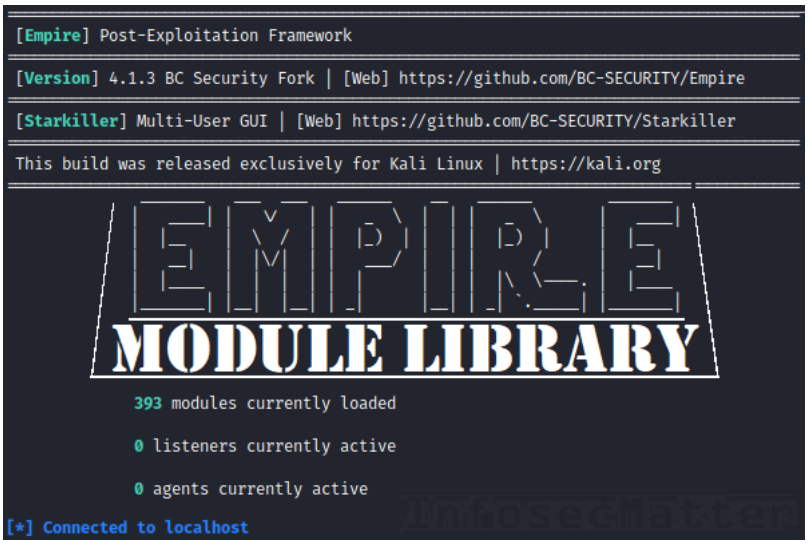
Empire Module Library

infosecmatter.com/empire-module-library



If you are looking for a list of Empire modules, this library might be just for you.

On this page you will find a complete list of all Empire modules that are available in the latest version of Empire 4 (BC Security fork), one of the most popular post-exploitation frameworks.

Introduction

The BC Security Empire 4, which is a successor of the discontinued PowerShell Empire project, is one of the top open source post-exploitation frameworks available to red teams and penetration testers today for conducting variety of security assessments.

Once supporting only Windows systems, today's modern version of Empire can be used on OS X and Linux based targets as well, thanks to the modern Python 3.x language support.

Empire Modules and Plugins

Empire offers plenty of additional functionality in forms of modules and plugins. In the current version (4.1.3) there are nearly 400 modules which are written in one of these languages:

- PowerShell
- Python
- C#

This page contains a library of all of these modules, in a form of table which you can easily search through and filter out based on what you are looking for.

Each module has a separate entry, with a detailed description, list of options and example usage providing details on how to use the module.

Filtering Examples

For searching through the table below, you can use the Search functionality on top of the table and for instance search for the following module categories:

- `Enumeration` – Modules for general recon and information gathering
- `Situation` – Situational awareness modules (scanners, detailed recon etc.)
- `Active directory` – Enumeration of Active Directory (groups, users, computers etc.)
- `Privesc` or `privilege` – Privilege escalation modules and scanners for local vulnerabilities
- `Credentials` – Dumping credentials, password hashes, impersonation, tokens, tickets etc.
- `Persistence` – Maintaining access to the system (install a backdoor etc.)
- `Lateral` – Lateral movement, invoking commands on remote systems
- `Code execution` – Executing code on the system using various methods
- `Collection` – Dumping browser data, packet capturing (sniffing), keylogging, screen capturing etc.
- `Management` – Modules for managing the system and performing various useful tasks
- `Exploit` – Modules for various known vulnerabilities (ZeroLogon, PrintNightmare, EternalBlue etc.)

You can also filter the modules based on a tool name or a technology that you are looking for. For instance: `mimikatz`, `rubeus`, `inveigh`, `mimipenguin`, `rdp`, `ssh`, `keylogger`, `seatbelt`, `portscan`, `sharpsploit`, `ghostpack`, `wdigest`, `registry`, `winpeas`.

Surely you've got the idea. Alright, here's the promised Empire module library..

Empire Module	Module Description
csharp/SharpSploit.PrivilegeEscalation/PrivExchange	Performs the PrivExchange attack by sending a push notification to EWS.
csharp/GhostPack/Rubeus	Use a rubeus command.
csharp/GhostPack/SharpDPAPI	Use a SharpDPAPI command.
csharp/GhostPack/SharpUp	Use a SharpUp command.
csharp/GhostPack/SharpDump	Use a SharpDump command.
csharp/GhostPack/Seatbelt	Use a Seatbelt command.
csharp/GhostPack/SharpWMI	Use a SharpWMI command.
csharp/DotNetCore/ListDirectory	Get a listing of the current directory.
csharp/DotNetCore/Assembly	Execute a dotnet Assembly EntryPoint.
csharp/DotNetCore/ShellCmd	Execute a Shell command using "cmd.exe /c".
csharp/DotNetCore/Shell	Execute a Shell command.
csharp/DotNetCore/WhoAmI	Gets the username of the currently used/impersonate token.
csharp/DotNetCore/ChangeDirectory	Change the current directory.
csharp/DotNetCore/ReadTextFile	Read a text file on disk.
csharp/DotNetCore/CreateDirectory	Creates all directories and subdirectories in the speci path unless they already exist.
csharp/DotNetCore/Delete	Delete a file or directory.
csharp/DotNetCore/Copy	Copy a file from one location to another.
csharp/DotNetCore/ProcessList	Get a list of currently running processes.
csharp/DotNetCore/Download	Download a file.
csharp/DotNetCore/Upload	Upload a file.
csharp/SharpSploit.LateralMovement/WMIGrunt	Execute a Grunt Launcher on a remote system using Win32_Process Create, optionally with alternate credentials.
csharp/SharpSploit.LateralMovement/WMICommand	Execute a process on a remote system using Win32_Process Create, optionally with alternate credentials.
csharp/SharpSploit.LateralMovement/PowerShellRemotingGrunt	Execute a Grunt Launcher on a remote system using PowerShell Remoting, optionally with alternate crede
csharp/SharpSploit.LateralMovement/PowerShellRemotingCommand	Execute a PowerShell command on a remote system PowerShell Remoting, optionally with alternate crede
csharp/SharpSploit.LateralMovement/DCOMGrunt	Execute a Grunt Launcher on a remote system using various DCOM methods.
csharp/SharpSploit.LateralMovement/DCOMCommand	Execute a process on a remote system using various DCOM methods.
csharp/SharpSploit.Persistence/PersistStartup	Installs a payload into the current users startup folder
csharp/SharpSploit.Persistence/PersistCOMHijack	Hijacks a CLSID key to execute a payload for persiste
csharp/SharpSploit.Persistence/PersistWMI	Creates a WMI Event, Consumer and Binding to exec payload.
csharp/SharpSploit.Persistence/PersistAutorun	Installs an autorun value in HKCU or HKLM to execut payload.
csharp/SharpSploit.Evasion/BypassAmsi	Bypasses AMSI by patching the AmsiScanBuffer func
csharp/SharpSploit.Enumeration/GetNetSession	Gets a list of `SessionInfo`s from specified remote computer(s).
csharp/SharpSploit.Enumeration/GetNetLoggedOnUser	Gets a list of `LoggedOnUser`s from specified remote computer(s).

