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

SEGURANÇA

Project 04	**Deadline: 2023/04/28 (16:00)**	21 abril 2023
Expected time: 180 minutes	Contact and Non-contact hours	Using lab resources

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 e screenshots dos 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 03.
- Estude o módulo 6 e 7 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 a apresentação "Authentication, Authorization, and Accounting" partilhada na plataforma Nónio.

1. Ligue ao *switch* SWB uma instância da AAA GNS3 appliance (denominada doravante AAA-1). Siga, para esta instância, as mesmas regras que foram enunciadas no primeiro projeto para endereçar a nível 3 (endereço IP) e 2 (endereço MAC) os terminais da rede. Tenha em consideração que este será o seu quarto terminal de SWB. Corra o comando `ifconfig` de modo a comprovar o correto endereçamento deste novo servidor. Faça um *screenshot* do comando e respetivo *output* produzido. Clicando com o botão direito sobre AAA-1 selecione a opção `Configure` e em seguida consulte o conteúdo do separador `Usage` das `Node properties` para conhecer algumas configurações por omissão deste nó.
2. Abra uma consola em AAA-1 e execute o comando que lhe permita ver os *sockets* UDP ativos com a indicação de que o porto de escuta é `radius` / `radius-acct`. Corra o mesmo comando mas parametrizado de forma a que surjam os números dos portos em causa (vai precisar dessa informação adiante) e não os nomes dos serviços associados. Faça um único *screenshot* dos comandos e respetivo *output* produzido. Nos enunciados anteriores encontra os comandos a usar.
3. Para descobrir o software específico que está a fornecer o serviço RADIUS, e desse modo investigar como o pode configurar (pretende criar um novo utilizador para além dos existentes – "alice" e "bob" – e dar-lhe uma senha escolhida por si), corra no terminal AAA-1 o comando `service --status-all`. Por vezes a instalação e configuração do mesmo software / serviço varia de sistema operativo para sistema operativo. Consulte o *flavor* Linux em causa (comum a todos os terminais da topologia pois são *containers* alojados na VM onde corre o próprio servidor GNS3): `uname -a`. Faça um único *screenshot* dos comandos e respetivo *output* produzido. Pesquise agora (Google) manuais *online* de apoio à configuração do serviço RADIUS (*Remote Authentication Dial In User Service*) que se encontra ativo no terminal AAA-1 no âmbito do sistema operativo em apreço. Nota: Quando se conhece o paradigma (mais ou menos semelhante) de configuração de serviços em Linux, uma forma mais rápida de descobrir como se configura um serviço específico passa por procurar as propriedades da conta criada para a sua instalação. Uma inspeção atenta à base de dados de utilizadores pode ajudar: `cat /etc/passwd`. Repare na última linha deste ficheiro e atente particularmente na *home directory* do utilizador aí registado. Liste o conteúdo de tal pasta. Inspecione as diretorias e localize o ficheiro que (suspeite) é usado para alojar as contas dos utilizadores autenticados pelo RADIUS. Leia resumidamente a totalidade do mesmo. Estude num dos *links* devolvidos na pesquisa que fez como deve proceder para adicionar utilizadores a essa base de dados (se não encontrou nenhuma fonte de informação esclarecedora use esta). Pretende-se que adicione (recorrendo ao editor `pico`, por exemplo) um novo utilizador (a esse ficheiro) cujo *username* seja igual à primeira letra do seu primeiro nome, concatenada com o seu último apelido (sem espaços, acentos ou carateres especiais). Defina

uma *password* distinta da que os restantes utilizadores registados possuem ("gns3"). Defina também uma `Reply-Message` distinta, mais personalizada. Mostre em *screenshot* a configuração que acrescentou ao respetivo ficheiro.

