Instituto Superior de Engenharia de Coimbra
Departamento de Engenharia Informática e de Sistema

SEGURANÇA

Project 02 (*self-assessment*)		2025/02/28
Expected time: 15 minutes		*in class*
Name: Diogo Antunes	N.: 2018016615	Total.:

Fulfil the header above with your data. Think first. Do not erase or scratch the test. Explain the reason behind your answers.

1. Qual o *MAC Address* e *IP Address* de A1 na sua topologia?

   MAC: 06:23:66:15:AA:01 // IP: 192.168.100.15.

2. A que site recorreu no ponto 4.k)? É seguro deixar o ficheiro de configuração do *router* arquivado sem qualquer proteção adicional?

   www.firewall.cx/cisco/cisco-routers/cisco-type7-password-crack.html

   Não, pois podem conter informações importantes, tais como lista de passwords que podem estar em clear text, ou até mesmo encriptadas. No entanto mesmo encriptadas, estas podem ser facilmente desincriptadas.

3. Qual a linha de comando que empregou no ponto 4.n)?

   R1-6615(config)# enable algorithm-type scrypt secret "password"

4. A seguinte entrada (`/etc/shadow`) suscita-lhe algum reparo a fazer ao gestor do sistema Linux?

   `security:$1$zHvrsmbQ$z5zsde3...:18109:0:130:7:14::`

   Com esse acesso pode-se encontrar o ficheiro que armazena as senhas dos usuários de forma criptografada, neste caso é em md5, no entanto da forma correta, podem ser facilmente descriptadas, o que a torna uma falha de segurança.

5. O que observou de interessante em 4.p)? Como classifica, quanto à segurança, o protocolo *telnet*?

   Ao verificar as capturas no wireshark, pode-se verificar quando é iniciada a comunicação telnet, pode-se ver cada letra que é inserida e enviada em clear text no pacote telnet. Até a password pode-se ver em clear text. Portanto, o protocolo telnet não se pode classificar como seguro.

6. Como resolveu o ponto 4.q)?

   Configurei com o código, "login block-for 90 attempts 3 within 30
   No entanto, quando testei, após 3 erros, não existe o bloqueio durante 90s, pois ainda não tinha sido usado em utilizador.

7. Como resolveu o ponto 4.r)?

   Com a configuração: login on-success log
   login on-failure log