Список инструментов BlackArch с описанием

Всего инструментов: 1410

Имя	Версия	Описание	Домашняя страница
0d1n	189.61913dc	Инструмент веб-безопасности для создания фаззинговых HTTP вводов, сделан на C с libCurl.	https://github.com/CoolerVoid/0d1n
0trace	1.5	Инструмент перечисления прыжков	http://jon.oberheide.org/0trace/
3proxy	0.7.1.2	Крошечный бесплатный прокси сервер.	http://3proxy.ru/
3proxy-win32	0.7.1.2	Крошечный бесплатный прокси сервер.	http://3proxy.ru/
42zip	42	Рекурсивная Zip архивная бомба.	http://blog.fefe.de/?ts=b6cea88d
acccheck	0.2.1	Инструмент для атаки на пароли по словарю, его целью является windows аутентификация посредством протокола SMB.	http://labs.portcullis.co.uk/tools/acccheck/
ace	1.10	ACE (Automated Corporate Enumerator — автоматизированный корпоративный перечислитель) — простой, но в то же время мощный инструмент для перебора корпоративной директории VoIP, который имитирует поведение IP телефона чтобы загрузить имя и расширенные записи, которые данный телефон может отобразить на своём экране.	http://ucsniff.sourceforge.net/ace.html
admid-pack	0.1	Инструменты спуфинга ADM DNS - Используют различные активные и пассивные методы для спуфа DNS пакетов. Очень мощный.	http://packetstormsecurity.com/files/10080/ADMid-pkg.tgz.html
adminpagefinder	0.1	Этот скрипт на python для поиска админок на заданном сайте.	http://packetstormsecurity.com/files/112855/Admin-Page-Finder-Script.html
admsnmp	0.1	Аудит сканер ADM SNMP.	
aesfix	1.0.1	Инструмент для поиска AES ключа в RAM	http://citp.princeton.edu/memory/code/
aeskeyfind	1.0	Инструмент для поиска AES ключа в RAM	http://citp.princeton.edu/memory/code/
aespipe	2.4d	Читает данные из стандартного ввода и выводит зашифрованные или расшифрованные результаты в стандартный вывод.	http://loop-aes.sourceforge.net/aespipe/
aesshell	0.7	Шэлл с обратной связью для Windows и Unix, написан на python и использует AES в режиме CBC в сочетании с HMAC-SHA256 для безопасного обмена данными.	https://packetstormsecurity.com/files/132438/AESshell.7.html
afflib	3.7.4	Расширяемый открытый формат для хранения образов дисков и связанной криминалистической информацией.	http://www.afflib.org
afl	2.10b	Фаззлер ориентированный на безопасность, использует инструментарий compile-time и генетические алгоритмы.	http://lcamtuf.coredump.cx/afl/
afpfs-ng	0.8.1	Клиент для Apple Filing Protocol (AFP)	http://alexthepuffin.googlepages.com/
against	0.2	Очень быстрый скрипт атаки на ssh, который включает многопотоковый модуль сканирования портов (tcp подключение) для обнаружения возможных целей и модуль	http://nullsecurity.net/tools/cracker.html

Имя	Версия	Описание	Домашняя страница
		многопотокового брутфорсинга, который атакует параллельно все обнаруженные хосты данных IP адресов из списка.	
aggroargs	50.d56728a	Брутфорсит переполнения буфера командной строки linux, агрессивные аргументы.	https://github.com/tintinweb/aggroArgs
aiengine	486.0311753	Движок анализа пакетов с возможностью обучения без вмешательства человека.	https://bitbucket.org/camp0/aiengine/
aimage	3.2.5	Программа для создания образов aff.	http://www.afflib.org
air	2.0.0	Внешний графический интерфейс dd/dc3dd созданный для простого создания криминалистических образов.	http://air-imager.sourceforge.net/
aircrack-ng	1.2rc4	Взломщик ключей для протоколов 802.11 WEP и WPA-PSK.	http://www.aircrack-ng.org
airflood	0.1	Модицикация aireplay, которая позволяет DOS'ить ТД. Эта программа заполняет таблицу клиенто ТД со случайными MAC, делая подключения невозможными.	http://packetstormsecurity.com/files/51127/airflood.1.tar.gz.html
airgraph-ng	2853	Инструмент графиков для пакета aircrack.	http://www.aircrack-ng.org
airoscript	45.0a122ee	Скрипт, который упрощает использование инструментов aircrack-ng.	http://midnightresearch.com/projects/wicrawl/
airpwn	1.4	Инструмент для генерации пакетов для инжекта в сеть 802.11.	http://airpwn.sourceforge.net
albatar	16.5c48c6a	Фреймворк эксплуатирования SQLi на Python.	https://github.com/lanjelot/albatar
allthevhosts	1.0	Инструмент обнаружения виртуальных хостов (сайтов на одном IP), который выскабливает различные веб-приложения.	http://labs.portcullis.co.uk/tools/finding-all-the-vhosts/
androguard	786.309aa68	Обратная инженерия, Анализ зловредных и хороших программ под Android и другое.	https://github.com/androguard/androguard
androick	5.35048d7	Инструмент на python для помощи в криминалистическом анализе на android.	https://github.com/Flo354/Androick
android-apktool	2.0.3	Инструмент для реинжиниринга файлов Android apk.	http://forum.xda-developers.com/showthread.php?t=1755243
android-ndk	r9c	Android C/C++ developer kit.	http://developer.android.com/sdk/ndk/index.html
android-sdk-platform-tools	r23.0.1	Platform-Tools для Google Android SDK (adb и fastboot).	http://developer.android.com/sdk/index.html
android-sdk	r24.4.1	Google Android SDK.	http://developer.android.com/sdk/index.html
android-udev-rules	205.9af6e55	Правила Android udev.	https://github.com/bbqlinux/android-udev-rules
androidpincrack	2.ddaf307	Брутфорс кода доступа Android из данного хеша и соли.	https://github.com/PentesterES/AndroidPINCrack
androidsniffer	0.1	Скрпипт на perl, который позволяет вам искать сторонние пароли, дампы логов звонков, дампы контактов, дампы беспроводных настроект и другое.	http://packetstormsecurity.com/files/97464/Andr01d-Magic-Dumper.1.html
angr	2782.c8f86ec	Платформа анализа исполнимых данных следующего поколения от UC Santa Barbara's Seclab.	https://github.com/angr/angr
anontwi	1.1b	Бесплатный программыний клиент на python, созданный для анонимной навигации в социальных сетях. Он поддерживает Identi.ca и Twitter.com.	http://anontwi.sourceforge.net/
apache-users	2.1	Скрипт на perl для перебора имён	https://labs.portcullis.co.uk/downloads/

Имя	Версия	Описание	Домашняя страница
		пользователей на системах unix, которые используют модуль apache UserDir.	
aphopper	0.3	AP Hopper - это программа, которая автоматически прыгает между точками доступа различных беспроводных сетей.	http://aphopper.sourceforge.net/
api-dnsdumpster	24.310488c	Неофициальные Python API для http://dnsdumpster.com/.	https://github.com/PaulSec/API-dnsdumpster.com
apnbf	0.1	Маленький скрипт на python, созданный для перебора валидных APN (Access Point Name - имени точки доступа) на устройствах для разговора GTP-C.	http://www.c0decafe.de/
arachni	1.4.4.gcd7b47b	Многофункциональный, модульный, высокопроизводительный фреймворк на Ruby, цель которого поддержать тестеров на проникновение и администраторов в оценке безопасности веб-приложений.	https://www.arachni-scanner.com
aranea	6.469b9ee	Быстрый и чистый инструмент сфуфинга dns.	https://github.com/TigerSecurity
arduino	1.0.5	Arduino SDK (включает патченные avrdude и librxtx)	http://arduino.cc/en/Main/Software
argus	3.0.8.1	Инструмент сетевого мониторинга с контролем потока.	http://qosient.com/argus/
argus-clients	3.0.8	Клиент сетевого мониторинга для Argus.	http://qosient.com/argus/
armitage	150813	Графический инструмент управления кибер атаками для Metasploit.	http://www.fastandeasyhacking.com/
armscgen	75.fdf2ff3	Генератор ARM Shellcode (в основном режим Thumb).	https://github.com/alexpark07/ARMSCGen
arp-scan	1.9	Инструмент, который использует ARP для обнаружения и снятия отпечатков с IP хостов локальной сети.	http://www.nta-monitor.com/tools/arp-scan/
arpalert	2.0.12	Монотир изменений ARP в ethernet сетях.	http://www.arpalert.org/
arpoison	0.7	UNIX утилита обновления arp кэша.	http://www.arpoison.net
arpon	2.7	Портативный обработчик демона, который делает ARP протокол безопасным, чтобы избежать атаку Man In The Middle (MITM) (человек-посередине) через ARP сфуфинг, атак травления ARP кэша или травления маршрутов ARP.	http://arpon.sourceforge.net/
arpwner	26.f300fdf	Основанный на графическом интерфейсе инструмент на python для атак arp травления и dns травления.	https://github.com/ntrippar/ARPwner
artillery	163.e9ef627	Комбинация приманки, мониторинга файловой системы, укрепителя системы и улучшения общего здоровья сервера для создания комплексного способа обезопасить систему.	https://www.trustedsec.com/downloads/artillery/
asleap	2.2	Активный восстановитель паролей LEAP/PPTP.	http://www.willhackforsushi.com/Asleap.html
asp-audit	2BETA	Инструмент снятия отпечатков ASP и сканер уязвимостей.	http://seclists.org/basics/2006/Sep/128
atftp	0.7.1	Реализация клиент/сервер протокола TFTP, который реализует RFCs 1350, 2090, 2347, 2348 и 2349	http://sourceforge.net/projects/atftp/
athena-ssl-scanner	0.6.2	Сканер шифра SSL, который проверяет все коды шифра. Он может идентифицировать примерно 150 различных шифров.	http://packetstormsecurity.com/files/93062/Athena-SSL-Cipher-Scanner.html
atscan	457.2fe5778	Сканер серверов, сайтов и дорков.	https://github.com/AlisamTechnology/AT

Имя	Версия	Описание	Домашняя страница
			SCAN-V3.1
atstaketools	0.1	Это архив различных инструментов @Stake, которые помогают выполнить сканирование уязвимостей и анали, сбор информации, аудит паролей и криминалистику.	http://packetstormsecurity.com/files/50718/AtStakeTools.zip.html
auto-xor-decryptor	5.1f552be	Автоматический инструмент XOR расшифровки.	http://www.blog.mrg-effitas.com/publishing-of-mrg-effitas-automatic-xor-decryptor-tool/
autopsy	2.24	Графический инструмент для Sleuth Kit.	http://www.sleuthkit.org/autopsy
autopwn	177.2f3f605	Укажите цель и запустите в отношении неё набор инструментов.	https://github.com/nccgroup/autopwn
azazel	12.16ca8ac	Руткит пользовательского окружения основанный на оригинальной LD_PRELOAD технике от Jynx rootkit.	https://github.com/chokepoint/azazel
b2sum	27.1c2b66c	Проверка хеш суммы файлов BLAKE2. Вычисляет криптографический хеш заданных файлов BLAKE2 (BLAKE2b или -s, -bp, -sp).	https://blake2.net/
backcookie	45.35fb0a3	Маленький бэкдор использующий куки.	https://github.com/mrjopino/backcookie
backdoor-factory	170.988f010	Патчит бинарные файлы win32/64 шэллкодом.	https://github.com/secretsquirrel/the-backdoor-factory
backdoorme	191.49b79e1	Мощная утилита способная бэкдорить Unix машины множеством бэкдоров.	https://github.com/Kkevsterrr/backdoorme
backfuzz	36.8e54ed6	Набор для фаззинга сетевых протоколов.	https://github.com/localh0t/backfuzz
balbuzard	67.d6349ef1bc55	Пакет инструментов вредоносных программ на python для извлечения интересных образцов подозрительных файлов (IP адреса, доменные имена, известные заголовки файлов, интересные строки и т.д.).	https://bitbucket.org/decalage/balbuzard/
bamf-framework	35.30d2b4b	Модульный фреймворк, созданный быть платформой для запуска атак в отношении ботнетов.	https://github.com/bwall/BAMF
base64dump	0.0.4	Извлекает и декодирует строки в base64 из файлов.	http://blog.didierstevens.com/2015/10/12/update-base64dump-py-version-0-3/
basedomainname	0.1	Инструмент для извлечения TLD (Top Level Domain - домена верхнего уровня),доменных расширений (Second Level Domain (домена второго уровня) + TLD), доменного имени и имени хоста из полностью определённого имени доменов.	http://www.morningstarsecurity.com/research
batctl	2016.0	B.A.T.M.A.N. продвинутый инструмент контроля и управления объединёнными сетями.	http://www.open-mesh.net/
batman-adv	2016.0	Модуль ядра Batman, (включён начиная с .38)	http://www.open-mesh.net/
batman-alfred	2016.0	Демон для децентрализованного распространения произвольной информации по сцепленным и не сцепленным сетям.	http://www.open-mesh.org/
bbqsql	259.4f7c086	Инструмент эксплуатации SQL инъекций.	https://github.com/neohapsis/bbqsql
bbscan	9.655a258	Крошечный скрипт для сканирования веб уязвимостей.	https://github.com/lijiejie/bbscan
bdfproxy	85.221d075	Патчит бинарники посредством MITM: BackdoorFactory + mitmProxy	https://github.com/secretsquirrel/BDFProxy
bdlogparser	1	Это утилита для парсинга лог файлов Bit Defender, чтобы отсортировать их в архив злонамеренного программного обеспечения для упрощённой поддержки вашей коллекции зловредов.	http://magikh0e.xyz/

Имя	Версия	Описание	Домашняя страница
bed	0.5	Коллекция скриптов для тестирования переполнения буффера, строковый формат уязвимостей.	http://www.aldeid.com/wiki/Bed
beef	0.4.7.0.157.g0e8e076	Фреймворк, который фокусируется на веб-браузерах.	http://beefproject.com/
beeswarm	1157.9793ae5	Делает простым развёртывание приманки http://www.beeswarm-ids.org/	https://github.com/honeynet/beeswarm/
beholder	0.8.10	Инструмент выявления беспроводного вторржения, он следит за аномалиями в wifi среде.	http://www.beholderwireless.org/
beleth	36.0963699	Многопотоковый взломщик SSH атакой по словарю.	https://github.com/chokepoint/Beleth
bettercap	781.dc2a01f	Законченный, модульный, портативный и легко расширяемый фреймворк MITM.	https://github.com/evilsocket/bettercap
bfbtester	2.0.1	Выполняет проверку единичного или множества аргументов командной строки на переполнение и переполнение переменной среды.	http://sourceforge.net/projects/bfbtester/
bgp-md5crack	0.1	Взломщик паролей RFC2385	http://www.c0decafe.de/
binaryninja-python	12.15ad8c2	Бинарный прототип Ninja, написанный на Python.	https://github.com/Vector35/binaryninja-python
bind-tools	9.10.4	Инструменты ISC DNS.	http://www.isc.org/software/bind/
bindead	4504.67019b9	Статичный анализ бинарников.	https://bitbucket.org/mihaila/bindead
bindiff	4.2.0	Инструмент сравнения бинарных файлов, который содействует исследователям уязвимостей и инжинерам в быстром поиске различий и схожестей в дизассемблированном коде.	http://www.zynamics.com/bindiff.html
binex	1.0	Инструмент построения формата строки эксплойта.	http://www.morxploit.com/morxtool
binflow	4.c4140d7	Трейсер функций POSIX. Намного лучше и быстрее чем ftrace.	https://github.com/elfmaster/binflow
bing-ip2hosts	0.4	Перечисляет все номера хостов, которые Bing проиндексировал для конкретного IP адреса. [Программа больше не работает!]	http://www.morningstarsecurity.com/research/bing-ip2hosts
bing-lfi-rfi	0.1	Это скрипт на python script для поиска по Bing сайтов, которые могут иметь локальные и удалённые файлы с уязвимостями.	http://packetstormsecurity.com/files/121590/Bing-LFI-RFI-Scanner.html
binnavi	6.1.0	Интегрированная среда разработки бинарного анализа, позволяет контролировать, управлять, редактировать и аннотировать графики управления потоком и графики вызова дизассемблированного кода.	https://github.com/google/binnavi
binwalk	2.1.1	Инструмент для поиска данного бинарного образа включённых файлов.	http://binwalk.org
binwally	4.0aabd8b	Инструмент для сравнения бинарников и дерева каталога в поиска изменений, использует концепт Fuzzy Hashing (ssdeep).	https://github.com/bmaia/binwally
bios_memimage	1.2	Инструмент для дампа содержимого RAM на диск (aka атака холодная загрузка).	http://citp.princeton.edu/memory/code/
birp	60.1d7c49f	Инструмент, который будет ассестировать в оценке безопасности приложений менжфреймов работающих на TN3270.	https://github.com/sensepost/birp
bitdump	34.6a5cbd8	Инструмент для извлечения базы данных из	https://github.com/nbshelton/bitdump