Empire Module	Module Description
csharp/SharpSploit.Enumeration/GetNetLocalGroupMember	Gets a list of `LocalGroupMember`s from specified re computer(s).
csharp/SharpSploit.Enumeration/GetNetLocalGroup	Gets a list of `LocalGroup`s from specified remote computer(s).
csharp/SharpSploit.Enumeration/GetDomainGroup	Gets a list of specified (or all) group `DomainObject`s current Domain.
csharp/SharpSploit.Enumeration/GetDomainUser	Gets a list of specified (or all) user `DomainObject`s i current Domain.
csharp/SharpSploit.Enumeration/GetDomainComputer	Gets a list of specified (or all) computer `DomainObje the current Domain.
csharp/SharpSploit.Enumeration/Keylogger	Monitor the keystrokes for a specified period of time.
csharp/SharpSploit.Enumeration/Kerberoast	Perform a "Kerberoast" attack that retrieves crackable service tickets for Domain User's w/ an SPN set.
csharp/SharpSploit.Enumeration/PortScan	Perform a TCP port scan.
csharp/SharpSploit.Enumeration/ListDirectory	Get a listing of the current directory.
csharp/SharpSploit.Enumeration/ProcessList	Get a list of currently running processes.
csharp/SharpSploit.Enumeration/SetRegistryKey	Sets a value into the registry.
csharp/SharpSploit.Enumeration/GetRegistryKey	Gets a value stored in registry.
csharp/SharpSploit.Enumeration/SetRemoteRegistryKey	Sets a value into the registry on a remote system.
csharp/SharpSploit.Enumeration/GetRemoteRegistryKey	Gets a value stored in registry on a remote system.
csharp/Sharpsploit.Credentials/MakeToken	Makes a new token with a specified username and password, and impersonates it to conduct future actio the specified user.
csharp/Sharpsploit.Credentials/GetSystem	Impersonate the SYSTEM user. Equates to ImpersonateUser("NT AUTHORITY\SYSTEM").
csharp/Sharpsploit.Credentials/ImpersonateProcess	Impersonate the token of the specified process. Usec execute subsequent commands as the user associate the token of the specified process.
csharp/Sharpsploit.Credentials/ImpersonateUser	Find a process owned by the specified user and impersonate the token. Used to execute subsequent commands as the specified user.
csharp/Sharpsploit.Credentials/BypassUACGrunt	Bypasses UAC through token duplication and execut Grunt Launcher with high integrity.
csharp/Sharpsploit.Credentials/BypassUACCommand	Bypasses UAC through token duplication and execut command with high integrity.
csharp/Sharpsploit.Credentials/RevertToSelf	Ends the impersonation of any token, reverting back initial token associated with the current process. Usef conjuction with functions ...
csharp/Sharpsploit.Credentials/LogonPasswords	Execute the 'privilege::debug sekurlsa::logonPasswo Mimikatz command.
csharp/Sharpsploit.Credentials/LsaSecrets	Execute the 'privilege::debug lsadump::secrets' Mimik command.
csharp/Sharpsploit.Credentials/LsaCache	Execute the 'privilege::debug lsadump::cache' Mimika command.
csharp/Sharpsploit.Credentials/SamDump	Execute the 'privilege::debug lsadump::sam' Mimikatz command.
csharp/Sharpsploit.Credentials/Wdigest	Execute the 'sekurlsa::wdigest' Mimikatz command.
csharp/Sharpsploit.Credentials/DCSync	Execute the 'lsadump::dcsync Mimikatz command.
csharp/Sharpsploit.Credentials/Mimikatz	Execute a mimikatz command.
csharp/Sharpsploit.Credentials/SafetyKatz	Use SafetyKatz.
csharp/SharpSC/SharpSC	Use a SharpSC command.
python/code_execution/powershell_execution	Executes Powershell code from a Python code.

Empire Module	Module Description
python/trollsploit/osx/change_background	Change the login message for the user.
python/trollsploit/osx/say	Performs text to speech using "say".
python/trollsploit/osx/thunderstruck	Open Safari in the background and play Thunderstru
python/trollsploit/osx/login_message	Change the login message for the user.
python/management/multi/kerberos_inject	Generates a kerberos keytab and injects it into the cu runspace.
python/management/multi/spawn	Spawns a new Empire agent.
python/management/multi/socks	Spawn an AROX relay to extend a SOCKS proxy thro your agent.
python/management/osx/shellcodeinject64	Inject shellcode into a x64 bit process.
python/management/osx/screen_sharing	Enables ScreenSharing to allow you to connect to the via VNC.
python/situational_awareness/network/find_fruit	Searches for low-hanging web applications.
python/situational_awareness/network/gethostbyname	Uses Python's socket.gethostbyname("example.com" function to resolve host names on a remote agent.
python/situational_awareness/network/port_scan	Simple Port Scanner.
python/situational_awareness/network/smb_mount	This module will attempt mount an smb share and ex a command on it.
python/situational_awareness/network/http_rest_api	Interacts with a HTTP REST API and returns the resu back to the screen.
python/situational_awareness/network/active_directory/dscl_get_groups	This module will use the current user context to query active directory for a list of Groups.
python/situational_awareness/network/active_directory/get_groups	This module will list all groups in active directory.
python/situational_awareness/network/active_directory/get_computers	This module will list all computer objects from active directory.
python/situational_awareness/network/active_directory/get_userinformation	This module will return the user profile specified.
python/situational_awareness/network/active_directory/get_fileservers	This module will list file servers.
python/situational_awareness/network/active_directory/get_users	This module list users found in Active Directory.
python/situational_awareness/network/active_directory/dscl_get_groupmembers	This module will use the current user context to query active directory for a list of users in a group.
python/situational_awareness/network/active_directory/get_groupmembers	This module will return a list of group members.
python/situational_awareness/network/active_directory/get_ous	This module will list all OUs from active directory.
python/situational_awareness/network/active_directory/dscl_get_users	This module will use the current user context to query active directory for a list of users.
python/situational_awareness/network/active_directory/get_groupmemberships	This module check what groups a user is member of.
python/situational_awareness/network/active_directory/get_domaincontrollers	This module will list all domain controllers from active directory.
python/situational_awareness/network/dcos/marathon_api_delete_app	Delete a Marathon App using Marathon's REST API.
python/situational_awareness/network/dcos/marathon_api_create_start_app	Create and Start a Marathon App using Marathon's R API.
python/situational_awareness/network/dcos/chronos_api_delete_job	Delete a Chronos job using the HTTP API service for Chronos Framework.
python/situational_awareness/network/dcos/etcd_crawler	Pull keys and values from an etcd configuration store
python/situational_awareness/network/dcos/chronos_api_add_job	Add a Chronos job using the HTTP API service for th Chronos Framework.
python/situational_awareness/network/dcos/chronos_api_start_job	Start a Chronos job using the HTTP API service for th Chronos Framework.
python/situational_awareness/host/multi/WorldWriteableFileSearch	This module can be used to identify world writeable fi
python/situational_awareness/host/multi/SuidGuidSearch	This module can be used to identify suid or guid bit se files.

