[technical] Pen-testing resources

Red C0de Follow

Aug 12, 2018 · 22 min read

Sites/Blogs/Forums/Report Platform

- Multi-func sites
- https://www.t00ls.net/
- FreeBuf
- Security guest
- 91ri.org
- Vulnerability bank
- mottoin
- seebug
- sec-wiki

- Sec-News
- Cyber security focus
- Ranger safety net
- hi 0 x 0
- Safety circle Info
- Love sharp knife
- Principal Online
- https://www.hellboundhackers.org/
- https://www.hackerone.com/
- https://navisec.it/
- Linux safety net
- myhack58
- Red-black alliance
- Evil hex

- nullsecurity

Blogs

- The road to Principal
- Tencent Xuanwu Laboratory
- Tencent Xuanwu Lab Security Dynamic Push
- Kotowicz
- Night shadow binary security
- Twosecurity
- https://null-byte.wonderhowto.com/
- Ethan
- https://www.n0tr00t.com/
- https://paper.seebug.org/
- Some technology blogs

- https://github.com/evilcos/papers
- bestwing.me
- MDSec
- evi1m0 (Evil-say)
- hackfun.org
- xsec.io
- Cosine
- Zhihu
- Parting song leavesongs—PHITHON
- Dark thread
- noob.ninja
- riusksk
- hackdog
- Qimingyu

- drop
- bluescreenofjeff
- 04z.net
- Blackbird Safety Net
- Adma Web Security
- dhb133
- neeao
- pkav
- Loneliness is more reliable
- virink
- error
- 5alt
- Ghost’s Blog
- Changting Technology Column

- x2know
- seay
- wing
- sky
- Ha1g0
- SecuritySite
- Some interesting blogs
- pentest-bookmarks

Report Platform

- http://0day5.com/
- https://www.exploit-db.com/
- w0rms.com
- https://x.threatbook.cn

- The latest vulnerability—not safe
- Crown exploit codebase—0day,Exploit,Shellcode
- WooYun
- https://wooyun.shuimugan.com/
- http://www.milw0rm.com/

Forums

- Prophet Security Technology Community
- Watching snow
- 8th man
- Evil octal
- My love crack
- China UNIX
- ichunqiu BBS

- Hack Forums
- https://security.stackexchange.com/
- https://reverseengineering.stackexchange.com/
- https://crypto.stackexchange.com/

Mailing Lists

- http://seclists.org/bugtraq/
- http://seclists.org/oss-sec/
- http://seclists.org/fulldisclosure/

Tools—pentest approx

- Time
- BlackArch Linux
- Parrot Security OS

- BackBox—Based on Ubuntu
- Fedora Security Lab—Based on Fedora
- Pentoo—Based on Gentoo
- URIX OS—Based on openSUSE
- Wifislax—Based on Slackware
- docker_msf
- Vulhub

Some Docker-Compose files for vulnerabilities environment

- VulApps
- PHPPHP : PHP VM implementation written in PHP.

Tools—Encode/Decode

- XSS'OR
- evilcos/xssor

- XSSEE
- oschina tools
- chinaz tools

Tools—Crypto

- Frequency/subsitition/…
- Frequency Counter
- quipqiup
- Substitution Cipher—Encoding/Decoding
- The_Black_Chamber
- Visualized monogram-bigram-and-trigram-frequency-counts

Steganography

- stegdetect

hash

- Hash-Buster
- Hash (MD5, NTLM, LM, SHA) password online crack website list

MD5

- http://www.cmd5.com/
- MD5Decrypter(uk)
- Plain-Text
- Crackfoo -NNC
- Hashcrack
- Gdata
- MD5this
- MD5crack
- Hazelnut

- Joomlaaa
- Igrkio
- MD5decrypter
- Shell
- NetMD5crack
- XMD5
- TheKaine
- InsidePro
- MD5pass
- Generate
- AuthSecu
- MD5decryption
- Schwett
- Crackfor.me

- MD5-piece
- Drasen
- Gromweb
- MD5hood
- MD5.my-addr
- MD5online
- Macrosoftware
- Bokehman
- MD5-decrypter
- Thoran
- C0llision
- Rednoize
- web-security-services
- MD5-lookup

- CMD5
- Tmto
- Shalla
- Hash-Database
- Bokehman
- Benramsey
- Digitalsun
- Calculator
- StringFunction
- Toolz
- Fox21
- Gat3way
- Without
- Appspot

- HashCracking.ru
- Anqel
- Offensive-Security
- Altervista
- Xanadrel
- Beeeer
- Kinginfet
- AskCheck
- hash-cracker.com
- agilobable.pl
- MD5finder
- Wordd
- MD5Rainbow
- overclock

- plain-text.info (irc.Plain-Text.info #rainbowcrack—irc.rizon.net #rainbowcrack)
- md5.overclock.ch (irc.rizon.net # md5)
- c0llision.net (irc.after-all.org #md5crack—ircd.hopto.org #md5crack—ix.dal.net #md5crack)

NTLM

- MD5decrypter(uk)
- Plain-Text
- NiceNameCrew
- HashCrack
- Tmto
- Fox21
- LMCrack
- hash-cracker.com

LM

- Plain-Text
- NiceNameCrew
- HashCrack
- C0llision
- Tmto
- Fox21
- LMCrack
- Offensive-Security

SHA1

- MD5Decrypter(uk)
- Rednoize
- Web-Security-Services

- SHA1-Lookup
- CMD5
- Tmto
- Hash-Database
- Toolz
- Without
- HashCracking.ru
- AskCheck
- stringfunction
- hash-cracker.com

SHA 256–512

- Shalla
- Hash-Database

- AskCheck

MySQL

- HashCrack
- CMD5
- HashCracking.ru

WPA-PSK)

- MD5Decrypter(uk)
- WPA2Crack.com
- WPACracker
- Question-Defense

Tools—domain name / ip

- Ip check the domain name
- dns.aizhan.com
- Subdomain enumeration
- Classic subdomain blasting enumeration script
- Subdomain dictionary exhaustive
- Subdomain enumeration and map tag
- Online subdomain information collection tool
- Query subdomains based on DNS records
- Subdomain query script based on Google SSL transparent certificate
- Script for subdomain name enumeration using CloudFlare
- A domain scanner
- Knock Subdomain Scan
- Collect target subdomain information in multiple ways
- Brother domain name query

