S3cur3Th1sSh1t / Pentest-Tools

No description, website, or topics provided.

22 commits **1** branch **0** releases **2** contributors

Branch: **master** New pull request Find file Clone or download

S3cur3Th1sSh1t Update README.md Latest commit `20bf7ad` 2 days ago

README.md Update README.md 2 days ago

README.md

Pentest-Tools

- General usefull Powershell Scripts
- AMSI Bypass restriction Bypass
- Lateral Movement / POST Exploitation / Pivot
- Backdoor finder
- Persistence on windows
- Web Application Pentest
- Framework Discovery
- Framework Scanner / Exploitation
- Web Vulnerability Scanner / Burp Plugins
- Network- / Service-level Vulnerability Scanner
- Crawler
- Web Exploitation Tools
- Windows Privilege Escalation / Audit
- T3 Enumeration
- Linux Privilege Escalation / Audit
- Credential harvesting Windows Specific
- Credential harvesting Linux Specific
- Data Exfiltration - DNS/ICMP/Wifi Exfiltration
- Git Specific
- Reverse Engineering / decompiler
- Forensics

- Network Attacks
- Specific MITM service Exploitation
- Sniffing / Evaluation / Filtering
- Scanner / Exploitation-Frameworks / Automation
- Default Credential Scanner
- Payload Generation / AV-Evasion / Malware Creation
- Domain Finding / Subdomain Enumeration
- Scanner network level
- Email Gathering
- Domain Auth + Exploitation
- Network service - Login Brute Force + Wordlist attacks
- Command & Control Frameworks
- Wifi Tools
- Raspberri PI Exploitation
- Social Engineering
- Wordlists / Wordlist generators
- Obfuscation
- Source Code Analysis
- No category yet
- Industrial Control Systems
- NAC bypass
- JMX Exploitation

And many more. I created this repo to have an overview over my starred repos. I was not able to filter in categories before. Feel free to use it for yourself.

Windows Active Directory Pentest

General usefull Powershell Scripts

https://github.com/S3cur3Th1sSh1t/WinPwn - 😎

https://github.com/dafthack/MailSniper

https://github.com/putterpanda/mimikittenz

https://github.com/dafthack/DomainPasswordSpray

https://github.com/mdavis332/DomainPasswordSpray - same but kerberos auth for more stealth and lockout-sleep

https://github.com/jnqpblc/SharpSpray - domainpasswordspray executable with lockout-sleep

https://github.com/Arvanaghi/SessionGopher

https://github.com/samratashok/nishang

https://github.com/PowerShellMafia/PowerSploit

https://github.com/fdiskyou/PowerOPS

https://github.com/giMini/PowerMemory

https://github.com/Kevin-Robertson/Inveigh

https://github.com/MichaelGrafnetter/DSInternals

https://github.com/PowerShellEmpire/PowerTools

https://github.com/FuzzySecurity/PowerShell-Suite

https://github.com/hlldz/Invoke-Phant0m

https://github.com/leoloobeek/LAPSToolkit

https://github.com/sense-of-security/ADRecon

https://github.com/Arno0x/PowerShellScripts

https://github.com/S3cur3Th1sSh1t/Grouper

https://github.com/l0ss/Grouper2

https://github.com/NetSPI/PowerShell

https://github.com/NetSPI/PowerUpSQL

https://github.com/GhostPack - Various Powersploit Tasks in C#

https://github.com/Kevin-Robertson/Powermad - Adidns Attacks

AMSI Bypass restriction Bypass

https://github.com/S3cur3Th1sSh1t/Amsi-Bypass-Powershell

https://github.com/p3nt4/PowerShdll

https://github.com/jaredhaight/PSAttack

https://github.com/Cn33liz/p0wnedShell

https://github.com/cobbr/InsecurePowerShell

https://github.com/Mr-Un1k0d3r/PowerLessShell

https://github.com/bitsadmin/nopowershell C# Powershell

https://github.com/OmerYa/Invisi-Shell

https://github.com/Hackplayers/Salsa-tools - Salsa Tools - ShellReverse TCP/UDP/ICMP/DNS/SSL/BINDTCP and AV bypass, AMSI patched