Имя	Версия	Описание	Домашняя страница
		уязвимости слепая SQL инъекция.	
bittwist	2.0	Простой, но мощный, генератор Ethernet пакетов, основан на libpcap. Он создан для дополнения tcpdump, который сам по себе проделал отличную работу по захвату сетевого трафика.	http://bittwist.sourceforge.net/
bkhive	1.1.1	Программа для дампа syskey bootkey из системного улья Windows NT/2K/XP.	http://sourceforge.net/projects/ophcrack
blackarch-menus	0.2	Особое меню BlackArch, совместимо с XDG.	http://www.blackarch.org/
blackarch-mirrorlist	20150529	Список зеркал проекта BlackArch для использования в pacman	
blackhash	0.2	Создаёт фильтры из системных хешей.	http://16s.us/blackhash/
bletchley	0.0.1	Коллекция криптоаналитических инструментов прикладного назначения.	https://code.google.com/p/bletchley/
blindelephant	7	Снимательь отпечатков веб-приложений. Пытается обнаружить версию (известного) веб-приложения сравнением статичных файлов в известных расположениях.	http://blindelephant.sourceforge.net/
blindsql	1.0	Набор Bash скриптов для слепых атак SQL инъекций	http://www.enye-sec.org/programas.html
bluebox-ng	0.1.8	Сканер уязвимостей GPL VoIP/UC.	https://github.com/jesusprubio/bluebox-ng
bluebugger	0.1	Реализация техники bluebug, которая открыта Martin Herfurt.	http://packetstormsecurity.com/files/54024/bluebugger.1.tar.gz.html
bluediving	0.9	Набор инструментов для тестирования на проникновение Bluetooth.	http://bluediving.sourceforge.net/
bluelog	1.1.2	Сканер и сниффер Bluetooth, написанный для выполнения единичной задачи - лог видимых устройств.	http://www.digifail.com/software/bluelog.shtml
bluepot	0.1	Bluetooth приманка, написанная на Java, работает на Linux	https://code.google.com/p/bluepot/
blueprint	0.1_3	Инструмент на perl для идентификации Bluetooth устройств.	http://trifinite.org/trifinite_stuff_blueprinting.html
blueranger	1.0	Простой Bash скрипт, который использует Link Quality для локации радиуста устройства Bluetooth.	http://www.hackfromacave.com/projects/blueranger.html
bluescan	1.0.6	Сканер устройств Bluetooth.	http://www.darknet.org.uk/2015/01/bluescan-bluetooth-device-scanner/
bluesnarfer	0.1	Инструмент атаки bluetooth.	http://www.alighieri.org/project.html
bluto	134.8defadb	Разведка, брут субдоменов, зоны передачи.	https://github.com/RandomStorm/Bluto
bmap-tools	3.2	Инструмент для копирования больших разрежанных файлов, используя информацию из блока карты файла.	http://git.infradead.org/users/dedekind/bmap-tools.git
bob-the-butcher	0.7.1	Пакет распределённого взломщика паролей.	http://btb.banquise.net/
bokken	1.8	Графический интерфейс для radare2 и pyew.	http://inguma.eu/projects/bokken/
bowcaster	172.a2b084f	Фреймворк, нацеленный на помощь разработчикам эксплойтов, путём предоставления полезного набора инструментов и модулей, таких как payloads, encoders, connect-back servers, etc. В настоящее время фреймворк фокусируется на архитектуре MIPS CPU, но конструкция предназначена быть достаточно модульной для поддержки других архитектур.	https://github.com/zcutlip/bowcaster

Имя	Версия	Описание	Домашняя страница
braa	0.82	Массовый сканер snmp.	http://s-tech.elsat.net.pl/braa/
braces	0.4	Утилита отслеживания Bluetooth.	http://braces.shmoo.com/
bro	2.4.1	Мощный фреймворк анализа сетей, который отличается от типичных систем обнаружения вторжений, которые вам знакомы.	https://www.bro.org/download/index.html
browser-fuzzer	3	Браузерный фаззер 3	http://www.krakowlabs.com/dev.html
brutessh	0.6	Простой брутфорсер паролей sshd, использующий словарь, он очень быстрый для интернет сетей. Мультипотоковый.	http://www.edge-security.com/edge-soft.php
brutex	43.6c199b1	Автоматический брутфорс всех служб запущенных на цели.	https://github.com/1N3/BruteX
brutus	2	Один из самых быстрых, гибких удалённых взломщиков паролей, который вы можете иметь.	http://www.hoobie.net/brutus/
bsdiff	4.3	bsdiff и bspatch - это инструменты для сборки и применения патчей к бинарным файлам.	http://www.daemonology.net/bsdiff/
bsqlbf	2.7	Брутфорсер слепой SQL инъекции.	http://code.google.com/p/bsqlbf-v2/
bsqlinjector	7.e1be4cf	Инструмент эксплуатации слепой SQL инъекции, написанный на ruby.	https://github.com/enjoiz/BSQLinjector
bss	0.8	Засоритель / фаззер стэка Bluetooth.	http://www.secuobs.com/news/15022006-bss_0_8.shtml
bt_audit	0.1.1	Аудит Bluetooth.	http://www.betaversion.net/btdsd/download/
btcrack	1.1	Первый в мире инструмент брутфорса пароля (PIN) Bluetooth. Брутфорсит Passkey и Link key из захваченного обмена при сопряжении.	http://www.nruns.com/_en/security_tools_btcrack.php
btscanner	2.1	Сканер устройств Bluetooth.	http://www.pentest.co.uk
bulk-extractor	1.5.5	Инструмент извлечения массы Email и URL.	https://github.com/simsong/bulk_extractor
bully	21.388df45	Инструмент для брутфорса wifi-protected-setup (WPS).	http://code.google.com/p/bully/
bunny	0.93	Слепой к протоколу фаззлер общего назначения и замкнутого цикла с высокой производительностью для программ C.	http://code.google.com/p/bunny-the-fuzzer/
burpsuite	1.6.32	Интегрированная платформа для атаки веб-приложений (бесплатное издание).	http://portswigger.net/burp/
buttinsky	138.1a2a1b2	Обеспечивает фреймворк с открытым кодом для автоматизированного мониторинга ботнета.	https://github.com/buttinsky/buttinsky
bvi	1.4.0	Ориентированный на дисплей редактор для бинарных файлов, работает как редактор "vi".	http://bvi.sourceforge.net/
bytecode-viewer	205.45c8bb4	Набор для обратного инженеринга Java 8/Android APK.	https://github.com/Konloch/bytecode-viewer
cadaver	0.23.3	Клиент командной строки WebDAV под Unix	http://www.webdav.org/cadaver
camscan	1.0057215	Инструмент, который анализирует CAM таблицу коммутаторов Cisco в поисках аномалий.	https://github.com/securestate/camscan
canari	1.1	Трансформирующий фреймворк для maltego.	http://www.canariproject.com/
cangibrina	114.57dc151	Поисковик админок / панелей управления.	https://github.com/fnk0c/cangibrina
cansina	139.47f6ac8	Инструмент поиска контента, основанный на python.	https://github.com/deibit/cansina
capstone	3.0.4	Легковесный мультиплатформенный, мультиархитектурных фреймворк дизассемблирования.	http://www.capstone-engine.org/index.html

Имя	Версия	Описание	Домашняя страница
captipper	66.98d63eb	Инструмент исследования вредоносного HTTP трафика.	http://www.omriher.com/2015/01/captipper-malicious-http-traffic.html
carwhisperer	0.2	Предназначен для анализа устройств громкой связи и другой Bluetooth техники без дисплея и клавиатуры на возможные угрозы безопасности от использования стандартных паролей.	http://trifinite.org/trifinite_stuff_carwhisperer.html
casefile	1.0.1	Младший брат Maltego без transforms, но комбинирует графический и ссылочный анализ для проверки связей между вручную добавленными данными для составления мысленной карты вашей информации	http://www.paterva.com/web6/products/casefile.php
catnthecanary	7.e9184fe	Приложение для запроса наборов данных с canary.pw в поисках утёкших данных.	https://github.com/packetassailant/catnthecanary
cdpsnarf	0.1.6	Сниффер протокола обнаружения Cisco (CDP).	https://github.com/Zapotek/cdpsnarf
cecster	5.15544cb	Инструмент для выполнения тестирования безопасности в отношении протоколов HDMI CEC (Consumer Electronics Control) и HEC (HDMI Ethernet Channel).	https://github.com/nccgroup/CECster
centry	72.6de2868	Защита Cold boot & DMA	https://github.com/0xPoly/Centry
cewl	5.1	Генератор пользовательского списка слов.	http://www.digininja.org/projects/cewl.php
cflow	1.4	Анализатор потока C программ.	http://www.gnu.org/software/cflow/
changeme	38.d8f589d	Сканер дефолтных учётных данных.	https://github.com/ztgrace/changeme
chaosmap	1.3	Инструмент сбора информации и сканер dns / whois / веь-серверов	http://freecode.com/projects/chaosmap
chaosreader	0.94	Бесплатный инструмент для трассировки tcp, udp и т.п. сессий и получения данных из логов snoop или tcpdump.	http://chaosreader.sourceforge.net/
chapcrack	17.ae2827f	Инструмент для парсинга и расшифровки сетевых рукопожатий MS-CHAPv2.	https://github.com/moxie0/chapcrack
check-weak-dh-ssh	0.1	Debian OpenSSL weak client Diffie-Hellman Exchange checker.	http://packetstormsecurity.com/files/66683/check_weak_dh_ssh.pl.bz2.html
checkiban	0.2	Checks the validity of an International Bank Account Number (IBAN).	http://kernel.embedromix.ro/us/
checkpwd	1.23	Oracle Password Checker (Cracker).	http://www.red-database-security.com/software/checkpwd.html
checksec	1.5	Tool designed to test which standard Linux OS and PaX security features are being used	http://www.trapkit.de/tools/checksec.html
cheetah-suite	21.2364713	Complete penetration testing suite (port scanning, brute force attacks, services discovery, common vulnerabilities searching, reporting etc.)	https://github.com/bl4de/Cheetah
chiron	0.9	Фреймворк всё-в-одном тестирования на проникновение IPv6.	http://www.secfu.net/tools-scripts/
chkrootkit	0.50	Checks for rootkits on a system	http://www.chkrootkit.org/
chntpw	140201	Offline NT Password Editor - reset passwords in a Windows NT SAM user database file	http://pogostick.net/~pnh/ntpasswd/
chownat	0.08b	Allows two peers behind two separate NATs with no port forwarding and no DMZ setup on their routers to directly communicate with each other	http://samy.pl/chownat/
chrome-decode	0.1	Chrome web browser decoder tool that demonstrates recovering passwords.	http://packetstormsecurity.com/files/119153/Chrome-Web-Browser-Decoder.html
chromefreak	24.12745b1	A Cross-Platform Forensic Framework for Google Chrome	http://osandamalith.github.io/ChromeFreak/

Имя	Версия	Описание	Домашняя страница
chromensics	1.0	Криминалистический инструмент Google chrome.	https://sourceforge.net/projects/chromensics/
chw00t	31.19a0726	Unices chroot breaking tool.	https://github.com/earthquake/chw00t
cidr2range	0.9	Script for listing the IP addresses contained in a CIDR netblock	http://www.cpan.org/authors/id/R/RA/RAYNERLUC
cintruder	0.2.0	An automatic pentesting tool to bypass captchas.	http://cintruder.sourceforge.net/
cipherscan	357.5d930c2	Очень простой способ узнать, какие наборы шифров SSL поддерживаются на цели.	https://github.com/jvehent/cipherscan
ciphertest	20.3224858	A better SSL cipher checker using gnutls.	https://github.com/OpenSecurityResearch/ciphertest
ciphr	105.db79691	A CLI tool for encoding, decoding, encryption, decryption, and hashing streams of data.	https://github.com/frohoff/ciphr
cirt-fuzzer	1.0	A simple TCP/UDP protocol fuzzer.	http://www.cirt.dk/
cisco-auditing-tool	1	Perl script which scans cisco routers for common vulnerabilities. Checks for default passwords, easily guessable community names, and the IOS history bug. Includes support for plugins and scanning multiple hosts.	http://www.scrypt.net
cisco-global-exploiter	1.3	A perl script that targets multiple vulnerabilities in the Cisco Internetwork Operating System (IOS) and Catalyst products.	http://www.blackangels.it
cisco-ocs	0.2	Cisco Router Default Password Scanner.	http://www.question-defense.com/2013/01/11/ocs-version-2-release-ocs-cisco-router-default-password-scanner
cisco-router-config	1.1	copy-router-config and merge-router-config to copy and merge Cisco Routers Configuration	
cisco-scanner	0.2	Multithreaded Cisco HTTP vulnerability scanner. Tested on Linux, OpenBSD and Solaris.	http://wayreth.eu.org/old_page/
cisco-snmp-enumeration	10.ad06f57	Automated Cisco SNMP Enumeration, Brute Force, Configuration Download and Password Cracking.	https://github.com/nccgroup/cisco-snmp-enumeration
cisco-snmp-slap	5.daf0589	IP address spoofing tool in order to bypass an ACL protecting an SNMP service on Cisco IOS devices.	https://github.com/nccgroup/cisco-snmp-slap
cisco-torch	0.4b	Cisco Torch mass scanning, fingerprinting, and exploitation tool.	http://www.arhont.com
cisco5crack	2.c4b228c	Crypt and decrypt the cisco enable 5 passwords.	https://github.com/madrisan/cisco7crack
cisco7crack	2.f1c21dd	Crypt and decrypt the cisco enable 7 passwords.	https://github.com/madrisan/cisco7crack
ciscos	1.3	Scans class A, B, and C networks for cisco routers which have telnet open and have not changed the default password from cisco.	
clamscanlogparser	1	This is a utility to parse a Clam Anti Virus log file, in order to sort them into a malware archive for easier maintanence of your malware collection.	http://magikh0e.xyz/
climber	30.5530a78	Проверяет системы UNIX/Linux на повышение привелегий.	https://github.com/raffaele-forte/climber
cloudflare-enum	9.c1d8fca	Cloudflare DNS Enumeration Tool for Pentesters.	https://github.com/mandatoryprogrammer/cloudflare_enum
cloudget	53.807d08e	Python script to bypass cloudflare from command line. Built upon cfscrape module.	https://github.com/eudemonics/cloudget
clusterd	143.d190b2c	Automates the fingerprinting, reconnaissance, and exploitation phases of an application server attack.	https://github.com/hatRiot/clusterd

