专注APT攻击与防御

https://micropoor.blogspot.com/

在办公区的内网中，充斥着大量的ftp文件服务器。其中不乏有部分敏感文件，也许有你需要的密码文件，也许有任务中的目标文件等。本季从讲述内网ftp服务器的发现以及常用的相关模块。

靶机介绍：

- 靶机一：Windows 2003 | 192.168.1.115
- 靶机二：Debian | 192.168.1.5

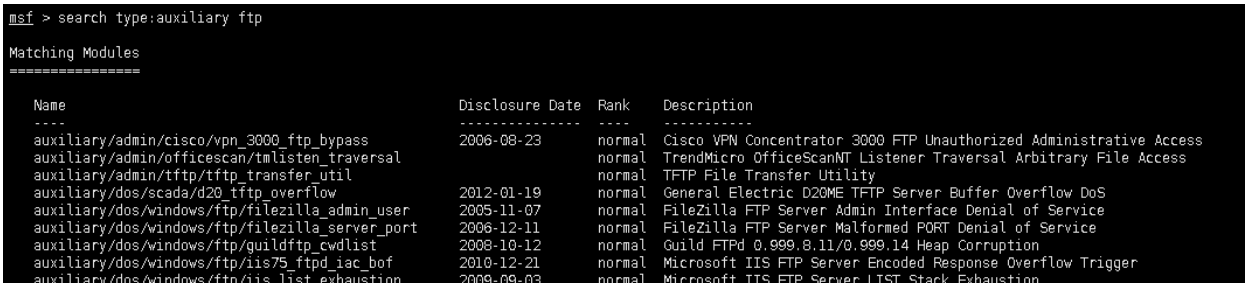
msf内置search模块，在实战中，为了更快速的找到对应模块，它提供了type参数（未来会具体讲到模块参数），以ftp模块为例。

msf > **search type:auxiliary ftp**

Matching Modules
==========

Name	Disclosure Date	Rank	Description
auxiliary/admin/cisco/vpn_3000_ftp_bypass	2006-08-23	normal	Cisco VPN Concentrator 3000 FTP Unauthorized Administrative Access
auxiliary/admin/officescan/tmlisten_traversal		normal	TrendMicro OfficeScanNT Listener Traversal Arbitrary File Access
auxiliary/admin/tftp/tftp_transfer_util		normal	TFTP File Transfer Utility
auxiliary/dos/scada/d20_tftp_overflow	2012-01-19	normal	General Electric D20ME TFTP Server Buffer Overflow DoS
auxiliary/dos/windows/ftp/filezilla_admin_user	2005-11-07	normal	FileZilla FTP Server Admin Interface Denial of Service

.....



auxiliary/scanner/ftp/ftp_version

```
msf 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   192.168.1.115        yes       The target address range or CIDR identifier
   RPORT    21                   yes       The target port (TCP)
   THREADS  20                   yes       The number of concurrent threads

msf auxiliary(scanner/ftp/ftp_version) > setg rhosts 192.168.1.254
rhosts => 192.168.1.254
msf auxiliary(scanner/ftp/ftp_version) > exploit

[+] 192.168.1.254:21      - FTP Banner: '220 ProFTPD 1.3.1 Server (Debian) [::ffff:192.168.1.254]\x0d\x0a'
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

auxiliary/scanner/ftp/ftp_login

```
msf auxiliary(scanner/ftp/ftp_login) > show options

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

   Name              Current Setting  Required  Description
   ----              ---------------  --------  -----------
   BLANK_PASSWORDS   false            no        Try blank passwords for all users
   BRUTEFORCE_SPEED  5                yes       How fast to bruteforce, from 0 to 5
   DB_ALL_CREDS      false            no        Try each user/password couple stored in the current database
   DB_ALL_PASS       false            no        Add all passwords in the current database to the list
   DB_ALL_USERS      false            no        Add all users in the current database to the list
   PASSWORD          123              no        A specific password to authenticate with
   PASS_FILE                          no        File containing passwords, one per line
   Proxies                            no        A proxy chain of format type:host:port[,type:host:port][...]
   RECORD_GUEST      false            no        Record anonymous/guest logins to the database
   RHOSTS            192.168.1.115    yes       The target address range or CIDR identifier
   RPORT             21               yes       The target port (TCP)
   STOP_ON_SUCCESS   false            yes       Stop guessing when a credential works for a host
   THREADS           20               yes       The number of concurrent threads
   USERNAME          123              no        A specific username to authenticate as
   USERPASS_FILE                      no        File containing users and passwords separated by space, one pair per
   USER_AS_PASS      false            no        Try the username as the password for all users
   USER_FILE                          no        File containing usernames, one per line
   VERBOSE           true             yes       Whether to print output for all attempts