Empire Module	Module Description
python/situational_awareness/host/osx/situational_awareness	This module will enumerate the basic items needed f
python/situational_awareness/host/osx/HijackScanner	This module can be used to identify applications vuln to dylib hijacking on a target system. This has been modified from the original to remove ...
python/privesc/linux/linux_priv_checker	This script is intended to be executed locally ona Linu to enumerate basic system info, and search for commonprivilege escalation vectors with ...
python/privesc/linux/unix_privesc_check	This script is intended to be executed locally ona Linu to enumerate basic system info, and search for commonprivilege escalation vectors with a ...
python/privesc/multi/bashdoor	Creates an alias in the .bash_profile to cause the sud command to execute a stager and pass through the origional command back to sudo.
python/privesc/multi/sudo_spawn	Spawns a new Empire agent using sudo.
python/privesc/osx/piggyback	Spawns a new Empire agent using an existing sudo session. This works up until El Capitan.
python/privesc/osx/dyld_print_to_file	This modules takes advantage of the environment va DYLD_PRINT_TO_FILE in order to escalate privilege all versions Mac OS X YosemiteWARNING: ...
python/privesc/windows/get_gpppasswords	This module will attempt to pull group policy preferen passwords from SYSVOL.
python/collection/linux/sniffer	This module will sniff all interfaces on the target, and in pcap format.
python/collection/linux/hashdump	Extracts the /etc/passwd and /etc/shadow, unshadow result.
python/collection/linux/xkeylogger	X userland keylogger based on pupy.
python/collection/linux/pillage_user	Pillages the current user for their bash_history, ssh kr hosts, recent folders, etc.
python/collection/linux/mimipenguin	Port of huntergregal mimipenguin. Harvest's current u cleartext credentials.
python/collection/linux/keylogger	Logs keystrokes to the specified file. Ruby based and heavily adapted from MSF's osx/capture/keylog_reco Kill the resulting PID when keylogging ...
python/collection/osx/osx_mic_record	Records audio through the MacOS webcam mic by leveraging the Apple AVFoundation API.
python/collection/osx/sniffer	This module will do a full network stack capture.
python/collection/osx/imessage_dump	This module will enumerate the entire chat and IMess SQL Database.
python/collection/osx/kerberosdump	This module will dump ccache kerberostickets to the specified directory.
python/collection/osx/keychaindump_chainbreaker	A keychain dump module that allows for decryption v known password.
python/collection/osx/prompt	Launches a specified application with an prompt for credentials with osascript.
python/collection/osx/hashdump	Extracts found user hashes out of /var/db/dslocal/nodes/Default/users/*.plist.
python/collection/osx/keychaindump_decrypt	Uses Apple Security utility to dump the contents of th keychain. WARNING: Will prompt user for access to key.On Newer versions of Sierra and ...
python/collection/osx/browser_dump	This module will dump browser history from Safari an Chrome.
python/collection/osx/pillage_user	Pillages the current user for their keychain, bash_hist ssh known hosts, recent folders, etc. For logon.keych use ...
python/collection/osx/webcam	Takes a picture of a person through OSX's webcam v ImageSnap binary.

Empire Module	Module Description
python/collection/osx/screenshot	Takes a screenshot of an OSX desktop using screencapture and returns the data.
python/collection/osx/keychaindump	Searches for keychain candidates and attempts to de the user's keychain.
python/collection/osx/search_email	Searches for Mail .emlx messages, optionally only ret messages with the specified SearchTerm.
python/collection/osx/screensaver_alleyoop	Launches a screensaver with a prompt for credentials osascript. This locks the user out until the password c unlock the user keychain. This ...
python/collection/osx/native_screenshot_mss	Takes a screenshot of an OSX desktop using the Pyt mss module. The python-mss module utilizes ctypes the CoreFoundation library.
python/collection/osx/clipboard	This module will write log output of clipboard to stdou disk).
python/collection/osx/keylogger	Logs keystrokes to the specified file. Ruby based and heavily adapted from MSF's osx/capture/keylog_reco Kill the resulting PID when keylogging ...
python/collection/osx/native_screenshot	Takes a screenshot of an OSX desktop using the Pyt Quartz libraries and returns the data.
python/exploit/web/jboss_jmx	Exploit JBoss java serialization flaw. Requires upload ysoserial payload.
python/persistence/multi/crontab	This module establishes persistence via crontab.
python/persistence/multi/desktopfile	Installs an Empire launcher script in ~/.config/autosta Linux versions with GUI.
python/persistence/osx/mail	Installs a mail rule that will execute an AppleScript sta when a trigger word is present in the Subject of an incoming mail.
python/persistence/osx/LaunchAgent	Installs an Empire Launch Agent.
python/persistence/osx/loginhook	Installs Empire agent via LoginHook.
python/persistence/osx/CreateHijacker	Configures and Empire dylib for use in a Dylib hijack, the path to a legitimate dylib of a vulnerable applicatio The architecture of the ...
python/persistence/osx/LaunchAgentUserLandPersistence	Installs an Empire launchAgent.
python/persistence/osx/RemoveLaunchAgent	Remove an Empire Launch Daemon.
python/lateral_movement/multi/ssh_launcher	This module will send an launcher via ssh.
python/lateral_movement/multi/ssh_command	This module will send a command via ssh.
powershell/code_execution/invoke_metasploitpayload	Spawns a new, hidden PowerShell window that downloadsand executes a Metasploit payload. This re on the exploit/multi/scripts/web_delivery ...
powershell/code_execution/invoke_ntsd	Use NT Symbolic Debugger to execute Empire launc code.
powershell/code_execution/invoke_shellcodemsil	Execute shellcode within the context of the running PowerShell process without making any Win32 functi calls. Warning: This script has no way to ...
powershell/code_execution/invoke_assembly	Loads the specified assembly into memory and invok main method. The Main method and class containing must both be PUBLIC for ...
powershell/code_execution/invoke_reflectivepeinjection	Uses PowerSploit's Invoke-ReflectivePEInjection to reflectively load a DLL/EXE in to the PowerShell proc reflectively load a DLL in to a remote ...
powershell/code_execution/invoke_ironpython	Executes IronPython code using the embedded IPY e
powershell/code_execution/invoke_clearscript	Executes JScript (or VBScript) using the embedded ClearScript engine.
powershell/code_execution/invoke_dllinjection	Uses PowerSploit's Invoke-DLLInjection to inject a Dl the process ID of your choosing.

