

Fighting Zombies with FastNMAP

MOREnet Security Symposium

Wednesday, March 16, 2011

Brian Allen, CISSP

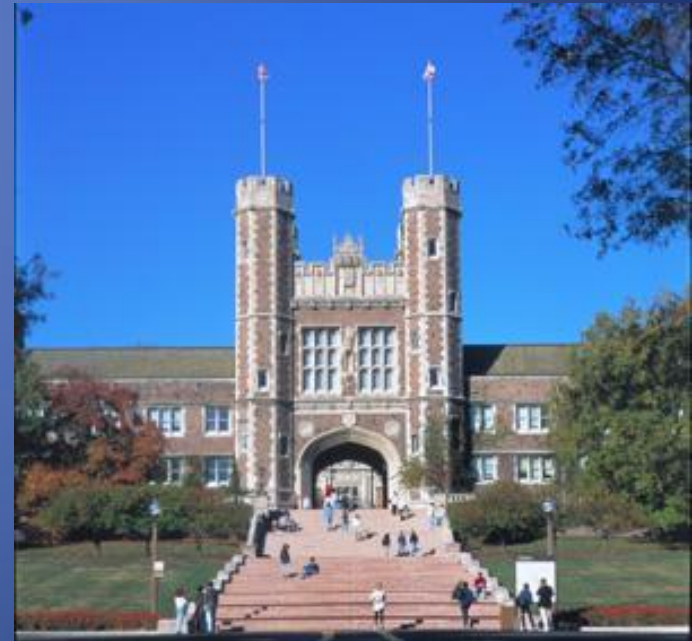
brianallen@wustl.edu

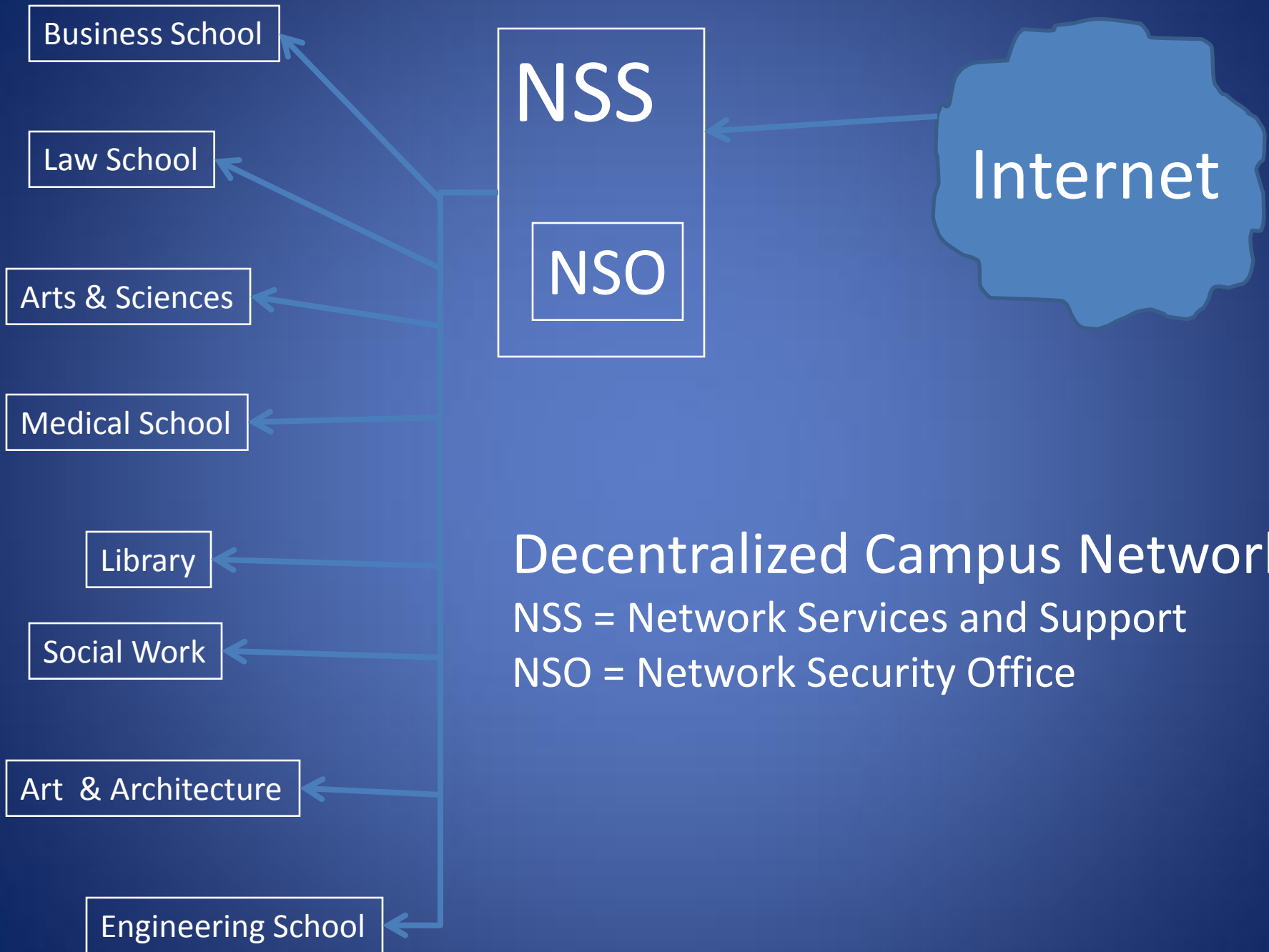
Network Security Analyst,
Washington University in St. Louis

