

Analysing Networks with NMAP



OWASP Ruhrpott Meetup
March 2019

Overview

- Networking Basics
- NMAP Basics
 - Scan types
 - Port states
 - Scan Speed
 - Output
 - Script Scans
- NSE Scripting
- NMAP Tool Suite

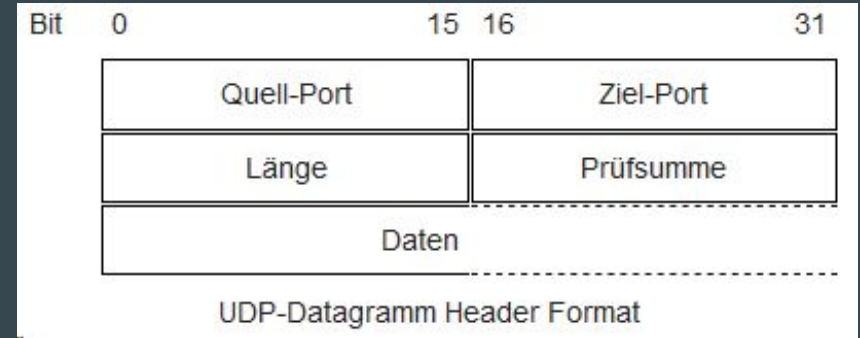
Networking Basics

Networking Basics - UDP

The User Datagram Protocol is:

- Minimalistic
- Stateless
- Unreliable
- Unordered
- Fast?

=> Best effort

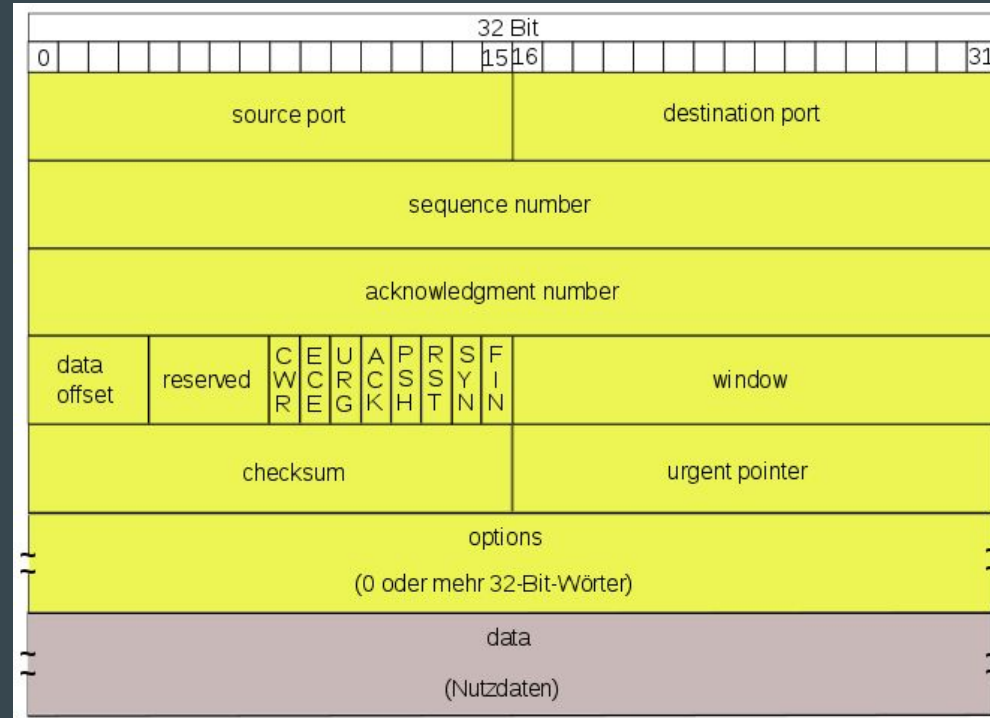


Networking Basics - TCP

The User Datagram Protocol is:

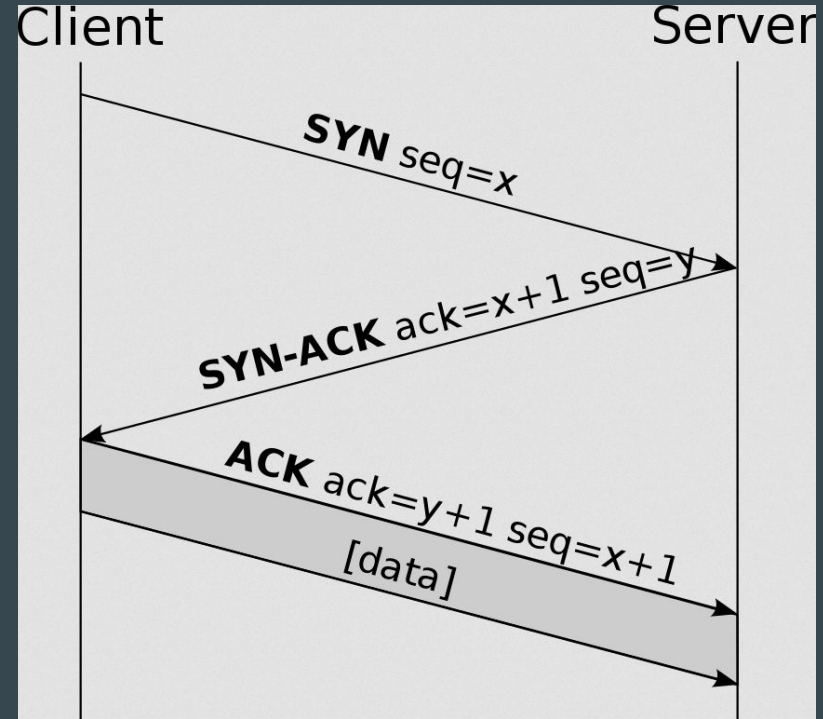
- Much overhead
- Stateful
- Reliable
- Ordered

