Scripting and Extending Nmap and Wireshark with Lua

by Gerald Combs & Gordon “Fyodor” Lyon

Sharkfest 2010 – June 16, 1:15 PM
http://insecure.org/presentations/Sharkfest10/

Nmap Security Scanner

Nmap – a cross-platform, open source tool for network exploration or security auditing. Many systems and network administrators also find it useful for tasks such as network inventory and monitoring host or service uptime. Nmap uses raw IP packets in novel ways to determine what hosts are available on the network, what services (application name and version) those hosts are offering, what operating systems they are running, and more.

Nmap <3 Wireshark

Presentation Overview

- Intro to Lua (15 minutes)
- Lua in Nmap (30 minutes)
- Lua in Wireshark (30 minutes)
- Questions

Introduction to Lua

- Lightweight embeddable scripting language
- Created in Brazil in 1993, still actively developed.
- Best known for its use in the game industry: World of Warcraft, Crysis, etc.
- Security tools: Nmap, Wireshark, Snort IDS
- Simple

Why Lua?

- Tiny - “Complete distribution (source code, manual, plus binaries for some platforms) fits comfortably on a floppy disk”.
- Widely used, known, and debugged.
- Extensible
- Safe and Secure
- Portable
- Interpreted

More on Lua

- http://lua.org
- Programming in Lua - 2nd Edition

Questions about Lua?

Lua in Action – Nmap Scripting Engine http://nmap.org/nsedoc/

```
# nmap -T4 -A scanme.nmap.org
Starting Nmap 5.30BETA1 ( http://nmap.org )
Nmap scan report for scanme.nmap.org (64.13.134.52)
Host is up (0.022s latency).
Not shown: 995 filtered ports
PORT      STATE  SERVICE VERSION
22/tcp    open   ssh     OpenSSH 4.3 (protocol 2.0)
| ssh-hostkey: 1024
60:ac:4d:51:b1:cd:85:09:12:16:92:76:1d:5d:27:6e (DSA)
|_2048 2c:22:75:60:4b:c3:3b:18:a2:97:2c:96:7e:28:dc:dd (RSA)
53/tcp    open   domain
80/tcp    open   http    Apache httpd 2.2.3 ((CentOS))
|_html-title: Go ahead and ScanMe!
| http-methods: Potentially risky methods: TRACE
|_See http://nmap.org/nsedoc/scripts/http-methods.html
113/tcp   closed auth
31337/tcp closed Elite
OS details: Linux 2.6.18 (CentOS 5.4)
Nmap done: 1 IP address (1 host up) scanned in 25.76 seconds
```

NSE Demonstration

- nmap -v -sV -F -O -T4 wireshark.org
- nmap -v -sV -F -O -T4 –script=safe wireshark.org

NSE Script Source

- A closer look at some scripts
  - daytime.nse
  - http-date.nse

An Unusual Example

- http-california-plates.nse

Lua In Action – Large Scale Scanning

SMB/MSRPC Scripts

Ron Bowes spent months researching SMB/MSRPC protocols and wrote a suite of 13 scripts.

Informational: smb-os-discovery, smb-server-stats, smb-system-info, smb-security-mode

Detailed Enumeration: smb-enum-users, smb-enum-domains, smb-enum-groups, smb-enum-processes, smb-enum-sessions, smb-enum-shares

More intrusive: smb-brute, smb-check-vulns, smb-pwdump

Who to test them out on?

Microsoft

Large Scale Scanning - Favicon.nse

- Initial Submission
- Improving the DB
- Going overboard

Questions and Resources

Download Nmap from http://nmap.org

Learn about NSE: http://nmap.org/nsedoc/

Slides are posted at: http://insecure.org/presentations/Sharkfest10/