HALCYON

UNOFFICIAL IDE FOR NMAP SCRIPT DEVELOPMENT

Sanoop Thomas | Twitter : @s4n7h0

A BIT INTRO

1. Challanges in developing Nmap Scripts
2. Extensive use of Nmap in Enterprise VA
3. Built in JAVA
4. **Open Source** (feel free to contribute)

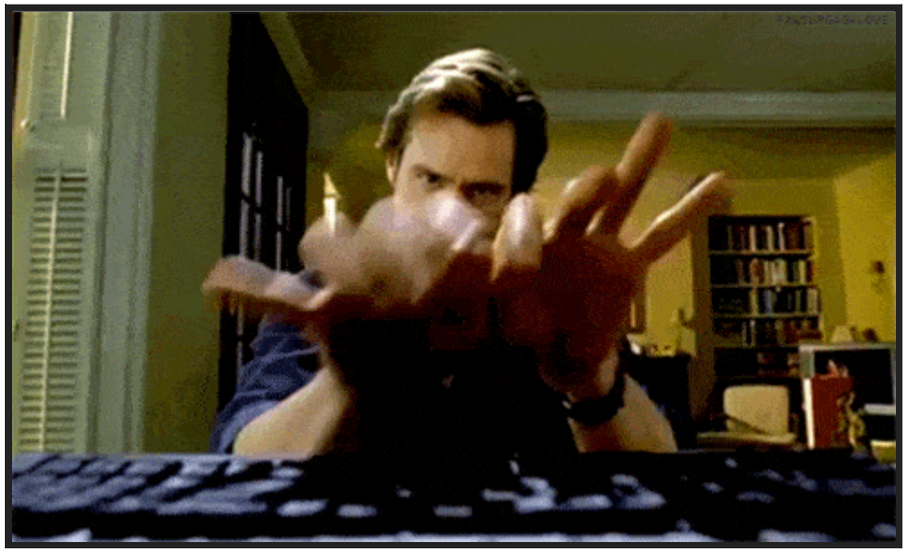
PROJECT PAGE

- Project Page : http://halcyon-ide.org/
- GitHub: https://github.com/s4n7h0/Halcyon

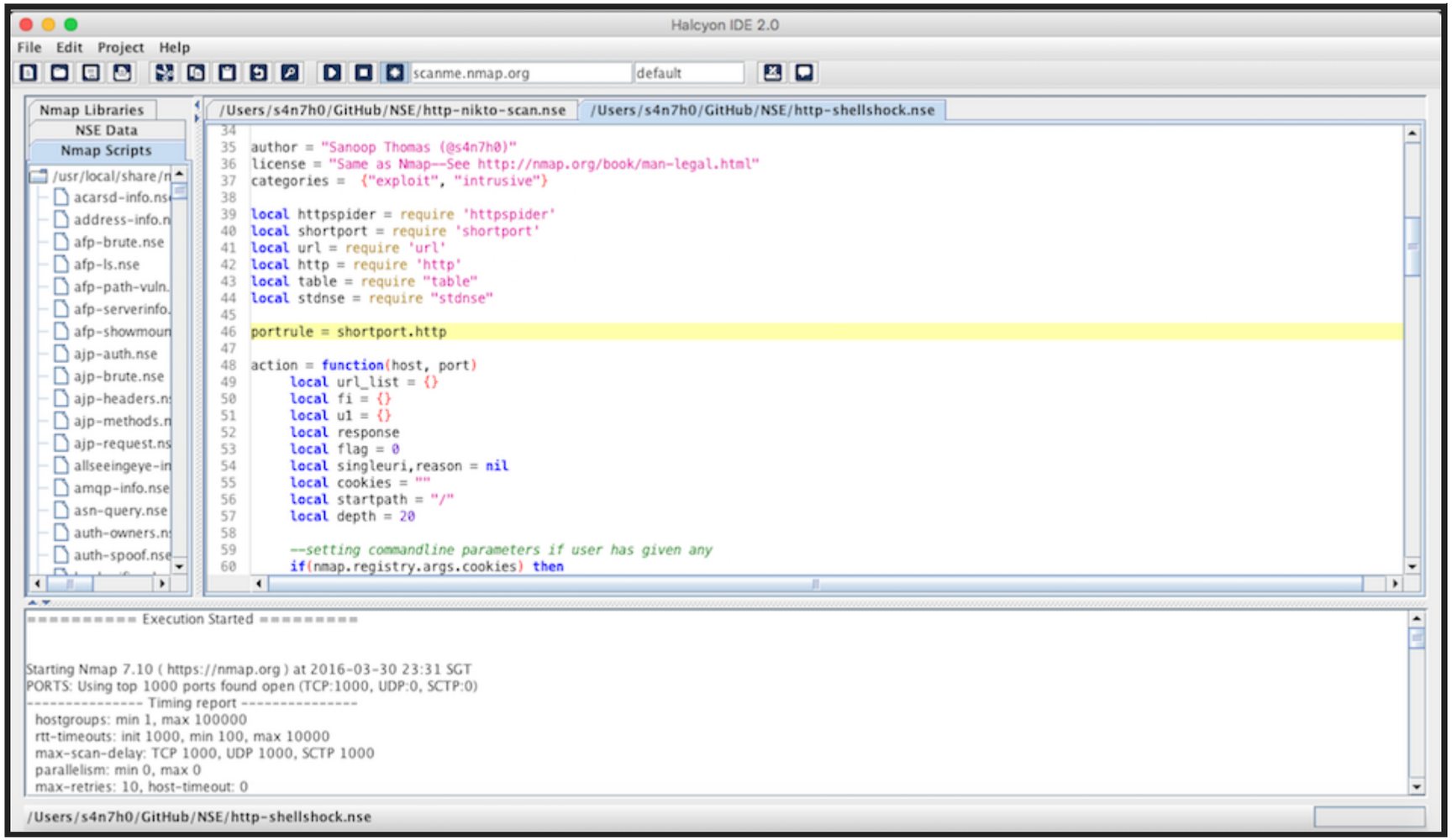
WHY HALCYON?

