

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
```

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.

