cesnet

NMAP: JEDEN ZE SÍŤAŘOVÝCH ŠVÝCARSKÝCH NOŽŮ

Tomáš Čejka

CESNET, z.s.p.o. / FIT ČVUT v Praze

3. 3. 2018, InstallFest, Praha

Zdroje informací

- Gordon “Fyodor” Lyon: NMAP Network Scanning (book)
- `man nmap`
- `https://nmap.org/book/man.html`
- `https://nmap.org/nsedoc/`

Síťové Protokoly

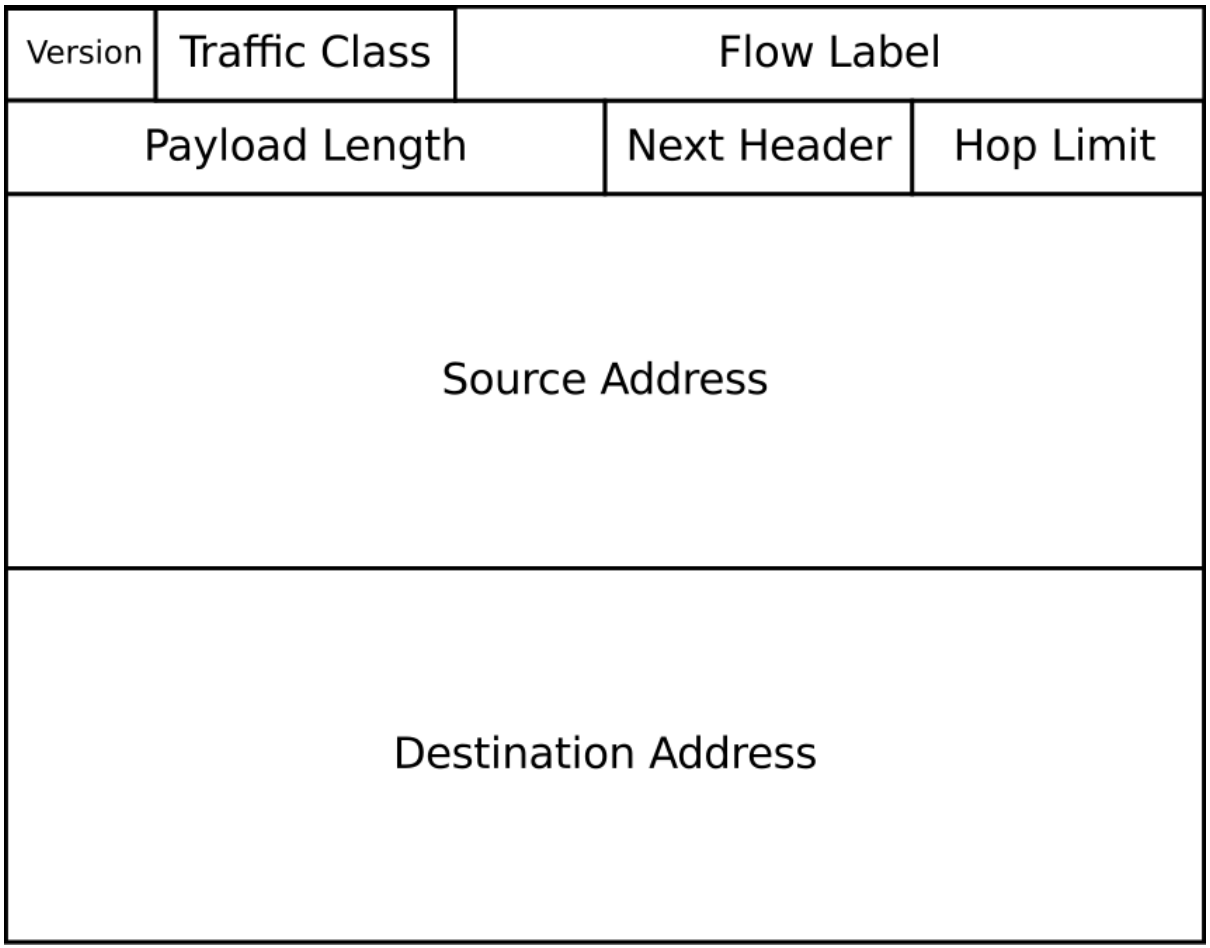
Internet Protocol I

https://wikipedia.org/wiki/IPv4

Offsets	0								1								2								3							
Octet	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
0	Version				IHL				DSCP						ECN		Total Length															
4	Identification																Flags			Fragment Offset											
8	Time To Live								Protocol								Header Checksum															
12	Source IP Address																															
16	Destination IP Address																															
20	Options (if IHL > 5)																															
24																																
28																																
32																																

