SEGURANÇA

Project 03	**Deadline: 2023/04/21 (16:00)**	15 abril 2023
Expected time: 180 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.

Tenha em atenção os seguintes requisitos prévios:

- Clone a topologia usada no Projeto 02.
- Reveja o módulo 4 e estude o módulo 5 do currículo CCNA Network Security. Pode encontrar informação mais detalhada no *site* da Cisco, nomeadamente no User Security Configuration Guide, Cisco IOS Release 15MT.
- Considere ainda as apresentações "Ameaças à segurança de redes de comunicação" e "Segurança de Dispositivos de Rede" partilhadas na plataforma Nónio.

1. Procure um CVE publicado na data do seu aniversário. Não é relevante o ano mas o CVE deve possuir um *score* CVSS 3.1 atribuído pelo NIST. Faça uma rápida investigação sobre esta vulnerabilidade. Anote o vetor de ataque (CVSS Vector String). Confirme o *Overall Score* reportado usando a calculadora do NIST e as *Base Score Metrics* (é suficiente construir um URL adequado (ex: https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator?name=CVE-2018-8011&vector=AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H&version=3.1). Analise os scores parciais (*Base*, *Impact*, *Exploitability*). Qual o EPSS associado? Investigue ainda e anote as possíveis CWE (*Common Weakness Enumerations*) associadas. Deve guardar a informação solicitada num documento para mostrar durante a avaliação. As várias páginas web que usou para obter a informação solicitada devem ainda estar abertas num *browser* no início da referida avaliação.
2. Crie três utilizadores locais em R1: `adminaXYZ`, `adminbXYZ` e `admincXYZ` (sendo `XYZ` os últimos três dígitos do seu número de aluno). Associe a cada um uma senha distinta. Que comando deve usar para obter a lista dos utilizadores criados?
3. Ative o serviço SSH no *router* R1 e configure o acesso remoto (*in-band*) a R1 exclusivamente por esse serviço. Nesta fase é importante certificar-se de que nunca fez acesso SSH a R1 a partir do terminal A1. Para tal investigue se possui na *home directory* de A1 uma pasta denominada "`.ssh`" (`ls -la`) e se a mesma possui algum ficheiro. Em caso afirmativo apague a pasta e o seu conteúdo antes de avançar com o resto da experiência. Inicie uma captura de tráfego à saída de A1 antes de arrancar os terminais e *routers* da topologia. Entre por SSH, a partir de A1, em R1 usando a conta `adminaXYZ`. Deve usar explicitamente o comando `ssh adminaXYZ@IP(R1.e0/0)`. Atente que `IP(R1.e0/0)` representa o endereço IP de R1 da interface `Ethernet 0/0`. Espere que lhe seja feita a pergunta "*Are you sure you want to continue connecting (yes/no)?*". Não responda. Analise o resumo do tráfego capturado e guarde um ficheiro com este tráfego (vai precisar disto na avaliação). Anote igualmente o número do último quadro capturado até este momento. Avance na experiência (próxima pergunta) para evitar *timeout* mas no final elabore um breve parágrafo explicando com o detalhe possível o motivo da presença de cada PDU (ou grupos de PDUs) capturada até aqui. Aspetos como a resolução de endereços (ARP) ou o *three-way handshake* devem ser claramente identificados.
4. Responda "*yes*" no terminal A1 à pergunta que lhe foi feita mas não se autentique ainda. Nota: um acesso SSH seguro implica a instalação da chave pública de R1 em A1 por um processo/canal que se saiba realmente seguro (uma forma manual, pouco prática, mas com alguma segurança num ambiente real pode passar simplesmente pela realização de uma cópia, através de uma *pen* (canal seguro), da chave pública instalada no servidor SSH para o terminal cliente). Em rigor, antes de responder "*yes*" temos de ter a certeza de que não estamos a ser vítimas de um ataque MITM nesse

preciso momento. Consulte a este respeito o ponto 3 da página 21 do RFC 4253 e transcreva para a sua resposta a frase que alude a "esta *simplificação*" processual. Analise o tráfego adicional entretanto produzido e elabore um pequeno parágrafo sobre o mesmo. Guarde novo ficheiro com esta parte da captura.