<http://nso.wustl.edu/>

Washington University in St. Louis, MO

- Private University Founded in 1853
- 3,000+ Full Time and Adjunct Faculty
- 13,000+ Full and Part Time Students
- 13,000+ Employees
- 4000+ Students Living on Campus
- Decentralized Campus Network





Decentralized Campus Network

NSS = Network Services and Support

NSO = Network Security Office

When your network looks like



How do you find



and



?

Nmap, of course!



GOAL

- Scan every IP address and every port on the network
- Tool of Choice = NMAP

Some NMAP Benefits

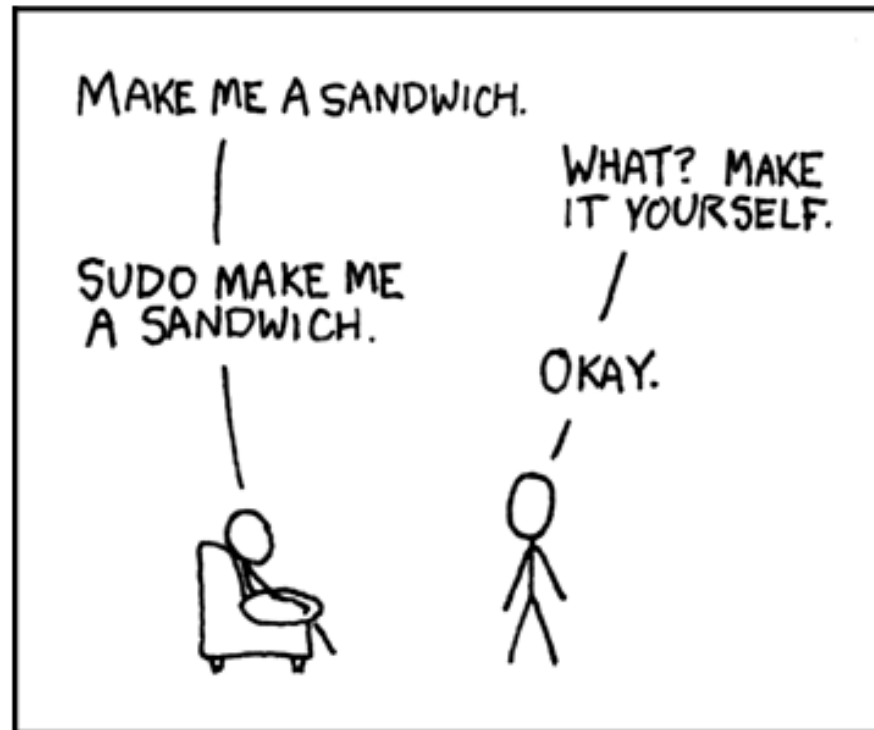
- NMAP is the top pick because it:
 - Finds backdoors, FTP servers, open proxies, rogue access points, etc
 - Can identify many services running like Apache servers, IIS 5.0, or RealVNC
 - Extensive series of scripts available similar to nessus or metasploit
 - Open Source

