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
halcyon

ˈhælsɪən,-ʃ(ə)n/

adjective

1. denoting a period of time in the past that was idyllcally happy and peaceful.
   "the halcyon days of the mid 1980s, when profits were soaring"
   synonyms: serene, calm, pleasant, balmy, tranquil, peaceful, temperate, mild, quiet, gentle,
   placid, still, windless, stormless  More

noun

1. a mythical bird said by ancient writers to breed in a nest floating at sea at the winter solstice,
   charming the wind and waves into calm.

2. a tropical Asian and African kingfisher with brightly coloured plumage.
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

http://halcyon-ide.org/
What

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

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

• Github
  • https://github.com/s4n7h0/Halcyon
Current Features

• Code intelligence
  • 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
Halcyon IDE in Action

```python
author = "Sandeep Thomas (@s4n7h0)"
license = "Same as Nmap—See http://nmap.org/book/nmap-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 u1 = {}
  local response
  local flag = 0
  local singleurl,reason = nil
  local cookies = ""
  local startpath = "/"
  local depth = 20

  --setting commandline parameters if user has given any
  if (nmap.registry.orgs.cookies) then
```

Starting Nmap 7.10 ( https://nmap.org ) at 2016-03-30 23:31 SCT
PORTS: Using 1000 ports found open (TCP:1000, UDP:0, SCTP:0)
--------- Timing report ----------
hostgroups: min 1, max 100000
rtt-timesout: min 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/ikuieh/NSE/http-shellshock.nse
```
Future works

• Smart help wizard
  • Not just an IDE to code, but to learn as well

• Send me your suggestions
Questions & Feedbacks

- www.halcyon-ide.org
- i.am.s4n7h0@gmail.com
- https://twitter.com/s4n7h0
- https://www.facebook.com/HalcyonIDE/
- https://github.com/s4n7h0/Halcyon