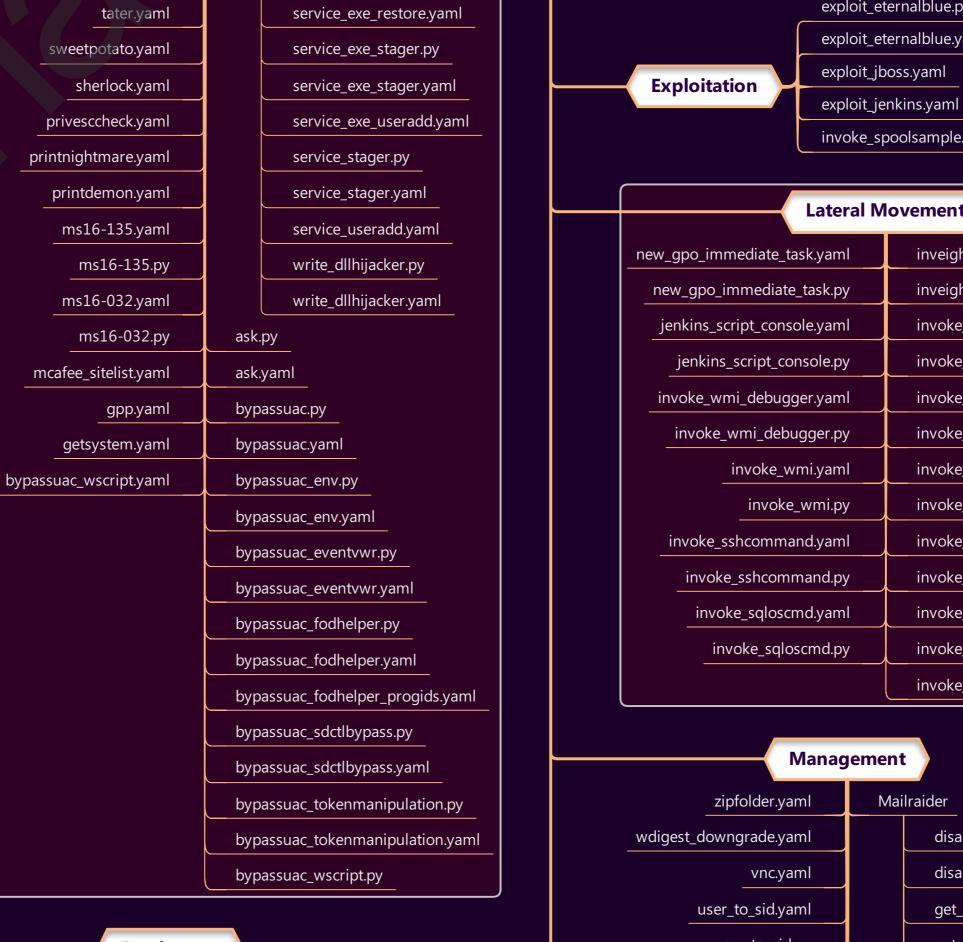
## **Powershell Empire** invoke\_assembly.py invoke\_assembly.yaml invoke\_bof.py invoke\_bof.yaml invoke\_boolang.yaml invoke\_clearscript.yaml invoke\_dllinjection.yaml invoke\_ironpython.yaml **Invoke Obfuscation** invoke\_ironpython3.yaml invoke\_metasploitpayload.yaml **Code Execution** invoke\_ntsd.py invoke\_ntsd.yaml invoke\_reflectivepeinjection.py invoke\_reflectivepeinjection.yaml invoke\_shellcode.py invoke\_shellcode.yaml invoke\_shellcodemsil.py get\_schwifty.yaml invoke\_shellcodemsil.yaml message.yaml invoke\_ssharp.yaml process\_killer.yaml rick\_ascii.yaml Collection rick\_astley.yaml **Trollsploit** toasted.yaml Vaults thunderstruck.yaml add\_keepass\_config\_trigger.yaml screenshot.yaml voicetroll.yaml screenshot.py find\_keepass\_config.yaml wallpaper.yaml get\_keepass\_config\_trigger.yaml prompt.yaml wlmdr.yaml keethief.yaml packet\_capture.yaml packet\_capture.py remove\_keepass\_config\_trigger.yaml **Situational Awareness** ChromeDump.yaml ninjacopy.yaml Host FoxDump.yaml netripper.yaml antivirusproduct.yaml minidump.yaml SauronEye.yaml applockerstatus.yaml minidump.py SharpChromium.py computerdetails.py keylogger.yaml SharpChromium.yaml computerdetails.yaml inveigh.yaml SharpLoginPrompt.yaml dnsserver.yaml USBKeylogger.yaml get\_sql\_query.yaml findtrusteddocuments.yaml get\_sql\_column\_sample\_data.yaml WebcamRecorder.yaml get\_pathacl.yaml WireTap.py get\_sql\_column\_sample\_data.py get\_proxy.yaml get\_indexed\_item.yaml WireTap.yaml get\_uaclevel.yaml browser\_data.yaml hostrecon.yaml clipboard\_monitor.yaml monitortcpconnections.yaml file\_finder.yaml paranoia.yaml find\_interesting\_file.yaml seatbelt.py get-winupdates.yaml seatbelt.yaml winenum.yaml **Credentials** vault\_credential.yaml Mimikatz tokens.yaml trust\_keys.yaml cache.yaml tokens.py trust\_keys.py certs.yaml terminal\_server.yaml sharpsecdump.yaml command.yaml sessiongopher.yaml silver\_ticket.yaml dcsync.yaml silver\_ticket.py dcsync\_hashdump.py rubeus.yaml dcsync\_hashdump.yaml powerdump.yaml sam.yaml invoke\_ntlmextract.yaml extract\_tickets.yaml purge.yaml golden\_ticket.py pth.yaml pth.py golden\_ticket.yaml keys.yaml mimitokens.yaml logonpasswords.yaml mimitokens.py Isadump.yaml lsadump.py fetch\_brute\_local.py DomainPasswordSpray.yaml fetch\_brute\_local.yaml VeeamGetCreds.yaml find\_fruit.py credential\_injection.py find\_fruit.yaml Recon credential\_injection.yaml get\_sql\_server\_login\_default\_pw.py enum\_cred\_store.yaml get\_sql\_server\_login\_default\_pw.yaml get\_lapspasswords.yaml http\_login.yaml invoke\_internal\_monologue.yaml invoke\_kerberoast.yaml Powerup egresscheck.yaml **Exfiltration** allchecks.yaml exfil\_dropbox.yaml find\_dllhijack.yaml exploit\_eternalblue.py exploit\_eternalblue.yaml exploit\_jboss.yaml **Exploitation** exploit\_jenkins.yaml invoke\_spoolsample.yaml **Lateral Movement** new\_gpo\_immediate\_task.yaml inveigh\_relay.py inveigh\_relay.yaml new\_gpo\_immediate\_task.py invoke\_dcom.py jenkins\_script\_console.yaml jenkins\_script\_console.py invoke\_dcom.yaml invoke\_wmi\_debugger.yaml invoke\_executemsbuild.py invoke\_wmi\_debugger.py invoke\_executemsbuild.yaml invoke\_wmi.yaml invoke\_portfwd.yaml invoke\_wmi.py invoke\_psexec.py invoke\_sshcommand.yaml invoke\_psexec.yaml invoke\_sshcommand.py invoke\_psremoting.py invoke\_sqloscmd.yaml invoke\_psremoting.yaml invoke\_smbexec.py invoke\_sqloscmd.py invoke\_smbexec.yaml Management rity.py ity.yaml ns.py ns.yaml rs.yaml /aml