NMAP Downsides

- But NMAP has trouble scanning more than a few hosts or small subnets at a time:
 - It returns too much data to reasonably wade through
 - It has performance issues scanning large networks

Must be Root to use all NMAP features: `sudo ./nmap -make_sandwich`

SANDWICH



PERMANENT LINK TO THIS COMIC: [HTTP://XKCD.COM/149/](http://xkcd.com/149/)

IMAGE URL (FOR HOTLINKING/EMBEDDING): [HTTP://IMGS.XKCD.COM/COMICS/SANDWICH.PNG](http://imgs.xkcd.com/comics/sandwich.png)

Solution: FastNMAP and NPWN

- Developed by Brandon Enright UC San Diego
- <http://sourceforge.net/projects/npwn>

- **Fastnmap.pl**
 - runs NMAP in a way to optimize it for scanning large networks
 - Splits your large network into small scan tasks
 - Manages several Nmap processes in parallel
 - Adjusts parallelism to meet a scan completion deadline
- **npwn.pl**
 - a tool that reads in large FastNMAP reports and quickly highlights important items
 - Analyzes Nmap XML output
 - Signature/Heuristic based with severity ratings
 - Handles host/CIDR based excludes

Potential Pitfalls of Scanning

- Pick a reasonable period to scan: 1 week < X < A Couple Months
- Identify Devices with Problems, Exclude Them, Work to Fix them
 - A Switch's one minute heartbeat was missed, and school's network engineers were paged
 - A KVM Switch Hung – It was old and needed to be updated, then it handled the scan fine

NMAP Scripting Engine

- I kept 92 nse scripts like:
 - "dns-recursion.nse"
 - "http-headers.nse"
 - "imap-capabilities.nse"
 - "irc-info.nse"
 - "p2p-conficker.nse"
 - "smb-enum-users.nse"
 - "ssl-cert.nse"
- I removed all the brute force ones

We Interrupt This NSO Presentation
For An Important Security
Announcement From XKCD.com

SECURITY

<

< PREV

RANDOM

NEXT >

>

A CRYPTO NERD'S
IMAGINATION:

HIS LAPTOP'S ENCRYPTED.
LET'S BUILD A MILLION-DOLLAR
CLUSTER TO CRACK IT.

BLAST! OUR
EVIL PLAN
IS FOILED!

NO GOOD! IT'S
4096-BIT RSA!



WHAT WOULD
ACTUALLY HAPPEN:

HIS LAPTOP'S ENCRYPTED.
DRUG HIM AND HIT HIM WITH
THIS \$5 WRENCH UNTIL
HE TELLS US THE PASSWORD.

GOT IT.



<

< PREV

RANDOM

NEXT >

>

PERMANENT LINK TO THIS COMIC: [HTTP://XKCD.COM/538/](http://xkcd.com/538/)

IMAGE URL (FOR HOTLINKING/EMBEDDING): [HTTP://IMGS.XKCD.COM/COMICS/SECURITY.PNG](http://imgs.xkcd.com/comics/security.png)

FastNMAP Command

```
# nmap -sL -n 128.252.0.0/16 |  
egrep '^Nmap scan' |  
awk '{print $5}' |  
./fastnmap.pl
```

