Escola de Engenharia
Universidade do Minho

DEPARTAMENTO DE ENGENHARIA INFORMÁTICA
Mestrado em Engenharia Informática
Engenharia de Segurança

Aula 3

2 de Março de 2020

Grupo 1

Ricardo Pereira a73577

Tiago Ramires pg41101

Braga, 9 de Março de 2020

1. Assinaturas cegas (Blind signatures) baseadas no Elliptic Curve Discrete Logarithm Problem (ECDLP)

Pergunta P1.1

Disponível na pasta "ex1".

2. Protocolo SSL/TLS

Pergunta P2.1

Escolhidos os dois sites de universidades portuguesas,

- Universidade do Minho - `https://www.uminho.pt/PT`
- Universidade de Aveiro - `https://www.ua.pt/PT`

executou-se um *SSL Server test* a cada um deles, tendo-se obtido uma avaliação dos mesmos e informação acerca dos certificados e das configurações.

I Resultados

Em baixo conseguimos ver a avaliação atribuída a cada site depois do teste.

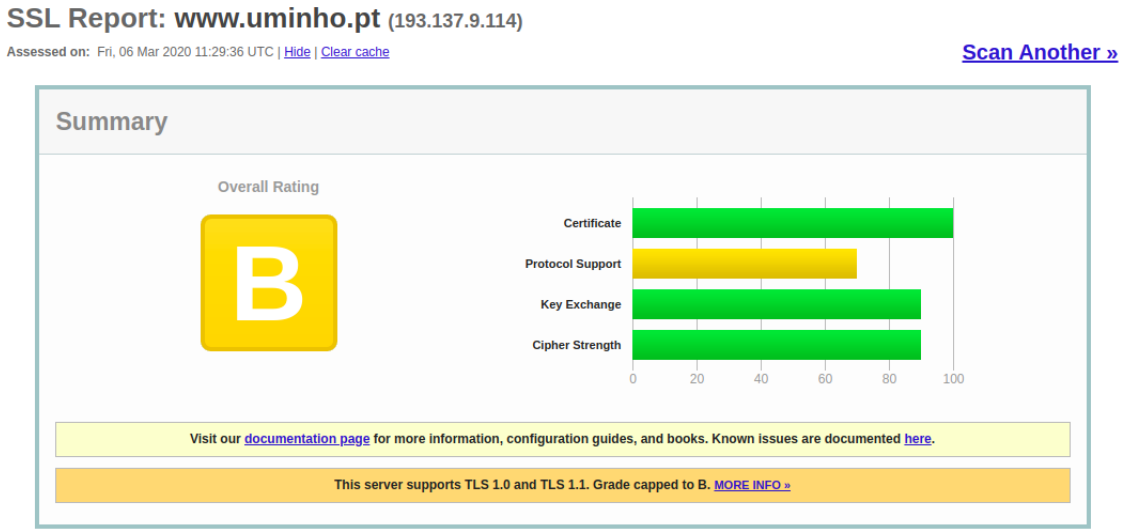

Figura 2.1: SSL Server test ao site da *Universidade do Minho*

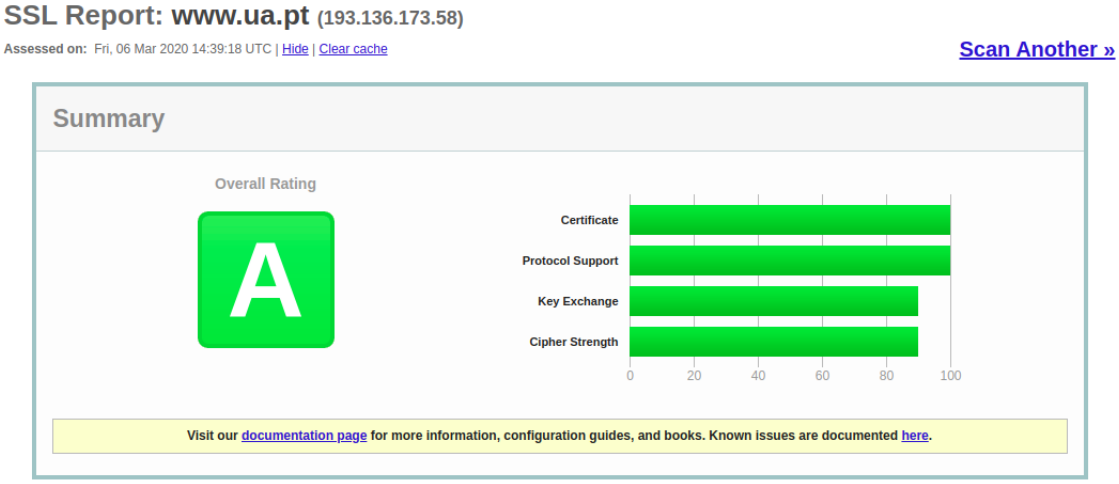

Figura 2.2: SSL Server test ao site do *Universidade de Aveiro*

II Site com pior *rating*

O site para o qual o *rating* atribuido pelo *SSL Server test* é pior, pertence à Universidade do Minho que perde no *Protocol Suport*. Esta classificação tem que ver com o facto dos protocolos *TLS 1.0* e *TLS 1.1* estarem ativos, não cumprindo uma recomendação enunciada em *RFC-7525*.

