SEGURANÇA INFORMÁTICA

FICHA PRÁTICA N.º3(1)

AUTENTICAÇÃO, AUTORIZAÇÃO E ACCOUNTING: RADIUS

NOTA: antes de realizar qualquer operação relembre-se das regras de funcionamento dos trabalhos práticos!

OBJECTIVOS

- Compreensão da necessidade de autenticação de utilizadores em sistemas informáticos
- Distinção entre autenticação, autorização e gestão de utilizadores
- Conhecimento da estrutura de um sistema RADIUS
- Configuração de servidores de autenticação RADIUS em Windows e Linux
- Familiarização e exploração de servidores RADIUS em múltiplos domínios.
- Compreensão e utilização de RADIUS proxy

Tópicos:

- Network Policy Server (Windows Server)
- Freeradius (Linux)
- JRadius – Ferramenta de teste de servidores RADIUS (Aconselhado)
- NTRadPing – Ferramenta de teste de servidores RADIUS (Usar apenas caso não tenha o java instalado)

EXERCÍCIOS

1. **Instalação do NAS**
    a. Numa máquina virtual Windows XP/7/10/11 use o software JRadius (precisa do java instalado) ou NTRadPing, disponíveis no moodle, que são ferramentas de teste de RADIUS e que atuam como um NAS. De preferência use o JRadius pois o NTRadPing apenas suporta autenticação usando PAP ou CHAP.

2. **Instalação e Configuração do servidor Radius Linux (FreeRadius)**
   Testado na versão Linux 16.04. A utilização em outras versões pode ter pequenas diferenças na instalação/configuração.

    a. Numa máquina virtual Linux instalar o servidor de Radius *Freeradius* via comando
       apt-get install freeradius
    b. Neste servidor Radius é necessário configurar quais vão ser os seus clientes NAS. Esta informação encontra-se no ficheiro **"/etc/freeradius/clients.conf"**. Para os parametrizar utilizem o exemplo ***client 10.10.10.10***, e para cada cliente NAS (no nosso trabalho, para além do JRadius também terão de configurar como um NAS o servidor IAS do Windows referido na 2 parte do trabalho):
        i. Manter o nome *client*
        ii. Alterar o endereço IP para a máquina de onde vai partir o pedido de autenticação
        iii. Configurar a *secret* que é a chave partilhada entre o RADIUS e o NAS.

c. Na mesma pasta da alínea anterior estão os ficheiros de configuração do servidor onde se podem definir as suas portas, o endereço IP (radiusd.conf), políticas de acesso (policy.conf) e de proxy (proxy.conf). Serve só para vossa consulta e não necessitam de alterar qualquer parâmetro.
d. No ficheiro ***users*** encontra-se informação sobre os utilizadores existentes que se podem autenticar no servidor. Através do exemplo *steve* criem utilizadores alterando este nome e activando a permissão de autenticação por password e/ou endereço IP ou outros atributos
e. Criem também um utilizador que seja rejeitado incluindo a mensagem de retorno. Para isto têm o exemplo *lameuser.*
f. Antes de colocar o servidor a correr temos de parar o processo iniciado assim que o programa se instala e que ocupa as portas de autenticação. O número deste processo está em /var/run/freeradius/freeradius.pid. Façam ***kill -9 nº processo***. É necessário fazer isto sempre que se alteram os programas de configuração.
g. Para iniciar o freeradius utilizar o comando: ***freeradius -X***
h. Após este comando podem ver na consola as mensagens de erro na compilação e os pedidos a chegar ao servidor e o tratamento feito a cada um incluindo a razão de ser rejeitado ou aceite.

