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

SEGURANÇA

Project 01	**Deadline: 2023/03/02**	2023/02/27
Expected time: 60 minutes	Non-contact hours	
Name: _____	N.: _____	Total.: _____

Este projeto deve ser realizado até à data acima mencionada (deadline). Será avaliado em aula por teste específico e não repetível. Deve estar preparado para mostrar a topologia funcional que desenvolveu em aula e para responder a perguntas com base nessa mesma topologia. Expressões a azul sublinhadas são ligações a recursos externos que o ajudam na realização do projeto. Leia o enunciado até ao final antes de mais. Não tem que entregar qualquer recurso a este respeito online.

1. Prepare o ambiente experimental no seu portátil. É muito importante pois vai-lhe dar experiência. Acresce que assim este ambiente estará sempre disponível, mesmo quando você não possuir acesso à Internet. Não solicite ajuda ao docente. Pode e deve trocar opiniões com os colegas. Mas primeiro faça um esforço por ser autónomo. Estará a ganhar competências para vir a ser um melhor profissional. Pesquise em inglês e instale sempre as versões em inglês de todo o software de que necessitar. O volume de informação à disposição dos motores de pesquisa sobre problemas e soluções é muito superior ao que encontrará para português. Consulte o ficheiro "GNS3-LabSetup-041.pdf" disponível neste repositório de software. Este ficheiro recebeu várias atualizações nos últimos dias e também se encontra no Nónio. Além de descrever como resolver alguns problemas comuns na preparação do ambiente agora também possui uma secção que explica, de forma detalhada, como juntar (*merge*) PDUs capturadas em diferentes pontos da mesma topologia ("*Merge multiple Wireshark captures*"). Este aspeto é crítico para a realização deste projeto e de próximos. Atente que no repositório mencionado se encontram disponíveis as últimas versões para Windows 64 bits de várias ferramentas importantes que provavelmente necessitará de instalar. Instale a versão GNS3 partilhada (2.2.37) pois deste modo poderá eventualmente usar topologias partilhadas nas aulas. Será mantida a mesma versão deste software durante todo o semestre. Existe um canal YouTube sobre GNS3 do David Bombal muito interessante de acompanhar a este respeito. Pode usar o servidor GNS3 do ISEC, mas faça-o apenas em última instância para realizar este projeto.
2. Crie uma topologia com duas redes IP (A e B) ligadas por um *router* (R1) Cisco IOU com imagem "i86bi-linux-l3-adventerprisek9-ms.155-2.T.bin". Como nós terminais recorra a *containers ipterm*. (corra o comando `uname -a` para compreender a versão Linux em apreço – ser-lhe-á útil para pesquisar sobre comandos necessários) Considere dois terminais por rede IP. Use *switches* emulados. Tenha em consideração o seguinte:
    a. O *MAC address* do terminal A1 deve receber um valor relacionado com o seu número de aluno do ISEC. O aluno número 2018016929 deve usar como *MAC address* de A1 o valor `06:23:69:29:AA:01`. Trata-se de um MAC universal ou local? Individual ou de grupo? (Justifique). A parte sublinhada do MAC deve refletir a parte menos significativa do seu número de aluno. De seguida vem o "nome" da rede em causa (`AA` - rede A) e o índice do terminal nessa rede (`01` para o terminal A1). Em termos de configuração no ipterm deverá acrescentar a seguinte linha `hwaddress ether 06:23:69:29:AA:01`. Os restantes terminais devem receber endereços seguindo o mesmo princípio. O *router* também deve respeitá-lo mas, nos últimos 8 bits, deve receber o valor F1 (*router* R1). Por exemplo, a interface E0/1 (ligada à rede B) deve receber a configuração `mac-address 0623.6929.BBF1`.

    b. Recorra em todos os exercícios a endereçamento IP privado (RFC 1918). Os dois dígitos menos significativos do *host ID* do IP do terminal de índice mais baixo (1) devem ser iguais aos dois dígitos menos significativos do seu número de aluno (K.X.Y.z29). Esse valor (29) deve ir aumentando unitariamente para cada incremento de índice do terminal (30, 31, …). Nos *routers* deve considerar apenas o segundo dígito menos significativo do *host ID* igual ao dígito menos significativo do seu número de aluno. Como dígito menos significativo do *host ID* do IP do *router* deve usar o índice da sua interface (se for E0/0 será "0", se for E0/1, será "1",

etc.). Por exemplo, K.X.Y.u90 será o IP da interface E0/0 na rede A para o aluno atrás mencionado.

3. Sobre a topologia criada reveja o funcionamento do encaminhamento direto e indireto conforme se descreve na RFC 1180. Realize experiências de comunicação IP entre terminais da mesma rede IP (pode recorrer ao *ping*). Consulte o conteúdo das caches ARP (Linux: `arp` // Cisco IOS: `show arp`). Assegure-se que as *caches* ARP se encontram limpas de entradas dinâmicas antes de iniciar a primeira experiência (Linux: `ip -s -s neigh flush all` // Cisco IOS: `clear arp cache`; `clear ip arp K.X.Y.Z`). De outra forma não conseguirá observar convenientemente todo o processo subjacente. No caso do *router* Cisco apenas consegue limpar *caches* ARP povoadas se os terminais estiverem desligados (capture tráfego enquanto corre um e outro comando atrás mencionado para descobrir as diferenças subjacentes). Capture e analise todo o tráfego presente relevante (explore a utilização de filtros de visualização do Wireshark consultando o documento partilhado no repositório de software). Quando analisar o encaminhamento indireto precisa de capturar tráfego sobre ambas as interfaces do router R1. Recorra à secção "*Merge multiple Wireshark captures*" do documento de preparação do ambiente laboratorial acima mencionado de forma a fundir as duas capturas. Crie e guarde um ficheiro com essa fusão. Vai precisar dele durante o seu estudo e durante a avaliação deste projeto. Analise as sequências de tráfego IP e ARP produzidas em cada situação. Foque-se nos endereços fonte e destino de quadros Ethernet e pacotes IP. Reveja a RFC mencionada e veja se os resultados das suas experiências estão de acordo com o descrito. Pode comparar as capturas obtidas numa experiência subsequente sem limpar as *caches* ARP para compreender as otimizações inerentes ao processo. Neste caso deve consultar as caches antes de iniciar o segundo ping.