Empire Module	Module Description
powershell/code_execution/invoke_ironpython3	Executes IronPython3 code using the embedded IPY engine.
powershell/code_execution/invoke_shellcode	Uses PowerSploit's Invoke--Shellcode to inject shellc into the process ID of your choosing or within the con the running PowerShell ...
powershell/code_execution/invoke_ssharp	Executes SSharp from an embedded compiler within PowerShell. Compilation does not call csc.exe.
powershell/code_execution/invoke_boolang	Executes Boo code from an embedded compiler.
powershell/trollsploit/rick_ascii	Spawns a a new powershell.exe process that runs Le Holmes' ASCII Rick Roll.
powershell/trollsploit/get_schwifty	Play's a hidden version of Rick and Morty Get Schwif video while maxing out a computer's volume.
powershell/trollsploit/wlmdr	Displays a balloon reminder in the taskbar.
powershell/trollsploit/rick_astley	Runs @SadProcessor's beeping rickroll.
powershell/trollsploit/wallpaper	Uploads a .jpg image to the target and sets it as the desktop wallpaper.
powershell/trollsploit/message	Displays a specified message to the user.
powershell/trollsploit/voicetroll	Reads text aloud via synthesized voice on target.
powershell/trollsploit/process_killer	Kills any process starting with a particular name.
powershell/trollsploit/thunderstruck	Play's a hidden version of AC/DC's Thunderstruck vic while maxing out a computer's volume.
powershell/exploitation/exploit_eternalblue	Port of MS17_010 Metasploit module to powershell. Exploits targeted system and executes specified shel Windows 7 and 2008 R2 supported. ...
powershell/exploitation/exploit_jenkins	Run command on unauthenticated Jenkins Script cor
powershell/exploitation/invoke_spoolsample	Runs SpoolSample C# binary through reflection.
powershell/exploitation/exploit_jboss	Exploit vulnerable JBoss Services.
powershell/credentials/rubeus	Rubeus is a C# toolset for raw Kerberos interaction a abuses.
powershell/credentials/vault_credential	Runs PowerSploit's Get-VaultCredential to display W vault credential objects including cleartext web crede
powershell/credentials/invoke_kerberoast	Requests kerberos tickets for all users with a non-nul service principal name (SPN) and extracts them into format ready for John or Hashcat.
powershell/credentials/DomainPasswordSpray	DomainPasswordSpray is a tool written in PowerShe perform a password spray attack against users of a domain.
powershell/credentials/sessiongopher	Extract saved sessions & passwords for WinSCP, Pu SuperPuTTY, FileZilla, RDP, .ppk files, .rdp files, .sdti
powershell/credentials/invoke_internal_monologue	Uses the Internal Monologue attack to force easily-decryptable Net-NTLMv1.
powershell/credentials/powerdump	Dumps hashes from the local system using an update version of Posh-SecMod's Invoke-PowerDump.
powershell/credentials/enum_cred_store	Dumps plaintext credentials from the Windows Crede Manager for the current interactive user.
powershell/credentials/invoke_ntlmextract	Extract local NTLM password hashes from the registr
powershell/credentials/get_lapspasswords	Dumps user readable LAPS passwords using kfosaa Get-LAPSPasswords.
powershell/credentials/sharpsecdump	.Net port of the remote SAM + LSA Secrets dumping functionality of impacket's secretsdump.py. By default in the context of the current user.
powershell/credentials/credential_injection	Runs PowerSploit's Invoke-CredentialInjection to crea logons with clear-text credentials without triggering a suspicious Event ID 4648 (Explicit ...

Empire Module	Module Description
powershell/credentials/tokens	Runs PowerSploit's Invoke-TokenManipulation to enumerate Logon Tokens available and uses them to create new processes. Similar to Incognito's ...
powershell/credentials/mimikatz/pth	Runs PowerSploit's Invoke-Mimikatz function to exec sekurlsa::pth to create a new process. with a specific hash. Use credentials/tokens to ...
powershell/credentials/mimikatz/silver_ticket	Runs PowerSploit's Invoke-Mimikatz function to gene silver ticket for a server/service and inject it into mem
powershell/credentials/mimikatz/cache	Runs PowerSploit's Invoke-Mimikatz function to extra MSCache(v2) hashes.
powershell/credentials/mimikatz/command	Runs PowerSploit's Invoke-Mimikatz function with a c command. Note: Not all functions require admin, but do.
powershell/credentials/mimikatz/terminal_server	Runs PowerSploit's Invoke-Mimikatz function to extra plaintext RDP credentials from memory.
powershell/credentials/mimikatz/extract_tickets	Runs PowerSploit's Invoke-Mimikatz function to extra kerberos tickets from memory in base64-encoded for
powershell/credentials/mimikatz/keys	Runs PowerSploit's Invoke-Mimikatz function to extra keys to the local directory.
powershell/credentials/mimikatz/sam	Runs PowerSploit's Invoke-Mimikatz function to extra hashes from the Security Account Managers (SAM) database.
powershell/credentials/mimikatz/trust_keys	Runs PowerSploit's Invoke-Mimikatz function to extra domain trust keys from a domain controller.
powershell/credentials/mimikatz/purge	Runs PowerSploit's Invoke-Mimikatz function to purg current kerberos tickets from memory.
powershell/credentials/mimikatz/logonpasswords	Runs PowerSploit's Invoke-Mimikatz function to extra plaintext credentials from memory.
powershell/credentials/mimikatz/certs	Runs PowerSploit's Invoke-Mimikatz function to extra certificates to the local directory.
powershell/credentials/mimikatz/dcsync	Runs PowerSploit's Invoke-Mimikatz function to extra given account password through Mimikatz's lsadump::dcsync module. This doesn't need code ...
powershell/credentials/mimikatz/lsadump	Runs PowerSploit's Invoke-Mimikatz function to extra particular user hash from memory. Useful on domain controllers.
powershell/credentials/mimikatz/mimitokens	Runs PowerSploit's Invoke-Mimikatz function to list o enumerate tokens.
powershell/credentials/mimikatz/golden_ticket	Runs PowerSploit's Invoke-Mimikatz function to gene golden ticket and inject it into memory.
powershell/credentials/mimikatz/dcsync_hashdump	Runs PowerSploit's Invoke-Mimikatz function to colle domain hashes using Mimikatz'slsadump::dcsync mo This doesn't need code execution on ...
powershell/recon/get_sql_server_login_default_pw	Based on the instance name, test if SQL Server is configured with default passwords.
powershell/recon/http_login	Tests credentials against Basic Authentication.
powershell/recon/find_fruit	Searches a network range for potentially vulnerable v services.
powershell/recon/fetch_brute_local	This module will logon to a member server using the account or a provided account, fetch the local accour perform a network based brute ...
powershell/management/timestomp	Executes time-stomp like functionality by invoking Se MacAttribute.
powershell/management/spawnas	Spawn an agent with the specified logon credentials.
powershell/management/zipfolder	Zips up a target folder for later exfiltration.
powershell/management/switch_listener	Overwrites the listener controller logic with the agent the logic from generate_comms() for the specified list

