Powershell Empire

Invoke Obfuscation
- Invoke-Obfuscation.ps1
- Invoke-Obfuscation.psd1
- Invoke-Obfuscation.psm1
- Out-CompressedCommand.ps1
- Out-EncodedAsciiCommand.ps1
- Out-EncodedBXORCommand.ps1
- Out-EncodedBinaryCommand.ps1
- Out-EncodedHexCommand.ps1
- Out-EncodedOctalCommand.ps1
- Out-EncodedSpecialCharOnlyCommand.ps1
- Out-EncodedWhitespaceCommand.ps1
- Out-ObfuscatedAst.ps1
- Out-ObfuscatedStringCommand.ps1
- Out-ObfuscatedTokenCommand.ps1
- Out-PowerShellLauncher.ps1
- Out-SecureStringCommand.ps1

Code Execution
- invoke_assembly.py
- invoke_assembly.yaml
- invoke_bof.py
- invoke_bof.yaml
- invoke_boolang.yaml
- invoke_clearscript.yaml
- invoke_dllinjection.yaml
- invoke_ironpython.yaml
- invoke_ironpython3.yaml
- invoke_metasploitpayload.yaml
- invoke_ntsd.py
- invoke_ntsd.yaml
- invoke_reflectivepeinjection.py
- invoke_reflectivepeinjection.yaml
- invoke_shellcode.py
- invoke_shellcode.yaml
- invoke_shellcodemsil.py
- invoke_shellcodemsil.yaml
- invoke_sharp.yaml

Trollsploit
- get_schwifty.yaml
- message.yaml
- process_killer.yaml
- rick_ascii.yaml
- rick_astley.yaml
- thunderstruck.yaml
- voicetroll.yaml
- wallpaper.yaml
- wlmdr.yaml

Collection
- **Vaults**
  - add_keepass_config_trigger.yaml
  - find_keepass_config.yaml
  - get_keepass_config_trigger.yaml
  - keethief.yaml
  - remove_keepass_config_trigger.yaml
- ChromeDump.yaml
- FoxDump.yaml
- SauronEye.yaml
- SharpChromium.py
- SharpChromium.yaml
- SharpLoginPrompt.yaml
- USBKeylogger.yaml
- WebcamRecorder.yaml
- WireTap.py
- WireTap.yaml
- browser_data.yaml
- clipboard_monitor.yaml
- file_finder.yaml
- find_interesting_file.yaml
- get-winupdates.yaml
- get_indexed_item.yaml
- get_sql_column_sample_data.py
- get_sql_column_sample_data.yaml
- get_sql_query.yaml
- inveigh.yaml
- keylogger.yaml
- minidump.py
- minidump.yaml
- netripper.yaml
- ninjacopy.yaml
- packet_capture.py
- packet_capture.yaml
- prompt.yaml
- screenshot.py
- screenshot.yaml
- toasted.yaml

Situational Awareness
- **Host**
  - antivirusproduct.yaml
  - applockerstatus.yaml
  - computerdetails.py
  - computerdetails.yaml
  - dnsserver.yaml
  - findtrusteddocuments.yaml
  - get_pathacl.yaml
  - get_proxy.yaml
  - get_uaclevel.yaml
  - hostrecon.yaml
  - monitortcpconnections.yaml
  - paranoia.yaml
  - seatbelt.py
  - seatbelt.yaml
  - winenum.yaml
- **Network**
  - **Powermad**
    - get_adidns_permission.yaml
    - get_adidns_zone.yaml
  - **Powerview**
    - find_foreign_group.yaml
    - find_foreign_user.yaml
    - find_gpo_computer_admin.yaml
    - find_gpo_location.yaml
    - find_localadmin_access.yaml
    - find_managed_security_group.yaml
    - get_cached_rdpconnection.yaml
    - get_computer.yaml
    - get_dfs_share.yaml
    - get_domain_controller.yaml
    - get_domain_policy.yaml
    - get_domain_trust.yaml
    - get_fileserver.yaml
    - get_forest.yaml
    - get_forest_domain.yaml
    - get_gpo.yaml
    - get_gpo_computer.py
    - get_gpo_computer.yaml
    - get_group.yaml
    - get_group_member.yaml
    - get_localgroup.yaml
    - get_loggedon.yaml
    - get_object_acl.yaml
    - get_ou.yaml
    - get_rdp_session.yaml
    - get_session.yaml
    - get_site.yaml
    - get_subnet.yaml
    - get_subnet_ranges.py
    - get_subnet_ranges.yaml
    - get_user.yaml
    - map_domain_trust.yaml
    - process_hunter.yaml
    - set_ad_object.yaml
    - share_finder.yaml
    - user_hunter.yaml
  - arpscan.yaml
  - bloodhound.yaml
  - bloodhound3.yaml
  - get_kerberos_service_ticket.yaml
  - get_spn.yaml
  - get_sql_instance_domain.yaml
  - get_sql_server_info.py
  - get_sql_server_info.yaml
  - portscan.yaml
  - reverse_dns.yaml
  - smbautobrute.yaml
  - smblogin.yaml
  - smbscanner.yaml