msf auxiliary(scanner/ftp/ftp_login) > run

[*] 192.168.1.115:21      - 192.168.1.115:21 - Starting FTP login sweep
[+] 192.168.1.115:21      - 192.168.1.115:21 - Login Successful: 123:123
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

auxiliary/scanner/ftp/anonymous

```
msf auxiliary(scanner/ftp/ftp_login) > use auxiliary/scanner/ftp/anonymous
msf auxiliary(scanner/ftp/anonymous) > show options

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

   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   192.168.1.115        yes       The target address range or CIDR identifier
   RPORT    21                   yes       The target port (TCP)
   THREADS  20                   yes       The number of concurrent threads

msf auxiliary(scanner/ftp/anonymous) > exploit

[+] 192.168.1.115:21      - 192.168.1.115:21 - Anonymous READ/WRITE (220 Slyar Ftpserver)
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

当然msf也内置了nmap，来内网大量发现FTP存活主机，参数与使用与nmap一致。

msf auxiliary(scanner/ftp/anonymous) > db_nmap -sS -T4 -p21 192.168.1.115

```
msf auxiliary(scanner/ftp/anonymous) > db_nmap -sS -T4 -p21 192.168.1.115
[*] Nmap: Starting Nmap 7.40 ( https://nmap.org ) at 2018-12-28 07:58 EST
[*] Nmap: Nmap scan report for 192.168.1.115
[*] Nmap: Host is up (0.0015s latency).
[*] Nmap: PORT   STATE  SERVICE
[*] Nmap: 21/tcp closed ftp
[*] Nmap: MAC Address: 00:0C:29:AF:CE:CC (VMware)
[*] Nmap: Nmap done: 1 IP address (1 host up) scanned in 0.41 seconds
msf auxiliary(scanner/ftp/anonymous) >
```

msf更多针对了ftpd。

