

Halcyon IDE

IDE for Nmap Script Developers

Introduction

Halcyon IDE is a development environment for Nmap Script developers, pretty much the **first IDE exclusively for NSE** development. Written in java to allow a “pull and run” easiness on different operating systems without much hustle.

```
2.0.1
Help
192.168.67.155 default
Data Nmap Libraries
C:\Users\s4n7h0\Documents\GitHub\NSE\MS15-034.nse
3 local http = require "http"
4 local shortport = require "shortport"
5
6 description = [[
7 HTTP.sys Denial of Service (BSoD). This script will check if scanned hosts are vulnerable to
8 This script will not cause BSoD. If the hosts are found to be vulnerable, sending request w
9
10 https://technet.microsoft.com/en-us/library/security/ms15-034.aspx
11 ]]
12
13 ---
14 -- @usage
15 --
16 -- nmap --script MS15-034 --script-args="MS15-034.uri=/iisstart.htm" <ip>
17 --
18 -- @args MS15-034.uri [default : /iisstart.htm]
19 --
20 --
21 --@output
22 --80/tcp open http syn-ack
23 --|_MS15-034: host is vulnerable to MS15-034
24 ---
25
26 author = "Sanoop Thomas"
27 license = "Same as Nmap--See https://nmap.org/book/man-legal.html"
28 categories = {"vuln", "safe"}
29
30 portrule = shortport.http
31
```

```
arp[18:4] = 0x005056C0 and arp[22:2] = 0x0008
s elapsed (1 total hosts)
0.66 bytes / s.
3.1.1
3.51.98
73.51.99
/ 1 host at 03:09
.0, NX: 0, DR: 0, SF: 0, TR: 6]
ation of 1 host at 03:09, 16.50s elapsed
19.63s. Mode: Async [#: 3, OK: 0, NX: 0, DR: 1, SF: 0, TR: 6, CN: 0]
at 03:09
[1000 ports]
ervice eth6): dst host 192.168.67.1 and (icmp or icmp6 or ((tcp or udp or sctp) and (src host 192.168.67.155)))
t 5900/tcp on 192.168.67.155
port 139/tcp on 192.168.67.155
```

Features

- Code-aware interface
- Interact with Nmap library, scripts and data files.
- Configurable settings for multiple scans
- Debug within the IDE by using Nmap settings
- Post development features.

- C:\Program Files (x86)\Nmap\scripts
 - acarsd-info.nse
 - address-info.nse
 - afp-brute.nse
 - afp-ls.nse
 - afp-path-vuln.nse
 - afp-serverinfo.nse
 - afp-showmount.nse
 - ajp-auth.nse
 - ajp-brute.nse
 - ajp-headers.nse
 - ajp-methods.nse
 - ajp-request.nse
 - allseeingeye-info.nse
 - amqp-info.nse
 - asn-query.nse
 - auth-owners.nse
 - auth-spoof.nse
 - backoffice-brute.nse
 - backoffice-info.nse
 - bacnet-info.nse
 - banner.nse
 - bitcoin-getaddr.nse
 - bitcoin-info.nse
 - bitcoirpc-info.nse
 - bittorrent-discovery.nse
 - bin-discover.nse

```
57     end
58     return Table
59 end
60
61 function craft_uri(startpos,endpos, str, r)
62     if(endpos == nil) then return string.sub(tostring(str),1,startpos) .. r
63     else return string.sub(tostring(str),1, startpos) .. r .. string.sub(tostring(str),endpos) end
64 end
65
66 action = function(host, port)
67     local parsed = ""
68     local url_split = {}
69     local url_list = {}
70     local fi = {}
71     local param="page="
72     local response,pattern,res
73     local WIN_PATTERN = "[boot loader]"
74     local NIX_PATTERN = "root:x:"
75     local flag = 0
76     local jump= "../"
77     local cookie = nil
78     local resource = "etc/passwd"
79     local depth = 20
80
81     --crawler to check all possible urls
82     local crawler = httpspider.Crawler:new(host, port, '/', { scriptname = SCRIPT_NAME })
83     crawler:set_timeout(10000)
84
85     --setting cookie for checking private pages
```

```
NSE: Loaded 1 scripts for scanning.
NSE: Script Pre-scanning.
NSE: Starting runlevel 1 (of 1) scan.
Initiating NSE at 03:09
Completed NSE at 03:09, 0.00s elapsed
Initiating ARP Ping Scan at 03:09
Scanning 192.168.67.155 [1 port]
Packet capture filter (device eth6): arp and arp[18:4] = 0x005056C0 and arp[22:2] = 0x0008
Completed ARP Ping Scan at 03:09, 0.83s elapsed (1 total hosts)
Overall sending rates: 1.21 packets / s, 50.66 bytes / s.
mass_rdns: Using DNS server 192.168.1.1
mass_rdns: Using DNS server 202.73.51.98
mass_rdns: Using DNS server 202.73.51.99
Initiating Parallel DNS resolution of 1 host. at 03:09
mass_rdns: 19.63s 0/1 [#: 3, OK: 0, NX: 0, DR: 0, SF: 0, TR: 6]
Completed Parallel DNS resolution of 1 host. at 03:09, 16.50s elapsed
DNS resolution of 1 IPs took 19.63s. Mode: Async [#: 3, OK: 0, NX: 0, DR: 1, SF: 0, TR: 6, CN: 0]
Initiating SYN Stealth Scan at 03:09
Scanning 192.168.67.155 [1000 ports]
Packet capture filter (device eth6): dst host 192.168.67.1 and (icmp or icmp6 or ((tcp or udp or sctp) and (src host 192.168.67.155)))
Discovered open port 5900/tcp on 192.168.67.155
Discovered open port 139/tcp on 192.168.67.155
```

