1. Specs and Details

- ram: 1024mb
- cpu: 1core
- memory: 10,93GB

Issue

- kok ini systemd nya udah nyala, pas shutdown mati lagi
- ternyata config systemd nya salah
- tadi gini

```
[Unit]
Description=App Backend for Go
After=network.target

[Service]
ExecStart=/opt/app/go_server
WorkingDirectory=/opt/app
Restart=always
User=www-data
Environment=PORT=8080

[Install]
WantedBy=multi-user.target
```

- sekarang gini bisa

```
[Unit]
Description=App Backend for Go
After=network.target

[Service]
ExecStart=/opt/app/go_server
WorkingDirectory=/opt/app
Restart=always
User=root
Environment="PORT=8080"

[Install]
WantedBy=multi-user.target
```

2. Creds

SSH

- username: mr_nasgor
- pass: nasgor_is_real

Login Page

- username: nasgorman
- pass: fried_egg

FTP

- username: nasgor_ftp
- pass: onion_ring

3. Foothold and Privilege Escalation

First Issue

```
E: Could not get lock /var/lib/dpkg/lock-frontend - open (11: Resource
temporarily unavailable)
E: Unable to acquire the dpkg frontend lock (/var/lib/dpkg/lock-frontend), is
another process using it?
```

- solution

```
mr_nasgor@telur_dadar:~$ sudo killall apt apt-get
mr_nasgor@telur_dadar:~$ sudo rm -f /var/lib/dpkg/lock-frontend
mr_nasgor@telur_dadar:~$ sudo rm -f /var/lib/dpkg/lock
```

- foothold udah ditulis di page http

Privilege Escalation

Sudo misconfig

- set /usr/bin/find buat jadi sudo

```
sudo visudo
```

- set bagian ini

```
%sudo   ALL=(ALL:ALL) NOPASSWD: /usr/bin/find
```

- dah tinggal sudo -l aja itu

4. Services

FTP

Install FTP

```
sudo apt install vsftpd
```

- confignya biarin aja soalnya ga nerapin anonymous, biar pemain brute ftp nya

Setup FTP User creds

```
sudo useradd -m nasgor_ftp
sudo passwd nasgor_ftp #kasih: onion_ring
```

Put your file in FTP folder

- lokasinya di /home/nasgor_ftp
- .for_you.txt

```
Hi Jim,

I forgot my SSH password. Can you put my recipe in my folder?
I'm so busy with my pizza right now.

Here's my SSH username: **mr_nasgor**
Please hurry up!
```

- dev.txt

```
Dear user,
I'm so sorry... The website is unfinished right now.
I forgot my login password... and even worse, I forgot my SSH password too.
Maybe I just can't handle multitasking.
```

```
This pizza is keeping me busy—I feel like I dropped my password somewhere...
but I can't remember anything right now.
Please help me!

- nasgorman
```

Setup permission file for FTP Users

```
sudo chown nasgor_ftp:nasgor_ftp dev.txt
sudo chown nasgor_ftp:nasgor_ftp .for_you.txt
```

Setup config biar user login ftp gabisa pindah pindah

- soalnya ini bukan anonymous di /srv/ftp jadi bisa cd ke mana aja
- set config di /etc/vsftpd.conf biar ga bisa pindah pindah

  ```
  chroot_local_user=YES
  ```

- biar ga error gini

```
500 OOPS: vsftpd: refusing to run with writable root inside chroot()
```

- tambahin set begini juga

```
allow_writeable_chroot=YES
```

HTTP

Build your Frontend and Backend

Frontend

- di frontend yang isinya react, build dulu projectnya biar gausah npm start npm start di server
- di /client, lakukan

```
npm run build
```

- hasilnya ada di /client/dist, nah dist nya jadiin zip aja biar bisa wget nanti 1 folder dist

Backend

- di backend yang isinya go lang, juga di build dulu biar nanti send binary nya aja dan gausah pakai go di server
- di /server, lakukan gini untuk shell powershell, bash beda lagi

```
$env:GOOS="linux"; $env:GOARCH="amd64"; $env:CGO_ENABLED="0"; go build -o backend
```