https://github.com/padovah4ck/PSByPassCLM - Constrained language mode bypass

https://github.com/rasta-mouse/AmsiScanBufferBypass

https://github.com/itm4n/VBA-RunPE - Applocker Bypass

Backdoor finder

https://github.com/linuz/Sticky-Keys-Slayer

https://github.com/ztgrace/sticky_keys_hunter

https://github.com/countercept/doublepulsar-detection-script

Lateral Movement , POST Exploitation , Pivot

https://github.com/fdiskyou/hunter

https://github.com/byt3bl33d3r/CrackMapExec

https://github.com/nccgroup/WMIcmd

https://github.com/byt3bl33d3r/DeathStar - Automate Getting Dom-Adm

https://github.com/BloodHoundAD/BloodHound

https://github.com/cyberark/ACLight

https://github.com/canix1/ADACLScanner

https://github.com/fox-it/Invoke-ACLPwn

https://github.com/0x36/VPNPivot

https://github.com/securesocketfunneling/ssf

https://github.com/p3nt4/Invoke-SocksProxy

https://github.com/sensepost/reGeorg - Webshell tunnel over socks proxy - pentesters dream

https://github.com/SpiderLabs/portia - automated lateral movement

https://github.com/Screetsec/Vegile - backdoor / rootkit

https://github.com/DanMcInerney/icebreaker - automation for various mitm attacks + vulns

https://github.com/MooseDojo/apt2 - automated penetration toolkit

https://github.com/hdm/nextnet - Netbios Network interface Enumeration (discovery of dual homed hosts)

https://github.com/nettitude/Invoke-PowerThIEf - Automatically scan any windows or tabs for login forms and then record what gets posted. A notification will appear when some have arrived.

https://github.com/trustedsec/egressbuster - check for internet access over open ports / egress filtering

https://github.com/emilyanncr/Windows-Post-Exploitation

https://github.com/vincentcox/bypass-firewalls-by-DNS-history

https://github.com/mubix/post-exploitation

https://github.com/ThunderGunExpress/BADministration - McAfee Epo or Solarwinds post exploitation

https://github.com/Hackplayers/evil-winrm

https://github.com/mwrlabs/SharpGPOAbuse

https://github.com/RedTeamOperations/PivotSuite

https://github.com/dirkjanm/krbrelayx - unconstrained delegation, printer bug (MS-RPRN) exploitation, Remote ADIDNS attacks

Persistence on windows

https://github.com/fireeye/SharPersist

Web Application Pentest

Framework Discovery

https://github.com/Tuhinshubhra/CMSeeK

https://github.com/Dionach/CMSmap - Wordpress, Joomla, Drupal Scanner

https://github.com/wpscanteam/wpscan

https://github.com/Ekultek/WhatWaf

Framework Scanner / Exploitation

https://github.com/wpscanteam/wpscan - wordpress

https://github.com/n00py/WPForce

https://github.com/m4ll0k/WPSeku https://github.com/swisskyrepo/Wordpresscan

https://github.com/rastating/wordpress-exploit-framework

https://github.com/coldfusion39/domi-owned - lotus domino

https://github.com/droope/droopescan - Drupal

https://github.com/whoot/Typo-Enumerator - Typo3

https://github.com/rezasp/joomscan - Joomla

Web Vulnerability Scanner / Burp Plugins

https://github.com/m4ll0k/WAScan - all in one scanner

https://github.com/s0md3v/XSStrike - XSS discovery

https://github.com/federicodotta/Java-Deserialization-Scanner

https://github.com/d3vilbug/HackBar

https://github.com/gyoisamurai/GyoiThon

https://github.com/snoopysecurity/awesome-burp-extensions

Network- / Service-level Vulnerability Scanner

https://github.com/scipag/vulscan

https://github.com/zdresearch/OWASP-Nettacker

File / Directory / Parameter discovery

https://github.com/OJ/gobuster

https://github.com/nccgroup/dirble

https://github.com/maK-/parameth

https://github.com/s0md3v/Arjun - 💗

https://github.com/Cillian-Collins/dirscraper - Directory lookup from Javascript files

