



Christopher D Hopkins (Hydroplane)

<https://github.com/cdhop/nmap101>



UtahSec

URUG

UPHPU

SLLUG

BsidesSLC

OpenWest

DC801

RubyHack

UtahSaint

HackWest

801Labs

SAINTCON

UTOS



A security scanner originally written by Gordon Lyon (Fyodor Vaskovich) used to discover hosts and services on a computer network, thus creating a "map" of the network.

— Wikipedia



- Host Discovery
- Port Scanner
- Version/OS Detection
- Additional functionality through NMAP Scripting Engine (NSE)



- I am not a lawyer
- I am definitely not your lawyer
- To be safe, only scan your own systems, or systems that you have explicit authorization to scan.
- Test Host: **scanme.nmap.org**

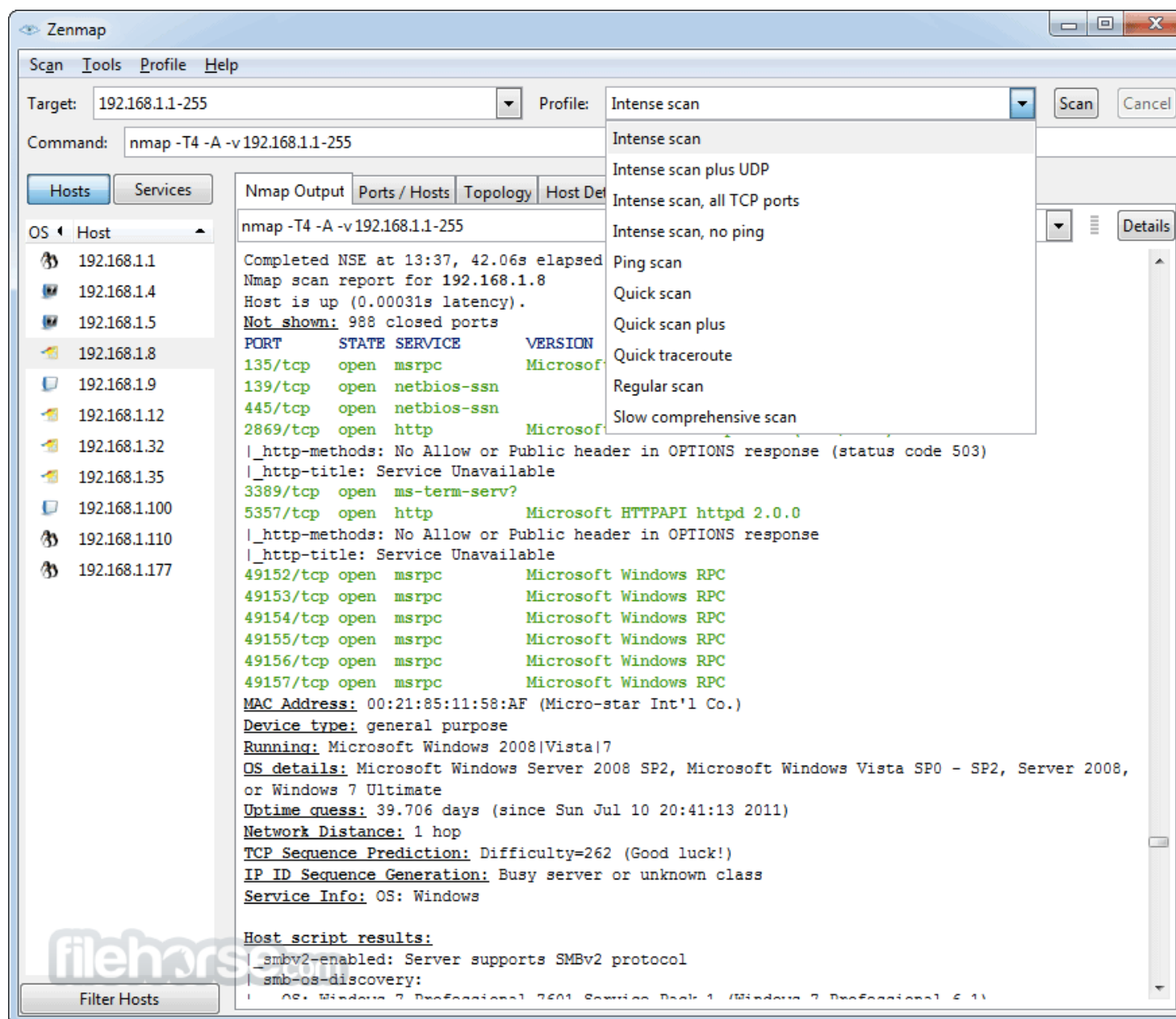


- Package Management
- Binaries (Windows/Macintosh)
- Source Code



NMAP 101

GUI (Zenmap)





A port is an end point/interface for communication on a system/host available over a network.

Specific port numbers are often used to identify specific services (for example: 80 http, 22 ssh, 443 https, etc)

Ports 1-1024 are considered 'well-known' and usually require root/administrator privileges.



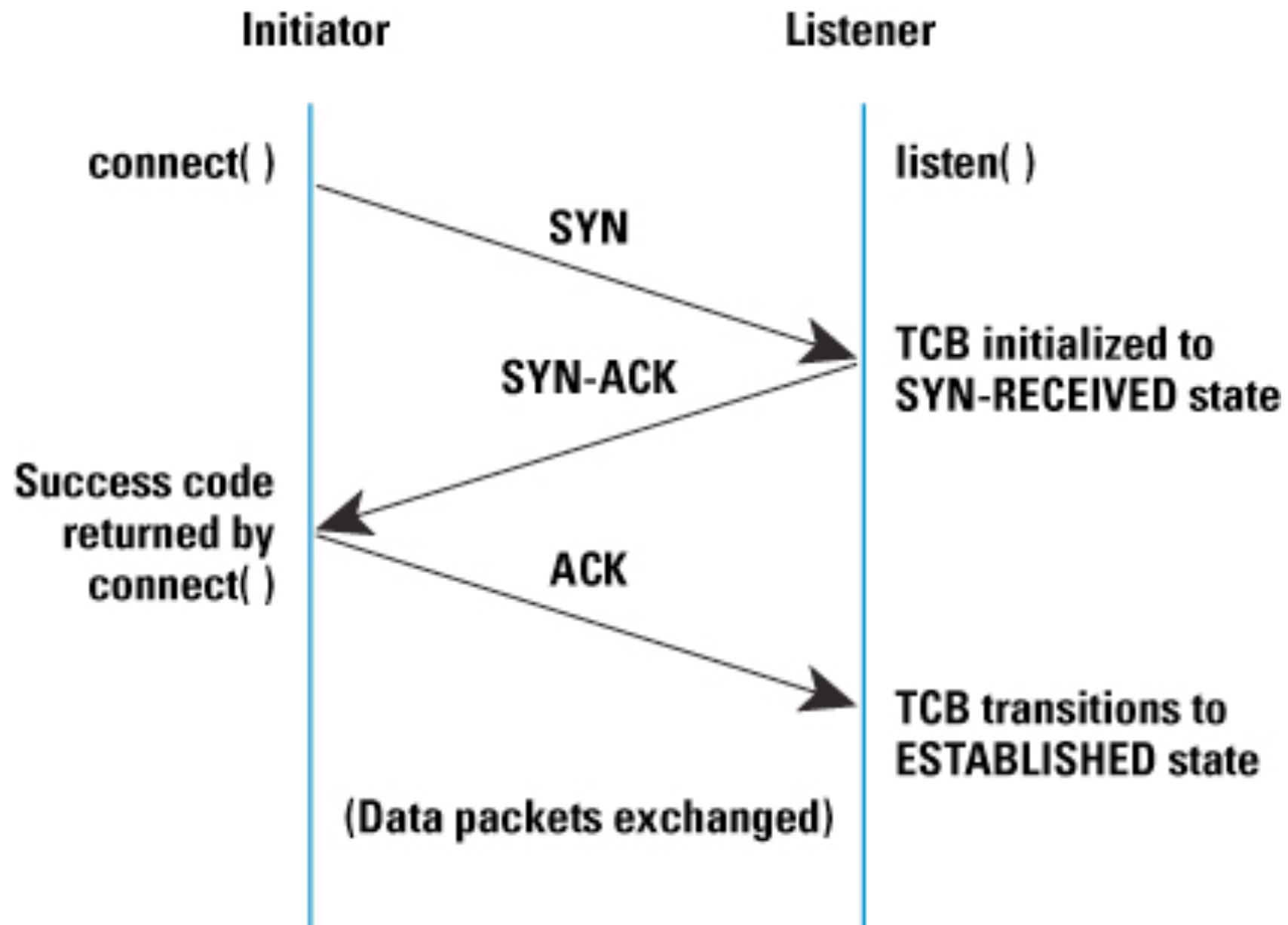
There are 65536 (0-65535/16 bits) possible ports.

