

KRESTEN JACOBSEN

NETWORK SCANNING

Hvad: Der findes mange værktøjer; men få er så gode og omfattende som NMAP.

- Rekognoscering på netværk (i form af portscanning)
- Opererer (primært) på netværks- og transportlaget i TCP/IP-modellen.

Hvorfor: Primært test formål (men kan principielt også bruges offensivt).

Eks. 1: Test af netværk for at finde sårbarheder.

BAGGRUND – NETWORK SCANNING

- Fire lag:
 - 1) Map netværket
 - 2) Identificer hosts
 - 3) Identificer services
 - 4) Identificer detaljer om services

1) Eks.: Find vej til specifik host: `tracert 192.168.232.138`

2) Eks.: Scan c-class netværk for aktive hosts: `nmap -sn 192.168.232.0/24`
(Udsender arp-requests vedr. alle hosts; se evt. i Wireshark)

3) Eks.: Scan hosts for populære porte: `nmap --top-ports 1000 192.168.232.138`
(Laver forespørgsler på de mest 1000 mest populære porte; se evt. i Wireshark)

4) Eks.: Scan host for at finde applikationer og versioner: `nmap -sV 192.168.232.138`

EKSEMPEL 1 – TRACEROUTE

```
keanet-sec — ~/repositories/it-sikkerhed/keanet-sec — bash — 89x23
kresten @ MINIAc in ~/repositories/it-sikkerhed/keanet-sec on master
$ nslookup log.logiskhave.dk
Server:      208.67.222.222
Address:     208.67.222.222#53

Non-authoritative answer:
Name:   log.logiskhave.dk
Address: 104.28.6.18
Name:   log.logiskhave.dk
Address: 104.28.7.18

kresten @ MINIAc in ~/repositories/it-sikkerhed/keanet-sec on master
$ traceroute 104.28.6.18
traceroute to 104.28.6.18 (104.28.6.18), 64 hops max, 52 byte packets
 1  10.0.0.1 (10.0.0.1)  711.336 ms  3.829 ms  6.049 ms
 2  xe-1/0/0.brl-soex.ip.cybercity.dk (192.38.7.36)  10.590 ms  22.403 ms  15.439 ms
 3  dix.as13335.net (192.38.7.70)  21.295 ms  15.939 ms  15.950 ms
 4  104.28.6.18 (104.28.6.18)  15.532 ms  1333.085 ms  12.454 ms

kresten @ MINIAc in ~/repositories/it-sikkerhed/keanet-sec on master
$
```

nslookup:

208.67.222.222 er dns-serveren, som svaret kommer fra.

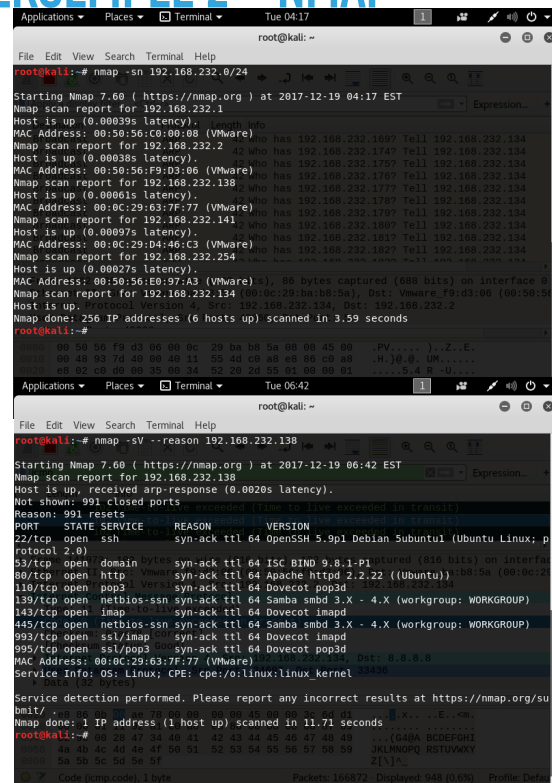
104.28.6.18 er log.logiskhave.dk's ip.

traceroute:

Viser fire hop 1) router 2) cybercity 3) dix 4) log.logiskhave.dk.

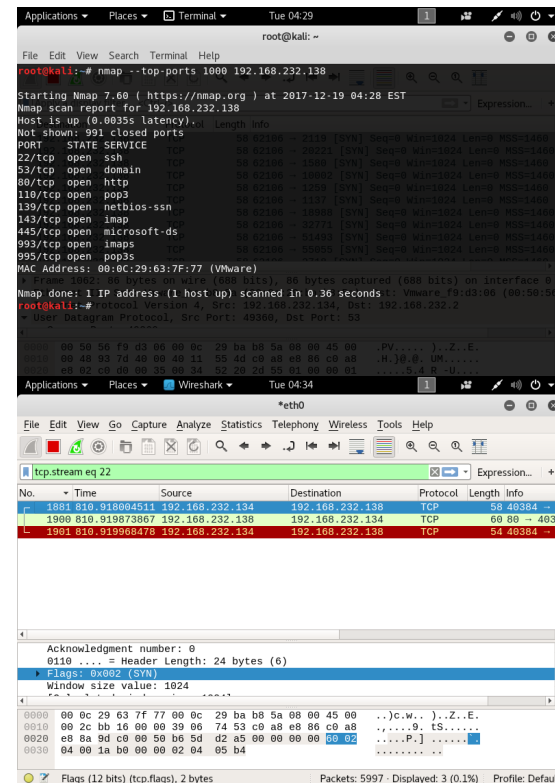
Traceroute virker ved at manipulere med TTL-værdien i ip-headeren i en icmp-pakke og ser på hvem der svarer, mens det inkrementerer TTL og dermed kommer tættere på målet for hver forespørgsel.