NPWN Command

```
# ./npwn.pl -x -oG -d ./log/ > output
```

```
sudo ./nmap
--datadir
  /home/<PATH>/nmap/
-p-
-PN
-sV
-O
--version-all
--script=all
-open
-ttl 12
-vv
-d
-T5
--min-parallelism 64
--max-parallelism 512
--min-rate 200
--max-rate 4000
--min-rtt-timeout 10
--host-timeout 120m
--min-hostgroup 64
--nogcc
--log-errors
-oA log/report_' . $scanid .'
--excludefile
  ./always_exclude.txt
@targets
> log/report_'.$scanid.'.txt
2> log/report_'.$scanid.'.err
```

Unix Screen Command

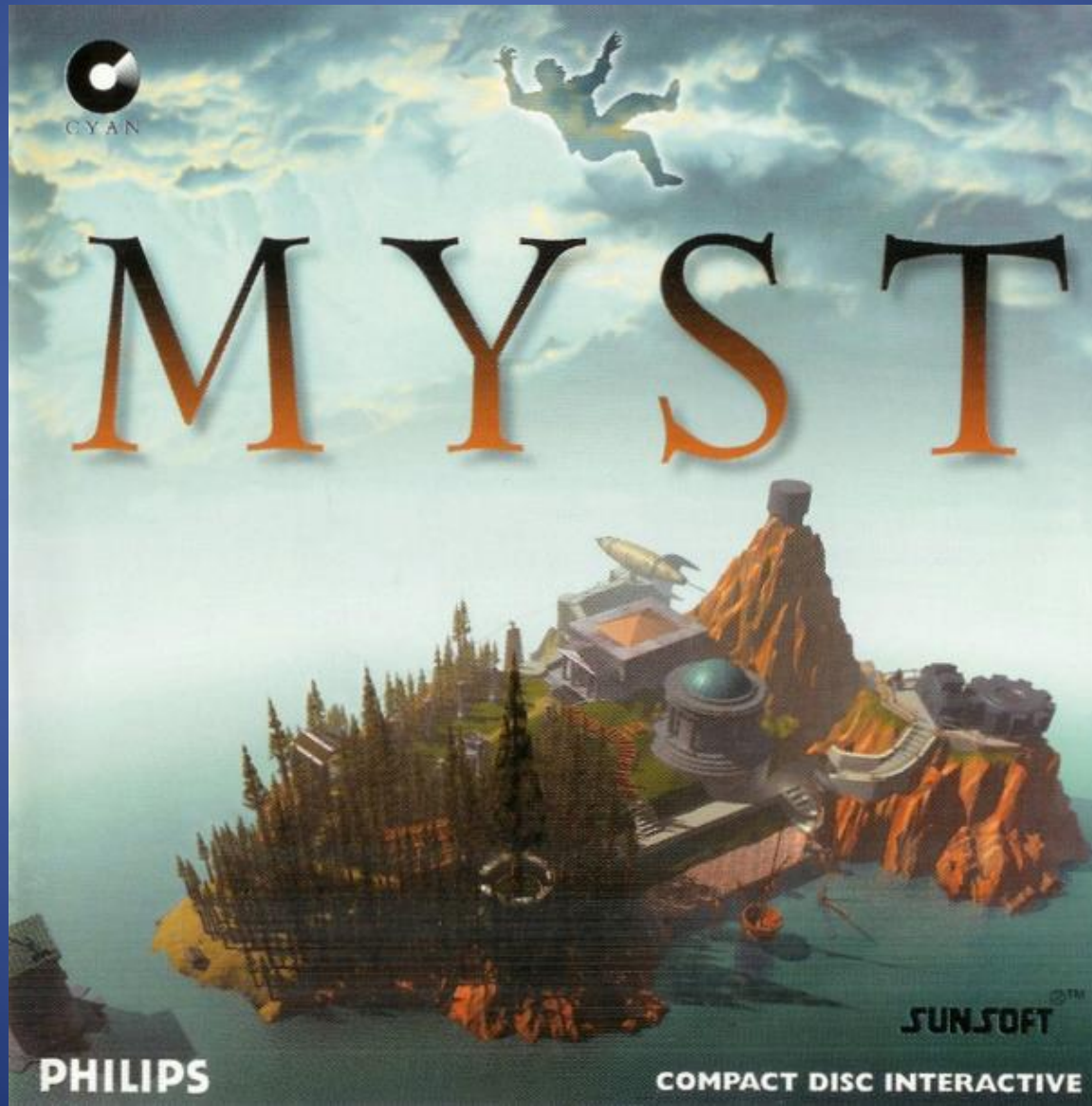
- If the shell dies, so does your work.
- To keep your shell alive—even across multiple sessions and dropped connections—use GNU Screen, a windowing system for your console.
- Step 1) Type: `$ screen`
- Step 2) Type: `$ man screen`