Empire Module	Module Description
powershell/management/start-processasuser	Executes a command using a specified set of creden
powershell/management/invoke_script	Run a custom script. Useful for mass-taskings or scri autoruns.
powershell/management/invoke_sharpchisel	Chisel is a fast TCP tunnel, transported over HTTP, s via SSH. Written in Go (golang). Chisel is mainly usef passing through firewalls, ...
powershell/management/get_domain_sid	Returns the SID for the current or specified domain.
powershell/management/enable_multi_rdp	[!] WARNING: Experimental! Runs PowerSploit's Invo Mimikatz function to patch the Windows terminal serv allow multiple users to establish ...
powershell/management/enable_rdp	Enables RDP on the remote machine and adds a fire exception.
powershell/management/reflective_inject	Utilizes Powershell to to inject a Stephen Fewer form ReflectivePick which executes PS codefrom memory remote process.
powershell/management/shinject	Injects a PIC shellcode payload into a target process, Invoke-Shellcode.
powershell/management/lock	Locks the workstation's display.
powershell/management/sid_to_user	Converts a specified domain sid to a user.
powershell/management/psinject	Utilizes Powershell to to inject a Stephen Fewer form ReflectivePick which executes PS codefrom memory remote process. ProcID or ProcName must ...
powershell/management/spawn	Spawns a new agent in a new powershell.exe proces
powershell/management/phant0m	Kills Event Log Service Threads.
powershell/management/disable_rdp	Disables RDP on the remote machine.
powershell/management/user_to_sid	Converts a specified domain\user to a domain sid.
powershell/management/wdigest_downgrade	Sets wdigest on the machine to explicitly use logon credentials. Counters kb2871997.
powershell/management/runas	Runas knockoff. Will bypass GPO path restrictions.
powershell/management/downgrade_account	Set reversible encryption on a given domain account then force the password to be set on next user login.
powershell/management/vnc	Invoke-Vnc executes a VNC agent in-memory and ini a reverse connection, or binds to a specified port. Password authentication is supported.
powershell/management/powercat	Powercat is a powershell function. First you need to l the function before you can execute it.You can put on the below commands into your ...
powershell/management/logoff	Logs the current user (or all users) off the machine.
powershell/management/invoke_socksproxy	The reverse proxy creates a TCP tunnel by initiating outbound SSL connections that can go through the system's proxy. The tunnel can then be used as ...
powershell/management/restart	Restarts the specified machine.
powershell/management/honeyhash	Inject artificial credentials into LSASS.
powershell/management/mailraider/get_subfolders	Returns a list of all the folders in the specified top lev folder.
powershell/management/mailraider/mail_search	Searches the given Outlook folder for items (Emails, Contacts, Tasks, Notes, etc. *Depending on the folde returns any matches found.
powershell/management/mailraider/send_mail	Sends emails using a custom or default template to specified target email addresses.
powershell/management/mailraider/view_email	Selects the specified folder and then outputs the ema at the specified index.

Empire Module	Module Description
powershell/management/mailraider/search_gal	Returns any exchange users that match the specified search criteria. Searchable fields are FirstName, LastName, JobTitle, Email-Address, and ...
powershell/management/mailraider/get_emailitems	Returns all of the items for the specified folder.
powershell/management/mailraider/disable_security	This function checks for the ObjectModelGuard, PromptOOMSend, and AdminSecurityMode registry k for Outlook security. This function must be run in ...
powershell/situational_awareness/network/arpscan	Performs an ARP scan against a given range of IPv4 Addresses.
powershell/situational_awareness/network/bloodhound3	Execute BloodHound data collection (ingestor for ver 3).
powershell/situational_awareness/network/reverse_dns	Performs a DNS Reverse Lookup of a given IPv4 IP F
powershell/situational_awareness/network/get_sql_server_info	Returns basic server and user information from targe Servers.
powershell/situational_awareness/network/smbscanner	Tests usernames/password combination across a nur of machines.
powershell/situational_awareness/network/bloodhound	Execute BloodHound data collection.
powershell/situational_awareness/network/get_kerberos_service_ticket	Retrieves IP addresses and usernames using event I 4769 this can allow identification of a users machine. only run on a domain controller.
powershell/situational_awareness/network/portscan	Does a simple port scan using regular sockets, based (pretty) loosely on nmap.
powershell/situational_awareness/network/get_sql_instance_domain	Returns a list of SQL Server instances discovered by querying a domain controller for systems with registe MSSQL service principal names. The ...
powershell/situational_awareness/network/smblogin	Validates username & password combination(s) acros host or group of hosts using the SMB protocol.
powershell/situational_awareness/network/smbautobrute	Runs an SMB brute against a list of usernames/passv Will check the DCs to interrogate the bad password c of the users and will keep bruting ...
powershell/situational_awareness/network/get_spn	Displays Service Principal Names (SPN) for domain accounts based on SPN service name, domain accou domain group via LDAP queries.
powershell/situational_awareness/network/powermad/get_adidns_zone	Query ADIDNS zones in the specified domain. Part o Powermad.
powershell/situational_awareness/network/powermad/get_adidns_permission	Query a DACL of an ADIDNS node or zone in the spe domain. Part of Powermad.
powershell/situational_awareness/network/powerview/get_cached_rdpconnection	Uses remote registry functionality to query all entries Windows Remote Desktop Connection Client" on a machine. Part of PowerView.
powershell/situational_awareness/network/powerview/find_foreign_user	Enumerates users who are in groups outside of their principal domain. Part of PowerView.
powershell/situational_awareness/network/powerview/find_gpo_computer_admin	Takes a computer (or GPO) object and determines w users/groups have administrative access over it. Part PowerView.
powershell/situational_awareness/network/powerview/get_subnet	Gets a list of all current subnets in a domain. Part of PowerView.
powershell/situational_awareness/network/powerview/get_ou	Gets a list of all current OUs in a domain. Part of PowerView.
powershell/situational_awareness/network/powerview/get_subnet_ranges	Pulls hostnames from AD, performs a Reverse DNS lookup, and parses the output into ranges.
powershell/situational_awareness/network/powerview/get_gpo_computer	Takes a GPO GUID and returns the computers the G applied to. (Note: This function was removed in Powe This now uses a combination of two ...
powershell/situational_awareness/network/powerview/get_forest	Return information about a given forest, including the domain and SID. Part of PowerView.