4. Para além de um novo utilizador pretende-se que adicione uma entrada específica para o cliente (que será no nosso caso o *router* R1) na configuração do serviço RADIUS. Se inspecionar a pasta onde está a base de dados de utilizadores (ou o *link* simbólico para a mesma) também encontrará um ficheiro `clients.conf` que constitui a base de dados de clientes. Edite esse ficheiro com a ferramenta `pico`. Crie uma nova entrada no final do ficheiro que identifique o cliente (*o router* R1) pelo seu IP. Associe-lhe uma senha distinta do valor por omissão ("gns3"). Mostre em *screenshot* a configuração que acrescentou ao respetivo ficheiro depois de completamente validada (processo que apenas se completará após resolver com sucesso os próximos exercícios: não esqueça por isso de regressar a este ponto mais tarde para realizar o *screenshot* com a configuração já validada).

5. Configure finalmente R1 para que o Cisco IOS se torne cliente RADIUS do servidor configurado para autenticação de sessões SSH. Inicie no GNS3 uma captura de tráfego à saída de AAA-1. Teste a configuração realizada abrindo uma sessão SSH com as credenciais do novo utilizador a partir de A1. Da autenticação tentada devem resultar duas PDUs RADIUS capturadas. Porém a autenticação deve falhar. Pode validar a configuração realizada sem recurso ao terminal A1. Para tal execute em R1 o comando `test aaa group radius usernamecriado passwordatribuida legacy`. Mostre em *screenshot* a configuração acrescentada em R1, o resumo das duas PDU RADIUS capturadas e o resultado reportado pelo comando `test`.

6. Os serviços Linux normalmente precisam de ser notificados de alterações nos ficheiros de configuração de modo a relerem os mesmos. Esse provavelmente é o único passo que ainda não fez sobre o serviço de RADIUS para que tudo funcione como pretendido. É necessário que o processo que implementa o serviço RADIUS releia as bases de dados de utilizadores e de clientes que você atualizou. Este tipo de notificação dos serviços em Linux normalmente é feito enviando um sinal ao processo (usando o comando `kill`). O sinal comummente escolhido é o `SIGHUP`. Tal implica saber o PID do processo. É por isso que os serviços normalmente ao arrancarem escrevem o seu PID num ficheiro de nome e localização definidos na sua documentação. Para simplificar todos estes procedimentos comuns a todos os serviços Linux existe uma abordagem padrão (que também este serviço RADIUS respeita) que permite recorrer à ferramenta `service` e a um conjunto de *shell scripts* desenvolvidos para cada serviço e que esta ferramenta invoca. O modo de configuração de todos os serviços tende por isto a ser uniforme o que simplifica as tarefas de administração. Para que o serviço de RADIUS releia todos os ficheiros alterados execute o comando `service freeradius reload`. Se ler a *manpage* do comando `service` percebe que o primeiro argumento (`freeradius`) é o nome de um *script*. Onde estará o *script* `freeradius`? Pela documentação da referida *manpage* é fácil de descobrir (`/etc/init.d/`). Inspecione (recorrendo ao editor `pico`, por exemplo) este ficheiro, localize e transcreva a parte do *script* relativa ao comando (`reload`) em apreço e que constitui o segundo argumento do comando `service`. Descubra, analisando o mesmo *script*, o argumento do comando `service` que deve usar para consultar o estado do serviço. Consulte o respetivo estado usando esse argumento e o comando `service`. Inspecione as capturas de PDUs RADIUS e proceda ao devido *troubleshooting* até a autenticação de sessões SSH com as credenciais do novo utilizador que criou ficar operacional. A sua captura de tráfego deve abranger este processo e por isso o melhor é fazê-la sobre a interface de R1 da rede onde reside o servidor RADIUS. Deve ter o cuidado de guardar a captura pois vai precisar dela na avaliação. Pode ser útil ativar os eventos de *logging* do serviço RADIUS afinando as definições de configuração (`pico /etc/freeradius/3.0/radiusd.conf`) e em seguida vigiando os eventos (`tail -f /var/log/freeradius/radius.log`). Por vezes apenas o `reload` dos serviços não é suficiente. Pode mesmo ter que parar e reiniciar o serviço: `service freeradius stop` seguido de `service freeradius start` (ou apenas `service freeradius restart`). Faça o *screenshot* dos comandos realizados e respetivo relatório, do resumo do par de PDUs `Access-Request` e `Access-Accept`, do conteúdo de cada uma das PDUs onde seja visível o *`username`* e a `Reply-Message` respetivamente. Investigue (na RFC 2865) como é ofuscada a *password* do utilizador quando R1 solicita a AAA-1 a validação das credenciais. Faça um resumo de 4 linhas do processo. Em que livro se inspiraram os autores da RFC para este efeito?

