# Pergunta P2.1

2.

Os sites para o departamento do Tesouro assim como o departamento da Defesa apresentam um *rating*, segundo o *SSL Server Test*, de A. Na realidade este *rating* representa que na realidade ambos os sites são bastante seguros.

Analisando os detalhes do protocolo utilizado, observamos que as vulnerabilidades mais conhecidas de implementação como o *Heartbleed*, *TicketBleed*, *ROBOT,* assim como no *OpenSSL*, *etc.* estão resolvidas e como tal não oferecem qualquer tipo de ameaça a este tipo de protocolo.

Outros fatores importantes que contribuem para que seja garantida a segurança deste servidor é por exemplo garantir a *Forward Secrecy*, apesar de apenas acontecer em *browsers* recentes. No entanto é um pormenor diminuto, pois hoje em dia todos os *browsers* utilizados incluem-se nessa categoria.

Também apresenta segurança face a ataques de *Downgrade attack,* através do uso do TLS\_FALLBACK\_SCSV, não permitindo que um atacante possa passar de um modo de operação de muita qualidade (por exemplo conexão encriptada) para um modo mais fraco (por exemplo texto limpo).

Apresenta também *Secure Renegotiation*, assim como *OCSP Stapling* o que permite verificar o estado de revogação dos certificados que sejam apresentados ao servidor.

3.

Neste caso como este servidor não suporta SSL 3, não existe a possibilidade de de sofrer um ataque *man-in-the-middle* e como tal não existe a possibilidade de serem decifrados bytes das mensagens encriptadas.