SEGURANÇA

Project 06	**Deadline: 2023/06/16 (16:00)**	Fase B (2023/06/13)
Expected time: 240 minutes	Non-contact hours	
Name: _____	N.: _____	Total.: _____

Esta fase do projeto deve ser realizada 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.

Tenha em atenção os seguintes requisitos prévios:

- Este enunciado vai crescer com o tempo para cobrir as três fases do seu último projeto. Cada uma das três fases é identificada no cabeçalho por uma letra e respetiva data. A cada fase corresponde um *deadline*.

Fase	Lançamento	Deadline
A	2023/05/31	2023/06/09 (16:00)
B	2023/06/12	2023/06/16 (16:00)

- O enunciado é extenso por incluir explicações e instruções detalhadas que o ajudarão a poupar tempo e compreender melhor os conceitos abordados. A maior parte dos pontos fazem-se num minuto ou menos. Existem alguns pontos que propositadamente desafiam a sua capacidade de estudo autónomo. Obviamente exigem muito mais tempo que os restantes pontos pois requerem alguma pesquisa e algum trabalho de tentativa e erro. Não estará a perder tempo. Estará a investi-lo no treino de uma das competências que mais lhe será útil no futuro: a sua autonomia / capacidade autodidata. O enunciado está redigido para tomar contacto com mais assuntos do que a Cisco aborda no CCNA Security. Isso vai-lhe ser útil no futuro. Tenha uma postura competitiva perante estes desafios. Você afinal ambiciona ser engenheiro e não um mero técnico. Você ambiciona compreender como a tecnologia funciona. Só isso lhe permitirá progredir e vir a criar soluções que ultrapassem as limitações das atuais. Evite solicitar qualquer ajuda (numa primeira fase) aos seus colegas. Só assim estará de facto a treinar competências que lhe serão fundamentais. Os resultados iniciais demorarão muito. Não desanime. É agora a altura certa para o ritmo lento acontecer. Aos poucos você tornar-se-á num engenheiro ágil.
- Leia sempre o enunciado todo uma vez antes de iniciar a sua resolução. Antes de iniciar a resposta a cada ponto releia-o por completo e releia também os dois ou três pontos seguintes. Trabalhe neste projeto apenas quando dispõe de duas ou três horas livres. Será mais eficiente pois não se perde no encadeamento de raciocínio. Para 15 minutos a cada 45 de trabalho.

A sequência de exercícios e passos solicitada tem de ser rigorosamente seguida. Vá guardando um histórico da configuração exata dos equipamentos no início de cada exercício. Deste modo poderá fazer pausas e retomar a realização do projeto sem prejuízo do resultado esperado. Ir salvando a configuração presente dos equipamentos também ajuda para poder repetir algum exercício mais rapidamente e sem alterações do contexto em que desejavelmente deve ser realizado.

Fase A

Comece por instalar no seu servidor GNS3 (2.2.37) as *appliances* QEMU pfSense (versão 2.6.0), Kali Linux (2023.1) e Cisco ASAv 9.12 (4.18) . Em alternativa, se for viável, pode recorrer a máquinas virtuais externas e integrá-las na sua topologia. De seguida ilustra-se como adaptar os *templates* de dispositivos GNS3 existentes às versões mais recentes dos respetivos sistemas operativos. Se já tiver VMs externas destes sistemas integradas no GNS3 pode usá-las, evitando este procedimento. Ao integrar *appliances* diretamente no GNS3, pode vir a reusá-las facilmente noutros projetos

