Trabalho pratico 1

Segurança

João coelho 2016016618

António Cassiano 2017019266

Francisco Amaral 2018019123

Segurança do equipamento

Configuração de username/passwords locais:

-Nos routers 7200 foram configurados os usernames e passwords(secrets) que foram pedidas(nos utilizamos secrets já que são mais seguras que as passwords já que são encryptadas);

-nos routers 2600 tambem foram configurados os usernames e passwords. Visto que não suporta secret usamos o comando “password” seguido do comando “service password encryption” para tentar proteger mais a palavra-passe;

Medidas anti acesso:

-As medidas de anti acesso não foram configuradas nos routers 2600 pois ao fim de uma longa pesquisa não foi encontrada nenhuma forma de ultrapassar este problema, porem no 7200 esta tudo como o que foi pedido;

Configuração do SSH permitindo apenas acesso via SSH aos equipamentos:

-Nos 2600 tivemos de usar o telnet já que o ssh não estava disponível, sabendo que o telnet e extremamente inseguro pois o trafego que vai desde o cliente ao servidor vai desincriptado, contudo mantivemos o telnet ativo para testar vários comandos introduzidos;

-Nos 7200 sempre que reiniciamos a topologia a chave desaparece e temos de introduzir o comando (crypto key generate rsa general-keys modulus 1024). Esta situação foi falada com o docente que leciona as aulas.

Configuração de privilégios

Vistas:

-Foi optado pela solução no router de gestão criarmos três vistas duas delas vistas normais e uma delas uma superview. Esta escolha foi optada muito pelo facto de existirem diversas restrições propostas no enunciado. Sendo estas:

“Nestes, apenas pode mexer no endereço IP e descritivo, tanto quando possível”;

“No router WAN e uplinks dos restantes routers deve poder alterar e visualizar o descritivo, apenas”;

-Onde foi executado os pontos atras descritos com sucesso, nas duas vistas anteriormente referidas, contudo deparamo-nos que juntando essas duas vistas numa superview reparamos que certos comandos foram negados, nomeadamente comandos de dentro das interfaces;

-De forma a tentar resolver este contratempo testamos colocar tudo numa vista apenas como foi “sugerido” pelo professor, mas, no entanto, deparamo-nos que este problema continuava a existir. Então apos vários dias de pesquisas (stack overflow, site da cisco, youtube, entre outros) não conseguimos encontrar uma solução para este problema (aplicar comandos a determinadas interfaces).

-Apesar de tudo no router WAN foi executado tudo como foi pedido no enunciado pelo facto do router WAN conter apenas interfaces de UPLINK.

-Nos routers 2600 devido haver muitos comandos associados a cada nível de privilégios optamos por apenas retirar alguns dos comandos já que seria muito demoroso de retirar todos os comandos, assim só retiramos alguns deles de forma a mostrar ao professor que sabemos fazer o que nos foi pedido;

Radius:

-Quando tentamos entrar as vezes não funciona devido a um erro de autorization fail, e reiniciando a máquina e inrtroduzing o comando “aaa autorization…” ele volta a dar. De resto foi tudo introduzido com sucesso.