Scan Settings

- Pluggable to multiple scans

The screenshot shows a dialog box titled "Scan Settings" with a standard Windows-style title bar (minimize, maximize, close buttons). The dialog is divided into three main sections:

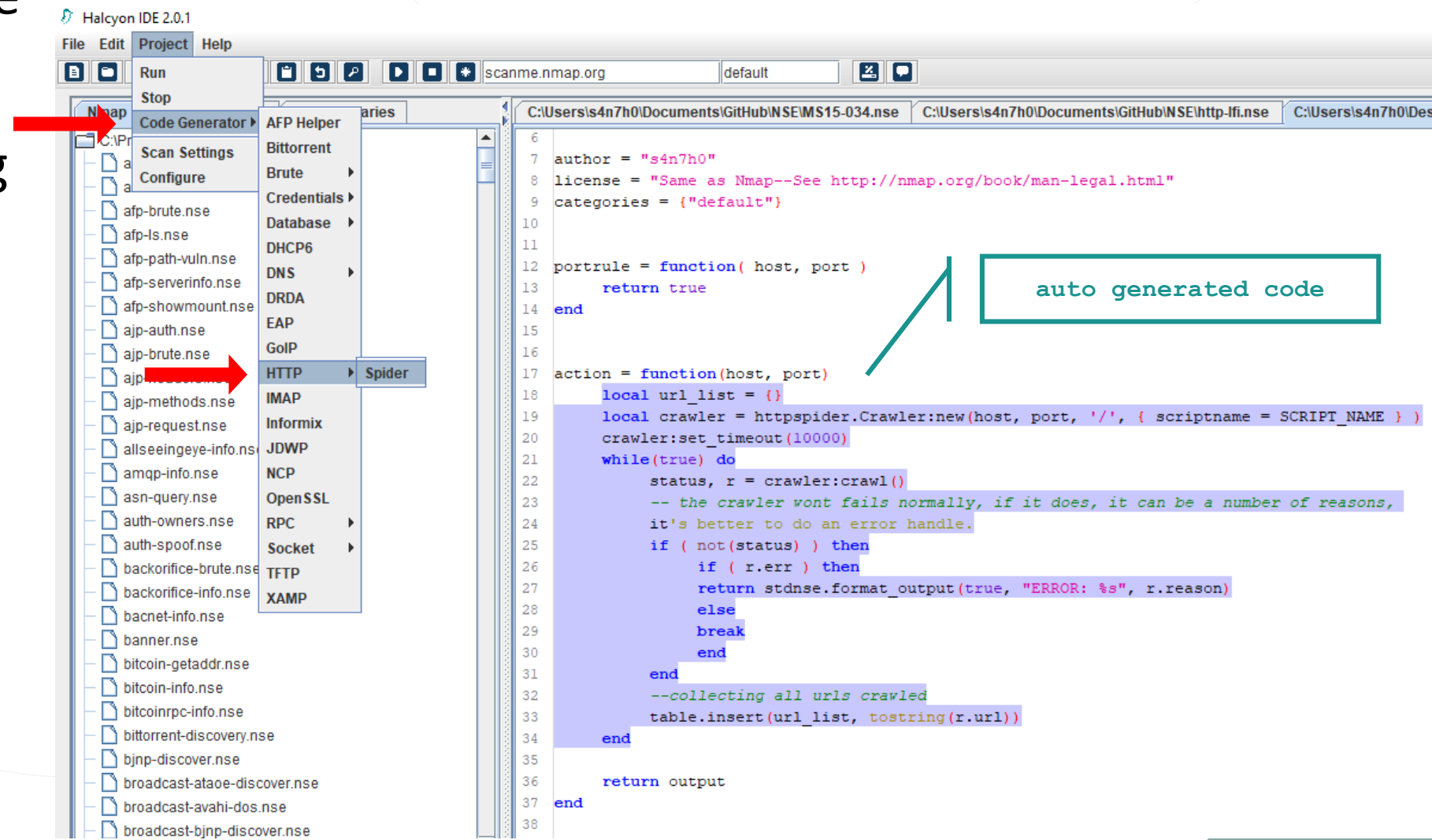
- Scan Type:** Contains two radio buttons. "TCP Scan" is selected (indicated by a filled circle), and "UDP Scan" is unselected (indicated by an empty circle).
- Script Arguments:** Contains two checkboxes and two text input fields.
 - The first checkbox is "Choose this option to select script arguments as command line option (--script-args)". It is unselected. Below it is an empty text input field.
 - The second checkbox is "Choose this option to upload file as script arguments (--script-args-file)". It is unselected. Below it is an empty text input field followed by a small button with three dots "...".
- Debugging Options:** Contains three checkboxes.
 - "Packet Trace" is unselected.
 - "Verbose Mode" is unselected.
 - "Debug" is selected (indicated by a checked box).