5. Investigue se, entretanto, em A1 já existe algum ficheiro com o registo da chave pública que foi enviada pelo servidor. Para o fazer no mesmo terminal recorde as aulas de Sistemas Operativos. Suspenda o processo cliente atual fazendo `Ctrl + Z` na sessão SSH e corra na linha de comando de A1 o comando `ls -l .ssh/known_hosts`. Se o ficheiro em apreço existir, analise o seu conteúdo: `cat .ssh/known_hosts`.
6. Retome o processo cliente SSH correndo ao comando `fg` (ou seja, passe para *foregroud* o último processo suspenso). Autentique-se na sessão SSH fornecendo nome de utilizador (*login*) e senha (*password*) do primeiro utilizador criado. Registe o número da última PDU capturada no Wireshark. Encerre a sessão SSH com o comando `exit`. Analise o resumo do tráfego entretanto gerado durante o processo de autenticação e elabore um pequeno parágrafo sobre o que se passa em cada PDU ou grupos de PDUs capturadas e a relação que têm com os vários eventos da sessão entretanto decorridos. Não invista tempo a perceber realmente o tráfego ligado à comunicação pois é cifrado e, por conseguinte, pouco dado a análises detalhadas. Termine a captura de tráfego e grave-a num novo ficheiro (esta captura deve possuir todo o tráfego produzido desde o início da experiência; as outras capturas devem possuir apenas as PDUs geradas no decurso das experiências em causa).
7. Use a funcionalidade "Follow TCP Stream" do Wireshark (rever enunciado do projeto anterior). Uma forma rápida de aceder a esta funcionalidade passa por colocar o ponteiro do rato sobre um pacote da sessão SSH e premir `Ctrl + Alt + Shift + T`. Na janela aberta use o campo ao fundo com a etiqueta `Find` para pesquisar a senha associada ao primeiro utilizador criado. Encontrou? Qual a diferença para a sessão Telnet testada em projeto anterior?
8. Investigue (ex.: aqui) melhor o formato do ficheiro `known_hosts`. Consulte a data e hora atuais em A1 (`date`). Corra o comando `ssh-keygen -F IP(R1.e0/0`. Explique o output recebido à luz da página de manual do comando `ssh-keygen`. No ficheiro `.ssh/known_hosts` o endereço IP é legível? Em que formato estará guardado? Encontra algum motivo para não surgir em *clear text*? Aceda a R1 por SSH mas desta feita através do endereço IP (R1.e0/1). É suficiente avançar até surgir a pergunta se pretende avançar e dizer que sim. Depois pode terminar a sessão com `Ctrl + C`. Houve atualizações ao ficheiro `.ssh/known_hosts`? Quais? Como relaciona a novidade com a entrada já consultada atrás? Execute o comando `ssh-keygen -F IP(R1.e0/1)` e comente.
9. Entre de novo por SSH, a partir de A1, em R1 usando a segunda conta criada: `adminbXYZ`. Foi-lhe feita a pergunta "*Are you sure you want to continue connecting (yes/no)?*"? Justifique.
10. Em R1 crie uma *view* cujo nome seja `FirstLast-VIEWA` (sendo *First* o seu primeiro nome e *Last* o seu último nome). Esta vista deve permitir alterar o endereço IP da interface `Ethernet 0/1`, alterar a sua descrição e desligar / ligar a interface. Associe a vista criada apenas ao primeiro dos utilizadores criados. Ative a utilização de vistas no *router*. Instrua R1 para realizar a autenticação e autorização a partir da base de dados local de utilizadores. Consulte em R1 a composição da vista que criou (`show running | begin parser`).
11. Entre em R1 a partir de A1 por SSH com o primeiro utilizador criado. Depois de entrar consulte a vista ativa. Consulte ainda o nível de privilégios ativo.
12. Repita as experiências da pergunta anterior mas entrando em R1 por SSH a partir de A2 e usando a segunda conta criada (`adminbXYZ`). Que conclusões pode retirar?
13. Crie uma nova vista `FirstLast-VIEWB`. Esta vista deve permitir alterar o endereço IP da interface `Ethernet 0/0`, alterar a sua descrição e desligar / ligar a interface. Associe a vista criada apenas ao segundo dos utilizadores criado. Teste a sua operacionalidade a partir de B1 demonstrando a sua correção, estabelecendo uma sessão SSH para R1.
14. Através de níveis de privilégios confira ao terceiro dos utilizadores criado a possibilidade de configurar interfaces. Mostre a configuração realizada. Teste a operacionalidade da configuração feita a partir de B2 demonstrando a correção ao estabelecer uma sessão SSH para R1.

15. Crie uma supervista `FirstLast-VIEWC` que seja a união das duas vistas anteriores. Associe a vista criada apenas ao terceiro dos utilizadores criado. Teste a sua operacionalidade a partir de B2 demonstrando a sua correção ao estabelecer uma sessão SSH para R1.

16. Instale o contentor Docker *Networker's Toolkit* no seu servidor GNS3. Pode encontrar uma breve descrição algo antiga do mesmo aqui. Este *container* oferece vários serviços de rede (www (nginx); ftp (vsftpd); tftp (tftpd); syslog (rsyslog); dhcp (isc-dhcpd); snmp server (snmpd + snmptrapd). Alguns dos serviços encontram-se ativos por omissão. Adicione à rede suportada pelo *switch* SWA uma instância do mesmo a atribua-lhe o *host id* com o byte menos significativo igual ao decimal 100 e o MAC Address a seguir as regras definidas em enunciado anterior e a terminar no hexadecimal "0x00". A etiqueta GNS3 do mesmo na topologia deve ser Toolbox-T1 (será adiante denominado apenas por T1). Explore o comando `netstat` para descobrir os serviços UDP e TCP ativos por omissão. Comece por consultar o endereço IP local atual (`ifconfig eth0`) de T1. Mostre num só comando esses serviços através de duas listagens. Numa deve aparecer o nome dos serviços e noutra os números dos portos. Consulte o ficheiro `/etc/services` e o serviço do IANA e infira que fonte de informação o comando `netstat` estará a usar para identificar o nome dos serviços.