A port that accepts connections is considered to be 'OPEN'. Conversely, a port that does not accept connections is considered to be 'CLOSED'.

It may be difficult to conclusively determine the status of a port.



- **Transmission Control Protocol (TCP)**
'guarantees' delivery of data/packets
(Examples: http, ssh, smtp).
- **User Datagram Protocol (UDP)**
provides 'best effort' delivery of data/packets
(Examples: dns, snmp, ntp).





1. Target Enumeration
2. Host Discovery
3. Reverse DNS Resolution
4. Port Scanning
5. Version Detection
6. OS Detection
7. Traceroute
8. Script Scanning
9. Output



- sn** find hosts that respond to ICMP, http, and/or https (No port scan)
- Pn** skips Nmap discovery stage altogether (No ping)
- PR** low-level local network host discovery (ARP scan)



```
# nmap -sn 172.28.128.0/24
```

```
Starting Nmap 7.40 ( https://nmap.org ) at 2017-07-09 14:55 EDT
```

```
Nmap scan report for 172.28.128.1
```

```
Host is up (0.00067s latency).
```

```
MAC Address: 0A:00:27:00:00:00 (Unknown)
```

```
Nmap scan report for 172.28.128.2
```

```
Host is up (0.00055s latency).
```

```
MAC Address: 08:00:27:32:B4:9C (Oracle VirtualBox virtual NIC)
```

```
Nmap scan report for 172.28.128.3
```

```
Host is up (0.00075s latency).
```

```
MAC Address: 08:00:27:24:AF:0A (Oracle VirtualBox virtual NIC)
```

```
Nmap scan report for 172.28.128.4
```

```
Host is up.
```

```
Nmap done: 256 IP addresses (4 hosts up) scanned in 2.04 seconds
```



- Parameter: **-sT**
- Can be used by an unprivileged user
- Completes the TCP Three Way Handshake
- Example: **nmap -sT scanme.nmap.org**



```
# nmap -sT 172.28.128.3
```

```
Starting Nmap 7.40 ( https://nmap.org ) at 2017-07-09 15:02 EDT
```

```
Nmap scan report for 172.28.128.3
```

```
Host is up (0.0010s latency).
```

```
Not shown: 977 closed ports
```

```
PORT      STATE SERVICE
```

```
21/tcp    open  ftp
```

```
22/tcp    open  ssh
```

```
23/tcp    open  telnet
```

```
MAC Address: 08:00:27:24:AF:0A (Oracle VirtualBox virtual NIC)
```

```
Nmap done: 1 IP address (1 host up) scanned in 0.21 seconds
```