- Subdomain name enumeration based on dns query
- 710Kit
- Subdomain query
- Side station query
- FTP brute force
- Gobuster
- Tools for collecting website URIs and DNS subdomains written in the Go language

Tools—XSS

- XSStrike
- XSStrike is a program which can crawl, fuzz and bruteforce parameters for XSS. It can also detect and bypass WAFs.
- xsschef
- a Chrome Extension Exploitation Framework

- mosquito
- XSS exploitation tool—access victims through HTTP proxy
- xssfork
- XSS data receiving platform
- ezXSS
- ezXSS is an easy way to test (blind) XSS
- scanning
- BruteXSS
- Cross-Site Scripting Bruteforcer
- XSSTracer
- A small python script to check for Cross-Site Tracing
- fuzzXssPHP
- Reflective xss scan for PHP version
- xss_scan

- Batch scan xss python script
- autoFindXssAndCsrf
- A browser plug-in that automates the detection of XSS and CSRF vulnerabilities on the page
- xss

Tools—Database Scanning, Injection Tool SQLi

- King of injection tools sqlmap
- NoSQLMap
- SQLiScanner
- A passive SQL injection vulnerability scanning tool based on SQLMAP and Charles
- DSSS
- Sql injection vulnerability scanner with 99 lines of code implementation
- Feigong

- MySQL injection scripts that change freely for various situations
- NoSQLAttack
- An attack tool for mongoDB
- bbqsql
- SQL blind use framework
- PowerUpSQL
- Powershell scripting framework that attacks SQLSERVER
- whitewidow
- Another database scanner
- mongoaudit
- MongoDB Auditing and Penetration Tools
- commix
- Injection point command execution utilization tool
- Short for command injection exploiter, web injection command detection tool

- sqli-hunter
- Web proxy, real-time detection of sqli by loading sqlmap api

Tools—weak password or information leak scanning

- awBruter
- Thousand times speed sentence password blasting tool
- Cr3dOv3r
- According to the mailbox to automatically search for leaked password information, you can also test whether the account password can be logged in at major websites.
- x-crack
- Weak password scanner, Support: FTP/SSH/MSSQL/MYSQL/PostGreSQL/REDIS/ElasticSearch/MONGODB
- htpwdScan

- A simple HTTP brute force attack, collision library attack script
- BBScan
- A mini information leak batch scan script
- GitHack
- `.git` Folder leak exploit tool
- BScanner
- Dictionary-based directory scan gadget
- Fenghuangscanner_v3
- Various ports and weak password detection, author wilson9x1, the original address is invalid
- F-Scrack
- Script for weak password detection for various services
- cupp
- Generate weak password detection dictionary script according to user habits

- genpAss
- Weak password generator with Chinese characteristics
- crack_ssh
- Go to write the coroutine version of ssh\redis\mongodb weak password cracking tool
- Comfortable
- Enter all Internet passport information registered by the user by entering email, phone, username
- GitPrey
- GitHub Sensitive Information Scanning Tool
- gitscan
- Github information collection, real-time scanning query git latest upload related email account password letter
- truffleHog

- GitHub sensitive information scanning tools, including detection commits, etc.
- GitHarvester
- Github Repo Information Collection Tool
- gitleaks
- Searches full repo history for secrets and keys
- x-patrol
- Github leak scanning system
- pydictor
- Violent crack dictionary building tool
- Blasting_dictionary
- Password dictionary
- xxe-recursive-download
- Xxe vulnerability recursive download tool
- xlog

- Web log scanning tool

Tools—port scanning, fingerprinting, and middleware scanning

- Nmap—the king of port scanners—https://svn.nmap.org/
- anoNmap
- anoNmap is a port scanner which utilizes Facebook's XSPA vulnerability to perform anonymous port scans
- wyportmap
- Target port scanning + system service fingerprint identification
- weakfilescan
- Dynamic multi-threaded sensitive information disclosure detection tool
- getcms
- A cms discover recognize tool in python
- wafw00f

- WAF product fingerprint recognition
- wafid
- Wafid identify and fingerprint Web Application Firewall (WAF) products.
- sslscan
- Ssl type identification
- whatweb
- Web fingerprinting
- FingerPrint
- Web application fingerprint recognition
- Scan-T
- Web crawler fingerprint recognition
- Nscan
- a fast Network scanner inspired by Masscan and Zmap
- F-NAScan

- Network asset information scanning, ICMP survivability detection, port scanning, port fingerprint service identification
- F-MiddlewareScan
- Middleware scanning
- dirsearch
- Web path scanner
- bannerscan
- C segment Banner and path scan
- RASscan
- Port service scan
- bypass_waf
- Waf automatic break
- WAFNinja
- Automation bypasses WAF scripts
- xcdn

- Try to find out the real ip behind cdn
- BingC
- C-segment/side-station query based on Bing search engine, multi-threading, API support
- DirBrute
- Multi-threaded WEB directory blasting tool
- httpscan
- A crawler-style network segment web host discovery gadget
- doom
- Ip port vulnerability scanner for distributed task distribution on thorn
- grab.js
- Fast TCP fingerprint capture parsing tool like zgrab, support more protocols
- whichCDN
- CDN identification, detection

- bcrpscan
- Reptile-based web path scanner
- Breacher
- An admin panel finder script written in python.
- DirBrute
- Multi-threaded WEB catalog blasting tool

Tools—Intranet security penetration test

- VulScritp
- Enterprise intranet penetration scripts, including banner scanning, port scanning; various general exploits, etc.
- VulScritp
- Intranet penetration script
- network_backdoor_scanner
- Intranet detection framework based on network traffic

- WebRtcXSS
- Automate the use of XSS to invade the intranet
- mimikatz
- Windows penetration artifact
- PowerSploit
- Powershell infiltration library collection
- PowerShell
- Powershell tools合集
- p0wnedShell
- PowerShell Runspace Post Exploitation Toolkit
- hunter
- Call the Windows API to enumerate user login information
- LaZagne
- Native password view extraction tool

- mimipenguin
- Linux password grabbing artifact
- johnny
- Password cracking tool
- LaZagne
- Locally stored various password extraction tools
- icebreaker
- A tool for automated attacking Active Directory in an intranet environment
- Powershell-RAT
- Python based backdoor that uses Gmail to exfiltrate data as an e-mail attachment. It tracks the user activity using screen capture and sends the information to an attacker as an e-mail attachment.

