Wie sicher ist Ihr Unternehmen?

www.netzsicher.net
info@netzsicher.net

Referent:
Bjoern Hering

Certified Ethical Hacker (CEH 312-50)
Penetration Tester
Red Team Offensive Attacker

offensive IT der Autohaus Trompeter GmbH

Ein Penetration Test beantwortet folgende Fragen:

Ein Penetration Test beantwortet folgende Fragen:

❏ Was sieht ein Angreifer von außen?

Ein Penetration Test beantwortet folgende Fragen:

❑ Was sieht ein Angreifer von außen?

❑ Was kann ein Angreifer alles anrichten?

Ein Penetration Test beantwortet folgende Fragen:

❑ Was sieht ein Angreifer von außen?

❑ Was kann ein Angreifer alles anrichten?

❑ Fällt jemanden der Angriff auf
(Logs, IDS etc.)

Alle klassischen Hacking / Angriffsmethoden wie:

❑ Aktive & passive Hacking-Angriffe auf Ihr Unternehmen

❑ Social Engineering Angriffe auf Ihre Mitarbeiter (Phishing, Spear Phishing, Telefon Scams)

❑ Angriff auf Ihre WLAN Infrastruktur, physische Angriffe in Ihrem Unternehmen

❑ “Innentäterangriff”

❑ Durchführung von AWARENESS-Schulungen ihrer Mitarbeiter

❑ Detailliertes Gespräch mit der Geschäftsleitung über die Risikobewertung Ihres Unternehmens

