The Ultimate List of Hacking Scripts for Metasploit's Meterpreter

Welcome back, my hacker apprentices!
Metasploit framework is an incredible hacking and pentesting tool that every hacker worth their salt should be conversant and capable on.
In a previous post, I had provided you a **cheat sheet of meterpreter commands**. These commands are essential to running Metasploit's meterpreter, but in recent years, numerous hackers and security pros have developed scripts that we can run from the meterpreter that can be much more effective and malicious.
In this post, I will try to provide you the most complete list and description available anywhere on the web. You will want to bookmark this page too, as no one remembers all these scripts and it's likely you will want to return here at a later time to find a particular script for a particular hack.

Please note that new meterpreter scripts are being developed every day. This list attempts to provide you with a complete list of scripts as of this writing. If you find errors or typos, please feel free to post them here, so I will try correct them as soon as humanly possible.

Script Commands with Brief Descriptions

- **arp_scanner.rb** - Script for performing an ARP's Scan Discovery.
- **autoroute.rb** - Meterpreter session without having to background the current session.
- **checkvm.rb** - Script for detecting if target host is a virtual machine.
- **credcollect.rb** - Script to harvest credentials found on the host and store them in the database.
- **domain_list_gen.rb** - Script for extracting domain admin account list for use.
- **dumplinks.rb** - Dumplinks parses .lnk files from a user's recent documents folder and Microsoft Office's Recent documents folder, if present. The .lnk

files contain time stamps, file locations, including share names, volume serial #s and more. This info may help you target additional systems.

- **duplicate.rb** - Uses a meterpreter session to spawn a new meterpreter session in a different process. A new process allows the session to take "risky" actions that might get the process killed by A/V, giving a meterpreter session to another controller, or start a keylogger on another process.
- **enum_chrome.rb** - Script to extract data from a chrome installation.
- **enum_firefox.rb** - Script for extracting data from Firefox. **enum_logged_on_users.rb** - Script for enumerating current logged users and users that have logged in to the system. **enum_powershell_env.rb** - Enumerates PowerShell and WSH configurations.
- **enum_putty.rb** - Enumerates Putty connections.
- **enum_shares.rb** - Script for Enumerating shares offered and history of mounted shares.
- **enum_vmware.rb** - Enumerates VMware configurations for VMware products.
- **event_manager.rb** - Show information about Event Logs on the target system and their configuration.
- **file_collector.rb** - Script for searching and downloading files that match a specific pattern.
- **get_application_list.rb** - Script for extracting a list of installed applications and their version.
- **getcountermeasure.rb** - Script for detecting AV, HIPS, Third Party Firewalls, DEP Configuration and Windows Firewall configuration. Provides also the option to kill the processes of detected products and disable the built-in firewall.
- **get_env.rb** - Script for extracting a list of all System and User environment variables.
- **getfilezillacreds.rb** - Script for extracting servers and credentials from Filezilla.
- **getgui.rb** - Script to enable Windows RDP.
- **get_local_subnets.rb** - Get a list of local subnets based on the host's routes.
- **get_pidgen_creds.rb** - Script for extracting configured services with username and passwords.