=> Reliable Heavyweight



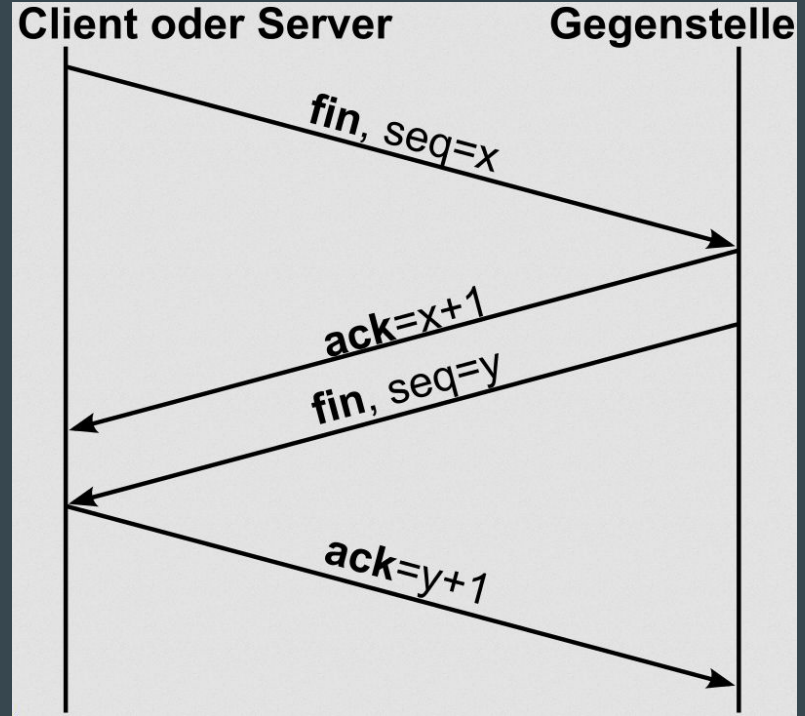
Networking Basics - TCP II - Handshake

- Formal handshake
- 3-Way-Handshake
- Parties are emancipated afterwards



Networking Basics - TCP III - Teardown

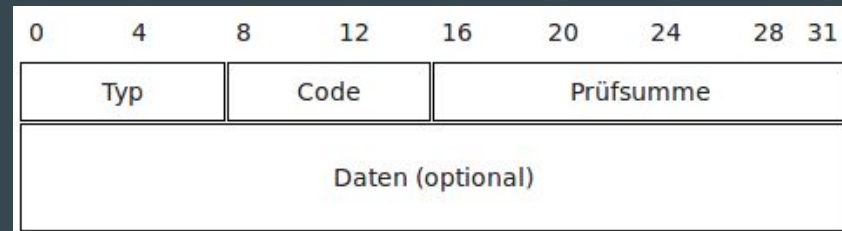
- TCP connections require teardown
- 4-Way-Handshake
- Closing party can no longer send data, but should still read incoming data.



Networking Basics - ICMP

The Internet Control Message Protocol is:

- Supporting protocol
- Not usually used to send data*
- Does things like:
 - ping
 - traceroute*



NMAP Basics

RISE AND SHINE GUYS.



IF YOU SCORED LAST NIGHT I NEED YOUR CONSENT FORMS.



NMAP Basics

```
context@build7R8: ~  
File Edit View Search Terminal Help  
[2019-03-12 09:41:40] ~ nmap scanme.nmap.org  
Starting Nmap 7.70 ( https://nmap.org ) at 2019-03-12 09:41 CET  
Nmap scan report for scanme.nmap.org (45.33.32.156)  
Host is up (0.20s latency).  
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f  
Not shown: 996 closed ports  
PORT      STATE SERVICE  
22/tcp    open  ssh  
80/tcp    open  http  
9929/tcp  open  nping-echo  
31337/tcp open  Elite  
  
Nmap done: 1 IP address (1 host up) scanned in 3.24 seconds  
[2019-03-12 09:41:51] ~
```

NMAP Basics - Default Privileges

Default NMAP behaviour depends on privileges:

- Privileged (root/Administrator*)
 - TCP SYN scan
- Unprivileged
 - TCP connect scan



NMAP Basics - Host Discovery

Several ways - different outcomes

- Ping scan (-sP):
 - `nmap -sP scanme.nmap.org`
- ICMP pings (-PE, -PP, -PM):
 - `nmap -PE scanme.nmap.org`
- ARP ping
 - `nmap -PR scanme.nmap.org`

Ultimative host discovery command (~93% detc):

- `nmap -PE -PS80 -PS443 -PP -PU40125 -PS3389 -PA21 -PU161 --source-port 53`

Hosts found Probe

```
62.47% -PE
44.17% -PS443
43.28% -PA80
43.01% -PA443
42.47% -PS80
40.65% -PA110
40.42% -PA3389
40.41% -PS110
39.89% -PA22
39.62% -PS21
39.62% -PA21
38.75% -PS22
37.50% -PS3389
36.66% -PP
31.17% -PU40125 --source-port 53 --data-length 24
29.96% -PU31338 --source-port 53 --data-length 24
29.05% -PU631 --source-port 53 --data-length 24
26.38% -PU40125
26.09% -PS25
```