EKSEMPEL 2 – NMAP

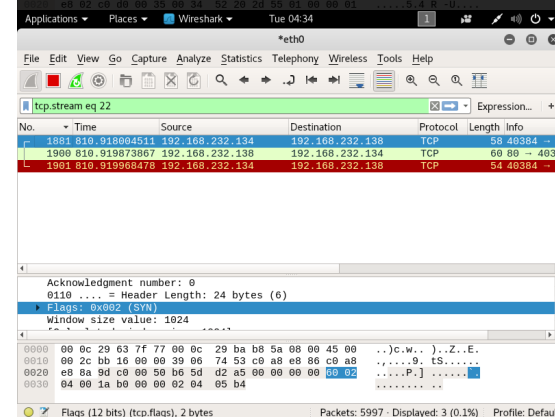


```
root@kali:~# nmap -sn 192.168.232.0/24
Starting Nmap 7.60 ( https://nmap.org ) at 2017-12-19 04:17 EST
Nmap scan report for 192.168.232.1
Host is up (0.00039s latency).
MAC Address: 00:50:56:C0:00:08 (VMware)
Nmap scan report for 192.168.232.2
Host is up (0.00038s latency).
MAC Address: 00:50:56:F9:D3:06 (VMware)
Nmap scan report for 192.168.232.138
Host is up (0.00061s latency).
MAC Address: 00:0C:29:63:7F:77 (VMware)
Nmap scan report for 192.168.232.141
Host is up (0.00097s latency).
MAC Address: 00:0C:29:D4:46:C3 (VMware)
Nmap scan report for 192.168.232.254
Host is up (0.00027s latency).
MAC Address: 00:50:56:E0:97:A3 (VMware)
Nmap scan report for 192.168.232.134
Host is up.
Nmap done: 256 IP addresses (6 hosts up) scanned in 3.59 seconds
root@kali:~#
```

```
root@kali:~# nmap -SV --reason 192.168.232.138
Starting Nmap 7.60 ( https://nmap.org ) at 2017-12-19 06:42 EST
Nmap scan report for 192.168.232.138
Host is up, received arp-response (0.0020s latency).
Not shown: 991 closed ports
Reason: 991 resets
PORT      STATE SERVICE REASON
22/tcp    open  ssh      syn-ack ttl 64 OpenSSH 5.9p1 Debian Subuntul (Ubuntu Linux; p
53/tcp    open  domain   syn-ack ttl 64 ISC BIND 9.8.1-P1
80/tcp    open  http     syn-ack ttl 64 Apache httpd 2.2.22 ((Ubuntu))
110/tcp   open  pop3     syn-ack ttl 64 Dovecot pop3d
139/tcp   open  netbios-ssn syn-ack ttl 64 Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
143/tcp   open  imap     syn-ack ttl 64 Dovecot imapd
445/tcp   open  netbios-ssn syn-ack ttl 64 Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
993/tcp   open  ssl/imap syn-ack ttl 64 Dovecot imapd
995/tcp   open  ssl/pop3 syn-ack ttl 64 Dovecot pop3d
MAC Address: 00:0C:29:63:7F:77 (VMware)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux kernel
Service detection performed. Please report any incorrect results at https://nmap.org/su
Nmap done: 1 IP address (1 host up) scanned in 11.71 seconds
root@kali:~#
```



```
root@kali:~# nmap --top-ports 1000 192.168.232.138
Starting Nmap 7.60 ( https://nmap.org ) at 2017-12-19 04:28 EST
Nmap scan report for 192.168.232.138
Host is up (0.0035s latency).
Not shown: 991 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
53/tcp    open  domain
80/tcp    open  http
110/tcp   open  pop3
139/tcp   open  netbios-ssn
143/tcp   open  imap
445/tcp   open  microsoft-ds
993/tcp   open  imaps
995/tcp   open  pop3s
MAC Address: 00:0C:29:63:7F:77 (VMware)
Nmap done: 1 IP address (1 host up) scanned in 0.36 seconds
root@kali:~#
```



No.	Time	Source	Destination	Protocol	Length	Info
1	1981.810.918004511	192.168.232.134	192.168.232.138	TCP	58	40384 → 80
2	1980.810.919873067	192.168.232.138	192.168.232.134	TCP	60	80 → 40384
3	1901.810.919968476	192.168.232.134	192.168.232.138	TCP	54	40384 → 80

