HALCYON IDE

First IDE for Nmap Script (NSE) Development

http://halcyon-ide.org/

#whoami

- **Sanoop Thomas**
  - Security Consultant at SEC Consult
  - One of core team moderator at Null Singapore chapter
  - Over 7 years in Information Security
  - Before that I used to often type {curly braces} and ;semicolons;.
  - Tweet Tweet @s4n7h0

How did it all start ?

- Repeated NSE development for internal pentesting
- Need of a developing environment
- Lot of things can be automated
- One of my coffee shop project
- Named it hal·cy·on, pronounced as ˈhalsēən/

- http://halcyon-ide.org/

What

- First IDE specifically focused on NSE development
- Java based development
- Understands NMAP and LUA
- Easy NSE scripting environment

Why do we need NSE ?

- Nmap capabilities
- Faster scan signature release
- Unusual device or version detection

NSE Trivia

```
portrule = function(host, port)
     return port.protocol == "tcp" and
     port.number == 80 and
     port.state == "open"
end

action = function(host, port)
     return "Hello world!"
end
```

Project Page

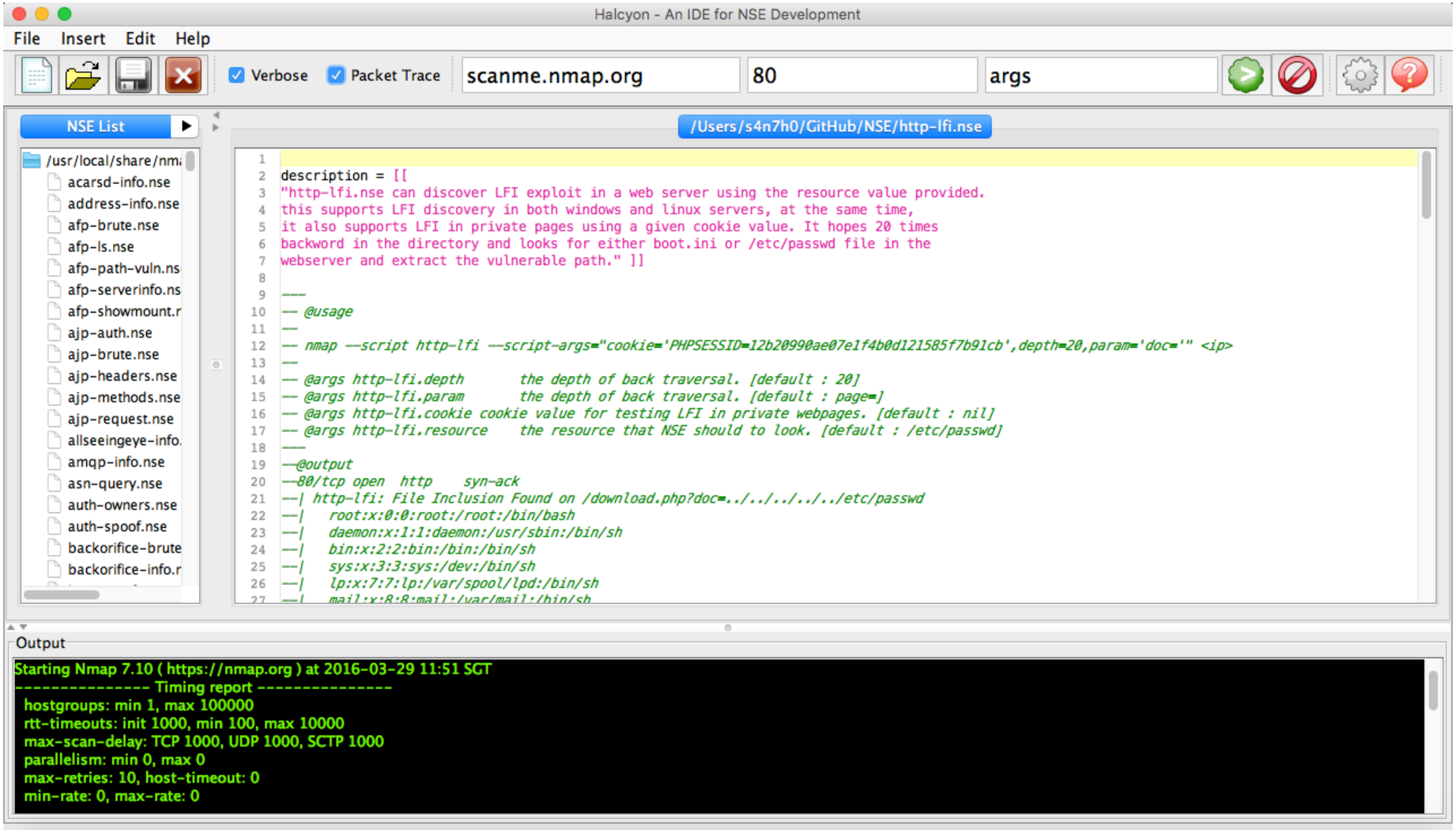
- Official Page
  - `http://halcyon-ide.org/`

