



Nmap: Beginner to advanced

By Adam Barns



What is Nmap

- A network scanning tool that supports multiple advanced techniques for network mapping
- Powerful and can be used to scan huge networks
- Portable and it runs on many different operating systems
- Well-documented by a vibrant community dedicated to keeping nmap great!
- Free!!



So why do we use it?

Information gathering is essential in any uni task, and in any real world engagement.

Nmap is easy to use... popular... and portable...

If you don't believe me, open up a terminal and type;

```
$ nmap -v -A <ip address>
```

```
# nmap -v -O <ip address>
```



Nmap: How to Scan

These are the basics...

```
nmap -v -sL <ip address range>
```

```
nmap -v -sn <ip address range>
```

```
nmap -v -O <ip address>
```

```
nmap -v -A <ip address>
```

```
nmap -v -iR <number of hosts to test>
```

```
nmap -v -sC <ip address>
```

```
nmap -v -sV <ip address>
```

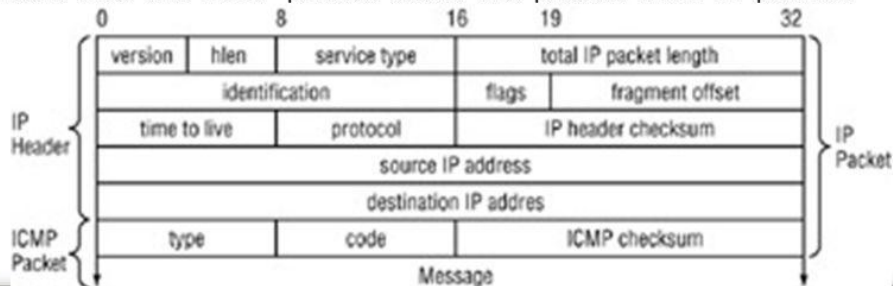
ICMP

The *Internet Control Message Protocol (ICMP)* is used to communicate with remote hosts on the network. Many popular network utilities, such as **ping** and **traceroute**, are based on ICMP.

ICMP was defined in **RFC 792** to allow network devices to report errors in datagram processing. ICMP is a robust means of communicating errors and network information among hosts.

ICMP uses **IP** to communicate across the network. The entire ICMP packet is then contained within the data section of the IP packet.

Figure shows how the ICMP packet fields are placed in an IP packet.




This is the ICMP protocol/packet used by default in nmap ping scans



For Intermediate Scans...

We can string together many of the queries to gain a multitude of information at once!

```
# nmap -v -sC -sV <ip address>
```



Nmap: The Intermediate Scans

There are also flags to add greater control and features to your scans!

`nmap -F <ip address>` (Scans fewer ports)

`nmap -sU <ip address>` (UDP scan)

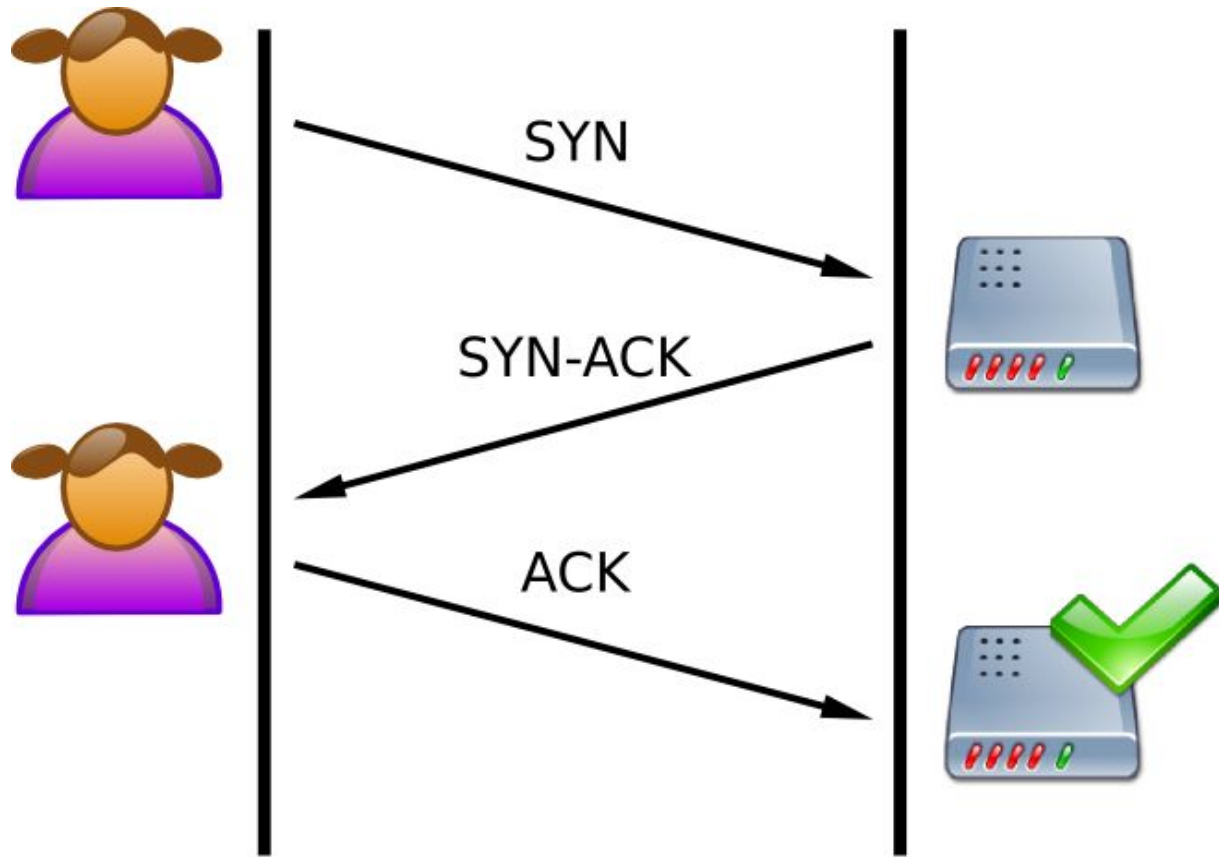
`nmap -p- <ip address>` (scan all 65k ports)

