Workshop Security Basics

Sniffing und Scanning

Felix Bauer

IT Security Consultant und Engineer

bei

Science + Computing AG an Atos Company

felix@ai4me.de

Ablauf

- 5 USB-Sticks
- Virtuelle Maschine
- Kali Linux mit allen Tools die wir verwenden
- SHA256
  826CA0196B85BE249E00B22202E7D95B63CC71B007C2
  657A2E96457383C9D192
- Folien
- VirtualBox

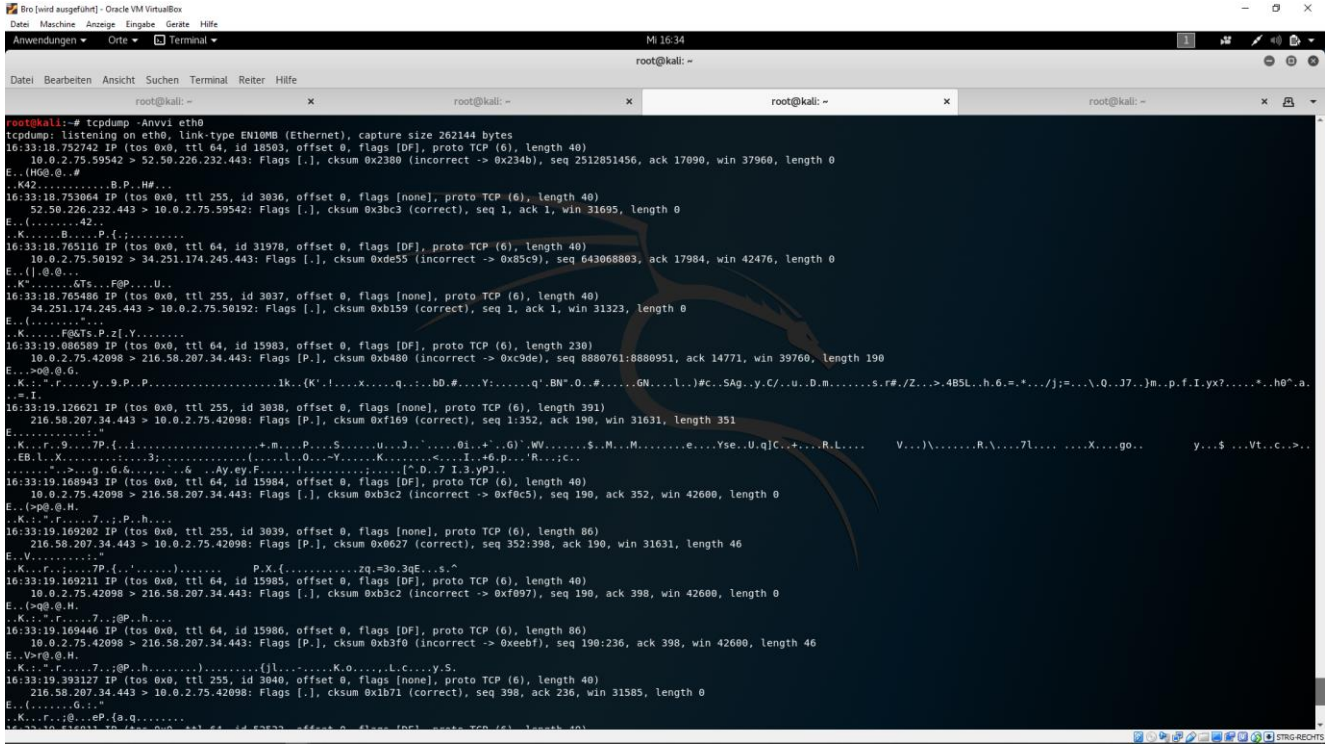
Sniffing

Sniffing

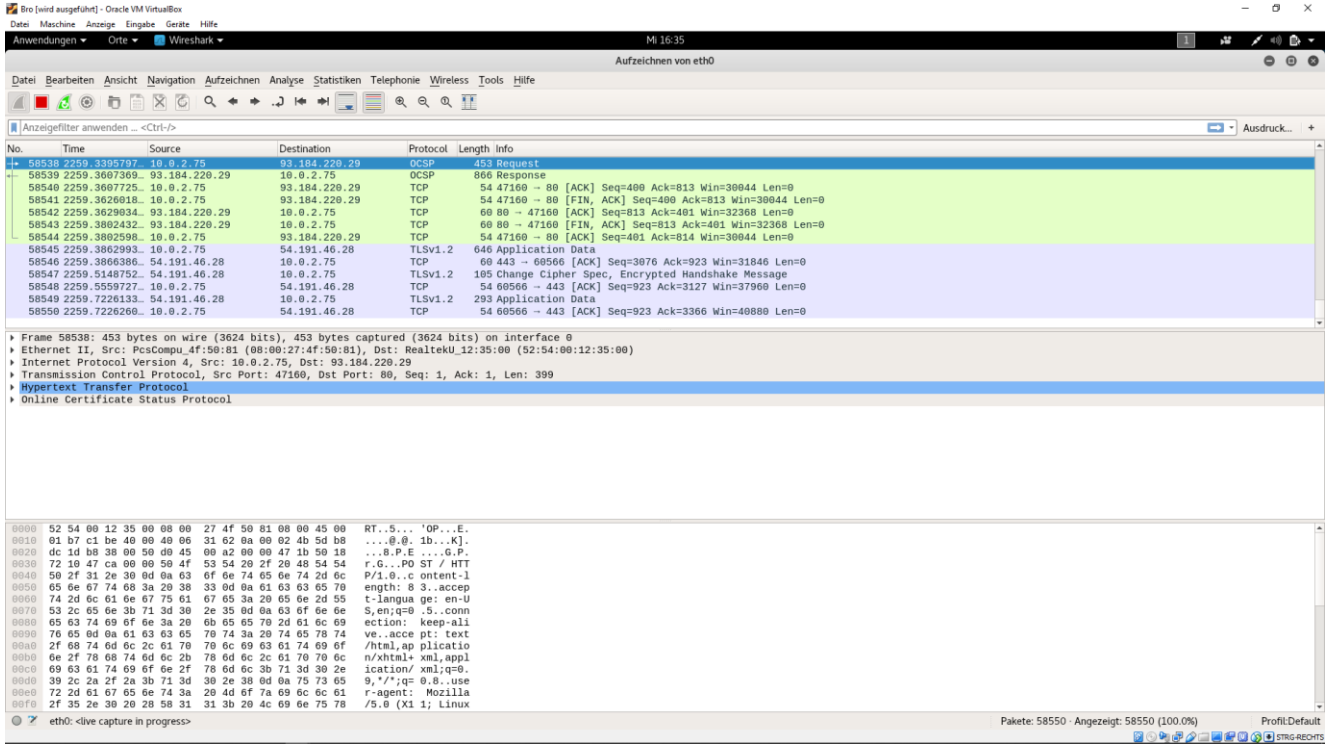
- Mitlesen von Datenübertragung
- Computernetzwerke
- USB
- Bus-Systeme
- Drahtlosnetzwerke
- WLAN
- GSM
- …

