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 'halsēən/

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
And now
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