Имя	Версия	Описание	Домашняя страница
cmospwd	5.0	Decrypts password stored in CMOS used to access BIOS setup.	http://www.cgsecurity.org/wiki/CmosPwd
cms-explorer	1.0	Designed to reveal the specific modules, plugins, components and themes that various cms driven websites are running	http://code.google.com/p/cms-explorer
cms-few	0.1	Joomla, Mambo, PHP-Nuke, and XOOPS CMS SQL injection vulnerability scanning tool written in Python.	http://packetstormsecurity.com/files/64722/cms_few.py.txt.html
cmsfuzz	5.6be5a98	Fuzzer for wordpress, cold fusion, drupal, joomla, and phpnuke.	https://github.com/nahamsec/CMSFuzz
cmsmap	3.37b64be	A python open source Content Management System scanner that automates the process of detecting security flaws of the most popular CMSs.	https://www.dionach.com/blog/cmsmap-%E2%80%93-a-simple-cms-vulnerability-scanner
cnamulator	5.4667c68	Утилита поиска телефонных номеров CNAM используя OpenCNAM API.	https://github.com/packetassailant/cnamulator
codetective	39.7f44df4	A tool to determine the crypto/encoding algorithm used according to traces of its representation.	https://www.digitalloft.org/init/plugin_wiki/page/codetective
commix	492.4decdec	Автоматизированный инструмент всё-в-одном для инъекции команд и эксплуатации ОС.	https://github.com/stasinopoulos/commix
complemento	0.7.6	A collection of tools for pentester: LetDown is a powerful tcp flooder ReverseRaider is a domain scanner that use wordlist scanning or reverse resolution scanning Httsquash is an http server scanner, banner grabber and data retriever	http://complemento.sourceforge.net
configpush	0.8.5	This is a tool to span /8-sized networks quickly sending snmpset requests with default or otherwise specified community string to Cisco devices.	http://packetstormsecurity.com/files/126621/Config-Push-snmpset-Utility.html
conpot	0.5.1	ICS приманка, нацелена на сбор разведданных о мотивах и методах противников, ориентированных на промышленные системы управления.	http://conpot.org
conscan	1.2	A blackbox vulnerability scanner for the Concre5 CMS.	http://nullsecurity.net/tools/scanner.html
cookie-cadger	1.08	An auditing tool for Wi-Fi or wired Ethernet connections.	https://cookiecadger.com/
corkscrew	2.0	A tool for tunneling SSH through HTTP proxies	http://www.agroman.net/corkscrew/
cowpatty	4.6	Wireless WPA/WPA2 PSK handshake cracking utility	http://www.wirelessdefence.org/Contents/Files/
cpfinder	0.1	This is a simple script that looks for administrative web interfaces.	http://packetstormsecurity.com/files/118851/Control-Panel-Finder-Script.html
cppcheck	1.73	Инструмент для статического анализа кода C/C++	http://cppcheck.sourceforge.net/
cpptest	1.1.2	A portable and powerful, yet simple, unit testing framework for handling automated tests in C++.	http://cpptest.sourceforge.net/
crackhor	2.ae7d83f	A Password cracking utility.	https://github.com/CoalfireLabs/crackHOR
crackle	71.20215f8	Crack and decrypt BLE encryption	https://github.com/mikeryan/crackle/
crackmapexec	238.079cf69	Швейцарский нож для тестирования на проникновение окружения Windows/Active Directory.	https://github.com/byt3bl33d3r/CrackMapExec
crackq	48.89b7318	Взломщик паролей Hashcrack.org с использованием GPU.	https://github.com/vnik5287/Crackq
crackserver	33.e5763ab	An XMLRPC server for password cracking.	https://github.com/averagesecurityguy/cr

Имя	Версия	Описание	Домашняя страница
			ack
crawlic	45.38944f0	Инструмент веб-разведки (ищет временные файлы, парсит robots.txt, ищет каталоги, дорки google и ищет домены, хостящиеся на этом же сервере).	https://github.com/Ganapati/Crawlic
creak	17.e367b9f	Poison, reset, spoof, redirect MITM script.	https://github.com/codepr/creak
create_ap	203.ac87711	Скрипт создаёт Точку Доступа NAT или Bridged.	https://github.com/oblique/create_ap
creddump	0.3	A python tool to extract various credentials and secrets from Windows registry hives.	https://code.google.com/p/creddump/
credmap	69.080273f	The Credential mapper (картограф учётных данных) - это инструмент, который был создан для повышения информативности об опасности повторного использования учётных данных.	https://github.com/lightos/credmap
creds	17.1ec8297	Harvest FTP/POP/IMAP/HTTP/IRC credentials along with interesting data from each of the protocols.	https://github.com/DanMcInerney/creds.py
creepy	137.9f60449	A geolocation information gatherer. Offers geolocation information gathering through social networking platforms.	http://github.com/ilektrojohn/creepy.git
crosstool-ng	1.22.0	Универсальный генератор (кросс-)toolchain.	http://crosstool-ng.org/
crowbar	77.67293cc	Инструмент брутфорса, который может использоваться во время тестирования на проникновение. Он разработан для поддержки протоколов, которые в настоящий момент не поддерживаются в thc-hydra и других популярных инструментов брутфорсинга..	https://github.com/galkan/crowbar
crunch	3.6	A wordlist generator for all combinations/permutations of a given character set.	http://sourceforge.net/projects/crunch-wordlist/
crypthook	17.0728cd1	TCP/UDP symmetric encryption tunnel wrapper.	https://github.com/chokepoint/CryptHook
cryptonark	0.5.6	SSL security checker.	http://blog.techstacks.com/cryptonark.html
csrftester	1.0	The OWASP CSRFTester Project attempts to give developers the ability to test their applications for CSRF flaws.	http://www.owasp.org/index.php/Category:OWASP_CSRFTester_Project
ctunnel	0.7	Tunnel and/or proxy TCP or UDP connections via a cryptographic tunnel.	http://nardcore.org/ctunnel
cuckoo	2.0	Система анализа зловредов.	http://cuckoosandbox.org/
cudahashcat	2.01	Самый быстрый в мире взломщик WPA и других паролей, может использовать словарь, маску и другие виды атак.	http://hashcat.net/oclhashcat/
cupp	3.0	Common User Password Profiler	http://www.remote-exploit.org/?page_id=418
cutycapt	10	A Qt and WebKit based command-line utility that captures WebKit's rendering of a web page.	http://cutycapt.sourceforge.net/
cvechecker	3.5	The goal of cvechecker is to report about possible vulnerabilities on your system, by scanning the installed software and matching the results with the CVE database.	http://cvechecker.sourceforge.net/
cymothoa	1	A stealth backdooring tool, that inject backdoor's shellcode into an existing process.	http://cymothoa.sourceforge.net/
damm	30.5aa2a1e	Differential Analysis of Malware in Memory.	https://github.com/504ensicsLabs/DAM

Имя	Версия	Описание	Домашняя страница
			M
darkbing	0.1	A tool written in python that leverages bing for mining data on systems that may be susceptible to SQL injection.	http://packetstormsecurity.com/files/111510/darkBing-SQL-Scanner.1.html
darkd0rk3r	1.0	Python script that performs dork searching and searches for local file inclusion and SQL injection errors.	http://packetstormsecurity.com/files/117403/Dark-D0rk3r.0.html
darkjumper	5.8	This tool will try to find every website that host at the same server at your target	http://sourceforge.net/projects/darkjumper/
darkmysqli	1.6	Multi-Purpose MySQL Injection Tool	https://github.com/BlackArch/darkmysqli
darkstat	3.0.719	Network statistics gatherer (packet sniffer)	http://dmr.ath.cx/net/darkstat/
dartspylru	7.5ef01b1	Simple dictionary with LRU behaviour.	https://pypi.python.org/pypi/darts.util.lru
davoset	1.2.8	A tool for using Abuse of Functionality and XML External Entities vulnerabilities on some websites to attack other websites.	http://websecurity.com.ua/davoset/
davtest	1.0	Tests WebDAV enabled servers by uploading test executable files, and then (optionally) uploading files which allow for command execution or other actions directly on the target	http://code.google.com/p/davtest/
dbd	1.50	A Netcat-clone, designed to be portable and offer strong encryption. It runs on Unix-like operating systems and on Microsoft Win32.	https://github.com/gitdurandal/dbd
dbpwaudit	0.8	A Java tool that allows you to perform online audits of password quality for several database engines	http://www.cqure.net/wp/dbpwaudit/
dc3dd	7.2.641	A patched version of dd that includes a number of features useful for computer forensics.	http://sourceforge.net/projects/dc3dd
dcfldd	1.3.4.1	DCFL (DoD Computer Forensics Lab) dd replacement with hashing	http://dcfldd.sourceforge.net/
ddrescue	1.20	GNU data recovery tool	http://www.gnu.org/software/ddrescue/ddrescue.html
deblaze	0.3	A remote method enumeration tool for flex servers	http://deblaze-tool.appspot.com/
delldrac	0.1a	DellDRAC and Dell Chassis Discovery and Brute Forcer.	https://www.trustedsec.com/september/owning-dell-drac-awesome-hack/
delorean	7.68139d1	NTP Main-in-the-Middle tool.	https://github.com/PentesterES/Delorean
depant	0.3a	Check network for services with default passwords.	http://midnightresearch.com/projects/depant/
depdep	2.0	A merciless sentinel which will seek sensitive files containing critical info leaking through your network.	https://github.com/galkan/depdep
detect-it-easy	50.6ae37ad	Программа для определения типа файлов.	https://github.com/horsicq/Detect-It-Easy
device-pharmer	37.e0e6281	Opens 1K+ IPs or Shodan search results and attempts to login.	https://github.com/DanMcInerney/device-pharmer
dex2jar	2.0	A tool for converting Android's .dex format to Java's .class format	http://code.google.com/p/dex2jar
dff-scanner	1.1	Tool for finding path of predictable resource locations.	http://netsec.rs/70/tools.html
dhcdrop	0.5	Remove illegal dhcp servers with IP-pool underflow.	http://www.netpatch.ru/dhcdrop.html
dhcpf	2.96bc8a9	Passive DHCP fingerprinting implementation.	https://github.com/elceef/dhcpf
dhcpig	69.cc4109a	Enumerates hosts, subdomains, and emails from a given domain using google	https://github.com/kamorin/DHCPig
dinouml	0.9.5	A network simulation tool, based on UML (User Mode Linux) that can simulate big Linux	http://kernel.embedromix.ro/us/

Имя	Версия	Описание	Домашняя страница
		networks on a single PC	
dirb	2.22	A web content scanner, brute forceing for hidden files.	http://dirb.sourceforge.net/
dirbuster	1.0_RC1	An application designed to brute force directories and files names on web/application servers	http://www.owasp.org/index.php/Category:OWASP_DirBuster_Project
dirbuster-ng	9.0c34920	C CLI implementation of the Java dirbuster tool.	https://github.com/digination/dirbuster-ng
directorytraversalscan	1.0.1.0	Detect directory traversal vulnerabilities in HTTP servers and web applications.	http://sourceforge.net/projects/httpdirscan/
dirs3arch	151.e2ff186	HTTP(S) брутфорсер директорий/файлов.	https://github.com/maurosoria/dirs3arch
dirscanner	0.1	This is a python script that scans webservers looking for administrative directories, php shells, and more.	http://packetstormsecurity.com/files/117773/Directory-Scanner-Tool.html
dislocker	0.3	A tool to exploit the hash length extension attack in various hashing algorithms. With FUSE capabilities built in.	http://www.hsc.fr/ressources/outils/dislocker/
dissector	1	This code dissects the internal data structures in ELF files. It supports x86 and x86_64 archs and runs under Linux.	http://packetstormsecurity.com/files/125972/Coloured-ELF-File-Dissector.html
dissy	10	A graphical frontend to the objdump disassembler for compiler-generated code.	http://dissy.googlecode.com/
dizzy	0.8.3	A Python based fuzzing framework with many features.	http://www.c0decafe.de/
dmitry	1.3a	Deepmagic Information Gathering Tool. Gathers information about hosts. It is able to gather possible subdomains, email addresses, and uptime information and run tcp port scans, whois lookups, and more.	http://www.mor-pah.net/
dnmap	0.6	The distributed nmap framework	http://sourceforge.net/projects/dnmap/
dns-reverse-proxy	18.bb497e8	Обратный DNS прокси, написан на Go.	https://github.com/StalkR/dns-reverse-proxy
dns-spoof	12.3918a10	Yet another DNS spoof utility.	https://github.com/maurotfilho/dns-spoof
dns2geoip	0.1	A simple python script that brute forces DNS and subsequently geolocates the found subdomains.	http://packetstormsecurity.com/files/118036/DNS-GeoIP.html
dns2tcp	0.5.2	A tool for relaying TCP connections over DNS.	http://www.hsc.fr/ressources/outils/dns2tcp/index.html.en
dnsa	0.5	DNSA is a dns security swiss army knife	http://packetfactory.openwall.net/projects/dnsa/index.html
dnsbf	0.3	Search for available domain names in an IP range.	http://code.google.com/p/dnsbf
dnsbrute	2.b1dc84a	Multi-theaded DNS bruteforcing, average speed 80 lookups/second with 40 threads.	https://github.com/d4rkcat/dnsbrute
dnschef	0.3	A highly configurable DNS proxy for pentesters.	http://thesprawl.org/projects/dnschef/
dnsdrdos	0.1	Proof of concept code for distributed DNS reflection DoS.	http://nullsecurity.net/tools/dos.html
dnsenum	1.2.4.2	Script that enumerates DNS information from a domain, attempts zone transfers, performs a brute force dictionary style attack, and then performs reverse look-ups on the results.	http://www2.packetstormsecurity.org/cgi-bin/search/search.cgi?searchvalue=dnsenum
dnsfilexfer	14.20743e0	Передача файлов через DNS.	https://github.com/leonjza/dnsfilexfer
dnsgoblin	0.1	Nasty creature constantly searching for DNS servers. It uses standard dns querys and waits for the replies.	http://nullsecurity.net/tools/scanner.html
dnsmap	0.30	Passive DNS network mapper	http://dnsmap.googlecode.com

Имя	Версия	Описание	Домашняя страница
dnspredict	0.0.2	DNS prediction	http://johnny.ihackstuff.com
dnsrecon	0.8.9	Python script for enumeration of hosts, subdomains and emails from a given domain using google.	https://github.com/darkoperator/dnsrecon
dnsspider	0.7	A very fast multithreaded bruteforcer of subdomains that leverages a wordlist and/or character permutation.	http://nullsecurity.net/tools/scanner.html
dnsteal	21.634fee8	Инструмент DNS эксфильтрации для незаметной отправки файлов по запросам DNS.	https://github.com/m57/dnsteal
dnstracer	1.9	Determines where a given DNS server gets its information from, and follows the chain of DNS servers	http://www.mavetju.org/unix/dnstracer.php
dnstwist	151.c4215ef	Движок по пермутации доменных имён для выявления сквоттинга доменов с опечатками, фишинга и корпоративного шпионажа.	https://github.com/elceef/dnstwist
dnswalk	2.0.2	A DNS debugger	http://sourceforge.net/projects/dnswalk/
domain-analyzer	0.8.1	Finds all the security information for a given domain name.	http://sourceforge.net/projects/domainanalyzer/
domi-owned	23.4a39baa	Инструмент, используемый для компрометации серверов IBM/Lotus Domino.	https://github.com/coldfusion39/domi-owned
doona	135.9fa1f8d	Форк Bruteforce Exploit Detector Tool (BED).	https://github.com/wireghoul/doona
doork	4.3e2d70a	Пассивный аудитор уязвимостей.	https://github.com/AeonDave/doork
doozer	9.5cfc8f8	A Password cracking utility.	https://github.com/CoalfireLabs/crackHOR
dotdotpwn	3.0	The Transversal Directory Fuzzer	http://dotdotpwn.blogspot.com
dpeparser	beta002	Default password enumeration project	http://www.toolswatch.org/dpe/
dpscan	0.1	Drupal Vulnerabilty Scanner.	https://github.com/insaneisnotfree/Blue-Sky-Information-Security
dradis	3.0.0.rc1	Фреймворк с открытым исходным кодом для эффективного совместного доступа к информации.	http://dradisframework.org/
dragon-backdoor	7.c7416b7	A sniffing, non binding, reverse down/exec, portknocking service Based on cd00r.c.	https://github.com/Shellntel/backdoors
driftnet	1.1.5	Listens to network traffic and picks out images from TCP streams it observes.	http://www.ex-parrot.com/~chris/driftnet/
dripper	v1.r1.gc9bb0c9	A fast, asynchronous DNS scanner; it can be used for enumerating subdomains and enumerating boxes via reverse DNS.	http://www.blackhatlibrary.net/Dripper
droopescan	1.34.3	Основанный на плагинах сканер, который помогает исследователям безопасности выявить проблемы с несколькими системами управления контентом, преимущественно с Drupal и Silverstripe.	https://github.com/droope/droopescan
drozer	2.3.4	Фреймворк тестирования безопасности для Android - предварительно скомпилированные бинарники из официального репозитория.	https://github.com/mwrlabs/drozer
dscanner	768.c5392e7	Swiss-army knife for D source code.	https://github.com/Hackerpilot/Dscanner
dsd	91.7ee04e5	Digital Speech Decoder	https://github.com/szechyjs/dsd
dsfs	32.e27d6cb	A fully functional File inclusion vulnerability scanner (supporting GET and POST parameters) written in under 100 lines of code.	https://github.com/stamparm/DSFS
dsjs	21.79cb2c4	A fully functional JavaScript library vulnerability scanner written in under 100 lines of code.	https://github.com/stamparm/DSJS
dsniff	2.4b1	Collection of tools for network auditing and	http://www.monkey.org/~dugsong/dsniff/

