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

[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):
  o  nmap -sP scanme.nmap.org
- ICMP pings (-PE, -PP, -PM):
  o  nmap -PE scanme.nmap.org
- ARP ping
  o  nmap -PR scanme.nmap.org

Ultimative host discovery command (~93% detc):

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

<table>
<thead>
<tr>
<th>Hosts found Probe</th>
</tr>
</thead>
<tbody>
<tr>
<td>62.47% -PE</td>
</tr>
<tr>
<td>44.17% -PS443</td>
</tr>
<tr>
<td>43.28% -PA80</td>
</tr>
<tr>
<td>43.01% -PA443</td>
</tr>
<tr>
<td>42.47% -PS80</td>
</tr>
<tr>
<td>40.65% -PA110</td>
</tr>
<tr>
<td>40.42% -PA3389</td>
</tr>
<tr>
<td>40.41% -PS110</td>
</tr>
<tr>
<td>39.89% -PA22</td>
</tr>
<tr>
<td>39.62% -PS21</td>
</tr>
<tr>
<td>39.62% -PA21</td>
</tr>
<tr>
<td>38.75% -PS22</td>
</tr>
<tr>
<td>37.50% -PS3389</td>
</tr>
<tr>
<td>36.66% -PP</td>
</tr>
<tr>
<td>31.17% -PU40125</td>
</tr>
<tr>
<td>30.96% -PU3338</td>
</tr>
<tr>
<td>29.05% -PU631</td>
</tr>
<tr>
<td>26.38% -PU40125</td>
</tr>
<tr>
<td>26.09% -PS25</td>
</tr>
</tbody>
</table>
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 caused
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  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)
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)

The first three can be accessed with -oA
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
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

```plaintext

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
  end

  if ( not(resp.body) ) then
    end
  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
      local output_tab = stdnse.output_table()
      output_tab.title = title
      output_tab.redirect_url = redirect_url
      output_tab.redirect_url = redirect_url

      local output_str = display_title
      if redirect_url then
        output_str = output_str .. "\n" .. ("Requested resource was %s")%redirect_url
      end
      return output_tab, output_str
  end
```
NMAP Tool Suite
NMAP Tool Suite - ncat

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

Further reading:

NMAP Tool Suite - ndiff

- Compares scans
- Takes in two XML files
NMAP Tool Suite - nping

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