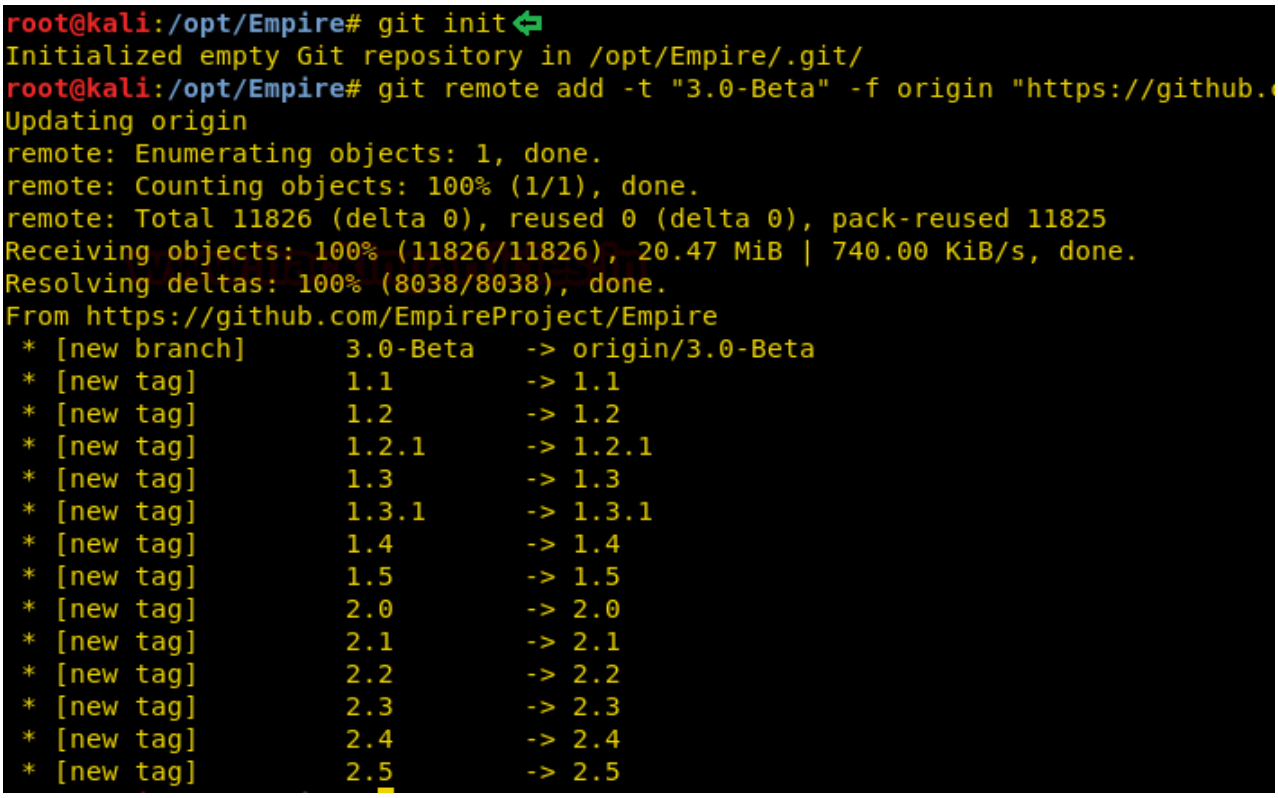
Empire GUI: Graphical Interface to the Empire Post-Exploitation Framework

hackingarticles.in/empire-gui-graphical-interface-to-the-empire-post-exploitation-framework

Raj March 27, 2019

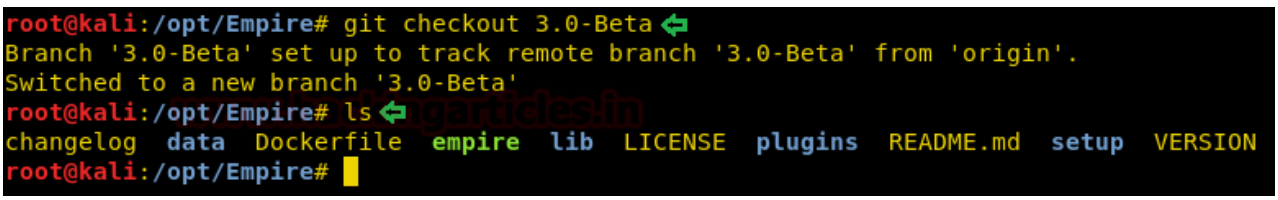
This is our 8th post in the series of the empire which covers how to use empire as GUI. Empire has a great GUI mechanism, but it's still developing as it has been released just a while back. For empire GUI to work, we need to download all of its dependencies and this is where it gets a bit complicated. So, first of all, we will download the beta 3.0 version of empire as it's the only version compatible with the GUI. Using the following commands:

```
git init
git remote add -t "3.0-beta" -f origin "//github.com/EmpireProject/Empire"
```