Имя	Версия	Описание	Домашняя страница
		penetration testing	
dsss	116.6d14edb	A fully functional SQL injection vulnerability scanner (supporting GET and POST parameters) written in under 100 lines of code.	https://github.com/stamparm/DSSS
dsxs	116.21427d6	A fully functional Cross-site scripting vulnerability scanner (supporting GET and POST parameters) written in under 100 lines of code.	https://github.com/stamparm/DSXS
dumb0	19.1493e74	A simple tool to dump users in popular forums and CMS.	https://github.com/0verl0ad/Dumb0
dump1090	386.bff92c4	A simple Mode S decoder for RTLSDR devices.	https://github.com/MalcolmRobb/dump1090
dumpacl	0.0	Dumps NTs ACLs and audit settings.	http://www.systemtools.com/cgi-bin/download.pl?DumpAcl
dumpzilla	03152013	A forensic tool for firefox.	http://www.dumpzilla.org/
dvcs-ripper	44.a9d3afe	Rip web accessible (distributed) version control systems: SVN/GIT/…	https://github.com/kost/dvcs-ripper
eapeak	91.2afd560	Analysis Suite For EAP Enabled Wireless Networks.	https://github.com/securestate/eapeak
eapmd5pass	1.4	An implementation of an offline dictionary attack against the EAP-MD5 protocol	http://www.willhackforsushi.com/?page_id=67
easy-creds	3.9	A bash script that leverages ettercap and other tools to obtain credentials.	https://github.com/brav0hax/easy-creds
easyda	7.0867f9b	Easy Windows Domain Access Script.	https://github.com/nccgroup/easyda
easyfuzzer	3.6	A flexible fuzzer, not only for web, has a CSV output for efficient output analysis (platform independant).	http://www.mh-sec.de/downloads.html.en
eazy	0.1	This is a small python tool that scans websites to look for PHP shells, backups, admin panels, and more.	http://packetstormsecurity.com/files/117572/EAZY-Web-Scanner.html
ecfs	229.faf2fc2	Extended core file snapshot format.	https://github.com/elfmaster/ecfs
edb	0.9.20	A QT4-based binary mode debugger with the goal of having usability on par with OllyDbg.	http://www.codef00.com/projects.php#Debugger
eindeutig	20050628_1	Examine the contents of Outlook Express DBX email repository files (forensic purposes)	http://www.jonesdykstra.com/
elettra	1.0	Encryption utility by Julia Identity	http://www.winstonsmith.info/julia/elettra/
elettra-gui	1.0	Gui for the elettra crypto application.	http://www.winstonsmith.info/julia/elettra/
elfkickers	3.0a	Collection of ELF utilities (includes sstrip)	http://www.muppetlabs.com/~breadbox/software/elfkickers.html
elfparser	7.39d21ca	Cross Platform ELF analysis.	https://github.com/jacob-baines/elfparser
elite-proxy-finder	51.1ced3be	Находит публичные элитные анонимные прокси и одновременно испытывает их.	https://github.com/DanMcInerney/elite-proxy-finder
enabler	1	Attempts to find the enable password on a cisco system via brute force.	http://packetstormsecurity.org/cisco/enabler.c
encodeshellcode	0.1b	This is an encoding tool for 32-bit x86 shellcode that assists a researcher when dealing with character filter or byte restrictions in a buffer overflow vulnerability or some kind of IDS/IPS/AV blocking your code.	http://packetstormsecurity.com/files/119904/Encode-Shellcode.1b.html
ent	1.0	Pseudorandom number sequence test.	http://www.fourmilab.ch/random
enteletaor	59.9afdbdd	Инструмент очереди сообщения (Message Queue) и Сломанного инжекта (Broker Injection), который реализует атаки на Redis,	https://github.com/cr0hn/enteletaor

Имя	Версия	Описание	Домашняя страница
		RabbitMQ и ZeroMQ.	
enum-shares	7.97cba5a	Tool that enumerates shared folders across the network and under a custom user account.	https://github.com/dejanlevaja/enum_shares
enum4linux	0.8.9	A tool for enumerating information from Windows and Samba systems.	http://labs.portcullis.co.uk/application/enum4linux/
enumiax	1.0	An IAX enumerator.	http://sourceforge.net/projects/enumiax/
enyelkm	1.2	Rootkit for Linux x86 kernels v2.6.	http://www.enye-sec.org/programas.html
epicwebhoneypot	2.0a	Tool which aims to lure attackers using various types of web vulnerability scanners by tricking them into believing that they have found a vulnerability on a host.	http://sourceforge.net/projects/epicwebhoneypot/
erase-registrations	1.0	An IAX flooder.	http://www.hackingexposedvoip.com/
etherape	0.9.13	A graphical network monitor for various OSI layers and protocols	http://etherape.sourceforge.net/
ettercap	0.8.2	A network sniffer/interceptor/logger for ethernet LANs - console	http://ettercap.github.com/ettercap/
evilgrade	2.0.0	Modular framework that takes advantage of poor upgrade implementations by injecting fake updates	http://www.infobyte.com.ar/developments.html
evilize	0.2	Инструмент для создания бинарных MD5 коллизий.	http://www.mathstat.dal.ca/~selinger/md5collision/
evilmaid	1.01	TrueCrypt loader backdoor to sniff volume password	http://theinvisiblethings.blogspot.com
exabgp	3183.2c3afc6	Шведский нож для BGP сетей.	https://github.com/Exa-Networks/exabgp
exiv2	0.25	Exif, Iptc and XMP metadata manipulation library and tools	http://exiv2.org
expimp-lookup	4.79a96c7	Looks for all export and import names that contain a specified string in all Portable Executable in a directory tree.	https://github.com/tr3w/ExpImp-Lookup
exploit-db	1.6	The Exploit Database (EDB) – an ultimate archive of exploits and vulnerable software - A collection of hacks	http://www.exploit-db.com
exploitpack	4.88aeccd	Проект пакета эксплойтов	https://github.com/juansacco/exploitpack
extracthosts	14.ec8b89c	Извлекает хосты (IP/имена хостов) из файлов.	https://github.com/bwall/ExtractHosts
extundelete	0.2.4	Utility for recovering deleted files from ext2, ext3 or ext4 partitions by parsing the journal	http://extundelete.sourceforge.net
eyepwn	1.0	Exploit for Eye-Fi Helper directory traversal vulnerability	http://www.pentest.co.uk
eyewitness	487.b154878	Создана для создания скриншотов веб-сайтов, обеспечивает некоторую информацию о заголовке сервера и, если возможно, находит дефольтные учётные данные.	https://github.com/ChrisTruncer/EyeWitness
facebot	23.57f6025	A facebook profile and reconnaissance system.	https://github.com/pun1sh3r/facebot
facebrute	7.ece355b	This script tries to guess passwords for a given facebook account using a list of passwords (dictionary).	https://github.com/emerinohdz/FaceBrute
fakeap	0.3.2	Black Alchemy's Fake AP generates thousands of counterfeit 802.11b access points. Hide in plain sight amongst Fake AP's cacophony of beacon frames.	http://www.blackalchemy.to/project/fakeap/
fakedns	42.b67ecab	A regular-expression based python MITM DNS server with correct DNS request passthrough and "Not Found" responses.	https://github.com/Crypt0s/FakeDns
fakemail	1.0	Fake mail server that captures e-mails as files for	http://sourceforge.net/projects/fakemail/

Имя	Версия	Описание	Домашняя страница
		acceptance testing.	
fakenetbios	7.b83701e	A family of tools designed to simulate Windows hosts (NetBIOS) on a LAN.	https://github.com/mubix/FakeNetBIOS
fang	20.4b176f3	A multi service threaded MD5 cracker.	https://github.com/evilsocket/fang
faraday	2045.d0bf67a	Новый концептт (IPE) интегрированного окружения тестирования на проникновения многопользовательской IDE для тестирования на проникновение. Предназначена для распределения, учёта и анализа сгенерированных во время процесса аудита безопасности данныхt.	http://www.faradaysec.com/
fbht	68.1ffc236	A Facebook Hacking Tool	https://github.com/chinoogawa/fbht-linux
fbid	11.b8106f8	Show info about the author by facebook photo url.	https://github.com/guelfoweb/fbid
fcrackzip	1.0	Zip file password cracker	http://oldhome.schmorp.de/marc/fcrackzip.html
fern-wifi-cracker	222	WEP, WPA wifi cracker for wireless penetration testing	http://code.google.com/p/fern-wifi-cracker/
fernmelder	6.c6d4ebe	Asynchronous mass DNS scanner.	https://github.com/stealth/fernmelder
fgscanner	11.893372c	An advanced, opensource URL scanner.	http://www.fantaghost.com/fgscanner
fhttp	1.3	This is a framework for HTTP related attacks. It is written in Perl with a GTK interface, has a proxy for debugging and manipulation, proxy chaining, evasion rules, and more.	http://packetstormsecurity.com/files/104315/FHTTP-Attack-Tool.3.html
fierce	0.9.9	A DNS scanner	http://ha.ckers.org/fierce/
fiked	0.0.5	Fake IDE daemon	http://www.roe.ch/FakeIKEd
filibuster	161.37b7f9c	A Egress filter mapping application with additional functionality.	https://github.com/subinacls/Filibuster
fimap	1.00	A little tool for local and remote file inclusion auditing and exploitation	http://code.google.com/p/fimap/
find-dns	0.1	A tool that scans networks looking for DNS servers.	https://packetstormsecurity.com/files/132449/Find-DNS-Scanner.html
findmyhash	1.1.2	Crack different types of hashes using free online services	http://code.google.com/p/findmyhash/
firewalk	5.0	An active reconnaissance network security tool	http://packetfactory.openwall.net/projects/firewalk/
firmware-mod-kit	099	Modify firmware images without recompiling.	http://code.google.com/p/firmware-mod-kit
firstexecution	6.a275793	A Collection of different ways to execute code outside of the expected entry points.	https://github.com/nccgroup/firstexecution
fl0p	0.1	A passive L7 flow fingerprinter that examines TCP/UDP/ICMP packet sequences, can peek into cryptographic tunnels, can tell human beings and robots apart, and performs a couple of other infosec-related tricks.	http://lcamtuf.coredump.cx/
flare	0.6	Flare processes an SWF and extracts all scripts from it.	http://www.nowrap.de/flare.html
flashlight	107.39594b5	Автоматизированный инструмент сбора информации для тестеров на проникновение.	https://github.com/galkan/flashlight
flashscanner	8.72c7933	Сканер Flash на XSS.	https://github.com/riusksk/FlashScanner
flasm	1.62	Disassembler tool for SWF bytecode	http://www.nowrap.de/flasm.html
flawfinder	1.31	Searches through source code for potential security flaws.	http://www.dwheeler.com/flawfinder
flowinspect	96.1f62b3b	A network traffic inspection tool.	https://github.com/7h3rAm/flowinspect
flunym0us	2.0	A Vulnerability Scanner for WordPress and	http://code.google.com/p/flunym0us/

Имя	Версия	Описание	Домашняя страница
		Moodle.	
foremost	1.5.7	A console program to recover files based on their headers, footers, and internal data structures	http://foremost.sourceforge.net/
forkingportscanner	1	Simple and fast forking port scanner written in perl. Can only scan on host at a time, the forking is done on the specified port range. Or on the default range of 1. Has the ability to scan UDP or TCP, defaults to tcp.	http://magikh0e.xyz/
formatstringexploiter	27.cd54eac	Скрипт-помощник по работе с багами форматирования строки.	https://github.com/Owlz/formatStringExploiter
fpdns	20130404	Program that remotely determines DNS server versions.	https://github.com/kirei/fpdns
fping	3.13	Утилита для одновременного пинга множества хостов.	http://www.fping.org/
fport	2.0	Identify unknown open ports and their associated applications.	http://www.foundstone.com/us/resources/proddesc/fport.htm
fprotlogparser	1	This is a utility to parse a F-Prot Anti Virus log file, in order to sort them into a malware archive for easier maintanence of your collection.	http://magikh0e.xyz/
fraud-bridge	10.775c563	ICMP and DNS tunneling via IPv4 and IPv6.	https://github.com/stealth/fraud-bridge
freeipmi	1.4.11	Sensor monitoring, system event monitoring, power control, and serial-over-LAN (SOL).	http://www.gnu.org/software/freeipmi/
freeradius	3.0.11	Главный опенсорсный сервер RADIUS.	http://www.freeradius.org/
frida	284.79d63f5	Интерактивный дисассемблер, основанный на LLVM и Qt.	https://www.frida.xyz/
frisbeelite	1.2	A GUI-based USB device fuzzer.	https://github.com/nccgroup/FrisbeeLite
fs-exploit	3.28bb9bb	Format string exploit generation.	https://github.com/miaouPlop/fs
fs-nyarl	1.0	A network takeover & forensic analysis tool - useful to advanced PenTest tasks & for fun and profit.	http://www.fulgursecurity.com/en/content/fs-nyarl
fsnoop	3.3	A tool to monitor file operations on GNU/Linux systems by using the Inotify mechanism. Its primary purpose is to help detecting file race condition vulnerabilities and since version 3, to exploit them with loadable DSO modules (also called "payload modules" or "paymods").	http://vladz.devzero.fr/fsnoop.php
fstealer	0.1	Automates file system mirroring through remote file disclosur vulnerabilities on Linux machines.	http://packetstormsecurity.com/files/106450/FStealer-Filesystem-Mirroring-Tool.html
ftester	1.0	A tool designed for testing firewall filtering policies and Intrusion Detection System (IDS) capabilities.	http://www.inversepath.com/ftester.html
ftp-fuzz	1337	The master of all master fuzzing scripts specifically targeted towards FTP server sofware.	http://nullsecurity.net/tools/fuzzer.html
ftp-scanner	0.2.5	Multithreaded ftp scanner/brute forcer. Tested on Linux, OpenBSD and Solaris.	http://wayreth.eu.org/old_page/
ftp-spider	1.0	FTP investigation tool - Scans ftp server for the following: reveal entire directory tree structures, detect anonymous access, detect directories with write permissions, find user specified data within repository.	http://packetstormsecurity.com/files/35120/ftp-spider.pl.html
ftpmap	52.cbeabbe	Scans remote FTP servers to identify what software and what versions they are running.	http://wcoserver.googlecode.com/files/
fuddly	164.12a656c	Фреймворк фаззинга и манипуляции данными (для GNU/Linux).	https://github.com/k0retux/fuddly
fusil	1.5	A Python library used to write fuzzing programs.	http://bitbucket.org/haypo/fusil/wiki/Ho

Имя	Версия	Описание	Домашняя страница
			me
fuzzap	14.f13932c	A python script for obfuscating wireless networks.	https://github.com/lostincynicism/FuzzAP
fuzzball2	0.7	A little fuzzer for TCP and IP options. It sends a bunch of more or less bogus packets to the host of your choice.	http://nologin.org/
fuzzdb	187.fb6aa78	База данных образцов для атаки и исследования для фазз тестирования.	https://code.google.com/p/fuzzdb/
fuzzdiff	1.0	A simple tool designed to help out with crash analysis during fuzz testing. It selectively 'un-fuzzes' portions of a fuzzed file that is known to cause a crash, re-launches the targeted application, and sees if it still crashes.	http://vsecurity.com/resources/tool
fuzztalk	1.0.0.0	An XML driven fuzz testing framework that emphasizes easy extensibility and reusability.	https://code.google.com/p/fuzztalk
g72x++	1	Decoder for the g72x++ codec.	http://www.ps-auxw.de/
galleta	20040505_1	Examine the contents of the IE's cookie files for forensic purposes	http://www.jonesdykstra.com/
gdb	7.11	Отладчик GNU.	http://www.gnu.org/software/gdb/
genlist	0.1	Generates lists of IP addresses.	
geoedge	0.2	This little tools is designed to get geolocalization information of a host, it get the information from two sources (maxmind and geoiptool).	
geoip	1.6.6	Non-DNS IP-to-country resolver C library & utils	http://www.maxmind.com/app/c
geoipgen	0.4	GeoIPgen is a country to IP addresses generator.	http://code.google.com/p/geoipgen/
gerix-wifi-cracker	1.1c3cd73	A graphical user interface for aircrack-ng and pyrit.	https://github.com/TigerSecurity
getsids	0.0.1	Getsids tries to enumerate Oracle Sids by sending the services command to the Oracle TNS listener. Like doing ‘lsnrctl service’.	http://www.cqure.net/wp/getsids/
gggooglescan	0.4	A Google scraper which performs automated searches and returns results of search queries in the form of URLs or hostnames.	http://www.morningstarsecurity.com/research/gggooglescan
ghettotooth	1.0	Ghettodriving for bluetooth	http://www.oldskoolphreak.com/tfiles/ghettotooth.txt
ghost-phisher	1.62	GUI suite for phishing and penetration attacks	http://code.google.com/p/ghost-phisher
ghost-py	0.2.3	Webkit based webclient (relies on PyQT).	http://jeanphix.github.com/Ghost.py/
giskismet	20110805	A program to visually represent the Kismet data in a flexible manner.	http://www.giskismet.org
githack	6.b83a744	A `.git` folder disclosure exploit.	https://github.com/lijiejie/githack
gitminer	21.9ee4902	Инструмент для продвинутой добычи содержимого на Github.	https://github.com/danilovazb/GitMiner
gitrob	0.0.6	Scan Github For Sensitive Files.	http://michenriksen.com/blog/gitrob-putting-the-open-source-in-osint/
gnuradio	3.7.9.1	Набор инструментов общего назначения DSP и SDR. С драйверами usrp и fcd.	http://gnuradio.org
gnutls2	2.12.23	A library which provides a secure layer over a reliable transport layer (Version 2)	http://gnutls.org/
gobd	81.e64b5a5	A Golang covert backdoor.	https://github.com/razc411/GoBD
goldeneye	16.7a38fe9	A HTTP DoS test tool. Attack Vector exploited: HTTP Keep Alive + NoCache.	https://github.com/jseidl/GoldenEye
golismero	35.36ed3d4	Opensource web security testing framework.	https://github.com/golismero/golismero
goodork	2.2	A python script designed to allow you to	http://goo-dork.blogspot.com/