Ø.V.) Fase 2: Scan c-class netværk for aktive hosts: `nmap -sn 192.168.232.0/24`
(Udsender arp-requests vedr. alle hosts; se evt. i Wireshark)

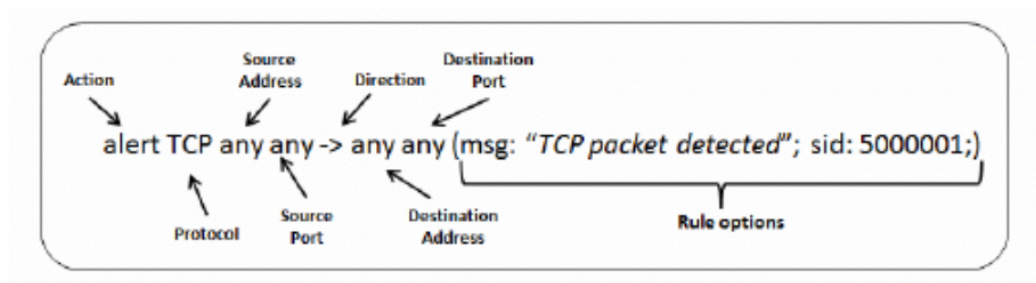
H.) Fase 3: Scan host for at finde applikationer og versioner: `nmap -SV 192.168.232.138`

N.V) Eks.: Scan hosts for populære porte: `nmap --top-ports 1000 192.168.232.138`
(Laver forespørgsler på de mest 1000 mest populære porte; se evt. i Wireshark)

RELATERET EMNE: IDS / IPS

- IDS / IPS'er kan bruges til at opdage og forhindre eks. syn-flooding.
- Eks. på snort-regel :

```
alert tcp any any -> 192.168.65.132 any (msg:"TCP SYN flood attack  
detected"; flags:S; threshold: type threshold, track by_dst, count 20,  
seconds 60; classtype=denial-of-service; priority:5; sid:5000001; rev:1;)
```



Snort-reglen sættes i `/etc/nsm/rules/local.rules`

Classtype overstreget, da jeg simpelthen ikke kunne få det til at virke med den sat og den derfor er pillet ud i reglen på næste side...

RELATERET EMNE: IDS / IPS

The screenshot shows the SGUIL-0.9.0 interface. At the top, a status bar indicates 'Connected To localhost' with 'ServerName: localhost', 'UserName: kresten', and 'UserID: 2'. The 'RealTime Events' tab is active, displaying a table of events. A red circle highlights the event with CNT 1, Sensor securi..., Date/Time 2017-12-14 12:48:05, Src IP 192.168.232.10, SPort 52329, Dst IP 192.168.232.138, DPort 80, and Event TCP S... Below the table, the 'Show Packet Data' and 'Show Rule' checkboxes are checked. The rule text is: 'alert tcp any any -> 192.168.232.138 any (msg:"TCP SYN flood attack detected"; flags:S; threshold: type threshold, track by_dst, count 20, seconds 60; priority:5; sid:5000001; rev:2;)'. The packet details show a TCP packet from 192.168.232.10 to 192.168.232.138 on port 80, with flags U A P R S F and sequence number 52329. The 'DATA' section is empty.

T	CNT	Sensor	Aler...	Date/Time	Src IP	SPort	Dst IP	DPort	Pr	Event...
ST	3	securi...	3.1	2017-12-14 11:33:18	192.168.142.129	68	192.168.142.254	67	17	ET P...
ST	1	securi...	3.4	2017-12-14 12:48:05	192.168.232.10	52329	192.168.232.138	80	6	TCP S...
ST	1	securi...	3.5	2017-12-14 12:48:07	192.168.232.11	52329	192.168.232.138	80	6	TCP S...
ST	1	securi...	3.6	2017-12-14 12:48:08	192.168.232.134	68	192.168.232.254	67	17	ET P...
ST	1	securi...	3.7	2017-12-14 12:48:08	192.168.232.12	52329	192.168.232.138	80	6	TCP S...

IP Resolution Agent Status: ☐ Reverse DNS ☒ Enable Ext...

Src IP:
Src Name:
Dst IP:
Dst Name:
Whois Query: ☒ None ☐ Src I

☒ Show Packet Data ☒ Show Rule

alert tcp any any -> 192.168.232.138 any (msg:"TCP SYN flood attack detected"; flags:S; threshold: type threshold, track by_dst, count 20, seconds 60; priority:5; sid:5000001; rev:2;)

IP	Source IP	Dest IP	Ver	HL	TOS	len	ID	Flags	Offset	TTL	ikSu
IP	192.168.232.10	192.168.232.138	4	5	0	40	1	0	0	64	10

U A P R S F

Source	Dest	R	R	R	C	S	S	Y	I
Port	Port	1	0	G	K	H	T	N	N

Seq # Ack # Offset Res Window Urp ikSu

52329	80	X	.	0	0	5	0	8192	0	28
-------	----	---	---	---	---	---	---	---	---	---	---	---	---	------	---	----

None .

DATA

Search Packet Payload ☐ Hex ☒ Text ☐ NoCase

Screenshot fra SGUIL af capture fra foregående snort-regel