Mastering the Nmap Scripting Engine
by Fyodor and David Fifield

http://insecure.org/presentations/BHDC10/

Black Hat Briefings Las Vegas
July 28; 4:45 PM; Augustus 5+6

Defcon 18
July 30; 5:00 PM; Track One
Outline

• NSE Intro & Usage
• Large-scale Scan: SMB/MSRPC
• Writing NSE Scripts
• Live Script Writing Demo
• Final Notes & Q/A
Nmap Scripting Engine

```
# nmap -A -T4 scanme.nmap.org

Starting Nmap 5.35DC18 ( http://nmap.org )
Nmap scan report for scanme.nmap.org (64.13.134.52)
Host is up (0.0018s latency).
Not shown: 995 filtered ports
PORT      STATE  SERVICE VERSION
22/tcp    open   ssh     OpenSSH 4.3 (protocol 2.0)
| ssh-hostkey: 1024
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 2.6.13 - 2.6.31, Linux 2.6.18
Nmap done: 1 IP address (1 host up) scanned in 23.32 seconds
```
Pre-written Scripts and the NSEDoc Portal
http://nmap.org/nsedoc/

<table>
<thead>
<tr>
<th>Scripts</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>afp-brute</td>
<td>Performs password guessing against Apple Filing Protocol (AFP)</td>
</tr>
<tr>
<td>afp-path-vuln</td>
<td>Detects the Mac OS X AFP directory traversal vulnerability, CVE-2010-0533.</td>
</tr>
<tr>
<td>afp-serverinfo</td>
<td>Shows AFP server information. This information includes the server's hostname, IPv4 and IPv6 addresses, and hardware type (for example Macmini or MacBookPro).</td>
</tr>
<tr>
<td>afp-showmount</td>
<td>Shows AFP shares and ACLs.</td>
</tr>
<tr>
<td>asn-query</td>
<td>Maps IP addresses to autonomous system (AS) numbers.</td>
</tr>
</tbody>
</table>
Script Collection Growth

Yearly Collection Growth:
- 2007-1: 20
- 2007-2: 40
- 2008-1: 60
- 2008-2: 80
- 2009-1: 100
- 2009-2: 120
- 2010-1: 140
- 2010-2: 160
Large Scale Scan #1: 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-pseexec
Who to test them out on?
MS Scan Details

- Step 1: Find target IP addresses. 1,004,632 located in ARIN DB.
- Step 2: Start broad version detection scan
  (nmap -T4 --top-ports 50 -sV -O --osscan-limit --osscan-guess --min-hostgroup 128 --host-timeout 10m -oA ms-vscan -iL ms.ips.lst)
  - Found 74,293 hosts up out of 1M IPs in 26 hours
- Step 3: Examine results
MS SMB Scan Results

• Vast majority of MS networks block Windows ports such as 135 and 445 at their gateways.
• ... but not all!
• Results
Writing NSE Scripts
Introduction to Lua & Why We Chose It

• Lightweight embeddable scripting language
  – Easy to learn
  – Tiny to embed: “Complete distribution (source code, manual, plus binaries for some platforms) fits comfortably on a floppy disk”.

• Widely used, known, and debugged
  – 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 3.0
Why We Chose Lua (Continued)

• **Extensible**
  – Hooked to Nmap's fast parallel networking libraries

• **Safe & Secure**
  – No buffer overflows, format string vulns, etc.

• **Portable**
  – Windows, Linux, Mac, *BSD, etc.

• **Interpreted**
Capabilities Added by Nmap

- Protocol/helper libraries
  - 45, including DNS, HTTP, MSRPC, Packet, SNMP, unpwdb, etc.
- Protocol brute forcers
- Easy SSL
- Dependencies
Script Example: rpcinfo.nse
Live Script Demonstration

Problem: Find my webcam on a dynamic IP address.

The webcam uses thttpd to serve /cam.jpg, so use a script to check those two things.
Make it a Production Script

To turn http-brute into distribution-ready script, I would next:

- expand the portrule to match more HTTP services,
- add script arguments to control the path retrieved and the method used,
- add NSEDoc @usage and @output examples, and
- let it cache credentials for other scripts to use.
What's Coming in NSE?

- Prerules & Postrules
- Target Acquisition Scripts
- Lots more scripts! Current queue:
  - Vnc-info (Patrik Karlsson)
  - Vnc-brute (Patrik Karlsson)
  - Svn-brute (Patrik Karlsson)
  - Hostmap (Ange Gutek)
  - Http-xst (Eduardo Garcia Melia)
  - Rmi-dumpregistry (Martin Swende)
Zenmap NSE Integration

Profile Editor

Profile Editor with selected script "nfs-ls".
Categories: discovery, safe

Attempts to get useful information about files from NFS exports.
The output is intended to resemble the output of "<code>ls</code>".
The script starts by enumerating and mounting.

Arguments

<table>
<thead>
<tr>
<th>Arguments</th>
<th>values</th>
</tr>
</thead>
<tbody>
<tr>
<td>nfs-ls.maxfiles</td>
<td>10</td>
</tr>
<tr>
<td>nfs-ls.human</td>
<td></td>
</tr>
<tr>
<td>nfs-ls.time</td>
<td></td>
</tr>
<tr>
<td>nfs.version</td>
<td></td>
</tr>
<tr>
<td>mount.version</td>
<td></td>
</tr>
<tr>
<td>ncp.protocol</td>
<td></td>
</tr>
</tbody>
</table>

Help

List of scripts
A list of all installed scripts. Activate or deactivate a script by clicking the box next to the script name.
Nmap Script Authors

Aaron Leininger
Andrew Orr
Ange Gutek
Arturo Busleiman
Bernd Stroessenreuther
Brandon Enright
David Fifield
Diman Todorov
Djalal Harouni
Doug Hoyte
Duarte Silva
Eddie Bell

Eugene V. Alexeev
Felix Groeber
Ferdy Riphagen
Jah
Jason DePriest
Joao Correa
Kris Katterjohn
Mak Kolybabi
Marek Majkowski
Martin Swende
Matthew Boyle
Michael Pattrick

Michael Schierl
Patrik Karlsson
Philip Pickering
Richard Sammet
Rob Nicholls
Ron Bowes
Sven Klemm
Thomas Buchanan
Tom Sellers
Vladz
Vlatko Kosturjak
Final Notes

• Slides: http://insecure.org/presentations/
• Download Nmap from: http://nmap.org
• NSEDoc portal: http://nmap.org/nsedoc/
• NSE system docs: http://nmap.org/book/nse.html
• Q&A in Track #1 Q&A Room