```
msf auxiliary(scanner/ftp/anonymous) > search ftpd

Matching Modules
================

   Name                                          Disclosure Date  Rank       Description
   ----                                          ---------------  ----       -----------
   auxiliary/dos/windows/ftp/guildftp_cwdlist    2008-10-12       normal     Guild FTPd 0.999.8.11/0.999.14 Heap Corruption
   auxiliary/dos/windows/ftp/iis75_ftpd_iac_bof  2010-12-21       normal     Microsoft IIS FTP Server Encoded Response Overflow Trigger
   exploit/freebsd/ftp/proftp_telnet_iac         2010-11-01       great      ProFTPD 1.3.2rc3 - 1.3.3b Telnet IAC Buffer Overflow (FreeBSD)
   exploit/linux/ftp/proftp_sreplace             2006-11-26       great      ProFTPD 1.2 - 1.3.0 sreplace Buffer Overflow (Linux)
   exploit/linux/ftp/proftp_telnet_iac           2010-11-01       great      ProFTPD 1.3.2rc3 - 1.3.3b Telnet IAC Buffer Overflow (Linux)
   exploit/linux/misc/netsupport_manager_agent   2011-01-08       average    NetSupport Manager Agent Remote Buffer Overflow
   exploit/multi/ftp/pureftpd_bash_env_exec      2014-09-24       excellent  Pure-FTPd External Authentication Bash Environment Variable Code Injection (Shellshock)
   exploit/multi/ftp/wuftpd_site_exec_format     2000-06-22       great      WU-FTPD SITE EXEC/INDEX Format String Vulnerability
   exploit/unix/ftp/proftpd_133c_backdoor        2010-12-02       excellent  ProFTPD-1.3.3c Backdoor Command Execution
   exploit/unix/ftp/proftpd_modcopy_exec         2015-04-22       excellent  ProFTPD 1.3.5 Mod_Copy Command Execution
   exploit/unix/ftp/vsftpd_234_backdoor          2011-07-03       excellent  VSFTPD v2.3.4 Backdoor Command Execution
   exploit/windows/ftp/ayukov_nftp               2017-10-21       normal     Ayukov NFTP FTP Client Buffer Overflow
   exploit/windows/ftp/comsnd_ftpd_fmtstr        2012-06-08       good       ComSndFTP v1.3.7 Beta USER Format String (Write4) Vulnerability
   exploit/windows/ftp/freeftpd_pass             2013-08-20       normal     freeFTPd PASS Command Buffer Overflow
   exploit/windows/ftp/freeftpd_user             2005-11-16       average    freeFTPd 1.0 Username Overflow
   exploit/windows/ftp/ms09_053_ftpd_nlst        2009-08-31       great      MS09-053 Microsoft IIS FTP Server NLST Response Overflow
   exploit/windows/ftp/netterm_netftpd_user      2005-04-26       great      NetTerm NetFTPD USER Buffer Overflow
   exploit/windows/ftp/open_ftpd_wbem            2012-06-18       excellent  Open-FTPD 1.2 Arbitrary File Upload
   exploit/windows/ftp/sami_ftpd_list            2013-02-27       low        Sami FTP Server LIST Command Buffer Overflow
   exploit/windows/ftp/sami_ftpd_user            2006-01-24       normal     KarjaSoft Sami FTP Server v2.02 USER Overflow
   exploit/windows/ftp/sasser_ftpd_port          2004-05-10       average    Sasser Worm avserve FTP PORT Buffer Overflow
   exploit/windows/ftp/servu_mdtm                2004-02-26       good       Serv-U FTPD MDTM Overflow
   exploit/windows/ftp/slimftpd_list_concat      2005-07-21       great      SlimFTPd LIST Concatenation Overflow
   exploit/windows/ftp/vermillion_ftpd_port      2009-09-23       great      Vermillion FTP Daemon PORT Command Memory Corruption
   exploit/windows/ftp/warftpd_165_pass          1998-03-19       average    War-FTPD 1.65 Password Overflow
   exploit/windows/ftp/warftpd_165_user          1998-03-19       average    War-FTPD 1.65 Username Overflow
   exploit/windows/ftp/wftpd_size                2006-08-23       average    Texas Imperial Software WFTPD 3.23 SIZE Overflow
   exploit/windows/ssh/freeftpd_key_exchange     2006-05-12       average    FreeFTPd 1.0.10 Key Exchange Algorithm String Buffer Overflow
   exploit/windows/tftp/tftpd32_long_filename    2002-11-19       average    TFTPD32 Long Filename Buffer Overflow
   exploit/windows/tftp/tftpdwin_long_filename   2006-09-21       great      TFTPDWIN v0.4.2 Long Filename Buffer Overflow
```

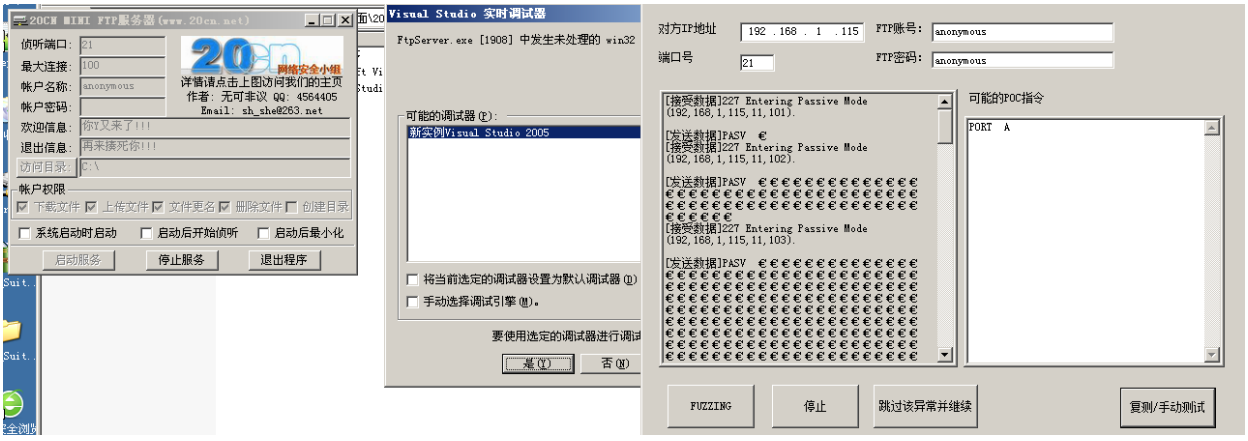
ftp本地模糊测试辅助模块：

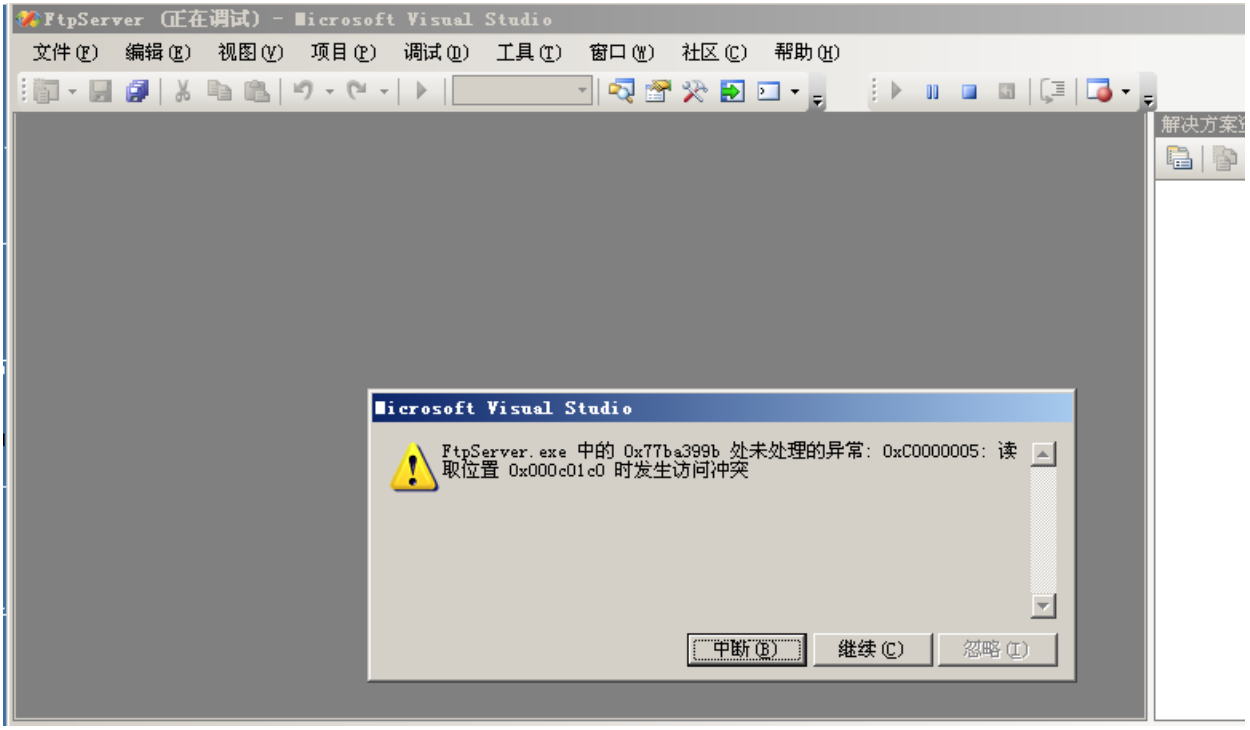
```
msf auxiliary(fuzzers/ftp/ftp_pre_post) > search fuzzers/ftp/

