4452 – Linux Security Servers in Cloud

Desafio – Aula 06: Servidor Apache - Parte II

Tema: Sistema de Logs via WEB

A empresa Dexter Courier precisa implementar uma solução para visualizar os Logs dos serviços das máquinas Audit, FileServer e Storage via WEB.

O seu desafio é implementar o PhpLogCon, na máquina Audit, gravando logs no banco de dados MySQL.

Poste no Fórum Temático - Entrega de Desafios o screenshot tirado da página na máquina interna.

Resolução do Desafio:

01 – Para começar, logue com o usuário **root** e senha **4linux** na máquina Audit;

02 – Em seguida, acesse o prompt do MySQL com o usuário root, e adicione privilégios para o **root** e o usuário **rsyslog** com senha **senha**:

root@audit:~# **mysql -u root -p**

mysql> **grant all on *.* to 'root'@'%' identified by '123456' with grant option;**

mysql> **GRANT SELECT, INSERT, UPDATE, DELETE ON Syslog.* TO 'rsyslog'@'%' IDENTIFIED BY 'senha';**

mysql> **exit**

03 – Na máquina Audit, abra o arquivo de configuração do Rsyslog e adicione a seguinte a configuração do MySQL, abaixo da diretiva UDPServerRun:

root@audit:~# **vim /etc/rsyslog.conf**

….

$ModLoad imudp

$UDPServerRun 514

$ModLoad ommysql

. :ommysql:192.168.200.30,Syslog,rsyslog,senha

04 – Reinicie o serviço do Rsyslog para aplicar as configurações:

root@audit:~# **service rsyslog restart**

05 – Antes de instalar o PhpLogCon, instale e configure o pacote rsyslog-mysql:

root@audit:~# **apt-get install rsyslog-mysql**

root@audit:~# **dpkg-reconfigure rsyslog-mysql**

- Comece a configuração selecionando a opção **Sim** para configurar o pacote do rsyslog-mysql;
- No método de conexão selecione a opção **tcp/ip** para conectar no banco de dados via rede;
- Digite o IP **192.168.200.30** da máquina Audit, onde esta localizado o servidor MySQL;
- Digite a porta **3306** do servidor MySQL;
- Digite o nome do usuário **root** que é o administrador do servidor MySQL;

- Digite a **senha do usuário administrador** do servidor MySQL;
- Agora digite o nome do usuário **rsyslog** que possui permissão de escrita no banco Syslog;
- Digite a senha **senha** do usuário rsyslog;
- Para terminar digite o nome do banco **Syslog** responsável em armazenar os Logs no PhpLogCon.

06 – Se o ambiente LAMP não estiver pronto na máquina Audit, instale os seguintes pacotes:

root@audit:~# **aptitude install libapache2-mod-php5 php5 php5-curl php5-gd php5-intl php5-xmlrpc php5-mysql php-pear**

07 – O PHP5 é ativado, por padrão, durante a instalação do módulo, porém, caso necessário, habilite o suporte manualmente:

root@audit:~# **a2enmod php5**

08 – O próximo passo é utilizar o comando wget para baixar o fonte do PhpLogCon:

root@audit:~# wget -c http://download.adiscon.com/phplogcon/phplogcon-2.8.1.tar.gz

09 – Desempacote e descompacte a fonte no diretório /usr/local:

root@audit:~# tar xzvf phplogcon-2.8.1.tar.gz -C /usr/local/

10 – Acesse o diretório do fonte do PHPLogCon e copie o conteúdo do diretório src/

para /var/www:

root@audit:~# cd /usr/local/phplogcon-2.8.1/

root@audit:~# cp -R src/* /var/www/

11 – Acesse o diretório raiz do Apache e remova o arquivo da página de teste:

root@audit:~# cd /var/www/

root@audit:~# rm index.html

12 – Para poder configurar o PHPLogCon, crie o arquivo config.php e altere a permissão para o usuário do Apache:

root@audit:~# touch config.php

root@audit:~# chown www-data config.php

13 – Restarte o Apache para aplicar as configurações:

root@audit:~# service apache2 restart

14 – Para configurar o PHPLogCon, acesse o endereço http://audit.dexter.com.br na máquina Linux Interna.

- O erro que aparece é normal e faz parte da configuração. Clique em **here** para configurar o phplogcon;
- Agora, o instalador verificará se o sistema tem os pré-requisitos necessários para rodar o programa. Clique em **Next** para continuar;
- Um teste foi feito para saber se o PHPLogCon tem acesso de escrita no arquivo

config.php, criado e definido com as permissões para o usuário www-data. Clique em **Next** para continuar;

- Nesta tela é possível alterar algumas configurações, como números de mensagens, caracteres, etc. Deixe como padrão e clique em **Next** para continuar;
- Em **Source Type**, selecione **MYSQL Native** e em **Database Type Options** preencha a caixa com o **IP da máquina Audit**, nome da base de dados do MYSQL (**Syslog**), Database Tablename (**SystemEvents**), nome do usuário (**rsyslog**) e senha (**senha**). Após preencher os dados, clique em **Next** para continuar;
- Chegamos ao final de nossa configuração, clique em **Finish!**
- Parabéns! Você acaba de implementar um sistema de monitoramento em tempo real para os servidores da empresa DEXTER.