Herramienta didáctica para realizar ataques de diccionario a plataformas Moodle

Objetivo

Construir una herramienta que permita realizar ataques de diccionario a plataformas moodle versiones 1.x.x y 2.x.x..

Descripción

La herramienta debe estar desarrollada en cualquiera de los lenguajes del módulo 2 (Perl, C, Python, C#), debe tener opciones de funcionamiento, y debe tener la capacidad de leer desde un archivo los usuarios y contraseñas para realizar el ataque de fuerza bruta.

Desarrollo

Para poder desarrollar la herramienta, debemos instalar alguna de las versiones a las cuales realizaremos el ataque.

Instalación de Moodle

Dentro de la página principal de moodle se encuentra la documentación necesaria para hacer la instalación, pero, esta se refiere a la última versión estable, para poder instalar una versión anterior que son las que competen a este desarrollo se debe realizar lo siguiente:

Requisitos mínimos:

- Base de datos (MariaDB, Postgres, MySQL)
- Servidor Apache
- PHP
- Si requiere mandar correos, servidor SMTP

La misma instalación verificará si existen deficiencias para la instalación.

Se debe descargar la versión de moodle que se desea instalar (en este caso la 2.7) desde un repositorio en GIT con la siguiente instrucción:

```
git clone -b MOODLE_27_STABLE git://git.moodle.org/moodle.git
```

Se debe tener instalado GIT para poder realizar esta operación.

Dentro del navegador web ingresamos a la siguiente dirección:

Nombre_del_servidor/moodle/

Donde el nombre del servidor debe ser el que tengan configurado, o en su defecto 'localhost'.

Al ingresar a dicha dirección se mostrará la página de inicio de la instalación que nos conducirá a través de ella para configurar las partes más importantes como son los directorios de trabajo y el manejador de la base de datos.

Desarrollo de la aplicación

La aplicación se desarrollo en Python 2.7, uno de los lenguajes sugeridos.
Para la parte principal se utilizaron las bibliotecas siguientes:

Httplib, Urllib, Sys, Os, Ssl, Re, HTMLParser, Mechanize.

Las bibliotecas o módulos que se encuentran disponibles para python se pueden instalar con la herramienta pip de la siguiente manera:
Si la herramienta no se encuentra instalada:
Como root:

`apt-get install python-pip` o `apt-get install pip3*`

*Depende de la versión de Pythona a utilizar.

Ya teniendo instalada la herramienta se instalan los módulos* de la siguiente manera:

```
pip install "nombre_del_modulo"
```

*Existen módulos que ya están instalados

Descripción del funcionamiento de la herramienta

La herramienta funciona de la siguiente forma:

1. Por medio de la línea de comandos tecleamos los siguiente:

```
./brutus.py -s moodle.org --user user.txt --pass passwd.txt -d
/login/index.php
```

Donde:
Brutus.py es el nombre de la herramienta,
-s indica el sitio moodle donde se realizará la prueba
--user archivo de usuarios o usuario con el que se probara el ataque
--pass archivo de passwords o password a probar para hacer el ataque
-d directorio donde normalmente se encuentra el login de usuario

Además cuenta con opciones para indicar puerto (--port), protocolo https(--sec), ayuda(-h) y generación de un reporte(--report).

2. Como se realiza el ataque.

Dependiendo de los parámetros ingresados en la línea de comandos la herramienta realizará lo siguiente:

-conformará una petición http o https, con los datos por default que usa el form de moodle para ingreso de usuario y contraseña (username y password), e ira armando, dependiendo de la combinación entre un solo usuario y password o archivos para uno o ambos casos.

- hará las peticiones una a una y marcará cuales de ellas han tenido éxito.
- Mostrará el código de respuesta y si la petición se realizó de manera correcta
- Creará un reporte html si se solicita

3. Observaciones

La herramienta prueba los usuarios más comúnmente usados al configurar moodle, de ahí que exista la vulnerabilidad del ataque de fuerza bruta para las versiones que se probaron.

Referencias.

https://docs.python.org

https://docs.moodle.org

Manual de uso de la herramienta brutus v.1

Herramienta para realizar ataques de diccionario a plataformas moodle a través de peticiones http y https.

La herramienta brutus cuenta con las siguientes opciones de funcionamiento:

BRUTUS

```
Brutus - Brute Force Tool (for Moodle)

Brutus es una herramienta que puede realizar ataques de diccionario

Puede generar reportes con un resumen de la configuración del ataque.

PARAMETROS

-d (obligatorio) - Especifica el recurso a analizar en el host. Si no se especifica,
por defecto se usa '/login/index.php'

--pass (obligatorio) - Especifica un diccionario de contraseñas. Si no es un archivo,
se toma como la contraseña a probar.

-r (opcional)    - Genera un reporte en 'html' y otro en 'texto plano' con la
configuración del ataque.

-s (obligatorio) - Especifica una dirección IP o nombre de dominio del objetivo.

--user (obligatorio) - Especifica un diccionario de usuarios. Si no es un archivo, se
toma como el usuario a probar.

--port (opcional)    - Especifica el puerto a usar. Si no se especifica, se usa el
puerto 80 (HTTP) o 443 (HTTPS).

--sec (opcional) - Especifica que el protocolo a usar es HTTPS. Si no se especifica,
se usa el protocolo HTTP

EJEMPLOS DE USO

thttp://aulavirtual.com/login/index.php\n\tbrutus.py --user usuarios.txt --pass
hola123., -s aulavirtual.com

https://192.168.2.56/index.php\n\tbrutus.py --user usuarios.txt --pass passwords.txt
-s 192.168.2.56 d /index.php --sec
```

Generación de reportes en el siguiente formato:

Reporte Brutus (Autogenerado)

En este reporte se detalla la actividad realizada con Brutus

DATOS GENERALES

Recurso	/login/index.php
Usuario	user.txt
Fecha	Fri Mar 10 09:19:38 2017
Password	passwd.txt
Moodle	2.9.0
Direccion	aula.cert.unam.mx
Intentos	50
https	False
Puerto	80

CREDENCIALES VÁLIDAS ENCONTRADAS 0

USUARIO	PASSWORD

RECOMENDACIONES

1. Deshabilitar usuarios por defecto
2. Usar contraseñas seguras
3. Autenticación de dos factores
4. Uso de Captcha
5. Validar Entradas de usuario
6. Validar peticiones HTTP
7. Limitar intentos de conexión y/o login
8. Recurrir a bitacoras
9. Respaldo de Bases de Datos y Archivos de configuración