iSEC
information security inc.

FlightSim

Information Security Inc.

Contents

- What is FlightSim?
- Testing Environment
- Installing FlightSim
- Running FlightSim
- References

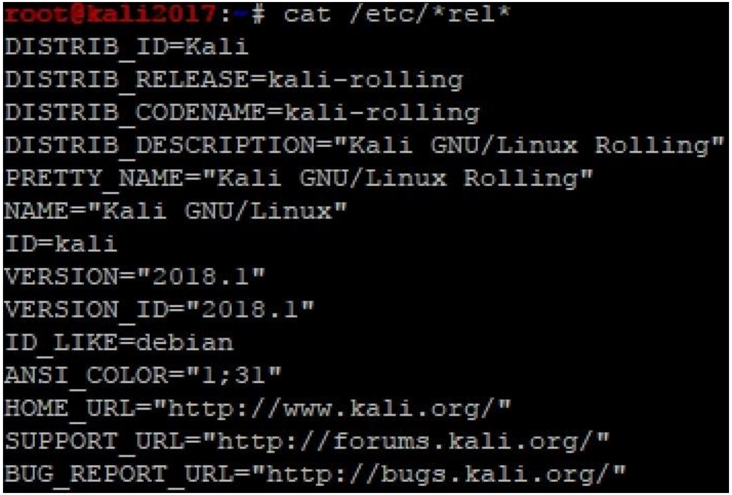
What is FlightSim?

- flightsim is a lightweight utility used to generate malicious network traffic and help security teams to evaluate security controls and network visibility
- The tool performs tests to simulate DNS tunneling, DGA traffic, requests to known active C2 destinations, and other suspicious traffic patterns

alphasoc / flightsim

Testing Environment

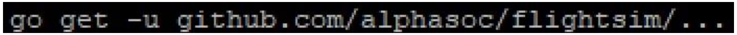
- Kali Linux 2018.1



```
root@kali2017:~# cat /etc/*rel*
DISTRIB_ID=Kali
DISTRIB_RELEASE=kali-rolling
DISTRIB_CODENAME=kali-rolling
DISTRIB_DESCRIPTION="Kali GNU/Linux Rolling"
PRETTY_NAME="Kali GNU/Linux Rolling"
NAME="Kali GNU/Linux"
ID=kali
VERSION="2018.1"
VERSION_ID="2018.1"
ID_LIKE=debian
ANSI_COLOR="1;31"
HOME_URL="http://www.kali.org/"
SUPPORT_URL="http://forums.kali.org/"
BUG_REPORT_URL="http://bugs.kali.org/"
```

Installing FlightSim

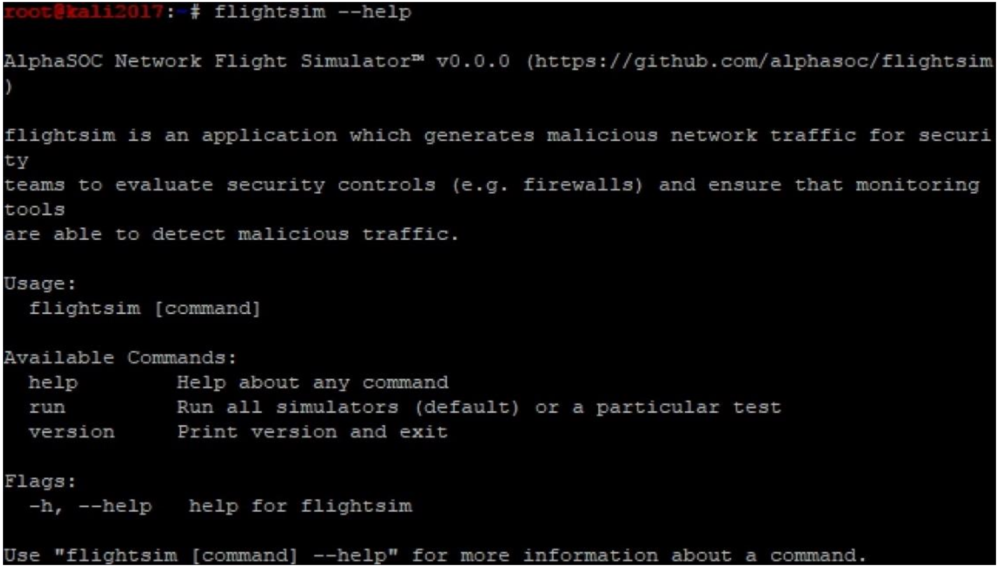
- Built using Golang in any environment (e.g. Linux, MacOS, Windows)



```
go get -u github.com/alphasoc/flightsim/...
```

