Idea del TPI

Integrantes del grupo (Curso: 5k2)

- Lambertucci Juan Pablo 90606
- Sampieri Matias 89465
- Daniele Valentina 90320
- Alfonso Agustin 90418

Idea

Teníamos pensado desarrollar una herramienta de línea de comandos para realizar ataques de fuerza bruta/IDOR de forma paralela y distribuida. La idea es que sea extremadamente simple de usar y configurar. Un ejemplo de como funcionaria:

```
bruteforce -b 1000 config.yaml
```

La opción -b define la cantidad máxima de peticiones en paralelo, si por ejemplo se quieren hacer 10.000 peticiones, se harán 10 tiradas de 1000 peticiones. El archivo config.yaml tendria la siguiente estructura:

```yaml
request:
  method: GET
  url: http://test.com/productos/$id$
  params:
    id: "$id$"
  headers:
    cookie: "sessionid=ab3235bac5"
    test: "test1=$id$"
  body: 'hola 123'

params:
  id:
    type: RANGE
    from: 1
    to: 10000

criteria:
  type: STOP
  response:
    status: 200
    body:
      '*ok*'

helpers:
  - 192.168.1.55
```

Se define como será la petición (método, headers, parámetros de URL, body) y entre signos peso se indican los parámetros que se modifican en cada petición. Por ejemplo en este caso se harán 10.000 peticiones donde `$id$` irá de 1 a 10.000. También se podrá especificar `type: DICT dict: ['hola', 'chau', 'test']` para usar un diccionario en vez de una secuencia de números. Los parámetros modificables pueden ser incluidos en headers, parámetros URL, path URL y el body.

Puede también haber un criterio de corte, en este se podrá especificar el resultado que se necesita para cortar el proceso. En este caso el body debe contener la cadena 'ok' y el código de respuesta debe ser 200. Tambien en vez de cortar se podrá especificar que las respuestas que cumplan con ese criterio sean logueadas (`type: LOG` en vez de STOP)

Los helpers son las direcciones IP de otras computadoras (ninguna o varias) a las que se le repartirá el trabajo. En este caso la máquina 192.168.1.55 hará las peticiones de 5.000 a 10.000 mientras que la máquina que ejecuto el comando hará de 1 a 4.999. Si alguna instancia (ya sea la principal o algún helper) llega al criterio de corte se cortaran todos los procesos y en el caso de que un helper haya sido el que llegó al criterio este le enviará a la instancia principal la respuesta que cumplio con el criterio.

Si se inicia el programa sin especificar el archivo de configuración se inicia en modo helper y escucha hasta que una instancia principal de la aplicación se comunique y le envíe su configuración.