Now run the following command as instructed on the GitHub page :

```
git checkout 3.0-Beta
```



Now to install the beta version, type the following command :

```
./setup/install.sh
```

```
root@kali:/opt/Empire# ./setup/install.sh
Hit:1 https://packages.microsoft.com/debian/9/prod stretch InRelease
Hit:2 https://packages.microsoft.com/repos/microsoft-debian-stretch-prod stretch InRelease
Hit:3 http://ftp.yzu.edu.tw/Linux/kali kali-rolling InRelease
Reading package lists... Done
Reading package lists... Done
Building dependency tree
Reading state information... Done
multiarch-support is already the newest version (2.28-2).
multiarch-support set to manually installed.
The following packages were automatically installed and are no longer required:
  libboost-program-options1.67.0 libboost-python1.62.0 libboost-serialization1.67.0 libboost-syst
  libfcgi-bin libfcgi0ldbl libicu-le-hb0 libicu60 liblwgeom-2.5-0 liblwgeom-dev libpoppler80 libp
  libqgis-analysis2.18.25 libqgis-analysis2.18.28 libqgis-core2.18.25 libqgis-core2.18.28 libqgis
  libqgis-networkanalysis2.18.28 libqgis-server2.18.25 libqgis-server2.18.28 libqgispython2.18.25
  libspatialindex4v5 libspatialindex5 python-cycler python-kiwisolver python-matplotlib python-ma
  python-pyside.qtnetwork python-pyside.qtwebkit python-pyspatialite python-qgis python-qgis-comm
  ruby-dm-serializer ruby-faraday ruby-geoip ruby-libv8 ruby-ref ruby-therubyracer
```

Now to run empire use the following as it will link the command line to GUI version :

```
./empire –server –shared_password 12345 –port 1337
```

```
root@kali:/opt/Empire# ./empire --server --shared_password 12345 --port 1337
[*] Loading stagers from: /opt/Empire//lib/stagers/
[*] Loading modules from: /opt/Empire//lib/modules/
[*] Loading listeners from: /opt/Empire//lib/listeners/
[*] Empire starting up...
```

And as shown in the image below, the Empire will start.

```
[+] Empire Collaboration Server started:
 Host => 0.0.0.0
 Port => 1337
 Password => 12345
WebSocket transport not available. Install eventlet or gevent and gevent-web
 * Serving Flask app "lib.common.server" (lazy loading)
 * Environment: production
   WARNING: Do not use the development server in a production environment.
   Use a production WSGI server instead.
 * Debug mode: off
 * Running on https://0.0.0.0:1337/ (Press CTRL+C to quit)
```

Now, download the GUI of empire from GitHub using the following command :

```
git clone //github.com/EmpireProject/EmpireGUI.git
```

```
root@kali:/opt# git clone https://github.com/EmpireProject/Empire-GUI.git
Cloning into 'Empire-GUI'...
remote: Enumerating objects: 15142, done.
remote: Total 15142 (delta 0), reused 0 (delta 0), pack-reused 15142
Receiving objects: 100% (15142/15142), 68.41 MiB | 664.00 KiB/s, done.
Resolving deltas: 100% (3008/3008), done.
Checking out files: 100% (16340/16340), done.
```

Now that GUI of empire and the beta version of empire has been downloaded, we need to install its dependencies for it to work successfully. And for that, we will have to download nodejs first and to download it, type :

```
apt install nodejs
```