- Parameter: **-sS**
- Must be a privileged user
- Sends the SYN packet, then waits for the SYN/ACK
- Faster than Connect Scan
- Example: **nmap -sS scanme.nmap.org**



```
# nmap -sS 172.28.128.3
```

```
Starting Nmap 7.40 ( https://nmap.org ) at 2017-07-09 15:04 EDT
```

```
Host is up (0.00035s latency).
```

```
Not shown: 977 closed ports
```

```
PORT      STATE SERVICE
```

```
21/tcp    open  ftp
```

```
22/tcp    open  ssh
```

```
23/tcp    open  telnet
```

```
MAC Address: 08:00:27:24:AF:0A (Oracle VirtualBox virtual NIC)
```

```
Nmap done: 1 IP address (1 host up) scanned in 0.23 seconds
```



- Parameter: **-sU**
- Must be a privileged user
- Only way to scan UDP Ports
- Recommend using **-sUV** in order to get more valuable results
- Example: **nmap -sUV scanme.nmap.org**



```
# nmap -sU 172.28.128.3
```

```
Starting Nmap 7.40 ( https://nmap.org ) at 2017-07-09 15:07 EDT
```

```
Host is up (0.00041s latency).
```

```
Not shown: 993 closed ports
```

PORT	STATE	SERVICE
------	-------	---------

53/udp	open	domain
--------	------	--------

68/udp	open filtered	dhcpc
--------	---------------	-------

69/udp	open filtered	tftp
--------	---------------	------

111/udp	open	rpcbind
---------	------	---------

137/udp	open	netbios-ns
---------	------	------------

138/udp	open filtered	netbios-dgm
---------	---------------	-------------

2049/udp	open	nfs
----------	------	-----

```
MAC Address: 08:00:27:24:AF:0A (Oracle VirtualBox virtual NIC)
```

```
Nmap done: 1 IP address (1 host up) scanned in 1070.89 seconds
```



- Parameters: **-sX** | **-sN**
- Must be a privileged user
- Exploits standards/RFCs
- Usually doesn't work against Windows
- Examples: **nmap -sX scanme.nmap.org**



```
# nmap -sX 172.28.128.3
```

Starting Nmap 7.40 (<https://nmap.org>) at 2017-07-09 16:32 EDT

Nmap scan report for 172.28.128.3

Host is up (0.00014s latency).

Not shown: 977 closed ports

PORT	STATE	SERVICE
------	-------	---------

21/tcp	open filtered	ftp
--------	---------------	-----

22/tcp	open filtered	ssh
--------	---------------	-----

23/tcp	open filtered	telnet
--------	---------------	--------

MAC Address: 08:00:27:24:AF:0A (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 1.56 seconds



```
# nmap -sN 172.28.128.3
```

Starting Nmap 7.40 (<https://nmap.org>) at 2017-07-09 16:34 EDT

Nmap scan report for 172.28.128.3

Host is up (0.00017s latency).

Not shown: 977 closed ports

PORT	STATE	SERVICE
------	-------	---------

21/tcp	open filtered	ftp
--------	---------------	-----

22/tcp	open filtered	ssh
--------	---------------	-----

23/tcp	open filtered	telnet
--------	---------------	--------

MAC Address: 08:00:27:24:AF:0A (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 1.56 seconds



- Parameter: **-sl**
- To the target it appears that the idle host is performing the port scan
- Stealth Scan
- Recommend disabling host discovery
- Example: **nmap -Pn -sl patsy.host target.host**



- Parameter: **-sV**
- Grabs and displays the service banners
- Increases the confidence in the identification of services
- Example: **nmap -sV scanme.nmap.org**



```
# nmap -sV 172.28.128.3
```

Starting Nmap 7.40 (<https://nmap.org>) at 2017-07-09 16:35 EDT

Nmap scan report for 172.28.128.3

Host is up (0.00066s latency).

Not shown: 977 closed ports

PORT	STATE	SERVICE	VERSION
------	-------	---------	---------

21/tcp	open	ftp	vsftpd 2.3.4
--------	------	-----	--------------

22/tcp	open	ssh	OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
--------	------	-----	--

23/tcp	open	telnet	Linux telnetd
--------	------	--------	---------------

MAC Address: 08:00:27:24:AF:0A (Oracle VirtualBox virtual NIC)

Service Info: Hosts: metasploitable.localdomain, localhost, irc.Metasploitable.LAN;

OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at <https://nmap.org/submit/> .