NMAP Basics - Scan Types I

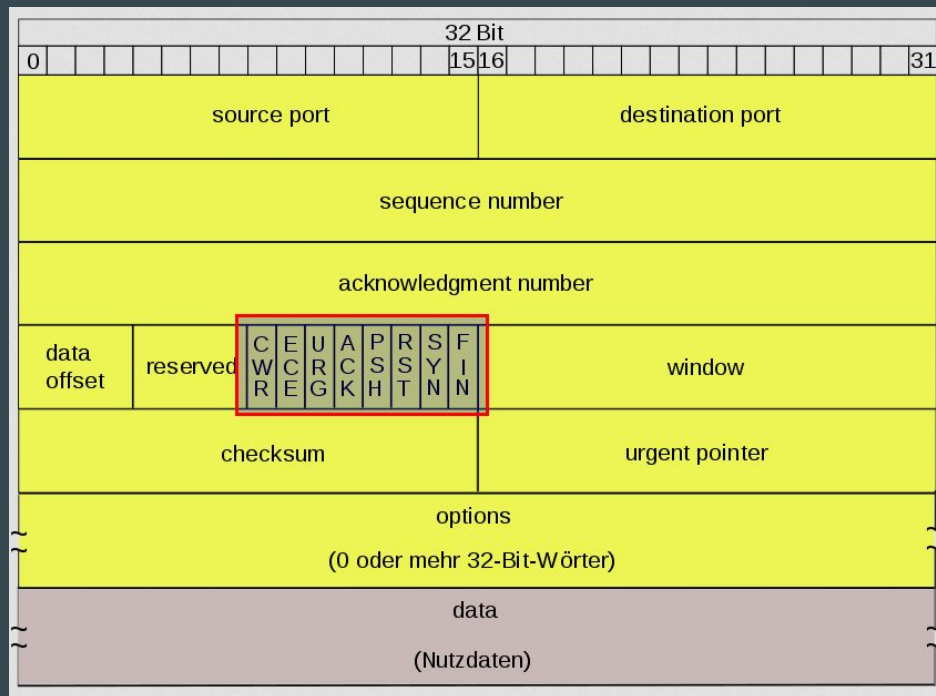
Scan types (most common):

- **TCP-SYN-Scan (-sS)**
 - Fast
 - Stealthy (?)
 - Requires privileges
- **TCP-Connect-Scan (-sT)**
 - Relies on OS
 - Slower than TCP-SYN-Scan
- **UDP-Scan (-sU)**
 - Slow
 - Unreliable

NMAP Basics - Scan Types II

More Scan Types:

- **TCP-NULL-Scan (-sN)**
 - None
- **TCP-FIN-Scan (-sF)**
 - FIN
- **TCP-Xmas-Scan (-sX)**
 - URG, PSH, FIN



NMAP Basics - Scan Types III

Even More Scan Types:

- **TCP-Idle-Scan (-sI) [Zombie]**
 - Spoofing packages
- **IP-Protocol-Scan (-sO)**
 - Enumerating IP Protocols

```
[2019-03-12 14:15:22] ~ sudo nmap -sO scanme.nmap.org
Starting Nmap 7.70 ( https://nmap.org ) at 2019-03-12 14:15 CET
Warning: 45.33.32.156 giving up on port because retransmission ca
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.16s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03
Not shown: 241 closed protocols
PROTOCOL STATE          SERVICE
1      open                  icmp
2      open|filtered         igmp
4      open|filtered         ipv4
6      open                  tcp
17     open                  udp
33     open|filtered         dccp
41     open|filtered         ipv6
47     open|filtered         gre
50     open|filtered         esp
51     open|filtered         ah
103    open|filtered         pim
108    open|filtered         ipcomp
132    open|filtered         sctp
136    open|filtered         udplite
137    open|filtered         mpls-in-ip

Nmap done: 1 IP address (1 host up) scanned in 371.73 seconds
```


NMAP Basics - Port States

NMAP distinguishes between different port states:

- open
 - “Proper” response received
- closed
 - RST received
- filtered
 - Something else happened
- open|filtered
 - Couldn't determine port state
 - often UDP related

NMAP Basics - Scan Speeds

Different Speed Settings (-T):

- paranoid (0)
- sneaky (1)
- polite (2)
- **normal (3) [default]**
- aggressive (4)
- insane (5)

```
[2019-03-12 15:11:45] ~ nmap -Pn -p22 -T paranoid scanme.nmap.org
Starting Nmap 7.70 ( https://nmap.org ) at 2019-03-12 15:11 CET
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.20s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:

PORT      STATE SERVICE
22/tcp    open  ssh

Nmap done: 1 IP address (1 host up) scanned in 300.54 seconds
```


```
[2019-03-12 15:16:59] ~ nmap -Pn -p22 -T5 scanme.nmap.org
Starting Nmap 7.70 ( https://nmap.org ) at 2019-03-12 15:19 CET
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.21s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f0

PORT      STATE SERVICE
22/tcp    open  ssh

Nmap done: 1 IP address (1 host up) scanned in 0.34 seconds
```