Tools—Targeted Vulnerability Testing Tool

- weblogic_unserialize_exploit

- The weblogic exploit command of the java deserialization vulnerability echoes exp
- cmsPoc
- Phpcmsv9.6.0 wap module sql injection to get passwd
- Icmsv7.0.1 admincp.php sql injection background arbitrary login
- hackUtils
- Penetration and web attack scripts
- Java deserialization exploit tool set
- ysoserial
- Java deserialization utility
- Jenkins
- Jenkins vulnerability detection, user crawling blasting
- dzscan
- Discuz vulnerability scan
- CMS-Exploit-Framework

- CMS attack framework
- IIS_shortname_Scanner
- IIS short file name vulnerability scan
- Flash scanner
- Flashxss scan
- SSTIF
- Semi-automated tool for server-side template injection vulnerability
- tplmap
- Server-side template injection vulnerability detection and utilization tool
- dockerscan
- Docker scanning tool
- break-fast-serial
- Detect Java Deserialization Vulnerability Tools with DNS Resolution
- dirtycow.github.io

- Dirty cattle empowerment vulnerability exp
- a2sv
- Auto Scanning to SSL Vulnerability
- msdat
- MSDAT: Microsoft SQL Database Attacking Tool
- xxegen
- Xxe online generation utilization tool
- DSXS
- Damn Small XSS Scanner (DSXS)
- a fully functional Cross-site scripting vulnerability scanner (supporting GET and POST parameters) written in under 100 lines of code.

Tools—code static scan, code run stack trace

- VulHint
- php-static-analysis-tools

- Php static scan toolset
- phpstan
- cobra
- White box code security audit system
- phpvulhunter
- Static php code audit
- php-malware-finder
- Detect potentially malicious PHP files
- phptrace
- Tools to track and analyze PHP operations
- hNodeJsScan
- NodeJS application code audit
- BadCode
- PHP code audit

- pyvulhunter
- Python audit tool
- dawnscanner
- Ruby source audit
- brakeman
- Security vulnerabilities in Ruby on Rails applications
- Mobile-Security-Framework-MobSF/
- App black box audit
- iOSSecAudit
- iOS security audit
- Found
- Multi-Architecture GDB Enhanced Features for exploit devs & reversers
- angr
- The next-generation binary analysis platform from UC Santa Barbara's Seclab

Tools—fuzz

- honggfuzz
- honggfuzz-rs
- Fuzz your Rust code with Honggfuzz!
- winafl
- NodeFuzz
- us-fuzz
- halphafuzzer/
- LibFuzzer
- wfuzz
- Web to Fuzz tool
- htpwdScan
- HTTP brute force attack, collision library attack script
- XSS-Radar

- Tools for fast XSS Fuzz testing, currently only supports Chrome browser extensions
- OSS Fuzz
- Continuous Fuzzing for Open Source Software
- kDriver-Fuzzer
- Driver vulnerability mining tool based on ioctlbf framework

Tools—Exploit and Attack Framework

- msf
- metasploitHelper
- OWASP-Nettacker
- pocscan
- Poc call framework, can load Pocsuite, Tangscan, Beebeeto, etc.
- Pocsuite
- Beehive

- Bugscan
- BugScan-Doc
- getsploit
- Command line utility for searching and downloading exploits
- One-Lin3r
- A lightweight attack framework similar to the Metasploit web-delivery module that simplifies complex attacks into one line of commands
- POC-T
- Penetration testing plug-in concurrency framework

Tools—Modular Scan, Integrated Scanner

- nmap-vulners
- NSE script using some well-known service to provide info on vulnerabilities
- Adding to Nmap

- vulners-scanner
- Vulnerability scanner based on vulners.com audit API https://vulners.com
- V3n0M-Scanner
- Popular Pentesting scanner in Python3.6 for SQLi/XSS/LFI/RFI and other Vulns
- BlackWidow
- Web crawler based on Python, used to collect intelligence information of target websites and fuzzing OWASP vulnerabilities
- w8scan
- A vulnerability scanner that mimics bugscan
- whitewidow
- SQL Vulnerability Scanner
- CMSmap
- AngelSword
- CMS vulnerability detection framework written in Python 3

- Luna
- An open source automated web vulnerability scanning tool
- Zeus-Scanner
- passive_scan
- S7scan
- Striker
- Xunfeng
- The patrol is a rapid emergency response and cruise scanning system for enterprise intranets.
- ZeroExploit
- Front and rear end combined detection
- ark
- Distributed scanning framework
- ReconDog
- http://www.arachni-scanner.com

- http://github.com/Arachni/arachni
- Web application security scanner framework
- AZScanner
- Automatic vulnerability scanner, subdomain blasting, port scanning, directory blasting, common framework vulnerability detection
- lalascan
- Distributed web vulnerability scanning framework, collection owasp top10 vulnerability scanning and border asset discovery capabilities
- BkScanner
- BkScanner distributed, plug-in web vulnerability scanner
- GourdScanV2
- Passive vulnerability scanning
- pentestdb
- WEB penetration test database
- passive_scan

- Http proxy based web vulnerability scanner
- Sn1per
- Automated scanners, including middleware scanning and device fingerprinting
- pentestEr_Fully-automatic-scanner
- Directional fully automated penetration testing tool
- 3xp10it
- Automated penetration testing framework
- lcyscan
- Scanning effect is not verified
- POC-T
- Penetration testing plug-in concurrency framework
- V3n0M-Scanner
- Scanner in Python3.5 for SQLi/XSS/LFI/RFI and other Vulns
- leakScan

- Online vulnerability scanning on the web
- AnyScan
- In development…
- Hscan-Win-Gui
- DorkNet
- Selenium powered Python script to automate searching for vulnerable web apps.
- AutoSploit
- Automated Mass Exploiter
- w9scan
- A versatile website vulnerability scanner that draws on the excellent code of your predecessors. Built-in 1200+ plug-in can detect the website once, including but not limited to web fingerprint detection, port fingerprint detection, website structure analysis, various popular vulnerability detection, crawler and SQL injection detection, XSS detection, etc., w9scan will Automatically generate beautiful HTML format result reports.

