Ninja Scaning

by Fyodor

CanSecWest 2009 – March 20, 3:50 PM
http://insecure.org/presentations/CSW09/

Ncat

http://nmap.org/ncat/

Modern Networking Features

- SSL encryption support (client or server)
- Proxy (act as proxy server, or client chaining through multiple proxies)
- Portability
- TCP/UDP port redirection
- IPv6
- Fine-grained access control
- Connection brokering
- Missing feature

Ncat Chat

A slight hack to broker mode enables a very rudimentary chat server.

Official chat server for this presentation:

ncat insecure.org

(or telnet insecure.org 31337)

Server was started with command:

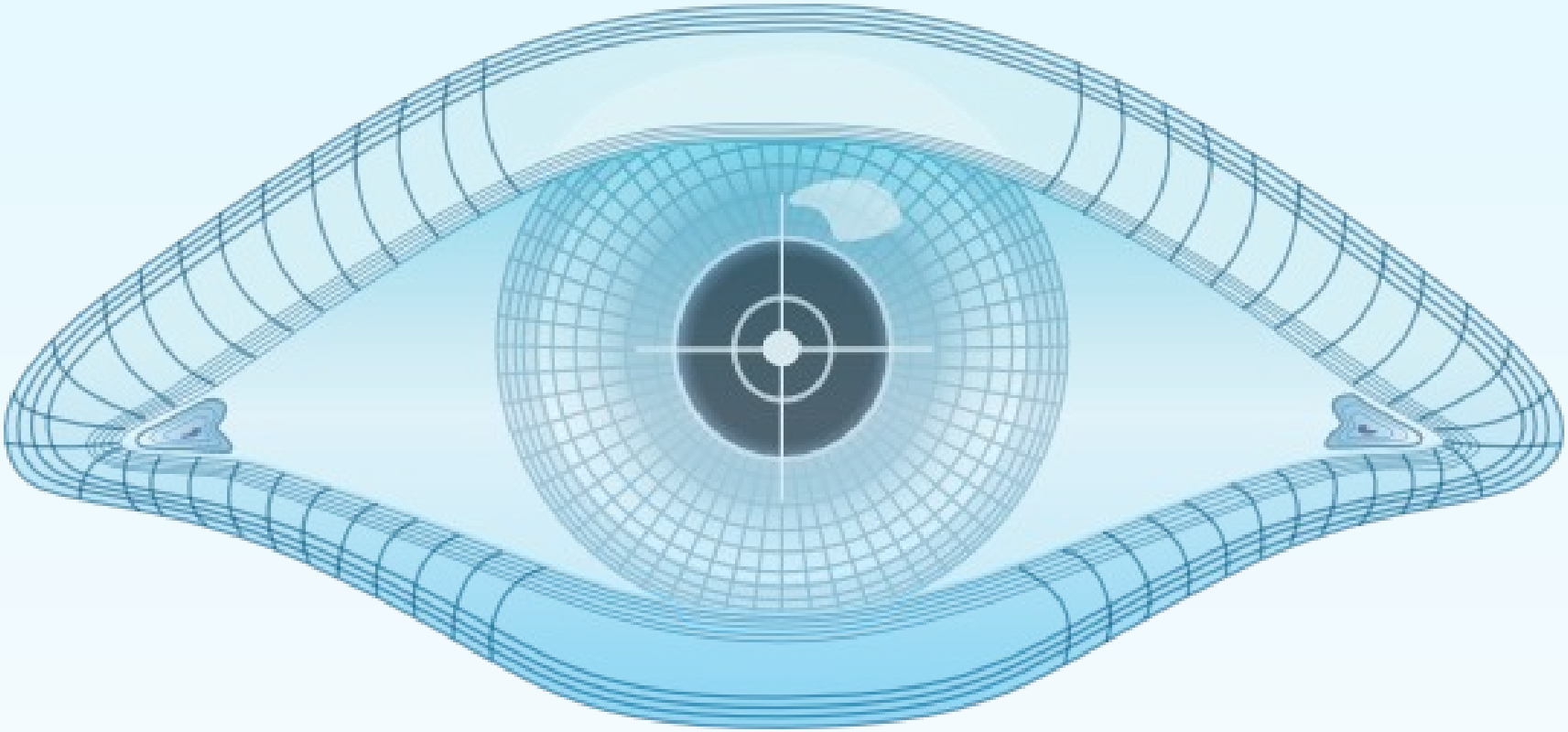
ncat -l --chat insecure.org

Final Ncat Notes

Available now in Nmap 4.85BETA4 at http://nmap.org/download.html

Practical usage examples are available in the users' guide: http://nmap.org/ncat/guide/

Nmap
http://nmap.org



CanSecWest Scans

Microsoft Scans

Nmap Scripting Engine
http://nmap.org/book/nse.html

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

Starting Nmap 4.85BETA4 ( http://nmap.org )
Interesting ports on scanme.nmap.org (64.13.134.52):
Not shown: 993 filtered ports
PORT      STATE  SERVICE VERSION
22/tcp    open   ssh     OpenSSH 4.3 (protocol 2.0)
|  ssh-hostkey: 1024
03:5f:d3:9d:95:74:8a:d0:8d:70:17:9a:bf:93:84:13 (DSA)
|_ 2048 fa:af:76:4c:b0:f4:4b:83:a4:6e:70:9f:a1:ec:51:0c
(RSA)
25/tcp    closed smtp
53/tcp    open   domain  ISC BIND 9.3.4
70/tcp    closed gopher
80/tcp    open   http    Apache httpd 2.2.2 ((Fedora))
|_ html-title: Go ahead and ScanMe!
113/tcp   closed auth
31337/tcp closed Elite
Device type: general purpose