netzsicher.net

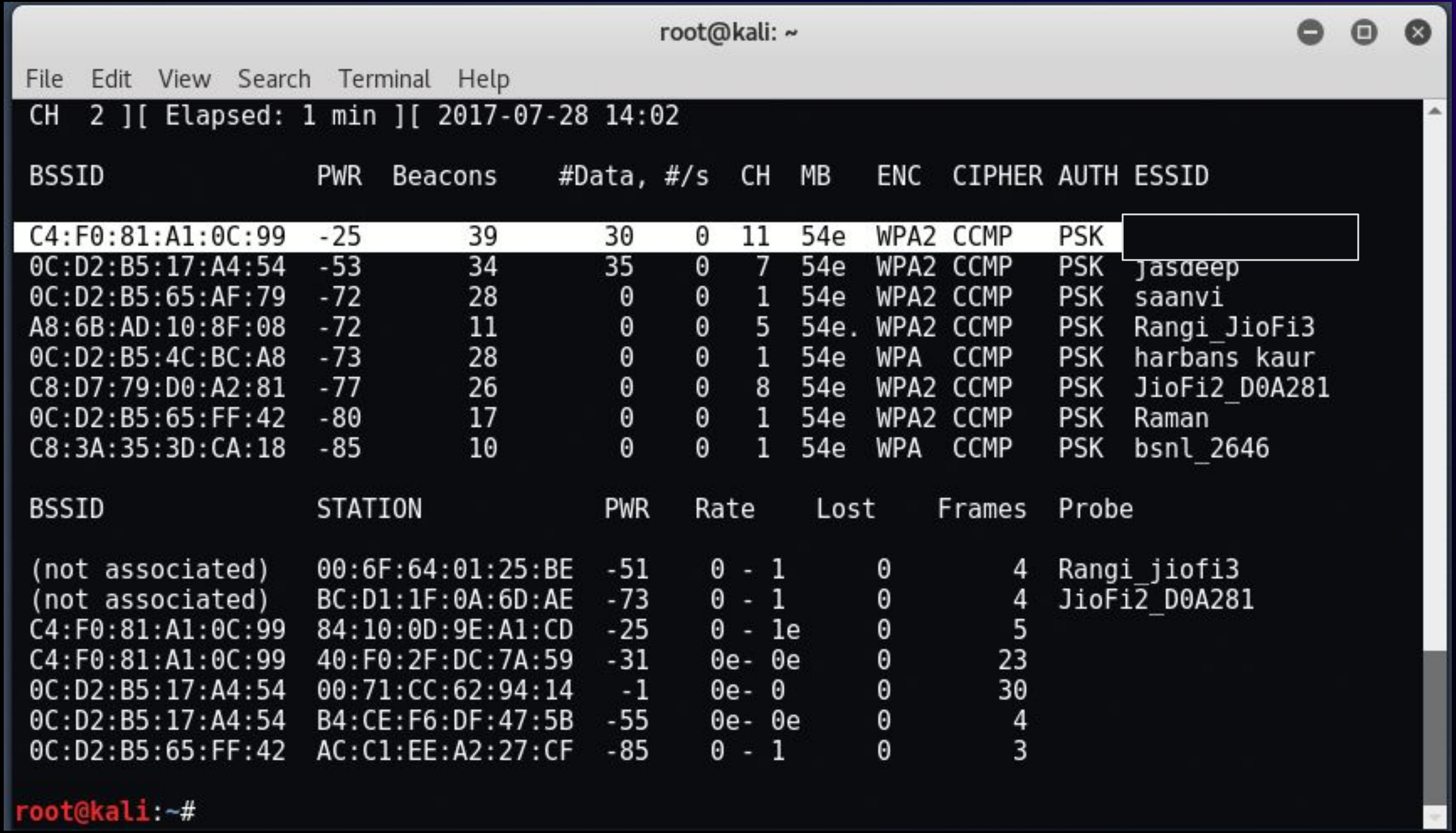
Red Team Angriff auf ein Autohaus

- Guest WLAN

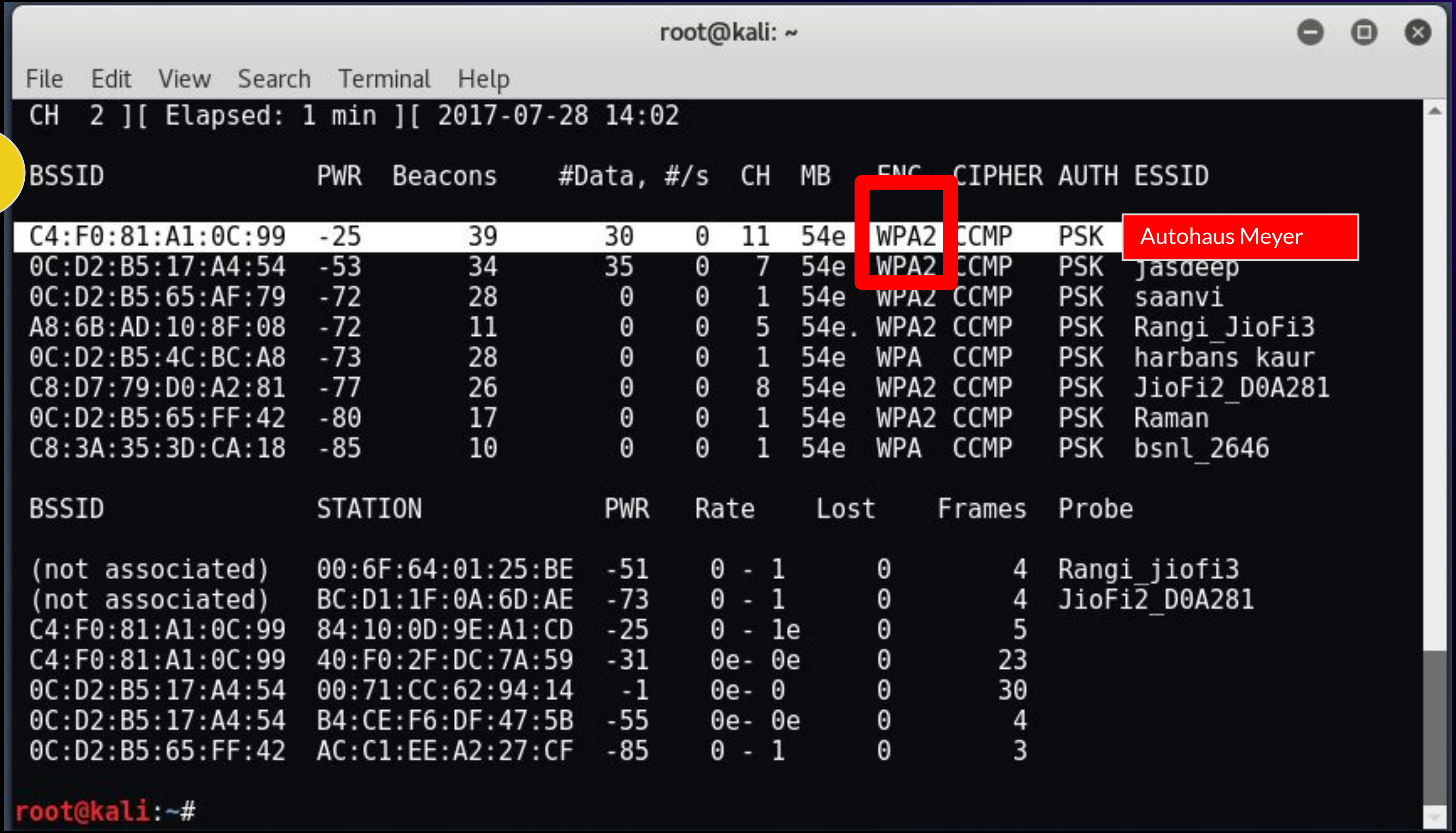
- **Guest WLAN**

Autohaus WLAN gesichert

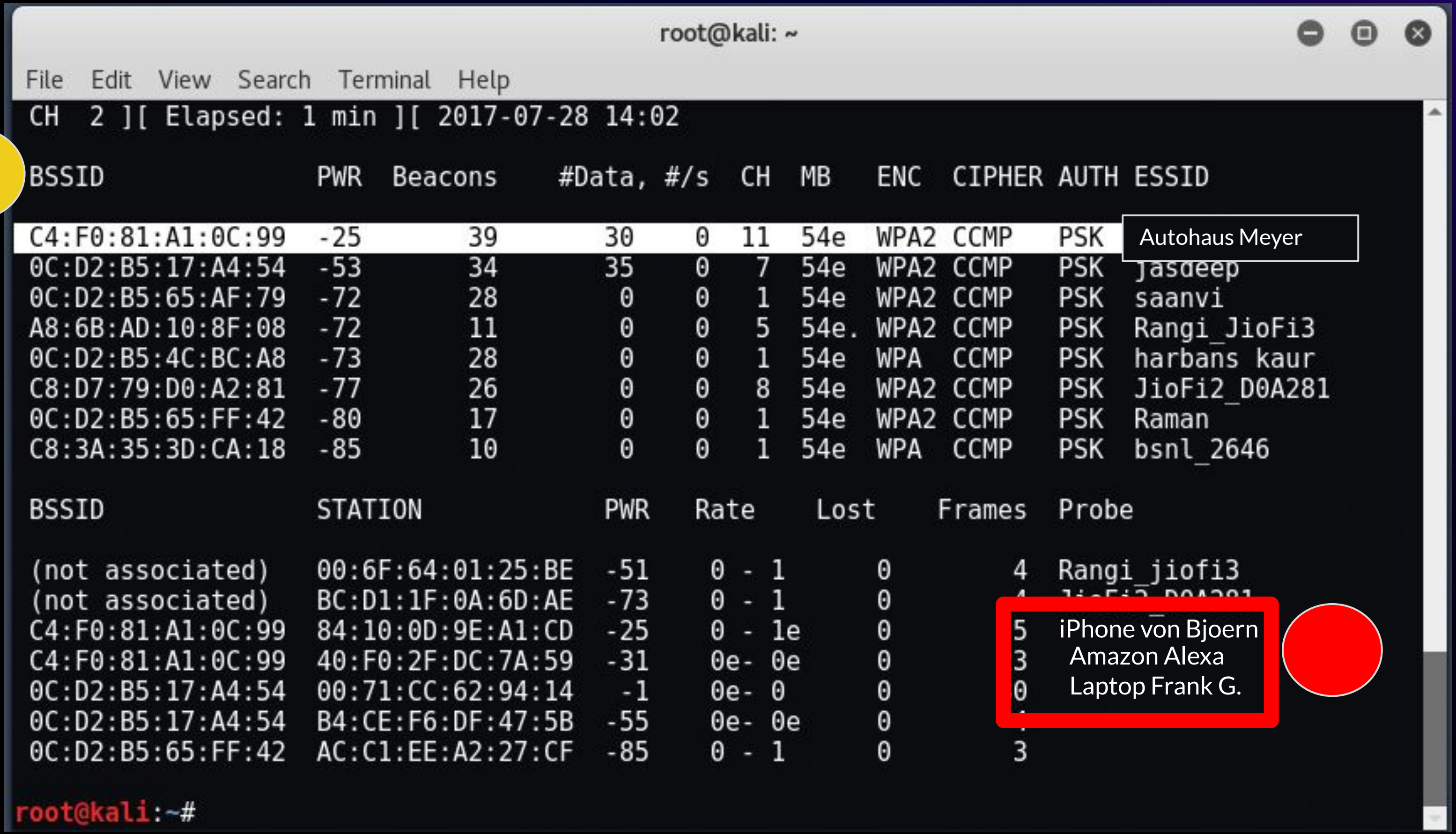
WPA2 verschlüsselt



```
 CH  2 ][ Elapsed: 1 min ][ 2017-07-28 14:02

 BSSID              PWR  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH ESSID

 C4:F0:81:A1:0C:99  -25       39       30    0  11  54e  WPA2 CCMP   PSK  [redacted]
 0C:D2:B5:17:A4:54  -53       34       35    0   7  54e  WPA2 CCMP   PSK  jasdeep
 0C:D2:B5:65:AF:79  -72       28        0    0   1  54e  WPA2 CCMP   PSK  saanvi
 A8:6B:AD:10:8F:08  -72       11        0    0   5  54e. WPA2 CCMP   PSK  Rangi_JioFi3
 0C:D2:B5:4C:BC:A8  -73       28        0    0   1  54e  WPA  CCMP   PSK  harbans kaur