FastNMAP.pl Status Update

- Less than four days to scan 128.252.0.0/16
- Much of the campus sits behind firewalls
- Some departments want different scan frequency
- Am not scanning any of our private IP space (student subnets, wireless, etc)
- Usually find about 4000 IP addresses online

```
-----  
Scan started at Fri Apr 23 14:25:12 2010 UTC  
Goal end time at Fri Apr 30 14:25:12 2010 UTC  
65297 IPs done (99.64%) in 265908 seconds with 8.02 average threads  
Average thread-work-factor: 30.63 mIST  
Currently using 8 threads, will finish at Mon Apr 26 16:33:16 2010 UTC  
Target off of goal by -5631.93 minutes  
Network rate: TX 22028 pps (1.35 MBps); RX 867 pps (0.08 MBps)  
-----
```

mIST Metric



CYAN

MYST

PHILIPS

SUNSOFT™

COMPACT DISC INTERACTIVE

mIST Metric

- The mIST metric is "mili-IPs per Thread-Second".
- $mIST = 30 \Rightarrow$ in 1000 seconds each thread will scan an average of 30 IPs.
- So if there are 8 threads, in 1000 seconds about 240 IPs will be scanned.

```
-----  
Scan started at Fri Apr 23 14:25:12 2010 UTC  
Goal end time at Fri Apr 30 14:25:12 2010 UTC  
65297 IPs done (99.64%) in 265908 seconds with 8.02 average threads  
Average thread-work-factor: 30.63 mIST  
Currently using 8 threads, will finish at Mon Apr 26 16:33:16 2010 UTC  
Target off of goal by -5631.93 minutes  
Network rate: TX 22028 pps (1.35 MBps); RX 867 pps (0.08 MBps)  
-----
```