https://github.com/hannob/snallygaster

https://github.com/maurosoria/dirsearch

https://github.com/s0md3v/Breacher - Admin Panel Finder

https://github.com/mazen160/server-status_PWN

Crawler

https://github.com/s0md3v/Photon - 💗

https://github.com/kgretzky/dcrawl

Web Exploitation Tools

https://github.com/OsandaMalith/LFiFreak - lfi

https://github.com/enjoiz/XXEinjector - xxe

https://github.com/tennc/webshell - shellz

https://github.com/flozz/p0wny-shell

https://github.com/epinna/tplmap - ssti

https://github.com/orf/xcat - xpath injection

https://github.com/almandin/fuxploider - File Uploads

https://github.com/nccgroup/freddy - deserialization

https://github.com/irsdl/IIS-ShortName-Scanner - IIS Short Filename Vuln. exploitation

https://github.com/frohoff/ysoserial - Deserialize Java Exploitation

https://github.com/pwntester/ysoserial.net - Deserialize .NET Exploitation

https://github.com/internetwache/GitTools - Exploit .git Folder Existence

https://github.com/cujanovic/SSRF-Testing - SSRF Tutorials

https://github.com/ambionics/phpggc - PHP Unserialize Payload generator

https://github.com/BuffaloWill/oxml_xxe - Malicious Office XXE payload generator

https://github.com/tijme/angularjs-csti-scanner - Angularjs Csti Scanner

https://github.com/0xacb/viewgen - Deserialize .NET Viewstates

https://github.com/Illuminopi/RCEvil.NET - Deserialize .NET Viewstates

REST API Audit

https://github.com/flipkart-incubator/Astra

Windows Privilege Escalation / Audit

https://github.com/AlessandroZ/BeRoot

https://github.com/rasta-mouse/Sherlock

https://github.com/hfiref0x/UACME

https://github.com/rootm0s/WinPwnage - UAC

https://github.com/abatchy17/WindowsExploits

https://github.com/dafthack/HostRecon

https://github.com/sensepost/rattler

https://github.com/WindowsExploits/Exploits

https://github.com/hatRiot/token-priv

https://github.com/Cybereason/siofra

https://github.com/0xbadjuju/Tokenvator

https://github.com/MojtabaTajik/Robber

https://github.com/411Hall/JAWS

https://github.com/GhostPack/SharpUp

https://github.com/GhostPack/Seatbelt

https://github.com/A-mIn3/WINspect

https://github.com/hausec/ADAPE-Script

https://github.com/SecWiki/windows-kernel-exploits

https://github.com/bitsadmin/wesng

https://github.com/rasta-mouse/Watson

https://github.com/itm4n/UsoDllLoader - load malicious dlls from system32

T3 Enumeration

https://github.com/quentinhardy/jndiat

Linux Privilege Escalation / Audit

https://github.com/mzet-/linux-exploit-suggester

https://github.com/rebootuser/LinEnum

https://github.com/diego-treitos/linux-smart-enumeration

https://github.com/CISOfy/lynis

https://github.com/AlessandroZ/BeRoot

https://github.com/future-architect/vuls

https://github.com/ngalongc/AutoLocalPrivilegeEscalation

https://github.com/b3rito/yodo

https://github.com/belane/linux-soft-exploit-suggester - lookup vulnerable installed software

https://github.com/sevagas/swap_digger

https://github.com/NullArray/RootHelper

https://github.com/NullArray/MIDA-Multitool

https://github.com/initstring/dirty_sock

https://github.com/jondonas/linux-exploit-suggester-2

https://github.com/sosdave/KeyTabExtract

https://github.com/DominicBreuker/pspy

https://github.com/itsKindred/modDetective

https://github.com/nongiach/sudo_inject

Exfiltration

Credential harvesting Windows Specific

https://github.com/gentilkiwi/mimikatz

https://github.com/GhostPack/SafetyKatz

https://github.com/GhostPack/Rubeus

https://github.com/Arvanaghi/SessionGopher

https://github.com/peewpw/Invoke-WCMDump

https://github.com/tiagorlampert/sAINT

https://github.com/AlessandroZ/LaZagneForensic - remote lazagne

https://github.com/eladshamir/Internal-Monologue

https://github.com/djhohnstein/SharpWeb - Browser Creds gathering

https://github.com/mwrlabs/SharpClipHistory - ClipHistory feature get the last 25 copy paste actions

https://github.com/outflanknl/Dumpert - dump lsass using direct system calls and API unhooking