- Current release 2.0 is available on the website.
- Version 2.1 will be released after ROOTCON X

Current Features

- Like other traditional IDEs
  - Syntax highlighting
  - Auto completing
- Easy configuration
  - Automated settings
  - Single click config
  - Manual configuration available
- Code generator
- Run/debug/fix within the IDE
- Pre/post development actions
- Build-in Decoder
- Scan-Diff

In the initial days



☑ Verbose ☑ Packet Trace

scanme.nmap.org

80

args

/Users/s4n7h0/GitHub/NSE/http-lfi.nse

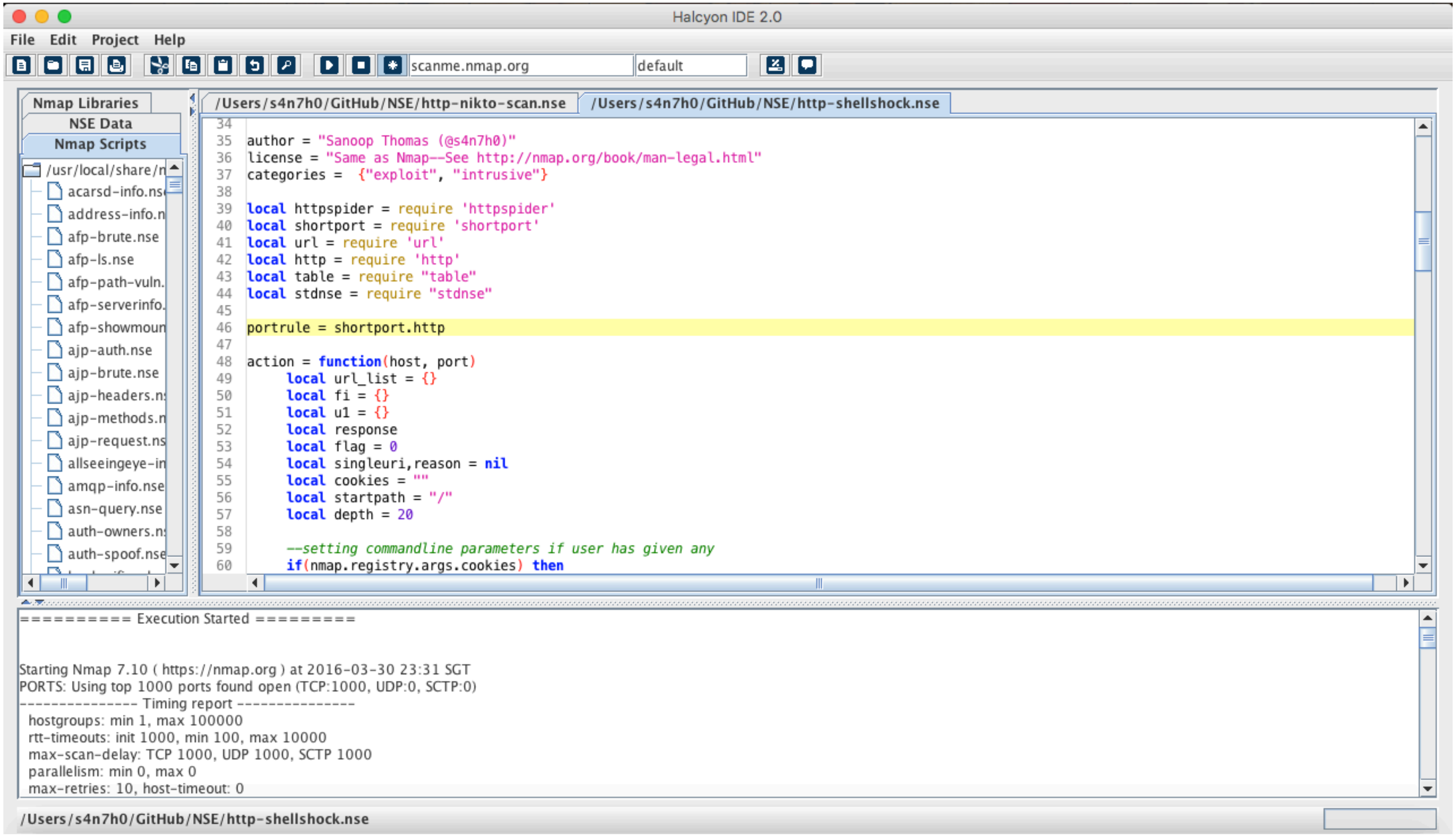
```

description = [[
"http-lfi.nse can discover LFI exploit in a web server using the resource value provided.
this supports LFI discovery in both windows and linux servers, at the same time,
it also supports LFI in private pages using a given cookie value. It hopes 20 times
backword in the directory and looks for either boot.ini or /etc/passwd file in the
webserver and extract the vulnerable path." ]]

---
-- @usage
--
-- nmap --script http-lfi --script-args="cookie='PHPSESSID=12b20990ae07e1f4b0d121585f7b91cb',depth=20,param='doc='" <ip>
--
-- @args http-lfi.depth       the depth of back traversal. [default : 20]
-- @args http-lfi.param       the depth of back traversal. [default : page=]
-- @args http-lfi.cookie cookie value for testing LFI in private webpages. [default : nil]
-- @args http-lfi.resource    the resource that NSE should to look. [default : /etc/passwd]
---
--@output
--80/tcp open  http    syn-ack