1. Code Intelligence & Autocompletion (just like other IDEs)
2. One Click Configuration
3. Scan Settings
4. Prewritten Code Generator Modules
5. Debugg within Halcyon IDE

SOURCE OF INSPIRATION



DEMO


Halcyon IDE 2.0
File Edit Project Help
scanme.nmap.org
default
Nmap Libraries
NSE Data
Nmap Scripts
/usr/local/share/n
acarsd-info.ns
address-info.n
afp-brute.nse
afp-ls.nse
afp-path-vuln.
afp-serverinfo.
afp-showmoun
ajp-auth.nse
ajp-brute.nse
ajp-headers.n
ajp-methods.n
ajp-request.ns
allseeingeye-in
amqp-info.nse
asn-query.nse
auth-owners.n
auth-spoof.nse
/Users/s4n7h0/GitHub/NSE/http-nikto-scan.nse
/Users/s4n7h0/GitHub/NSE/http-shellshock.nse
34
35 author = "Sanoop Thomas (@s4n7h0)"
36 license = "Same as Nmap--See http://nmap.org/book/man-legal.html"
37 categories = {"exploit", "intrusive"}
38
39 local httpspider = require 'httpspider'
40 local shortport = require 'shortport'
41 local url = require 'url'
42 local http = require 'http'
43 local table = require "table"
44 local stdnse = require "stdnse"
45
46 portrule = shortport.http
47
48 action = function(host, port)
49 local url_list = {}
50 local fi = {}
51 local u1 = {}
52 local response
53 local flag = 0
54 local singleuri,reason = nil
55 local cookies = ""
56 local startpath = "/"
57 local depth = 20
58
59 --setting commandline parameters if user has given any
60 if(nmap.registry.args.cookies) then
========== Execution Started ==========
Starting Nmap 7.10 (https://nmap.org) at 2016-03-30 23:31 SGT
PORTS: Using top 1000 ports found open (TCP:1000, UDP:0, SCTP:0)
---------- Timing report ----------
hostgroups: min 1, max 100000
rtt-timeouts: init 1000, min 100, max 10000
max-scan-delay: TCP 1000, UDP 1000, SCTP 1000
parallelism: min 0, max 0
max-retries: 10, host-timeout: 0
/Users/s4n7h0/GitHub/NSE/http-shellshock.nse

FUTURE WORKS

- An offline wiki for nmap libraries
- Custom module writing option for code generator
- Share your ideas to improve

ANY QUESTIONS

Sanoop Thomas | Twitter : @s4n7h0