conservando espaço em disco (por exemplo, para cada instância QEMU o GNS3 cria um disco diferencial onde são guardados apenas os ficheiros da imagem original que são modificados naquele projeto específico). Para integrar novas *appliances* no GNS3 é necessário carregar as suas imagens para o servidor GNS3. É possível completar este processo pela interface gráfica GNS3 GUI mas nem sempre esse processo se mostra fluído. Em alternativa, comece por estabelecer uma sessão `ssh` para o seu servidor e escolher, no menu apresentado, a opção de `Shell (Open a shell)`. Para instalar uma imagem do Kali atual, por exemplo:

```
cd /opt/gns3/images/QEMU/
mkdir kali
cd kali
wget https://cdimage.kali.org/kali-2023.1/kali-linux-2023.1-qemu-amd64.7z
sudo apt-get install p7zip-full
7z x kali-linux-2023.1-qemu-amd64.7z
mv kali-linux-2023.1-qemu-amd64.qcow2 ..
cd ..
rm -fr kali
chmod 444  kali-linux-2023.1-qemu-amd64.qcow2
ls -l kali-linux-2023.1-qemu-amd64.qcow2
-r--r--r-- 1 gns3 gns3 13216645120 Mar 10 14:56 kali-linux-2023.1-qemu-amd64.qcow2
```

Para a *appliance* pfSense (2.6.0) o procedimento é semelhante:

```
cd /opt/gns3/images/QEMU/
mkdir pfsense
cd pfsense
wget https://frafiles.netgate.com/mirror/downloads/pfSense-CE-2.6.0-RELEASE-amd64.iso.gz
gzip -d pfSense-CE-2.6.0-RELEASE-amd64.iso.gz
mv pfSense-CE-2.6.0-RELEASE-amd64.iso ..
cd ..
rm -fr pfsense
ls -l pfSense-CE-2.6.0-RELEASE-amd64.iso
-rw-rw-r-- 1 gns3 gns3 767463424 Jan 31  2022 pfSense-CE-2.6.0-RELEASE-amd64.iso
```

O procedimento é semelhante para a imagem ASAv. Quando se recorre a este processo de carregamento de imagens é necessário reiniciar o GNS3 GUI (2.2.37) para que a interface gráfica fique conhecedora das novas imagens disponíveis no servidor.

Depois de reiniciar o GNS3 GUI:

`GNS3 GUI > File > New Template > Install an appliance from the GNS3 server >`

Selecionar o *template* com a versão mais próxima da imagem que se pretende usar:

`Create a new version > Install > Install the appliance on the main server > Next`

Após afinar o nome da imagem e da *appliance* o processo fica concluído e o dispositivo surge pronto a usar num dos grupos (*End Devices*, *Security Devices*, etc.) conforme a interface gráfica informa.

Estude os módulos 8 a 13 do currículo CCNA Network Security. Pode encontrar informação mais detalhada no *site* da Cisco, nomeadamente no Security Configuration Guide: Zone-Based Policy Firewall, Cisco IOS Release 15M&T; no Cisco IOS Intrusion Prevention System Configuration Guide, Cisco IOS Release 15M (alguns destes recursos encontram-se disponíveis no Nónio em PDF). Compreenda ainda o contexto de aplicação das tecnologias 802.1X (módulo 13), IPSec (módulo 18 e 19) e *firewalls* ASA (módulo 20 e 21). Nas próximas fases deste projeto precisará de estudar com profundidade estes módulos. Para já apenas precisa de compreender o enquadramento das tecnologias mencionadas.

Para completar a fase A deste projeto é necessário a) possuir as *appliances* mencionadas instaladas; b) construir uma rede que seja representativa da sua empresa (invente um nome e anote-o no projeto GNS3); c) propor, adotar e justificar um plano de endereçamento coerente (não esqueça que a sua empresa possui vinte filiais); d) estudar com detalhe uma regra Snort.

A sua empresa possui uma sede e 20 filiais. No seu projeto GNS3 deve criar a LAN da sede e da 10ª filial. Pode admitir que as várias redes locais da empresa se encontram ligadas ao mesmo ISP. Deve

representar este ISP na sua topologia com uma rede própria. Na rede do ISP pode haver dois *routers* que representam os dois PoPs (*Points of Presence*) que servem cada uma das LANs da empresa representadas na topologia (e que, portanto, modelam a presença do ISP na cidade da sede e na cidade da 10ª filial). Pode ainda existir um terceiro *router* nesta rede que assegura a ligação do ISP à Internet. Esta ligação deve ser feita através da nuvem NAT do GNS3. Deve programar o encaminhamento de modo que, quer a filial quer a sede, tenham acesso à Internet. Se os seus recursos forem limitados pode reduzir a rede do ISP a um único *router* (i86bi_linux_l2-adventerprise-ms.high_iron_2) ligado à nuvem NAT.