 C8:D7:79:D0:A2:81  -77       26        0    0   8  54e  WPA2 CCMP   PSK  JioFi2_D0A281
 0C:D2:B5:65:FF:42  -80       17        0    0   1  54e  WPA2 CCMP   PSK  Raman
 C8:3A:35:3D:CA:18  -85       10        0    0   1  54e  WPA  CCMP   PSK  bsnl_2646

 BSSID              STATION            PWR   Rate    Lost    Frames  Probe

 (not associated)   00:6F:64:01:25:BE  -51    0 - 1      0        4  Rangi_jiofi3
 (not associated)   BC:D1:1F:0A:6D:AE  -73    0 - 1      0        4  JioFi2_D0A281
 C4:F0:81:A1:0C:99  84:10:0D:9E:A1:CD  -25    0 - 1e     0        5
 C4:F0:81:A1:0C:99  40:F0:2F:DC:7A:59  -31    0e- 0e     0       23
 0C:D2:B5:17:A4:54  00:71:CC:62:94:14   -1    0e- 0      0       30
 0C:D2:B5:17:A4:54  B4:CE:F6:DF:47:5B  -55    0e- 0e     0        4
 0C:D2:B5:65:FF:42  AC:C1:EE:A2:27:CF  -85    0 - 1      0        3

root@kali:~#
```