At the bottom right of the dialog, there are two buttons: "Apply" and "Cancel".

Code window features

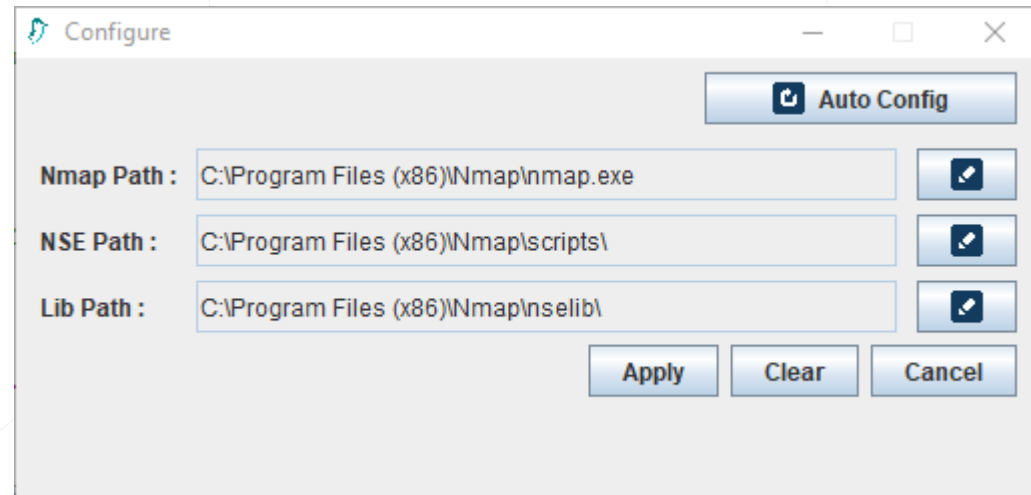
- Autocomplete
- Syntax-aware
- Code building

halcyon-ide.org



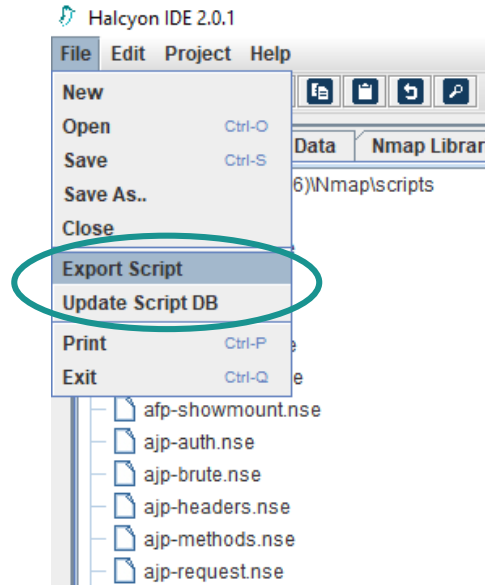
Configuration

- Nmap configuration
 - Auto config options
 - Manual settings



Post Development Actions

- Export script
- Update script-db



```
Exporting C:\Users\ls4n7h0\Documents\GitHub\NSE\MS15-034.nse to Nmap Script path C:\Program Files (x86)\Nmap\scripts\MS15-034.nse

===== Updating Script DB =====

Starting Nmap 7.60 ( https://nmap.org ) at 2018-08-06 19:06 Pacific Summer Time
NSE: Updating rule database.
NSE: Script Database updated successfully.
Nmap done: 0 IP addresses (0 hosts up) scanned in 1.01 seconds
===== Script DB Updated =====
```




CONTRIBUTE

- Contribute your code
- Share feedback or user experience
- Test the project and report bugs if you found any
- Suggest features to improve
- Write or talk about the project



THANK YOU

halcyon-ide.org

<https://github.com/s4n7h0/Halcyon>



SANOOP THOMAS



@s4n7h0