Internet Protocol II

https://wikipedia.org/wiki/IPv6



User Datagram Protocol

Offsets	Octet	0								1								2								3							
Octet	Bit	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
0	0	Source port																Destination port														
4	32	Length																Checksum														

Wireshark:

```
▸ Frame 40: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface 0
▸ Ethernet II, Src: IntelCor_3a:71:a9 (f4:06:69:3a:71:a9), Dst: CzNicZSP_00:0e:df (d8:
▸ Internet Protocol Version 4, Src: 192.168.1.153, Dst: 192.168.1.1
▸ User Datagram Protocol, Src Port: 37640, Dst Port: 53
▸ Domain Name System (query)

0000  d8 58 d7 00 0e df f4 06  69 3a 71 a9 08 00 45 00   .X...... i:q...E.
0010  00 34 ed 76 00 00 40 11  09 58 c0 a8 01 99 c0 a8   .4.v..@. .X......
0020  01 01 93 08 00 35 00 20  19 ec 00 6e 01 00 00 01   .....5.  ...n....
0030  00 00 00 00 00 00 03 61  62 63 02 64 65 00 00 01   .......a bc.de...
0040  00 01                                             ..
```

UDP: princip

Transmission Control Protocol

https://wikipedia.org/wiki/Transmission_Control_Protocol

Offsets	Octet	0								1								2								3							
Octet	Bit	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
0	0	Source port																Destination port															
4	32	Sequence number																															
8	64	Acknowledgment number (if ACK set)																															
12	96	Data offset				Reserved 0 0 0				NS	CWR	ECE	URG	ACK	PSH	RST	SYN	FIN	Window Size														
16	128	Checksum																Urgent pointer (if URG set)															
20 ...	160 ...	Options (if *data offset* > 5. Padded at the end with "0" bytes if necessary.) ...																															

Wireshark:

```
▸ Frame 61: 655 bytes on wire (5240 bits), 655 bytes captured (5240 bits) on interface 0
▸ Ethernet II, Src: IntelCor_3a:71:a9 (f4:06:69:3a:71:a9), Dst: Giga-Byt_bd:60:d9 (1c:1b:0d:bd:
▸ Internet Protocol Version 4, Src: 192.168.1.153, Dst: 192.168.1.230
▸ Transmission Control Protocol, Src Port: 42470, Dst Port: 80, Seq: 714, Ack: 1128, Len: 589
▸ Hypertext Transfer Protocol

0000  1c 1b 0d bd 60 d9 f4 06  69 3a 71 a9 08 00 45 00   ....`... i:q...E.
0010  02 81 69 94 40 00 40 06  4a 13 c0 a8 01 99 c0 a8   ..i.@.@. J.......
0020  01 e6 a5 e6 00 50 f6 c5  0f a0 d3 52 5a 1a 80 18   .....P.. ...RZ...
0030  03 82 49 2e 00 00 01 01  08 0a 25 53 b4 05 5d e9   ..I..... ..%S..].
0040  24 63 47 45 54 20 2f 6f  63 73 2f 76 32 2e 70 68   $cGET /o cs/v2.ph
0050  70 2f 61 70 70 73 2f 6e  6f 74 69 66 69 63 61 74   p/apps/n otificat
```

TCP: Navázání spojení

Internet Control Message Protocol

https://wikipedia.org/wiki/Internet_Control_Message_Protocol

Offsets	Octet	0								1								2								3							
Octet	Bit	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
0	0	Type								Code								Checksum															
4	32	Rest of Header																															