Running FlightSim

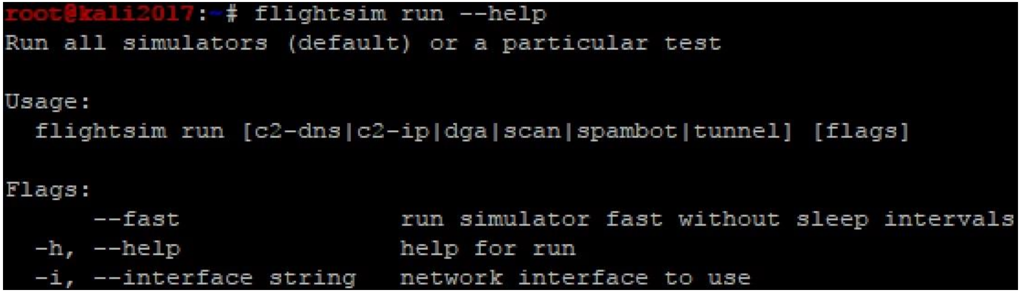
- Help menu



```
root@kali2017:~# flightsim --help

AlphaSOC Network Flight Simulator™ v0.0.0 (https://github.com/alphasoc/flightsim
)

flightsim is an application which generates malicious network traffic for securi
ty
teams to evaluate security controls (e.g. firewalls) and ensure that monitoring
tools
are able to detect malicious traffic.

Usage:
  flightsim [command]

Available Commands:
  help        Help about any command
  run         Run all simulators (default) or a particular test
  version     Print version and exit

Flags:
  -h, --help   help for flightsim

Use "flightsim [command] --help" for more information about a command.
```

Running FlightSim

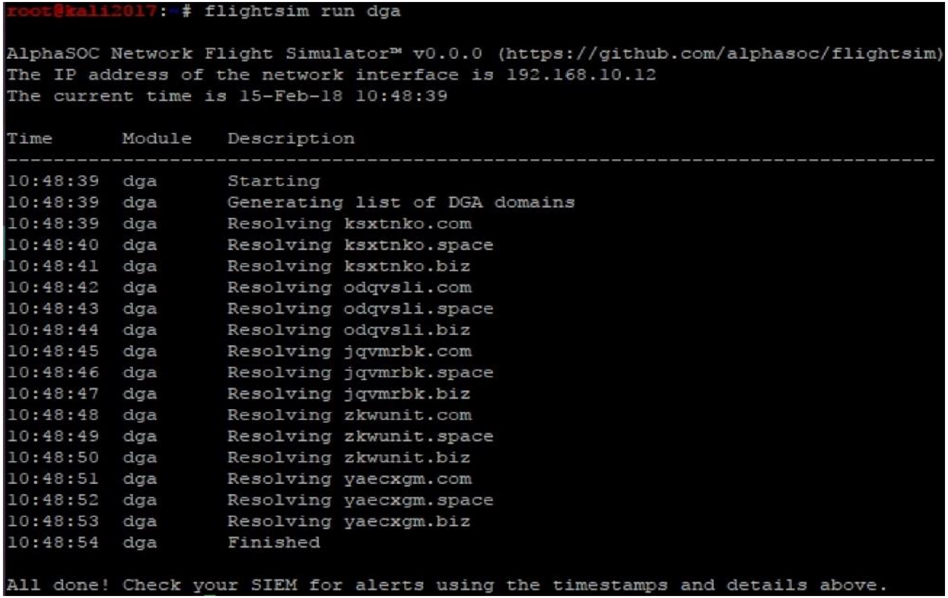
- To list the available modules => flightsim run --help



```
root@kali2017:~# flightsim run --help
Run all simulators (default) or a particular test

Usage:
  flightsim run [c2-dns|c2-ip|dga|scan|spambot|tunnel] [flags]

Flags:
      --fast                 run simulator fast without sleep intervals
  -h, --help                 help for run
  -i, --interface string   network interface to use
```