Credential harvesting Linux Specific

https://github.com/huntergregal/mimipenguin

https://github.com/n1nj4sec/mimipy

https://github.com/dirtycow/dirtycow.github.io

https://github.com/mthbernardes/sshLooterC - SSH Credential loot

https://github.com/blendin/3snake - SSH / Sudo / SU Credential loot

https://github.com/0xmitsurugi/gimmecredz

Data Exfiltration - DNS/ICMP/Wifi Exfiltration

https://github.com/FortyNorthSecurity/Egress-Assess

https://github.com/p3nt4/Invoke-TmpDavFS

https://github.com/DhavalKapil/icmptunnel

https://github.com/iagox86/dnscat2

https://github.com/Arno0x/DNSExfiltrator

https://github.com/spieglt/FlyingCarpet - Wifi Exfiltration

https://github.com/SECFORCE/Tunna - Tunna is a set of tools which will wrap and tunnel any TCP communication over HTTP

Git Specific

https://github.com/dxa4481/truffleHog

https://github.com/zricethezav/gitleaks

Windows / Linux

https://github.com/AlessandroZ/LaZagne

https://github.com/Dionach/PassHunt

https://github.com/vulmon/Vulmap

Reverse Engineering / decompiler

https://github.com/mattifestation/PowerShellArsenal

https://github.com/0xd4d/dnSpy - .NET Disassembler

https://github.com/NationalSecurityAgency/ghidra

https://github.com/icsharpcode/ILSpy

Forensics

https://github.com/Invoke-IR/PowerForensics

https://github.com/Neo23x0/Loki

https://github.com/gfoss/PSRecon

Network Attacks

https://github.com/bettercap/bettercap - 💗

https://github.com/SpiderLabs/Responder

https://github.com/lgandx/Responder - more up to date

https://github.com/evilsocket/bettercap - Deprecated but still good

https://github.com/r00t-3xp10it/morpheus

https://github.com/fox-it/mitm6

https://github.com/DanMcInerney/LANs.py

Specific MITM service Exploitation

https://github.com/jtesta/ssh-mitm - SSH

https://github.com/pimps/wsuxploit - WSUS

https://github.com/SySS-Research/Seth - RDP

https://github.com/infobyte/evilgrade - Fake Updates for various Software

https://github.com/samdenty/injectify - web application live recording, keystroke logger