Some Interesting Npwn Tags

NPWN TAG	Severity
[VNCAUTHBYPASS]	{10}
[BACKDOOR]	{10}
[IMAPWEAKAUTHNOSSL]	{7}
[POP3WEAKAUTHNOSSL]	{7}
[NOPASSWD]	{7}
[OPENX11]	{7}
[SERV-U]	{6}
[OLD_MSFTP]	{4}
[SSLCERT_WILDCARD]	{4}
[NSFTP]	{3}

```
Nmap scan report for .wustl.edu (128.252.
Host is up, received user-set (0.0027s latency).
Scanned at 2010-04-23 14:25:15 CDT for 309s
Not shown: 65530 closed ports
Reason: 65530 resets
PORT      STATE SERVICE      REASON  VERSION
23/tcp    open  telnet       syn-ack HP JetDirect printer telnetd (No password)
|_banner: \xFF\xFB\x03
80/tcp    open  http         syn-ack Virata-EmWeb 6.0.1 (HP JetDirect http config)
```

```
128.252. ( .wustl.edu) (14):
-----
(1) [HTTP] -- Web server on 80 is Virata-EmWeb 6.0.1 (HP JetDirect http config)
(1) [PRINTER_HTTP] -- Device appears printer running Virata-EmWeb 6.0.1 (HP JetDirect http config)
(1) [HTTP] -- Web server on 280 is Virata-EmWeb 6.0.1 (HP JetDirect http config)
(2) [TELNET] -- Telnet server on 23
(2) [PRINTER_TELNET] -- Device appears printer running HP JetDirect printer telnetd (No password)
(7) [NOPASSWD] -- Service on 23 does not require password
```

```
Nmap scan report for .wustl.edu (128.252. )
Scanned at 2010-04-18 06:48:31 CDT for 635s
PORT      STATE SERVICE      REASON  VERSION
135/tcp   open  msrpc        syn-ack Microsoft Windows RPC
139/tcp   open  netbios-ssn syn-ack
445/tcp   open  microsoft-ds syn-ack Microsoft Windows XP microsoft-ds
1025/tcp  open  mstask       syn-ack Microsoft mstask (task server - c:\winnt\system32\Mstask.exe)
5800/tcp  open  vnc-http     syn-ack RealVNC 4.0 (Resolution 400x250; VNC TCP port: 5900)
5900/tcp  open  vnc          syn-ack VNC (protocol 3.8)
|_realvnc-auth-bypass: Vulnerable

Host script results:
| nbstat:
|   NetBIOS name: RAMA, NetBIOS user: <unknown>, NetBIOS MAC: 00:b0:d0:d9:31:8a (Dell Computer)
|   Names
|     RAMA<20>           Flags: <unique><active>
|     RAMA<00>           Flags: <unique><active>
|     WORKGROUP<00>     Flags: <group><active>
|     WORKGROUP<1e>     Flags: <group><active>
|     WORKGROUP<1d>     Flags: <unique><active>
|     \x01\x02__MSBROWSE__\x02<01>  Flags: <group><active>
|_ smb-os-discovery:
|   OS: Windows 2000 (Windows 2000 LAN Manager)
|   Name: WORKGROUP\RAMA
|   System time: 2010-04-18 08:01:00 UTC-5
|_ smb-enum-users:
|   RAMA\Administrator (RID: 500)
|   RAMA\Guest (RID: 501)
|_ smb-enum-shares:
|   ERROR: Enumerating shares failed, guessing at common ones (NT_STATUS_WERR_ACCESS_DENIED (srvsvc.netshareenumall))
|   IPC$ (WARNING: Couldn't get details for share: NT_STATUS_WERR_ACCESS_DENIED (srvsvc.netsharegetinfo))
|_   Anonymous access: READ
```

```
128.252. ( .wustl.edu) (10):
-----
(10) [VNCAUTHBYPASS] -- RealVNC server on 5900 vulnerable to auth bypass
```

```
443/tcp open  ssl/http syn-ack BarracudaHTTP 1.00 (Barracuda Networks
Load Balancer http config)
| ssl-cert: Subject: commonName=
.wustl.edu/organizationName=Washington University/stateOrProvinceName=Missouri/countryName=US
/localityName=St. Louis/organizationalUnitName=Terms of use at www.verisign.com/rpa (c)05
| Issuer: organizationName=RSA Data Security, Inc./countryName=US/org
anizationalUnitName=Secure Server Certification Authority
| Not valid before: 2005-08-19 00:00:00
| Not valid after: 2007-08-19 23:59:59
| MD5: 53ed 1003 113e 30ec ab01 3d7e e0a5 5d7a
| SHA-1: 44e7 6311 fefd 974a fd8e f20d 7a5c 2e86 745b bf3e
| -----BEGIN CERTIFICATE-----
| MIIEDCCA4GgAwIBAgIQbKHE1KH7w2gjVgxwOhOgNjANBgkqhkiG9wOBAQUFADBf
| MQswCQYDVQQGEwJVUzEgMB4GA1UEChMXU1NBIERhdGEgU2VjdXJpdHksIEluYy4x
| LjAsBgNVBAstJVN1Y3VyZSBTZXB2ZXJ2ZXIgaWQ2VydGlmaWNhdGlvbiBBdXRob3JpdHkw
| HhcNMDUwODE5MDAwMDAwWheNMDcwODE5MjM1OTU5WjCBYTELMARGA1UEBhMCMVVMx
| ETAPBgNVBAgTCE1pc3NvdXJpMRIwEAYDVQQHFA1TdC4gTG91aXMxHjAcBgNVBAoU
```

```
128.252.. ( .wustl.edu) (21):
```

```
-----
(1) [MAYBEWAP] -- Device may be router or wireless access point
(1) [SMTP] -- SMTP server on 25 is Barracuda Networks Spam Firewall smtpd
(1) [HTTP] -- Web server on 443 is BarracudaHTTP 1.00 (Barracuda Networks Load Balancer http config)
(2) [FIREWALLED] -- There are 65531 filtered ports, a firewall is blocking the scan
(3) [SSLCERT_EXPIRED] -- SSL Cert on 443 has expired
(5) [SSLV2] -- Service on 443 supports SSLv2
(8) [SSLV2_40BIT] -- Service on 443 supports 40-bit SSLv2
```