And in time, it will be installed as shown in the image below :

```
root@kali:/opt/Empire-GUI# apt install nodejs
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following packages were automatically installed and are no longer required:
  gyp libjs-inherits libjs-is-typedarray libnode-dev libssl-dev libuv1-dev
Use 'apt autoremove' to remove them.
Suggested packages:
  npm
The following NEW packages will be installed:
  nodejs
0 upgraded, 1 newly installed, 0 to remove and 0 not upgraded.
Need to get 0 B/86.1 kB of archives.
After this operation, 161 kB of additional disk space will be used.
Selecting previously unselected package nodejs.
(Reading database ... 445064 files and directories currently installed.)
Preparing to unpack .../nodejs_10.15.1~dfsg-5_amd64.deb ...
Unpacking nodejs (10.15.1~dfsg-5) ...
Setting up nodejs (10.15.1~dfsg-5) ...
update-alternatives: using /usr/bin/nodejs to provide /usr/bin/js (js) in auto mode
Processing triggers for man-db (2.8.5-2) ...
```

After nodejs, we have to download npm and for that type :

```
apt install npm
```

```
root@kali:/opt/Empire-GUI# apt install npm
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following additional packages will be installed:
  node-abbrev node-ajv node-ansi node-ansi-align node-ansi-regex node-ansi-styles no
  node-aws4 node-balanced-match node-bcrypt-pbkdf node-bluebird node-boxen node-brac
  node-chownr node-cli-boxes node-cliui node-clone node-co node-color-convert node-c
  node-copy-concurrently node-core-util-is node-cross-spawn node-cyclist node-dashda
  node-detect-indent node-detect-newline node-duplexer3 node-duplexify node-ecc-jsbr
  node-extsprintf node-find-up node-flush-write-stream node-forever-agent node-form-
  node-get-stream node-getpass node-glob node-got node-graceful-fs node-gyp node-har
  node-hosted-git-info node-http-signature node-iconv-lite node-iferr node-import-la
  node-is-object node-is-plain-obj node-is-retry-allowed node-is-stream node-is-type
  node-json-stable-stringify node-json-stringify-safe node-jsonify node-jsonparse no
  node-lowercase-keys node-lru-cache node-mem node-mime-types node-mimic-fn node-mim
  node-node-uuid node-nopt node-normalize-package-data node-npm-package-arg node-npm
  node-p-cancelable node-p-finally node-p-limit node-p-locate node-p-timeout node-pa
  node-prepend-http node-process-nextick-args node-promise-inflight node-promzard no
  node-readable-stream node-registry-auth-token node-registry-url node-request node-
  node-semver node-semver-diff node-set-blocking node-sha node-shebang-command node-
  node-spdx-license-ids node-sshpk node-ssri node-stream-each node-stream-iterate no
  node-supports-color node-tar node-term-size node-text-table node-through node-thro
  node-unique-filename node-unpipe node-url-parse-lax node-url-to-options node-util-
  node-which node-which-module node-wide-align node-widest-line node-wrap-ansi node-
The following NEW packages will be installed:
```

As its download, like in the image above, now run the following command in order to install it :

```
npm install
```