Running FlightSim

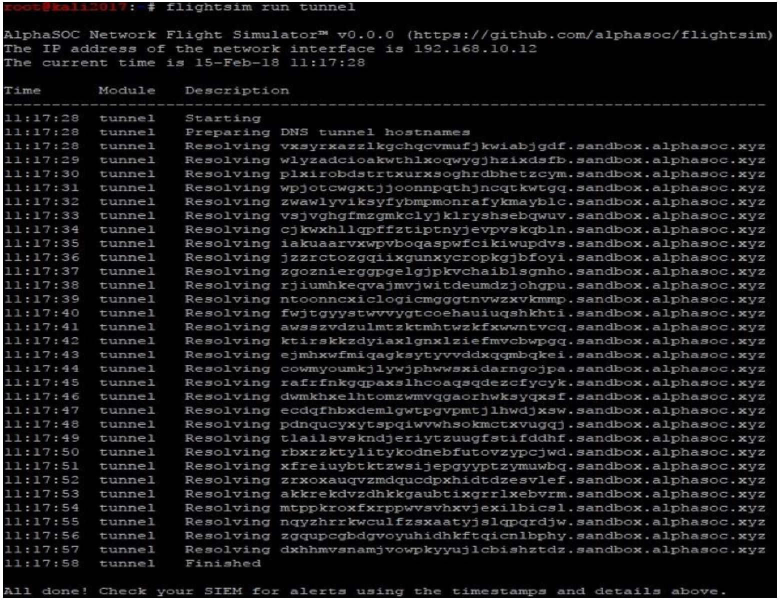
- Generating list of DGA domains



```
root@kali2017:~# flightsim run dga

AlphaSOC Network Flight Simulator™ v0.0.0 (https://github.com/alphasoc/flightsim)
The IP address of the network interface is 192.168.10.12
The current time is 15-Feb-18 10:48:39

Time      Module   Description
--------------------------------------------------------------------------------
10:48:39  dga      Starting
10:48:39  dga      Generating list of DGA domains
10:48:39  dga      Resolving ksxtnko.com
10:48:40  dga      Resolving ksxtnko.space
10:48:41  dga      Resolving ksxtnko.biz
10:48:42  dga      Resolving odqvsli.com
10:48:43  dga      Resolving odqvsli.space
10:48:44  dga      Resolving odqvsli.biz
10:48:45  dga      Resolving jqvmrbk.com
10:48:46  dga      Resolving jqvmrbk.space
10:48:47  dga      Resolving jqvmrbk.biz
10:48:48  dga      Resolving zkwunit.com
10:48:49  dga      Resolving zkwunit.space
10:48:50  dga      Resolving zkwunit.biz
10:48:51  dga      Resolving yaecxgm.com
10:48:52  dga      Resolving yaecxgm.space
10:48:53  dga      Resolving yaecxgm.biz
10:48:54  dga      Finished

All done! Check your SIEM for alerts using the timestamps and details above.
```