O Kali representará um adversário genérico da sua empresa. Repare que se este nó tiver várias interfaces em múltiplos pontos da rede pode, através apenas dessa instância, desferir ataques internos e externos na sede e na filial. A rede do ISP deve por este motivo alojar também uma interface de rede do Kali. Esta flexibilidade é facilitada pelo ambiente GNS3. Numa rede física seria difícil uma vez que as LAN da empresa se encontram geograficamente separadas.

Tanto para a filial como para a sede deve a) escolher topologias representativas e alinhadas com boas práticas de segurança; b) posicionar os diversos equipamentos/funcionalidades de segurança nos locais adequados e c) justificar as escolhas feitas elaborando uma memória descritiva escrita com as devidas fundamentações. A rede não precisa de ficar toda operacional na primeira fase. Nas fases seguintes do projeto completará essa missão.

O conteúdo atual do CCNA Security foca-se, ainda que moderadamente, no paradigma de Segurança de Perímetro, no qual a rede é dividida em zonas e o tráfego que flui entre elas sujeito a políticas de segurança escrupulosas. Para compreender o funcionamento dos dispositivos de segurança abordados no currículo tal é suficiente. No entanto, com a multiplicação de serviços alojados na *cloud*, a explosão do teletrabalho e a progressiva sofisticação dos adversários novos paradigmas têm surgido sendo Zero Trust o mais popular deles. Na subsecção 2.2 de Limitations of Network Perimeter-based Protections pode encontrar um conjunto de limitações da Segurança de Perímetro.

O Cisco ASAv deverá ser a escolha da *firewall* de entrada da sede. Estas *firewalls* estão vocacionadas para suportar volumes de tráfego consideráveis e esta é a justificação para esta escolha. Já na filial será suficiente usar a funcionalidade de *firewall stateless* e *statefull* (ZPF) do *router* de entrada. A rede da sede provavelmente possuirá (pelo menos) duas *firewalls*. Uma delas deve ser implementada por PfSense (assim estará a tomar contacto com um equipamento diferente). Antes do tráfego chegar à ASAv deve passar por um *stateless firewall*. Porquê? O *router* de entrada pode perfeitamente servir esta missão.

Para desenhar as duas LANs da empresa de forma adequada comece por atender ao ponto *9.2 Firewalls in Network Design* do curso CCNA Security. Consulte também outros recursos. Existem documentos de referência dentro da família ISO/IEC 27K sobre este tema mas a ISO infelizmente entende manter a documentação normativa paga o que não estimula um acesso universal. Por exemplo, no documento ISO/IEC 27033-4 "*Securing communications between networks using security gateways*" são apresentados os conceitos de *packet filter firewalls*, *stateful firewall* e *proxies* aplicacionais (norma ISO 27001). As recomendações destes documentos são genéricas. Os Estados Unidos, através do NIST, oferecem acesso aberto a orientações mais práticas e porventura mais úteis (ex.: Guide to a Secure Enterprise Network Landscape, Guidelines on Firewalls and Firewall Policy). Poderá ainda inspirar-se nestes artigos II, III, e outros que encontre na sua pesquisa. A localização dos vários serviços na topologia é outro dos assuntos sobre o qual deve efetuar algum estudo (consulte, por exemplo, este documento). A Cisco possui documentação muito rica sobre *designs* validados pela indústria. Apesar destes guiões envolverem aspetos técnicos que estão para além do âmbito da unidade curricular e da temática da segurança pode também inspirar-se neles.