- **gettelnet.rb** - Checks to see whether telnet is installed.
- **get_valid_community.rb** - Gets a valid community string from SNMP.
- **getvncpw.rb** - Gets the VNC password.
- **hashdump.rb** - Grabs password hashes from the SAM.
- **hostedit.rb** - Script for adding entries in to the Windows Hosts file.
- **keylogrecorder.rb** - Script for running keylogger and saving all the keystrokes.
- **killav.rb** - Terminates nearly every antivirus software on victim.
- **metsvc.rb** - Delete one meterpreter service and start another.
- **migrate** - Moves the meterpreter service to another process.
- **multicommand.rb** - Script for running multiple commands on Windows 2003, Windows Vistaand Windows XP and Windows 2008 targets.
- **multi_console_command.rb** - Script for running multiple console commands on a meterpreter session.
- **multi_meter_inject.rb** - Script for injecting a reverce tcp Meterpreter Payload into memory of multiple PIDs, if none is provided a notepad process will be created and a Meterpreter Payload will be injected in to each.
- **multiscript.rb** - Script for running multiple scripts on a Meterpreter session.
- **netenum.rb** - Script for ping sweeps on Windows 2003, Windows Vista, Windows 2008 and Windows XP targets using native Windows commands.
- **packetrecorder.rb** - Script for capturing packets in to a PCAP file.
- **panda2007pavsrv51.rb** - This module exploits a privilege escalation vulnerability in Panda Antivirus 2007. Due to insecure permission issues, a local attacker can gain elevated privileges.
- **persistence.rb** - Script for creating a persistent backdoor on a target host.
- **pml_driver_config.rb** - Exploits a privilege escalation vulnerability in Hewlett-Packard's PML Driver HPZ12. Due to an insecure SERVICE_CHANGE_CONFIG DACL permission, a local attacker can gain elevated privileges.
- **powerdump.rb** - Meterpreter script for utilizing purely PowerShell to extract username and password hashes through registry keys. This script requires you to be running as system in order to work properly. This has currently been tested on Server 2008 and Windows 7, which installs PowerShell by default.

- **prefetchtool.rb** - Script for extracting information from windows prefetch folder.
- **process_memdump.rb** - Script is based on the paper Neurosurgery With Meterpreter.
- **remotewinenum.rb** - This script will enumerate windows hosts in the target environment given a username and password or using the credential under which Meterpeter is running using WMI wmic windows native tool.
- **scheduleme.rb** - Script for automating the most common scheduling tasks during a pentest. This script works with Windows XP, Windows 2003, Windows Vista and Windows 2008.
- **schelevator.rb** - Exploit for Windows Vista/7/2008 Task Scheduler 2.0 Privilege Escalation. This script exploits the Task Scheduler 2.0 XML 0day exploited by Stuxnet.
- **schtasksabuse.rb** - Meterpreter script for abusing the scheduler service in Windows by scheduling and running a list of command against one or more targets. Using schtasks command to run them as system. This script works with Windows XP, Windows 2003, Windows Vista and Windows 2008.
- **scraper.rb** - The goal of this script is to obtain system information from a victim through an existing Meterpreter session.
- **screenspy.rb** - This script will open an interactive view of remote hosts. You will need Firefox installed on your machine.
- **screen_unlock.rb** - Script to unlock a windows screen. Needs system privileges to run and known signatures for the target system.
- **screen_dwld.rb** - Script that recursively search and download files matching a given pattern.
- **service_manager.rb** - Script for managing Windows services.
- **service_permissions_escalate.rb** This script attempts to create a service, then searches through a list of existing services to look for insecure file or configuration permissions that will let it replace the executable with a payload. It will then attempt to restart the replaced service to run the payload. If that fails, the next time the service is started (such as on reboot) the attacker will gain elevated privileges.
- **sound_recorder.rb** - Script for recording in intervals the sound capture by a target host microphone.
- **srt_webdrive_priv.rb** - Exploits a privilege escalation vulnerability in South River Technologies WebDrive.

- **uploadexec.rb** - Script to upload executable file to host.
- **virtualbox_sysenter_dos** - Script to DoS Virtual Box.
- **virusscan_bypass.rb** - Script that kills Mcafee VirusScan Enterprise v8.7.0i+ processes.
- **vnc.rb** - Meterpreter script for obtaining a quick VNC session.
- **webcam.rb** - Script to enable and capture images from the host webcam.
- **win32-sshclient.rb** - Script to deploy & run the "plink" commandline ssh-client. Supports only MS-Windows-2k/XP/Vista Hosts.
- **win32-sshserver.rb** - Script to deploy and run OpenSSH on the target machine.
- **winbf.rb** - Function for checking the password policy of current system. This policy may resemble the policy of other servers in the target environment.
- **winenum.rb** - Enumerates Windows system including environment variables, network interfaces, routing, user accounts, etc
- **wmic.rb** - Script for running WMIC commands on Windows 2003, Windows Vista and Windows XP and Windows 2008 targets.