Еще больше полезных инструментов. Автор: Игумнова Карина (заголовок)

Фреймворки CTF или универсальные инструменты для CTF (подзаголовок)

PwnTools — фреймворк CTF и библиотека разработки эксплойтов, используемые Gallopsled в каждом CTF.

ctf-tools — Github-репозиторий скриптов с открытым исходным кодом для ваших нужд CTF, таких как binwalk и apktool.

Metasploit Framework — помимо среды и программного обеспечения для тестирования на проникновение, Metasploit имеет модули для автоматической эксплуатации и инструменты для создания ваших эксплойтов, таких как find\_badchars.rb, egghunter.rb, patter\_offset.rb, pattern\_create.rb и т. д.

ROPgadget — используется для эксплуатации ROP

Peda — помощь в разработке эксплойтов Python для GDB

Google – где вы можете задать несколько вопросов

Инструменты обратного проектирования, декомпиляторы и отладчики (подзаголовок)

Immunity Debugger — отладчик, похожий на OllyDbg, в котором есть классные плагины с использованием Python.

OllyDbg — наиболее основанный на дизассемблировании отладчик с графическим интерфейсом для Windows.

SWFScan — позволяет декомпилировать Flash-файлы

gdb — отладчик GNU

IDA Pro - многопроцессорный дизассемблер и отладчик на базе Windows, Linux или Mac OS X.

WinDbg — отладчик Windows, распространяемый Microsoft.

Apktool — инструмент для реверсирования файлов apk для Android.

PE Tool — предоставляет несколько полезных инструментов для работы с исполняемыми файлами Windows PE.

UPX — Ultimate Packer для исполняемых файлов

dex2jar (Андроид)

Radare2 - Unix-подобная среда обратного проектирования и инструменты командной строки.

Strace — трассировщик системных вызовов и еще один инструмент отладки.

Objdump — часть GNU Binutils

PEID — используется для определения того, использовался ли какой-либо обфускатор для упаковки исполняемого файла. Упаковщик с открытым исходным кодом, который часто используется, - это упаковщик UPX.

Инструменты для статического анализа кода (подзаголовок)

RIPS — статический анализатор кода для проверки уязвимостей в PHP-приложениях.

HP Fortify Static Code Analyzer, также известный как Fortify SCA, представляет собой коммерческое программное обеспечение, которое является многоязычным аудитором на наличие уязвимостей.

OWASP Code Crawler — инструмент статической проверки кода для кода .NET и J2EE/JAVA, который поддерживает проект проверки кода OWASP.

OWASP LAPSE Project — инструмент аудита безопасности для обнаружения уязвимостей в приложениях Java EE.

Flawfinder — статический анализатор исходного кода, который исследует исходный код C/C++ и сообщает о возможных уязвимостях безопасности.

Forensics (подзаголовок)

Strings — позволяет искать и извлекать строки ASCII и UNICODE из двоичного файла.

SANS SIFT — SANS Investigative Forensic Toolkit (SIFT) — это Ubuntu Live CD.

ProDiscover Basic — анализатор улик и инструмент визуализации данных

Volatility — структура криминалистической экспертизы памяти

The Sleuth Kit — инструмент цифровой криминалистики с открытым исходным кодом.

FTK Imager — инструмент предварительного просмотра данных и визуализации

IPhone Analyzer — используется для iPhone Forensics, но поддерживает только устройства iOS 2, iOS 3, iOS 4 и iOS 5.

Xplico — инструмент сетевой криминалистики

Binwalk — инструмент анализа прошивки, позволяющий извлечь образ прошивки.

ExifTool — независимая от платформы библиотека Perl плюс приложение командной строки для чтения, записи и редактирования метаинформации в самых разных форматах файлов, таких как EXIF, GPS, IPTC, XMP, JFIF, GeoTIFF, профиль ICC, Photoshop IRB, FlashPix, AFCP и ID3, а также заметки производителя многих цифровых камер Canon, Casio, FLIR, FujiFilm, GE, HP, JVC/Victor, Kodak, Leaf, Minolta/Konica-Minolta, Nikon, Nintendo, Olympus/Epson, Panasonic. /Leica, Pentax/Asahi, Phase One, Reconyx, Ricoh, Samsung, Sanyo, Sigma/Foveon и Sony

dd — утилита командной строки для Unix и Linux, позволяющая копировать и конвертировать файлы.

CAINE — Computer Aided INvestigative Environment — это действующий дистрибутив GNU/Linux, предназначенный для цифровой криминалистики.

Autopsy— графический интерфейс для инструментов анализа цифровых расследований из командной строки в The Sleuth Kit.

Подойдет любой шестнадцатеричный редактор.