OS details: Linux 2.6.20-1 (Fedora Core 5)
```

NSE Scripts

Nmap 4.85BETA4 has 55 of them

Examples: sql-injection, asn-query, dns-zone-transfer, http-open-proxy, irc-info, pop3-brute, snmp-brute

All scripts & libraries documented at: http://nmap.org/nsedoc/

SMB/MSRPC Scripts

Ron Bowes spent months researching SMB/MSRPC protocols and wrote 12 scripts.

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

Detailed Enumeration: smb-enum-users, smb-enum-domains, 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

Facebook Scans

BunnyLOL.Facebook.Com

```
# nmap -T4 -O -sCV bunnylol.facebook.com
Starting Nmap 4.85BETA4 ( http://nmap.org )
Interesting ports on bunnylol.facebook.com
(69.63.176.80):
Not shown: 999 filtered ports
PORT   STATE SERVICE VERSION
80/tcp open  http    CherryPy httpd 3.1.1
|  html-title: Site doesn't have a title
(text/html).
|_ Did not follow redirect to
http://www.dev.facebook.com/intern/authorize_lolb
unny.php?next=http%3A%2F%2Fbunnylol.facebook.com
%2F
Device type: load balancer
Running (JUST GUESSING) : F5 Networks embedded
(86%)
Aggressive OS guess: F5 BIG-IP load balancer
(86%)
IP ID Sequence Generation: Randomized
Nmap done: 1 IP address ... scanned in 15.21s
```

Facebook's Moochspot.Com


```
# nmap -T4 -v -sCV moochspot.com
Starting Nmap 4.85BETA4 ( http://nmap.org )
Interesting ports on www.moochspot.com
(69.63.178.60):
Not shown: 999 filtered ports
PORT   STATE SERVICE VERSION
80/tcp open  http    Jetty httpd 5.1.4
(Linux/2.6.12-1.1398_FC4smp amd64
java/1.6.0_07)
|  robots.txt: has 1 disallowed entry
|_ /admin/
|_ html-title: MoochSpot - Home