Running FlightSim

- Generates DNS tunneling requests to *.sandbox.alphasoc.xyz



```
root@kali2017:~# flightsim run tunnel

AlphaSOC Network Flight Simulator™ v0.0.0 (https://github.com/alphasoc/flightsim)
The IP address of the network interface is 192.168.10.12
The current time is 15-Feb-18 11:17:28

Time      Module   Description
--------------------------------------------------------------------------------
11:17:28  tunnel   Starting
11:17:28  tunnel   Preparing DNS tunnel hostnames
11:17:28  tunnel   Resolving vxsyrxazzlkgchqcvmufjkwiabjgdf.sandbox.alphasoc.xyz
11:17:29  tunnel   Resolving wlyzadcioakwthlxoqwygjhzixdsfb.sandbox.alphasoc.xyz
11:17:30  tunnel   Resolving plxirobdstrtxurxsoghrdbhetzcym.sandbox.alphasoc.xyz
11:17:31  tunnel   Resolving wpjotcwgxtjjoonnpqthjncqtkwtgq.sandbox.alphasoc.xyz
11:17:32  tunnel   Resolving zwawlyviksyfybmpmonrafykmayblc.sandbox.alphasoc.xyz
11:17:33  tunnel   Resolving vsjvghgfmzgmkclyjklryshsebqwuv.sandbox.alphasoc.xyz
11:17:34  tunnel   Resolving cjkwxhllqpffztiptnyjevpvskqbln.sandbox.alphasoc.xyz
11:17:35  tunnel   Resolving iakuaarvxwpvboqaspwfcikiwupdvs.sandbox.alphasoc.xyz
11:17:36  tunnel   Resolving jzzrctozgqiixgunxycropkgjbfoyi.sandbox.alphasoc.xyz
11:17:37  tunnel   Resolving zgoznierggpgelgjpkvchaiblsgnho.sandbox.alphasoc.xyz
11:17:38  tunnel   Resolving rjiumhkeqvajmvjwitdeumdzjohgpu.sandbox.alphasoc.xyz
11:17:39  tunnel   Resolving ntoonncxiclogicmgggtnvwzxvkmmp.sandbox.alphasoc.xyz
11:17:40  tunnel   Resolving fwjtgyystwvvygtcoehauiuqshkhti.sandbox.alphasoc.xyz
11:17:41  tunnel   Resolving awsszvdzulmtzktmhtwzkfxwwntvcq.sandbox.alphasoc.xyz
11:17:42  tunnel   Resolving ktirskkzdyiaxlgnxlziefmvcbwpgq.sandbox.alphasoc.xyz
11:17:43  tunnel   Resolving ejmhxwfmiqagksytyvvddxqqmbqkei.sandbox.alphasoc.xyz
11:17:44  tunnel   Resolving cowmyoumkjlywjphwwsxidarngojpa.sandbox.alphasoc.xyz
11:17:45  tunnel   Resolving rafrfnkgqpaxslhcoaqsqdezcfycyk.sandbox.alphasoc.xyz
11:17:46  tunnel   Resolving dwmkhxelhtomzwmvqgaorhwksyqxsf.sandbox.alphasoc.xyz
11:17:47  tunnel   Resolving ecdqfhbxdemlgwtpgvpmtjlhwdjxsw.sandbox.alphasoc.xyz
11:17:48  tunnel   Resolving pdnqucyxytspqiwvwhsokmctxvugqj.sandbox.alphasoc.xyz
11:17:49  tunnel   Resolving tlailsvskndjeriytzuugfstifddhf.sandbox.alphasoc.xyz
11:17:50  tunnel   Resolving rbxrzktylitykodnebfutovzypcjwd.sandbox.alphasoc.xyz
11:17:51  tunnel   Resolving xfreiuybtktzwsijepgyyptzymuwbq.sandbox.alphasoc.xyz
11:17:52  tunnel   Resolving zrxoxauqvzmdqucdpxhidtdzesvlef.sandbox.alphasoc.xyz
11:17:53  tunnel   Resolving akkrekdvzdhkkgaubtixgrrlxebvrm.sandbox.alphasoc.xyz
11:17:54  tunnel   Resolving mtppkroxfxrppwvsvhxvjexilbicsl.sandbox.alphasoc.xyz
11:17:55  tunnel   Resolving nqyzhrrkwculfzsxaatyjslqpqrdjw.sandbox.alphasoc.xyz
11:17:56  tunnel   Resolving zgqupcgbdgvoyuhidhkftqicnlbphy.sandbox.alphasoc.xyz
11:17:57  tunnel   Resolving dxhhmvsnamjvowpkyyujlcbishztdz.sandbox.alphasoc.xyz
11:17:58  tunnel   Finished

All done! Check your SIEM for alerts using the timestamps and details above.
```

References

- FlightSim GitHub
https://github.com/alphasoc/flightsim