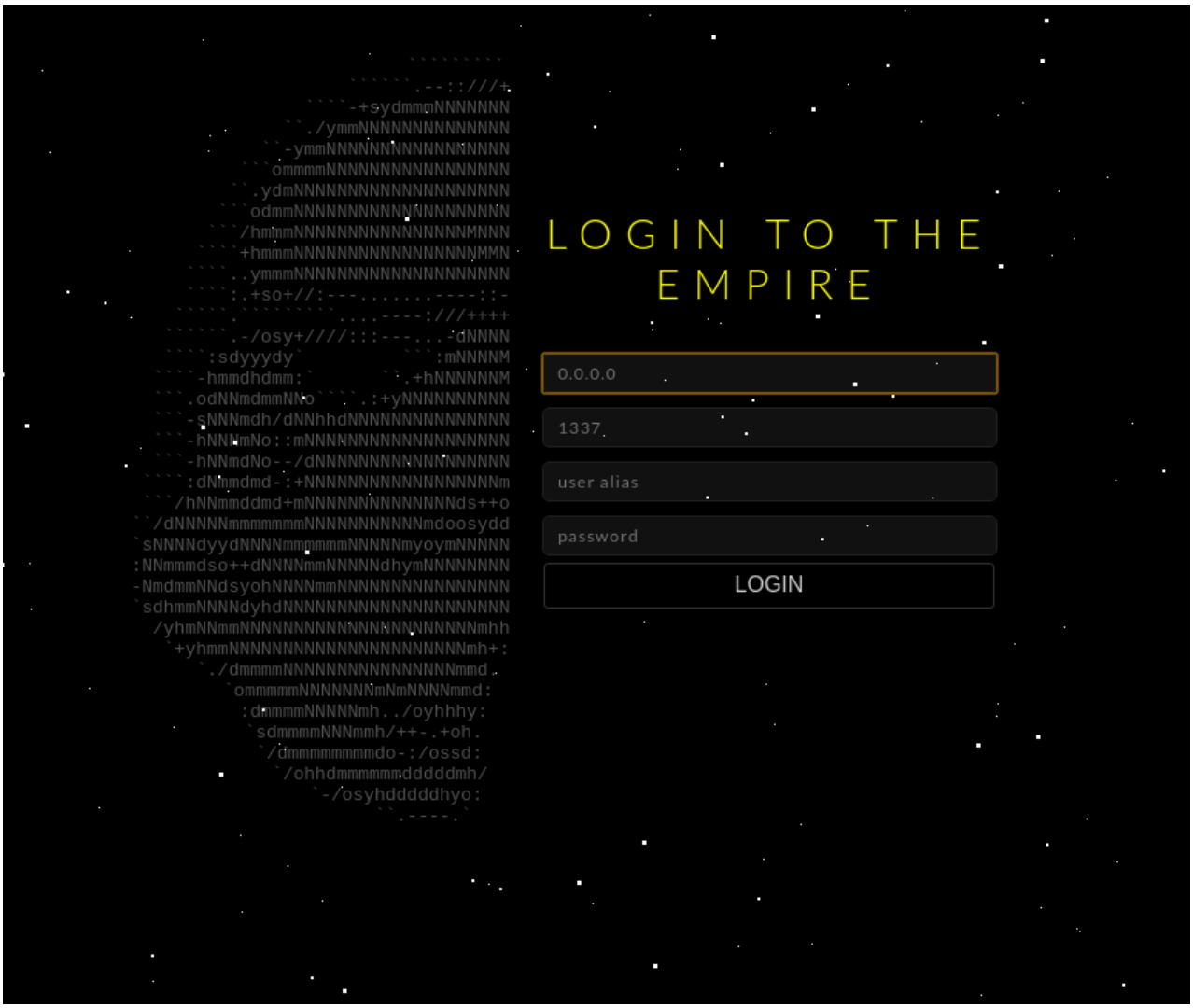
```
root@kali:/opt/Empire-GUI# npm install
npm WARN npm npm does not support Node.js v10.15.1
npm WARN npm You should probably upgrade to a newer version of node as we
npm WARN npm can't make any promises that npm will work with this version.
npm WARN npm Supported releases of Node.js are the latest release of 4, 6, 7, 8, 9.
npm WARN npm You can find the latest version at https://nodejs.org/
npm WARN deprecated browserslist@1.7.7: Browserslist 2 could fail on reading Browserslist

> electron@1.8.8 postinstall /opt/Empire-GUI/node_modules/electron
> node install.js

Downloading SHASUMS256.txt
[============================================>] 100.0% of 5.74 kB (5.74 kB/s)
npm WARN lifecycle empire-framework-gui@0.0.0~postinstall: cannot run in wd empire-framewo
npm WARN ajv-keywords@2.1.1 requires a peer of ajv@^5.0.0 but none is installed. You must
npm WARN optional SKIPPING OPTIONAL DEPENDENCY: fsevents@1.2.7 (node_modules/fsevents):
npm WARN notsup SKIPPING OPTIONAL DEPENDENCY: Unsupported platform for fsevents@1.2.7: wan

added 5 packages from 28 contributors in 139.686s
```

And then start the npm service, as shown in the image below, with the following command :

```
npm start
```

```
root@kali:/opt/Empire-GUI# npm start
npm WARN npm npm does not support Node.js v10.15.1
npm WARN npm You should probably upgrade to a newer version of node as we
npm WARN npm can't make any promises that npm will work with this version.
npm WARN npm Supported releases of Node.js are the latest release of 4, 6, 7, 8, 9.
npm WARN npm You can find the latest version at https://nodejs.org/

> empire-framework-gui@0.0.0 start /opt/Empire-GUI
> node build/start.js
```