Nmap done: 1 IP address (1 host up) scanned
in 10.32s
```

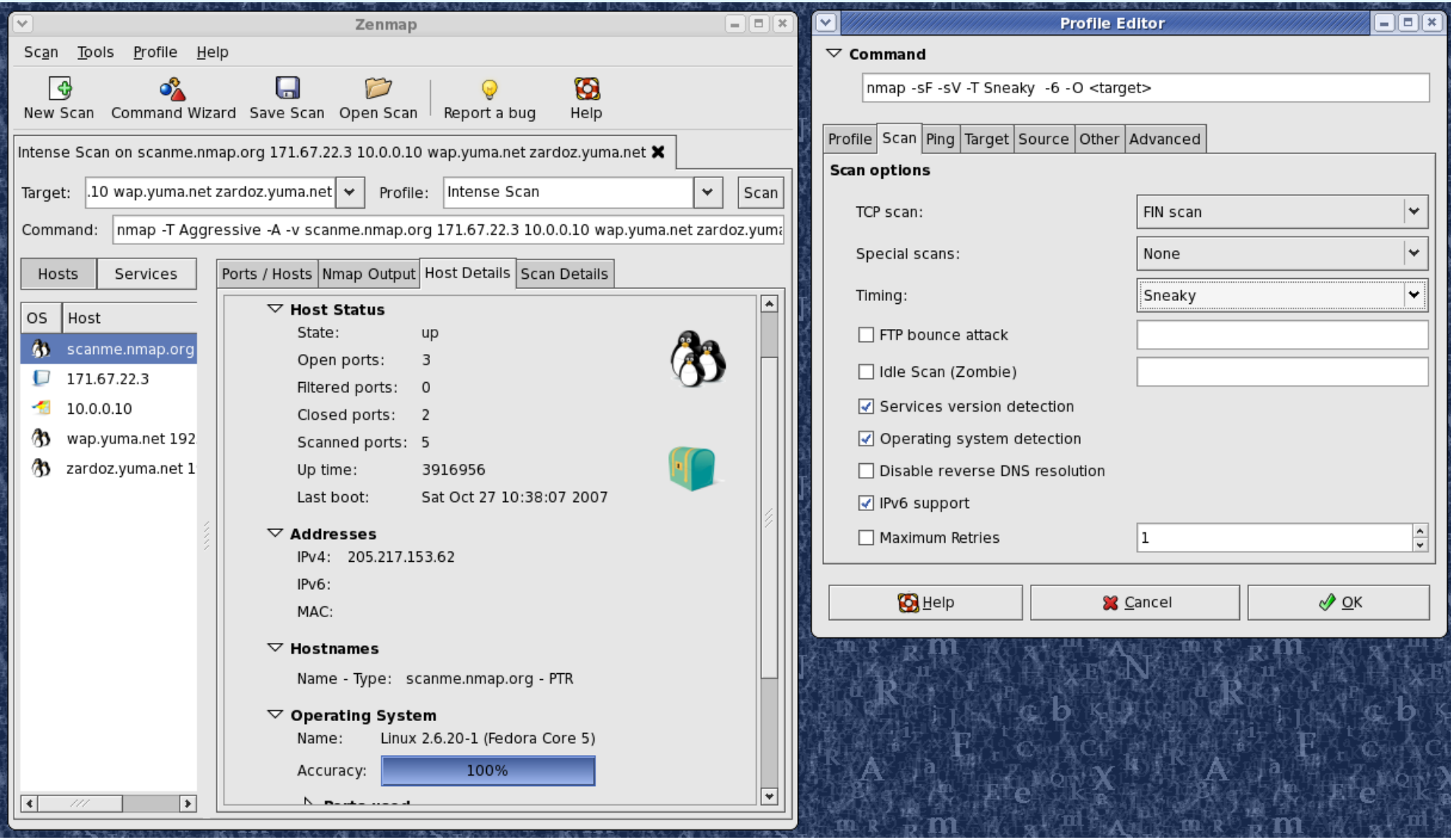
Ndiff

