TÉCNICO LISBOA

Gestão e Segurança de Redes
LETI - 2015/16

Projeto 2

Objetivo

Este projecto é a continuação do projecto anterior. Será usada a rede construída para o primeiro projecto.

O objectivo deste projecto é aumentar a segurança da rede da Autocar, limitando o seu acesso aos elementos autorizados e recorrendo a serviços seguros. Para tal a Autocar vai necessitar de configurar o serviço de firewall, utilizar SSH, usar HTTPS no acesso à sua página web, restringir o uso do DNS e disponibilizar um serviço de VPN.

Para a realização deste projecto, o encaminhamento e o serviço DNS, configurados na entrega anterior, têm de funcionar a 100%. Recorram aos horários de dúvidas se necessário.

SSH

A Autocar contratou um administrador de rede. Este trabalha remotamente, a partir da Internet. Deverá ser criada uma nova máquina, ligada ao router externo, para uso do administrador.

O administrador precisa de ter acesso de super-utilizador aos 4 servidores da Autocar. Para tal, criou um utilizador em cada um dos servidores (públicos e privados), aos quais acede com autenticação por chave pública. Esse utilizador utiliza o comando *sudo*[1] para executar comandos como root. O servidor SSH deverá impedir o login remoto como root.

Quando quer aceder aos servidores privados, que não são alcançáveis de fora, em alternativa a usar a VPN, o administrador usa um túnel SSH para um dos servidores públicos. Escreva um ou mais scripts com os comandos SSH necessários para criar o túnel e efectuar a ligação SSH ao servidor privado através do túnel. Para lançar vários programa em simultâneo, pode ser usado o programa *screen* para ter "vários écrans".

HTTPS

O site www.autocar.ttt contém informação privadas dos clientes que é necessário salvaguardar de terceiros. Como tal, o primeiro trabalho que foi solicitado ao administrador de rede foi configurar o

1 A imagem fornecida com o netkit não tem o *sudo* instalado. Esta aplicação pode ser instalada obtendo um pacote de https://archive.debian.net/lenny/i386/sudo/download e instalando-o com o comando *dpkg -i <ficheiro>*

acesso por HTTPS a este site. Por uma questão de custos, será usado um certificado auto-assinado. O acesso a este site por HTTP deverá resultar no redireccionamento automático para o mesmo site por HTTPS.

No interior da rede da Autocar, apenas os PCs da LAN dos serviços administrativos na Sede podem aceder ao site www.autocar.ttt. O acesso de outras máquinas deverá ser negado.

DNS

Os servidores DNS da Autocar servem dois propósitos: resolver nomes globais em nome das máquinas no interior da rede da Autocar; resolver os nomes da zona autocar.ttt para todas as máquinas que o solicitem, independentemente da sua origem.

Garanta que os servidores DNS da Autocar não resolvem pedidos DNS de zonas diferentes de autocar.ttt para máquinas no exterior da rede da Autocar.

Outra vulnerabilidade presente nos sistema de replicação master/slave dos servidores de DNS é que qualquer um se pode fazer passar pelo servidor master e obrigar o slave a carregar uma nova definição de zona falseada. Proteja a comunicação entre master e slave [BIND].

Firewall e NAT

O novo administrador de rede resolveu limitar os riscos de ataque à rede da Autocar reduzindo os acessos do exterior ao mínimo necessário.

Todas as máquinas existentes no interior da rede da Autocar devem poder aceder à Internet sem restrições. Mesmo às máquinas que usam IPs privados deve ser dada essa possibilidade, recorrendo a NAT (com masquerade).

Do exterior não pode ser possível aceder a nenhuma das máquinas com endereçamento privado. Aos servidores públicos apenas deverá ser possível aceder aos serviço que estas disponibilizam como sua função primária (e.g. HTTP, HTTPS, SMTP, IMAP, DNS, SSH).

Também não é possível iniciar uma ligação do exterior para nenhum dos PCs da Autocar com IP público, embora seja possível iniciar uma ligação destes para o exterior, como referido anteriormente. A excepção são os PCs de visitantes, que usufruem de um acesso à Internet sem quaisquer bloqueios em ambos os sentidos.

Todas estas configurações devem ser realizadas no router da sede.

VPN

O administrador de rede acede a todas as máquinas por telnet através do utilizador *guest* (com password *guest*). Também acede à intranet.

Com as novas regras de firewall, deixou de ser possível ao administrador de rede aceder às máquinas que gere. Antes também já não era possível aceder à máquinas com IP privado de fora. Além disso o telnet não é seguro. Assim, o administrador decidiu implementar um serviço de VPN para que possa trabalhar remotamente como se estivesse no interior da Autocar. Este corre no servidor DNS secundário.

As condições ao ligar à VPN devem ser as mesmas como se estivesse no interior da rede, nomeadamente devem ser usados os mesmos servidores de DNS e permitido o acesso a todas as máquinas da Autocar. A VPN não dá acesso à Internet.

Realização do projecto

Em informática e redes, o que não foi testado raramente funciona. Os grupos devem testar tudo o que fizeram e prepararem-se para mostrar esses testes durante a visualização do projecto.

As várias tarefas a realizar são independentes, podendo ser realizadas em paralelo. Recomenda-se o uso de um sistema de controlo de versões (tipo git).

Todos os elementos do grupo devem saber justificar e explicar as opções tomadas, dominando de igual forma o trabalho realizado por si e pelos colegas. É esperado que o trabalho seja distribuído de forma equitativa pelos elementos do grupo.

O projecto deve ser realizado de modo a não ser necessário entregar as imagens dos sistemas de ficheiros das máquinas virtuais (ou seja, os ficheiros *.disk*), já que são ficheiros muito grandes. Para o efeito, as configurações devem ser feitas usando os ficheiros *.startup* e as directorias com os nomes das máquinas virtuais.

Entrega e relatório

A entrega do projecto é realizada através do fenix até dia 20 de Maio às 17h00. A entrega é feita através do sistema Fénix e inclui um único ficheiro "**zip**" com: um relatório com 2 páginas (em **PDF**) a explicar as opções tomadas (ou seja, aquilo que for feito que não esteja explicitamente indicado neste enunciado, nomeadamente as escolhas efectuadas); todos os ficheiros do projecto na pasta "proj" (o "laboratório Netkit" criado).

Bibliografia

[Apache] Apache HTTP Server Documentation, http://httpd.apache.org/docs/

[GSR] Slides da cadeira

[BIND] BIND 9 Administrator Reference Manual http://www.bind9.net/Bv9.6ARM.pdf

[Netkit] Netkit documentation, http://wiki.netkit.org

[OpenVPN] OpenVPN Howto, https://openvpn.net/index.php/open-source/documentation/howto.html