- Scanners-Box
- The toolbox of open source scanners—Security industry practitioners self-developed open source scanners
- HUNT
- Identify common parameters vulnerable to certain vulnerability classes

Tools—Shell

- webshell
- Cknife
- Chinese ant sword
- antSword
- antSword-shells
- PyShell
- Python backdoor
- PyCmd

- Python+php+jsp WebShell (a sentence Trojan)
- Detailed reference: thief.one
- hackUtils
- Penetration and web attack scripts
- phpsploit
- PhpSploit is a remote control framework, aiming to provide a stealth interactive shell-like connection over HTTP between client and web server. It is a post-exploitation tool capable to maintain access to a compromised web server for privilege escalation purposes.
- hack_tools_for_me
- Web penetration gadgets collection
- p0wnedShell
- An environment that does not rely on powershell.exe to execute PowerShell script code

Tools—Wireless wifi / IoT

- Wireless network penetration, scanning
- fern-wifi-cracker
- Wireless security audit tool
- PytheM
- Python network / penetration testing tool
- WiFi-Pumpkin
- Wireless Security Penetration Test Suite
- wifi-arsenal
- wifitest
- A simple WIFI weak password hacking python script, can automatically crack in real time, do not need to use aircrack-ng to capture packets, just a little slow…
- Wireless-Router-Vulnerability
- IoT device scanning

- IoTSeeker
- IoT device default password scanning detection tool
- iotdb
- Scan an IoT device with nmap
- Routerhunter-2.0
- Router vulnerability scanning
- routersploit
- Router exploit framework
- telnet-scanner
- Telnet service password collision library
- PRICE
- Printer attack framework

Tools—Enterprise Network Self Test

- LNScan
- Detailed internal network information scanner
- LocalNetworkScanner
- Local web scanner implemented by javascript
- Xunfeng
- Network asset recognition engine, vulnerability detection engine
- theHarvester
- Enterprises are indexed by search engines for sensitive asset information monitoring scripts: employee mailboxes, subdomains, and Hosts
- Multisearch-v2
- Search engine aggregate search, which can be used to discover sensitive asset information that companies are indexed by search engines.

Tools—EXP writing framework and tools

- rop-tool

- Binary EXP authoring tool
- pwntools
- CTF Pwn class topic scripting framework
- uncle
- an easy-to-use io library for pwning development
- frida
- Cross-platform injection tool
- Inject JavaScript to explore native apps on Windows, Mac, Linux, iOS and Android
- Sickle
- Shellcode development tool
- radare2
- unix-like reverse engineering framework and commandline tools
- CHAOS
- CHAOS allow generate payloads and control remote Windows systems.

Tools—MIM & phishing

- MIM man-in-the-middle attack framework
- https://github.com/secretsquirrel/the-backdoor-factory
- https://github.com/secretsquirrel/BDFProxy
- https://github.com/byt3bl33d3r/MITMf
- mallory
- Scalable middleman agent tool
- LANs.py
- Inject code, jam wifi, and spy on wifi users
- wifiphisher
- Wifi fishing
- PhishLulz
- a Ruby toolset aimed at automating Phishing activities
- mitmproxy

- An interactive TLS-capable intercepting HTTP proxy for penetration testers and software developers.

Tools—Defense

- Malware analysts and reverse-engineering env
- REMnux—Based on Debian
- Webshell detection and virus analysis tools
- Find_webshell
- Php backdoor detection, script is simple, so there are problems with high false positives and low efficiency
- Webshell sample library
- ScanBackdoor
- Webshell scanning tool
- BackdoorMan
- PHP backdoor scanning

- findWebshell
- Another webshell detection tool
- HaboMalHunter
- Hubble Analysis System, Linux System Virus Analysis and Security Detection
- PlagueScanner
- Integrated Python implementation of ClamAV, ESET, Bitdefender's anti-virus engine
- php-malware-finder
- An efficient PHP-webshell scanning tool
- PHP-Shell-Detector
- Webshell detection tool with up to 99% efficiency
- malwarecage
- A component for automated malware collection/analysis systems, written in Python 2, supporting REST API

- x-waf
- Cloud waf for small and medium enterprises
- Binary and code analysis tools
- binwalk
- binmap
- System scanner for finding programs and libraries and then collecting their dependencies, links, etc.
- rp
- rp++ is a full-cpp written tool that aims to find ROP sequences in PE/Elf/Mach-O (doesn't support the FAT binaries) x86/x64 binaries.
- badger
- Windows Exploit Development工具
- amoco
- Binary static analysis tool (python)
- peda

- Python Exploit Development Assistance for GDB
- billgates-botnet-tracker
- Monitoring tool for BillGates Linux Botnet Trojan activity
- RATDecoders
- Trojan configuration parameter extraction tool
- angr
- Binary analysis tool written by Shellphish (CTF)
- pysonar2
- Static code analysis tool for python
- shellcheck
- An automated script analysis tool to give warnings and suggestions
- andcsufbo
- Simple Javascript anti-aliasing aid based on AST transformation
- Waf open source and rules

- x-waf
- tx_lua_waf
- owasp-modsecurity-crs
- waf-research
- phpwaf
- DDOS protection
- Dshield
- Database firewall
- DBShield/
- Yulong-hids
- 驭龙HIDS—A host intrusion detection system developed by YSRC

Tools—Mining

- xmrig

- coin-hive
- CoinHive cryptocurrency miner for node.js

Tools—Miscellaneous

- SocialEngineeringPayloads
- github_arsenal
- Github arsenal
- SecLists
- fuzzdb
- malwares
- ExploitKit
- nullsecurity
- BlueLotus_XSSReceiver
- XSS platform