NMAP Basics - Target Syntax

Everything that isn't an option is considered a host :-)

- **Hostname:** `nmap scanme.nmap.org`
- **IP-Address:** `nmap 45.33.32.156`
- **CIDR-ish notation:**
 - `nmap 45.33.32.156/32`
 - `nmap scanme.nmap.org/32`
 - NOT `nmap 45.33.32.156/255.255.255.255`
- **Octet ranges:** `nmap 45.33.32-35.1-254` 

Everything above can be combined and loaded from a file as well (-iL)

NMAP Basics - Port Syntax

Ports are scanned in a (mostly) random order

- Scan top 100 ports only (“fast”, -F)
 - `nmap -F scanme.nmap.org`
- Scan “all” (1-65535) ports
 - `nmap -p- scanme.nmap.org`
- Scan all ports (0-65535)
 - `nmap -p0-65535 scanme.nmap.org`
- Scan specific ports and port ranges
 - `nmap -p 22,53,80,443,500-1000 scanme.nmap.org`

NMAP Basics - Output


- Normal (-oN)
- XML (-oX)
- Greppable (-oG)
- s|<rIpt kIddi3 (-oS)

```
Starting Nmap 7.70 ( https://Nmap.ORG ) at 2019-03-17 20:24 C3T
Nmap $can reP0rt F0r $Canm3.nMap.0rg (45.33.32.156)
Host |s Up (0.17z laTENcy).
Oth3r addr3$$ez f0r scanMe.nMap.0rg (n0t $CaNned): 2600:3c01::f03c:91ff:F318:bb2f
N0t $hown: 993 cl0S3d p0Rt$
p0Rt    $T4T3    $SERVICE
22/tcp  opEn      ssh
80/tcp  0p3n      http
135/tcp filter3d  m$rpc
139/tcp filter3d  nETb!0s-$Sn
445/tcp fIlt3r3D micR0$0Ft-dz
9929/tcp 0pEN      np!ng-ech0
31337/tcp opEn      3lit3

Nmap d0nE: 1 IP aDRr3$$s (1 host up) Scann3d 1n 182.12 S3c0ndS
```

The first three can be accessed with -oA

NMAP Basic - Misc. Switches

- Generate 100 random targets and log your crimes 
 - `nmap -iR 100 -Pn -oA admissible-evidence`
- IPv6 scan:
 - `nmap -6 scanme.nmap.org`
- Service version probing:
 - `nmap -sV scanme.nmap.org`
- OS detection:
 - `nmap -O scanme.nmap.org`
- Aggressive (-A) scan, includes OS and version detection, script scanning and traceroute:
 - `nmap -A scanme.nmap.org`

NMAP Basics - Script Scan I

More than just port scanning

- Script-Scan (-sC)
 - Equivalent to `--script=default`
- `--script` accepts:
 - Filename
 - Directory
 - Category
 - Expressions

```
[2019-03-12 15:19:20] nmap -sC scanme.nmap.org
Starting Nmap 7.70 ( https://nmap.org ) at 2019-03-12 16:12 CET
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.16s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03
Not shown: 996 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
| ssh-hostkey:
|   1024 ac:00:a0:1a:82:ff:cc:55:99:dc:67:2b:34:97:6b:75 (DSA)
|   2048 20:3d:2d:44:62:2a:b0:5a:9d:b5:b3:05:14:c2:a6:b2 (RSA)
|   256 96:02:bb:5e:57:54:1c:4e:45:2f:56:4c:4a:24:b2:57 (ECDSA)
|_  256 33:fa:91:0f:e0:e1:7b:1f:6d:05:a2:b0:f1:54:41:56 (ED25519)
80/tcp    open  http
|_ http-title: Go ahead and ScanMe!
9929/tcp  open  nping-echo
31337/tcp open  Elite
```

NMAP Basics - Script Scan II

Script Categories:

- auth
- broadcast
- brute
- discovery
- dos
- exploit
- external
- fuzzer
- intrusive
- malware
- safe
- version
- vuln

Expressions are supported:

- `--script="default or save"`
- `--script="(default and save) and not http-*`

NSE Scripting

NSE Scripting I

Four Classes of Scripts:

- Service scripts
 - Executed once per port
- Host scripts
 - Executed once per host
- Pre-rule script
 - Executed prior any scan
- Post-rule script
 - Executed after all scans

NSE Scripting - Example http-title

```
author = "Diman Todorov"
license = "Same as Nmap--See https://nmap.org/book/man-legal.html"
categories = {"default", "discovery", "safe"}

portrule = shortport.http
action = function(host, port)
  local resp, redirect_url, title
  resp = http.get( host, port, stdnse.get_script_args(SCRIPT_NAME..".url") or "/" )

  -- check for a redirect
  if resp.location then
    end

  if ( not(resp.body) ) then
    end

  -- try and match title tags
  title = string.match(resp.body, "<[Tt][Ii][Tt][Ll][Ee][^>]*(<[^<]*></[Tt][Ii][Tt][Ll][Ee]>")
  local display_title = title

  if display_title and display_title ~= "" then
  else
    end
  local output_tab = stdnse.output_table()
  output_tab.title = title
  output_tab.redirect_url = redirect_url

  local output_str = display_title
  if redirect_url then
    output_str = output_str .. "\n" .. ("Requested resource was %s"):format( redirect_url )
  end
  return output_tab, output_str
end
```

<https://svn.nmap.org/nmap/scripts/http-title.nse>

NMAP Tool Suite

NMAP Tool Suite - ncat

- Netcat (nc) alternative
 - Supports SSL
 - Supports IPv6
 - Proxying

```
balthasar:~ # ncat -v --ssl google.com 443
Ncat: Version 7.70 ( https://nmap.org/ncat )
Ncat: SSL connection to 216.58.207.78:443. Google LLC
Ncat: SHA-1 fingerprint: F81E 3171 FA08 5BC0 4C83 B664 489F 229F 0CBA 8E57
GET / HTTP/1.1

HTTP/1.1 200 OK
Date: Sun, 17 Mar 2019 18:10:57 GMT
Expires: -1
Cache-Control: private, max-age=0
Content-Type: text/html; charset=ISO-8859-1
P3P: CP="This is not a P3P policy! See g.co/p3phelp for more info."
Server: gws
X-XSS-Protection: 1; mode=block
X-Frame-Options: SAMEORIGIN
Set-Cookie: 1P_JAR=2019-03-17-18; expires=Tue, 16-Apr-2019 18:10:57 GMT; path=/; domain=.google.com
Set-Cookie: NID=179=PojweaI57Awb_bHlh7pRzW9rc_UDUMR-sgKPCLOGCzkJRh7sYk6BLWwL3qDU7CNoy7eLN90dEvx_6Vbai-ft9KVkl0nq0M4WQZ4Tat
j4J2oKQxJQZgaZfiDGZZ2qixe1_AGmfY_wk4Cun28vRJj_ly9rdGRJyuGXteWI06DyMA; expires=Mon, 16-Sep-2019 18:10:57 GMT; path=/; domain
=.google.com; HttpOnly
Alt-Svc: quic=":443"; ma=2592000; v="46,44,43,39"
Accept-Ranges: none
Vary: Accept-Encoding
Transfer-Encoding: chunked
```

Further reading:

- <https://nmap.org/ncat/guide/ncat-tricks.html>
- <http://alexcreek.com/ncat-cheatsheet.html>