https://github.com/skorov/ridrelay - User Enumeration with SMB Relay Attacks

https://github.com/Kevin-Robertson/Invoke-TheHash

Sniffing / Evaluation / Filtering

https://github.com/DanMcInerney/net-creds

https://github.com/lgandx/PCredz

https://github.com/Srinivas11789/PcapXray

Scanner / Exploitation-Frameworks / Automation

https://github.com/threat9/routersploit

https://github.com/nccgroup/autopwn

https://github.com/1N3/Sn1per

https://github.com/byt3bl33d3r/CrackMapExec

https://github.com/Cn33liz/p0wnedShell

https://github.com/archerysec/archerysec

https://github.com/vulnersCom/nmap-vulners

https://github.com/m4ll0k/AutoNSE - automate nmap with scripting capabilities

https://github.com/v3n0m-Scanner/V3n0M-Scanner

https://github.com/zdresearch/OWASP-Nettacker

Default Credential Scanner

https://github.com/ztgrace/changeme

https://github.com/FortyNorthSecurity/EyeWitness

Default Credential Lookup

https://github.com/ViralManiar/Passhunt

Payload Generation / AV-Evasion / Malware Creation

https://github.com/nccgroup/Winpayloads

https://github.com/Screetsec/TheFatRat

https://github.com/xillwillx/tricky.lnk

https://github.com/trustedsec/unicorn

https://github.com/z0noxz/powerstager

https://github.com/curi0usJack/luckystrike

https://github.com/enigma0x3/Generate-Macro

https://github.com/Cn33liz/JSMeter

https://github.com/Mr-Un1k0d3r/MaliciousMacroGenerator

https://github.com/Cn33liz/StarFighters

https://github.com/BorjaMerino/Pazuzu

https://github.com/mwrlabs/wePWNise

https://github.com/Mr-Un1k0d3r/UniByAv

https://github.com/govolution/avet

https://github.com/Pepitoh/VBad

https://github.com/mdsecactivebreach/CACTUSTORCH

https://github.com/D4Vinci/Dr0p1t-Framework

https://github.com/g0tmi1k/msfpc

https://github.com/bhdresh/CVE-2017-0199 - Office RCE POC

https://github.com/GreatSCT/GreatSCT

https://github.com/mthbernardes/rsg - reverse shell generator

https://github.com/sevagas/macro_pack

https://github.com/mdsecactivebreach/SharpShooter

https://github.com/hlldz/SpookFlare

https://github.com/0xdeadbeefJERKY/Office-DDE-Payloads

https://github.com/paranoidninja/CarbonCopy - Sign an executable for AV-Evasion

https://github.com/peewpw/Invoke-PSImage

https://github.com/Arvanaghi/CheckPlease - Sandbox Evasion techniques

https://github.com/trustedsec/nps_payload

https://github.com/stormshadow07/HackTheWorld

https://github.com/r00t-3xp10it/FakeImageExploiter

Android

https://github.com/sensepost/kwetza

External Penetration Testing

Domain Finding / Subdomain Enumeration

https://github.com/aboul3la/Sublist3r

https://github.com/TheRook/subbrute

https://github.com/michenriksen/aquatone

https://github.com/darkoperator/dnsrecon

https://github.com/fwaeytens/dnsenum

https://github.com/s0md3v/Striker + Scanner

https://github.com/leebaird/discover

https://github.com/eldraco/domain_analyzer - more like an audit

https://github.com/caffix/amass - 💗

https://github.com/subfinder/subfinder

https://github.com/TypeError/domained

https://github.com/SilverPoision/Rock-ON

File Search / Metadata extraction

https://github.com/dafthack/PowerMeta

https://github.com/ElevenPaths/FOCA

Scanner

https://github.com/vesche/scanless

https://github.com/1N3/Sn1per

https://github.com/DanMcInerney/pentest-machine

Email Gathering

https://github.com/leapsecurity/InSpy

https://github.com/dchrastil/ScrapedIn

https://github.com/SimplySecurity/SimplyEmail

https://github.com/clr2of8/GatherContacts

https://github.com/s0md3v/Zen - Find Emails of Github Users

https://github.com/m8r0wn/CrossLinked

https://github.com/m4ll0k/Infoga

Domain Auth + Exploitation

https://github.com/nyxgeek/o365recon

https://github.com/True-Demon/raindance - office 365 recon

https://github.com/dafthack/MailSniper

https://github.com/sensepost/ruler

https://github.com/Greenwolf/Spray - lockout Time integrated

https://github.com/sensepost/SPartan - Sharepoint Fingerprint + Exploitation

https://github.com/nyxgeek/lyncsmash - Lync Credential Finder

https://github.com/byt3bl33d3r/SprayingToolkit - Scripts to make password spraying attacks against Lync/S4B & OWA a lot quicker, less painful and more efficient

https://github.com/mdsecresearch/LyncSniper - Lync Credential Finder

Specific Service Scanning / Exploitation

Login Brute Force + Wordlist attacks

https://github.com/galkan/crowbar - Brute force non hydra compliant services - RDP, VNC, OpenVPN