A rede da sede deve integrar pelo menos a) uma DMZ (com endereçamento público) e servidores públicos e, na sua intranet, b) dois departamentos internos (use nomes realistas para os mesmos) e c) uma *server farm* destinada a alojar servidores e serviços internos. Na *server farm* deve vir a ser usado IEEE 802.1X.

A ligação (lógica) segura da filial à sede, a programar numa fase posterior do projeto, deverá assentar num túnel IPSec *site-to-site*. Deve prever esta necessidade na sua topologia.

Preveja ainda a utilização do Snort como IDS na sede. Projete a rede para que este IDS possa inspecionar todo o tráfego recebido (e ainda não filtrado) pela sede, bem como o tráfego que flui nas

suas redes internas (DMZ, etc.). Como tal torna-se útil nestes casos recorrer a *switches* Cisco IOU L2 (i86bi_linux_l2-adventerprise-ms.high_iron_20170202.bin). Na realidade à entrada da sede pode evitar este *switch* e, em alternativa, recorrer a um *router* com a imagem i86bi_linux_l2-adventerprise-ms.high_iron_2 (que tb pode atuar como *stateless firewall*). Este equipamento possui *port mirroring* e por isso permitir-lhe ligação direta ao IDS.

Se o Snort fosse usado como IPS poderia recorrer ao seu *Reputation Preprocessor* e rejeitar tráfego oriundo de endereços IP com má reputação. Como não é o caso deve filtrar este tráfego com apoio de outros dispositivos com funcionalidades de *stateless firewalls*. Aproveite no entanto os recursos do sítio do Snort (consider estes endereços) e a lista pública de Bogon IP Addresses. Essa parte pode programar já na primeira fase do projeto.

Neste Fase A do presente projeto pretende-se ainda que examine com detalhe uma regra do Snort. Use a ferramenta Rule Doc Search do Snort e pesquise (por CVE ID) se existe alguma regra no repositório das Community Rules (ou noutro qualquer repositório do Snort) elaborada para o CVE que elegeu quando realizou o projeto 3. Se não existir tente explicar o porquê e procure nas Community Rules do Snort um outro CVE, coberto pelo IDS, que tenha data próxima do seu CVE original. (O mais fácil será descarregar o ficheiro e pesquisar no seu interior com ajuda de um editor de texto). Transcreva para o documento onde regista as notas de resposta a este projeto a regra associada, explique por suas palavras o ataque, explique a regra criada e explique como a mesma pode (ajudar) mitigar a vulnerabilidade em causa. Precisará de estudar a estrutura das regras do Snort (são apresentadas no CCNA Security mais pode também complementar com informação adicional).

Fase B

Se ainda não operacionalizou a *firewall* ASAv atenda às seguintes considerações de apoio. O primeiro cuidado a ter é reservar 4 GB de RAM para esta *appliance*. Sem esta quantidade de RAM pode observar comportamentos inexplicáveis (mudos) como o não processamento de tráfego sem que as mensagens de *logging* mencionem o motivo.

O segundo aspeto a corrigir é um pouco mais trabalhoso mas compensa o investimento. O acesso à CLI da ASAv é mais estável por Telnet que por TightVNC Viewer. Acresce que o Telnet integra com a *clipboard* do Windows (*copy & paste*) e permite reproduzir qualquer carater do teclado português. Para configurar este acesso deve ler estas instruções que são já de seguida resumidas e, mais importante, complementadas:

- Iniciar a ASAv e abrir a consola por omissão (TightVNC Viewer)
- `enable` (definir uma senha de acesso ao modo de configuração privilegiado)
- `configuration terminal` (entrar no modo de configuração)
- `cd coredumpinfo` (ativar a porta série da ASAv)
- `copy coredump.cfg disk0:/use_ttyS0` (é um zero “0” e não a letra “O” na terminação; repare que no Windows deve comutar o *imput method* do teclado para ENG/UK por exemplo para conseguir reproduzir o carcater “/” usando a tecla “-”.)
- `dir disk0:/` (confirmar a presença do ficheiro `coredump.cfg`)

- `reload` (não é necessário gravar qualquer configuração)

Assim que a ASAv arrancar confirme que vê a mensagem `Lina to use serial port /dev/ttyS0 for console IO`. Deve parar a ASAv de novo pelo GNS3 GUI, aceder às propriedades da *appliance* (de novo com o GNS3 GUI) e mudar o tipo de consola de TightVNC para Telnet. Por último arranque a ASAv e volte a abrir a sua consola.