Имя	Версия	Описание	Домашняя страница
		leverage the power of google dorking straight from the comfort of your command line.	
goofile	1.5	Command line filetype search	https://code.google.com/p/goofile/
goog-mail	1.0	Enumerate domain emails from google.	http://www.darkc0de.com/others/goog-mail.py
googlesub	1.3	A python script to find domains by using google dorks.	https://github.com/zombiesam/googlesub
gooscan	1.0.9	A tool that automates queries against Google search appliances, but with a twist.	http://johnny.ihackstuff.com/downloads/task,doc_details&Itemid=/gid,28/
gophish	0.1.1	Фишинговый фреймворк с открытым исходным кодом.	https://getgophish.com/
gpredict	1.3	A real-time satellite tracking and orbit prediction application.	http://gpredict.oz9aec.net/
gqrx	2.5.3	Интерактивный рессивер программно-определяемой радиосистемы для многих устройств, строит различные графики.	http://gqrx.dk/
grabber	0.1	A web application scanner. Basically it detects some kind of vulnerabilities in your website.	http://rgaucher.info/beta/grabber/
greenbone-security-assistant	6.0.6	Greenbone Security Assistant (gsa) - OpenVAS web frontend	http://www.openvas.org/
grepforrfi	0.1	Simple script for parsing web logs for RFIs and Webshells v1.2	http://www.irongeek.com/downloads/grepforrfi.txt
grokevt	0.5.0	A collection of scripts built for reading Windows® NT/2K/XP/2K eventlog files.	http://code.google.com/p/grokevt/
gtalk-decode	0.1	Google Talk decoder tool that demonstrates recovering passwords from accounts.	http://packetstormsecurity.com/files/119154/Google-Talk-Decoder.html
gtp-scan	0.7	A small python script that scans for GTP (GPRS tunneling protocol) speaking hosts.	http://www.c0decafe.de/
guymager	0.7.4	A forensic imager for media acquisition.	http://guymager.sourceforge.net/
gwcheck	0.1	A simple program that checks if a host in an ethernet network is a gateway to Internet.	http://packetstormsecurity.com/files/62047/gwcheck.c.html
gwtenum	7.f27a5aa	Enumeration of GWT-RCP method calls.	http://www.gdssecurity.com/l/t/d.php?k=GwtEnum
hackersh	0.2.0	A shell for with Pythonect-like syntax, including wrappers for commonly used security tools.	http://www.hackersh.org/
hackredis	1.67eeb6c	Простой инструмент для сканирования и эксплуатации серверов Redis.	https://github.com/Ridter/hackredis
haka	0.2.2	A collection of tool that allows capturing TCP/IP packets and filtering them based on Lua policy files.	https://github.com/haka-security/haka
halberd	0.2.4	Halberd discovers HTTP load balancers. It is useful for web application security auditing and for load balancer configuration testing.	http://halberd.superadditive.com/
halcyon	0.1	A repository crawler that runs checksums for static files found within a given git repository.	http://www.blackhatlibrary.net/Halcyon
hamster	2.0.0	Tool for HTTP session sidejacking.	http://hamster.erratasec.com/
handle	0.0	An small application designed to analyze your system searching for global objects related to running proccess and display information for every found object, like tokens, semaphores, ports, files,..	http://www.tarasco.org/security/handle/index.html
hasere	1.0	Discover the vhosts using google and bing.	https://github.com/galkan/hasere
hashcat	2.00	A multithreaded cross platform hash cracker.	http://hashcat.net/hashcat/

Имя	Версия	Описание	Домашняя страница
hashcat-utils	1.2	Utilites for Hashcat	http://hashcat.net/wiki/doku.php?id=hashcat_utils
hashdeep	4.4	Advanced checksum hashing tool.	http://md5deep.sourceforge.net/
hasher	48.40173c5	A tool that allows you to quickly hash plaintext strings, or compare hashed values with a plaintext locally.	https://github.com/ChrisTruncer/Hasher
hashfind	8.e9a9a14	A tool to search files for matching password hash types and other interesting data.	https://github.com/rurapenthe/hashfind
hashid	397.7e8473a	Software to identify the different types of hashes used to encrypt data.	https://github.com/psypanda/hashID
hashpump	45.2d01d3b	A tool to exploit the hash length extension attack in various hashing algorithms.	https://github.com/bwall/HashPump
hashtag	0.41	A python script written to parse and identify password hashes.	https://github.com/SmeegeSec/HashTag
haystack	1745.e3554f8	Фреймворк на Python для поиска C структур в памяти процесса - анализ кучи - Криминалистическое исследование структуры памяти.	https://github.com/trolldbois/python-haystack
hbad	1.0	This tool allows you to test clients on the heartbleed bug.	http://www.curesec.com/
hcraft	1.0.0	HTTP Vuln Request Crafter	http://sourceforge.net/projects/hcraft/
hdcp-genkey	18.e8d342d	Generate HDCP source and sink keys from the leaked master key.	https://github.com/rjw57/hdcp-genkey
hdmi-sniff	5.f7fbc0e	HDMI DDC (I2C) inspection tool. It is designed to demonstrate just how easy it is to recover HDCP crypto keys from HDMI devices.	https://github.com/ApertureLabsLtd/hdmi-sniff
heartbleed-honeypot	0.1	Script that listens on TCP port 443 and responds with completely bogus SSL heartbeat responses, unless it detects the start of a byte pattern similar to that used in Jared Stafford's	http://packetstormsecurity.com/files/126068/hb_honeypot.pl.txt
hemingway	6.d4ec5f1	A simple and easy to use spear phishing helper.	https://github.com/ytisf/hemingway
hex2bin	2.1	Converts Motorola and Intel hex files to binary.	http://hex2bin.sourceforge.net/
hexinject	1.5	A very versatile packet injector and sniffer that provides a command-line framework for raw network access.	http://hexinject.sourceforge.net
hexorbase	6	A database application designed for administering and auditing multiple database servers simultaneously from a centralized location. It is capable of performing SQL queries and bruteforce attacks against common database servers (MySQL, SQLite, Microsoft SQL Server, Oracle, PostgreSQL).	https://code.google.com/p/hexorbase/
hharp	1beta	This tool can perform man-in-the-middle and switch flooding attacks. It has 4 major functions, 3 of which attempt to man-in-the-middle one or more computers on a network with a passive method or flood type method.	http://packetstormsecurity.com/files/81368/Hackers-Hideaway-ARP-Attack-Tool.html
hidattack	0.1	HID Attack (attacking HID host implementations)	http://mulliner.org/bluetooth/hidattack.php
honeyd	1.6.7	A small daemon that creates virtual hosts on a network.	https://github.com/DataSoft/Honeyd/
honggfuzz	0.6	A general-purpose fuzzer with simple, command-line interface.	https://code.google.com/p/honggfuzz/
honssh	86.0843542	Приманка выской степени взаимодействия, создана для записи всех SSH подключений между клиентом и сервером.	https://code.google.com/p/honssh/

Имя	Версия	Описание	Домашняя страница
hookanalyser	3.1	A hook tool which can be potentially helpful in reversing applications and analyzing malware. It can hook to an API in a process and search for a pattern in memory or dump the buffer.	http://hookanalyser.blogspot.de/
hoover	4.9bda860	Wireless Probe Requests Sniffer.	https://github.com/xme/hoover/
hoppy	1.8.1	A python script which tests http methods for configuration issues leaking information or just to see if they are enabled.	https://labs.portcullis.co.uk/downloads/
host-extract	9	Ruby script tries to extract all IP/Host patterns in page response of a given URL and JavaScript/CSS files of that URL.	https://code.google.com/p/host-extract/
hostapd-wpe	2.2	IEEE 802.11 AP, IEEE 802.1X/WPA/WPA2/EAP/RADIUS Authenticator - Wireless Pwnage Edition.	https://github.com/OpenSecurityResearch/hostapd-wpe
hostbox-ssh	0.1.1	A ssh password/account scanner.	http://stridsmanit.wordpress.com/2012/12/02/brute-forcing-passwords-with-hostbox-ssh-1-1/
hotpatch	0.2	Hot patches executables on Linux using .so file injection.	http://www.selectiveintellect.com/hotpatch.html
hotspotter	0.4	Hotspotter passively monitors the network for probe request frames to identify the preferred networks of Windows XP clients, and will compare it to a supplied list of common hotspot network names.	http://www.remote-exploit.org/?page_id=418
hpfeeds	164.f18712d	Honeynet Project generic authenticated datafeed protocol.	https://github.com/rep/hpfeeds
hping	3.0.0	A command-line oriented TCP/IP packet assembler/analyzer.	http://www.hping.org
hqlmap	38.bb6ab46	A tool to exploit HQL Injections.	https://github.com/PaulSec/HQLmap
hsecscan	36.0f5ac2f	A security scanner for HTTP response headers.	https://github.com/riramar/hsecscan
htcap	8.30e7222	Инструмент анализа веб-приложений для выявления соединений между javascript и сервером.	https://github.com/segment-srl/htcap
htexploit	0.77	A Python script that exploits a weakness in the way that .htaccess files can be configured to protect a web directory with an authentication process	http://www.mkit.com.ar/labs/htexploit/
htpwdscan	16.99697fc	A python HTTP weak pass scanner.	https://github.com/lijiejie/htpwdScan
htrosbif	134.9dc3f86	Active HTTP server fingerprinting and recon tool.	https://github.com/lkarsten/htrosbif
htshells	79.399feaa	Self contained web shells and other attacks via .htaccess files.	https://github.com/wireghoul/htshells
http-enum	0.3	A tool to enumerate the enabled HTTP methods supported on a webserver.	https://www.thexero.co.uk/tools/http-enum/
http-fuzz	0.1	A simple http fuzzer.	none
http-put	1.0	Simple http put perl script	
http-traceroute	0.5	This is a python script that uses the Max-Forwards header in HTTP and SIP to perform a traceroute-like scanning functionality.	http://packetstormsecurity.com/files/107167/Traceroute-Like-HTTP-Scanner.html
httpbog	1.0.0.0	A slow HTTP denial-of-service tool that works similarly to other attacks, but rather than leveraging request headers or POST data Bog consumes sockets by slowly reading responses.	http://sourceforge.net/projects/httpbog/
httpforge	11.02.01	A set of shell tools that let you manipulate, send, receive, and analyze HTTP messages. These tools can be used to test, discover, and assert the	http://packetstormsecurity.com/files/98109/HTTPForge.02.01.html

Имя	Версия	Описание	Домашняя страница
		security of Web servers, apps, and sites. An accompanying Python library is available for extensions.	
httping	2.4	A 'ping'-like tool for http-requests.	http://www.vanheusden.com/httping/
httprint	301	A web server fingerprinting tool.	http://www.net-square.com/httprint.html
httprint-win32	301	A web server fingerprinting tool (Windows binaries).	http://net-square.com/httprint
httpry	0.1.8	A specialized packet sniffer designed for displaying and logging HTTP traffic.	http://dumpsterventures.com/jason/httpry/
httpsniff	0.4	Tool to sniff HTTP responses from TCP/IP based networks and save contained files locally for later review.	http://www.sump.org/projects/httpsniff/
httpsscanner	1.2	A tool to test the strength of a SSL web server.	https://code.google.com/p/libre-tools/
httptunnel	3.3	Creates a bidirectional virtual data connection tunnelled in HTTP requests	http://www.nocrew.org/software/httptunnel
httrack	3.48.21	An easy-to-use offline browser utility.	http://www.httrack.com/
hubbit-sniffer	69.4ef732f	Simple application that listens for WIFI-frames and records the mac-address of the sender and posts them to a REST-api.	https://github.com/cthit/hubbIT-sniffer
hulk	11.a9b9ad4	A webserver DoS tool (Http Unbearable Load King) ported to Go with some additional features.	https://github.com/grafov/hulk
hungry-interceptor	296.a87dcd3	Перехватывает данные, что-либо с ними делает, сохраняет их.	https://github.com/nbuechler/hungry-interceptor
hwk	0.4	Collection of packet crafting and wireless network flooding tools	http://www.nullsecurity.net/
hyde	5.22d8e91	Just another tool in C to do DDoS (with spoofing).	https://github.com/CoolerVoid/Hyde
hydra	8.1	A very fast network logon cracker which support many different services	http://www.thc.org/thc-hydra/
hyenae	0.36_1	flexible platform independent packet generator	http://sourceforge.net/projects/hyenae/
hyperfox	45.79ffeb5	A security tool for proxying and recording HTTP and HTTPs traffic.	github.com/xiam/hyperfox
hyperion	1.2	A runtime encrypter for 32-bit portable executables.	http://nullsecurity.net/tools/binary.html
iaxflood	0.1	IAX flooder.	http://www.hackingexposedvoip.com/
iaxscan	0.02	A Python based scanner for detecting live IAX/2 hosts and then enumerating (by bruteforce) users on those hosts.	http://code.google.com/p/iaxscan/
ibrute	12.3a6a11e	An AppleID password bruteforce tool. It uses Find My Iphone service API, where bruteforce protection was not implemented.	https://github.com/hackappcom/ibrute/
icmpquery	1.0	Send and receive ICMP queries for address mask and current time.	http://www.angio.net/security/
icmptx	0.2	IP over ICMP tunnel.	http://thomer.com/icmptx/
idswakeup	1.0	A collection of tools that allows to test network intrusion detection systems.	http://www.hsc.fr/ressources/outils/idswakeup/index.html.en
ifchk	1.0.1	A network interface promiscuous mode detection tool.	http://www.noorg.org/ifchk/
iheartxor	0.01	A tool for bruteforcing encoded strings within a boundary defined by a regular expression. It will bruteforce the key value range of 0x1 through 0x255.	http://hooked-on-mnemonics.blogspot.com.es/p/iheartxor.html
iis-shortname-	4.b92772a	An IIS shortname Scanner.	https://github.com/lijiejie/IIS_shortname_Scanner