https://github.com/1N3/BruteX - Brute Force various services

https://github.com/x90skysn3k/brutespray - 😎

https://github.com/lanjelot/patator

https://github.com/dafthack/RDPSpray - RDP Password Spray - No Event Logs

SNMP

https://github.com/hatlord/snmpwn

Open X11

https://github.com/sensepost/xrdp

Printers

https://github.com/RUB-NDS/PRET

MSSQL

https://github.com/quentinhardy/msdat

Oracle

https://github.com/quentinhardy/odat

IKE

https://github.com/SpiderLabs/ikeforce

SMB Null Session Exploitation

https://github.com/m8r0wn/nullinux

Intel AMT Exploitation

https://github.com/Coalfire-Research/DeathMetal

SAP Exploitation

https://github.com/comaeio/OPCDE

https://github.com/gelim/sap_ms

https://github.com/chipik/SAP_GW_RCE_exploit

General Recon

https://github.com/FortyNorthSecurity/EyeWitness

Command & Control Frameworks

https://github.com/n1nj4sec/pupy

https://github.com/nettitude/PoshC2

https://github.com/FortyNorthSecurity/WMImplant

https://github.com/quasar/QuasarRAT

https://github.com/EmpireProject/Empire

https://github.com/zerosum0x0/koadic

https://github.com/Mr-Un1k0d3r/ThunderShell

https://github.com/Ne0nd0g/merlin

https://github.com/Arno0x/WebDavC2

https://github.com/malwaredllc/byob

https://github.com/byt3bl33d3r/SILENTTRINITY

https://github.com/Arno0x/WSC2

https://github.com/BC-SECURITY/Empire - Empire with embedded AMSI-Bypass

https://github.com/cobbr/Covenant

https://github.com/BishopFox/sliver

Android

https://github.com/AhMyth/AhMyth-Android-RAT

Linux MacOSX Specific

https://github.com/neoneggplant/EggShell

Wifi Tools

https://github.com/wifiphisher/wifiphisher

https://github.com/P0cL4bs/WiFi-Pumpkin

https://github.com/s0lst1c3/eaphammer

https://github.com/h0nus/RogueSploit

https://github.com/Tylous/SniffAir

https://github.com/FluxionNetwork/fluxion

https://github.com/derv82/wifite2

https://github.com/ICSec/airpwn-ng

https://github.com/xdavidhu/mitmAP

https://github.com/ZerBea/hcxdumptool

Android / Nethunter

https://github.com/faizann24/wifi-bruteforcer-fsecurify

https://github.com/chrisk44/Hijacker

Raspberri PI Exploitation

https://github.com/secgroundzero/warberry

https://github.com/samyk/poisontap

https://github.com/mame82/P4wnP1

https://github.com/mame82/P4wnP1_aloa

https://github.com/pi-hole/pi-hole

Physical Security / HID/ETH Emulator

https://github.com/carmaa/inception - PCI-based DMA

https://github.com/samratashok/Kautilya

https://github.com/ufrisk/pcileech - PCI based DMA

https://github.com/Screetsec/Brutal - Teensy Payloads

https://github.com/insecurityofthings/jackit

https://github.com/BastilleResearch/mousejack

Social Engineering

https://github.com/kgretzky/evilginx

https://github.com/threatexpress/domainhunter

https://github.com/netevert/dnsmorph - lookup valid phishing-Domains

https://github.com/elceef/dnstwist - lookup valid phishing-Domains

https://github.com/quickbreach/SMBetray - Change SMB Files on the fly

https://github.com/SteveLTN/https-portal

https://github.com/ryhanson/phishery

https://github.com/Dviros/CredsLeaker

Defender Guides / Tools

https://github.com/PaulSec/awesome-windows-domain-hardening

https://github.com/Invoke-IR/Uproot

https://github.com/danielbohannon/Revoke-Obfuscation

https://github.com/0xd4d/de4dot - .NET Revoke-Obfuscation

https://github.com/securitywithoutborders/hardentools

https://github.com/x0rz/phishing_catcher

https://github.com/Ben0xA/PowerShellDefense

https://github.com/emposha/PHP-Shell-Detector

https://github.com/LordNoteworthy/al-khaser

https://github.com/Security-Onion-Solutions/security-onion - ids

https://github.com/ptresearch/AttackDetection

https://github.com/MHaggis/hunt-detect-prevent

https://github.com/JPCERTCC/LogonTracer - Investigate malicious Windows logon by visualizing and analyzing Windows event log

