.2, legacy algorithm
                    ^- [warn] using encrypt-and-MAC mode
                    ^- [warn] using weak hashing algorithm
                    ^- [info] available since OpenSSH 2.5.0

# algorithm recommendations (for OpenSSH 5.3)
(rec) -diffie-hellman-group1-sha1 -- kex algorithm to remove
(rec) -diffie-hellman-group14-sha1 -- kex algorithm to remove
(rec) -diffie-hellman-group-exchange-sha1 -- kex algorithm to remove
(rec) -ssh-dss -- key algorithm to remove
(rec) -3des-cbc -- enc algorithm to remove
(rec) -blowfish-cbc -- enc algorithm to remove
(rec) -cast128-cbc -- enc algorithm to remove
(rec) -arcfour -- enc algorithm to remove
(rec) -arcfour128 -- enc algorithm to remove
(rec) -arcfour256 -- enc algorithm to remove
(rec) -aes128-cbc -- enc algorithm to remove
(rec) -aes192-cbc -- enc algorithm to remove
(rec) -aes256-cbc -- enc algorithm to remove
(rec) -rijndael-cbc@lysator.liu.se -- enc algorithm to remove
(rec) -hmac-sha1-96 -- mac algorithm to remove
(rec) -hmac-md5 -- mac algorithm to remove
(rec) -hmac-md5-96 -- mac algorithm to remove
(rec) -hmac-ripemd160 -- mac algorithm to remove
(rec) -hmac-ripemd160@openssh.com -- mac algorithm to remove

```

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](#)
[Cvov 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](#) » **5.3p1 : Security Vulnerabilities**

Cpe Name: `cpe:/a:openbsd:openssh:5.3p1`
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](#)
[Cvov 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>