Имя	Версия	Описание	Домашняя страница
scanner			
iisbruteforcer	15	HTTP authentication cracker. It's a tool that launchs an online dictionary attack to test for weak or simple passwords against protected areas on an IIS Web server.	http://www.open-labs.org/
ike-scan	1.9	A tool that uses IKE protocol to discover, fingerprint and test IPSec VPN servers	http://www.nta-monitor.com/tools/ike-scan/
ikecrack	1.00	An IKE/IPSec crack tool designed to perform Pre-Shared-Key analysis of RFC compliant aggressive mode authentication	http://sourceforge.net/projects/ikecrack/
ikeprobe	0.1	Determine vulnerabilities in the PSK implementation of the VPN server.	http://www.ernw.de/download/ikeprobe.zip
ikeprober	1.12	Tool crafting IKE initiator packets and allowing many options to be manually set. Useful to find overflows, error conditions and identifiyng vendors	http://ikecrack.sourceforge.net/
ilty	1.0	An interception phone system for VoIP network.	http://chdir.org/~nico/ilty/
imagejs	48.1faf262	Small tool to package javascript into a valid image file.	https://github.com/jklmnn/imagejs
inception	431.34f207d	A FireWire physical memory manipulation and hacking tool exploiting IEEE 1394 SBP DMA.	http://www.breaknenter.org/projects/inception/
indxparse	166.14839a6	A Tool suite for inspecting NTFS artifacts.	http://www.williballenthin.com/forensics/mft/indxparse/
inetsim	1.2.5	A software suite for simulating common internet services in a lab environment, e.g. for analyzing the network behaviour of unknown malware samples.	http://www.inetsim.org
infip	0.1	A python script that checks output from netstat against RBLs from Spamhaus.	http://packetstormsecurity.com/files/104927/infIP.1-Blacklist-Checker.html
inguma	0.1.1	A free penetration testing and vulnerability discovery toolkit entirely written in python. Framework includes modules to discover hosts, gather information about, fuzz targets, brute force usernames and passwords, exploits, and a disassembler.	http://inguma.sourceforge.net
intercepter-ng	0.9.10	sniffer следующего покаления, включает множество функций: захват паролей/хэший, сниффинг сообщений часта, выполняет атаки man-in-the-middle attacks и т.д.	http://intercepter.nerf.ru/#down
interrogate	0.0.4	A proof-of-concept tool for identification of cryptographic keys in binary material (regardless of target operating system), first and foremost for memory dump analysis and forensic usage.	https://github.com/carmaa/interrogate
intersect	2.5	Post-exploitation framework	https://github.com/ohdae/Intersect.5
intrace	1.5	Traceroute-like application piggybacking on existing TCP connections	http://intrace.googlecode.com
inundator	0.5	An ids evasion tool, used to anonymously inundate intrusion detection logs with false positives in order to obfuscate a real attack.	http://inundator.sourceforge.net/
inurlbr	31.5bb8b38	Advanced search in the search engines - Inurl scanner, dorker, exploiter.	https://code.google.com/p/inurlbr/
inviteflood	2.0	Flood a device with INVITE requests	https://launchpad.net/~wagungs/+archive/kali-linux/+build/4386635
iodine	0.7.0	Tunnel IPv4 data through a DNS server	http://code.kryo.se/iodine
iosforensic	1.0	iOS forensic tool https://www.owasp.org/index.php/Projects/OWA	https://github.com/Flo354/iOSForensic

Имя	Версия	Описание	Домашняя страница
		SP_iOSForensic	
ip-https-tools	7.170691f	Tools for the IP over HTTPS (IP-HTTPS) Tunneling Protocol.	https://github.com/takeshixx/ip-https-tools
ipaudit	1.0rc9	Monitors network activity on a network.	http://ipaudit.sourceforge.net
ipba2	032013	IOS Backup Analyzer	http://www.ipbackupanalyzer.com/
ipdecap	69.f3a08f6	Can decapsulate traffic encapsulated within GRE, IPIP, 6in4, ESP (ipsec) protocols, and can also remove IEEE 802.1Q (virtual lan) header.	http://www.loicp.eu/ipdecap#dependances
iphoneanalyzer	2.1.0	Allows you to forensically examine or recover date from in iOS device.	http://www.crypticbit.com/zen/products/iphoneanalyzer
ipmipwn	6.74a08a8	Инструмент 0 атаки на шифр IPMI.	https://github.com/AnarchyAngel/IPMIPWN
ipmitool	1.8.16	Интерфейс командной строки для устройств с IPMI.	http://ipmitool.sourceforge.net
ipscan	3.4.1	Кроссплатформенный быстрый сканер IP адресов и портов.	http://www.angryziber.com/
iptv	134.720cc12	Поиск и брутфорс незаконных iptv серверов.	https://github.com/Pinperepette/IPTV
iputils	20150815.1c59920	Инструменты мониторинга сети, включая ping	http://www.skbuff.net/iputils/
ipv6toolkit	2.0	SI6 Networks' IPv6 Toolkit	http://www.si6networks.com/tools/ipv6toolkit/
ircsnapshot	94.cb02a85	Tool to gather information from IRC servers.	https://github.com/bwall/ircsnapshot
irpas	0.10	Internetwork Routing Protocol Attack Suite.	http://phenoelit-us.org/irpas
isip	2.fad1f10	Interactive sip toolkit for packet manipulations, sniffing, man in the middle attacks, fuzzing, simulating of dos attacks.	https://github.com/halitalptekin/isip
isme	0.12	Scans a VOIP environment, adapts to enterprise VOIP, and exploits the possibilities of being connected directly to an IP Phone VLAN.	https://packetstormsecurity.com/files/123534/IP-Phone-Scanning-Made-Easy.12.html
isr-form	1.0	Simple html parsing tool that extracts all form related information and generates reports of the data. Allows for quick analyzing of data.	http://www.infobyte.com.ar/
ivre	858.4ef1a48	Фреймворк разведки сети.	https://github.com/cea-sec/ivre
jad	1.5.8e	Java decompiler	http://www.varaneckas.com/jad
jaidam	10.a7d7c4a	Penetration testing tool that would take as input a list of domain names, scan them, determine if wordpress or joomla platform was used and finally check them automatically, for web vulnerabilities using two well-known open source tools, WPScan and Joomscan.	https://github.com/stasinopoulos/jaidam
javasnoop	1.1	A tool that lets you intercept methods, alter data and otherwise hack Java applications running on your computer	https://code.google.com/p/javasnoop/
jboss-autopwn	1.3bc2d29	A JBoss script for obtaining remote shell access.	https://github.com/SpiderLabs/jboss-autopwn
jbrofuzz	2.5	Web application protocol fuzzer that emerged from the needs of penetration testing.	http://sourceforge.net/projects/jbrofuzz/
jbrute	0.99	Open Source Security tool to audit hashed passwords.	http://sourceforge.net/projects/jbrute/
jcrack	0.3.3beta	Утилита для создания файлов словарей для использования во взломе паролей некоторых беспроводных шлюзов.	http://www.thedrahos.net/jcrack/
jd-gui	1.4.0	A standalone graphical utility that displays Java source codes of .class files.	http://java.decompiler.free.fr/?q=jdgui
jhead	3.00	EXIF JPEG info parser and thumbnail remover	http://www.sentex.net/~mwandel/jhead/

Имя	Версия	Описание	Домашняя страница
jnetmap	0.5.3	A network monitor of sorts	http://www.rakudave.ch/jnetmap/?file=introduction
john	1.7.9	John The Ripper - A fast password cracker (jumbo included)	http://www.openwall.com/john/
johnny	20120424	GUI for John the Ripper.	http://openwall.info/wiki/john/johnny
jomplug	0.1	This php script fingerprints a given Joomla system and then uses Packet Storm's archive to check for bugs related to the installed components.	http://packetstormsecurity.com/files/121390/Janissaries-Joomla-Fingerprint-Tool.html
jooforce	11.43c21ad	A Joomla password brute force tester.	https://github.com/rastating/jooforce
joomlascan	1.2	Joomla scanner scans for known vulnerable remote file inclusion paths and files.	http://packetstormsecurity.com/files/62126/joomlascan.2.py.txt.html
joomlavs	203.c86d628	Сканер уязвимостей Joomla по принципу чёрного ящика, написан на Ruby.	https://github.com/rastating/joomlavs
joomscan	2012.03.10	Detects file inclusion, sql injection, command execution vulnerabilities of a target Joomla! web site.	http://joomscan.sourceforge.net/
js-beautify	1.5.10	This little beautifier will reformat and reindent bookmarklets, ugly JavaScript, unpack scripts packed by Dean Edward?s popular packer, as well as deobfuscate scripts processed by javascriptobfuscator.com.	https://github.com/einars/js-beautify
jsql	0.73	A lightweight application used to find database information from a distant server.	https://code.google.com/p/jsql-injection/
junkie	1365.70a83d6	A modular packet sniffer and analyzer.	https://github.com/securactive/junkie
jwscan	6.b0306f0	Scanner for Jar to EXE wrapper like Launch4j, Exe4j, JSmooth, Jar2Exe.	https://github.com/katjahahn/JWScan
jynx2	2.0	An expansion of the original Jynx LD_PRELOAD rootkit	http://www.blackhatlibrary.net/Jynx2
kacak	1.0	Tools for penetration testers that can enumerate which users logged on windows system.	https://github.com/galkan/kacak
kadimus	43.bbb1f2f	LFI Scan & Exploit Tool.	https://github.com/P0cL4bs/Kadimus
kalibrate-rtl	11.aae11c8	Fork of http://thre.at/kalibrate/ for use with rtl-sdr devices.	https://github.com/steve-m/kalibrate-rtl
katana	0.0.0.7	A framework that seekss to unite general auditing tools, which are general pentesting tools (Network,Web,Desktop and others).	http://sourceforge.net/projects/katanas/
katsnoop	0.1	Utility that sniffs HTTP Basic Authentication information and prints the base64 decoded form.	http://packetstormsecurity.com/files/52514/katsnoop.tbz2.html
kautilya	0.5.5	Pwnage with Human Interface Devices using Teensy++2.0 and Teensy 3.0 devices.	https://github.com/samratashok/Kautilya/releases
keimpx	165.aab7213	Tool to verify the usefulness of credentials across a network over SMB.	http://code.google.com/p/keimpx/
khc	0.2	A small tool designed to recover hashed known_hosts fiels back to their plain-text equivalents.	http://packetstormsecurity.com/files/87003/Known-Host-Cracker.2.html
killerbee	99	Framework and tools for exploiting ZigBee and IEEE 802.15.4 networks.	https://code.google.com/p/killerbee/
kippo	0.9	A medium interaction SSH honeypot designed to log brute force attacks and most importantly, the entire shell interaction by the attacker.	https://github.com/desaster/kippo
kismet	2013_03_R1b	802.11 layer2 wireless network detector, sniffer, and intrusion detection system	http://www.kismetwireless.net/
kismet-earth	0.1	Various scripts to convert kismet logs to kml file to be used in Google Earth.	http://

Имя	Версия	Описание	Домашняя страница
kismet2earth	1.0	A set of utilities that convert from Kismet logs to Google Earth .kml format	http://code.google.com/p/kismet2earth/
kitty	88.6f7616b	Фреймворк фаззинга, написан на Python.	https://github.com/cisco-sas/kitty
klogger	1.0	A keystroke logger for the NT-series of Windows.	http://ntsecurity.nu/toolbox/klogger/
knock	223.61a1b8f	Сканер субдоменов.	https://github.com/guelfoweb/knock
kolkata	3.0	A web application fingerprinting engine written in Perl that combines cryptography with IDS evasion.	http://www.blackhatlibrary.net/Kolkata
kraken	32.368a837	A project to encrypt A5/1 GSM signaling using a Time/Memory Tradeoff Attack.	http://opensource.srlabs.de/projects/a51-decrypt
laf	12.7a456b3	Login Area Finder: scans host/s for login panels.	https://github.com/takeshixx/laf
lanmap2	127.1197999	Passive network mapping tool.	http://github.com/rflynn/lanmap2
lans	168.4ad2333	Многопоточный асинхронный спуфер arp пакетов, может разбирать и делать инъекции.	https://github.com/DanMcInerney/LANs.py
latd	1.31	A LAT terminal daemon for Linux and BSD.	http://sourceforge.net/projects/linux-decnet/files/latd/1.31/
laudanum	1.0	A collection of injectable files, designed to be used in a pentest when SQL injection flaws are found and are in multiple languages for different environments.	http://laudanum.inguardians.com/#
lbd	20130719	Load Balancing detector	http://ge.mine.nu/code/lbd
lbmap	145.93e6b71	Proof of concept scripts for advanced web application fingerprinting, presented at OWASP AppSecAsia 2012.	https://github.com/wireghoul/lbmap
ldap-brute	21.acc06e3	A semi fast tool to bruteforce values of LDAP injections over HTTP.	https://github.com/droope/ldap-brute
ldapenum	0.1	Enumerate domain controllers using LDAP.	https://gobag.googlecode.com/svn-history/r2/trunk/ldap/ldapenum/
leo	5.2	Грамотный редактор программера, структуризатор и менеджер проектов.	http://webpages.charter.net/edreamleo/front.html
leroy-jenkins	3.bdc3965	A python tool that will allow remote execution of commands on a Jenkins server and its nodes.	https://github.com/captainhooligan/Leroy-Jenkins
letmefuckit-scanner	3.f3be22b	Scanner and Exploit Magento.	https://github.com/onthefrontline/LetMeFuckIt-Scanner
levye	84.5406303	A brute force tool which is support sshkey, vnckey, rdp, openvpn.	https://github.com/galkan/levye
lfi-autopwn	3.0	A Perl script to try to gain code execution on a remote server via LFI	http://www.blackhatlibrary.net/Lfi_autopwn.pl
lfi-exploiter	1.1	This perl script leverages /proc/self/environ to attempt getting code execution out of a local file inclusion vulnerability..	http://packetstormsecurity.com/files/124332/LFI-Exploiter.1.html
lfi-fuzzploit	1.1	A simple tool to help in the fuzzing for, finding, and exploiting of local file inclusion vulnerabilities in Linux-based PHP applications.	http://packetstormsecurity.com/files/106912/LFI-Fuzzploit-Tool.1.html
lfi-image-helper	0.8	A simple script to infect images with PHP Backdoors for local file inclusion attacks.	http://packetstormsecurity.com/files/129871/LFI-Image-Helper.8.html
lfi-scanner	4.0	This is a simple perl script that enumerates local file inclusion attempts when given a specific target.	http://packetstormsecurity.com/files/102848/LFI-Scanner.0.html
lfi-sploiter	1.0	This tool helps you exploit LFI (Local File Inclusion) vulnerabilities. Post discovery, simply pass the affected URL and vulnerable parameter to this tool. You can also use this tool to scan a URL for LFI vulnerabilities.	http://packetstormsecurity.com/files/96056/Simple-Local-File-Inclusion-Exploiter.0.html

Имя	Версия	Описание	Домашняя страница
lfifreak	21.0c6adef	A unique automated LFi Exploiter with Bind/Reverse Shells.	https://github.com/OsandaMalith/LFiFreak/
lfimap	1.4.8	This script is used to take the highest beneficts of the local file include vulnerability in a webserver.	https://code.google.com/p/lfimap/
lft	3.73	A layer four traceroute implementing numerous other features.	http://pwhois.org/lft/
libdisasm	0.23	A disassembler library.	http://bastard.sourceforge.net/libdisasm.html
libpst	0.6.66	Outlook .pst file converter	http://www.five-ten-sg.com/libpst/
liffy	65.8011cdd	A Local File Inclusion Exploitation tool.	https://github.com/rotlogix/liffy
linenum	18.b4c2541	Scripted Local Linux Enumeration & Privilege Escalation Checks	https://github.com/rebootuser/LinEnum
linset	9.8746b1f	Evil Twin Attack Bash script - An automated WPA/WPA2 hacker.	https://github.com/vk496/linset
linux-exploit-suggester	32.9db2f5a	A Perl script that tries to suggest exploits based OS version number.	https://github.com/PenturaLabs/Linux_Exploit_Suggester
lisa.py	28.5b3156b	An Exploit Dev Swiss Army Knife.	https://github.com/ant4g0nist/lisa.py
list-urls	0.1	Extracts links from webpage	http://www.whoppix.net
littleblackbox	0.1.3	Penetration testing tool, search in a collection of thousands of private SSL keys extracted from various embedded devices.	http://code.google.com/p/littleblackbox/wiki/FAQ
lldb	3.7.1	Высокопроизводительный отладчик следующего поколения.	http://lldb.llvm.org/
lodowep	1.2.1	Lodowep is a tool for analyzing password strength of accounts on a Lotus Domino webserver system.	http://www.cqure.net/wp/lodowep/
logkeys	0.1.1a	Simple keylogger supporting also USB keyboards.	http://logkeys.googlecode.com/
loot	51.656fb85	Sensitive information extraction tool.	https://github.com/GuerrillaWarfare/Loot
lorcon	2.0.0.20091101	Generic library for injecting 802.11 frames	http://802.11ninja.net/
lotophagi	0.1	a relatively compact Perl script designed to scan remote hosts for default (or common) Lotus NSF and BOX databases.	http://packetstormsecurity.com/files/55250/lotophagi.rar.html
lsrtunnel	0.2	Spoofs connections using source routed packets.	http://www.synacklabs.net/projects/lsrtunnel/
lte-cell-scanner	57.5fa3df8	LTE SDR cell scanner optimized to work with very low performance RF front ends (8bit A/D, 20dB noise figure).	https://github.com/Evrytania/LTE-Cell-Scanner
luksipc	0.01	A tool to convert unencrypted block devices to encrypted LUKS devices in-place.	http://www.johannes-bauer.com/linux/luksipc
luyten	0.4.6	Графический интерфейс Procyon с открытым исходным кодом декомпилятора Java.	https://github.com/deathmarine/Luyten
lynis	2.2.0	Инструмент безопасности и системного аудита для усиления систем Unix/Linux.	https://cisofy.com/lynis/
mac-robber	1.02	A digital investigation tool that collects data from allocated files in a mounted file system.	http://www.sleuthkit.org/mac-robber/download.php
macchanger	1.7.0	A small utility to change your NIC's MAC address	http://www.gnu.org/software/macchanger
machinae	42.776930a	Инструмент для сбора знаний с публичных сайтов/фидов связанных с безопасностью.	https://github.com/HurricaneLabs/machinae
maclookup	0.4	Lookup MAC addresses in the IEEE MA-L/OUI public listing.	https://github.com/paraxor/maclookup
magicrescue	1.1.9	Find and recover deleted files on block devices	http://freshmeat.net/projects/magicrescue