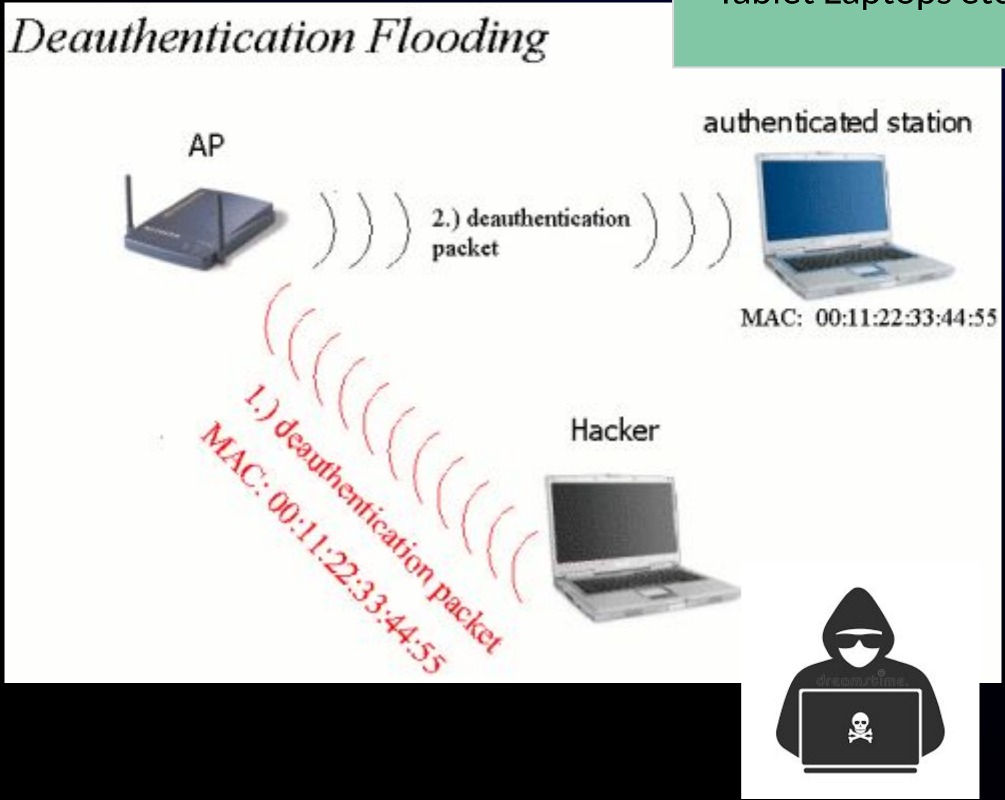


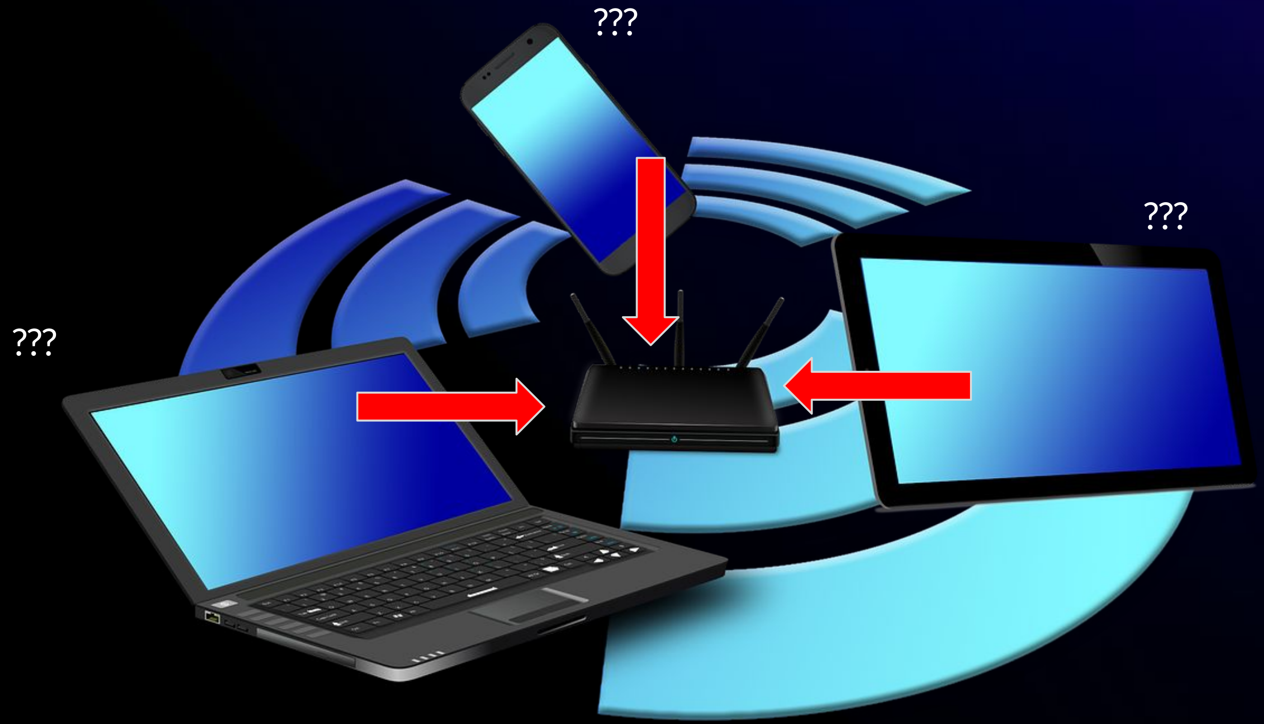
```
 CH  2 ][ Elapsed: 1 min ][ 2017-07-28 14:02

 BSSID              PWR  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH ESSID

 C4:F0:81:A1:0C:99  -25       39       30    0  11  54e  WPA2 CCMP   PSK  Autohaus Meyer
 0C:D2:B5:17:A4:54  -53       34       35    0   7  54e  WPA2 CCMP   PSK  jasdeep
 0C:D2:B5:65:AF:79  -72       28        0    0   1  54e  WPA2 CCMP   PSK  saanvi
 A8:6B:AD:10:8F:08  -72       11        0    0   5  54e. WPA2 CCMP   PSK  Rangi_JioFi3
 0C:D2:B5:4C:BC:A8  -73       28        0    0   1  54e  WPA  CCMP   PSK  harbans kaur
 C8:D7:79:D0:A2:81  -77       26        0    0   8  54e  WPA2 CCMP   PSK  JioFi2_D0A281
 0C:D2:B5:65:FF:42  -80       17        0    0   1  54e  WPA2 CCMP   PSK  Raman
 C8:3A:35:3D:CA:18  -85       10        0    0   1  54e  WPA  CCMP   PSK  bsnl_2646

 BSSID              STATION            PWR   Rate    Lost    Frames  Probe

 (not associated)   00:6F:64:01:25:BE  -51    0 - 1      0        4  Rangi_jiofi3
 (not associated)   BC:D1:1F:0A:6D:AE  -73    0 - 1      0        4  JioFi2_D0A281
 C4:F0:81:A1:0C:99  84:10:0D:9E:A1:CD  -25    0 - 1e     0        5
 C4:F0:81:A1:0C:99  40:F0:2F:DC:7A:59  -31   0e- 0e      0       23
 0C:D2:B5:17:A4:54  00:71:CC:62:94:14   -1   0e- 0       0       30
 0C:D2:B5:17:A4:54  B4:CE:F6:DF:47:5B  -55   0e- 0e      0        4
 0C:D2:B5:65:FF:42  AC:C1:EE:A2:27:CF  -85    0 - 1      0        3

root@kali:~#
```