tcpdump

```
tcpdump -Anvvi eth0 [Filter]
```



wireshark

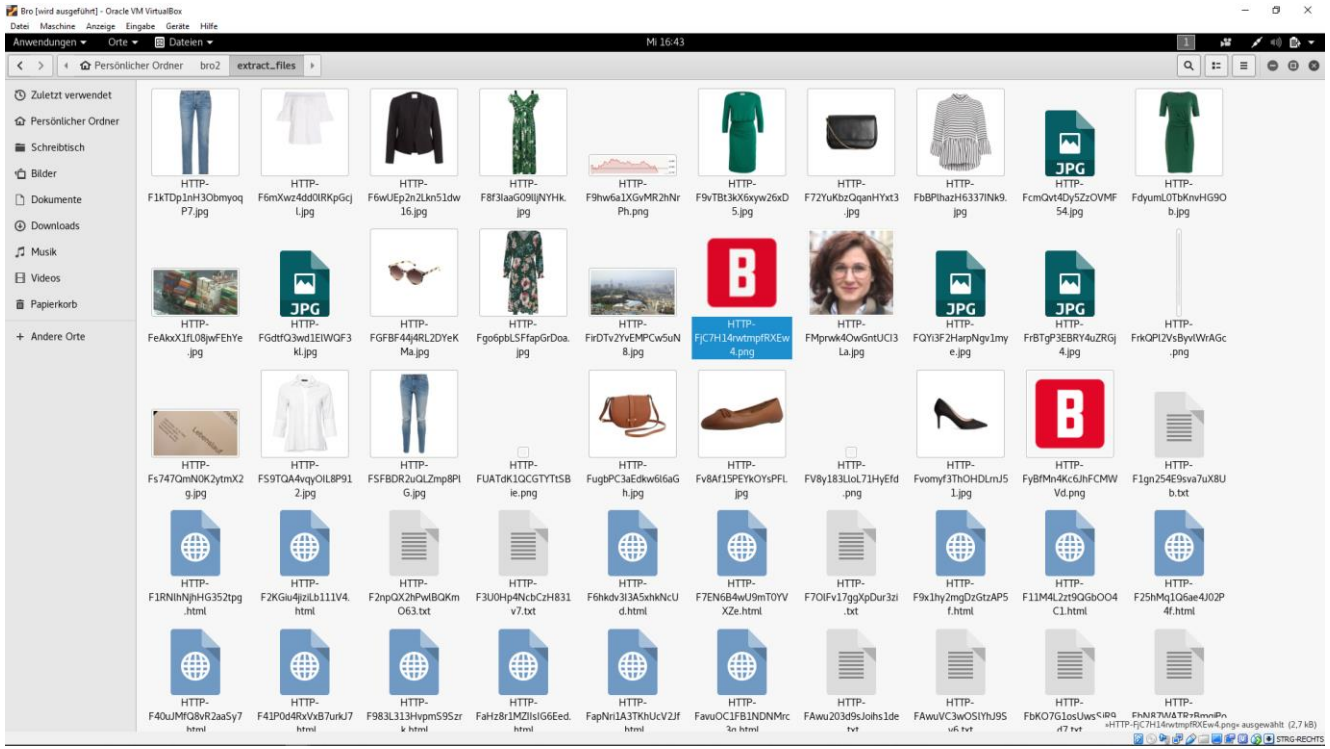

Bro [wird ausgeführt] - Oracle VM VirtualBox
Datei Maschine Anzeige Eingabe Geräte Hilfe
Anwendungen Orte Wireshark Mi 16:35
Aufzeichnen von eth0
Datei Bearbeiten Ansicht Navigation Aufzeichnen Analyse Statistiken Telephonie Wireless Tools Hilfe
Anzeigefilter anwenden … <Ctrl-/>
Ausdruck…
No. Time Source Destination Protocol Length Info
58538 2259.3395797… 10.0.2.75 93.184.220.29 OCSP 453 Request
58539 2259.3607369… 93.184.220.29 10.0.2.75 OCSP 866 Response
58540 2259.3607725… 10.0.2.75 93.184.220.29 TCP 54 47160 → 80 [ACK] Seq=400 Ack=813 Win=30044 Len=0
58541 2259.3626018… 10.0.2.75 93.184.220.29 TCP 54 47160 → 80 [FIN, ACK] Seq=400 Ack=813 Win=30044 Len=0
58542 2259.3629034… 93.184.220.29 10.0.2.75 TCP 60 80 → 47160 [ACK] Seq=813 Ack=401 Win=32368 Len=0
58543 2259.3802432… 93.184.220.29 10.0.2.75 TCP 60 80 → 47160 [FIN, ACK] Seq=813 Ack=401 Win=32368 Len=0
58544 2259.3802598… 10.0.2.75 93.184.220.29 TCP 54 47160 → 80 [ACK] Seq=401 Ack=814 Win=30044 Len=0
58545 2259.3862993… 10.0.2.75 54.191.46.28 TLSv1.2 646 Application Data
58546 2259.3866386… 54.191.46.28 10.0.2.75 TCP 60 443 → 60566 [ACK] Seq=3076 Ack=923 Win=31846 Len=0
58547 2259.5148752… 54.191.46.28 10.0.2.75 TLSv1.2 105 Change Cipher Spec, Encrypted Handshake Message
58548 2259.5559727… 10.0.2.75 54.191.46.28 TCP 54 60566 → 443 [ACK] Seq=923 Ack=3127 Win=37960 Len=0
58549 2259.7226133… 54.191.46.28 10.0.2.75 TLSv1.2 293 Application Data
58550 2259.7226260… 10.0.2.75 54.191.46.28 TCP 54 60566 → 443 [ACK] Seq=923 Ack=3366 Win=40880 Len=0
Frame 58538: 453 bytes on wire (3624 bits), 453 bytes captured (3624 bits) on interface 0