NMAP Tool Suite - ndiff

- Compares scans
- Takes in two XML files

```
[2019-03-18 14:10:26] < ~ ndiff scan2.xml scan3.xml
-Nmap 7.70 scan initiated Mon Mar 18 14:01:51 2019 as: nmap -p- -T4 -A -oA scan2
+Nmap 7.70 scan initiated Mon Mar 18 14:05:34 2019 as: nmap -p- -T4 -A -oA scan3

-scanme.nmap.org (45.33.32.156):
-Host is up.
-Not shown: 65531 closed ports
-PORT      STATE SERVICE      VERSION
-22/tcp    open  ssh          OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.11 (Ubuntu Linux; pr
-|_ ssh-hostkey:
-|_   1024 ac:00:a0:1a:82:ff:cc:55:99:dc:67:2b:34:97:6b:75 (DSA)
-|_   2048 20:3d:2d:44:62:2a:b0:5a:9d:b5:b3:05:14:c2:a6:b2 (RSA)
-|_   256 96:02:bb:5e:57:54:1c:4e:45:2f:56:4c:4a:24:b2:57 (ECDSA)
-|_   256 33:fa:91:0f:e0:e1:7b:1f:6d:05:a2:b0:f1:54:41:56 (ED25519)
-80/tcp    open  http         Apache httpd 2.4.7 ((Ubuntu))
-|_ http-server-header: Apache/2.4.7 (Ubuntu)
-|_ http-title: Go ahead and ScanMe!
-9929/tcp  open  nping-echo   Nping echo
-31337/tcp open  tcpwrapped

-OS details:
- Linux 3.10 - 4.11
- Linux 3.2 - 4.9
- Linux 3.16 - 4.6
- Linux 2.6.32 - 3.13
- Linux 4.10
- Linux 2.6.22 - 2.6.36
- Linux 3.10
- Linux 4.4
- Linux 2.6.32
- Linux 2.6.32 - 3.10

+ack.nmap.org, www.nmap.org (45.33.49.119):
+Host is up.
+Not shown: 65528 filtered ports
+PORT      STATE SERVICE      VERSION
+22/tcp    open  ssh          OpenSSH 7.4 (protocol 2.0)
+|_ ssh-hostkey:
+|_   2048 48:e0:c6:cd:14:00:00:db:b6:b0:3d:f2:0a:2a:3b:6d (RSA)
+|_   256 88:2b:29:00:d0:c7:81:ac:dd:f4:90:42:d2:aa:f0:5b (ECDSA)
```

