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

SEGURANÇA

Project 05	**Deadline: 2023/05/12 (16:00)**	2023/04/25
Expected time: 240 minutes	Non-contact hours	
Name: _____	N.: _____	Total.: _____

Este projeto deve ser realizado até à data e hora acima mencionadas (campo deadline). Será avaliado em aula por teste específico e não repetível. Deve estar preparado para mostrar em aula a topologia funcional que desenvolveu e para responder a perguntas com base na mesma, nas capturas realizadas e na pesquisa realizada. O melhor será anotar em documento as respostas aos vários desafios para consulta posterior. Expressões a azul sublinhadas são ligações a recursos externos. Leia o enunciado até ao final antes de iniciar a resolução. Contabilize o tempo despendido e anote-o nesse documento. Não tem que entregar online qualquer recurso a este respeito.

No alinhamento curricular do ramo de Redes e Administração de Sistemas da LEI o funcionamento dos *switches* (equipamentos que processam o tráfego principalmente na camada 2 / ligação) apenas é aprofundado em Tecnologias de Ligação no 5º semestre. Porém, para completar o CCNA Security é necessário possuir conhecimentos acerca do seu funcionamento. Este conhecimento é necessário para compreender técnicas envolvidas na realização e mitigação de ataques de segurança a este nível. Por norma estes ataques são simples de realizar mas o seu impacto pode ser devastador uma vez que facilmente comprometem a segurança de protocolos e aplicações de camadas superiores.

O Capítulo 14 do curso CCNA Security foca alguns dos ataques. Pretende-se neste projeto que recrie três deles (ataque A: *ARP Poisoning Attack*, ataque B1: *DHCP Starvation/Exhaustion Attack* e B2: *DHCP Spoofing Attack*). Além dos ataques pretende-se que coloque igualmente em prática as estratégias de mitigação indicadas no referido capítulo, avaliando se são ou não eficazes perante os ataques realizados. Recorra ao GNS3, use *switches* Cisco IOU L2 (Iron // i86bi_linux_l2-adventerprise-ms.high_iron_20170202.bin) e *routers* Cisco IOU L3 (155-2T // i86bi-linux-l3-adventerprisek9-ms.155-2.T.bin). Recorra a terminais como o software necessário para desferir os ataques. Para poupar tempo pode usar GNS3 appliances que já disponham das ferramentas necessárias (e.g, ?Kali Linux?) ou instalar VMs (VMware ou VirtualBox) e integrá-las no GNS3.

Se lhe surgir o erro DUPLEX MISMATCH identifique as interfaces que ligam os *routers* aos *switches* IOU e, em todas, aplique e grave a configuração `duplex half`.

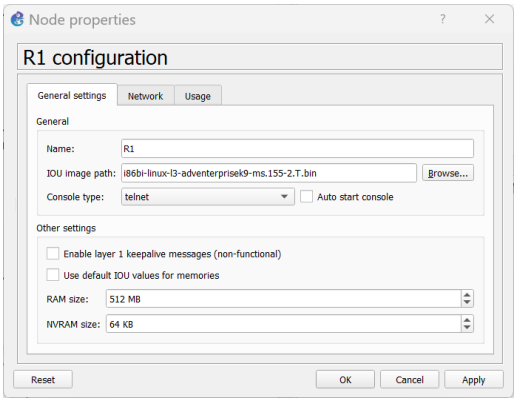
Respeite as regras de endereçamento L2 (MAC) e L3 (IP) apresentadas no primeiro projeto, quer para terminais quer para *routers* (este ponto é crítico: se não o respeitar a sua avaliação será automaticamente nula).

Deve começar por estudar ambos os ataques e técnicas de mitigação disponíveis no IOS. Redija um resumo destes temas. Deve testar se as imagens IOS acima mencionada lhe permitem pôr em práticas as mitigações sugeridas. Após essas validações planeie uma única topologia que lhe possibilite realizar ambos os ataques, elabore um pequeno guião de como se realizam os ataques e de como funcionam (na verdade é isto que importa saber: como funcionam!), faça e guarde capturas de tráfego bem como *screenshots* que lhe permitam comprovar a realização dos mesmos e das respetivas mitigações. Realize capturas simultâneas nas zonas críticas da rede (isto torna-se especialmente relevante para o ataque A). Realize depois o *merge* das mesmas com o TraceWrangler (releia "GNS3-LabSetup-041.pdf" em repositório de software). Analise depois o tráfego aplicando os filtros de visualização necessários no Wireshark. Só assim conseguirá compreender como realmente são realizados os ataques. Isto será crítico na avaliação em aula. Os resumos que fizer também lhe devem permitir rapidamente recriar as experiências durante a avaliação.

