Lab 4: Web Server Packet Analysis

Objective: Student will learn following:

- How to setup webserver
- Packet sniffing

[0] Prerequisites:
Create a VM for LAMP server: (Hostname:www/256MB RAM / 4GB HDD)

[1] Installation: on www

1-1 Required packages:

- **http: mysql mysql-server php php-gd php-mbstring php-mysql mod_auth_mysql httpd**
- **https: mysql mysql-server php php-gd php-mbstring php-mysql mod_auth_mysql httpd mod_ssl openssl crypto-utils**

1-2 Configuration files: (1) /etc/httpd/conf/httpd.conf (2)/etc/httpd/conf.d/ssl.conf

1-3 Installation:

[root@www /root]# **yum –y install mysql mysql-server php php-mysql **
mod_auth_mysql httpd mod_ssl openssl crypto-utils

[2] Install WordPress on the LAMP server.

Download WordPress from http://wordpress.org/latest.tar.gz
Create a WordPress driven website.

[3] From the Lin (Linux Workstation), install tcpdump and Wireshark.

While you are logging into WordPress driven website, sniff network traffic into a file using tcpdump and run WireShark to open it and find the following:

- **login name and password**
- **look for TCP packet, UDP packet**
- **look for IP packet**

[4] Configure the website to use SSL to make https website:

Make sure the your users will use http://www.coyoteone.net address instead of https://www.coyoteone.net

Come up with solution that redirects the http traffic to https automatically.

Remove private key file and certificate file:

[root@www /root]# **rm –vf /etc/pki/tls/private/*.key**
[root@www /root]# **rm –vf /etc/pki/tls/certs/*.crt**

Generate CA Certificate and Private key: www.coyoteone.net is an example.
[root@www /root]# **genkey www.coyoteone.net --days 365**

Next → Next → No →
US
California
San Bernardino
CSUSB.
CSE
www.coyote.net
Next → Encrypt the private key → Next → Passphrase(twice) → Next

Edit: /etc/httpd/conf.d/ssl.conf

SSLCertificateFile	**/etc/pki/tls/certs/www.coyote.net.cert**
SSLCertificateKeyFile	**/etc/pki/tls/private/www.coyote.net.key**
DocumentRoot	**"/var/www/html"**
ServerName	**www.coyote.net:443**

[5] Firewall Configuration:
[root@www /root]# **setup**
Firewall Configuration → SELinux (Disabled) → Customize → Select (SSH, HTTP,HTTPS) → OK → OK→ Quit
[4] Start the web service and testing:
[root@www /root]# **service httpd start**

Browse your http and https sites:
(1) http:// www.coyote.net -> https://www.coyote.net

[6] Get rid of pass phrase from httpd startup
[root@www /root]# **cd /etc/pki/tls/private**
[root@www private]# **cp www.coyote.net.key www.coyote.net.key.org**
[root@www private]# **openssl rsa -in www.coyote.net.key.org –out www.coyote.net.key**
[root@www private]# **chmod 400 www.coyote.net.key**
[root@www private]# **service httpd restart**
[root@www private]# **chkconfig httpd on**

[7] From the Lin (Linux Workstation):

While you are logging into WordPress driven website, sniff network traffic again and trying to find the following:

- **login name and password**
- **look for TCP packet, UDP packet**
- **look for IP packet**

[8] MySQL Configuration Example:

Edit /etc/my.cnf (add skip-networking in [mysqld] section)

[mysqld]
datadir=/var/lib/mysql
socket=/var/lib/mysql/mysql.sock
user=mysql
old_passwords=1
skip-networking

[root@www /root]#**mysql_secure_installation**

Start MySQL Server:

[root@www /root]# **/sbin/chkconfig mysqld on**
[root@www /root]# **/sbin/service mysqld start**

Remove /tmp/my.sql and MySQL History:

[root@www /root]# **rm -f /tmp/my.sql**
[root@www /root]# **cat /dev/null > $HOME/.mysql_history**

Set MySQL Admin Password:

[root@www /root]# **mysqladmin -u root password '*password*'**
[root@www /root]# **history –c**

Add database and user: ken is a example user. Please use your own.

[root@www /root]# **mysql –u root –p**
mysql>**use mysql;**
mysql> **CREATE DATABASE INVENTORY;**
mysql>**GRANT CREATE,INSERT,DELETE,UPDATE,SELECT,DROP,INDEX,ALTER ON INVENTORY.* to ken@localhost;**
mysql> **update user set password=password('*password*') where user='ken';**
mysql> **flush privileges;**
mysql> **exit;**

[9] MySQL Administration:

Remove MySQL History:

[root@www /root]# **cat /dev/null > $HOME/.mysql_history**

Set MySQL Admin Password:

[root@www /root]# **mysqladmin -u mydba password '*password*'**
[root@www /root]# **history –c**

Add / Remove Databases:

Add database:

[root@www /root]# **mysql –u mydba –p**

mysql> **CREATE DATABASE inventory;**

Drop database:
[root@www /root]# **mysql –u mydba –p**
mysql> **DROP DATABASE inventory;**

User management:

Add new user:
[root@www /root]# **mysql –u mydba –p**
mysql>**use mysql;**
mysql>**GRANT CREATE,INSERT,DELETE,UPDATE,SELECT,DROP,INDEX,ALTER ON inventory.* to ken@localhost;**
mysql> **update user set password=password('*password*') where user='ken';**
mysql> **flush privileges;**
mysql> **exit;**

Delete a user:
[root@www /root]# **mysql –u mydba –p**
mysql>**use mysql;**
mysql> **delete from user where user='ken';**
mysql> **flush privileges;**
mysql> **exit;**

How to reset my forgotten 'mydba' password:

Add new user:
[root@www /root]# **mysql –u mydba –p**
mysql>**use mysql;**
Shut down mysqld:
[root@www /root]# **service mysqld stop**

Start MySQL with skip-grant-tables mode:
[root@www /root]# **/usr/bin/mysqld_safe --skip-grant-tables --user=root &**
[root@www /root]# **mysql**
mysql>**UPDATE USER SET PASSWORD=PASSWORD('password') WHERE USER='mysqldba';**
mysql>**FLUSH PRIVILEGES;**

Restart MySQL Daemon:
[root@www /root]# **/sbin/service mysqld stop;**
[root@www /root]# **/sbin/service mysqld start;**

Back up and Restore:

Back up a database:
[root@www /root]# **mysqldump –u mydba –p invent > invent.sql**

Back up a table:
[root@www /root]# **mysqldump –u mydba –p invent Tb_invent > Tb_invent.sql**

Back up a table definition:
[root@www /root]# **mysqldump –u mydba –p –no-data invent Tb_invent > Td_invent.sql**

Restoring a database:
[root@www /root]# **mysql –u mydba –p –D invent < invent.sql**

Lab 4 Report

[1] Step by step installation and configuration procedures on:

- **tcpdump and WireShark**

[2] Step by step packet sniffing procedures using tcpdump and WireShark

[3] What did you learn from this lab?

[4] What was the difficult part of lab and troubleshooting method did you use?