Empire Module	Module Description
powershell/situational_awareness/network/powerview/get_domain_controller	Returns the domain controllers for the current domain the specified domain. Part of PowerView.
powershell/situational_awareness/network/powerview/user_hunter	Finds which machines users of a specified group are logged into. Part of PowerView.
powershell/situational_awareness/network/powerview/find_localadmin_access	Finds machines on the local domain where the curren has local administrator access. Part of PowerView.
powershell/situational_awareness/network/powerview/find_foreign_group	Enumerates all the members of a given domain's gro and finds users that are not in the queried domain. Pa PowerView.
powershell/situational_awareness/network/powerview/get_group	Gets a list of all current groups in a domain, or all the groups a given user/group object belongs to. Part of PowerView.
powershell/situational_awareness/network/powerview/get_session	Execute the NetSessionEnum Win32API call to query given host for active sessions on the host. Part of PowerView.
powershell/situational_awareness/network/powerview/get_computer	Queries the domain for current computer objects. Par PowerView.
powershell/situational_awareness/network/powerview/set_ad_object	Takes a SID, name, or SamAccountName to query fo specified domain object, and then sets a specified "PropertyName" to a specified "PropertyValue". ...
powershell/situational_awareness/network/powerview/get_domain_policy	Returns the default domain or DC policy for a given d or domain controller. Part of PowerView.
powershell/situational_awareness/network/powerview/get_gpo	Gets a list of all current GPOs in a domain. Part of PowerView.
powershell/situational_awareness/network/powerview/get_domain_trust	Return all domain trusts for the current domain or a specified domain. Part of PowerView.
powershell/situational_awareness/network/powerview/get_forest_domain	Return all domains for a given forest. Part of PowerVi
powershell/situational_awareness/network/powerview/map_domain_trust	Maps all reachable domain trusts with .CSV output. P PowerView.
powershell/situational_awareness/network/powerview/get_fileserver	Returns a list of all file servers extracted from user homedirectory, scriptpath, and profilepath fields. Part PowerView.
powershell/situational_awareness/network/powerview/process_hunter	Query the process lists of remote machines, searchin processes with a specific name or owned by a specifi Part of PowerView.
powershell/situational_awareness/network/powerview/get_site	Gets a list of all current sites in a domain. Part of PowerView.
powershell/situational_awareness/network/powerview/get_rdp_session	Query a given RDP remote service for active session originating IPs (replacement for qwinsta). Note: needs admin rights on the remote server ...
powershell/situational_awareness/network/powerview/get_object_acl	Returns the ACLs associated with a specific active di object. Part of PowerView. WARNING: specify a spec object, otherwise a huge amount ...
powershell/situational_awareness/network/powerview/get_localgroup	Returns a list of all current users in a specified local g on a local or remote machine. Part of PowerView.
powershell/situational_awareness/network/powerview/share_finder	Finds shares on machines in the domain. Part of PowerView.
powershell/situational_awareness/network/powerview/get_group_member	Returns the members of a given group, with the optio "Recurse" to find all effective group members. Part of PowerView.
powershell/situational_awareness/network/powerview/get_loggedon	Execute the NetWkstaUserEnum Win32API call to qu given host for actively logged on users. Part of Power
powershell/situational_awareness/network/powerview/get_user	Query information for a given user or users in the spe domain. Part of PowerView.
powershell/situational_awareness/network/powerview/find_gpo_location	Takes a user/group name and optional domain, and determines the computers in the domain the user/gro local admin (or RDP) rights to. Part of ...