- CTF tool
- Web security tool
- scanner
- BB2 scanner
- AWVS
- Vulnerability scanning
- OwaspZAP
- Vulnerability scanning
- Burp suite
- Vulnerability scanning
- [Artifact] Burp Suite Pro Loader & Keygen By surferxyz (with v1.7.31 original)
- Burp_Suite_Pro_v1.7.31.zip with cracker
- Solve the full version of the Burp time expiration problem—h4ck0ne.docx
- Worthwhile BurpSuite Plugins

- Literally anything by James Kettle
- backslash-powered-scanner
- ActiveScan++
- Cloud Storage Tester
- Ability to read responses to links to different cloud services (Amazon, Microsoft, Google) and perform some security checks on those objects.
- JSON Beautifie
- Content Type Converter
- Copy As Python-Requests (possibly other 'Copy As' plugins)
- HUNT
- Identify some parameters that are vulnerable to vulnerabilities
- Metadata
- payloads
- Nessus
- Crawl Microsoft vulnerability information

- reGeorg
- udfhack
- Science online
- XX-Net
- xsocks
- Reliable , light-weight reverse socks5 server for windows&linux.
- v2ray-core
- TangScan
- Beebeeto-framework
- httpie
- The http command line client can send various http requests from the command line construct (similar to Curl)
- Browser Exploitation Framework
- BeEF
- Vtools

- webscanner
- a web path scanner
- phpaudit
- An env for php code audit (code review) with xdebug
- Filter some useful online URLs
- Must know the security tools
- Penetration test information collection tool
- frida
- Dynamic instrumentation toolkit for developers, reverse-engineers, and security researchers.
- pwn
- A Javascript library for browser exploitation
- Firefox-Security-Toolkit
- A tool that transforms Firefox browsers into a penetration testing suite
- al-khaser

- Public malware techniques used in the wild: Virtual Machine, Emulation, Debuggers, Sandbox detection.
- pcap-analyzer
- Online lightweight Pcap traffic file analysis tool
- awesome-spider
- pentest_tools\
- Java High Concurrency Spike System API

Tools—CTF tools

- Miscellaneous
- pwndocker
- vFuckingTools
- A CTFer tools bag
- ctf-tools
- Attacks

- Bettercap—Framework to perform MITM (Man in the Middle) attacks.
- Layer 2 attacks—Attack various protocols on layer 2
- Crypto
- FeatherDuster—An automated, modular cryptanalysis tool
- PkCrack—A tool for Breaking PkZip-encryption
- RSATool—Generate private key with knowledge of p and q
- XORTool—A tool to analyze multi-byte xor cipher
- Bruteforcers
- Hashcat—Password Cracker
- John The Jumbo—Community enhanced version of John the Ripper
- John The Ripper—Password Cracker
- Nozzlr—Nozzlr is a bruteforce framework, trully modular and script-friendly.
- Ophcrack—Windows password cracker based on rainbow tables.
- Patator—Patator is a multi-purpose brute-forcer, with a modular design.

- Exploits
- DLLInjector—Inject dlls in processes
- libformatstr—Simplify format string exploitation.
- Metasploit—Penetration testing software
- one_gadget—A tool to find the one gadget `execve('/bin/sh', NULL, NULL)` call
- `gem install one_gadget`
- Pwntools—CTF Framework for writing exploits
- Qira—QEMU Interactive Runtime Analyzer
- ROP Gadget—Framework for ROP exploitation
- V0lt—Security CTF Toolkit
- Forensics
- Aircrack-Ng—Crack 802.11 WEP and WPA-PSK keys
- `apt-get install aircrack-ng`
- Audacity—Analyze sound files (mp3, m4a, whatever)

- `apt-get install audacity`
- Bkhive and Samdump2—Dump SYSTEM and SAM files
- `apt-get install samdump2 bkhive`
- CFF Explorer—PE Editor
- Creddump—Dump windows credentials
- DVCS Ripper—Rips web accessible (distributed) version control systems
- Exif Tool—Read, write and edit file metadata
- Extundelete—Used for recovering lost data from mountable images
- Fibratus—Tool for exploration and tracing of the Windows kernel
- Foremost—Extract particular kind of files using headers
- `apt-get install foremost`
- Fsck.ext4—Used to fix corrupt filesystems
- Malzilla—Malware hunting tool
- NetworkMiner—Network Forensic Analysis Tool

- PDF Streams Inflater—Find and extract zlib files compressed in PDF files
- ResourcesExtract—Extract various filetypes from exes
- Shellbags—Investigate NT_USER.dat files
- UsbForensics—Contains many tools for usb forensics
- Volatility—To investigate memory dumps
- RegistryViewer—Used to view windows registries
- Windows Registry Viewers—More registry viewers
- Networking
- Masscan—Mass IP port scanner, TCP port scanner
- Nipe—Nipe is a script to make Tor Network your default gateway.
- Nmap—open source utility for network discovery and security auditing
- Wireshark—Analyze the network dumps
- `apt-get install wireshark`
- Zmap—an open-source network scanner

- Reversing
- Androguard—Reverse engineer Android applications
- Angr—platform-agnostic binary analysis framework
- Apk2Gold—Yet another Android decompiler
- ApkTool—Android Decompiler
- Barf—Binary Analysis and Reverse engineering Framework
- Binary Ninja—Binary analysis framework
- BinUtils—Collection of binary tools
- BinWalk—Analyze, reverse engineer, and extract firmware images.
- Boomerang—Decompile x86 binaries to C
- ctf_import—run basic functions from stripped binaries cross platform
- GDB—The GNU project debugger
- GEF—GDB plugin
- Hopper—Reverse engineering tool (disassembler) for OSX and Linux

- IDA Pro—Most used Reversing software
- Jadx—Decompile Android files
- Java Decompilers—An online decompiler for Java and Android APKs
- Krakatau—Java decompiler and disassembler
- PEDA—GDB plugin (only python2.7)
- Plasma—An interactive disassembler for x86/ARM/MIPS which can generate indented pseudo-code with colored syntax.
- Pwndbg—A GDB plugin that provides a suite of utilities to hack around GDB easily.
- radare2—A portable reversing framework
- Uncompyle—Decompile Python 2.7 binaries (.pyc)
- WinDbg—Windows debugger distributed by Microsoft
- Z3—a theorem prover from Microsoft Research
- Detox—A Javascript malware analysis tool
- Revelo—Analyze obfuscated Javascript code

