渗透技能树之利器 v1

LanT34m 汇编整理 | 20170528 更新

[Windows]
PowerShell: PowerSploit, Empire, Nishang, PowerShell-Suite
Mimikatz
https://github.com/secretsquirrel/the-backdoor-factory
https://github.com/secretsquirrel/BDFProxy

Mimikatz in JS
https://gist.github.com/subTee/b30e0bcc7645c790fcd993cfd0ad622f

CrackMapExec
A swiss army knife for pentesting Windows/Active Directory environments
https://github.com/byt3bl33d3r/CrackMapExec

WMImplant
https://github.com/ChrisTruncer/WMImplant
This is a PowerShell based tool that is designed to act like a RAT.

PoshC2
https://github.com/nettitude/PoshC2
Powershell C2 Server and Implants

pemcracker
https://github.com/bwall/pemcracker
Tool to crack encrypted PEM files

BeRoot
https://github.com/AlessandroZ/BeRoot
Windows Privilege Escalation Tool

RedSnarf
https://github.com/nccgroup/redsnarf
RedSnarf is a pen-testing / red-teaming tool for Windows environments.

[Linux]
mimipenguin
https://github.com/huntergregal/mimipenguin
A tool to dump the login password from the current linux user

Auto-Root-Exploit
https://github.com/nilotpalbiswas/Auto-Root-Exploit

[Tunnel]
nc
socat
http://tgcd.sourceforge.net/

cryptcat
https://sourceforge.net/projects/cryptcat/
towfish加密的nc版本

proxychains

DNSCat2
https://github.com/iagox86/dnscat2
Create an encrypted command-and-control (C&C) channel over the DNS protocol

Kaola
https://github.com/mrschyte/pentestkoala
A patched version of the dropbear SSH server

powercat
https://github.com/besimorhino/powercat
Powershell Netcat

ABPTTS
https://n0where.net/tunnel-tcp-traffic-abptts/
Tunnel TCP Traffic Over an HTTP/HTTPS Connection

[JavaScript]
XSS'OR
http://xssor.io/
Hack with JavaScript

BeEF

OWASP Xenotix XSS Exploit Framework
https://xenotix.in/

LocalNetworkScanner
https://github.com/SkyLined/LocalNetworkScanner

[Browser]
Tamper Chrome
https://github.com/google/tamperchrome
Chrome extension to modify HTTP on the fly

[OSINT]
https://github.com/upgoingstar/datasploit/
http://www.spiderfoot.net/
https://github.com/techgaun/github-dorks
https://bitbucket.org/LaNMaSteR53/recon-ng
https://github.com/ilektrojohn/creepy
https://github.com/laramies/theHarvester

Infoga
https://github.com/m4ll0k/infoga
Infoga is a tool for gathering e-mail accounts information from different public sources (search engines, pgp key servers)

vFeed
https://vfeed.io

GoogleHack Dorks
https://gist.github.com/cmartinbaughman/5877945

Exploit Database
https://github.com/offensive-security/exploit-database
searchsploit

[Domain]
DNSRecon
https://github.com/darkoperator/dnsrecon

[Dir]
https://github.com/maurosoria/dirsearch

[Social-Engineer]
https://github.com/trustedsec/social-engineer-toolkit
https://github.com/antisnatchor/phishlulz

dnstwist
https://github.com/elceef/dnstwist
可以生成及检测一堆相似钓鱼域名

[Pentest]
Cobalt Strike

https://github.com/infobyte/faraday
http://www.acunetix.com/vulnerability-scanner/manual-tools/

Pentest-Scripts
https://github.com/bitvijays/Pentest-Scripts
Github for the scripts utilised during Penetration test - https://bitvijays.github.io

PloitKit
https://github.com/rajeshmajumdar/PloitKit
The Hacker's ToolBox

[Exploit]
Exploit Pack
http://exploitpack.com/
看去很牛的攻击系统，免费版可以体验体验，收费版37000+ Exploits+未知0day

Metasploit

ShellSploit
https://github.com/b3mb4m/shellsploit-framework
New Generation Exploit Development Kit

EAST
https://github.com/C0reL0ader/EaST
Exploits And Security Tools

[Virus]
Dr0p1t-Framework
https://github.com/D4Vinci/Dr0p1t-Framework
A Framework That Creates An Advanced FUD Dropper With Some Tricks

Veil
https://github.com/Veil-Framework/Veil
Veil is a tool designed to generate metasploit payloads that bypass common anti-virus solutions.

Stitch
https://github.com/nathanlopez/Stitch
Python Remote Administration Tool (RAT)

Koala
https://github.com/mrschyte/pentestkoala
Modified dropbear server which acts as a client and allows authless login

InjectPE
http://www.kitploit.com/2017/04/infectpe-inject-custom-code-into-pe-file.html

BrainDamage
https://github.com/mehulj94/BrainDamage
A fully featured backdoor that uses Telegram as a C&C server

strutszeiro
https://github.com/mthbernardes/strutszeiro
Telegram Bot to manage botnets created with struts vulnerability(CVE-2017-5638)

FakeImageExploiter
https://github.com/r00t-3xp10it/FakeImageExploiter
extensions to exploit targets

TRSH
https://github.com/fnzv/trsh
Telegram Remote-Shell is a python script that allows to comunicate to your Linux server via Telegram API (with bots).

PowerStager
https://github.com/z0noxz/powerstager
This script creates an executable stager that downloads a selected powershell payload, loads it into memory and executes it using obfuscated EC methods.

Cypher
https://github.com/NullArray/Cypher
Cypher is a proof of concept ransomware which implements the PyCrpto module and uses gmail(Currently) as a simple command and control server.