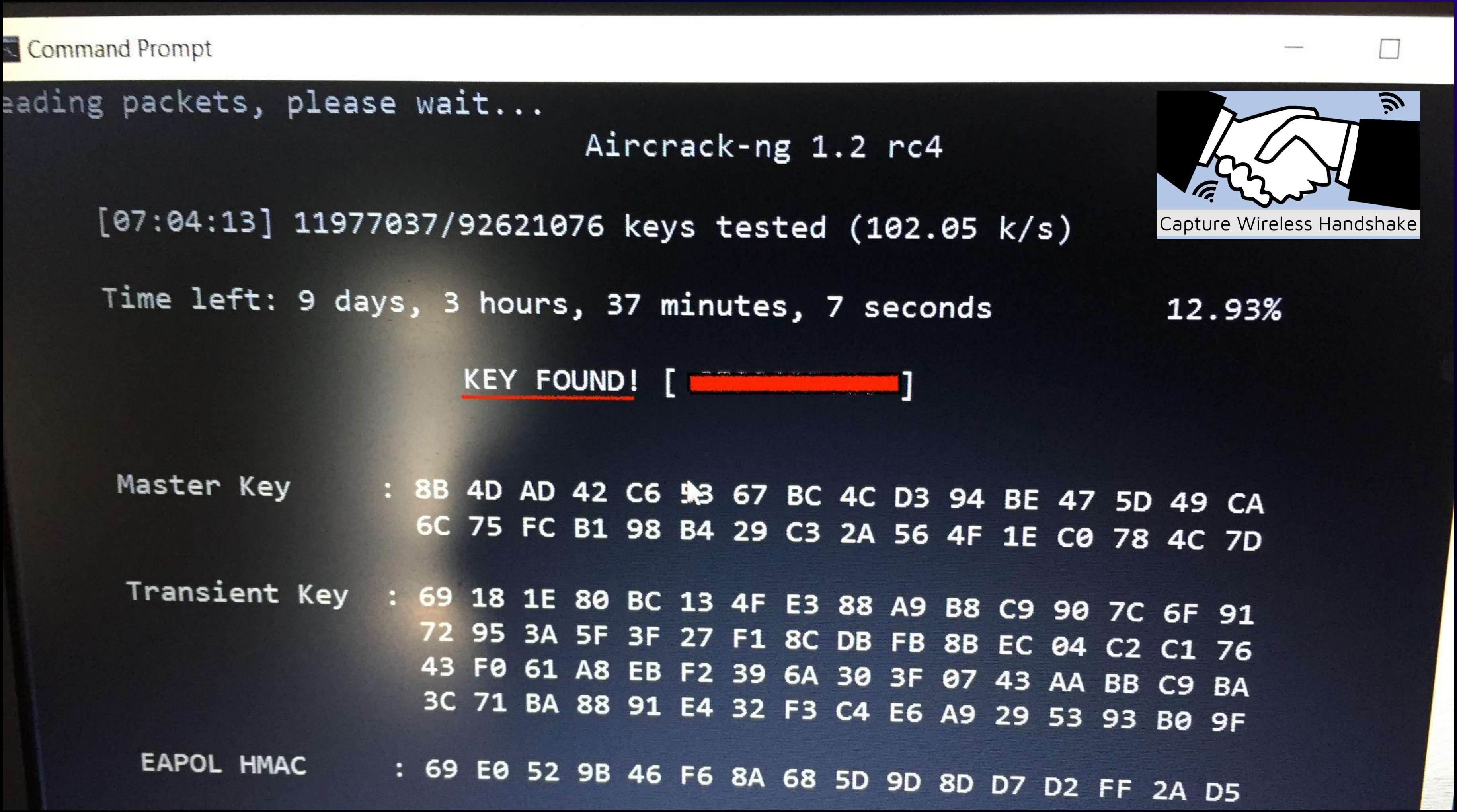
```
CH  2 ][ Elapsed: 1 min ][ 2017-07-28 14:02

BSSID              PWR  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH ESSID

C4:F0:81:A1:0C:99  -25       39       30    0  11  54e  WPA2 CCMP   PSK  Autohaus Meyer
0C:D2:B5:17:A4:54  -53       34       35    0   7  54e  WPA2 CCMP   PSK  jasdeep
0C:D2:B5:65:AF:79  -72       28        0    0   1  54e  WPA2 CCMP   PSK  saanvi
A8:6B:AD:10:8F:08  -72       11        0    0   5  54e. WPA2 CCMP   PSK  Rangi_JioFi3
0C:D2:B5:4C:BC:A8  -73       28        0    0   1  54e  WPA  CCMP   PSK  harbans kaur
C8:D7:79:D0:A2:81  -77       26        0    0   8  54e  WPA2 CCMP   PSK  JioFi2_D0A281
0C:D2:B5:65:FF:42  -80       17        0    0   1  54e  WPA2 CCMP   PSK  Raman
C8:3A:35:3D:CA:18  -85       10        0    0   1  54e  WPA  CCMP   PSK  bsnl_2646

BSSID              STATION            PWR   Rate    Lost    Frames  Probe

(not associated)   00:6F:64:01:25:BE  -51    0 - 1      0        4  Rangi_jiofi3
(not associated)   BC:D1:1F:0A:6D:AE  -73    0 - 1      0        4  JioFi2_D0A281
C4:F0:81:A1:0C:99  84:10:0D:9E:A1:CD  -25    0 - 1e     0        5  iPhone von Bjoern
C4:F0:81:A1:0C:99  40:F0:2F:DC:7A:59  -31    0e- 0e     0        3  Amazon Alexa
0C:D2:B5:17:A4:54  00:71:CC:62:94:14   -1    0e- 0      0        0  Laptop Frank G.
0C:D2:B5:17:A4:54  B4:CE:F6:DF:47:5B  -55    0e- 0e     0        4
0C:D2:B5:65:FF:42  AC:C1:EE:A2:27:CF  -85    0 - 1      0        3

root@kali:~#
```

PC im Haus, Smartphone,
Tablet Laptops etc.