Wireshark:

```
▸ Frame 4: 102 bytes on wire (816 bits), 102 bytes captured (816 bits) on interface 0
▸ Ethernet II, Src: 00:00:00_00:00:00 (00:00:00:00:00:00), Dst: 00:00:00_00:00:00 (00:00
▸ Internet Protocol Version 4, Src: 127.0.0.1, Dst: 127.0.0.1
▾ Internet Control Message Protocol
    Type: 3 (Destination unreachable)
    Code: 3 (Port unreachable)
    Checksum: 0x949f [correct]
    [Checksum Status: Good]
    Unused: 00000000
  ▸ Internet Protocol Version 4, Src: 127.0.0.1, Dst: 127.0.0.1
  ▸ Transmission Control Protocol, Src Port: 43344, Dst Port: 11111, Seq: 1905694606
```

```
0000  00 00 00 00 00 00 00 00  00 00 00 00 08 00 45 d0   ........ ......E.
0010  00 58 52 b5 00 00 40 01  29 1e 7f 00 00 01 7f 00   .XR...@. ).......
0020  00 01 03 03 94 9f 00 00  00 00 45 10 00 3c 48 45   ........ ..E..<HE
0030  40 00 40 06 f4 64 7f 00  00 01 7f 00 00 01 a9 50   @.@..d.. .......P
0040  2b 67 71 96 97 8e 00 00  00 00 a0 02 aa aa fe 30   +gq..... .......0
0050  00 00 02 04 ff d7 04 02  08 0a e7 ad 48 02 00 00   ........ ....H...
0060  00 00 01 03 03 07                                 ......
```

nmap

Varování!!!

Pozor! Skenování může mít vážné následky!

- Skenovat cizí síť/zařízení se **nedoporučuje**
- V minulosti se některé případy objevili u soudu…
- …existují různé názory:

"Port Scanning is not Crime"

- Každopádně je jistější mít povolení od vlastníka:

`scanme.nmap.org` ;-)

nmap (Network Mapper)

- Umožňuje testovat dostupnost zařízení
  (ICMP echo, ARP dotaz, navázání komunikace)
- Překládá doménová jména a IP adresy
- Testuje „porty“, na kterých cíl odpovídá
  (nebo se aspoň vrátí „ICMP chyba“)
- Zjišťuje operační systém (databáze otisků) (`-O`)
  `/usr/share/nmap/nmap-os-db`
- Zjišťuje aplikaci, která na portu poslouchá (`-sV`)
  `/usr/share/nmap/nmap-service-probes`
  `/usr/share/nmap/nmap-payloads`
- Zkouší, které protokoly jsou povolené (`-sO`)
  `/usr/share/nmap/nmap-protocols`
- Spouští skripty (`-sC`, `--script`)
- a další...