Empire Module	Module Description
powershell/situational_awareness/network/powerview/get_dfs_share	Returns a list of all fault-tolerant distributed file syster a given domain. Part of PowerView.
powershell/situational_awareness/network/powerview/find_managed_security_group	This function retrieves all security groups in the doma identifies ones that have a manager set. It also deterr whether the manager has the ...
powershell/situational_awareness/host/hostrecon	Invoke-HostRecon runs a number of checks on a sys help provide situational awareness to a penetration te during the reconnaissance phase It ...
powershell/situational_awareness/host/winenum	Collects revelant information about a host and the cu user context.
powershell/situational_awareness/host/applockerstatus	This script is used to query the current AppLocker po the target and check the status of a user-defined executable or all executables in a ...
powershell/situational_awareness/host/get_uaclevel	Enumerates UAC level.
powershell/situational_awareness/host/dnsserver	Enumerates the DNS Servers used by a system.
powershell/situational_awareness/host/antivirusproduct	Get antivirus product information.
powershell/situational_awareness/host/get_pathacl	Enumerates the ACL for a given file path.
powershell/situational_awareness/host/get_proxy	Enumerates the proxy server and WPAD conents for current user. Part of PowerView.
powershell/situational_awareness/host/findtrusteddocuments	This module will enumerate the appropriate registry k determine what, if any, trusted documents exist on th It will also enumerate ...
powershell/situational_awareness/host/monitortcpconnections	Monitors hosts for TCP connections to a specified do name or IPv4 address. Useful for session hijacking ar finding users interacting with ...
powershell/situational_awareness/host/seatbelt	Seatbelt is a C# project that performs a number of se oriented host-survey "safety checks" relevant from bo offensive and defensive security ...
powershell/situational_awareness/host/paranoia	Continuously check running processes for the presen suspicious users, members of groups, process name for any processes running off of USB ...
powershell/situational_awareness/host/computerdetails	Enumerates useful information on the system. By def all checks are run.
powershell/privesc/bypassuac	Runs a BypassUAC attack to escape from a medium integrity process to a high integrity process. This atta originally discovered by Leo Davidson. ...
powershell/privesc/bypassuac_env	Bypasses UAC (even with Always Notify level set) by performing an registry modification of the "windir" valu "Environment" based on James ...
powershell/privesc/bypassuac_tokenmanipulation	Bypass UAC module based on the script released by Nelson @enigma0x3 at Derbycon 2017.
powershell/privesc/winPEAS	WinPEAS is a script that search for possible paths to escalate privileges on Windows hosts.
powershell/privesc/sweetpotato	Abuses default privileges given to Local Service acco to spawn a process as SYSTEM. Tested on Server 2(and Windows 10 1909 (Build 18363.1316). ...
powershell/privesc/tater	Tater is a PowerShell implementation of the Hot Pota Windows Privilege Escalation exploit from @breenma and @foxglovesec.
powershell/privesc/ms16-135	Spawns a new Listener as SYSTEM by leveraging th MS16-135 local exploit. This exploit is for x64 only an works on unlocked session. Note: the ...
powershell/privesc/ask	Leverages Start-Process' -Verb runAs option inside a Required loop to prompt the user for a high integrity c before running the agent code. ...
powershell/privesc/bypassuac_wscript	Drops wscript.exe and a custom manifest into C:\Win and then proceeds to execute VBScript using the wsc executablewith the new manifest. The ...

Empire Module	Module Description
powershell/privesc/mcafee_sitelist	Retrieves the plaintext passwords for found McAfee's SiteList.xml files.
powershell/privesc/privesccheck	Find Windows local privilege escalation vulnerabilities
powershell/privesc/sherlock	Find Windows local privilege escalation vulnerabilities
powershell/privesc/ms16-032	Spawns a new Listener as SYSTEM by leveraging th MS16-032 local exploit. Note: ~1/6 times the exploit v work, may need to retry.
powershell/privesc/bypassuac_eventvwr	Bypasses UAC by performing an image hijack on the file extension and starting eventvwr.exe. No files are dropped to disk, making this opsec safe.
powershell/privesc/zerologon	CVE-2020-1472 or ZeroLogon exploits a flaw in the Netlogon protocol to allow anyone on the network to r the domain administrators hash and ...
powershell/privesc/printdemon	This is an Empire launcher PoC using PrintDemon, th CVE-2020-1048 is a privilege escalation vulnerability allows a persistent threat through ...
powershell/privesc/getsystem	Gets SYSTEM privileges with one of two methods.
powershell/privesc/gpp	Retrieves the plaintext password and other informatic accounts pushed through Group Policy Preferences.
powershell/privesc/bypassuac_sdctlbypass	Bypasses UAC by performing an registry modificatior sdclt (based onhttps://enigma0x3.net/2017/03/17/filel uac-bypass-using-sdclt-exe/).
powershell/privesc/watson	Watson is a .NET tool designed to enumerate missing and suggest exploits for Privilege Escalation vulnerab
powershell/privesc/bypassuac_fodhelper	Bypasses UAC by performing an registry modificatior FodHelper (based onhttps://winscripting.blog/2017/05/12/first-entry-welc and-uac-bypass/).
powershell/privesc/printnightmare	Exploits CVE-2021-1675 (PrintNightmare) locally to a new local administrator user with a known password. Optionally, this can be used to execute ...
powershell/privesc/powerup/service_exe_useradd	Backs up a service's binary and replaces the original binary that creates/adds a local administrator.
powershell/privesc/powerup/write_dllhijacker	Writes out a hijackable .dll to the specified path along stager.bat that's called by the .dll. wlbsctrl.dll works w Windows 7. The ...
powershell/privesc/powerup/service_stager	Modifies a target service to execute an Empire stager
powershell/privesc/powerup/service_exe_restore	Restore a backed up service binary.
powershell/privesc/powerup/service_exe_stager	Backs up a service's binary and replaces the original binary that launches a stager.bat.
powershell/privesc/powerup/find_dllhijack	Finds generic .DLL hijacking opportunities.
powershell/privesc/powerup/service_useradd	Modifies a target service to create a local user and ac the local administrators.
powershell/privesc/powerup/allchecks	Runs all current checks for Windows privesc vectors.
powershell/collection/get_sql_query	Executes a query on target SQL servers.
powershell/collection/SharpLoginPrompt	This Program creates a login prompt to gather usernа and password of the current user. This project allows team to phish username and password ...
powershell/collection/file_finder	Finds sensitive files on the domain.
powershell/collection/get_indexed_item	Gets files which have been indexed by Windows desl search.
powershell/collection/ninjacopy	Copies a file from an NTFS partitioned volume by rea the raw volume and parsing the NTFS structures.
powershell/collection/clipboard_monitor	Monitors the clipboard on a specified interval for char copied text.