7. Na sessão SSH que estabeleceu no ponto anterior (a partir de A1 para aceder a R1) execute o comando `show privilege`. Em que nível de privilégio se encontra depois de uma autenticação bem-sucedida sobre RADIUS? Mostre um *screenshot* do comando acompanhado do respetivo *output*. É possível recorrer ao RADIUS para atribuir a determinado utilizador um nível de privilégios específico após uma correta autenticação. Repare que este processo de Autorização ocorre em simultâneo com o processo de Autenticação. Não se trata propriamente de um processo de autorização quer próprio para o efeito quer aplicado comando-a-comando (como o TACACS+ permite) mas, ainda assim, e usando apenas RADIUS, permite que seja atribuído um nível de privilégios específico a cada utilizador aquando da sua correta autenticação. A Cisco esclarecer o assunto deste modo: "*Because RADIUS user authorization information is piggybacked in authentication responses, the authentication and authorization methods must use the same RADIUS scheme.*". Este processo de Autorização recorre a pares atributo-valor RADIUS (também denominados *Av Pair* : *Attribute-Value Pair*). O IETF previu um tipo de pares, denominado *vendor-specific* que os fabricantes (como a Cisco) exploram para operacionalizar funcionalidades proprietárias sobre RADIUS. Estes pares atributo-valor podem ser enviados do cliente RADIUS (*router*, neste caso) para o serviço RADIUS (neste caso alojado no terminal AAA-1) ou em sentido inverso. Tudo depende do serviço que se pretenda oferecer e da estratégia do próprio fabricante. Encontra um dicionário dos *Av Pairs* suportados pela Cisco aqui. O primeiro passo para operacionalizar o processo de Autorização descrito passa por instruir o IOS de R1 para proceder à Autorização por AAA / RADIUS. Tal como sucede com o processo de Autenticação, também no processo de Autorização podemos criar listas de métodos ou configurar a lista *default*. Neste caso específico sugere-se adotar a segunda estratégia por envolver menos comandos. No modo de configuração de R1 execute o comando `aaa authorization exec default group radius if-authenticated`. (Atenção!!! Antes de realizar este comando deve estar criada em R1 uma conta local que permita o nível máximo de privilégios. De outra forma pode perder-se acesso administrativo ao equipamento.) Com isto estará a indicar que, se corretamente autenticado, um utilizador também deverá ser autorizado via RADIUS. Ao fazê-lo R1 irá procurar, na mensagem de `Access-Accept` que recebe do serviço RADIUS, um par atributo-valor do tipo `Vendor-Specific` com um `Vendor ID` de valor 9 (valor reservado para identificar o fabricante Cisco). Ou seja, este será um `Cisco-AVPair`. A estrutura deste atributo é responsabilidade do fabricante. A Cisco estrutura-o em três campos, conhecidos por TLV. Trata-se de uma abordagem usada pelo próprio IETF nos protocolos modernos. Cada atributo é, portanto, caracterizado pelo tipo (*Type*), tamanho em bytes (*Length*) e valor (*Value*). O valor neste caso particular é uma *string* ASCII com o texto "`shell:priv-lvl=N`", onde `N` representa o nível de privilégio (1 a 15) a atribuir ao utilizador quando bem autenticado. O segundo passo para operacionalizar o processo de Autorização consiste em programar o serviço RADIUS convenientemente, indicando, na conta do utilizador pretendido (`/etc/freeradius/3.0/users`), os atributos específicos a usar (exemplo):

```
lsantos  Cleartext-Password := "12#$56/("
         Reply-Message = "Olá %{User-Name}, seja bem-vindo!",
         Service-Type = NAS-Prompt-User,
         Cisco-AVPair = "shell:priv-lvl=10"
```