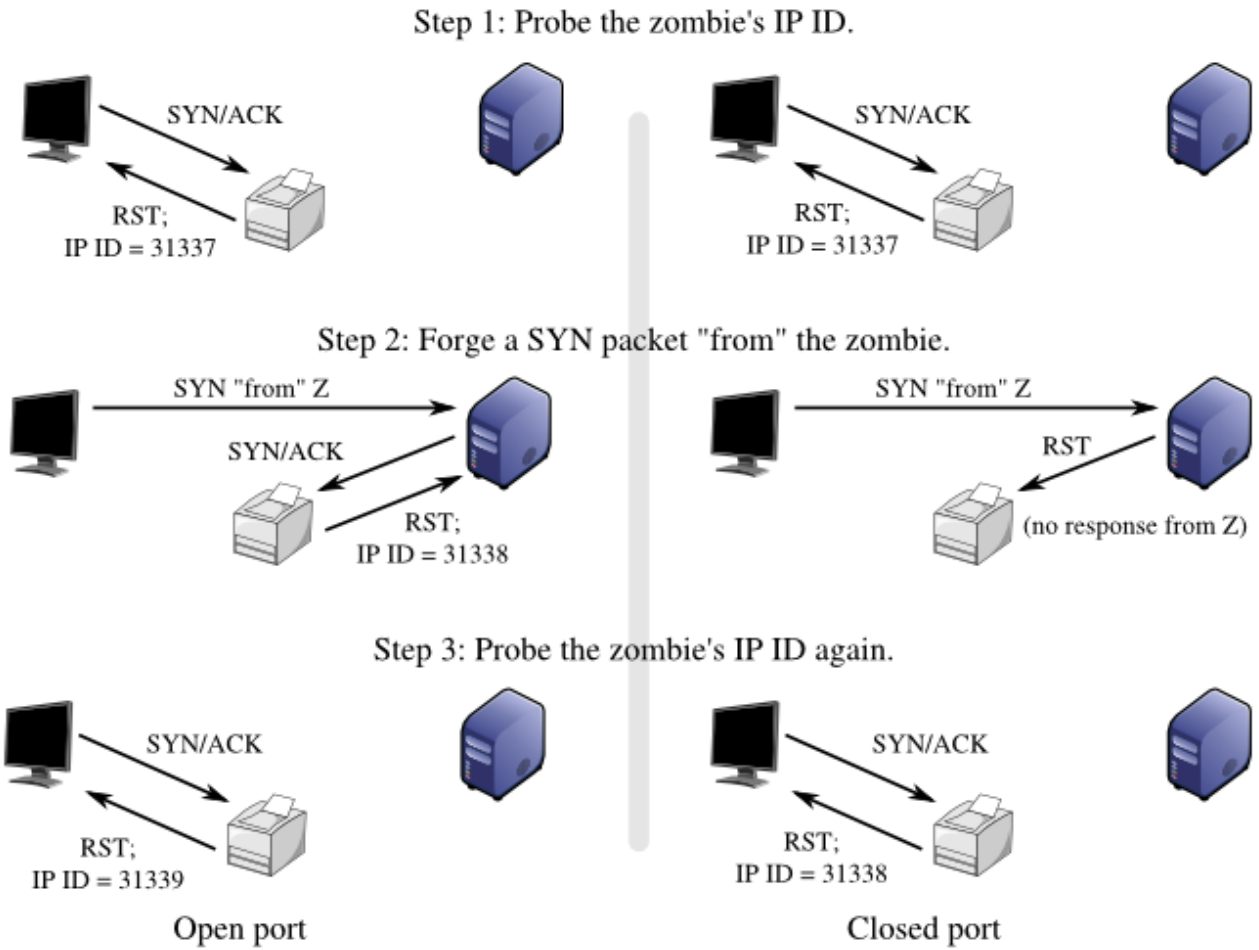
Skenování portů

- Připojování k portům, jako běžná aplikace (`-sT`)
  funguje i bez root oprávnění
- SYN scan (`-sS`) pošle se jen SYN paket, ale ACK už ne $\longrightarrow$ polootevřené spojení
- různé kombinace TCP příznaků (ACK, FIN, NULL, Xmas: FIN|PSH|URG) (`-sA` | `-sF` | `-sN` | `-sX`)
- Window scan (`-sW`)
- UDP scan (`-sU`)
- Idle scan (`-sI`)
  využívá predikovatelnosti IP ID u některých OS

Idle scan (-sI)

„David's wiki | Nmap“:

`https://www.bamsoftware.com/wiki/Nmap/IdleScanDiagrams`



Detekce operačního systému

Různé systémy reagují různě. Seznam známých „otisků“ systému `/usr/share/nmap/nmap-os-db`.

```
Fingerprint OpenWrt Chaos Calmer 15.05 (Linux 3.18)
Class Linux | Linux | 3.X | broadband router
CPE cpe:/o:linux:linux_kernel:3.18 auto
SEQ(SP=102-10C%GCD=1-6%ISR=103-10D%TI=Z%CI=I%TS=7)
OPS(O1=M5B4ST11NW2%O2=M5B4ST11NW2%O3=M5B4NNT11NW2%O4=
    M5B4ST11NW2%O5=M5B4ST11NW2%O6=M5B4ST11)
WIN(W1=7120%W2=7120%W3=7120%W4=7120%W5=7120%W6=7120)
ECN(R=Y%DF=Y%T=3B-45%TG=40%W=7210%O=M5B4NNSNW2%CC=N%Q=)
T1(R=Y%DF=Y%T=3B-45%TG=40%S=O%A=S+%F=AS%RD=0%Q=)
T2(R=N)
T3(R=N)
T4(R=Y%DF=Y%T=3B-45%TG=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)
T5(R=Y%DF=Y%T=3B-45%TG=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)
T6(R=Y%DF=Y%T=3B-45%TG=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)
T7(R=N)
U1(DF=N%T=3B-45%TG=40%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%
    RUCK=G%RUD=G)
IE(DFI=N%T=3B-45%TG=40%CD=S)
```