- RABCDAsm—Collection of utilities including an ActionScript 3 assembler/disassembler.
- Swftools—Collection of utilities to work with SWF files
- Xxxswf—A Python script for analyzing Flash files.
- Services
- CSWSH—Cross-Site WebSocket Hijacking Tester
- Request Bin—Lets you inspect http requests to a particular url
- Steganography
- Convert—Convert images b/w formats and apply filters
- Exif—Shows EXIF information in JPEG files
- Exiftool—Read and write meta information in files
- Exiv2—Image metadata manipulation tool
- ImageMagick—Tool for manipulating images
- Outguess—Universal steganographic tool
- Pngtools—For various analysis related to PNGs

- `apt-get install pngtools`
- SmartDeblur—Used to deblur and fix defocused images
- Steganabara—Tool for stegano analysis written in Java
- Stegbreak—Launches brute-force dictionary attacks on JPG image
- Steghide—Hide data in various kind of images
- Stegsolve—Apply various steganography techniques to images
- Web
- Commix—Automated All-in-One OS Command Injection and Exploitation Tool.
- Hackbar—Firefox addon for easy web exploitation
- OWASP ZAP—Intercepting proxy to replay, debug, and fuzz HTTP requests and responses
- Postman—Add on for chrome for debugging network requests
- SQLMap—Automatic SQL injection and database takeover tooli
- W3af—Web Application Attack and Audit Framework.

- XSSer—Automated XSS testor
- WhatWaf

Learning—Web application pentesting

- Prerequisites:
- **Usage of**
- Burp
- nikto
- Openvas
- SQLMap
- Netcat
- Dirbuster/ wfuzz
- Hydra
- Kewl

- Wp-scan
- dig
- Knowledge of
- HTTP protocol and HTTP Methods (GET, POST, OPTIONS, PUT, TRACE)
- DNS
- **CGI**
- **Web session management**
- Cookies and their parameters
- Concepts of **XSS** (reflected, stored, DOM based), CSRF, SQLi, Remote/Local File Inclusion, Direct Object Reference, Forceful Browsing, Log Poisoning
- Latest/common **web application** vulnerabilities (e.g. vulnerabilities in WordPress, XAMPP, etc.)
- **Heartbleed** & **ShellShock**

sites

- Security
- Web-Security-Learning
- Software-Security-Learning
- Web application penetration testing process
- Web test method tool articles
- Mysql injection map—learning articles
- Database query basis
- Sql injection learning summary
- General ideas and wonderful skills of SQL injection
- Wide character injection and actual combat
- webgoat-Injection
- Postgresql database utilization
- Pentester Lab SQL to shell

- WAF-Bypass
- Browser's XSS Filter Bypass Cheat Sheet
- PHP code audit segment explanation
- Advanced PHP Application Vulnerability Review Technology
- On the common vulnerabilities in PHP
- Php code audit
- Audit-Learning
- PHP code audit summary
- PHP+Mysql injection protection and bypass
- Summary of background bypass methods common in PHP open source programs
- PHP-code-audit
- Advanced PHP Application Vulnerability Review Technology
- PHP code auditing—security issues in the sprintf function
- XSS Cheat Sheet

- AwesomeXSS
- XSS-Filter-Evasion-Cheat-Sheet-CN
- XSS Filter Evasion Cheat Sheet Chinese version
- EN address
- XSS study notes [1]
- XSS study notes [two]
- XSS test load
- Code security upload file
- Code security file contains
- Code Security SSRF
- Ten minutes to bring you to know XXE
- XPath Injection: Attack and Defense Technology
- Wonderful webshell skills
- Know Chuangyu R&D Skills Table

- Web Hacking 101 Chinese version
- Burpsuite practical guide
- Penetration Test Node.js application
- awesome#security
- awesome-infosec
- Web security data and resource list
- How To Become A Hacker
- What are the places where you can learn about information security and network security?
- How do hackers learn?
- How does zero-based learning Web security?
- Looking for a hacker list?
- Older, zero-based, want to switch to network security. How is it more feasible?

- How to learn hacking techniques across industries? Is the profession not correct?
- How to learn information security?
- Hacker Manifesto
- https://support.portswigger.net/customer/portal/topics/792273-burp-testing-methodologies/articles
- https://digi.ninja/blog/when_all_you_can_do_is_read.php
- https://www.exploit-db.com/docs/12389.pdf
- http://www.slideshare.net/SOURCEConference/wfuzz-para-penetration-testers
- https://en.wikipedia.org/wiki/List_of_HTTP_status_codes
- http://www.tutorialspoint.com/http/http_methods.htm
- http://www.elated.com/articles/your-first-cgi-script/
- https://www.idontplaydarts.com/2011/02/using-php-filter-for-local-file-inclusion/

- http://www.enigmagroup.org/articles/view/Linux%20Hacking/115-LFI-Apache-log-poisoning
- http://pentestmonkey.net/cheat-sheet/sql-injection/mysql-sql-injection-cheat-sheet
- https://www.owasp.org/index.php/OWASP_Testing_Guide_v4_Table_of_Contents
- http://resources.infosecinstitute.com/file-upload-vulnerabilities/
- http://excess-xss.com/
- https://www.owasp.org/index.php/XSS_Filter_Evasion_Cheat_Sheet
- http://www.vsecurity.com/download/papers/XMLDTDEntityAttacks.pdf
- ttp://resources.infosecinstitute.com/practical-shellshock-exploitation-part-1/
- http://resources.infosecinstitute.com/practical-shellshock-exploitation-part-2/
- 2018 PHP application security design refers to North
- Security options related to http header security

- sqlmap wiki
- API-Security-Checklist
- Books
- The Web Application Hacker's Handbook
- Ethical Hacking and Penetration Testing Guide
- The Hacker Playbook 2: Practical Guide to Penetration Testing
- Kali Linux Web penetration test cheats Chinese version
- node-sec-roadmap
- Some thoughts on how Node.js might respond to a changing security environment
- The security roadmap is a gitbook publication available at https://nodesecroadmap.fyi/