```
# ndiff facebook-031709.xml facebook-031809.xml
[...]
arborvip.tfbnw.net (69.63.179.23):
        Host is up, was unknown.
        Add ipv4 address 69.63.179.23.
        Add hostname arborvip.tfbnw.net.
        100 tcp ports are filtered.
vpnhub01-lo2.tfbnw.net (204.15.21.243):
        Remove hostname vpnhub01-lo2.tfbnw.net.
metroid.tfbnw.net (204.15.21.206):
        Remove hostname metroid.tfbnw.net.
69.63.184.144:
        Host is up, was unknown.
        Add ipv4 address 69.63.184.144.
        +80/tcp open http
        +443/tcp open http Apache httpd
1.3.41.fb1
        98 tcp ports are filtered.
```

Simple Ndiff Cron Script

```
#!/bin/sh
date=`date "+%s"`
cd /hack/facebook/scripts/
nmap -T4 -F -sV -O --osscan-limit --osscan-
guess -oA facebook-${date} [netblocks]  >
/dev/null
ndiff facebook-old.xml facebook-${date}.xml >
facebook-diff-${date}
cp facebook-${date}.xml facebook-old.xml
echo "\n********** NDIFF RESULTS **********\n"
cat facebook-vscan-diff-${date}
echo "\n********** SCAN RESULTS **********\n"
cat facebook-vscan-${date}.nmap
```

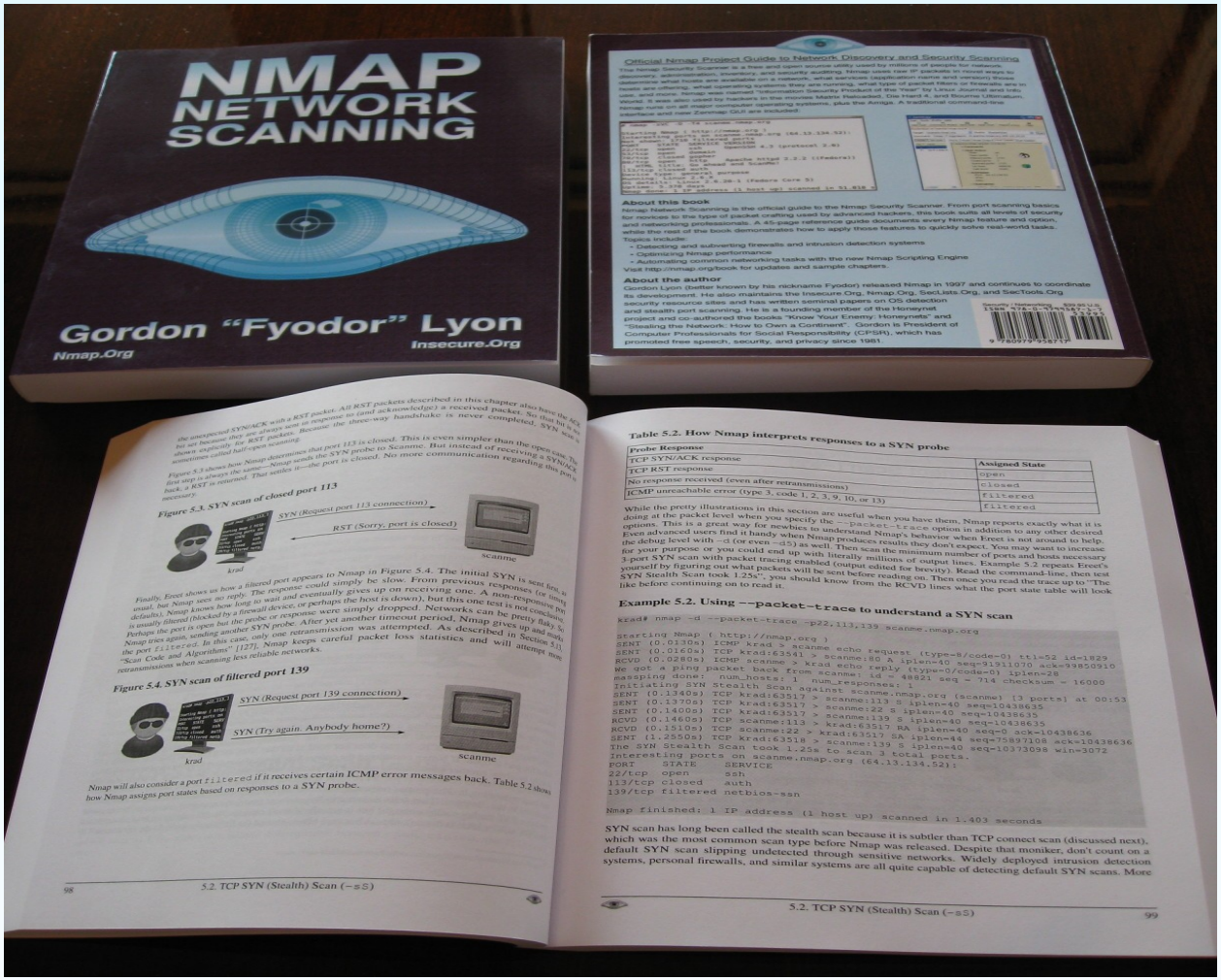
Zenmap GUI


Zenmap
Scan Tools Profile Help
New Scan
Command Wizard
Save Scan
Open Scan
Report a bug
Help
Intense Scan on scanme.nmap.org 171.67.22.3 10.0.0.10 wap.yuma.net zardoz.yuma.net
Target: .10 wap.yuma.net zardoz.yuma.net
Profile: Intense Scan
Scan
Command: nmap -T Aggressive -A -v scanme.nmap.org 171.67.22.3 10.0.0.10 wap.yuma.net zardoz.yuma
Hosts
Services
OS
Host
scanme.nmap.org
171.67.22.3
10.0.0.10
wap.yuma.net 192
zardoz.yuma.net 1
Ports / Hosts
Nmap Output
Host Details
Scan Details
Host Status
State: up
Open ports: 3