Ethernet II, Src: PcsCompu_4f:50:81 (08:00:27:4f:50:81), Dst: RealtekU_12:35:00 (52:54:00:12:35:00)
Internet Protocol Version 4, Src: 10.0.2.75, Dst: 93.184.220.29
Transmission Control Protocol, Src Port: 47160, Dst Port: 80, Seq: 1, Ack: 1, Len: 399
Hypertext Transfer Protocol
Online Certificate Status Protocol
0000 52 54 00 12 35 00 08 00 27 4f 50 81 08 00 45 00 RT..5... 'OP...E.
0010 01 b7 c1 be 40 00 40 06 31 62 0a 00 02 4b 5d b8 ....@.@. 1b...K].
0020 dc 1d b8 38 00 50 d0 45 00 a2 00 00 47 1b 50 18 ...8.P.E ....G.P.
0030 72 10 47 ca 00 00 50 4f 53 54 20 2f 20 48 54 54 r.G...PO ST / HTT
0040 50 2f 31 2e 30 0d 0a 63 6f 6e 74 65 6e 74 2d 6c P/1.0..c ontent-l
0050 65 6e 67 74 68 3a 20 38 33 0d 0a 61 63 63 65 70 ength: 8 3..accep
0060 74 2d 6c 61 6e 67 75 61 67 65 3a 20 65 6e 2d 55 t-langua ge: en-U
0070 53 2c 65 6e 3b 71 3d 30 2e 35 0d 0a 63 6f 6e 6e S,en;q=0 .5..conn
0080 65 63 74 69 6f 6e 3a 20 6b 65 65 70 2d 61 6c 69 ection: keep-ali
0090 76 65 0d 0a 61 63 63 65 70 74 3a 20 74 65 78 74 ve..acce pt: text
00a0 2f 68 74 6d 6c 2c 61 70 70 6c 69 63 61 74 69 6f /html,ap plicatio
00b0 6e 2f 78 68 74 6d 6c 2b 78 6d 6c 2c 61 70 70 6c n/xhtml+ xml,appl
00c0 69 63 61 74 69 6f 6e 2f 78 6d 6c 3b 71 3d 30 2e ication/ xml;q=0.
00d0 39 2c 2a 2f 2a 3b 71 3d 30 2e 38 0d 0a 75 73 65 9,*/*;q= 0.8..use
00e0 72 2d 61 67 65 6e 74 3a 20 4d 6f 7a 69 6c 6c 61 r-agent: Mozilla
00f0 2f 35 2e 30 20 28 58 31 31 3b 20 4c 69 6e 75 78 /5.0 (X1 1; Linux
eth0: <live capture in progress>
Pakete: 58550 · Angezeigt: 58550 (100.0%)
Profil:Default
STRG-RECHTS

bro

- `bro -i eth0`
- conn.log dhcp.log dns.log files.log http.log packet_filter.log reporter.log ssl.log weird.log x509.log
- …

