

Instalada desde el repo de github:

```
# Windows

amcache           # Print AmCache information
apihooks          # Detect API hooks in process and kernel memory
atoms             # Print session and window station atom tables
atomscan         # Pool scanner for atom tables
auditpol         # Prints out the Audit Policies from HKLM\SECURITY\Policy\PolAdtEv
bigpools         # Dump the big page pools using BigPagePoolScanner
bioskbd          # Reads the keyboard buffer from Real Mode memory
cachedump        # Dumps cached domain hashes from memory
callbacks        # Print system-wide notification routines
clipboard        # Extract the contents of the windows clipboard
cmdline          # Display process command-line arguments
cmdscan         # Extract command history by scanning for _COMMAND_HISTORY
connections      # Print list of open connections [Windows XP and 2003 Only]
connscan        # Pool scanner for tcp connections
consoles         # Extract command history by scanning for _CONSOLE_INFORMATION
crashinfo        # Dump crash-dump information
deskscan        # Poolscanner for tagDESKTOP (desktops)
devicetree       # Show device tree
dlldump         # Dump DLLs from a process address space
dlllist         # Print list of loaded dlls for each process
driverirp       # Driver IRP hook detection
drivermodule     # Associate driver objects to kernel modules
driverscan      # Pool scanner for driver objects
dumpcerts       # Dump RSA private and public SSL keys
dumpfiles       # Extract memory mapped and cached files
dumpregistry    # Dumps registry files out to disk
editbox         # Displays information about Edit controls. (Listbox experimental.)
envvars         # Display process environment variables
eventhooks      # Print details on windows event hooks
evtlogs         # Extract Windows Event Logs (XP/2003 only)
filescan        # Pool scanner for file objects
gahti           # Dump the USER handle type information
gditimers       # Print installed GDI timers and callbacks
gdt             # Display Global Descriptor Table
getservicesids  # Get the names of services in the Registry and return Calculated SID
getsids        # Print the SIDs owning each process
handles        # Print list of open handles for each process
hashdump       # Dumps passwords hashes (LM/NTLM) from memory
hibinfo        # Dump hibernation file information
hivedump       # Prints out a hive
hivelist       # Print list of registry hives.
hivescan       # Pool scanner for registry hives
hpakextract    # Extract physical memory from an HPAK file
hpakinfo       # Info on an HPAK file
idt            # Display Interrupt Descriptor Table
iehistory      # Reconstruct Internet Explorer cache / history
imagecopy      # Copies a physical address space out as a raw DD image
imageinfo      # Identify information for the image
impscan       # Scan for calls to imported functions
joblinks       # Print process job link information
kdbgscan      # Search for and dump potential KDBG values
kpcrscan      # Search for and dump potential KPCR values
ldrmodules    # Detect unlinked DLLs
limeinfo       # Dump Lime file format information
lsadump       # Dump (decrypted) LSA secrets from the registry
machoinfo     # Dump Mach-0 file format information
malfind       # Find hidden and injected code
mbrparser     # Scans for and parses potential Master Boot Records (MBRs)
memdump       # Dump the addressable memory for a process
memmap        # Print the memory map
messagehooks   # List desktop and thread window message hooks
mftparser     # Scans for and parses potential MFT entries
moddump       # Dump a kernel driver to an executable file sample
modscan       # Pool scanner for kernel modules
```

```
modules # Print list of loaded modules
multiscan # Scan for various objects at once
mutantscan # Pool scanner for mutex objects
netscan # Scan a Vista (or later) image for connections and sockets
notepad # List currently displayed notepad text
objtypescan # Scan for Windows object type objects
patcher # Patches memory based on page scans
poolpeek # Configurable pool scanner plugin
pooltracker # Show a summary of pool tag usage
printkey # Print a registry key, and its subkeys and values
privs # Display process privileges
procdump # Dump a process to an executable file sample
pslist # Print all running processes by following the EPROCESS lists
psscan # Pool scanner for process objects
pstree # Print process list as a tree
psxview # Find hidden processes with various process listings
qemuinfo # Dump Qemu information
raw2dmp # Converts a physical memory sample to a windbg crash dump
screenshot # Save a pseudo-screenshot based on GDI windows
servicediff # List Windows services (ala Plugx)
sessions # List details on _MM_SESSION_SPACE (user logon sessions)
shellbags # Prints ShellBags info
shimcache # Parses the Application Compatibility Shim Cache registry key
shutdowntime # Print ShutdownTime of machine from registry
sockets # Print list of open sockets
sockscan # Pool scanner for tcp socket objects
ssdt # Display SSDT entries
strings # Match physical offsets to virtual addresses (may take a while, VERY verbose)
svcsan # Scan for Windows services