Empire Module	Module Description
powershell/collection/FoxDump	This module will dump any saved passwords from Fir to the console. This should work for any versionof Fir above version 32. This will only be ...
powershell/collection/prompt	Prompts the current user to enter their credentials in a forms box and returns the results.
powershell/collection/minidump	Generates a full-memory dump of a process. Note: To dump another user's process, you must be running fr elevated prompt (e.g to dump lsass).
powershell/collection/netripper	Injects NetRipper into targeted processes, which uses hooking in order to intercept network traffic and encry related functions from a low ...
powershell/collection/SauronEye	SauronEye is a search tool built to aid red teams in fi files containing specific keywords.
powershell/collection/toasted	Spawns a native toast notification that, if clicked, pror the current user to enter their credentials into a native looking prompt. Notification ...
powershell/collection/screenshot	Takes a screenshot of the current desktop and return output as a .PNG.
powershell/collection/find_interesting_file	Finds sensitive files on the domain.
powershell/collection/inveigh	Inveigh is a Windows PowerShell LLMNR/mDNS/NBI spoofer/man-in-the-middle tool. Note that this module exposes only a subset of Inveigh's parameters. ...
powershell/collection/browser_data	Search through browser history or bookmarks.
powershell/collection/WireTap	WireTap is a .NET 4.0 project to consolidate several functions used to interact with a user's hardware, incl Screenshots (Display + WebCam ...
powershell/collection/WebcamRecorder	This module uses the DirectX.Capture and DShowNE .NET assemblies to capture video from a webcam.
powershell/collection/ChromeDump	This module will decrypt passwords saved in chrome display them in the console.
powershell/collection/USBKeylogger	Logs USB keys pressed using Event Tracing for Wind (ETW).
powershell/collection/get_sql_column_sample_data	Returns column information from target SQL Servers Supports search by keywords, sampling data, and validating credit card numbers.
powershell/collection/keylogger	Logs keys pressed, time and the active window (whe changed) to the keystrokes.txt file. This file is located agents downloads directory ...
powershell/collection/get-winupdates	This module will list the Microsoft update history, inclu pending updates, of the machine.
powershell/collection/packet_capture	Starts a packet capture on a host using netsh.
powershell/collection/SharpChromium	This module will retrieve cookies, history, saved login Google Chrome, Microsoft Edge, and Microsoft Edge
powershell/collection/vaults/remove_keepass_config_trigger	This module removes all triggers from all KeePass co found by Find-KeePassConfig.
powershell/collection/vaults/add_keepass_config_trigger	This module adds a KeePass exfiltration trigger to all KeePass configs found by Find-KeePassConfig.
powershell/collection/vaults/keethief	This module retrieves database mastey key informati unlocked KeePass database.
powershell/collection/vaults/find_keepass_config	This module finds and parses any KeePass.config.xm and KeePass.ini (1.X) files.
powershell/collection/vaults/get_keepass_config_trigger	This module extracts out the trigger specifications fro KeePass 2.X configuration XML file.
powershell/persistence/userland/schtasks	Persist a stager (or script) using schtasks. This has a moderate detection/removal rating.

Empire Module	Module Description
powershell/persistence/userland/registry	Persist a stager (or script) via the HKCU:SOFTWARE\Microsoft\Windows\CurrentVersi registry key. This has an easy detection/removal ratin
powershell/persistence/userland/backdoor_lnk	Backdoor a specified .LNK file with a version that lau the original binary and then an Empire stager.
powershell/persistence/powerbreach/deaduser	Backup backdoor for a backdoor user.
powershell/persistence/powerbreach/eventlog	Starts the event-loop backdoor.
powershell/persistence/powerbreach/resolver	Starts the Resolver Backdoor.
powershell/persistence/misc/debugger	Sets the debugger for a specified target binary to be cmd.exe, another binary of your choice, or a listern st This can be launched from the ...
powershell/persistence/misc/disable_machine_acct_change	Disables the machine account for the target system f changing its password automatically.
powershell/persistence/misc/get_ssps	Enumerates all loaded security packages (SSPs).
powershell/persistence/misc/add_sid_history	Runs PowerSploit's Invoke-Mimikatz function to exec misc::addsid to add sid history for a user. ONLY APPLICABLE ON DOMAIN CONTROLLERS!.
powershell/persistence/misc/add_netuser	Adds a domain user or a local user to the current (or remote) machine, if permissions allow,.
powershell/persistence/misc/install_ssp	Installs a security support provider (SSP) dll.
powershell/persistence/misc/memssp	Runs PowerSploit's Invoke-Mimikatz function to exec misc::memssp to log all authentication events to C:\Windows\System32\mimisla.log.
powershell/persistence/misc/skeleton_key	Runs PowerSploit's Invoke-Mimikatz function to exec misc::skeleton to implant a skeleton key w/ password 'mimikatz'. ONLY APPLICABLE ON DOMAIN ...
powershell/persistence/elevated/wmi_updater	Persist a stager (or script) using a permanent WMI subscription. This has a difficult detection/removal rat
powershell/persistence/elevated/schtasks	Persist a stager (or script) using schtasks running as SYSTEM. This has a moderate detection/removal rat
powershell/persistence/elevated/registry	Persist a stager (or script) via the HKLM:SOFTWARE\Microsoft\Windows\CurrentVersi registry key. This has an easy detection/removal ratin
powershell/persistence/elevated/wmi	Persist a stager (or script) using a permanent WMI subscription. This has a difficult detection/removal rat
powershell/persistence/elevated/rid_hijack	Runs Invoke-RIDHijacking. Allows setting desired pri to an existent account by modifying the Relative Iden value copy used to create the ...
powershell/exfiltration/exfil_dropbox	Upload a file to dropbox.
powershell/exfiltration/egresscheck	This module will generate traffic on a provided range ports and supports both TCP and UDP. Useful to ider direct egress channels.
powershell/lateral_movement/invoke_sqloscmd	Executes a command or stager on remote hosts usin xp_cmdshell.
powershell/lateral_movement/invoke_psremoting	Executes a stager on remote hosts using PSRemotin
powershell/lateral_movement/invoke_executemsbuild	This module utilizes WMI and MSBuild to compile an execute an xml file containing an Empire launcher.
powershell/lateral_movement/invoke_dcom	Execute a stager or command on remote hosts using DCOM.
powershell/lateral_movement/invoke_portfwd	Forward a port with no admin rights required.
powershell/lateral_movement/invoke_psexec	Executes a stager on remote hosts using PsExec typ functionality.
powershell/lateral_movement/jenkins_script_console	Exploit unauthenticated Jenkins Script consoles.
powershell/lateral_movement/new_gpo_immediate_task	Builds an 'Immediate' schtask to push out through a specified GPO.

Empire Module	Module Description
powershell/lateral_movement/invoke_smbexec	Executes a stager on remote hosts using SMBExec.p This module requires a username and NTLM hash.
powershell/lateral_movement/invoke_wmi	Executes a stager on remote hosts using WMI.
powershell/lateral_movement/inveigh_relay	Inveigh's SMB relay function. This module can be use relay incoming HTTP/Proxy NTLMv1/NTLMv2 authentication requests to an SMB target. If the ...
powershell/lateral_movement/invoke_wmi_debugger	Uses WMI to set the debugger for a target binary on a remote machine to be cmd.exe or a stager.
powershell/lateral_movement/invoke_sshcommand	Executes a command on a remote host via SSH.
external/generate_agent	Generates an agent code instance for a specified liste pre-staged, and register the agent in the database. T allows the agent to begin ...

Showing 1 to 393 of 393 entries

If you find this useful and you would like more content like this, please subscribe to my mailing list and follow InfosecMatter on Twitter and Facebook to keep up with the latest developments. You can also buy me a coffee.