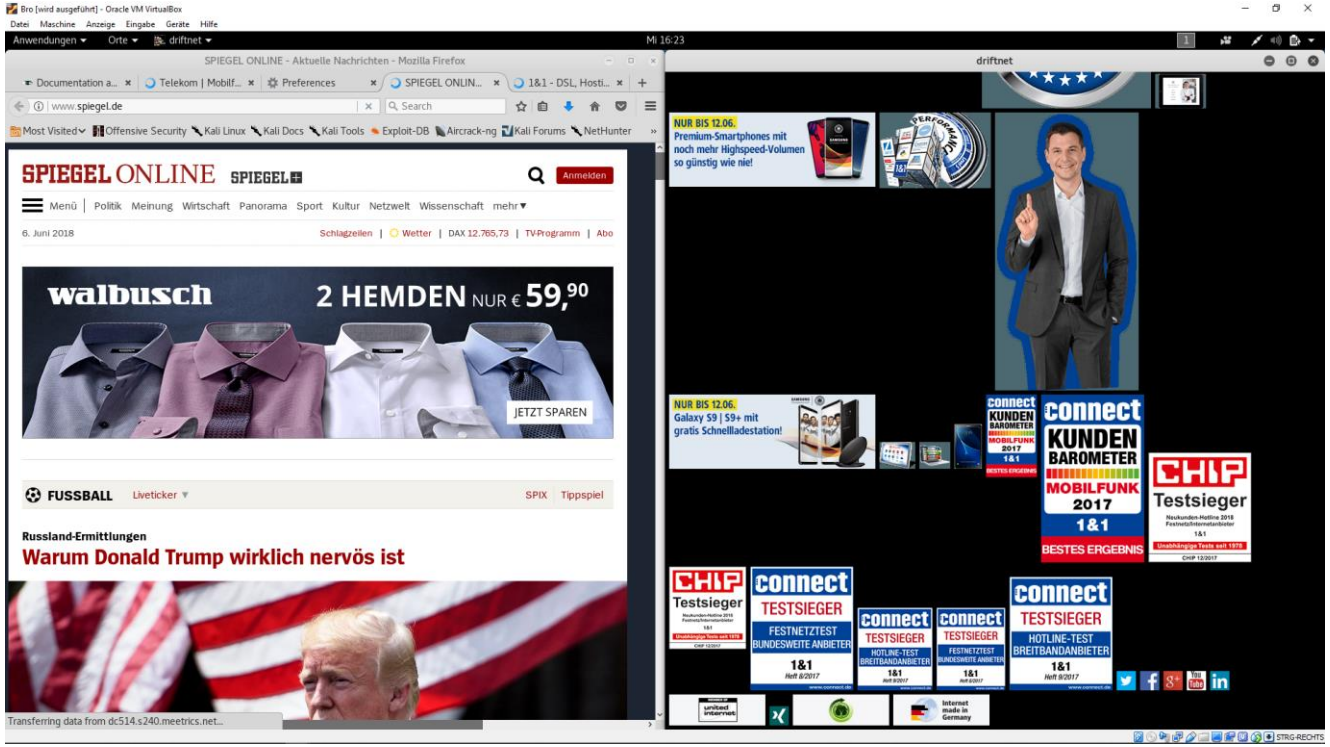
bro

```
bro -i lo fileextraction.bro
```



driftnet

```
driftnet -i eth0
```



sslstrip

- `sslstrip`
- http proxy 127.0.0.1:10000
- s/https/http/g

scapy

- **Python**
- **Pakete zusammenbauen und auseinandernehmen**
- **Empfangen und verschicken**
- `send(IP(dst="192.168.1.12")/TCP(dport=80))`
- `ls(IPv6)`
- `packet.summary()`
  `packet.show()`
- `sniff(count=100)`