3. Instalação e configuração do servidor Radius em Windows

A utilização deste guia depende da versão usada versões pois existem pequenas diferenças na instalação/configuração.

a. Numa máquina virtual Windows Server (pode necessitar o respetivo ISO):
    i. Seguir os passos: Ir para o *Server Manager*
    ii. Em Roles escolher "Add Roles" e seguir o wizard escolhendo adicionar o "*Network Policy Server*" (em versões mais recentes - "*Network Policy and Access Services*").
    iii. **Configurar o clientes NAS** – Para inserirem novos clientes no RADIUS aceder ao *Network Policy Server* >> *Clientes Radius* >> novo cliente RADIUS. Definir um nome, o endereço IP de onde ele se vai ligar e a palavra passe desse cliente. Os NAS deste servidor vão ser o *JRadius / NTRadPing* e o servidor Radius Linux via proxy.
    iv. **Definir a política de pedido de ligação** – para cada NAS criado vamos ter de definir a sua política de acesso: No RADIUS aceder às Politicas e definir uma nova política de ligação >> nas condições da política definam quais os parâmetros de controlo (p.e. o endereço IP ou nome de onde vão partir os pedidos)>> dar ou não acesso >>concluir.
    v. Vamos definir o que fazer aos pedidos vindos de cada cliente NAS: podemos definir se o pedido é autenticado neste servidor ou se é encaminhado para outro RADIUS >>concluir. Deve ver as opções existentes nas "politicas de rede"
    vi. Para testar com utilizadores Windows, deverá criar um utilizador, por exemplo em "*Computer management*" >> "*Local users And Groups*" e dar "permissões de acesso telefónico".
    vii. Pode ter que reiniciar o NPS (*Network Policy Server*) para que as alterações sejam implementadas rapidamente.

4. **Testes de autenticação de utilizadores com login/password utilizando o *JRadius***:
    a. Caso esteja a utilizar o *NTRadPing*, terá que alterar as politicas de segurança do Windows server para permitir o uso de autenticação por PAP ou CHAP.
    b. Efetue testes de autenticação a partir do *JRadius* para os RADIUS Windows e Linux. Registe as respostas e eventuais razões de rejeição no *JRadius*, na consola do Linux, ou no visualizador de Eventos do *Windows Server* (*Event Viewer>>"Security" e "System"*) nas seguintes situações:
        i. Testar autenticação e atributos devolvidos com os utilizadores criados na RADIUS Linux e Windows Server;
        ii. Testar o acesso com utilizadores inexistentes e verificar os atributos devolvidos;
        iii. Testar o acesso com utilizadores existentes, mas passwords erradas e verificar os atributos devolvidos;
    c. Implemente a possibilidade de envio de mensagens de resposta ao utilizador aquando da sua autenticação;
    d. Na máquina Windows cliente instalar e ativar o *Wireshark*; Verificar se conseguimos visualizar a password enviada pelo *JRadius* ao RADIUS Linux quando a encriptação é CHAP e PAP (desmarcar a opção CHAP no *NTRadPing*). Explique os resultados.

5. **Integração de uma estrutura RADIUS com proxy baseada em Realms utilizando os servidores Windows e Linux.**
    a. **Configurar o servidor Windows para proxy baseado em Realms para encaminhar pedidos ao servidor Linux**. - No servidor Windows criar uma política de pedido de ligação que direcione os utilizadores cujo nome seja xxx@linux para o servidor Radius da máquina Linux.
    b. Nos Grupos de Servidores RADIUS remotos temos de criar o servidor Linux.
    c. Aquando da construção da política que encaminha os pedidos para o Linux ter o cuidado de no campo "Atributo" do Perfil da Política de acesso retirar o @linux do user antes de o enviar ((.*)@(.*) -- Replace with $1 …. $2)
    d. Verificar e comprovar o encaminhamento dos pedidos entre os servidores;
    e. Verificar e comprovar o encaminhamento de um utilizador inexistente desde que tenha @linux no nome.
    f. Questão Teórica: Indique um sistema real seu conhecido que utilize a propriedade de RADIUS proxy dando um exemplo concreto do objetivo da sua utilização.

Nota 1: Caso pretendam fazer o encaminhamento de utilizadores a partir do Linux para o Windows, é necessário alterar o ficheiro *"proxy.conf",* de forma a redirecionar as conexões que pertençam ao realm @win (por exemplo) para o servidor em Windows