Nmap done: 1 IP address (1 host up) scanned in 12.00 seconds



- Parameter: **-O**
- Scans the target and attempts to detect the OS by comparing it to Nmap's OS fingerprint profiles
- Example: **nmap -O scanme.nmap.org**



```
# nmap -O 172.28.128.3
```

```
Starting Nmap 7.40 ( https://nmap.org ) at 2017-07-09 16:38 EDT
```

```
Nmap scan report for 172.28.128.3
```

```
Host is up (0.00033s latency).
```

```
Not shown: 977 closed ports
```

```
...
```

```
MAC Address: 08:00:27:24:AF:0A (Oracle VirtualBox virtual NIC)
```

```
Device type: general purpose
```

```
Running: Linux 2.6.X
```

```
OS CPE: cpe:/o:linux:linux_kernel:2.6
```

```
OS details: Linux 2.6.9 - 2.6.33
```

```
Network Distance: 1 hop
```

```
OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
```

```
Nmap done: 1 IP address (1 host up) scanned in 2.05 seconds
```



- Parameter: **-T(1-5)**
- Increase/Decrease scan speeds
- Faster scans may be unreliable
- Default speed is 3
- Might try slow scan speeds to 'hide' a port scan
- Example: **nmap -T4 scanme.nmap.org**



- Parameter: **--host-timeout 1m**
- Helpful with coping with latency
- Example: **nmap scanme.nmap.org --host-timeout 1m**



- Parameters: **-oN** | **-oX** | **-oS** | **-oG** | **-oA**
- Available Formats: Normal, XML, Script Kiddie, Grepable
- Can be used to feed other tools
- Example: **nmap -oN target.nmap target.host**



- An arbitrary scripting framework that allows users to trigger additional checks/actions based on certain open ports or services
- Added to NMAP through a Google Summer of Code in 2006
- There are over 500+ scripts included
- Example: **`nmap -p443 --script=ssl-enum-ciphers`**
`scanme.nmap.org`



```
# nmap -p443 --script=ssl-enum-ciphers cryptopartyutah.org
```

```
Starting Nmap 7.12 ( https://nmap.org ) at 2017-07-10 18:04 MDT
```

```
Nmap scan report for cryptopartyutah.org (107.170.219.231)
```

```
Host is up (0.047s latency).
```

```
PORT      STATE SERVICE
```

```
443/tcp open  https
```

```
| ssl-enum-ciphers:
```

```
| TLSv1.2:
```

```
|   ciphers:
```

```
|     TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (secp384r1) - A
```

```
|     TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (secp384r1) - A
```

```
|     TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (secp384r1) - A
```

```
|     TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (secp384r1) - A
```

```
|   compressors:
```

```
|     NULL
```

```
|   cipher preference: server
```

```
|_ least strength: A
```

```
Nmap done: 1 IP address (1 host up) scanned in 3.04 seconds
```



- NSE scripts define a list of categories they belong to.
- Currently defined categories are **auth**, **broadcast**, **brute**, **default**, **discovery**, **dos**, **exploit**, **external**, **fuzzer**, **intrusive**, **malware**, **safe**, **version**, and **vuln**.
- Scripts can/usually belong to more than one category



- Scripts are written in LUA
- Generally have three sections: **head**, **rule**, **action**
- Using the -d option flag can be useful when writing/ debugging scripts
- Over 120 standard libraries available



```
description = [[ A simple example NSE script ]]  
  
---  
--@output  
-- 22/tcp open  ssh  
-- |_simple-example: Open!  
  
author = "hydroplane"  
license = "Same as Nmap--See http://nmap.org/book/man-legal.html"  
categories = {'safe'}  
  
portrule = function(host, port)  
  return port.state == 'open'  
end  
  
action = function(host, port)  
  return 'Open!'  
end
```