	bypassuac_tokenmanipulation.py	zipfolder.yaml	Mailraider
	bypassuac_tokenmanipulation.yaml	_wdigest_downgrade.yaml	disable_security.py
	bypassuac_wscript.py	vnc.yaml	disable_security.yan
		user_to_sid.yaml	get_emailitems.py
Persis	tence	_user_to_sid.py	get_emailitems.yam
Userland	Elevated	timestomp.yaml	get_subfolders.yam
ackdoor_Ink.py	registry.py	switch_listener.yaml	mail_search.yaml
door_Ink.yaml	registry.yaml	switch_listener.py	search_gal.yaml
Powerbreach	rid_hijack.yaml	start-processasuser.yaml	send_mail.yaml
deaduser.py	schtasks.py	spawnas.yaml	view_email.yaml
deaduser.yaml	schtasks.yaml	spawnas.py	disable_rdp.yaml
eventlog.py	wmi.py	spawn.yaml	downgrade_account.yaml
eventlog.yaml	wmi.yaml	spawn.py	enable_multi_rdp.yaml
resolver.py	wmi_updater.py	sid_to_user.yaml	enable_rdp.yaml
resolver.yaml	wmi_updater.yaml	shinject.yaml	get_domain_sid.yaml
	Misc	shinject.py	honeyhash.yaml
	add_netuser.yaml	runas.yaml	invoke-downloadfile.yaml
	add_sid_history.py	runas.py	invoke_script.py
	add_sid_history.yaml	restart.yaml	invoke_script.yaml
	debugger.py	reflective_inject.yaml	invoke_sharpchisel.yaml
	debugger.yaml		invoke_socksproxy.yaml
	disable_machine_acct_change.yaml		lock.yaml
	get_ssps.yaml		logoff.py
	install_ssp.yaml		logoff.yaml
	memssp.yaml		phant0m.yaml
	skeleton_key.yaml		powercat.yaml
	Skeretori_key.yarrii		psinject.py
			psinject.yaml