`nmap -S <ip address>` (Spoof from IP)

`nmap -T <0-5> <ip address>` (Set timing)

`nmap -n <ip address>` (no DNS)

`nmap -6 <ip address>` (IPv6 scan)

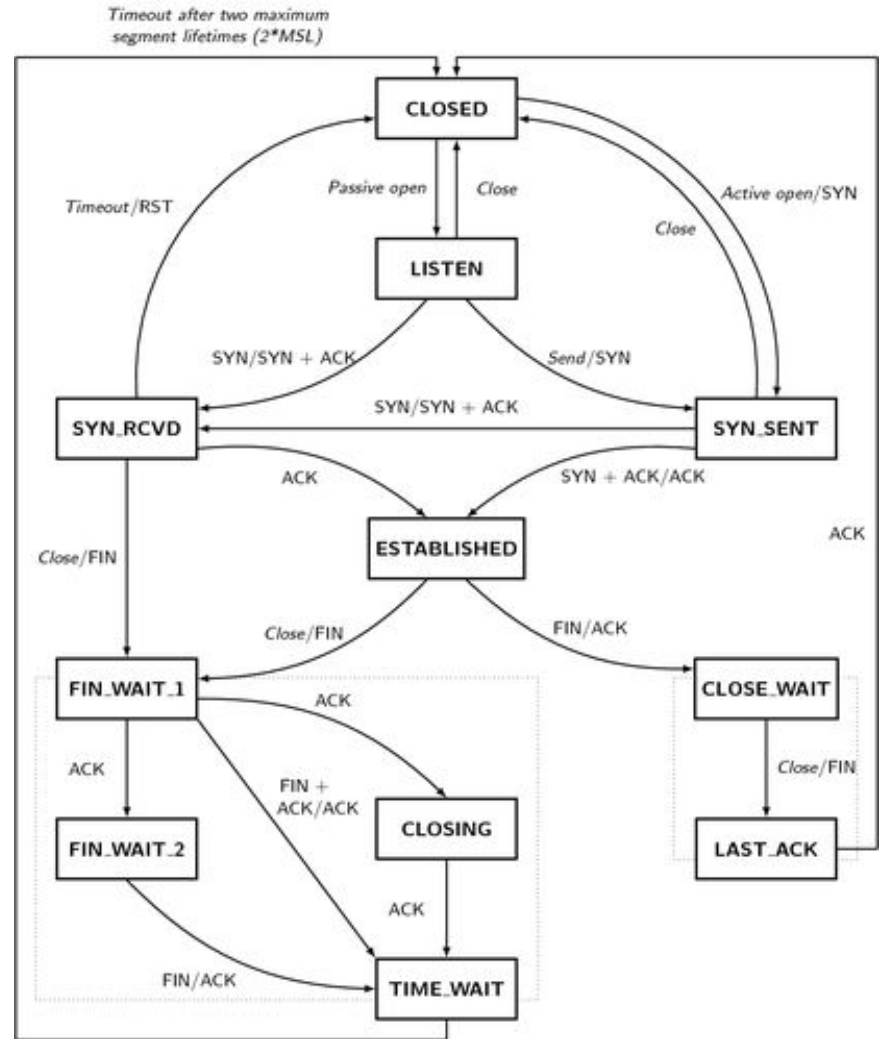


Simple 3-way handshake datagram

TCP

3-way handshake

This is the full life-cycle of the three way handshake.





There are advanced scans too...

`nmap -sS <ip address>` (stealth scan: taking advantage of TCP handshake and SYN packets and RST)


`nmap -sF <ip address>` (low chance of logs scan: only using FIN flags to avoid IDS/Firewalls)

`nmap -sN <ip address>` (lower chance still: only uses packets with no flags set to test response)

`nmap -sX <ip address>` (Xmas scan: sends FIN, URG and PUSH flags, read books for more info!)

`nmap -sA <ip address>` (ACK scan: to be used in conjunction with other scans to detect firewall rules)

These scans don't tend to work on windows targets. Source: <https://nmap.org/bennioston-tutorial/>



Advanced stealth techniques

These aren't always guaranteed to work but are a good starting point

```
nmap --scan-delay <time>
```

```
nmap --max-rate <number per second>
```

```
nmap -D <decoy ip address>
```

```
nmap --spoof-mac <mac address>
```

```
nmap -sl <zombie host [:probe port]>
```

```
Nmap --proxies <url/ip address>
```



The Advanced Scripting Engine... Or nse

To search for the scripts we will be using with nmap scripting engine, we type this command:

```
$ locate *.nse
```

OR:

```
$ locate *vuln*.nse (for vulnerability scanners only)
```



We can also get the help text for most scripts...

```
nmap --script-help <name of script>
```

Bonus:

You can output any of the scans we've looked at today into a file... Try this and see the results:

```
$ nmap -sS -A -n <target IP> -T4 -oS testnmap.txt
```

```
$ cat testnmap.txt
```