https://github.com/lithnet/ad-password-protection - AD Passwort Blacklisting

https://github.com/R3MRUM/PSDecode - Powershell DE-Obfuscation

https://github.com/matterpreter/DefenderCheck

Wordlists / Wordlist generators

https://github.com/danielmiessler/SecLists

https://github.com/berzerk0/Probable-Wordlists

https://github.com/govolution/betterdefaultpasslist

https://github.com/insidetrust/statistically-likely-usernames

https://github.com/LandGrey/pydictor

https://github.com/sc0tfree/mentalist

https://github.com/skahwah/wordsmith

https://github.com/1N3/IntruderPayloads

https://github.com/fuzzdb-project/fuzzdb

https://github.com/Bo0oM/fuzz.txt

https://github.com/laconicwolf/Password-Scripts

Obfuscation

https://github.com/xoreaxeaxeax/movfuscator

https://github.com/danielbohannon/Invoke-DOSfuscation

https://github.com/unixpickle/gobfuscate - GO Obfuscator

https://github.com/javascript-obfuscator/javascript-obfuscator - Javascript Obfuscator

https://github.com/danielbohannon/Invoke-Obfuscation - Powershell Obfuscator

Source Code / Binary Analysis

Binary Analysis

https://github.com/avast/retdec

https://github.com/MobSF/Mobile-Security-Framework-MobSF

Source Code Analysis

https://github.com/mre/awesome-static-analysis

https://github.com/eslint/eslint - Javascript

https://github.com/dpnishant/jsprime - Javascript

https://github.com/phpstan/phpstan - PHP

No category yet

https://github.com/pentestmonkey/gateway-finder

https://github.com/Cybellum/DoubleAgent

https://github.com/ytisf/theZoo

https://github.com/kbandla/APTnotes

https://github.com/WindowsLies/BlockWindows

https://github.com/secrary/InjectProc

https://github.com/AlsidOfficial/WSUSpendu

https://github.com/SigPloiter/SigPloit

https://github.com/virajkulkarni14/WebDeveloperSecurityChecklist

https://github.com/PowerShell/PowerShell

https://github.com/landhb/HideProcess

https://github.com/meliht/Mr.SIP

https://github.com/XiphosResearch/exploits

https://github.com/worawit/MS17-010

https://github.com/DiabloHorn/yara4pentesters

https://github.com/D4Vinci/Cr3dOv3r

https://github.com/a2u/CVE-2018-7600 - Drupal Exploit

https://github.com/joxeankoret/CVE-2017-7494 - SAMBA Exploit

https://github.com/D4Vinci/One-Lin3r - Reverse Shell Oneliner / Payload Generation

https://github.com/0x00-0x00/ShellPop - Reverse/Bind Shell Generator

https://github.com/Acceis/crypto_identifier

https://github.com/sensepost/UserEnum - check if a user is valid in a domain

https://github.com/LOLBAS-Project/LOLBAS - Living of the Land Binaries

https://github.com/peewpw/Invoke-BSOD - Windows Denial of Service Exploit

https://github.com/mtivadar/windows10_ntfs_crash_dos - Windows Denial of Service Exploit

https://github.com/deepzec/Bad-Pdf PDF Steal NTLMv2 Hash Exploit - CVE-2018-4993

https://github.com/SecureAuthCorp/impacket - 💥 🔥 💥

https://github.com/blacknbunny/libSSH-Authentication-Bypass - LibSSH Authentication Bypass vuln.

https://github.com/vletoux/pingcastle - AD-Audit

https://github.com/OneLogicalMyth/zeroday-powershell - windows Privesc Exploit

https://github.com/smicallef/spiderfoot - OSINT

https://github.com/ShawnDEvans/smbmap

https://github.com/Coalfire-Research/java-deserialization-exploits - Deserialisation Exploits

https://github.com/quentinhardy/jndiat - WEblogic Server Tests

https://github.com/RhinoSecurityLabs/GCPBucketBrute - S3 bucket tester

https://github.com/NetSPI/MicroBurst - AWS Security Framework

https://github.com/khast3x/h8mail

https://github.com/dirkjanm/adidnsdump - Zone transfer like for internal assessment

