第十四课 MetaSploit探测内网存活ftp服务.

Author：陈殷

公众号：山丘安全攻防实验室

这里我们用到的模块是：

• auxiliary/scanner/ftp/ftp_version 发现内网ftp服务

使用模块

```
msf5 > use auxiliary/scanner/ftp/ftp_
use auxiliary/scanner/ftp/ftp_login    use auxiliary/scanner/ftp/ftp_version
msf5 > use auxiliary/scanner/ftp/ftp_version
```

查看选项

```
msf5 auxiliary(scanner/ftp/ftp_version) > show options

Module options (auxiliary/scanner/ftp/ftp_version):

   Name     Current Setting      Required  Description
   ----     ---------------      --------  -----------
   FTPPASS  mozilla@example.com  no        The password for the specified username
   FTPUSER  anonymous            no        The username to authenticate as
   RHOSTS                        yes       The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>'
   RPORT    21                   yes       The target port (TCP)
   THREADS  1                    yes       The number of concurrent threads
```

填写参数

```
msf5 auxiliary(scanner/ftp/ftp_version) > set rhosts 192.168.30.0/24
rhosts => 192.168.30.0/24
msf5 auxiliary(scanner/ftp/ftp_version) > set threads 50
threads => 50
msf5 auxiliary(scanner/ftp/ftp_version) > run
```

运行

```
msf5 auxiliary(scanner/ftp/ftp_version) > run

[*] 192.168.30.0/24:21     - Scanned  52 of 256 hosts (20% complete)
[*] 192.168.30.0/24:21     - Scanned  87 of 256 hosts (33% complete)
[*] 192.168.30.0/24:21     - Scanned  96 of 256 hosts (37% complete)
[*] 192.168.30.0/24:21     - Scanned 103 of 256 hosts (40% complete)
[+] 192.168.30.134:21      - FTP Banner: '220 (vsFTPd 2.3.4)\x0d\x0a'
[*] 192.168.30.0/24:21     - Scanned 129 of 256 hosts (50% complete)
[*] 192.168.30.0/24:21     - Scanned 191 of 256 hosts (74% complete)
[*] 192.168.30.0/24:21     - Scanned 215 of 256 hosts (83% complete)
[*] 192.168.30.0/24:21     - Scanned 217 of 256 hosts (84% complete)
[*] 192.168.30.0/24:21     - Scanned 236 of 256 hosts (92% complete)
[*] 192.168.30.0/24:21     - Scanned 256 of 256 hosts (100% complete)
[*] Auxiliary module execution completed
```

扫描完成

文章作者：陈殷

文章出处：山丘安全攻防实验室


山丘