Имя	Версия	Описание	Домашняя страница
			/
magictree	1.3	A penetration tester productivity tool designed to allow easy and straightforward data consolidation, querying, external command execution and report generation	http://www.gremwell.com
make-pdf	0.1.6	This tool will embed javascript inside a PDF document.	http://blog.didierstevens.com/programs/pdf-tools/
makepasswd	1.10_10	Generates true random passwords with the emphasis on security over pronounceability (Debian version)	http://packages.qa.debian.org/m/makepaswd.html
malcom	704.ec915a3	Analyze a system's network communication using graphical representations of network traffic.	https://github.com/tomchop/malcom
malheur	0.5.4	A tool for the automatic analyze of malware behavior.	http://www.mlsec.org/malheur/
maligno	2.5	An open source penetration testing tool written in python, that serves Metasploit payloads. It generates shellcode with msfvenom and transmits it over HTTP or HTTPS.	http://www.encripto.no/tools/
malmon	0.3	Hosting exploit/backdoor detection daemon. It's written in python, and uses inotify (pyinotify) to monitor file system activity. It checks files smaller then some size, compares their md5sum and hex signatures against DBs with known exploits/backdoor.	http://sourceforge.net/projects/malmon/
maltego	3.6.0.6640	An open source intelligence and forensics application, enabling to easily gather information about DNS, domains, IP addresses, websites, persons, etc.	http://www.paterva.com/web5
maltrieve	342.b9e7560	Originated as a fork of mwcrawler. It retrieves malware directly from the sources as listed at a number of sites.	https://github.com/technoskald/maltrieve
malware-check-tool	1.2	Python script that detects malicious files via checking md5 hashes from an offline set or via the virustotal site. It has http proxy support and an update feature.	http://packetstormsecurity.com/files/93518/Malware-Check-Tool.2.html
malwareanalyser	3.3	A freeware tool to perform static and dynamic analysis on malware.	http://malwareanalyser.blogspot.de/2011/10/malware-analyser.html
malwaredetect	0.1	Submits a file's SHA1 sum to VirusTotal to determine whether it is a known piece of malware	http://www.virustotal.com
malwasm	0.2	Offline debugger for malware's reverse engineering.	https://code.google.com/p/malwasm/
malybuzz	1.0	A Python tool focused in discovering programming faults in network software.	http://eternal-todo.com/tools/malybuzz-network-fuzzer
mana	68.56bcfcd	A toolkit for rogue access point (evilAP) attacks first presented at Defcon 22.	https://github.com/sensepost/mana
marc4dasm	6.f11860f	This python-based tool is a disassembler for the Atmel MARC4 (a 4 bit Harvard micro).	https://github.com/ApertureLabsLtd/marc4dasm
maskprocessor	0.73	A High-Performance word generator with a per-position configurable charset.	http://hashcat.net/wiki/doku.php?id=maskprocessor
masscan	1.0.3	TCP port scanner, spews SYN packets asynchronously, scanning entire Internet in under 5 minutes	https://github.com/robertdavidgraham/masscan
masscan-automation	24.2df3467	Masscan integrated with Shodan API.	https://github.com/trevordavenport/MasscanAutomation

Имя	Версия	Описание	Домашняя страница
mat	0.6.1	Набор инструментов анализа метаданных, включает приложение с графическим пользовательским интерфейсом, приложение командной строки и библиотеку.	https://mat.boum.org/
matahari	0.1.30	A reverse HTTP shell to execute commands on remote machines behind firewalls.	http://matahari.sourceforge.net
mausezahn	0.40	A free fast traffic generator written in C which allows you to send nearly every possible and impossible packet.	http://www.perihel.at/sec/mz/
mbenum	1.5.0	Queries the master browser for whatever information it has registered.	http://www.cqure.net/wp/mbenum/
mboxgrep	0.7.9	A small, non-interactive utility that scans mail folders for messages matching regular expressions. It does matching against basic and extended POSIX regular expressions, and reads and writes a variety of mailbox formats.	http://mboxgrep.sourceforge.net
mdbtools	0.7.1	Utilities for viewing data and exporting schema from Microsoft Access Database files	http://sourceforge.net/projects/mdbtools/
mdcrack	1.2	MD4/MD5/NTLM1 hash cracker	http://c3rb3r.openwall.net/mdcrack/
mdk3	v6	WLAN penetration tool	http://aspj.aircrack-ng.org/
mdns-recon	6.2d6b5e3	An mDNS recon tool written in Python.	https://github.com/chadillac/mdns_recon
mdns-scan	0.5	Scan mDNS/DNS-SD published services on the local network.	
medusa	2.2	Speedy, massively parallel and modular login brute-forcer for network	http://www.foofus.net/jmk/medusa/medusa.html
melkor	1.0	An ELF fuzzer that mutates the existing data in an ELF sample given to create orcs (malformed ELFs), however, it does not change values randomly (dumb fuzzing), instead, it fuzzes certain metadata with semi-valid values through the use of fuzzing rules (knowledge base).	http://packetstormsecurity.com/files/127924/Melkor-ELF-Fuzzer.0.html
memdump	1.01	Dumps system memory to stdout, skipping over holes in memory maps.	http://www.porcupine.org/forensics/tct.html
memfetch	0.05b	Dumps any userspace process memory without affecting its execution.	http://lcamtuf.coredump.cx/
metacoretex	0.8.0	MetaCoretex is an entirely JAVA vulnerability scanning framework for databases.	http://metacoretex.sourceforge.net/
metagoofil	1.4b	An information gathering tool designed for extracting metadata of public documents	http://www.edge-security.com/metagoofil.php
metasploit	37458.e059f42	Платформа с открытым исходным кодом, которая позволяет исследовать уязвимости, разработку эксплойтов и создание пользовательских инструментов безопасности, представляет самую большую коллекцию эксплойтов с проверенным качеством.	http://www.metasploit.com
meterssh	10.ebb6f4e	A way to take shellcode, inject it into memory then tunnel whatever port you want to over SSH to mask any type of communications as a normal SSH connection.	https://github.com/trustedsec/meterssh
metoscan	05	Tool for scanning the HTTP methods supported by a webserver. It works by testing a URL and checking the responses for the different requests.	http://www.open-labs.org/
mfcuk	0.3.8	MIFARE Classic Universal toolKit	http://code.google.com/p/mfcuk/
mfoc	0.10.7	Mifare Classic Offline Cracker	http://code.google.com/p/mfoc/
mfsniffer	0.1	A python script for capturing unencrypted TSO	http://packetstormsecurity.com/files/1208

Имя	Версия	Описание	Домашняя страница
		login credentials.	02/MF-Sniffer-TN3270-Password-Grabber.html
mibble	2.9.3	Mibble is an open-source SNMP MIB parser (or SMI parser) written in Java. It can be used to read SNMP MIB files as well as simple ASN.1 files.	http://www.mibble.org/
middler	1.0	A Man in the Middle tool to demonstrate protocol middling attacks.	http://code.google.com/p/middler/
mikrotik-npk	11.d54e97c	Python tools for manipulating Mikrotik NPK format.	https://github.com/kost/mikrotik-npk
minimodem	319.3a8d490	Программа командной строки, которая декодирует (или генерирует) тоны аудио модемов на любой заданной скорости передачи, используя различные фреймовые протоколы.	https://github.com/kamalmostafa/minimodem
minimysqlator	0.5	A multi-platform application used to audit web sites in order to discover and exploit SQL injection vulnerabilities.	http://www.scrt.ch/en/attack/downloads/mini-mysqlat0r
miranda-upnp	1.3	A Python-based Universal Plug-N-Play client application designed to discover, query and interact with UPNP devices	http://code.google.com/p/miranda-upnp/
miredo	1.2.6	Teredo client and server.	http://www.remlab.net/miredo/
missidentify	1.0	A program to find Win32 applications.	http://missidentify.sourceforge.net/
missionplanner	1.2.55	A GroundControl Station for Ardupilot.	https://code.google.com/p/ardupilot-mega/wiki/Mission
mitmap	0.1	Shell Script for launching a Fake AP with karma functionality and launches ettercap for packet capture and traffic manipulation.	http://www.darkoperator.com/tools-and-scripts/
mitmer	22.b01c7fe	A man-in-the-middle and phishing attack tool that steals the victim's credentials of some web services like Facebook.	https://github.com/husam212/MITMer
mitmf	429.06ef1da	Фреймворк для атак Человек-Посередине, написан на Python.	https://github.com/byt3bl33d3r/MITMf
mitmproxy	0.16	Совместимый с SSL прокси HTTP человек-посередине.	http://mitmproxy.org/
mkbrutus	1.0.2	Password bruteforcer for MikroTik devices or boxes running RouterOS.	http://mkbrutusproject.github.io/MKBRUTUS/
mobiusft	0.5.21	An open-source forensic framework written in Python/GTK that manages cases and case items, providing an abstract interface for developing extensions.	http://savannah.nongnu.org/projects/mobiusft
mobsf	129.a594b08	Умный, сделанный по принципу "всё в одном" фреймворк с открытым исходным кодом для автоматического тестирования на проникновение мобильных приложений (Android/iOS), способный выполнять статичный, динамический анализ и тестирование веб API.	https://github.com/ajinabraham/Mobile-Security-Framework-MobSF
modscan	0.1	A new tool designed to map a SCADA MODBUS TCP based network.	https://code.google.com/p/modscan/
moloch	0.11.3	С открытым исходным кодом, захват в больших масштабах IPv4 полных PCAP, индексирование и система базы данных.	https://github.com/aol/moloch
monocle	1.0	A local network host discovery tool. In passive mode, it will listen for ARP request and reply packets. In active mode, it will send ARP	http://packetstormsecurity.com/files/99823/Monocle-Host-Discovery-Tool.0.html

Имя	Версия	Описание	Домашняя страница
		requests to the specific IP range. The results are a list of IP and MAC addresses present on the local network.	
morxbook	1.0	A password cracking tool written in perl to perform a dictionary-based attack on a specific Facebook user through HTTPS.	http://www.morxploit.com/
morxbrute	1.01	A customizable HTTP dictionary-based password cracking tool written in Perl	http://www.morxploit.com/morxbrute/
morxbtcrack	1.0	Single Bitcoin private key cracking tool released.	http://www.morxploit.com/tools/
morxcoinpwn	1.0	Mass Bitcoin private keys brute forcing/Take over tool released.	http://www.morxploit.com/tools/
morxcrack	1.2	A cracking tool written in Perl to perform a dictionary-based attack on various hashing algorithm and CMS salted-passwords.	http://www.morxploit.com/morxcrack/
morxkeyfmt	1.0	Read a private key from stdin and output formatted data values.	http://www.morxploit.com/tools/
morxtraversal	1.0	Path Traversal checking tool.	http://www.morxploit.com/tools/
morxtunnel	1.0	Network Tunneling using TUN/TAP interfaces over TCP tool.	http://www.morxploit.com/tools/
mosca	76.e67dcfd	Инструмент статического анализа для поиска ошибок, наподобие команды unix grep.	https://github.com/CoolerVoid/Mosca
mosquito	39.fe54831	Инструмент исследования XSS - доступ к жертвам через HTTP прокси.	https://github.com/koto/mosquito
mots	5.34017ca	Man on the Side Attack - experimental packet injection and detection.	https://github.com/kevinkoo001/MotS
mp3nema	0.4	A tool aimed at analyzing and capturing data that is hidden between frames in an MP3 file or stream, otherwise noted as "out of band" data.	http://packetstormsecurity.com/files/76432/MP3nema-Forensic-Analysis-Tool.html
mptcp	1.9.0	A tool for manipulation of raw packets that allows a large number of options.	http://packetstormsecurity.com/files/119132/Mptcp-Packet-Manipulator.9.0.html
mptcp-abuse	6.b0eeb27	A collection of tools and resources to explore MPTCP on your network. Initially released at Black Hat USA 2014.	https://github.com/Neohapsis/mptcp-abuse
mrtparse	395.48eb6f1	A module to read and analyze the MRT format data.	https://github.com/YoshiyukiYamauchi/mrtparse
ms-sys	2.5.3	Инструмент для написания Win9x-.. главных загрузочный записей (mbr) под linux - RTM!	http://ms-sys.sourceforge.net/
msf-mpc	19.b18f793	Генератор рабочей нагрузки для msfvenom (часть Metasploit).	https://github.com/g0tmi1k/mpc
mssqlscan	0.8.4	A small multi-threaded tool that scans for Microsoft SQL Servers.	http://www.cqure.net/wp/mssqlscan/
msvpwn	65.328921b	Bypass Windows' authentication via binary patching.	https://bitbucket.org/mrabault/msvpwn
mtr	0.86	Combines the functionality of traceroute and ping into one tool (CLI version)	http://www.bitwizard.nl/mtr/
multiinjector	0.3	Automatic SQL injection utility using a lsit of URI addresses to test parameter manipulation.	http://chaptersinwebsecurity.blogspot.de/2008/11/multiinjector-v03-released.html
multimac	1.0.3	Multiple MACs on an adapter	http://sourceforge.net/projects/multimac/
multimon-ng	20160303	Декодер sdr, поддерживает pocsag, ufsk, clipfsk, afsk, hapn, fsk, dtmf, zvei.	http://dekar.wc3edit.net/2012/05/24/multimonng/
multitun	43.9804513	Tunnel arbitrary traffic through an innocuous WebSocket.	https://github.com/covertcodes/multitun
mutator	51.164132d	This project aims to be a wordlist mutator with hormones, which means that some mutations will be applied to the result of the ones that have been	https://bitbucket.org/alone/mutator/

Имя	Версия	Описание	Домашняя страница
		already done, resulting in something like: corporation -> C0rp0r4t10n_2012	
mwebfp	16.a800b98	Mass Web Fingerprinter.	https://github.com/falcon-lnhg/mwebfp
mysql2sqlite	14.e5b2c31	Converts a mysqldump file into a Sqlite 3 compatible file.	https://gist.github.com/esperlu/943776
nacker	23.b67bb39	A tool to circumvent 802.1x Network Access Control on a wired LAN.	https://github.com/carmaa/nacker
nasnum	5.df5df19	Скрипт для перечисления подключённых к сети хранилищ.	https://github.com/tcstool/nasnum
nbnspoof	1.0	NBNSpoof - NetBIOS Name Service Spoofer	http://www.mcgrewsecurity.com/tools/nbnspoof/
nbtenum	3.3	A utility for Windows that can be used to enumerate NetBIOS information from one host or a range of hosts.	http://reedarvin.thearvins.com/
nbtool	2.bf90c76	Some tools for NetBIOS and DNS investigation, attacks, and communication.	http://wiki.skullsecurity.org/Nbtool
nbtscan	1.5.1	NBTscan is a program for scanning IP networks for NetBIOS name information.	http://www.inetcat.net/software/nbtscan.html
ncpfs	2.2.6	Allows you to mount volumes of NetWare servers under Linux.	http://www.novell.com/
ncrack	0.4a	A high-speed network authentication cracking tool	http://nmap.org/ncrack/
necromant	3.acbc448	Python Script that search unused Virtual Hosts in Web Servers.	https://github.com/PentesterES/Necromant
neglected	8.68d02b3	Facebook CDN Photo Resolver.	https://github.com/GuerrillaWarfare/neglected
neighbor-cache-fingerprinter	83.f1e596f	An ARP based Operating System version scanner.	https://github.com/PherricOxide/Neighbor-Cache-Fingerprinter
nemesis	1.4	command-line network packet crafting and injection utility	http://nemesis.sourceforge.net/
net-creds	58.30b16c0	Sniffs sensitive data from interface or pcap.	https://github.com/DanMcInerney/net-creds
netbios-share-scanner	1.0	This tool could be used to check windows workstations and servers if they have accessible shared resources.	http://www.secpoint.com/netbios-share-scanner.html
netcommander	1.3	An easy-to-use arp spoofing tool.	https://github.com/evilsocket/netcommander
netcon	0.1	A network connection establishment and management script.	http://www.paramecium.org/~leendert/
netdiscover	0.3	An active/passive address reconnaissance tool, mainly developed for those wireless networks without dhcp server, when you are wardriving. It can be also used on hub/switched networks.	http://nixgeneration.com/~jaime/netdiscover/
netmap	0.1.3	Can be used to make a graphical representation of the surounding network.	http://netmap.sourceforge.net
netmask	2.4.3	Helps determine network masks	http://packages.qa.debian.org/n/netmask.html
netreconn	1.78	A collection of network scan/recon tools that are relatively small compared to their larger cousins.	http://packetstormsecurity.com/files/86076/NetReconn-Scanning-Tool-Collection.76.html
netscan	1.0	Tcp/Udp/Tor port scanner with: synpacket, connect TCP/UDP and socks5 (tor connection).	http://packetstormsecurity.com/files/125569/Netscan-Port-Scanner.0.html
netscan2	43.c225f25	Активное / пассивное сканирование сети.	https://github.com/walchko/netscan2
netsed	1.2	Small and handful utility design to alter the	http://silicone.homelinux.org/projects/net