https://github.com/gquere/pwn_jenkins

https://github.com/JavelinNetworks/IR-Tools - Get-ShellContent.ps1 get the typed content for all open shells

https://github.com/taviso/ctftool - windows CTF Exploitation

https://github.com/jedisct1/dsvpn

https://github.com/GoSecure/dtd-finder

https://github.com/tyranid/DotNetToJScript

https://github.com/cfreal/exploits - Apache Privilege Escalation

Anonymous / Tor Projects

https://github.com/realgam3/pymultitor

https://github.com/Und3rf10w/kali-anonsurf

https://github.com/GouveaHeitor/nipe

https://github.com/cryptolok/GhostInTheNet

https://github.com/DanMcInerney/elite-proxy-finder

Exploit Search

https://github.com/vulnersCom/getsploit

https://github.com/1N3/Findsploit

Industrial Control Systems

https://github.com/dark-lbp/isf

https://github.com/klsecservices/s7scan

https://github.com/w3h/isf

Network access control bypass

https://github.com/scipag/nac_bypass

JMX Exploitation

https://github.com/mogwailabs/mjet

https://github.com/siberas/sjet

Red Team infrastructure setup

https://github.com/obscuritylabs/RAI

Redis Exploitation

https://github.com/Ridter/redis-rce

SSRF Exploitation

https://github.com/swisskyrepo/SSRFmap

LFI exploitation

https://github.com/mzfr/liffy

MondoDB Redis Couchdb Exploitation

https://github.com/torque59/Nosql-Exploitation-Framework

Elasticsearch / Kibana Exploitation

https://github.com/0xbug/Biu-framework

RMI attacks

https://github.com/NickstaDB/BaRMIe

Cloud attack tools

https://github.com/mdsecactivebreach/o365-attack-toolkit

Bluetooth / low energy

https://github.com/ojasookert/CVE-2017-0785

https://github.com/evilsocket/bleah

https://github.com/virtualabs/btlejack

Wireless / Radio Exploitation

https://github.com/mame82/LOGITacker

APT / Malware Emulation / Defense Check

https://github.com/TryCatchHCF/DumpsterFire

https://github.com/NextronSystems/APTSimulator

https://github.com/redhuntlabs/RedHunt-OS

https://github.com/guardicore/monkey

Hash Crack / Lookup

https://github.com/k4m4/dcipher-cli

https://github.com/s0md3v/Hash-Buster

https://github.com/initstring/passphrase-wordlist

OSCP Lists / tools / help

https://github.com/sailay1996/expl-bin

https://github.com/CyDefUnicorn/OSCP-Archives

ASPX Webshells

https://github.com/antonioCoco/SharPyShell

PHP Webshells

https://github.com/flozz/p0wny-shell

Other Tool-Lists / Cheat Sheets

https://github.com/Hack-with-Github/Awesome-Hacking

https://github.com/enaqx/awesome-pentest

https://github.com/HarmJ0y/CheatSheets

https://github.com/vysecurity/RedTips

https://github.com/toolswatch/blackhat-arsenal-tools

https://github.com/jivoi/awesome-osint

https://github.com/qazbnm456/awesome-cve-poc

https://github.com/swisskyrepo/PayloadsAllTheThings

https://github.com/dsasmblr/hacking-online-games

https://github.com/meirwah/awesome-incident-response

https://github.com/carpedm20/awesome-hacking

https://github.com/rshipp/awesome-malware-analysis

https://github.com/thibmaek/awesome-raspberry-pi

https://github.com/vitalysim/Awesome-Hacking-Resources

https://github.com/mre/awesome-static-analysis

https://github.com/coreb1t/awesome-pentest-cheat-sheets

https://github.com/infosecn1nja/Red-Teaming-Toolkit

https://github.com/rmusser01/Infosec_Reference

https://github.com/trimstray/the-book-of-secret-knowledge

https://github.com/qazbnm456/awesome-web-security

https://github.com/chryzsh/awesome-windows-security

https://github.com/blaCCkHatHacEEkr/PENTESTING-BIBLE

https://github.com/We5ter/Scanners-Box

https://github.com/smgorelik/Windows-RCE-exploits