symlinkscan # Pool scanner for symlink objects
thrdscan # Pool scanner for thread objects
threads # Investigate _ETHREAD and _KTHREADs
timeliner # Creates a timeline from various artifacts in memory
timers # Print kernel timers and associated module DPCs
truecryptmaster # Recover TrueCrypt 7.1a Master Keys
truecryptpassphrase # TrueCrypt Cached Passphrase Finder
truecryptsummary # TrueCrypt Summary
unloadedmodules # Print list of unloaded modules
userassist # Print userassist registry keys and information
userhandles # Dump the USER handle tables
vaddump # Dumps out the vad sections to a file
vadinfo # Dump the VAD info
vadtree # Walk the VAD tree and display in tree format
vadwalk # Walk the VAD tree
vboxinfo # Dump virtualbox information
verinfo # Prints out the version information from PE images
vmwareinfo # Dump VMware VMSS/VMSN information
volshell # Shell in the memory image
win10cookie # Find the ObHeaderCookie value for Windows 10
windows # Print Desktop Windows (verbose details)
wintree # Print Z-Order Desktop Windows Tree
wndscan # Pool scanner for window stations
yarascan # Scan process or kernel memory with Yara signatures

# Linux
linux_apihooks # Checks for userland apihooks
linux_arp # Print the ARP table
linux_aslr_shift # Automatically detect the Linux ASLR shift
linux_banner # Prints the Linux banner information
linux_bash # Recover bash history from bash process memory
linux_bash_env # Recover a process' dynamic environment variables
linux_bash_hash # Recover bash hash table from bash process memory
linux_check_afinfo # Verifies the operation function pointers of network protocols
linux_check_creds # Checks if any processes are sharing credential structures
linux_check_evt_arm # Checks the Exception Vector Table to look for syscall table hooking
linux_check_fop # Check file operation structures for rootkit modifications
linux_check_idt # Checks if the IDT has been altered
linux_check_inline_kernel # Check for inline kernel hooks
linux_check_modules # Compares module list to sysfs info, if available
```

```

linux_check_syscall # Checks if the system call table has been altered
linux_check_syscall_arm # Checks if the system call table has been altered
linux_check_tty # Checks tty devices for hooks
linux_cpuinfo # Prints info about each active processor
linux_dentry_cache # Gather files from the dentry cache
linux_dmesg # Gather dmesg buffer
linux_dump_map # Writes selected memory mappings to disk
linux_dynamic_env # Recover a process' dynamic environment variables
linux_elfs # Find ELF binaries in process mappings
linux_enumerate_files # Lists files referenced by the filesystem cache
linux_find_file # Lists and recovers files from memory
linux_getcwd # Lists current working directory of each process
linux_hidden_modules # Carves memory to find hidden kernel modules
linux_ifconfig # Gathers active interfaces
linux_info_regs # It's like 'info registers' in GDB. It prints out all the
linux_iomem # Provides output similar to /proc/iomem
linux_kernel_opened_files # Lists files that are opened from within the kernel
linux_keyboard_notifiers # Parses the keyboard notifier call chain
linux_ldrmodules # Compares the output of proc maps with the list of libraries from libdl
linux_library_list # Lists libraries loaded into a process
linux_librarydump # Dumps shared libraries in process memory to disk
linux_list_raw # List applications with promiscuous sockets
linux_lsmod # Gather loaded kernel modules
linux_lsof # Lists file descriptors and their path
linux_malfind # Looks for suspicious process mappings
linux_memmap # Dumps the memory map for linux tasks
linux_moddump # Extract loaded kernel modules
linux_mount # Gather mounted fs/devices
linux_mount_cache # Gather mounted fs/devices from kmem_cache
linux_netfilter # Lists Netfilter hooks
linux_netscan # Carves for network connection structures
linux_netstat # Lists open sockets
linux_pidhashtable # Enumerates processes through the PID hash table
linux_pkt_queues # Writes per-process packet queues out to disk
linux_plthook # Scan ELF binaries' PLT for hooks to non-NEEDED images
linux_proc_maps # Gathers process memory maps
linux_proc_maps_rb # Gathers process maps for linux through the mappings red-black tree
linux_procdump # Dumps a process's executable image to disk
linux_process_hollow # Checks for signs of process hollowing
linux_psaux # Gathers processes along with full command line and start time
linux_psend # Gathers processes along with their static environment variables
linux_pslist # Gather active tasks by walking the task_struct->task list
linux_pslist_cache # Gather tasks from the kmem_cache
linux_psscan # Scan physical memory for processes
linux_pstree # Shows the parent/child relationship between processes
linux_psview # Find hidden processes with various process listings
linux_recover_filesystem # Recovers the entire cached file system from memory
linux_route_cache # Recovers the routing cache from memory
linux_sk_buff_cache # Recovers packets from the sk_buff kmem_cache
linux_slabinfo # Mimics /proc/slabinfo on a running machine
linux_strings # Match physical offsets to virtual addresses (may take a while, VERY verbose)
