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

Abstract

Most hackers can use Nmap for simple port scanning and OS detection, but the Nmap Scripting Engine (NSE) takes scanning to a whole new level. Nmap's high-speed networking engine can now spider web sites for SQL injection vulnerabilities, brute-force crack and query MSRPC services, find open proxies, and more. Nmap includes more than 125 NSE scripts for network discovery, vulnerability detection, exploitation, and authentication cracking.

Rather than give a dry overview of NSE, Fyodor and Nmap co-maintainer David Fifield demonstrate practical solutions to common problems. They have scanned millions of hosts with NSE and will discuss vulnerabilities found on enterprise networks and how Nmap can be used to quickly detect those problems on your own systems. Then they demonstrate how easy it is to write custom NSE scripts to meet the needs of your network. Finally they take a quick look at recent Nmap developments and provide a preview of what is soon to come. This presentation does not require any NSE experience, but it wouldn't hurt to read http://nmap.org/book/nse.html.

Resources

These slides are just a teaser. Final slides will be posted by August 1, 2010 to http://insecure.org/presentations/BHDC10/.

Our goal is to make this presentation useful, informative, and entertaining even to those who know very little about Nmap and the Nmap Scripting Engine. But you can get the most out of this presentation by first reading about (and trying!) Nmap at http://nmap.org and the Nmap Scripting Engine at http://nmap.org/book/nse.html.

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
```