Detekce verze aplikace

Nmap (`-sV`) kontroluje, jaká data přichází od aplikace.
Opět existuje seznam:
`/usr/share/nmap/nmap-service-probes`

```
match ssh m|^SSH-([\d.]+)-OpenSSH_([\w._-]+)[ -]{1,2}
    Debian[ -_]([^\r\n]+)\r?\n| p/OpenSSH/ v/$2 Debian
    $3/ i/protocol $1/ o/Linux/ cpe:/a:openbsd:openssh:
    $2/ cpe:/o:debian:debian_linux/ cpe:/o:linux:
    linux_kernel/a
```

Ukázka:

```
Nmap scan report for nas (192.168.1.230)
Host is up (0.0017s latency).
PORT    STATE  SERVICE VERSION
22/tcp  open   ssh     OpenSSH 6.7p1 Debian 5+deb8u3 (
    protocol 2.0)
80/tcp  open   http    nginx
443/tcp closed https
MAC Address: 1C:1B:0D:BD:60:D9 (Giga-byte Technology)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

Načasování

Různé šablony intenzity skenů (0-5)

`-T`

`paranoid|sneaky|polite|normal|aggressive|insane`

Dále existují přepínače:

`--max-rtt-timeout`

`--min-rtt-timeout`

`--initial-rtt-timeout`

`--max-retries`

`--host-timeout`

Výstup nmapu I

Normální / interaktivní

```
Nmap scan report for nas (192.168.1.230)
Host is up (-0.055s latency).

PORT    STATE  SERVICE
22/tcp  open   ssh
80/tcp  open   http
443/tcp closed https
MAC Address: 1C:1B:0D:BD:60:D9 (Giga-byte Technology)
```

Výstup nmapu II

XML (ukázka jen pro ilustraci...)

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE nmaprun>
<?xml-stylesheet href="file:///usr/bin/../share/nmap/nmap.xsl" type="
2 17:17:08 2018 as: nmap -p22,80,443 -oA /tmp/mujsken 192.168.1.0/24
<nmaprun scanner="nmap" args="nmap -p22,80,443 -oA /tmp/mujsken 192.1
2 17:17:08 2018" version="7.60" xmloutputversion="1.04"><scaninfo typ
<host starttime="1520007428" endtime="1520007436"><status state="up"
<address addr="192.168.1.230" addrtype="ipv4"/><address addr="1C:1B:0
<hostname name="nas" type="PTR"/></hostnames><ports>
<port protocol="tcp" portid="22"><state state="open" reason="syn-ack"
<port protocol="tcp" portid="80"><state state="open" reason="syn-ack"
<port protocol="tcp" portid="443"><state state="closed" reason="reset
<runstats><finished time="1520007436" timestr="Fri Mar  2 17:17:16 20
2 17:17:16 2018; 256 IP addresses (6 hosts up) scanned in 8.75 second
</nmaprun>
```

