HTB Analytics

Enumeration

`sudo nmap -sC -sV -oA nmap/analytics 10.10.11.233`
`gobuster vhost -u http://analytical.htb -w /opt/SecLists/Discovery/DNS/subdomains-top1million-20000.txt`

Discovery

Endpoints

- `analytical.htb`
- `data.analytical.htb`
  - `/api`
    - `/session/properties`
    - `/setup/validate`

Technologies

- Postgres
- Metabase
- H2 Database
- Linux Kernel 6.2.0

Findings

- found via — `api/session/properties`
  - `{"setup-token":"249fa03d-fd94-4d5b-b94f-b4ebf3df681f"}`
- found via — reverse shell enviroment
  - META_PASS=An4lytics_ds20223#
  - META_USER=metalytics
- found via — `cat /metabase.db/metabase.db.mv.db | grep metalytics`
  - `metalytics@data.htb`
  - `metalytics@analytical.htb`

Credentials

- User

- email: `metalytics@analytical.htb`
- user: `metalytics`
- password: `An4lytics_ds20223#`

Vulnerabilites

- Outdated Metabase — CVE-2023–38646
- LPE OverlayFS — CVE-2023-2640-CVE-2023-32629
- LPE OverlayFS — CVE-2021-3493

Exploitation

- Run `rev-shell.py` to RCE and gain reverse shell
- Explore the metabase container and gain credentials
- ssh to machine using stolen credentials
- use either the `privesc` or `privesc.sh` to LPE privesc

Appendix

User Flag: `a4912527f033ae8deb46338f0ff3c6a2`
Root Flag: `837945ee80cde75d6be855cae8dfd22a`