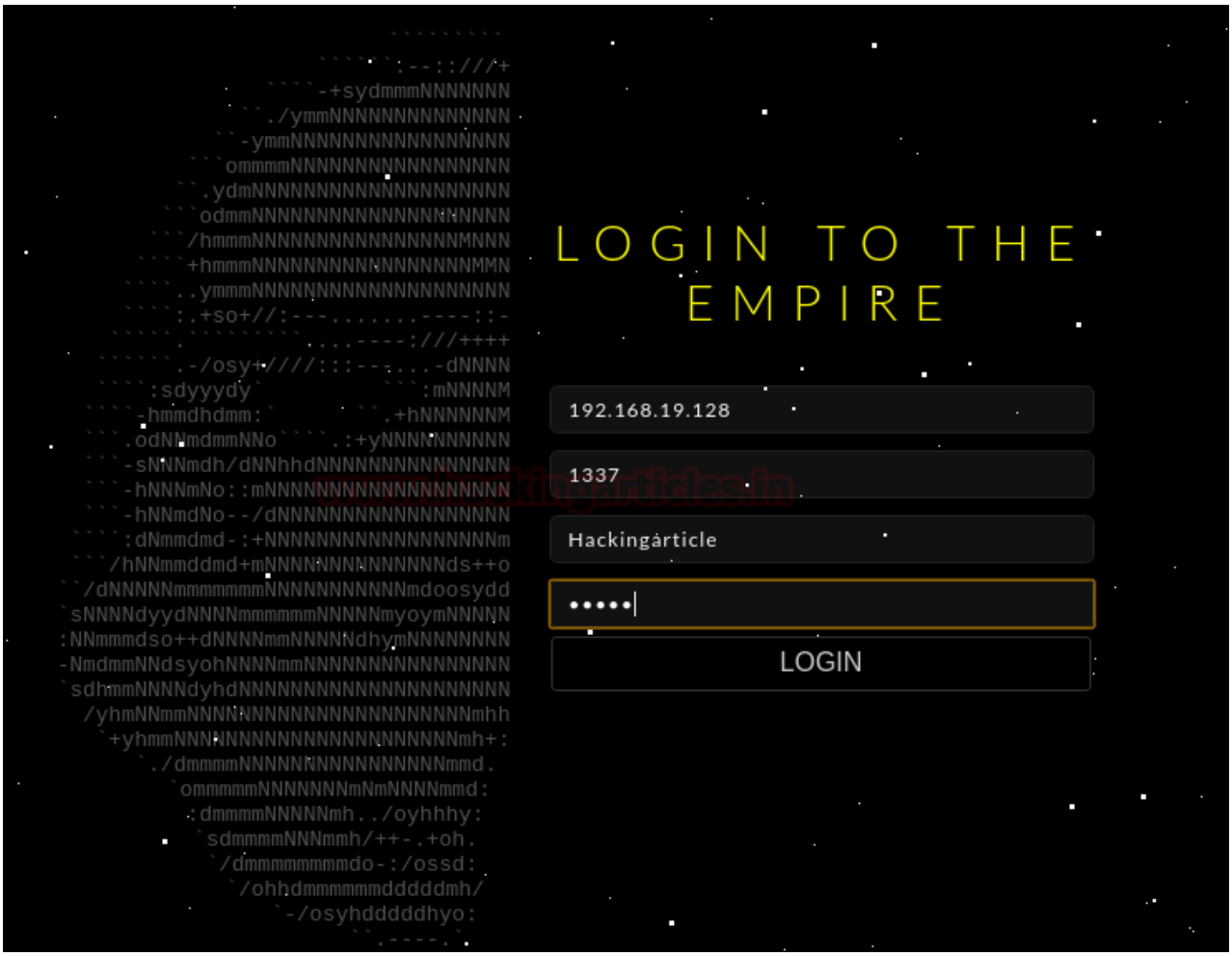
After all this, the GUI of empire will start as shown in the image below :



Moving further once the GUI of empire is up and running, create a stager and get an agent from the beta version of empire, while getting a session, remember to use port 1337 as that is the port the GUI works on.