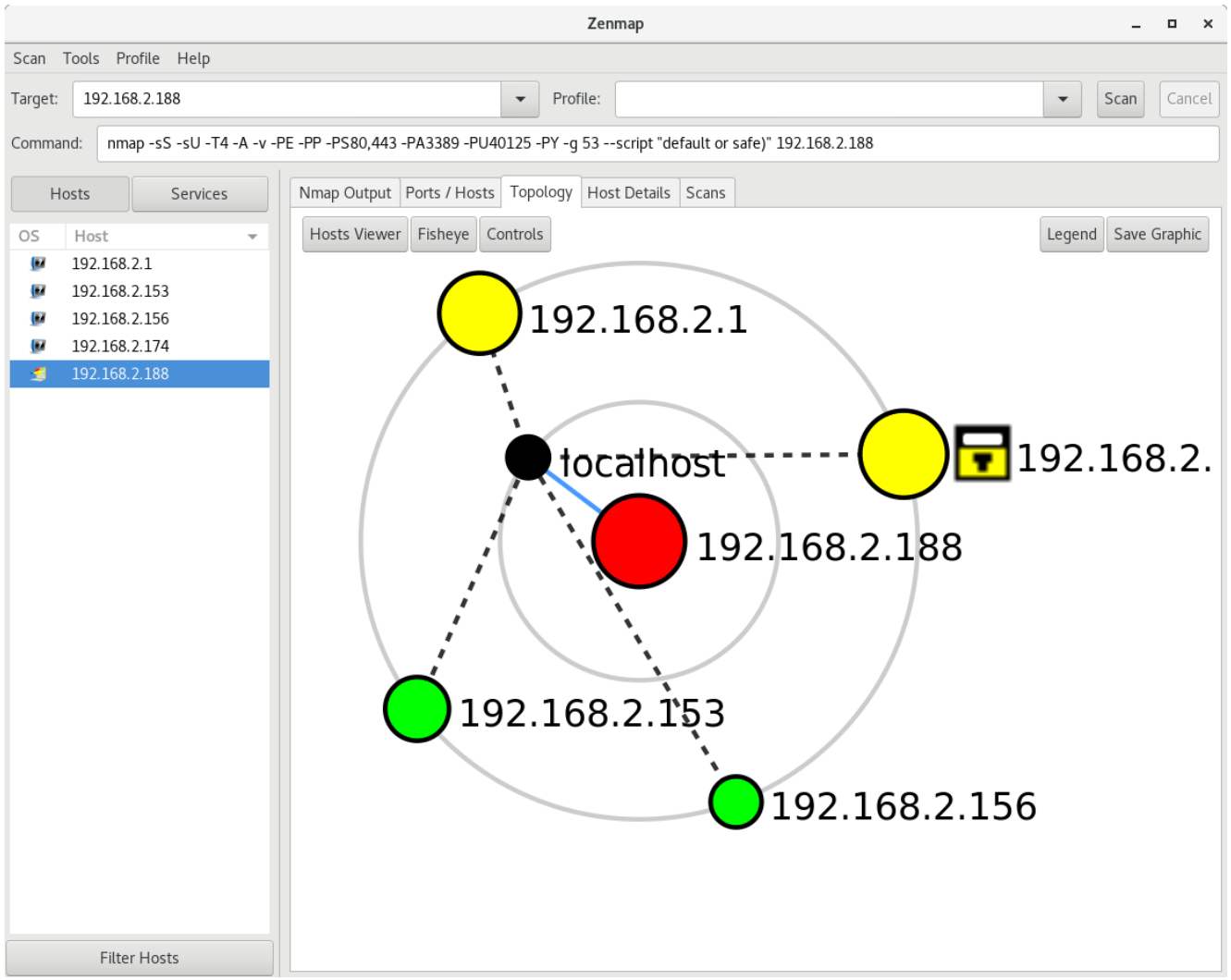
Výstup nmapu III

Grepable

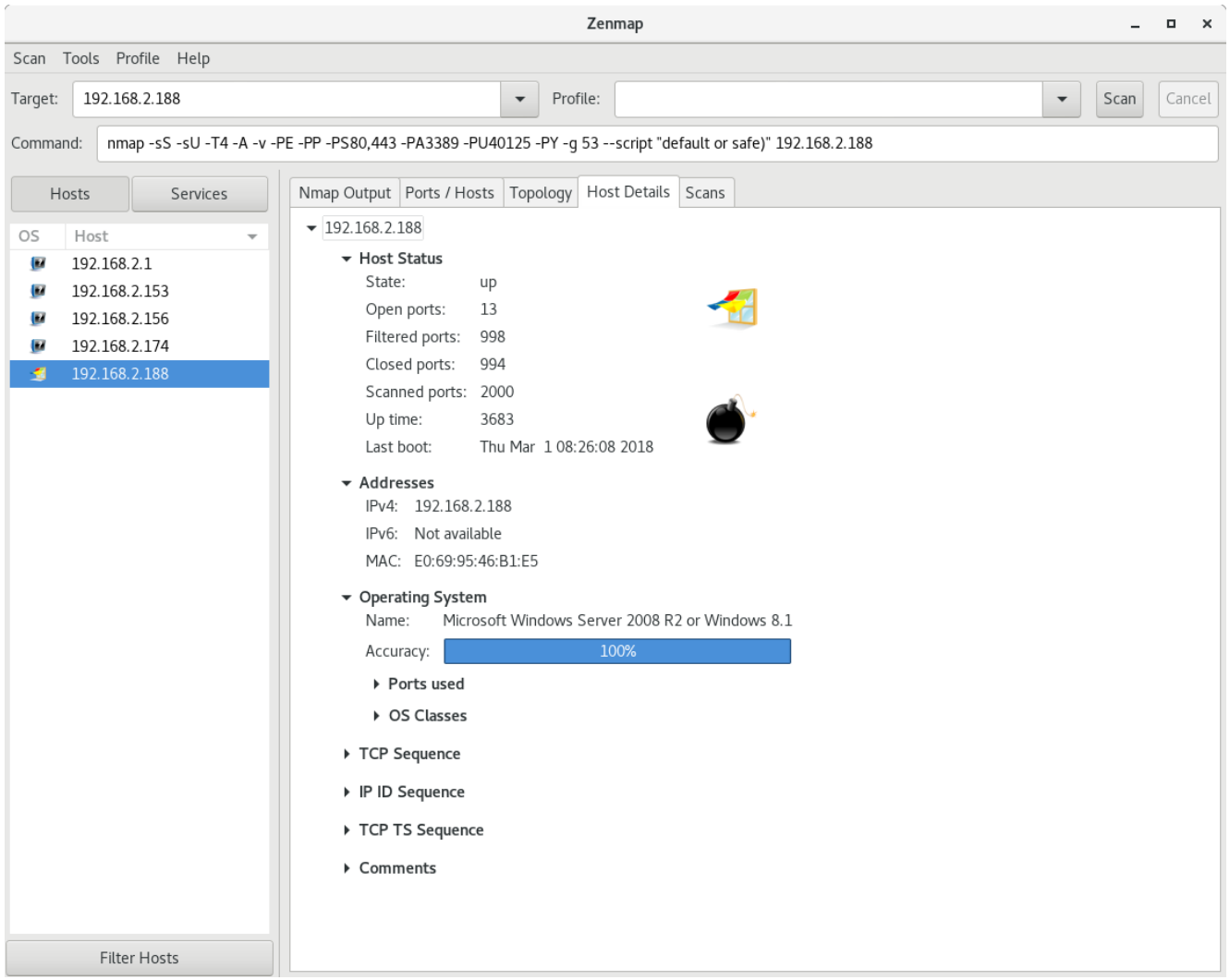
```
# Nmap 7.60 scan initiated Fri Mar  2 17:17:08 2018 as: nmap -p22,80,
Host: 192.168.1.230 (nas)   Status: Up
Host: 192.168.1.230 (nas)   Ports: 22/open/tcp//ssh///, 80/open/tcp//
# Nmap done at Fri Mar  2 17:17:16 2018 -- 256 IP addresses (6 hosts
```

Všechny varianty zároveň: `-oA` + název souborů

GUI - zenmap I


Zenmap
Scan Tools Profile Help
Target: 192.168.2.188
Profile:
Scan
Cancel
Command: nmap -sS -sU -T4 -A -v -PE -PP -PS80,443 -PA3389 -PU40125 -PY -g 53 --script "default or safe)" 192.168.2.188
Hosts
Services
OS
Host
192.168.2.1
192.168.2.153
192.168.2.156
192.168.2.174
192.168.2.188
Filter Hosts
Nmap Output
Ports / Hosts
Topology
Host Details
Scans
Hosts Viewer
Fisheye
Controls
Legend
Save Graphic
192.168.2.1
localhost
192.168.2.
192.168.2.188
192.168.2.153
192.168.2.156

GUI - zenmap II



Klamání

- Nastavení zdrojových portů
- Fragmentace paketů
- Podvržení zdrojových IP adres
  znesnadněno dodržováním BCP38 a BCP84
  (filtrace provozu)
- Generování falešných cizích skenů

