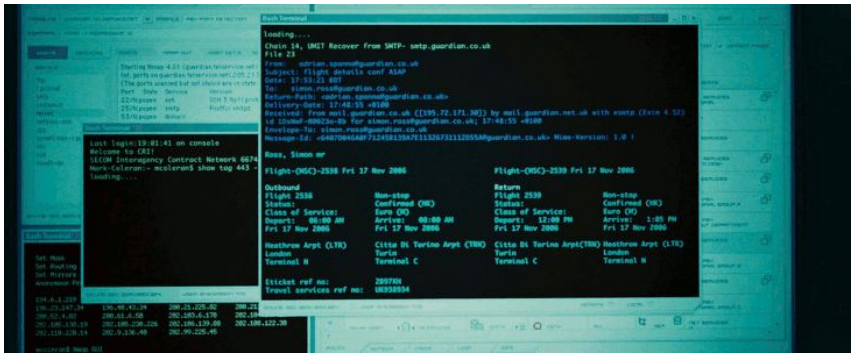
Nmap (“Network Mapper”) is a free and open source (license) utility for network exploration or security auditing. Many systems and network administrators also find it useful for tasks such as network inventory, managing service upgrade schedules, and monitoring host or service uptime.



In addition to my list you can also check out this Comprehensive Guide to Nmap here and of course the man pages
Here are some really cool scanning techniques using Nmap

1) Get info about remote host ports and OS detection

nmap -sS -P0 -sV -O <target>

Where < target > may be a single IP, a hostname or a subnet

-sS TCP SYN scanning (also known as half-open, or stealth scanning)

-P0 option allows you to switch off ICMP pings.

-sV option enables version detection

-O flag attempt to identify the remote operating system

Other option:

-A option enables both OS fingerprinting and version detection

-v use -v twice for more verbosity.

nmap -sS -P0 -A -v < target >

2) Get list of servers with a specific port open

nmap -sT -p 80 -oG – 192.168.1.* | grep open

Change the -p argument for the port number. See “man nmap” for different ways to specify address ranges.

3) Find all active IP addresses in a network

nmap -sP 192.168.0.*

There are several other options. This one is plain and simple.

Another option is:

nmap -sP 192.168.0.0/24

for specific subnets

4) Ping a range of IP addresses

nmap -sP 192.168.1.100-254

nmap accepts a wide variety of addressing notation, multiple targets/ranges, etc.

5) Find unused IPs on a given subnet

nmap -T4 -sP 192.168.2.0/24 && egrep “00:00:00:00:00:00” /proc/net/arp

6) Scan for the Conficker virus on your LAN ect.

nmap -PN -T4 -p139,445 -n -v –script=smb-check-vulns –script-args safe=1 192.168.0.1-254

replace 192.168.0.1-256 with the IP’s you want to check.

7) Scan Network for Rogue APs.

nmap -A -p1-85,113,443,8080-8100 -T4 –min-hostgroup 50 –max-rtt-timeout 2000 –initial-rtt-timeout 300 –max-retries 3 –host-timeout 20m –max-scan-delay 1000 -oA wapscan 10.0.0.0/8

I've used this scan to successfully find many rogue APs on a very, very large network.

8) Use a decoy while scanning ports to avoid getting caught by the sys admin

sudo nmap -sS 192.168.0.10 -D 192.168.0.2

Scan for open ports on the target device/computer (192.168.0.10) while setting up a decoy address (192.168.0.2). This will show the decoy ip address instead of your ip in targets security logs. Decoy address needs to be alive. Check the targets security log at /var/log/secure to make sure it worked.

9) List of reverse DNS records for a subnet

nmap -R -sL 209.85.229.99/27 | awk '{if($3=="not")print"("$2")no PTR";else print$3" is "$2}' | grep '('

This command uses nmap to perform reverse DNS lookups on a subnet. It produces a list of IP addresses with the corresponding PTR record for a given subnet. You can enter the subnet in CDIR notation (i.e. /24 for a Class C)). You could add "–dns-servers x.x.x.x" after the "-sL" if you need the lookups to be performed on a specific DNS server. On some installations nmap needs sudo I believe. Also I hope awk is standard on most distros.

10) How Many Linux And Windows Devices Are On Your Network?

```
sudo nmap -F -O 192.168.0.1-255 | grep "Running: " > /tmp/os; echo "$(cat /tmp/os | grep Linux | wc -l) Linux device(s)"; echo "$(cat /tmp/os | grep Windows | wc -l) Window(s) devices"
```

Hope you have fun, and remember don't practice these techniques on machines or networks that are not yours.

NMAP

PREVIOUS POST
Top 25 SED Commands

NEXT POST
25 More – Sick Linux Commands

19 THOUGHTS ON "10 COOL NMAP TRICKS AND TECHNIQUES"

Pingback: Tweets that mention 10 Cool Ways to Use Nmap -- Topsy.com

Kyurietto
DECEMBER 1, 2010 AT 2:24 AM
Good article. I was searching for this for a long time Thanks alot! stumbled

REPLY

Jackie
DECEMBER 1, 2010 AT 8:21 AM
Great post Isaiah! Thank you for sharing it with the world :)

REPLY

Rod
DECEMBER 1, 2010 AT 9:23 AM
nmap -sT -p 80 -oG – 192.168.1.* | grep open
does not work for me

Responses are four lines, with ‘open’ and the IP on different lines

Interesting ports on 172.16.23.251:
PORT STATE SERVICE
80/tcp open http
MAC Address: 00:02:B3:E9:4B:15 (Intel)

nmap -sT -p 80 -oG – 172.16.23.*|\
grep -B2 open|grep -o 172.16.23.[0-9]*

REPLY

Isaiah

DECEMBER 1, 2010 AT 10:30 AM

@Rod I replaced the command with
nmap -sT -p 80 -oG – 192.168.100.* | grep open
since my router gives me a 192.168.100.2 address
Find out your local IP and substitute the IP for yours.
Hope that works.

REPLY

Ma Diga

DECEMBER 1, 2010 AT 2:37 PM

Nmap is one of the most underrated tools out there for various tasks. Thanks for the examples!

REPLY

Rioting_pacifist

DECEMBER 1, 2010 AT 2:58 PM

sudo nmap -F -O 192.168.0.1-255 | grep “Running: ” > /tmp/os | echo $(grep -c Linux /tmp/os) Linux device(s)”; echo “$(grep -c Windows /tmp/os) Window(s) devices”

The cats where annoying me! Other than that it was a great