DEFT Linux — Linux-дистрибутив Digital Evidence & Forensics Toolkit

Windows Sysiternals — состоит из системных утилит Windows, содержащих различные полезные программы.

Криптография (подзаголовок)

John The Ripper – это бесплатный и быстрый взломщик паролей, доступный для многих разновидностей Unix, Windows, DOS, BeOS и OpenVMS.

Cryptool – инструмент электронного обучения с открытым исходным кодом, иллюстрирующий криптографические и криптоаналитические концепции

crypo.in.ua — онлайн-декодер и кодировщик для криптографии, и у большинства людей, которые присоединяются к соревнованиям CTF, этот сайт открыт во время игры.

Стеганография (подзаголовок)

Steghide - инструмент stega, который можно использовать для встраивания или извлечения данных в различные типы изображений и аудиофайлов.

Ffmpeg — кроссплатформенное программное обеспечение для записи, конвертации и потоковой передачи аудио и видео.

Gimp — программа для работы с изображениями GNU

Audacity — бесплатный аудиоаудитор и рекордер

Stepic — стеганография изображений Python

Pngcheck - тестер и отладчик PNG, который проверяет целостность файлов PNG, JNG и MNG (путем проверки внутренних 32-битных CRC [контрольных сумм] и распаковки данных изображения)

OpenStego — бесплатное решение для стеганографии

MP3Stego — позволяет скрывать текст в файлах MP3.

AtomicParsley - программа командной строки для чтения, анализа и установки метаданных в файлы MPEG-4.

Foremost — консольная программа, используемая для восстановления файлов.

Поиск веб-уязвимостей или веб-эксплуатаций (подзаголовок)

Burp Suite — обычно используется для тестирования безопасности веб-приложений и обычно для поиска веб-уязвимостей вручную, имеет перехватывающий прокси-сервер и настраиваемые плагины.

OWASP ZAP — открытый проект безопасности веб-приложений, похожий на Burp, но бесплатный и с открытым исходным кодом.

WPScan — черный ящик сканера уязвимостей WordPress

W3af — сканер безопасности веб-приложений с открытым исходным кодом

OWASP Dirbuster — инструмент для подбора или обнаружения каталогов

Bizploit - среда тестирования на проникновение ERP с открытым исходным кодом

Сеть (подзаголовок)

aircrack-ng Suite — инструмент для взлома WEP/WPA/WPA2 с открытым исходным кодом, который обычно входит в состав большинства дистрибутивов для пентестинга.

reaver — инструмент для атаки WiFi Protected Setup

Kismet - детектор беспроводной сети уровня 2 802.11, анализатор и система обнаружения вторжений

Pixiewps — инструмент, используемый для перебора вывода WPS в автономном режиме, используя низкую или несуществующую энтропию некоторых точек доступа (атака пикси-пыль).

Nmap — сканер портов с открытым исходным кодом, в котором есть плагины для оценки уязвимостей и сетевого обнаружения.

Wireshark — сетевой сниффер и анализатор сетевых протоколов для Unix и Windows

Netcat — швейцарская армия TCP/IP

Captipper — инструмент Python для анализа, исследования и восстановления вредоносного HTTP-трафика.

Scapy — мощная интерактивная программа для управления пакетами.

Для вашей защиты в атаке в защите (подзаголовок)

Snort — легкая и бесплатная система обнаружения сетевых вторжений для UNIX и Windows.

Iptables

Подойдет любой антивирус и двухсторонний брандмауэр.

Chellam — IDS/брандмауэр Wi-Fi для Windows, которые обнаруживают атаки Wi-Fi, такие как Honeypots, Evil Twins, Mis-association, бэкдоры на основе размещенной сети и т. д., против клиента на базе Windows без необходимости специального оборудования или водители

peepdf — инструмент Python для изучения PDF-файлов, чтобы выяснить, может ли файл быть опасным или нет.

Android IMSI-Catcher Detector – Android-приложение для обнаружения IMSI-Catcher

Некоторые дистрибутивы Linux идеально подходят для CTF (подзаголовок)

Santoku Linux — дистрибутив или дистрибутив GNU/Linux, разработанный, чтобы помочь вам во всех аспектах вашей мобильной криминалистики, анализа мобильных вредоносных программ, обратного проектирования и тестирования безопасности.

Kali Linux — полностью упакованный дистрибутив Linux для тестирования на проникновение на основе Debian.

BackBox Linux — упрощенный дистрибутив для тестирования на проникновение, основанный на Ubuntu.

CAINE — Computer Aided INvestigative Environment — это действующий дистрибутив GNU/Linux, предназначенный для цифровой криминалистики.

DEFT Linux — Linux-дистрибутив Digital Evidence & Forensics Toolkit