--| http-lfi: File Inclusion Found on /download.php?doc=../../../../../etc/passwd
--|   root:x:0:0:root:/root:/bin/bash
--|   daemon:x:1:1:daemon:/usr/sbin:/bin/sh
--|   bin:x:2:2:bin:/bin:/bin/sh
--|   sys:x:3:3:sys:/dev:/bin/sh
--|   lp:x:7:7:lp:/var/spool/lpd:/bin/sh
--|   mail:x:8:8:mail:/var/mail:/bin/sh
```

```
Starting Nmap 7.10 ( https://nmap.org ) at 2016-03-29 11:51 SGT
--------------- 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
  min-rate: 0, max-rate: 0
```

And now



```
author = "Sanoop Thomas (@s4n7h0)"
license = "Same as Nmap--See http://nmap.org/book/man-legal.html"
categories =  {"exploit", "intrusive"}

local httpspider = require 'httpspider'
local shortport = require 'shortport'
local url = require 'url'
local http = require 'http'
local table = require "table"
local stdnse = require "stdnse"

portrule = shortport.http

action = function(host, port)
     local url_list = {}
     local fi = {}
     local u1 = {}
     local response
     local flag = 0
     local singleuri,reason = nil
     local cookies = ""
     local startpath = "/"
     local depth = 20

     --setting commandline parameters if user has given any
     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
```

Future works

- Report Explorer and Parsers
- NSE help wizard to lean NSE scripting

- You got more ideas, send to me

Thanks

- To all NSE developers
- Thanks to all baristas who served me tantalizing aroma of strong coffee throughout this work ☺

www.halcyon-ide.org
Twitter: @s4n7h0
i.am.s4n7h0@gmail.com