Matching Modules
================

   Name                                Disclosure Date  Rank    Description
   ----                                ---------------  ----    -----------
   auxiliary/fuzzers/ftp/client_ftp                     normal  Simple FTP Client Fuzzer
   auxiliary/fuzzers/ftp/ftp_pre_post                   normal  Simple FTP Fuzzer
```

auxiliary/fuzzers/ftp/ftp_pre_post

```
msf auxiliary(fuzzers/ftp/ftp_pre_post) > show options

Module options (auxiliary/fuzzers/ftp/ftp_pre_post):

   Name          Current Setting      Required  Description
   ----          ---------------      --------  -----------
   CONNRESET     true                 no        Break on CONNRESET error
   DELAY         1                    no        Delay between connections in seconds
   ENDSIZE       20000                no        Fuzzing string endsize
   FASTFUZZ      true                 no        Only fuzz with cyclic pattern
   PASS          mozilla@example.com  no        Password
   RHOSTS        192.168.1.115        yes       The target address range or CIDR identifier
   RPORT         21                   yes       The target port (TCP)
   STARTATSTAGE  1                    no        Start at this test stage
   STARTSIZE     10                   no        Fuzzing string startsize
   STEPSIZE      10                   no        Increase string size each iteration with this number of chars
   STOPAFTER     2                    no        Stop after x number of consecutive errors
   THREADS       20                   yes       The number of concurrent threads
   USER          anonymous            no        Username

msf auxiliary(fuzzers/ftp/ftp_pre_post) > exploit

[*] 192.168.1.115:21 - Connecting to host 192.168.1.115 on port 21
[*] 192.168.1.115:21 - [Phase 1] Fuzzing without command - 2018-12-28 07:06:20 -0500
[*] 192.168.1.115:21 -  Character : Cyclic (1/1)
[*] 192.168.1.115:21 -    -> Fuzzing size set to 10 (Cyclic)
```

关于ftp的f本地uzzer，更推荐的是本地fuzz，msf做辅助poc。





关于后期利用，poc编写，在未来的季中会继续讲述。

- Micropoor