Networking Basics

OSI-Modell

OSI-Schicht		Einordnung	DoD-Schicht	Einordnung	Protokollbeispiele	Einheiten	Kopplungselemente
7	Anwendungen (Application)	Anwendungs-orientiert	Anwendung	Ende zu Ende (Multihop)	HTTP FTP HTTPS SMTP XMPP DNS LDAP NCP	Daten	Gateway, Content-Switch, Proxy, Layer-4-7-Switch
6	Darstellung (Presentation)						
5	Sitzung (Session)						
4	Transport (Transport)	Transport-orientiert	Transport		TCP UDP SCTP SPX	TCP = Segmente UDP = Datagramme	
3	Vermittlung-/Paket (Network)		Internet		ICMP IGMP IP IPsec IPX	Pakete	Router, Layer-3-Switch
2	Sicherung (Data Link)		Netzzugriff	Punkt zu Punkt	Ethernet Token Ring FDDI MAC ARCNET	Rahmen (Frames)	Bridge, Layer-2-Switch
1	Bitübertragung (Physical)					Bits, Symbole, Pakete	Netzwerkkabel, Repeater, Hub

Quelle: Wikipedia

Routing

- `ip a`
- `ip a a 192.168.0.5/24 dev eth0`
- `ip r`
- `ip r add 0.0.0.0/1 via 192.168.0.2`
- `ip r add 128.0.0.0/1 via 192.168.0.2`
- `ip r delete default via 192.168.0.1`

PING

ping 8.8.8.8

```
[felix@felix-pc ~]$ ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=58 time=18.0 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=58 time=17.5 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=58 time=15.1 ms
64 bytes from 8.8.8.8: icmp_seq=4 ttl=58 time=15.3 ms
64 bytes from 8.8.8.8: icmp_seq=5 ttl=58 time=15.7 ms
64 bytes from 8.8.8.8: icmp_seq=6 ttl=58 time=15.5 ms
64 bytes from 8.8.8.8: icmp_seq=7 ttl=58 time=19.3 ms
64 bytes from 8.8.8.8: icmp_seq=8 ttl=58 time=15.3 ms
64 bytes from 8.8.8.8: icmp_seq=9 ttl=58 time=16.3 ms
64 bytes from 8.8.8.8: icmp_seq=10 ttl=58 time=14.6 ms
64 bytes from 8.8.8.8: icmp_seq=1 ttl=58 time=23.4 ms (DUP!)
64 bytes from 8.8.8.8: icmp_seq=11 ttl=58 time=15.6 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=58 time=15.7 ms (DUP!)
64 bytes from 8.8.8.8: icmp_seq=12 ttl=58 time=20.2 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=58 time=14.7 ms (DUP!)
64 bytes from 8.8.8.8: icmp_seq=13 ttl=58 time=14.6 ms
64 bytes from 8.8.8.8: icmp_seq=4 ttl=58 time=21.3 ms (DUP!)
64 bytes from 8.8.8.8: icmp_seq=14 ttl=58 time=15.1 ms
64 bytes from 8.8.8.8: icmp_seq=5 ttl=58 time=16.1 ms (DUP!)
64 bytes from 8.8.8.8: icmp_seq=15 ttl=58 time=15.1 ms
64 bytes from 8.8.8.8: icmp_seq=16 ttl=58 time=15.5 ms
64 bytes from 8.8.8.8: icmp_seq=17 ttl=58 time=15.4 ms
64 bytes from 8.8.8.8: icmp_seq=18 ttl=58 time=15.1 ms
64 bytes from 8.8.8.8: icmp_seq=19 ttl=58 time=14.7 ms
```