Deauthentication Flooding
AP
authenticated station
2.) deauthentication packet
MAC: 00:11:22:33:44:55
Hacker
1.) deauthentication packet
MAC: 00:11:22:33:44:55



In dem Anmeldeprozess wird das Wi-Fi Passwort verschlüsselt übertragen



```
eading packets, please wait...
                                Aircrack-ng 1.2 rc4

     [07:04:13] 11977037/92621076 keys tested (102.05 k/s)

     Time left: 9 days, 3 hours, 37 minutes, 7 seconds          12.93%

                          KEY FOUND! [ [redacted] ]


      Master Key      : 8B 4D AD 42 C6 53 67 BC 4C D3 94 BE 47 5D 49 CA
                        6C 75 FC B1 98 B4 29 C3 2A 56 4F 1E C0 78 4C 7D

      Transient Key   : 69 18 1E 80 BC 13 4F E3 88 A9 B8 C9 90 7C 6F 91
                        72 95 3A 5F 3F 27 F1 8C DB FB 8B EC 04 C2 C1 76
                        43 F0 61 A8 EB F2 39 6A 30 3F 07 43 AA BB C9 BA
                        3C 71 BA 88 91 E4 32 F3 C4 E6 A9 29 53 93 B0 9F

      EAPOL HMAC      : 69 E0 52 9B 46 F6 8A 68 5D 9D 8D D7 D2 FF 2A D5
```

Dauer des Angriffs: 4 Minuten.

Passwort: “Autohaus1956Meyer?”

Passwort: “Autohaus1956Meyer?”

18 Zeichen, Groß- und Kleinschreibung, Zahlen und Sonderzeichen

Passwort: “Autohaus1956Meyer?”

18 Zeichen, Groß- und Kleinschreibung, Zahlen und Sonderzeichen

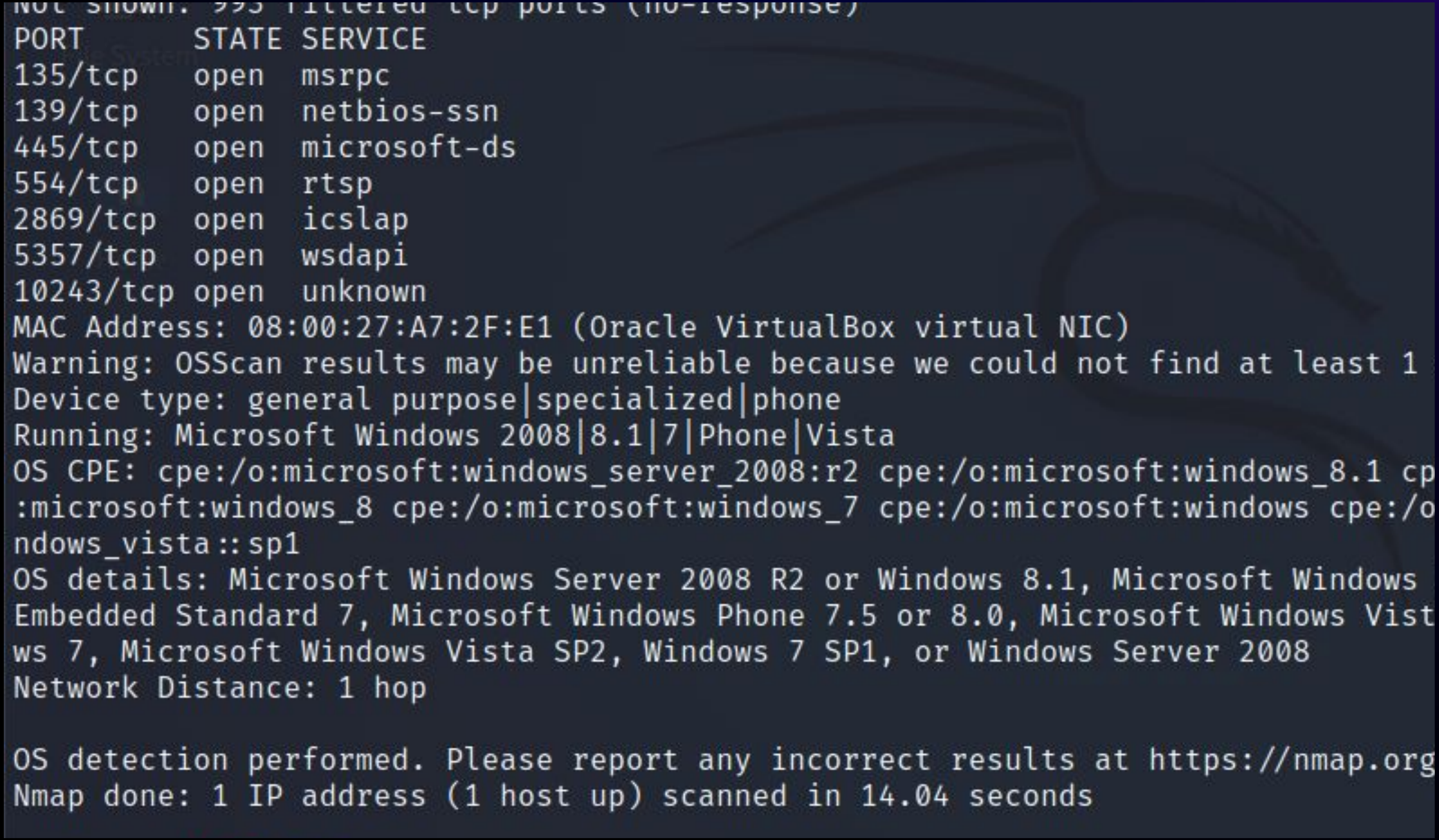
Wörterbuch - Attacke

“Autohaus”
“Meyer”
“Gründungsjahr 1956”
“?”