Durante o funcionamento da ASAv surgem periodicamente as seguintes mensagens:

```
Warning: ASAv platform license state is Unlicensed.
Install Asav platform license for full functionality.
```

Ignore-as. Trata-se de um "falso positivo" 😊. Na verdade a Cisco fornece acesso a todas as funcionalidades da firewall mas com o *throughput* limitado a 100 kbps (*You must install a smart license on the ASAv. Until you install a license, throughput is limited to 100 Kbps so you can perform preliminary connectivity tests. A smart license is required for regular operation.*). Para as nossas experiências tal não será obstáculo.

Pretende-se que sobre a topologia que operacionalizou faça várias experiências de ataques externos (sempre a partir da rede do ISP) que permitam mostrar que os vários dispositivos / tecnologias de defesa (*firewalls stateless*, *firewalls stateful*, IDS, etc.) conseguem mitigar (ou pelo menos detetar) certos ataques mas são incapazes de lidar com outros. Abaixo estão algumas sugestões que correspondem a um conjunto mínimo de ataques / acessos indevidos. O objetivo é compreender que dispositivos conseguem lidar com que ataques. Pode e deve idealizar outros cenários que sejam diferentes na sua natureza em termos de abordagem e de defesa para enriquecer as seguintes sugestões:

- Realizar um ataque com o hping3 que permita comprovar o envio de pacotes forjados (por exemplo, com um endereço IP fonte igual ao endereço destino) e a efetiva barreira interposta pela defesa da sua LAN da sede (por exemplo).
- Realizar um ataque/acesso a um *webserver* estabelecendo uma sessão TCP para o seu porto *well-known* (80) mas recorrendo a um protocolo de aplicação distinto do HTTP (pode usar simplesmente a aplicação *Telnet* para este acesso).
- Realizar um ataque de reconhecimento à sede com o nmap.
- Estude o Metasploit, uma *penetration testing framework* popular e que se encontra disponível no Kali. Identifique (seguindo, por exemplo, as dicas deste tutorial) que vulnerabilidades em serviços de rede pode explorar com esta ferramenta. Dos serviços cobertos escolha um serviço que lhe pareça interessante (seja original, não imite os seus colegas nesta escolha!) e instale-o na sua DMZ. Confirme que o IDS se encontra a analisar todo o tráfego (i.e., tráfego ainda não filtrado) que entra na sede. Confirme ainda que permite nas suas políticas de segurança que utilizadores externos acedam ao (novo) serviço instalado. Explore, a partir do exterior (i.e., da rede do ISP), a vulnerabilidade identificada deste serviço recorrendo ao Metasploit instalado no Kali. O IDS consegue detetar o ataque? Identifique a regra do Snort que intercetou o ataque. Programe essa regra de modo que o Snort registe (*log*) o tráfego associado ao ataque. Repita o ataque para confirmar a funcionalidade em apreço. Se esse ataque não for reconhecido pelo Snort deverá identificar outro que o seja e repetir as experiências já descritas.

Antes de abraçar um vendedor de soluções de *networking* convém ver o tempo de suporte e de resposta perante vulnerabilidades. Consulte aqui o histórico de vulnerabilidades da ASA e veja também nas Security Vulnerabilities desse equipamento o tempo que mediou entre a *Publish Date* e a *Update Date* nas várias vulnerabilidades. Foque-se em especial nas que possuem o *score* mais elevado. Esta análise permite-nos estimar a confiança que podemos depositar em cada fabricante. Que tempo médio demora a Cisco a atuar para vulnerabilidades com um *score* de 7 ou mais?