17. Consulte resumidamente a especificação do protocolo Syslog no RFC 5424 (leia calmamente até à página 12 e dê especial atenção às páginas 10 e 11). Estude ainda como funciona o sistema de logs do Linux e qual a sua interação com o serviço Syslog. Recordando o que aprendeu em Sistemas Operativos, consulte em T1 os *logs* recebidos e aguarde pelos vindouros (`tail -f /var/log/syslog`). Ative uma captura de tráfego à entrada de T1 na topologia GNS3 com o Wireshark. Ative o *logging* em R1 e a entrega das mesmas no servidor Syslog de T1. Analise com detalhe a PDU capturada em resultado desta ativação (expanda a camada *syslog message*). Explique o conteúdo capturado à luz da RFC que leu.

18. Ative o *logging* de todos os eventos como autenticações de entrada bem e mal sucedidas. Aceda por SSH a partir do terminal A2 a R1 e forneça propositadamente a senha incorreta na primeira tentativa e a correta na segunda tentativa. Qual o resultado do processo.

19. Inative (em R1) a entrega de mensagens de *log*. O que sucedeu em termos de tráfego Syslog?

    Reative (em R1) a entrega de *logs* ao serviço Syslog de T1. No entanto agora pretende-se que armazene no *router* todos os *logs* produzidos mas que restrinja os que são entregues ao serviço de Syslog apenas àqueles cuja severidade é `informational` ou superior. Crie e descreve um conjunto de ações que despoletem logs de nível 7 e 6 de modo a validar a configuração que fez. Para tal deve a) causar a produção de um *log* de severidade `debugging`, mostrar que fica registado localmente em RAM mas não é entregue a T1; b) causar a produção de um *log* de severidade `informational` que, além de ficar localmente registado é entregue ao serviço de Syslog.

20. Estude (de forma autónoma) e exercite o processo de *backup* automatizado da configuração de R1. Pode começar por recorrer a esta fonte. Ative o processo para realizar uma backup de 5 em 5 minutos em T1. O nome dos ficheiros deve incluir o nome do router e a hora de backup. Anote a configuração feita, descreva o processo e consulte a listagem (`ls -l`) da pasta do serviço TFTP que comprove a periodicidade programada. Altere a configuração de R1 entre dois backups para ser visível a diferença na listagem mas recorra também ao comando `diff` em T1. No final da experiência desative este *backup* periódico.

21. Será útil para algum efeito fazer o *log* dos comandos que se vão digitando no IOS? Estude com detalhe esta fonte de informação. Realize a configuração abaixo apresentada em R1 e analise (com apoio do comando `tail` como acima se sugeriu) a produção de *logs* à medida que acede a R1 por SSH a partir de A3, entra no seu modo de configuração, muda a descrição da interface `e0/0` e conclui a configuração. Descreva num breve relatório o objetivo de cada um dos seguintes comandos.

```
archive
 log config
  logging enable
  logging size 100
  notify syslog
```

```
    hidekeys
```

22. Realize um *backup* manual da *running-config* de R1 para o servidor TFTP de T1 (`copy running-config tftp`). Torne também esta configuração não volátil em R1. Execute o comando `auto secure` no modo EXEC em R1. Atente a todo o processo interativo e responda convenientemente. Realize novo *backup* manual da *running-config* de R1 para o servidor TFTP. Use o comando `diff`, comente as diferenças e tente relacioná-las com as perguntas a que foi respondendo.
23. Para concluir esta unidade adicione um terminal BRW-1 (linux-tinycore-linux-6.4) com interface gráfico a SWA, configure-o na mesma rede IP, adicione um novo utilizador em R1 denominado webadmin com privilégios 15, ative o serviço HTTP em R1 e a respeita autenticação de acessos com base na base de dados local. Aceda através do Firefox de BRW-1 à interface Web do router e explore-a. Faça um relatório muito resumido das suas potencialidades. Capture o tráfego do processo de autenticação e investigue se a senha circula em *clear text* ou se é protegida.

Nota: Se houver texto dúbio releia o enunciado. Se as dúvidas persistirem assuma uma interpretação razoável do mesmo e esclareça na resposta à pergunta em causa a interpretação assumida e a razoabilidade da mesma. Não contacte o docente para clarificações quanto ao enunciado.

Nota: Discuta o enunciado com os colegas e até eventuais respostas. No entanto deve realizar a sua própria resolução, deve realizar todas as experiências descritas e compreendê-las com clareza assim como compreender os resultados obtidos pelas mesmas.