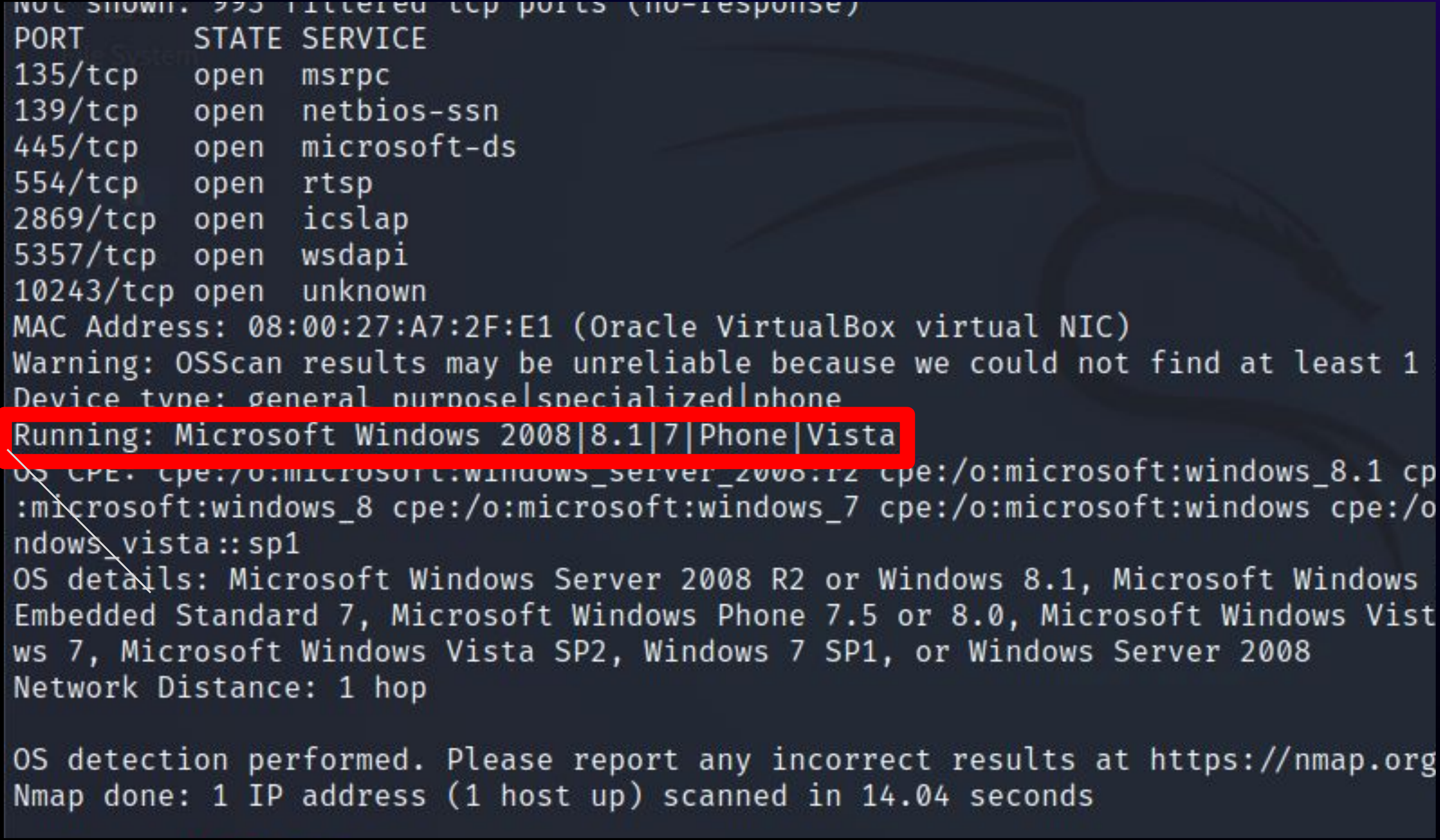
netzsicher.net

Was können wir im Netzwerk anstellen?