NMAP Tool Suite - nping

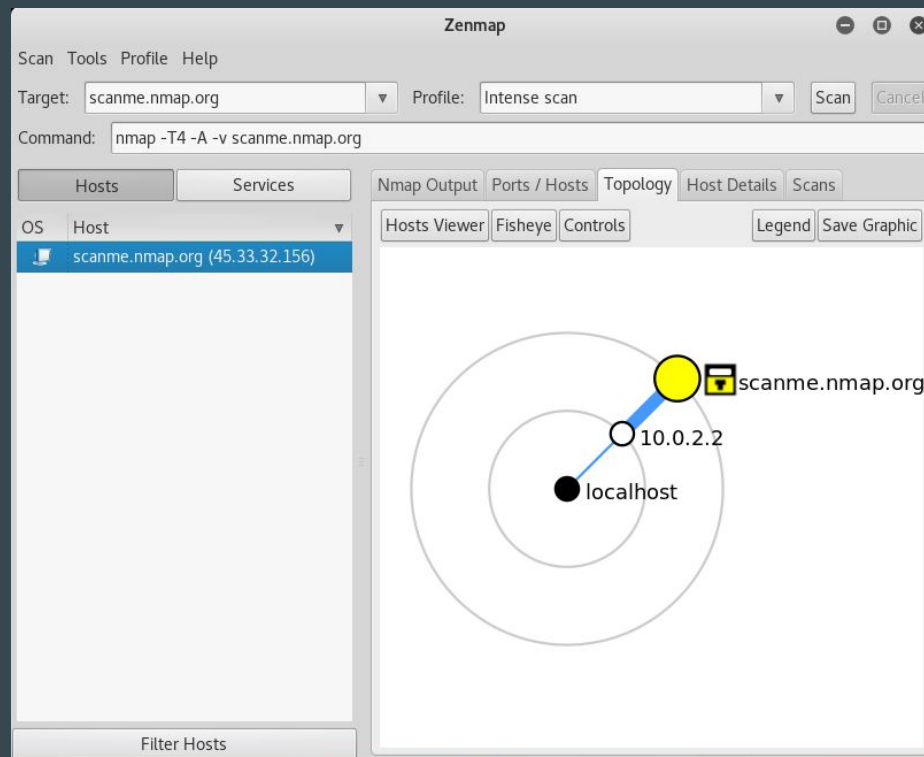
- Network packet generator
- Response analysis
- Response time measurement.
- Also does ping :-)

```
balthasar:~ # nping --echo-client "public" echo.nmap.org --udp
Starting Nping 0.7.70 ( https://nmap.org/nping ) at 2019-03-17 19:19 CET
SENT (1.7587s) UDP 192.168.178.48:53 > 45.33.32.156:40125 ttl=64 id=47777 iplen=28
CAPT (1.8941s) UDP 91.58.198.165:53 > 45.33.32.156:40125 ttl=57 id=47777 iplen=28
RCVD (2.1479s) ICMP [45.33.32.156 > 192.168.178.48 Port unreachable (type=3/code=3) ] IP [ttl=56 id=58344 iplen=56 ]
SENT (2.7594s) UDP 192.168.178.48:53 > 45.33.32.156:40125 ttl=64 id=47777 iplen=28
CAPT (2.8553s) UDP 91.58.198.165:53 > 45.33.32.156:40125 ttl=57 id=47777 iplen=28
RCVD (2.9634s) ICMP [45.33.32.156 > 192.168.178.48 Port unreachable (type=3/code=3) ] IP [ttl=56 id=58384 iplen=56 ]
SENT (3.7623s) UDP 192.168.178.48:53 > 45.33.32.156:40125 ttl=64 id=47777 iplen=28
CAPT (3.8686s) UDP 91.58.198.165:53 > 45.33.32.156:40125 ttl=57 id=47777 iplen=28
RCVD (3.9874s) ICMP [45.33.32.156 > 192.168.178.48 Port unreachable (type=3/code=3) ] IP [ttl=56 id=58668 iplen=56 ]
SENT (4.7644s) UDP 192.168.178.48:53 > 45.33.32.156:40125 ttl=64 id=47777 iplen=28
CAPT (4.8818s) UDP 91.58.198.165:53 > 45.33.32.156:40125 ttl=57 id=47777 iplen=28
RCVD (5.0078s) ICMP [45.33.32.156 > 192.168.178.48 Port unreachable (type=3/code=3) ] IP [ttl=56 id=58691 iplen=56 ]
SENT (5.7678s) UDP 192.168.178.48:53 > 45.33.32.156:40125 ttl=64 id=47777 iplen=28
CAPT (5.8955s) UDP 91.58.198.165:53 > 45.33.32.156:40125 ttl=57 id=47777 iplen=28
RCVD (6.0275s) ICMP [45.33.32.156 > 192.168.178.48 Port unreachable (type=3/code=3) ] IP [ttl=56 id=58825 iplen=56 ]

Max rtt: 388.931ms | Min rtt: 201.544ms | Avg rtt: 262.352ms
Raw packets sent: 5 (140B) | Rcvd: 5 (280B) | Lost: 0 (0.00%) | Echoed: 5 (230B)
Nping done: 1 IP address pinged in 6.81 seconds
```

NMAP Tool Suite - zenmap

- GUI for NMAP
- Quick profile selection
- Graphical organisation
- Topology



Training with NMAP

Training with NMAP

Don't go wandering off, scanning networks without consent!

This could get you into trouble. Things could break, people could sue you.

To experiment with NMAP use:

- Dedicated hosts like scanme.nmap.org,
- Dedicated lab environments (e.g. Hack-in-the-Box),
- Your own network (NOT the hotel WiFi, NOT your friends WiFi!)
- Virtual machines with interesting services (e.g. metasploitable)

Metasploitable v2: <https://sourceforge.net/projects/metasploitable/files/latest/download>

Analysing Networks with NMAP

Questions?