Realize os dois passos mencionados adaptando as configurações ao seu caso específico. Não esqueça de, após atualizar com os atributos necessários o registo de autenticação do utilizador inicialmente criado, instruir o serviço RADIUS para reler o ficheiro alterado: `service freeradius reload` (ou `service freeradius restart`) se a primeira alternativa não surdir efeito). Termine a sessão SSH que abriu em A1 para R1. Estabeleça nova sessão para que se repita o processo de Autenticação (e de Autorização, neste caso). Analise o nível de privilégio que detêm agora. Inspecione as PDUs RADIUS capturadas neste processo. Guarde um *screenshot* da consola de A1 onde seja visível o acesso SSH, o comando de consulta de nível de privilégios e respetivo resultado. Guarde outro *screenshot* da mensagem `Access-Accept` onde sejam visíveis os detalhes dos *Av Pairs* acima mencionados.

8. Teste agora o serviço de Accounting sobre RADIUS. Tal como sucede com os processos de Autenticação e Autorização, também aqui podemos criar listas de métodos novas ou configurar a lista *default*. Por brevidade da configuração necessária vamos adotar a segunda das estratégias. No modo

de configuração de R1 execute o comando `aaa accounting exec default start-stop group radius`. Termine a sessão SSH que abriu em A1 para R1. Estabeleça nova sessão para que se repita o processo de *Authentication*, *Authorization* e, neste caso, de *Accounting*. Inspecione o nível de privilégios atribuído e termine a sessão. Guarde um *screenshot* do resumo das capturas de todas as PDUs RADIUS envolvidas e outro com os detalhes das novas mensagens relativas ao processo de *Accounting*.

9. Inicie uma nova captura em AAA-1 e grave a anterior para posterior consulta / apresentação durante o processo de avaliação. No capítulo anterior constatou que as *Views* (*Role Based Access Control* - RBAC) fornecem um mecanismo mais flexível que os privilégios para controlo de permissões. É possível, usando uma abordagem em tudo semelhante à seguida para os privilégios (e atrás testada), atribuir uma vista (e não um nível de privilégios) a um utilizador corretamente autenticado por RADIUS. Descubra o padrão do valor *Cisco-AVPair* que permite operacionalizar no IOS esta funcionalidade. Crie uma vista em R1 que permita apenas executar comandos `show`, crie um novo utilizador na base de dados do serviço RADIUS cujo *username* seja igual ao que começou por criar mas que termine em "2" e afine o respetivo *Cisco-AVPair* de modo que, ao ser bem autenticado, fique associado à vista criada. Estabeleça nova sessão SSH de A1 para R1 com o novo utilizador e consulte a vista ativa assim que entra. Inclua *screenshots* das configurações realizadas para o efeito, do novo acesso a R1 com a *view* reportada, do resumo das PDUs RADIUS associadas à autenticação/autorização em causa e os detalhes da mensagem `Access-Accept`. Indique ainda a fonte de informação que consultou para descobrir o *Cisco-AVPair*.

10. Inicie uma nova captura em AAA-1 e grave a anterior para entrega. O *appliance* GNS3 AAA possui o serviço TACACS+ ativo conforme viu atrás (`service --status-all`). Investigue como se configura este serviço. Programe R1 de modo que o processo de autenticação, autorização e *accounting* seja agora assegurado por TACACS+. Mostre por *screenshots* as configurações necessárias (em R1 e AAA-1) para que o primeiro utilizador, mencionado no início desta ficha, possa apenas realizar um subconjunto restrito de comandos (definidos por si) autorizados pelo serviço TACACS+. Mostre e explique, em *screenshot* distintos, vários resumos do tráfego TACACS+ capturado que está associado a cada processo em particular (autenticação, autorização e *accounting*) bem como os detalhes mais relevantes dos pacotes capturados.

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.