CTF TOOLS

Tools used for solving CTF challenges

Attacks

Tools used for performing various kinds of attacks

- Bettercap – Framework to perform MITM (Man in the Middle) attacks.
- Layer 2 attacks – Attack various protocols on layer 2

Crypto

Tools used for solving Crypto challenges

- FeatherDuster – An automated, modular cryptanalysis tool
- Hash Extender – A utility tool for performing hash length extension attacks
- PkCrack – A tool for Breaking PkZip-encryption
- RSACTFTool – A tool for recovering RSA private key with various attack
- RSATool – Generate private key with knowledge of p and q
- XORTool – A tool to analyze multi-byte xor cipher

Bruteforcers

Tools used for various kind of bruteforcing (passwords etc.)

- 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

Tools used for solving Exploits challenges

- 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 Analyser
- ROP Gadget – Framework for ROP exploitation
- V0lt – Security CTF Toolkit

Forensics

Tools used for solving Forensics challenges

- 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

Registry Viewers

- RegistryViewer – Used to view windows registries
- Windows Registry Viewers – More registry viewers

Networking

Tools used for solving Networking challenges

- Bro – An open-source network security monitor.
- Masscan – Mass IP port scanner, TCP port scanner.
- Monit – A linux tool to check a host on the network (and other non-network activities).
- Nipe – Nipe is a script to make Tor Network your default gateway.
- Nmap – An 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

Tools used for solving Reversing challenges

- 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)
- Pin A dynamic binary instrumentaion tool by Intel
- 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
- Xocopy – Program that can copy executables with execute, but no read permission
- Z3 – a theorem prover from Microsoft Research

JavaScript Deobfustcators

- Detox – A Javascript malware analysis tool
- Revelo – Analyze obfuscated Javascript code

SWF Analyzers

- 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

Various kind of useful services available around the internet

- CSWSH – Cross-Site WebSocket Hijacking Tester
- Request Bin – Lets you inspect http requests to a particular url

Steganography

Tools used for solving Steganography challenges

- 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

Tools used for solving Web challenges

- BurpSuite – A graphical tool to testing website security.
- 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