Nmap Script Engine

Nmap Script Engine (NSE)

- Umožňuje rozšířit funkcionalitu
- Skripty v jazyce LUA
- nmap poskytuje sadu funkcí, které může LUA skript volat

OT: NERD

Network Entity Reputation Database (NERD)

- `https://nerd.cesnet.cz`
- Zpracovává hlášení o bezpečnostních událostech
- Seznam entit — „Zdroje problémů“ (Source of Trouble)
- Dohledává informace k entitám
- Počítá „Reputaci“

Více informací na bartos@cesnet.cz

Ukázka nového NSE skriptu I

Skript pro získání informací o cíli v NERDu

Ukázka nového NSE skriptu II

Načtení potřebných knihoven:

```
1 local http = require "http"
2 local ipOps = require "ipOps"
3 local io = require "io"
4 local stdnse = require "stdnse"
5 local json = require "json"
```

Ukázka nového NSE skriptu III

Součástí kódu skriptu je dokumentace:

```
7  description = [[
8  Looks up info about the target in the NERD system.
9  ]]
10
11 ---
12 -- @args nerd Takes the following optional argument:
13 -- * <code>nerd.apifile=file</code> Path to file with
       NERD API key, default is ./nerdapifile.
14 -- @usage
15 -- # Basic usage:
16 -- nmap target --script nerd
17 -- nmap target --script nerd --script-args nerd.apifile
       =/home/user/apifile
18 --
19 -- @output
20 -- Host script results:
21 -- |_nerd: IP not found in NERD
22 --
```

Ukázka nového NSE skriptu IV

```
23 -- Host script results:
24 -- |_nerd: {"asn": [], "bgppref": "", "bl": [], "geo":
       {"ctry": "CZ"}, "hostname": "ns.cesnet.cz", "ip":
       "195.113.144.194", "ipblock": "", "rep": 0.2, "tags
       ": []}
25
26 author = "Tomas Cejka <cejkat@cesnet.cz>"
27 license = "Same as Nmap--See https://nmap.org/book/man-
       legal.html"
28 categories = {"external"}
```

Ukázka nového NSE skriptu V

Adresy privátních rozsahů nechceme zjišťovat v NERDu:

```
31 hostrule = function( host )
32   local is_private, err = ipOps.isPrivate( host.ip )
33   if is_private == nil then
34     stdnse.debug1( "Error in Hostrule: %s.", err )
35     return false
36   end
37   return not is_private
38 end
```

Ukázka nového NSE skriptu VI

Chceme si načíst API klíč k NERDu ze souboru:

```
40 function load_key()
41    local file = nil
42    local apifile = stdnse.get_script_args('nerd.apifile'
          )
43    if type( apifile ) ~= "string" or apifile == "" then
44       apifile = "nerdapifile"
45    end
46    file = io.input( apifile )
47
48    if file then
49       local content = file:read "l"
50       file:close()
51       return content
52    else
53       return nil
54    end
55 end
```

Ukázka nového NSE skriptu VII

Akce! Ptáme se NERDu a vrátíme odpověď:

```
57 action = function( host )
58    local apitoken = load_key()
59    local header = {header={Authorization= "token " ..
          apitoken}}
60    local resp = http.get_url("https://nerd.cesnet.cz/
          nerd/api/v1/ip/" .. host.ip, header)
61    local content = resp.body
62    local status, parsed = json.parse(content)
63    if not(status) or parsed.err_n == 404 then
64       return "IP not found in NERD"
65    end
66    return content
67 end
```

Závěrem...

Detekce skenů

Mnoho nástrojů detekuje skeny

Existují pravidla pro snort, suricata, …

NEMEA systém obsahuje `vportscan` a `haddrscan`,
Vaše vylepšení bude vítáno!
(`https://github.com/CESNET/NEMEA-Detectors`)

liberouter cesnet

Děkuji za pozornost.

Kontakt:

cejkat@cesnet.cz, cejkato2@fit.cvut.cz

Twitter:

@tomcejka, @liberouter, @CESNET_CERTS

Zajímavé odkazy ;-)

`https://liberouter.org`
`https://cesnet.cz`