Insgesamt 225 Endgeräte



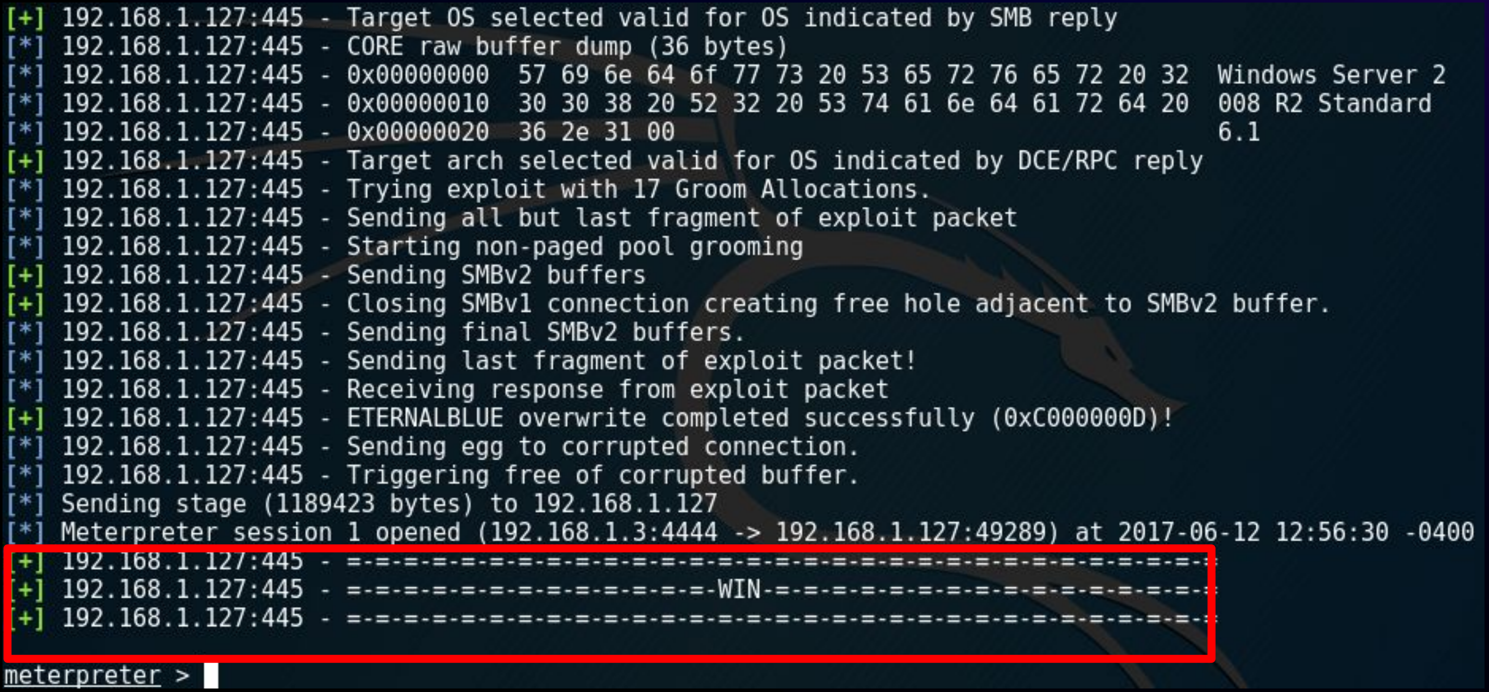
```
Not shown: 993 filtered tcp ports (no-response)
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
554/tcp   open  rtsp
2869/tcp  open  icslap
5357/tcp  open  wsdapi
10243/tcp open  unknown
MAC Address: 08:00:27:A7:2F:E1 (Oracle VirtualBox virtual NIC)
Warning: OSScan results may be unreliable because we could not find at least 1
Device type: general purpose|specialized|phone
Running: Microsoft Windows 2008|8.1|7|Phone|Vista
OS CPE: cpe:/o:microsoft:windows_server_2008:r2 cpe:/o:microsoft:windows_8.1 cp
:microsoft:windows_8 cpe:/o:microsoft:windows_7 cpe:/o:microsoft:windows cpe:/o
ndows_vista::sp1
OS details: Microsoft Windows Server 2008 R2 or Windows 8.1, Microsoft Windows
Embedded Standard 7, Microsoft Windows Phone 7.5 or 8.0, Microsoft Windows Vist
ws 7, Microsoft Windows Vista SP2, Windows 7 SP1, or Windows Server 2008
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at https://nmap.org
Nmap done: 1 IP address (1 host up) scanned in 14.04 seconds
```



```
Not shown: 993 filtered tcp ports (no-response)
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
554/tcp   open  rtsp
2869/tcp  open  icslap
5357/tcp  open  wsdapi
10243/tcp open  unknown
MAC Address: 08:00:27:A7:2F:E1 (Oracle VirtualBox virtual NIC)
Warning: OSScan results may be unreliable because we could not find at least 1
Device type: general purpose|specialized|phone
Running: Microsoft Windows 2008|8.1|7|Phone|Vista
OS CPE: cpe:/o:microsoft:windows_server_2008:r2 cpe:/o:microsoft:windows_8.1 cp
:microsoft:windows_8 cpe:/o:microsoft:windows_7 cpe:/o:microsoft:windows cpe:/o
ndows_vista::sp1
OS details: Microsoft Windows Server 2008 R2 or Windows 8.1, Microsoft Windows
Embedded Standard 7, Microsoft Windows Phone 7.5 or 8.0, Microsoft Windows Vist
ws 7, Microsoft Windows Vista SP2, Windows 7 SP1, or Windows Server 2008
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at https://nmap.org
Nmap done: 1 IP address (1 host up) scanned in 14.04 seconds
```

netzsicher.net

In der Realität sieht das dann so aus:



```
[+] 192.168.1.127:445 - Target OS selected valid for OS indicated by SMB reply
[*] 192.168.1.127:445 - CORE raw buffer dump (36 bytes)
[*] 192.168.1.127:445 - 0x00000000  57 69 6e 64 6f 77 73 20 53 65 72 76 65 72 20 32  Windows Server 2
[*] 192.168.1.127:445 - 0x00000010  30 30 38 20 52 32 20 53 74 61 6e 64 61 72 64 20  008 R2 Standard
[*] 192.168.1.127:445 - 0x00000020  36 2e 31 00                                      6.1
[+] 192.168.1.127:445 - Target arch selected valid for OS indicated by DCE/RPC reply
[*] 192.168.1.127:445 - Trying exploit with 17 Groom Allocations.
[*] 192.168.1.127:445 - Sending all but last fragment of exploit packet
[*] 192.168.1.127:445 - Starting non-paged pool grooming
[+] 192.168.1.127:445 - Sending SMBv2 buffers
[+] 192.168.1.127:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 192.168.1.127:445 - Sending final SMBv2 buffers.
[*] 192.168.1.127:445 - Sending last fragment of exploit packet!
[*] 192.168.1.127:445 - Receiving response from exploit packet
[+] 192.168.1.127:445 - ETERNALBLUE overwrite completed successfully (0xC000000D)!
[*] 192.168.1.127:445 - Sending egg to corrupted connection.
[*] 192.168.1.127:445 - Triggering free of corrupted buffer.
[*] Sending stage (1189423 bytes) to 192.168.1.127
[*] Meterpreter session 1 opened (192.168.1.3:4444 -> 192.168.1.127:49289) at 2017-06-12 12:56:30 -0400
[+] 192.168.1.127:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 192.168.1.127:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-WIN-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 192.168.1.127:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=

meterpreter >
```

netzsicher.net

Exploit: EternalBlue

1. Admin Rechte auf dem System
2. Screensharing
3. Mikrofon Access
4. Webcam Access
5. Keylogger Funktionen
6. Hashdump
7. **Remote Access**

netzsicher.net

Phishing

netzsicher.net

Phishing

Zwei Absichten:

1. Schadsoftware ins Haus schleusen

2. Wichtige Zugangsdaten abgreifen

netzsicher.net

Spoofing

Spoofing:

www.paypal.com

Spoofing:

www.paypal.com

Spoofing:

www.paypal.com

Spoofing:

www.paypaI.com

www.netzsicher.net

info@netzsicher.net

0231 999 440 15