- fungsinya ini kan khusus binary linux karna env nya ubuntu jadi ya compiler nya harus di custom

Tips

- jadiin 1 folder aja, binary go server nya taruh di dist nya frontend aja /dist client
- nah nanti kompres ke zip aja wget dari target machine

```
python -m http.server
```

- di ubuntu server

```
wget [ip_windows]:8000/dikirim.zip
```

Settings Apache2 server

Setup Frontend server

- install apache2

```
sudo apt install apache2
```

- cek status and start

```
sudo systemctl status apache2
```

- taruh frontend app di server path, dan replace biar jadi main page

```
sudo mv app /var/www
cd /var/www
sudo rm -rf html
sudo mv app html
```

- access frontend server

```
http://[ip_ubuntu]/
```

Setup Backend server

- buat file systemd for backend go server

```
sudo vim /etc/systemd/system/go_server.service
```

- set begini

```

[Unit]
Description=App Backend for Go
After=network.target

[Service]
ExecStart=/opt/app/go_server
WorkingDirectory=/opt/app
Restart=always
User=root
Environment="PORT=8080"

[Install]
WantedBy=multi-user.target
```

- then move ur file

```
sudo mv go_server /opt/app/
```

- chmod file binary nya, then run the services

```
sudo chmod +x go_server
sudo systemctl daemon-reload
sudo systemctl restart go_server
sudo systemctl status go_server
```

- test server, access api server

```
http://[ip_ubuntu]:8080/test
```

Set reverse proxy

- biar ga cors sama biar enak aja gitu
- set di /etc/apache2/sites-available/000-default.conf

```
<VirtualHost *:80>
    ServerName localhost  # Ganti dengan domain jika pakai
    # Atur agar frontend bisa diakses dari /var/www/html
    DocumentRoot /var/www/html
    <Directory "/var/www/html">
        AllowOverride All
        Require all granted
    </Directory>
    # Reverse Proxy untuk backend API
    ProxyPass "/api/" "http://127.0.0.1:8080/" -> jalannya back end dimana
    ProxyPassReverse "/api/" "http://127.0.0.1:8080/" -> response backend
sesuai frontend
    # Log (opsional)
    ErrorLog ${APACHE_LOG_DIR}/error.log
    CustomLog ${APACHE_LOG_DIR}/access.log combined
</VirtualHost>
```

- dan sekalian restart server nya

```
sudo vim /etc/apache2/sites-available/000-default.conf
```

- enable proxypass nya

```
sudo a2enmod proxy
sudo a2enmod proxy_http
sudo a2enmod rewrite
sudo systemctl reload apache2
sudo systemctl status apache2
```

- sekarang coba login di login page nya, nasgorman:fried_egg

Settings the others

- set robots.txt di /var/www/html/robots.txt

```
sudo vim /var/www/html/robots.txt
```

- set begini

```
User-agent: *
Disallow: /username_ftp_is
Disallow: /nasgor_ftp
```

- set secret page, and wordlists in there

```
sudo mkdir /var/www/html/secret
sudo vim /var/www/html/secret/recipes.txt
```

- recipes.txt begini

```
fried_egg
sauce
ketchup
burger
noodle
meatball
pizza
coffee
fries
chips
ramen
chocolate
lasagna
onion_ring
spaghetti
taco
sandwich
donut
cheesecake
hotdog
curry
sushi
steak
burrito
milkshake
```

Next step

- karna kalau udah selesai login dapatnya ini

> /bmFzZ29y

- atau itu base64 dari /nasgor
- jadi nanti di /var/www/html/nasgor
- kasih index.html isinya ini

```
<body>
  <p>this pizza is make me busy</p>
  <p>i cant do programming with cook in 1 moment</p>
  <p>maybe i need to rest</p>
  <small>soon will be useful</small>
  <small>nasgor_is_real</small>
</body>
```

- buat attacker login nantinya

5. Flags

Then set your flags

- di /home/mr_nasgor/user.txt sama di /root/root.txt
- user: FLAG{ef24b324f3de13c6fc62cacfe2ba6fe5}
- root: FLAG{fa0712037e35cc38bbff0863f349cb26}