linux_threads # Prints threads of processes
linux_tmpfs # Recovers tmpfs filesystems from memory
linux_truecrypt_passphrase # Recovers cached Truecrypt passphrases
linux_vma_cache # Gather VMAs from the vm_area_struct cache
linux_volshell # Shell in the memory image
linux_yarascan # A shell in the Linux memory image

# MAC
mac_adium # Lists Adium messages
mac_apihooks # Checks for API hooks in processes
mac_apihooks_kernel # Checks to see if system call and kernel functions are hooked
mac_arp # Prints the arp table
mac_bash # Recover bash history from bash process memory
mac_bash_env # Recover bash's environment variables
mac_bash_hash # Recover bash hash table from bash process memory
mac_calendar # Gets calendar events from Calendar.app
mac_check_fop # Validate File Operation Pointers
mac_check_mig_table # Lists entires in the kernel's MIG table

```

```

mac_check_syscall_shadow # Looks for shadow system call tables
mac_check_syscalls      # Checks to see if system call table entries are hooked
mac_check_sysctl        # Checks for unknown sysctl handlers
mac_check_trap_table    # Checks to see if mach trap table entries are hooked
mac_compressed_swap     # Prints Mac OS X VM compressor stats and dumps all compressed pages
mac_contacts            # Gets contact names from Contacts.app
mac_dead_procs         # Prints terminated/de-allocated processes
mac_dead_sockets        # Prints terminated/de-allocated network sockets
mac_dead_vnodes         # Lists freed vnode structures
mac_devfs               # Lists files in the file cache
mac_dmesg               # Prints the kernel debug buffer
mac_dump_file           # Dumps a specified file
mac_dump_maps           # Dumps memory ranges of process(es)
mac_dyld_maps           # Gets memory maps of processes from dyld data structures
mac_find_aslr_shift     # Find the ASLR shift value for 10.8+ images
mac_get_profile         # Automatically detect Mac profiles
mac_ifconfig            # Lists network interface information for all devices
mac_interest_handlers  # Lists IOKit Interest Handlers
mac_ip_filters          # Reports any hooked IP filters
mac_kernel_classes     # Lists loaded c++ classes in the kernel
mac_kevents             # Show parent/child relationship of processes
mac_keychaindump        # Recovers possible keychain keys. Use chainbreaker to open related keychain files
mac_ldrmodules          # Compares the output of proc maps with the list of libraries from libdl
mac_librarydump         # Dumps the executable of a process
mac_list_files          # Lists files in the file cache
mac_list_kauth_listeners # Lists Kauth Scope listeners
mac_list_kauth_scopes  # Lists Kauth Scopes and their status
mac_list_raw            # List applications with promiscuous sockets
mac_list_sessions       # Enumerates sessions
mac_list_zones          # Prints active zones
mac_lsmod               # Lists loaded kernel modules
mac_lsmod_iokit         # Lists loaded kernel modules through IOKit
mac_lsmod_kext_map     # Lists loaded kernel modules
mac_lsof                 # Lists per-process opened files
mac_machine_info        # Prints machine information about the sample
mac_malfind             # Looks for suspicious process mappings
mac_memdump             # Dump addressable memory pages to a file
mac_moddump             # Writes the specified kernel extension to disk
mac_mount               # Prints mounted device information
mac_netstat             # Lists active per-process network connections
mac_network_conns      # Lists network connections from kernel network structures
mac_notesapp           # Finds contents of Notes messages
mac_notifiers           # Detects rootkits that add hooks into I/O Kit (e.g. LogKext)
mac_orphan_threads     # Lists threads that don't map back to known modules/processes
mac_pgrp_hash_table    # Walks the process group hash table
mac_pid_hash_table     # Walks the pid hash table
mac_print_boot_cmdline # Prints kernel boot arguments
mac_proc_maps          # Gets memory maps of processes
mac_procdump           # Dumps the executable of a process
mac_psaux              # Prints processes with arguments in user land (**argv)
mac_psenv              # Prints processes with environment in user land (**envp)
mac_pslist             # List Running Processes
mac_pstree             # Show parent/child relationship of processes
mac_psxview            # Find hidden processes with various process listings
mac_recover_filesystem # Recover the cached filesystem
mac_route              # Prints the routing table
mac_socket_filters     # Reports socket filters
mac_strings            # Match physical offsets to virtual addresses (may take a while, VERY verbose)
mac_tasks              # List Active Tasks
mac_threads            # List Process Threads
mac_threads_simple     # Lists threads along with their start time and priority
mac_timers             # Reports timers set by kernel drivers
mac_trustedbsd         # Lists malicious trustedbsd policies
mac_version            # Prints the Mac version
mac_vfsevents          # Lists processes filtering file system events
mac_volshell           # Shell in the memory image
mac_yarascan           # Scan memory for yara signatures

```