backd

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-ObfuscatedAst.ps1

Out-Encoded Special Char Only Command.ps 1

Network

smbscanner.yaml

smbautobrute.yaml

get\_sql\_server\_info.yaml

get\_sql\_server\_info.py

reverse\_dns.yaml

portscan.yaml

smblogin.yaml

Powermad

get\_adidns\_permission.yaml

Powerview

find\_foreign\_group.yaml

find\_foreign\_user.yaml

find\_gpo\_location.yaml

get\_computer.yaml

get\_dfs\_share.yaml

find\_localadmin\_access.yaml

find\_managed\_security\_group.yaml

get\_cached\_rdpconnection.yaml

get\_domain\_controller.yaml

get\_domain\_policy.yaml

get\_domain\_trust.yaml

get\_forest\_domain.yaml

get\_gpo\_computer.py

get\_gpo\_computer.yaml

Privesc

zerologon.yaml

winPEAS.yaml

watson.yaml

get\_fileserver.yaml

get\_forest.yaml

get\_gpo.yaml

find\_gpo\_computer\_admin.yaml

get\_adidns\_zone.yaml

user\_hunter.yaml

share\_finder.yaml

set\_ad\_object.yaml

process\_hunter.yaml

get\_user.yaml

map\_domain\_trust.yaml

get\_subnet\_ranges.yaml

get\_subnet\_ranges.py

get\_subnet.yaml

get\_session.yaml

get\_rdp\_session.yaml

get\_object\_acl.yaml

get\_loggedon.yaml

get\_localgroup.yaml

get\_group.yaml

get\_kerberos\_service\_ticket.yaml

get\_sql\_instance\_domain.yaml

get\_group\_member.yaml

arpscan.yaml

get\_spn.yaml

bloodhound.yaml

bloodhound3.yaml

get\_site.yaml

get\_ou.yaml

Out-EncodedWhitespaceCommand.ps1

Out-ObfuscatedStringCommand.ps1

Out-ObfuscatedTokenCommand.ps1

Out-PowerShellLauncher.ps1

Out-SecureStringCommand.ps1

reflective\_inject.py