Cheatography

Basic Mimikatz Usage Cheat Sheet

by HangryHippo (wbtaylor) via cheatography.com/147129/cs/31951/

MODULES

standard	This is the main module of mimikatz, it contains quick commands to operate with the tool. For this particular one, no need to prefix command by the module name (but it works too), eg: exit is the same as standard::exit.
privilege	This module provides some commands to manipulate privilege on mimikatz process.
crypto	This module, one of the oldest, plays with CryptoAPI functions. Basically it's a little certutil that benefit of token impersonation, patch legacy CryptoAPI functions and patch CNG key isolation service.
sekurlsa	This module extracts passwords, keys, pin codes, tickets from the memory of lsass (Local Security Authority Subsystem Service)
kerberos	This module can be used without any privilege. It permits to play with official Microsoft Kerberos API and to create offline 'Golden tickets', free, long duration TGT tickets for any users
lsadump	This module interacts with the Windows Local Security Authority (LSA) to extract credentials. Most of these commands require either debug rights (privlege::debug) or local System. By default, the Administrators group has Debug rights. Debug still has to be “activated” by running “privilege::debug”.
vault	This module dumps passwords saved in the Windows Vault.

MODULES (cont)

token	This module deals with the Windows tokens (who does not really like elevating to NT AUTHORITY\ SYSTEM).
event	This module deals with the Windows Event logs (to clear footprints after compromise).
ts	This module deals with the Terminal Services. It can be an alternative for getting clear-text passwords.
process	This module deals with Windows processes. It can also be used for process injection and parent process spoofing.
service	This module can interact with Windows services plus installing the mimikatzsvc service.
net	some functionalities in this module are similar to the Windows net commands. Enumerating sessions and servers configured with different types of Kerberos delegations is also included.
misc	This module is kind of a catch-all for commands that don’t quite fit elsewhere. The most well known commands in this module are MISC::AddSID, MISC::MemSSP, and MISC::Skeleton.

CRYPTO

providers	This command list all providers: CryptoAPI, then CNG if available (NT 6).
stores	This command lists logical store in a system store.

CRYPTO (cont)

sc	This command lists smartcard/token reader(s) on, or deported to, the system. When the CSP is available, it tries to list keys on the smartcard.
scauth	This command creates a client certificate for smartcard authentication, signed by a Certificate Authority
certificates	This command lists certificates and properties of theirs keys. It can export certificates too.
keys	This command lists keys, by provider. It can export keys too.
capi	This patch modify a CryptoAPI function, in the mimikatz process, in order to make unexportable keys, exportable (no specifig right other than access to the private key is needed) This is only useful when the keys provider is one of: Microsoft Base Cryptographic Provider v1.0, Microsoft Enhanced Cryptographic Provider v1.0, Microsoft Enhanced RSA and AES Cryptographic Provider, Microsoft RSA SChannel Cryptographic Provider, Microsoft Strong Cryptographic Provider
cng	This patch modify KeyIso service, in LSASS process, in order to make unexportable keys, exportable. This is only useful when the keys provider is Microsoft Software Key Storage Provider (you do not need to patch CNG for other providers).

VAULT

cred	Enumerates vault credentials
list	Lists saved credentials in the Windows Vault such as scheduled tasks, RDP, Internet Explorer for the current user

TS

multirdp	(experimental) Patch Terminal Server service to allow multiple users
sessions	List TS/RDP sessions.

STANDARD

exit	Quits mimikatz, after cleaning routines.
cls	Clears screen, by filling the console window with spaces.
answer	Gives the Answer to the Ultimate Question of Life, the Universe, and Everything.
coffee	Because everyone deserves a good coffee.
sleep	Sleeps an amount of milliseconds (1000 ms by default).
log	Logs all outputs to a file (mimikatz.log by default).
base64	Switches from file writing on the disk, to Base64 output instead.
version	Displays versions of mimikatz and Windows
cd	Change or display current directory

SEKURLSA

logonpasswords	Lists all available provider credentials. This usually shows recently logged on user and computer credentials.
pth	Pass-the-Hash and Over-Pass-the-Hash (aka pass the key).

SEKURLSA (cont)

tickets	List and export Kerberos tickets of all sessions.
ekeys	List Kerberos encryption keys
dpapi	Read masterkeys from memory
minidump	Switch to LSASS minidump process context
process	Switches (or reinits) to LSASS process context
searchpasswords	Present username and passwords available in memory
msv	Responsible for collecting password hashes from the LSASS address space
wdigest	List WDigest credentials
kerberos	List Kerberos credentials for all authenticated users (including services and computer account)
tspkg	Used for Terminal Server authentication
krbtg	Get Domain Kerberos service account (KRBTGT)password data
ssp	Lists Security Support Provider credentials
credman	List Credentials Manager

EVENT

clear	Clear an event log
drop	(experimental) Patch Events service to avoid new events

Run privilege::debug then event::drop to patch the event log. Then run Event::Clear to clear the event log without any log cleared event (1102) being logged.