Learning—Binary and memory exploitation

- Prerequisites:

- **Usage of**
- Gdb (inc. gdb-peda), Valgrind
- Edb, OllyDBG
- Metasploit (generating payloads)
- Knowledge of
- Program execution flow
- Stack vs Heap (inc. details on how they work)
- Registers
- Reading assembly code
- **Modern mechanisms** of buffer overflow prevention (NX/DEP, ASLR, Stack Canaries)
- sites
- awesome-malware-analysis
- Reverseng
- 《reverse-engineering-for-beginners》

- RE-for-beginners
- Getting started with Linux exploit development
- http://insecure.org/stf/smashstack.html
- http://www.intelligentexploit.com/articles/Linux-Stack-Based-Buffer-Overflows.pdf
- http://beej.us/guide/bggdb/
- http://protostar-solutions.googlecode.com/hg/Stack%206/ret2libc.pdf
- https://www.corelan.be/index.php/2009/07/19/exploit-writing-tutorial-part-1-stack-based-overflows/
- http://www.slideshare.net/saumilshah/dive-into-rop-a-quick-introduction-to-return-oriented-programming
- https://speakerdeck.com/barrebas/rop-primer
- https://crypto.stanford.edu/cs155/papers/formatstring-1.2.pdf
- https://www.defcon.org/images/defcon-18/dc-18-presentations/Haas/DEFCON-18-Haas-Adv-Format-String-Attacks.pdf

- http://codearcana.com/posts/2013/05/02/introduction-to-format-string-exploits.html
- http://blog.knapsy.com/blog/2015/11/25/easy-file-sharing-web-server-v7-dot-2-remote-seh-buffer-overflow-dep-bypass-with-rop/
- secure-ios-app-dev
- browser-security-whitepaper-2017
- X41 Browser Security White Paper—Tools and PoCs

Learning—Windows and Linux Privilege Escalation

- Prerequisites:
- **Usage of**
- Metasploit
- SysInternals Suite (psexec, etc.)
- Scalpel / Autopsy
- dd

- **Knowledge of**
- Basic networking concepts
- Binary file structure
- Underlying operating systems architecture
- File and directory permissions on Unix & Windows
- sites
- Linux
- http://blog.g0tmi1k.com/2011/08/basic-linux-privilege-escalation/
- http://www.0daysecurity.com/penetration-testing/enumeration.html
- http://incolumitas.com/wp-content/uploads/2012/12/blackhats_view.pdf
- https://github.com/rebootuser/LinEnum/blob/master/LinEnum.sh
- Cobalt Strike first experience
- Linux penetration test
- Linux local information collection

- Common usage of curl in infiltration
- Kali penetration test tool method
- Crossing the border
- Bounce shell posture under linux
- How many of these orders have you used?
- Linux penetration test command quick reference manual
- Windows
- Intranet penetration learning from scratch
- I understand the intranet penetration—the internal network penetration knowledge summary
- Common remote execution command method
- Empowerment skills
- How to elegantly bypass the killing soft to get system permissions
- Windows command to execute the posture of uploading files
- Information collection under Windows environment

- Windows empowerment series
- Windows privilege series
- Windows common commands
- Have you studied the posture of downloading files with powershell?
- http://www.fuzzysecurity.com/tutorials/16.html
- http://it-ovid.blogspot.com.au/2012/02/windows-privilege-escalation.html
- http://www.r00tsec.com/2012/11/howto-manual-pentest-windows-cheatsheet.html
- http://www.windowsecurity.com/articles-tutorials/misc_network_security/Dissecting-Pass-Hash-Attack.html
- http://www.windowsecurity.com/articles-tutorials/misc_network_security/PsExec-Nasty-Things-It-Can-Do.html
- Steganography
- http://domnit.org/stepic/doc/

- http://www.sonicvisualiser.org/index.html
- General Forensics
- http://www.gfi.com/blog/top-20-free-digital-forensic-investigation-tools-for-sysadmins/
- Breaking out of restricted shells
- https://speakerdeck.com/knaps/escape-from-shellcatraz-breaking-out-of-restricted-unix-shells

Learning—Miscellaneous

- Vulnerability POC & EXP
- Php vulnerability code analysis
- 100php
- 1000 PHP code audit cases (before 2016.7 black cloud open vulnerability)
- poc from bugscan beebeeto
- Some-PoC-oR-ExP

- exploits
- awesome-cve-poc
- Vulnerability Labs for security analysis
- windows-kernel-exploits
- Windows platform privilege vulnerability collection
- linux-kernel-exploits
- Linux platform elevation vulnerability collection
- office-exploits
- Office vulnerability collection
- poc or exp of android vulnerability
- POC-Collect
- Simple test for CVE-2016–2107
- CVE-2015–7547 POC
- JAVA deserialization POC generation tool

- JAVA deserialization EXP
- JavaDeserH2HC
- Sample codes written for the Hackers to Hackers Conference magazine 2017 (H2HC).
- marshalsec
- Java Unmarshaller Security
- Jenkins CommonCollections EXP
- CVE-2015–2426 EXP (Windows kernel privilege)
- Use docker to show web attack (php local file contains a demo with phpinfo getshell and ssrf combined with curl)
- Php7 cache overwrite vulnerability Demo and related tools
- XcodeGhost Trojan sample
- does
- secbook
- hacker101

- Hacker101 is a free class for web security
- collection-document awesome
- ctf-wiki
- ctf-wiki
- A hodgepodge guide in the CTF field
- Ctf and hacker resource collection
- Large collection of ctf and security tools
- CTF-notes
- ctf-write-ups
- Know Chuangyu R&D Skills Table v3.1
- Security Skills Tree
- Vulnerability bank
- sec-jobs
- Information security internships and school recruiting, truth and information to reduce the pain of security players looking for

internships/work

- OSG-TranslationTeam
- Hack with GitHub
- Hack-with-Github/Awesome-Hacking
- carpedm20/awesome-hacking
- chinese version
- sbilly/awesome-security
- awesome-threat-detection
- Resource set for threat detection and pursuit
- Mind-Map
- Information security tools and resource collections
- Awesome Pentest Cheat Sheets
- bugbounty-cheatsheet
- paragonie/awesome-appsec