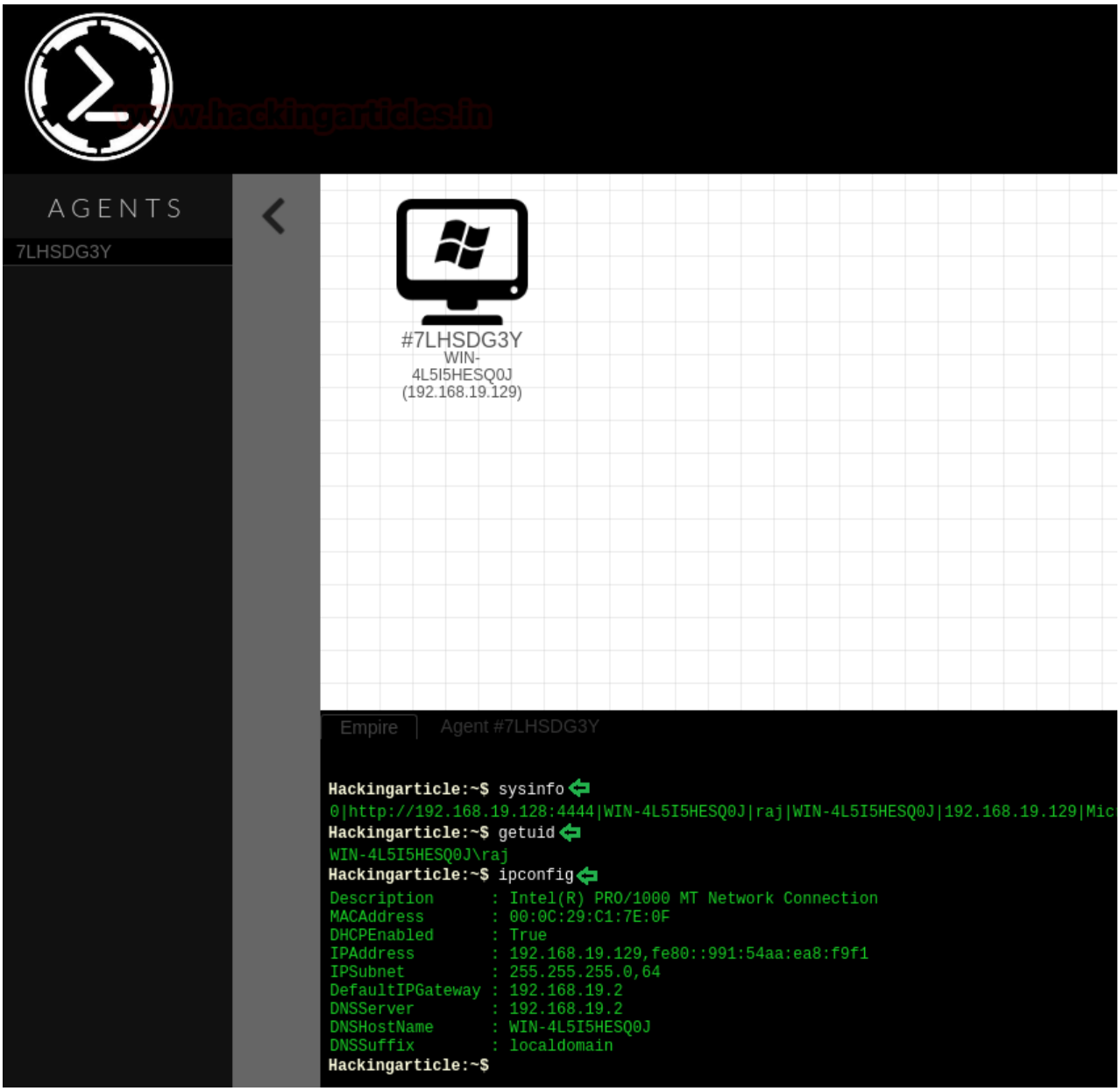
```
(Empire: stager/windows/hta) > agents

[*] Active agents:

 Name     La Internal IP     Machine Name      Username                Process
 ----     -- -----------     ------------      --------                -------
 7LHSDG3Y ps 192.168.19.129  WIN-4L5I5HESQ0J   WIN-4L5I5HESQ0J\raj     powershell
```

Now, on the GUI, log in using your IP and port and other details as shown in the image below :



And as you will login, it will show you all the sessions you have, just like in the image below :

Here, all the shell commands will work as shown in the image above. As the GUI is still developing, we can't use it for post exploitations. But it, it comes pretty handy in order to manage multiple sessions and it helps you understand it's working better.



Author: Sanjeet Kumar is an Information Security Analyst | Pentester | Researcher
Contact **Here**