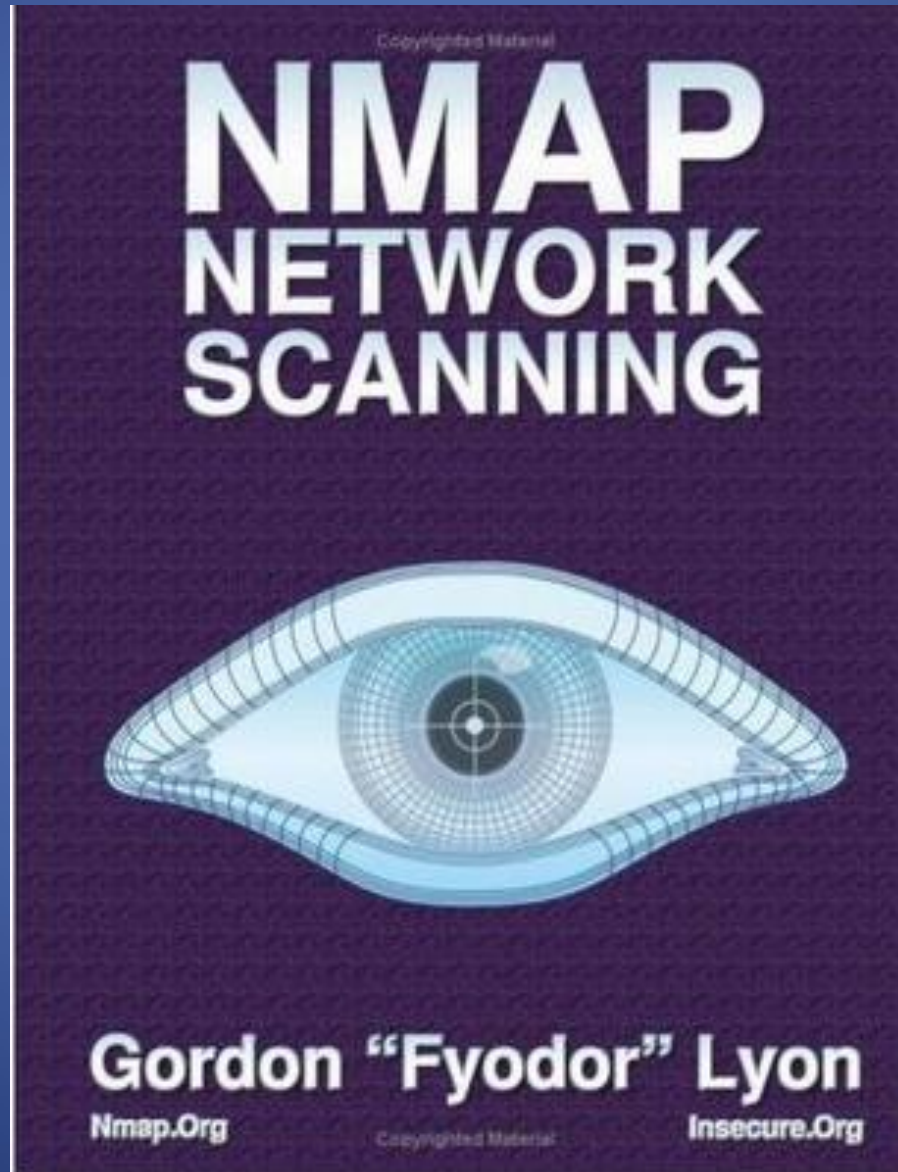
```
Nmap scan report for .wustl.edu (128.252. )
Host is up, received user-set (0.00060s latency).
Scanned at 2010-04-24 04:01:15 CDT for 499s
Not shown: 65501 closed ports, 13 filtered ports
Reason: 65501 resets and 13 no-responses
PORT      STATE SERVICE      REASON  VERSION
21/tcp    open  ftp          syn-ack Microsoft ftpd
|_banner: 220 Microsoft FTP Service
135/tcp   open  msrpc        syn-ack Microsoft Windows RPC
139/tcp   open  netbios-ssn syn-ack
445/tcp   open  microsoft-ds syn-ack Microsoft Windows 2003 or 2008 microsoft-ds
515/tcp   open  printer      syn-ack Microsoft lpd
548/tcp   open  afp?         syn-ack
1001/tcp  open  ftp          syn-ack Serv-U ftpd (SSL Required)
|_banner: 220 Welcome to Paradise...
|_ftp-bounce: no banner
1047/tcp  open  msrpc        syn-ack Microsoft Windows RPC
1048/tcp  open  msrpc        syn-ack Microsoft Windows RPC
1097/tcp  open  jrmi         syn-ack Java RMI
3500/tcp  open  ms-sql-s     syn-ack Microsoft SQL Server 2000 8.00.2039; SP4
51500/tcp open  tcpwrapped   syn-ack
51501/tcp open  tcpwrapped   syn-ack
51502/tcp open  tcpwrapped   syn-ack
51503/tcp open  tcpwrapped   syn-ack
51504/tcp open  tcpwrapped   syn-ack
51505/tcp open  tcpwrapped   syn-ack
51506/tcp open  tcpwrapped   syn-ack
51507/tcp open  tcpwrapped   syn-ack
51508/tcp open  tcpwrapped   syn-ack
```

```
~/flexmap# openssl s_client -connect 128.252.:1001
CONNECTED(00000003)
depth=0 /CN=The Microsoft Corporation/L=Washington DC/ST=DC/O=Microsoft.com/C=US/emailAddress=Support@Microsoft.com/OU=FTP - Server
verify error:num=18:self signed certificate
```