ping 8.8.8.8

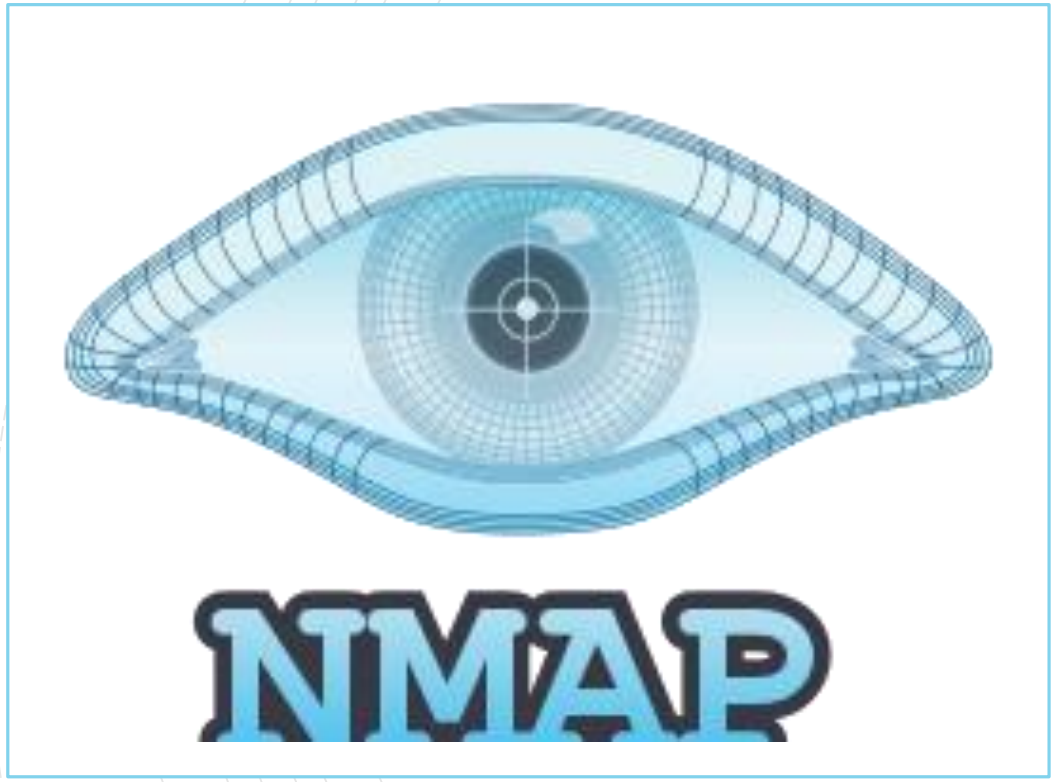
```
[felix@felix-pc ~]$ ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=58 time=23.4 ms
64 bytes from 8.8.8.8: icmp_seq=11 ttl=58 time=15.6 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=58 time=15.7 ms
64 bytes from 8.8.8.8: icmp_seq=12 ttl=58 time=20.2 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=58 time=14.7 ms
64 bytes from 8.8.8.8: icmp_seq=13 ttl=58 time=14.6 ms
64 bytes from 8.8.8.8: icmp_seq=4 ttl=58 time=21.3 ms
64 bytes from 8.8.8.8: icmp_seq=14 ttl=58 time=15.1 ms
64 bytes from 8.8.8.8: icmp_seq=5 ttl=58 time=16.1 ms
^C[felix@felix-pc ~]$
```

Scanning

Scanning

- Host discovery
- Service discovery
- Fingerprinting
- Vulnerability Scanning

nmap



- -sP
- -sS
- -sV
- -A
- -T4
- -p 22,80-140
- -sC

arp-scan

arp-scan -I enp0s3 -l

masscan

- `masscan -p22,80,445 192.168.1.0/24`
- `masscan 192.168.1.0/24 -p22 --banners --source-ip 192.168.1.200`
- `masscan 0.0.0.0/0 -p0-65535`

- https://github.com/robertdavidgraham/masscan

- `docker run -d -p 443:443 mikesplain/openvas`

SHODAN

https://shodan.io

ENDE