Filtered ports: 0
Closed ports: 2
Scanned ports: 5
Up time: 3916956
Last boot: Sat Oct 27 10:38:07 2007
Addresses
IPv4: 205.217.153.62
IPv6:
MAC:
Hostnames
Name - Type: scanme.nmap.org - PTR
Operating System
Name: Linux 2.6.20-1 (Fedora Core 5)
Accuracy: 100%
Profile Editor
Command
nmap -sF -sV -T Sneaky -6 -O <target>
Profile
Scan
Ping
Target
Source
Other
Advanced
Scan options
TCP scan: FIN scan
Special scans: None
Timing: Sneaky
FTP bounce attack
Idle Scan (Zombie)
Services version detection
Operating system detection
Disable reverse DNS resolution
IPv6 support
Maximum Retries
1
Help
Cancel
OK

Top Contributors Since CSW '08

4N9e Gutek, Adriano Monteiro Marques, Allison Randal, Andrew J. Bennieston, Arturo Buanzo Busleiman, Benson Kalahar, Bill Pollock, Brandon Enright, Chad Loder, Chris Clements, Chris Leick, Daniel Roethlisberger, David Fifield, Diman Todorov, Doug Hoyte, Dudi Itzhakov, Eddie Bell, Gisle Vanem, Guilherme Polo, Guz Alexander, Henri Doreau, Jabra, Jah, James Messer, Jason DePriest, Jesse Burns, Joao Medeiros, Jurand Nogiec, Kris Katterjohn, Lamont Jones, Lance Spitzner, Martin Macok, Matt Selsky, Michael Pattrick, Michal Januszewski, Mixter, Nathan Bills, Patrick Donnelly, Philip Pickering, Rainer Müller, Raven Alder, Robert Mead, Rob Nicholls, Ron Bowes, Stephan Fijneman, Steve Christensen, Sven Klemm, Thomas Buchanan, Tom Duffy, Tom Sellers, Trevor Bain, Tyler Reguly, Vlad Alexa, Vladimir Mitrovic, Vlatko Kosturjak

Nmap Network Scanning
http://nmap.org/book/



Questions and Resources

Download Nmap from http://nmap.org

Slides are posted at: http://insecure.org/presentations/CSW09/