III Comentário à informação "This site works only in browsers with SNI support."

Neste caso, não nos confrontamos com a frase em questão, contudo o *Server Name Indication* é uma extensão do protocolo TLS que se tem vindo a abordar, que introduz mais alguns passos no *handshake* do cliente. Assim, as partes que implementem *SNI* permitem que haja um

grupo de domínios para os quais é impossível ter um certificado comum.

3. Protocolo SSH

Pergunta P3.1

Como é referido na *nota 1* usamos o *shodan* para descobrir os servidores de duas organizações específicas que usam *ssh* em Portugal. Como já tínhamos escolhido anteriormente, decidimos continuar a analisar as mesmas universidades:

- para a Universidade do Minho fez-se a pesquisa "port:22 country:pt org:"Universidade do Minho e obtivemos, entre outros, o servidor que corre no IP 193.136.19.43 que aloja o site `mooshak41.di.uminho.pt`.
- para a Universidade de Aveiro fez-se a pesquisa "port:22 country:pt org:"Universidade de Aveiro e obtivemos, entre outros, o servidor que corre no IP 193.136.93.21 que aloja o site `cloud.nap.av.it.pt`.

I Resultados do *ssh-audit*

Universidade do Minho

Após a execução do comando python ssh-audit.py mooshak41.di.uminho.pt obteve-se o seguinte *output*:

Listing 3.1: Universidade do Minho

```
# general
(gen) banner: SSH-2.0-OpenSSH_7.2p2 Ubuntu-4ubuntu2.8
(gen) software: OpenSSH 7.2p2
(gen) compatibility: OpenSSH 7.2+, Dropbear SSH 2013.62+
(gen) compression: enabled (zlib@openssh.com)

# key exchange algorithms
(kex) curve25519-sha256@libssh.org                  -- [info] available since Oper
(kex) ecdh-sha2-nistp256                            -- [fail] using weak elliptic
                                                    `- [info] available since Oper
(kex) ecdh-sha2-nistp384                            -- [fail] using weak elliptic
                                                    `- [info] available since Oper
(kex) ecdh-sha2-nistp521                            -- [fail] using weak elliptic
                                                    `- [info] available since Oper
(kex) diffie-hellman-group-exchange-sha256          -- [warn] using custom size m
                                                    `- [info] available since Oper
(kex) diffie-hellman-group14-sha1                   -- [warn] using weak hashing
                                                    `- [info] available since Oper
```

```
# host-key algorithms
(key) ssh-rsa                                -- [info] available since Oper
(key) rsa-sha2-512                           -- [info] available since Oper
(key) rsa-sha2-256                           -- [info] available since Oper
(key) ecdsa-sha2-nistp256                    -- [fail] using weak elliptic
                                             `- [warn] using weak random n
                                             `- [info] available since Oper
(key) ssh-ed25519                            -- [info] available since Oper

# encryption algorithms (ciphers)
(enc) chacha20-poly1305@openssh.com          -- [info] available since Oper
                                             `- [info] default cipher since
(enc) aes128-ctr                             -- [info] available since Oper
(enc) aes192-ctr                             -- [info] available since Oper
(enc) aes256-ctr                             -- [info] available since Oper
(enc) aes128-gcm@openssh.com                 -- [info] available since Oper
(enc) aes256-gcm@openssh.com                 -- [info] available since Oper

# message authentication code algorithms
(mac) umac-64-etm@openssh.com                -- [warn] using small 64-bit
                                             `- [info] available since Oper
(mac) umac-128-etm@openssh.com               -- [info] available since Oper
(mac) hmac-sha2-256-etm@openssh.com          -- [info] available since Oper
(mac) hmac-sha2-512-etm@openssh.com          -- [info] available since Oper
(mac) hmac-sha1-etm@openssh.com              -- [warn] using weak hashing
                                             `- [info] available since Oper
(mac) umac-64@openssh.com                    -- [warn] using encrypt-and-M
                                             `- [warn] using small 64-bit
                                             `- [info] available since Oper
(mac) umac-128@openssh.com                   -- [warn] using encrypt-and-M
                                             `- [info] available since Oper
(mac) hmac-sha2-256                          -- [warn] using encrypt-and-M
                                             `- [info] available since Oper
(mac) hmac-sha2-512                          -- [warn] using encrypt-and-M
                                             `- [info] available since Oper
(mac) hmac-sha1                              -- [warn] using encrypt-and-M
                                             `- [warn] using weak hashing
                                             `- [info] available since Oper

# algorithm recommendations (for OpenSSH 7.2)
(rec) -ecdh-sha2-nistp521                    -- kex algorithm to remove
(rec) -ecdh-sha2-nistp384                    -- kex algorithm to remove
(rec) -ecdh-sha2-nistp256                    -- kex algorithm to remove
(rec) -diffie-hellman-group14-sha1           -- kex algorithm to remove
(rec) -ecdsa-sha2-nistp256                   -- key algorithm to remove
(rec) -hmac-sha2-512                         -- mac algorithm to remove
(rec) -umac-128@openssh.com                  -- mac algorithm to remove
```

```
(rec) -hmac-sha2-256                          -- mac algorithm to remove
(rec) -umac-64@openssh.com                    -- mac algorithm to remove
(rec) -hmac-sha1                              -- mac algorithm to remove
(rec) -hmac-sha1-etm@openssh.com              -- mac algorithm to remove
(rec) -umac-64-etm@openssh.com                -- mac algorithm to remove
```

Universidade de Aveiro

Após a execução do comando python ssh-audit.py cloud.nap.av.it.pt obteve-se o seguinte *output*:

Listing 3.2: Universidade de Aveiro

```
# general
(gen) banner: SSH-2.0-OpenSSH_7.6p1 Ubuntu-4ubuntu0.3
(gen) software: OpenSSH 7.6p1
(gen) compatibility: OpenSSH 7.3+, Dropbear SSH 2016.73+
(gen) compression: enabled (zlib@openssh.com)

# key exchange algorithms
(kex) curve25519-sha256                       -- [warn] unknown algorithm
(kex) curve25519-sha256@libssh.org            -- [info] available since Oper
(kex) ecdh-sha2-nistp256                      -- [fail] using weak elliptic
                                              `- [info] available since Oper
(kex) ecdh-sha2-nistp384                      -- [fail] using weak elliptic
                                              `- [info] available since Oper
(kex) ecdh-sha2-nistp521                      -- [fail] using weak elliptic
                                              `- [info] available since Oper
(kex) diffie-hellman-group-exchange-sha256    -- [warn] using custom size m
                                              `- [info] available since Oper
(kex) diffie-hellman-group16-sha512           -- [info] available since Oper
(kex) diffie-hellman-group18-sha512           -- [info] available since Oper
(kex) diffie-hellman-group14-sha256           -- [info] available since Oper
(kex) diffie-hellman-group14-sha1             -- [warn] using weak hashing
                                              `- [info] available since Oper

# host-key algorithms
(key) ssh-rsa                                 -- [info] available since Oper
(key) rsa-sha2-512                            -- [info] available since Oper
(key) rsa-sha2-256                            -- [info] available since Oper
(key) ecdsa-sha2-nistp256                     -- [fail] using weak elliptic
                                              `- [warn] using weak random n
                                              `- [info] available since Oper
(key) ssh-ed25519                             -- [info] available since Oper

# encryption algorithms (ciphers)
(enc) chacha20-poly1305@openssh.com           -- [info] available since Oper
                                              `- [info] default cipher since
(enc) aes128-ctr                              -- [info] available since Oper
(enc) aes192-ctr                              -- [info] available since Oper
```

```
(enc) aes256-ctr                                -- [info] available since Oper
(enc) aes128-gcm@openssh.com                    -- [info] available since Oper
(enc) aes256-gcm@openssh.com                    -- [info] available since Oper

# message authentication code algorithms
(mac) umac-64-etm@openssh.com                   -- [warn] using small 64-bit
                                                `- [info] available since Oper
(mac) umac-128-etm@openssh.com                  -- [info] available since Oper
(mac) hmac-sha2-256-etm@openssh.com             -- [info] available since Oper
(mac) hmac-sha2-512-etm@openssh.com             -- [info] available since Oper
(mac) hmac-sha1-etm@openssh.com                 -- [warn] using weak hashing
                                                `- [info] available since Oper
(mac) umac-64@openssh.com                       -- [warn] using encrypt-and-M
                                                `- [warn] using small 64-bit
                                                `- [info] available since Oper
(mac) umac-128@openssh.com                      -- [warn] using encrypt-and-M
                                                `- [info] available since Oper
(mac) hmac-sha2-256                             -- [warn] using encrypt-and-M
                                                `- [info] available since Oper
(mac) hmac-sha2-512                             -- [warn] using encrypt-and-M
                                                `- [info] available since Oper
(mac) hmac-sha1                                 -- [warn] using encrypt-and-M
                                                `- [warn] using weak hashing
                                                `- [info] available since Oper

# algorithm recommendations (for OpenSSH 7.6)
(rec) -ecdh-sha2-nistp521                       -- kex algorithm to remove
(rec) -ecdh-sha2-nistp384                       -- kex algorithm to remove
(rec) -diffie-hellman-group14-sha1              -- kex algorithm to remove
(rec) -ecdh-sha2-nistp256                       -- kex algorithm to remove
(rec) -diffie-hellman-group-exchange-sha256     -- kex algorithm to remove
(rec) -ecdsa-sha2-nistp256                      -- key algorithm to remove
(rec) -hmac-sha2-512                            -- mac algorithm to remove
(rec) -umac-128@openssh.com                     -- mac algorithm to remove
(rec) -hmac-sha2-256                            -- mac algorithm to remove
(rec) -umac-64@openssh.com                      -- mac algorithm to remove
(rec) -hmac-sha1                                -- mac algorithm to remove
(rec) -hmac-sha1-etm@openssh.com                -- mac algorithm to remove
(rec) -umac-64-etm@openssh.com                  -- mac algorithm to remove
```

II *Software* e versão utilizada pelos servidores *ssh*

Universidade do Minho

Software e versão: *OpenSSH 7.2p2*

Universidade de Aveiro

Software e versão: *OpenSSH 7.6p1*

III Versões com mais vulnerabilidades

Universidade do Minho

Tal como se pode ver no *CVE Details*, são apresentadas 6 vulnerabilidades para esta versão.

Universidade de Aveiro

Já para o software do outro servidor, o site *CVE Details* apenas apresenta uma vulnerabilidade.

Assim sendo, é o primeiro servidor que tem a versão com mais vulnerabilidades.

IV Versão com a vulnerabilidade mais grave

O primeiro servidor tem a vulnerabilidade mais grave que tem o seguinte identificador: *CVE-2016-6515*. Esta vulnerabilidade tem um *score* de 7.8.

V Gravidade da vulnerabilidade anterior para efeitos práticos

De acordo com a informação disponibilizada, a vulnerabilidade não tem qualquer impacto na confidencialidade ou na integridade, contudo a exploração da mesma pode afetar totalmente a disponibilidade do sistema.

O problema está no facto de um utilizador poder submeter *passwords* do tamanho que quiser, consumindo assim CPU caso a *password* seja extremamente grande.