SERVICE

+ (plus sign)	Install Mimikatz service (‘mimikatzsvc’)
- (minus sign)	Uninstall Mimikatz service (‘mimikatzsvc’)

SERVICE (cont)

list	List Services
preshutdown	Pre-shuts down a specified service by sending a SERVICE_CONTROL_PRESHUTDOWN signal
remove	Removes the specified service (It must be used with caution)
resume	Resumes a specified service, after successful suspending, by sending a SERVICE_CONTROL_CONTINUE signal
shutdown	Shuts down a specified service by sending a SERVICE_CONTROL_SHUTDOWN signal
start	Start a service
stop	Stops a specified service by sending a SERVICE_CONTROL_STOP signal
suspend	Suspend the service. It sends a SERVICE_CONTROL_PAUSE signal

MISC

aadcookie	Can be used to dump the Azure Panel's session cookie from login.microsoftonline.com
clip	Monitors clipboard. CTRL+C stops the monitoring
cmd	Launches the command prompt
compress	Performs a self compression of mimikatz
detours	(Experimental) Tries to enumerate all modules with Detours-like hooks
efs	Mimikatz's implementation of the MS-EFSR abuse (PetitPotam), an authentication coercion technique
lock	Locks the screen. It can come in handy with misc::memssp

MISC (cont)

memssp	Patches LSASS by injecting a new Security Support Provider (a DLL is registered)
mflt	Identifies Windows minifilters inside mimikatz, without using fltmc.exe. It can also assist in fingerprinting security products, by altitude too (Gathers details on loaded drivers, including driver altitude)
ncroutemon	Displays Juniper network connect (without route monitoring)
ngcsign	Can be used to dump the NGC key (Windows Hello keys) signed with the symmetric pop key.
printnightmare	Can be used to exploit the PrintNightMare vulnerability in both [MS-RPRN RpcAddPrinterDriverEx] and [MS-PAR AddPrinterDriverEx].
regedit	Launches the registry editor
sccm	Decrypts the password field in the SC_UserAccount table in the SCCM database
shadowcopies	Used to list the available shadow copies on the system
skeleton	Injects a "Skeleton Key" into the LSASS process on the domain controller
spooler	Mimikat's implementation of the MS-RPRN abuse (PrinterBug), an authentication coercion technique
taskmgr	Launches the task manager
wp	Sets up a wallpaper
xor	Performs XOR decoding/encoding on a provided file with 0x42 default key

PRIVILEGE

debug	Ask for debug privilege for mimikatz process.

The debug privilege allows someone to debug a process that they wouldn’t otherwise have access to. For example, a process running as a user with the debug privilege enabled on its token can debug a service running as local system.
Remark: ERROR kuhl_m_privilege_simple ; RtlAdjustPrivilege (20) c0000061 means that the required privilege is not held by the client

LSADUMP

sam	This command dumps the Security Account Managers (SAM) database. It contains NTLM, and sometimes LM hash, of users passwords.
secrets	Get the SysKey to decrypt SECRETS entries (from registry or hives).
setntlm	Used to perform a password reset without knowing the user's current password. It can be useful during an active directory Access Control (ACL) abuse scenario
lsa	Ask LSA Server to retrieve SAM/AD enterprise (normal, patch on the fly or inject). Use to dump all Active Directory domain credentials from a Domain Controller or lsass.dmp dump file. Also used to get specific account credential such as krbtgt with the parameter /name: “/name:krbtgt”
dcsync	Ask a DC to synchronize an object (get password data for account). No need to run code on DC.
trust	Ask LSA Server to retrieve Trust Auth Information (normal or patch on the fly). Dumps trust keys (passwords) for all associated trusts (domain/forest).

LSADUMP (cont)

backupkeys	Dumps the DPAPI backup keys from the Domain Controller
cache	Can be used to enumerate Domain Cached Credentials from registry. It does so by acquiring the SysKey to decrypt NL$KM (binary protected value) and then MSCache(v1/v2)
changentlm	Used to change the password of a user
zerologon	Detects and exploits the ZeroLogon vulnerability

KERBEROS

ptt	Pass-the-Ticket. Typically used to inject a stolen or forged Kerberos ticket (golden/silver/trust).
golden / silver	This command create Kerberos ticket, a TGT or a TGS with arbitrary data, for any user you want, in groups you want
tgt	Displays informations about the TGT of the current session.
list	Lists and export Kerberos tickets (TGT and TGS) of the current session.
purge	Purges all tickets of the current session.

TOKEN

elevate	Used to impersonate a token. Used to elevate permissions to SYSTEM (default) or find a domain admin token on the box using the Windows API.
list	List all tokens of the system
revert	Revert to previous token
run	Executes a process with its token
whoami	Display current identity

PROCESS

exports	Lists all the exported functions from the DLLs each running process is using. If a /pid is not specified, then exports for mimikatz.exe will be displayed
imports	Lists all the imported functions from the DLLs each running process is using. If a /pid is not specified, then imports for mimikatz.exe will be displayed
list	Lists all running processes. It uses the NtQuerySystemInformation Windows Native API function
resume	Resumes a suspended process by using the NtResumeProcess Windows Native API function
start	Starts a process by using the CreateProcess Win32 API function. The PID of the process is also displayed
stop	Terminates a process by using the NtTerminateProcess Windows Native API function. The Win32 API equal one is TerminateProcess
suspend	Suspends a process by using the NtSuspendProcess Windows Native API function
run	Creates a process by using the CreateProcessAsUser Win32 API function. The CreateEnvironmentBlock is also utilized
runp	Runs a subprocess under a parent process (Default parent process is LSASS.exe). It can also be used for lateral movement and process spoofing

NET

alias	Displays more information about the local group memberships including Remote Desktop Users, Distributed COM Users, etc
deleg	Checks for Kerberos delegations
group	Displays the local groups
if	Displays the available local IP addresses and the hostname
serverinfo	Displays information about the logged in server
session	Displays the active sessions through NetSessionEnum() Win32 API function
share	Displays the available shares
stats	Displays when the target was booted
tod	Displays the current time
trust	Displays information for the active directory forest trust(s)
user	Displays the local users
wsession	Displays the active sessions through NetWkstaUserEnum() Win32 API function