NMAP

BRIEF INTRODUCTION

Nmap ("Network Mapper") is a free and open source utility for network exploration or security auditing. Many systems and network administrators also find it useful for tasks such as network inventory, managing service upgrade schedules, 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 (and OS versions) they are running, what type of packet filters/firewalls are in use, and dozens of other characteristics.

usage: nmap [-scanning technique] [-option] <host address/subnet>

Warning: Nmap can't damage any hardware, but, in some situation, it can block a system until the reboot of the system itself. So be careful about using it on systems that owns necessary services.

STORY

Nmap is a security scanner originally written by Gordon Lyon (*Fyodor*), who take care about 3 web site: Insecure.Org, SecLists.Org, and SecTools.Org.
Nmap, "Network Mapper", was first released in 1997. It was designed to rapidly scan large networks, but works fine against single hosts.

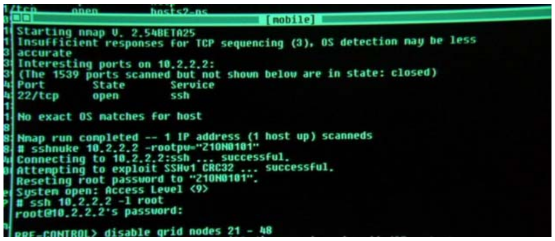
Nmap 3.50, instead of using a simple nmap-services table lookup to determine a port's likely purpose, will (if asked) interrogate that TCP or UDP port to determine what service is really listening. In many cases it can determine the application name and version number as well. Obstacles like SSL encryption and Sun RPC are no threat, as Nmap can connect using OpenSSL (if available) as well as utilizing Nmap's RPC bruteforcer. Simply add "-sV" to your normal scan command-line options.

Nmap Security Scanner version 4.00 includes a rewritten (for speed and memory efficiency) port scanning engine, ARP scanning, runtime interaction, massive version detection improvements, MAC address spoofing, increased Windows performance, 500 new OS detection fingerprints, and completion time estimates.

Afterwards the venerable but dated NmapFE was replaced with a new cross-platform GUI named Zenmap. It is cross platform (tested on Linux, Windows, Mac OS X) and supports all Nmap options. Its results viewer allows easier browsing, searching, sorting, and saving of Nmap results.

On the occasion of the 10th anniversary of the first release of Nmap, a new version, Nmap 4.50, has been released. Major new features since 4.00 include the Zenmap cross-platform GUI, 2nd Generation OS Detection, the Nmap Scripting Engine, a rewritten host discovery system, performance optimization, advanced traceroute functionality, TCP and IP options support, and nearly 1,500 new version detection signatures.

CURIOSITY



```
Starting nmap V. 2.54BETA25
Insufficient responses for TCP sequencing (3), OS detection may be less
accurate
Interesting ports on 10.2.2.2:
(The 1539 ports scanned but not shown below are in state: closed)
Port       State       Service
22/tcp     open        ssh

No exact OS matches for host

Nmap run completed -- 1 IP address (1 host up) scanneds
# sshnuke 10.2.2.2 -rootpw="Z10N0101"
Connecting to 10.2.2.2:ssh ... successful.
Attempting to exploit SSHv1 CRC32 ... successful.
Reseting root password to "Z10N0101".
System open: Access Level <9>
# ssh 10.2.2.2 -l root
root@10.2.2.2's password:

RRF-CONTROL> disable grid nodes 21 - 48
```

We have all seen many movies which pass off ridiculous 3D animated eye-candy scenes as hacking. But Trinity does it properly in The Matrix Reloaded. She whips out Nmap version 2.54BETA25, uses it to find a vulnerable SSH server, and then proceeds to exploit it using the SSH1 CRC32 exploit from 2001.

In The Bourne Ultimatum, the CIA needs to hack the mail server of a newspaper (The Guardian UK) to read the email of a reporter they assassinated. So they turn to Nmap and its new official GUI Zenmap to hack the mail server! Nmap reports that the mail server is running SSH 3.9p1, Posfix smtpd, and a name server.

US President George W. Bush visited the NSA (national security agency) headquarters at Fort Meade in January 2006. A wall-sized status screen in the background displays the latest versions of Nmap and some of other open source tools such as Nessus or Ethereal.

INSTALL GUIDE ON A UNIX SYSTEM

First of all download the source code of Nmap 4.50. The link is the following and includes the GUI frontend, Zenmap: http://download.insecure.org/nmap/dist/nmap-4.50.tar.bz2
Be sure to have C and C++ compiler installed on your system (eg: gcc and g++).
Execute the following commands:

```
bzip2 -cd nmap-4.50.tar.bz2 | tar xvf -
cd nmap-4.50
./configure
make
su root
make install
```

SOURCES:

http://insecure.org/
http://en.wikipedia.org/wiki/Nmap
http://sicurezza.html.it/articoli/leggi/995/nmap-guida-allinstallazione-e-alluso/
http://www.iana.org/assignments/port-numbers

Barbagallo Valerio
Da Lozzo Giordano
Mellini Giampiero