- awesome-application-security
- Awesome-Fuzzing
- exploit-database
- exploit-database-bin-sploits
- wooyun_public
- Python security tutorial (original link http://www.primalsecurity.net/tutorials/python-tutorials/)
- python_sec
- Python security and code audit related data collection resource collection of python security and code review
- Data_hacking collection
- mobile-security-wiki
- Some information security standards and device configurations
- APT related notes
- Kcon information

- Code-Audit-Challenges
- Awesome CTF Book
- 《DO NOT FUCK WITH A HACKER》
- Kali Linux Tools Chinese Manual
- Vulnerability era
- awesome-incident-response
- Cosine—not afraid of offending people recommend these 9 hacking books
- ICS/SCADA Security Resource (integrated industrial security related resources)
- Crypto 101, the introductory book on cryptography.
- Awesome-Red-Teaming
- Threat intelligence, malicious sample analysis, open source Malware code collection
- bugbounty-cheatsheet
- awesome-bug-bounty

- bug-bounty-reference
- bug bounty guide
- Safe mind map collection
- Various security-related mind maps collected
- Backup
- Network security penetration test
- OWASP Top 10 key point record
- Port penetration summary_91Ri.org
- Common port and security testing
- 2017-Security-ppt
- Port scanning those things
- Web dog to understand the intranet port forwarding
- Password cracking those things
- About password dictionary things

- Pydictor blasting dictionary generation guide
- Use the rainbow table to crack the hash
- Wireless Penetration Testing Cheat Sheet
- Syn-Flood attack
- SOCKSTRESS attack principle and defense
- Slowhttptest attack principle
- Principles and examples of local DNS attacks
- DNS tunneling technology analysis
- TCP session hijacking principle and test
- HTTPS attack principle and defense
- Intranet middleman's gameplay
- See how I collect whois information for the entire network IP
- On various postures of second-level domain name collection
- Intranet penetration host discovery skills

- Intranet host discovery skills supplement
- Information Collection—Zombie Scanning
- bWAPP game summary
- Analysis of RPO Attack Technology

Wargrames/CTFs/VulEnvApp

- Ichunqiu
- google CTF
- Facebook
- facebook CTF
- hackercup
- picoctf
- picoctf 2017
- picoctf.com

- comp for middle and high school students. 31 Mar—14 Apr
- picoctf.com/past
- past competitions
- CySCA
- csaw
- ctf.projectdu.org
- ctf for beginners from Deakin uni. Already over but challenges are always available
- pentesterlab
- Web for Pentecost
- Web for Pentecost II
- From SQL Injection to Shell
- From SQL Injection to Shell II
- PHP Include And Post Exploitation
- metasploitable

- WebGoat
- mutilidae
- https://sourceforge.net/projects/mutillidae
- OWASP DVWA
- vulnerable php/mysql web application to do penetration testing
- OWASP Bricks
- bwapp
- damn vulnerable web application
- root-me
- hackthis
- hackthissite
- workshop.chaurocks.com/hackgame/
- overthewire.org
- overthewire.org/wargames/bandit/

- gameofhacks
- ctf.infosecinstitute.com
- vulnhub
- wargame.cs.nctu.edu.tw
- Pwnable.tw
- try2hack.nl
- ctftime.org
- hackgame.chaurocks.com
- Awesome CTF wargames
- Backdoor—Security Platform by SDSLabs.
- Ctfs.me—CTF All the time
- Exploit Exercises—Variety of VMs to learn variety of computer security issues.
- Gracker—Binary challenges having a slow learning curve, and write-ups for each level.

- Hack This Site—Training ground for hackers.
- IO—Wargame for binary challenges.
- Over The Wire—Wargame maintained by OvertheWire Community
- Pwnable.kr—Pwn Game
- Ringzer0Team—Ringzer0 Team Online CTF
- SmashTheStack—A variety of wargames maintained by the SmashTheStack Community.
- VulnHub—VM-based for practical in digital security, computer application & network administration.
- WebHacking—Hacking challenges for web.
- WeChall—Always online challenge site.
- WTHack OnlineCTF—CTF Practice platform for every level of cyber security enthusiasts.
- What “hacking” competitions/challenges exist?
- http://cff.cnmstl.net/

- geekpwn
- https://infosec.rocks/
- testenv
- A collection of web pages vulnerable to SQL injection flaws
- n0js Challenges
- ZVulDrill
- VAuditDemo
- ctf-challenges
- Code-Audit-Challenges
- 34c3ctf
- Exploit-Challenges
- ctf-web-prob
- FOS:RASP-PHP

WriteUps

- ctfs
- picoctf_2017_writeup
- Awesome CTF writeups-collections
- Captf—Dumped CTF challenges and materials by psifertex
- CTF write-ups (community)—CTF challenges + write-ups archive maintained by the community
- CTFTime Scrapper—Scraps all writeup from ctf time and organize which to read first
- pwntools writeups—A collection of CTF write-ups all using pwntools
- Shell Storm—CTF challenge archive maintained by Jonathan Salwan
- Smoke Leet Everyday—CTF write-ups repo maintained by SmokeLeetEveryday team.
- ctf
- CTF (Capture The Flag) writeups

- Awesome-CTF-Book
- repo
- gitbook
- python-challenge
- Solutions For The Python Challenge
- My_CTF_Challenges
- p4-team/ctf
- bl4de/ctf
- 2018-QWB-CTF

Miscellaneous

- https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project
- https://www.metasploit.com/
- https://www.coursera.org/specializations/cyber-security

- https://cwe.mitre.org/top25/
- CySCA
- 2014
- 2015
- https://www.cybrary.it/
- one stop shop for cyber security
- course
- https://www.cyberciti.biz/faq/grep-regular-expressions/

course

- http://smashthestack.org/
- http://pwnable.kr/
- https://w3challs.com/
- bugcrowd bug-bounty-list

- Chrome Reward
- Google Vulnerability Reward Program
- Vulnerability box

Security | Penetration Testing | Hacker | Pentesting | Information Security

47 claps

Red C0de

Follow

Responses

Write a response...