Pyekaboo
https://github.com/SafeBreach-Labs/pyekaboo
Pyekaboo is a proof-of-concept program that is able to to hijack/hook/proxy Python module(s) thanks to $PYTHONPATH variable. It's like "DLL Search Order Hijacking" for Python.

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

[Proxy]
Burp Suite
Fiddler

[Java]
https://github.com/frohoff/ysoserial

Strut2Shell
https://github.com/s1kr10s/Struts2Shell

[CTF]
https://github.com/Gallopsled/pwntools

[DDoS]
https://github.com/NewEraCracker/LOIC/
http://metacortexsecurity.com/tools/anon/LOIC/LOICv1.html

[IoT]
https://github.com/reverse-shell/routersploit
https://github.com/rapid7/IoTSeeker
http://www.routerpwn.com/

[SSL]
https://github.com/nabla-c0d3/sslyze
https://github.com/alexoslabs/HTTPSScan

[Web]
http://w3af.org/
https://github.com/urbanadventurer/whatweb
http://www.kitploit.com/2017/01/davscan-fingerprints-servers-finds.html

https://wpscan.org/
https://github.com/drego85/JoomlaScan
https://www.owasp.org/index.php/OWASP_VBScan_Project
https://github.com/droope/droopescan
https://github.com/anarcoder/google_explorer
https://github.com/mubix/shellshocker-pocs
https://github.com/tennc/webshell
OWASP ZAP

HatCloud
https://github.com/HatBashBR/HatCloud
Bypass CloudFlare with Ruby

Kadimus
https://github.com/P0cL4bs/Kadimus
A tool to check sites to LFI vulnerability and Exploit

[Brute-Force]
Hashcat
https://github.com/vanhauser-thc/thc-hydra

CUPP
https://github.com/Mebus/cupp
https://null-byte.wonderhowto.com/how-to/use-cupp-generate-password-lists-0162625/
Common User Passwords Profiler (CUPP)，可以生成用户习惯的密码字典

John the Ripper
Cain and Abel

https://null-byte.wonderhowto.com/how-to/hack-like-pro-crack-passwords-part-1-principles-technologies-0156136/

Cheetah
https://github.com/sunnyelf/cheetah
Cheetah is a dictionary-based brute force password webshell tool, running as fast as a cheetah hunt for prey.

[Fuzz]
Peach Fuzzer
http://www.peachfuzzer.com/

[Port]
ZMap+ZGrab
Masscan
Nmap

[Cyber]
IVRE

Leviathan
https://github.com/leviathan-framework/leviathan
Leviathan is a mass audit toolkit which has wide range service discovery, brute force, SQL injection detection and running custom exploit capabilities. It consists open source tools such masscan, ncrack, dsss and gives you the flexibility of using them with a combination.

ssh_scan
https://github.com/mozilla/ssh_scan

telnet-scanner
https://github.com/scu-igroup/telnet-scanner

[Search-Engineer]

Google
Shodan
ZoomEye
Censys
Bing

[Wi-Fi]
Fluxion
Wifite
Aircrack-ng

Wifiphisher
https://github.com/sophron/wifiphisher
很猥琐的钓鱼AP方式

[MITM]
Ettercap
cSploit
zANTI
MITMf
https://github.com/DanMcInerney/LANs.py
mitmproxy

Evilgrade
攻击升级过程，很猥琐很强大
https://github.com/infobyte/evilgrade/

Evilgnix
http://www.4hou.com/technology/4184.html
2FA Phishing

[DNS]
dns2proxy
可以灵活进行DNS中间人攻击
https://github.com/LeonardoNve/dns2proxy
http://www.darknet.org.uk/2017/01/dns2proxy-offensive-dns-server/

DNSChef
http://thesprawl.org/projects/dnschef/

https://github.com/mandatoryprogrammer/JudasDNS

rldns
https://packetstormsecurity.com/files/142054/rldns-mitm.tar.gz
DNS MITM

[Docker]
https://github.com/cr0hn/dockerscan

[Android]
Inspeckage
MobFS
Frida

MARA
https://github.com/xtiankisutsa/MARA_Framework
MARA is a Mobile Application Reverse engineering and Analysis Framework.

AndroL4b
https://github.com/sh4hin/Androl4b

AndroL4b is an android security virtual machine based on ubuntu-mate includes the collection of latest framework, tutorials and labs from different security geeks and researchers for reverse engineering and malware analysis.

[OS]
Kali Linux
Pentest Box

cgPwn
https://github.com/0xM3R/cgPwn
Cyber Grand Pwnage Box

[Defense]
https://github.com/triaquae/CrazyEye
https://github.com/FallibleInc/security-guide-for-developers
https://github.com/forter/security-101-for-saas-startups/blob/chinese/security.md
https://github.com/hannob/bashcheck
Lynis

PyT
https://github.com/python-security/pyt
Python Taint

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

No More Ransom
https://www.nomoreransom.org/

Cuckoo Sandbox
https://cuckoosandbox.org
Malware analysis System

GoAccess
https://www.cyberciti.biz/faq/how-to-install-goaccess-web-log-analyzer-with-nginx-on-linux-or-unix/

Dionaea
https://github.com/rep/dionaea
Low interaction honeypot.

[Hardware]
nRF24 Playset
https://github.com/SySS-Research/nrf24-playset
The nRF24 Playset is a collection of software tools for wireless input devices like keyboards, mice, and presenters based on Nordic Semiconductor nRF24 transceivers, e.g. nRF24LE1 and nRF24LU1+.

SySS Radio Hack Box
https://github.com/SySS-Research/radio-hackbox
The SySS Radio Hack Box is a proof-of-concept software tool to demonstrate the replay and keystroke injection vulnerabilities of the wireless keyboard Cherry B.Unlimited AES.

[Other]
Truehunter
https://github.com/adoreste/truehunter
Tool to detect TrueCrypt containers