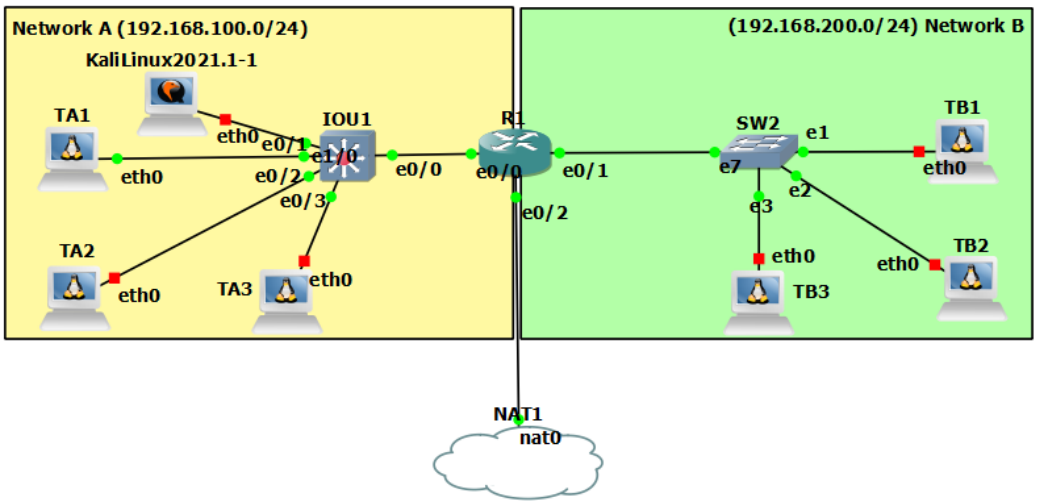
A respeito do ataque A e depois de ler o capítulo da Cisco atrás mencionado estude também o RFC 6959 (*Source Address Validation Improvement (SAVI) Threat Scope*). Depois de mitigar o ataque com as técnicas sugeridas pela Cisco, associe as mesmas a uma ou mais secções deste RFC.

Em qualquer ataque pode usar as ferramentas que entender. Por exemplo, a respeito do ataque B a Cisco menciona a ferramenta The Gobbler mas o DHCPIG é alternativa comum em Linux. A respeito do ataque B empregue as variantes de ataque que sejam mais difíceis de mitigar e valide, perante as mesmas, as estratégias de mitigação sugeridas pela Cisco.

Se recorrer a máquinas virtuais (VirtualBox ou VMware) como nós terminais, a instalação do software necessário pode fazer-se antes destas serem integradas na topologia GNS3. Se usar nós QEMU ou mesmo *containers* Linux a instalação de software pode requerer acesso à Internet. Terá de ligar um *endpoint* NAT ao seu *router* (R1 na figura seguinte). Antes de iniciar R1 aumente-lhe a RAM para 512 MB – opção `Configure` (ver figura ao lado) para suportar o serviço NAT que de seguida vai ativar.



Na interface desse *router* deve programar o endereçamento IP para recorrer ao serviço DHCP (que o GNS3 oferece através do *endpoint NAT*. No *router* em apreço deve ainda ativar o serviço NAT/PAT para partilhar o acesso à Internet pelos restantes terminais da topologia. Nestes últimos deve, por fim, configurar como endereço do servidor de resolução de nomes um servidor DNS público (ex.: 8.8.8.8). De seguida ilustra-se como configurar R1, não só para fornecer acesso IP à Internet à rede A e B, como também para permitir na sua linha de comando usar nomes registados na árvore DNS pública.




```
R1# configure terminal
R1(config)# interface Ethernet 0/2
R1(config-if)# ip address dhcp
R1(config-if)# no shutdown
R1(config-if)# ip nat outside
R1(config)# interface Ethernet 0/0
R1(config-if)# ip nat inside
R1(config)# interface Ethernet 0/1
R1(config-if)# ip nat inside
R1(config-if)# exit
R1(config)# access-list 1 permit 192.168.100.0 0.0.0.255
R1(config)# access-list 1 permit 192.168.200.0 0.0.0.255
R1(config)# ip nat inside source list 1 interface Ethernet 0/2 overload
R1(config)# ip domain-lookup
R1(config)# ip name-server 8.8.8.8
R1(config)# end
R1#ping www.isec.pt
Translating "www.isec.pt"...domain server (8.8.8.8) [OK]

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 193.137.78.72, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
R1#
```

Aproveite e estude o resto do capítulo 14 do CCNA Security.