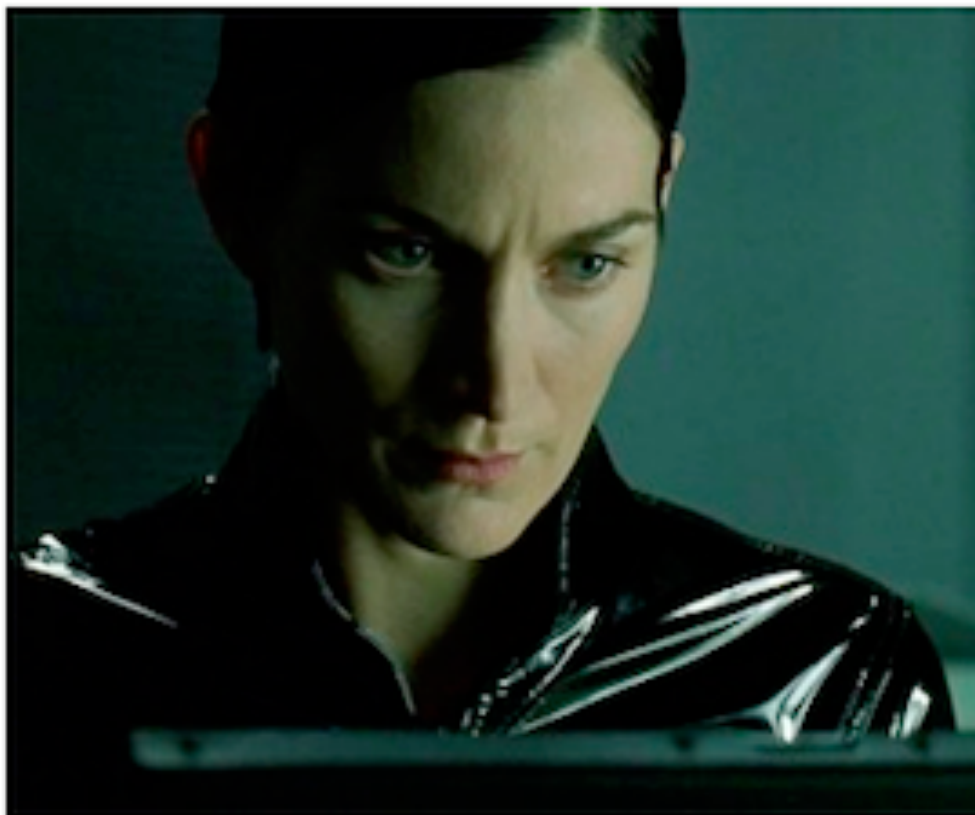
Practical Examples



- Homepage: **<https://nmap.org>**
- **Nmap Network Scanning**: The Official Nmap Project Guide to Network Discovery and Security Scanning (ISBN: 978-0979958717)
- **Nmap Essentials** (ISBN: 978-1783554065)
- **SANS Nmap Cheat Sheet**: <https://blogs.sans.org/pentesting/files/2013/10/NmapCheatSheetv1.0.pdf>



Questions?



```
80/tcp    open      http
81/tcp    open      hosts2.nc
10.0.0.0   [nobile]
11 # nmap -v -ss -O 10.2.2.2
11
13 Starting nmap V. 2.54BETA25
13 Insufficient responses for TCP sequencing (3). OS detection
13 accurate
14 Interesting ports on 10.2.2.2:
44 (The 1539 ports scanned but not shown below are in state: cl
51 Port      State      Service
51 22/tcp    open      ssh
58
68 No exact OS matches for host
68
24 Nmap run completed -- 1 IP address (1 host up) scanned
50 # sshnuke 10.2.2.2 -rootpw-"210N0101"
Connecting to 10.2.2.2:ssh ... successful.
Re Attempting to exploit SSHv1 CRC32 ... successful.
IP Resetting root password to "210N0101".
System open: Access Level (9)
10 # ssh 10.2.2.2 -l root
root@10.2.2.2's password: █
```