Scanned at 2010-08-16 14:54:08 CDT for 945s

PORT	STATE	SERVICE	REASON	VERSION
53/tcp	open	domain	syn-ack	Microsoft DNS
88/tcp	open	tcpwrapped	syn-ack	
135/tcp	open	msrpc	syn-ack	Microsoft Windows RPC
139/tcp	open	netbios-ssn	syn-ack	
389/tcp	open	ldap	syn-ack	
464/tcp	open	kpasswd5?	syn-ack	
593/tcp	open	ncacn_http	syn-ack	Microsoft Windows RPC over HTTP 1.0
636/tcp	open	tcpwrapped	syn-ack	
1026/tcp	open	msrpc	syn-ack	Microsoft Windows RPC
1027/tcp	open	ncacn_http	syn-ack	Microsoft Windows RPC over HTTP 1.0
1059/tcp	open	msrpc	syn-ack	Microsoft Windows RPC
3268/tcp	open	ldap	syn-ack	
3269/tcp	open	tcpwrapped	syn-ack	
3389/tcp	open	microsoft-rdp	syn-ack	Microsoft Terminal Service
32000/tcp	open	ftp	syn-ack	Rhinosoft Serv-U FTP
_ banner:		220 DHCP Service		

Very Good Book on NMAP



Any Questions?

<http://sourceforge.net/projects/npwn>