# Instalação do DVWA em uma máquina virtual vbox

# Créditos: Jean R T Delefrati <jeandelefrati@gmail.com>

# Documentação completa do Vagrant: https://docs.vagrantup.com

# AVISO! Este arquivo instala o DVWA (Damn Vulnerable Web Application)

# uma aplicação que pode comprometer a segurança do seu computador

# por favor não libere a porta 8080 para acesso externo e após terminar

# seus estudos, execute o seguinte comando para fechar a máquina virtual:

# vagrant halt

# encoding: UTF-8

Vagrant.configure(2) do |config|

# Instala a box Ubuntu Xenial 64bits

config.vm.box = "ubuntu/xenial64"

config.vm.box\_check\_update = false

# Encaminha a porta 80 da máquina virtual para a porta 8080

# do seu computador, para acessar: http://localhost:8080 em

# qualquer navegador

config.vm.network "forwarded\_port", guest: 80, host: 8080

# Configura a Virtualbox

config.vm.provider "virtualbox" do |vb|

# Ignora o visual, usar só terminal

vb.gui = false

# Memória da máquina virtual, 1G

vb.memory = "1024"

end

# Os comandos abaixo serão executados na primeira vez que você

# iniciar o "vagrant up" ou quando executar um

# "vagrant up --provision" (não recomendado)

config.vm.provision "shell", inline: <<-SHELL

echo '-- Atualizando os repositórios'

sudo apt-get -qq update -y

echo '-- Instalando o Apache web server'

sudo apt-get -qq install -y apache2 apache2.2-common apache2-utils apache2-mpm-prefork >> /vagrant/inst.log

echo '-- Instalando o PHP'

sudo apt-get -qq install -y libapache2-mod-php php php-common php-gd >> /vagrant/inst.log

echo '-- Instalando o editor NANO'

sudo apt-get -qq install -y nano >> /vagrant/inst.log

echo '-- Configurando o web server'

sudo service apache2 stop >> /vagrant/inst.log

sudo sed -i 's/www-data/vagrant/g' /etc/apache2/envvars

sudo sed -i '51iServerName 127.0.1.1' /etc/apache2/apache2.conf

sudo chown -R vagrant:root /var/lock/apache2

sudo service apache2 start >> /vagrant/inst.log

echo '-- Instalando o MySQL'

DBPASSWD=p@ssw0rd

debconf-set-selections <<< "mysql-server mysql-server/root\_password password $DBPASSWD"

debconf-set-selections <<< "mysql-server mysql-server/root\_password\_again password $DBPASSWD"

debconf-set-selections <<< "phpmyadmin phpmyadmin/dbconfig-install boolean true"

debconf-set-selections <<< "phpmyadmin phpmyadmin/app-password-confirm password $DBPASSWD"

debconf-set-selections <<< "phpmyadmin phpmyadmin/mysql/admin-pass password $DBPASSWD"

debconf-set-selections <<< "phpmyadmin phpmyadmin/mysql/app-pass password $DBPASSWD"

debconf-set-selections <<< "phpmyadmin phpmyadmin/reconfigure-webserver multiselect none"

sudo apt-get -y install mysql-server phpmyadmin php-mysql php-mysqli

echo '-- Configurando o PHP'

sudo sed -i "s/error\_reporting = .\*/error\_reporting = E\_ALL/" /etc/php/\*/apache2/php.ini

sudo sed -i "s/display\_errors = .\*/display\_errors = On/" /etc/php/\*/apache2/php.ini

sudo sed -i "s/allow\_url\_include = Off/allow\_url\_include = On/" /etc/php/\*/apache2/php.ini

echo '-- Executando os comandos pós instalação'

sudo service apache2 restart

sudo locale-gen UTF-8

echo '-- Baixando o DVWA'

cd ~

git clone https://github.com/ethicalhack3r/DVWA >> /vagrant/inst.log

sudo unlink /var/www/html/index.html

sudo mv DVWA/\* /var/www/html

sudo sed -i "s/recaptcha\_public\_key' ] = ''/recaptcha\_public\_key' ] = 'insecurekey'/" /var/www/html/config/config.inc.php.dist

sudo sed -i "s/recaptcha\_private\_key' ] = ''/recaptcha\_private\_key' ] = 'insecurekey'/" /var/www/html/config/config.inc.php.dist

sudo sed -i "s/'impossible'/'low'/" /var/www/html/config/config.inc.php.dist

sudo cp /var/www/html/config/config.inc.php.dist /var/www/html/config/config.inc.php

echo "-- Criando o arquivo para o ataque XSS"

echo "<?php @file\_put\_contents('cookies.txt', json\_encode(\$\_REQUEST) . ' - ' . json\_encode(\$\_SERVER) . PHP\_EOL, FILE\_APPEND);" > /var/www/html/cookie.php

echo '-- Script finalizado'

SHELL

end