Credentials
- **Mimikatz**
  - cache.yaml
  - certs.yaml
  - command.yaml
  - dcsync.yaml
  - dcsync_hashdump.py
  - dcsync_hashdump.yaml
  - extract_tickets.yaml
  - golden_ticket.py
  - golden_ticket.yaml
  - keys.yaml
  - logonpasswords.yaml
  - lsadump.py
  - lsadump.yaml
  - mimitokens.py
  - mimitokens.yaml
  - pth.py
  - pth.yaml
  - purge.yaml
  - sam.yaml
  - silver_ticket.py
  - silver_ticket.yaml
  - terminal_server.yaml
  - trust_keys.py
  - trust_keys.yaml
- DomainPasswordSpray.yaml
- VeeamGetCreds.yaml
- credential_injection.py
- credential_injection.yaml
- enum_cred_store.yaml
- get_lapspasswords.yaml
- invoke_internal_monologue.yaml
- invoke_kerberoast.yaml
- invoke_ntlmextract.yaml
- powerdump.yaml
- rubeus.yaml
- sessiongopher.yaml
- sharpsecdump.yaml
- tokens.py
- tokens.yaml
- vault_credential.yaml

Recon
- fetch_brute_local.py
- fetch_brute_local.yaml
- find_fruit.py
- find_fruit.yaml
- get_sql_server_login_default_pw.py
- get_sql_server_login_default_pw.yaml
- http_login.yaml

Exfiltration
- egresscheck.yaml
- exfil_dropbox.yaml

Exploitation
- exploit_eternalblue.py
- exploit_eternalblue.yaml
- exploit_jboss.yaml
- exploit_jenkins.yaml
- invoke_spoolsample.yaml

Privesc
- **Powerup**
  - allchecks.yaml
  - find_dllhijack.yaml
  - service_exe_restore.yaml
  - service_exe_stager.py
  - service_exe_stager.yaml
  - service_exe_useradd.yaml
  - service_stager.py
  - service_stager.yaml
  - service_useradd.yaml
  - write_dllhijacker.py
  - write_dllhijacker.yaml
- ask.py
- ask.yaml
- bypassuac.py
- bypassuac.yaml
- bypassuac_env.py
- bypassuac_env.yaml
- bypassuac_eventvwr.py
- bypassuac_eventvwr.yaml
- bypassuac_fodhelper.py
- bypassuac_fodhelper.yaml
- bypassuac_fodhelper_progids.yaml
- bypassuac_sdctlbypass.py
- bypassuac_sdctlbypass.yaml
- bypassuac_tokenmanipulation.py
- bypassuac_tokenmanipulation.yaml
- bypassuac_wscript.py
- bypassuac_wscript.yaml
- getsystem.yaml
- gpp.yaml
- mcafee_sitelist.yaml
- ms16-032.py
- ms16-032.yaml
- ms16-135.py
- ms16-135.yaml
- printdemon.yaml
- printnightmare.yaml
- privesccheck.yaml
- sherlock.yaml
- sweetpotato.yaml
- tater.yaml
- watson.yaml
- winPEAS.yaml
- zerologon.yaml

Lateral Movement
- inveigh_relay.py
- inveigh_relay.yaml
- invoke_dcom.py
- invoke_dcom.yaml
- invoke_executemsbuild.py
- invoke_executemsbuild.yaml
- invoke_portfwd.yaml
- invoke_psexec.py
- invoke_psexec.yaml
- invoke_psremoting.py
- invoke_psremoting.yaml
- invoke_smbexec.py
- invoke_smbexec.yaml
- invoke_sqloscmd.py
- invoke_sqloscmd.yaml
- invoke_sshcommand.py
- invoke_sshcommand.yaml
- invoke_wmi.py
- invoke_wmi.yaml
- invoke_wmi_debugger.py
- invoke_wmi_debugger.yaml
- jenkins_script_console.py
- jenkins_script_console.yaml
- new_gpo_immediate_task.py
- new_gpo_immediate_task.yaml

Management
- **Mailraider**
  - disable_security.py
  - disable_security.yaml
  - get_emailitems.py
  - get_emailitems.yaml
  - get_subfolders.yaml
  - mail_search.yaml
  - search_gal.yaml
  - send_mail.yaml
  - view_email.yaml
- disable_rdp.yaml
- downgrade_account.yaml
- enable_multi_rdp.yaml
- enable_rdp.yaml
- get_domain_sid.yaml
- honeyhash.yaml
- invoke-downloadfile.yaml
- invoke_script.py
- invoke_script.yaml
- invoke_sharpchisel.yaml
- invoke_socksproxy.yaml
- lock.yaml
- logoff.py
- logoff.yaml
- phant0m.yaml
- powercat.yaml
- psinject.py
- psinject.yaml
- reflective_inject.py
- reflective_inject.yaml
- restart.yaml
- runas.py
- runas.yaml
- shinject.py
- shinject.yaml
- sid_to_user.yaml
- spawn.py
- spawn.yaml
- spawnas.py
- spawnas.yaml
- start-processasuser.yaml
- switch_listener.py
- switch_listener.yaml
- timestomp.yaml
- user_to_sid.py
- user_to_sid.yaml
- vnc.yaml
- wdigest_downgrade.yaml
- zipfolder.yaml

Persistence
- **Elevated**
  - registry.py
  - registry.yaml
  - rid_hijack.yaml
  - schtasks.py
  - schtasks.yaml
  - wmi.py
  - wmi.yaml
  - wmi_updater.py
  - wmi_updater.yaml
- **Misc**
  - add_netuser.yaml
  - add_sid_history.py
  - add_sid_history.yaml
  - debugger.py
  - debugger.yaml
  - disable_machine_acct_change.yaml
  - get_ssps.yaml
  - install_ssp.yaml
  - memssp.yaml
  - skeleton_key.yaml
- **Powerbreach**
  - deaduser.py
  - deaduser.yaml
  - eventlog.py
  - eventlog.yaml
  - resolver.py
  - resolver.yaml
- **Userland**
  - backdoor_lnk.py
  - backdoor_lnk.yaml