Имя	Версия	Описание	Домашняя страница
		contents of packets forwarded thru network in real time.	sed/
netsniff-ng	0.6.1	Высокопроизводительный сниффер сети под Linux для инспекции пакетов.	http://netsniff-ng.org/
network-app-stress-tester	19.df75391	Network Application Stress Testing Yammer.	https://github.com/PherricOxide/Network-App-Stress-Tester
netzob	1.0rc1	Инструмент с открытым исходным кодом для обратной инженерии, генерации трафика и фаззинга протоколов коммуникации.	http://www.netzob.org/
nfcutils	0.3.2	Provides a simple 'lsnfc' command that list tags which are in your NFC device field	http://code.google.com/p/nfc-tools
nfdump	1.6.13	A set of tools to collect and process netflow data.	http://sourceforge.net/projects/nfdump/
nfex	2.5	A tool for extracting files from the network in real-time or post-capture from an offline tcpdump pcap savefile.	https://code.google.com/p/nfex/
nfspy	1.0	A Python library for automating the falsification of NFS credentials when mounting an NFS share.	https://github.com/bonsaiviking/NfSpy
nfsshell	19980519	Userland NFS command tool.	http://www.paramecium.org/~leendert/
ngrep	1.45	A grep-like utility that allows you to search for network packets on an interface.	http://ngrep.sourceforge.net/
nield	0.6.1	A tool to receive notifications from kernel through netlink socket, and generate logs related to interfaces, neighbor cache(ARP,NDP), IP address(IPv4,IPv6), routing, FIB rules, traffic control.	http://nield.sourceforge.net/
nikto	2.1.6	A web server scanner which performs comprehensive tests against web servers for multiple items	https://github.com/sullo/nikto
nimbostratus	54.c7c206f	Tools for fingerprintinging and exploiting Amazon cloud infrastructures.	https://github.com/andresriancho/nimbostratus
nipper	0.11.7	Network Infrastructure Parser	https://www.titania-security.com/
nishang	0.5.0	Using PowerShell for Penetration Testing.	https://code.google.com/p/nishang/
nkiller2	2.0	A TCP exhaustion/stressing tool.	http://sock-raw.org/projects.html
nmap	7.11	Утилита исследования сети и аудита безопасности.	http://nmap.org/
nmbscan	1.2.6	Tool to scan the shares of a SMB/NetBIOS network, using the NMB/SMB/NetBIOS protocols.	http://nmbscan.gbarbier.org/
nomorexor	0.1	Tool to help guess a files 256 byte XOR key by using frequency analysis	https://github.com/hiddenillusion/NoMoreXOR
nosqlmap	169.b2da8f5	Автоматизированный инструмент эксплуатации баз данных Mongo и веб-приложений NoSQL.	https://github.com/tcstool/NoSQLMap
notspikefile	0.1	A Linux based file format fuzzing tool	http://packetstormsecurity.com/files/39627/notSPIKEfile.tgz.html
nsdtool	0.1	A netgear switch discovery tool. It contains some extra features like bruteoforce and setting a new password.	http://www.curesec.com/en/publications/tools.html
nsec3walker	20101223	Enumerates domain names using DNSSEC	http://dnscurve.org/nsec3walker.html
nsia	1.0.6	A website scanner that monitors websites in realtime in order to detect defacements, compliance violations, exploits, sensitive information disclosure and other issues.	http://threatfactor.com/Products/
nsoq	1.9.5	A Network Security Tool for packet	http://www.nsoq.org/

Имя	Версия	Описание	Домашняя страница
		manipulation that allows a large number of options.	
ntds-decode	0.1	This application dumps LM and NTLM hashes from active accounts stored in an Active Directory database.	http://packetstormsecurity.com/files/121543/NTDS-Hash-Decoder.b.html
ntp-ip-enum	0.1	Script to pull addresses from a NTP server using the monlist command. Can also output Maltego resultset.	http://www.securepla.net/
o-saft	932.d9d5450	Инструмент для показа информации о SSL сертефикате, а также для тестирования SSL соединения в соответствии с данным списком шифров и различных SSL конфигураций.	https://www.owasp.org/index.php/O-Saft
oat	1.3.1	A toolkit that could be used to audit security within Oracle database servers.	http://www.cqure.net/wp/test/
obexstress	0.1	Script for testing remote OBEX service for some potential vulnerabilities.	http://bluetooth-pentest.narod.ru/
obfsproxy	0.2.13	A pluggable transport proxy written in Python	https://pypi.python.org/pypi/obfsproxy
oclhashcat	2.01	Worlds fastest WPA cracker with dictionary mutation engine.	http://hashcat.net/oclhashcat/
ocs	0.2	Compact mass scanner for Cisco routers with default telnet/enable passwords.	http://packetstormsecurity.com/files/119462/OCS-Cisco-Scanner.2.html
ohrwurm	0.1	A small and simple RTP fuzzer.	http://mazzoo.de/
oledump	0.0.22	Анализ файлов OLE (объединённый файловый двоичный формат). Эти файлы содержат потоки данных. Этот инструмент позволяет вам анализировать эти потоки.	http://blog.didierstevens.com/programs/oledump-py/
oletools	0.44	Инструмент для анализа файлов Microsoft OLE2.	http://www.decalage.info/python/oletools
ollydbg	201g	A 32-bit assembler-level analysing debugger	http://www.ollydbg.de
onesixtyone	0.7	An SNMP scanner that sends multiple SNMP requests to multiple IP addresses	http://labs.portcullis.co.uk/application/onesixtyone/
onionshare	590.3ed1f96	Безопасно и анонимно делитесь файлами любого размера.	https://github.com/micahflee/onionshare/
openstego	0.6.1	A tool implemented in Java for generic steganography, with support for password-based encryption of the data.	http://www.openstego.info/
opensvp	64.56b2b8f	A security tool implementing "attacks" to be able to the resistance of firewall to protocol level attack.	https://github.com/regit/opensvp
openvas-cli	1.4.3	The OpenVAS Command-Line Interface	http://www.openvas.org/
openvas-libraries	8.0.5	The OpenVAS libraries	http://www.openvas.org/
openvas-manager	6.0.6	A layer between the OpenVAS Scanner and various client applications	http://www.openvas.org/
openvas-scanner	5.0.4	The OpenVAS scanning Daemon	http://www.openvas.org/
ophcrack	3.6.0	A free Windows password cracker based on rainbow tables	http://ophcrack.sourceforge.net
orakelcrackert	1.00	This tool can crack passwords which are encrypted using Oracle's latest SHA1 based password protection algorithm.	http://freeworld.thc.org/thc-orakelcrackert11g/
origami	1.2.7	Aims at providing a scripting tool to generate and analyze malicious PDF files.	http://code.google.com/p/origami-pdf
oscanner	1.0.6	An Oracle assessment framework developed in Java.	http://www.cqure.net/wp/oscanner/

Имя	Версия	Описание	Домашняя страница
osinterator	3.8447f58	Open Source Toolkit for Open Source Intelligence Gathering.	https://github.com/guitarmanj/OSINTerator
ostinato	0.6	An open-source, cross-platform packet/traffic generator and analyzer with a friendly GUI. It aims to be "Wireshark in Reverse" and thus become complementary to Wireshark.	http://code.google.com/p/ostinato/
osueta	65.90323e2	A simple Python script to exploit the OpenSSH User Enumeration Timing Attack.	https://github.com/c0r3dump3d/osueta
otori	0.3	A python-based toolbox intended to allow useful exploitation of XML external entity ("XXE") vulnerabilities.	http://www.beneaththewaves.net/Software/On_The_Outside_Reaching_In.html
outguess	0.2	A universal steganographic tool.	http://www.outguess.org/
outlook-webapp-brute	1.61d7177	Microsoft Outlook WebAPP Brute.	https://github.com/lijiejie/OutLook_WebAPP_Brute
owabf	1.3	Outlook Web Access bruteforcer tool.	http://netsec.rs/70/tools.html
owasp-bywaf	26.e730d1b	A web application penetration testing framework (WAPTF).	https://github.com/depasonico/OWASP-ByWaf
owtf	1017.0bbeea1	The Offensive (Web) Testing Framework.	https://www.owasp.org/index.php/OWASP_OWTF
p0f	3.08b	Purely passive TCP/IP traffic fingerprinting tool	http://lcamtuf.coredump.cx/p0f3/
pack	0.0.4	Password Analysis and Cracking Kit	http://thesprawl.org/projects/pack/
packerid	1.4	Script which uses a PEiD database to identify which packer (if any) is being used by a binary.	http://handlers.sans.org/jclausing/
packet-o-matic	351	A real time packet processor. Reads the packet from an input module, match the packet using rules and connection tracking information and then send it to a target module.	http://www.packet-o-matic.org/
packeth	1.8.1	A Linux GUI packet generator tool for ethernet.	http://packeth.sourceforge.net/
packetsender	147.5f2c755	Утилита с открытым кодом, которая позволяет отправлять и получать TCP и UDP пакеты.	https://github.com/dannagle/PacketSender
packit	1.0	A network auditing tool. Its value is derived from its ability to customize, inject, monitor, and manipulate IP traffic.	http://packit.sourceforge.net/
pacumen	1.92a0884	Packet Acumen - Analyse encrypted network traffic and more (side-channel attacks).	https://github.com/bniemczyk/pacumen
padbuster	0.3.3	Automated script for performing Padding Oracle attacks.	http://www.gdssecurity.com/l/t.php
paketto	1.10	Advanced TCP/IP Toolkit.	http://www.doxpara.com/paketto
panhunt	26.cd58866	Searches for credit card numbers (PANs) in directories.	https://github.com/Dionach/PANhunt
panoptic	182.b5eae6b	A tool that automates the process of search and retrieval of content for common log and config files through LFI vulnerability.	https://github.com/lightos/Panoptic
pappy-proxy	30.9a58a91	Прокси перехватчик для тестирования веб-приложений.	https://github.com/roglew/pappy-proxy
paranoic	1.7	A simple vulnerability scanner written in Perl.	http://packetstormsecurity.com/files/128065/Paranoic-Scan.7.html
paros	3.2.13	Java-based HTTP/HTTPS proxy for assessing web app vulnerabilities. Supports editing/viewing HTTP messages on-the-fly, spiders, client certificates, proxy-chaining, intelligent scanning for XSS and SQLi, etc.	http://www.parosproxy.org
parsero	81.e5b585a	A robots.txt audit tool.	https://github.com/behindthefirewalls/Parsero

Имя	Версия	Описание	Домашняя страница
pasco	20040505_1	Examines the contents of Internet Explorer's cache files for forensic purposes	http://www.jonesdykstra.com/
passcracking	20131214	A little python script for sending hashes to passcracking.com and milw0rm	http://github.com/jensp/passcracking
passe-partout	0.1	Tool to extract RSA and DSA private keys from any process linked with OpenSSL. The target memory is scanned to lookup specific OpenSSL patterns.	http://www.hsc.fr/ressources/outils/passe-partout/index.html.en
passhunt	5.332f374	Search drives for documents containing passwords.	https://github.com/Dionach/PassHunt
passivedns	1.1.4	A network sniffer that logs all DNS server replies for use in a passive DNS setup.	https://github.com/gamelinux/passivedns
pastenum	0.4.1	Search Pastebins for content, fork from nullthreat corelan pastenum2	http://github.com/shadowbq/pastenum
pasv-agrsv	51.446bed4	Passive recon / OSINT automation script.	https://github.com/isaudits/pasv-agrsv
patator	119.142d48c	Многоцелевой брутфорсер.	https://github.com/lanjelot/patator
pblind	1.0	Little utility to help exploiting blind sql injection vulnerabilities.	http://www.edge-security.com/pblind.php
pcapfix	1.1.0	Tries to repair your broken pcap and pcapng files.	http://f00l.de/pcapfix/
pcapsipdump	0.2	A tool for dumping SIP sessions (+RTP traffic, if available) to disk in a fashion similar to 'tcpdump -w' (format is exactly the same), but one file per sip session (even if there is thousands of concurrect SIP sessions).	http://pcapsipdump.sourceforge.net/
pcapteller	0.2	A tool designed for traffic manipulation and replay.	https://www.encripto.no/nb/downloads/tools/
pcredz	29.05ae40f	A tool that extracts credit card numbers, NTLM(DCE-RPC, HTTP, SQL, LDAP, etc), Kerberos (AS-REQ Pre-Auth etype 23), HTTP Basic, SNMP, POP, SMTP, FTP, IMAP, and more from a pcap file or from a live interface.	https://github.com/lgandx/PCredz
pdf-parser	0.6.4	Parses a PDF document to identify the fundamental elements used in the analyzed file.	http://blog.didierstevens.com/programs/pdf-tools/
pdfbook-analyzer	2	Utility for facebook memory forensics.	http://sourceforge.net/projects/pdfbook/
pdfcrack	0.15	Password recovery tool for PDF-files.	http://pdfcrack.sourceforge.net/
pdfid	0.2.1	Scan a file to look for certain PDF keywords.	http://blog.didierstevens.com/programs/pdf-tools/
pdfresurrect	0.12	A tool aimed at analyzing PDF documents.	http://packetstormsecurity.com/files/118459/PDFResurrect-PDF-Analyzer.12.html
pdgmail	1.0	A password dictionary attack tool that targets windows authentication via the SMB protocol	http://www.jeffbryner.com/code/pdgmail
peach	3.0.202	A SmartFuzzer that is capable of performing both generation and mutation based fuzzing.	http://peachfuzzer.com/
peda	76.c9ceca7	Python Exploit Development Assistance for GDB.	https://github.com/longld/peda
peepdf	0.3	A Python tool to explore PDF files in order to find out if the file can be harmful or not	http://eternal-todo.com/tools/peepdf-pdf-analysis-tool
peepingtom	56.bc6f4d8	A tool to take screenshots of websites. Much like eyewitness.	https://bitbucket.org/LaNMaSteR53/peepingtom
peframe	90.c9dba76	Инструмент выполняет статический анализ (портативно исполняемого) зловреда.	https://github.com/guelfoweb/peframe
pemcrack	11.a0fecd7	Cracks SSL PEM files that hold encrypted private keys. Brute forces or dictionary cracks.	https://github.com/robertdavidgraham/pemcrack

Имя	Версия	Описание	Домашняя страница
pemcracker	9.a741c93	Tool to crack encrypted PEM files.	https://github.com/bwall/pemcracker.git
pentbox	1.8	A security suite that packs security and stability testing oriented tools for networks and systems.	http://www.pentbox.net
pev	0.70	Command line based tool for PE32/PE32+ file analysis.	http://pev.sourceforge.net/
pextractor	0.18b	A forensics tool that can extract all files from an executable file created by a joiner or similar.	http://packetstormsecurity.com/files/62977/PExtractor_v0.18b_binary_and_src.rar.html
pfff	0.29	Tools and APIs for code analysis, visualization and transformation	https://github.com/facebook/pfff
pgdbf	94.baa1d95	Convert XBase / FoxPro databases to PostgreSQL	https://github.com/kstrauser/pgdbf
phemail	27.7ae21f2	A python open source phishing email tool that automates the process of sending phishing emails as part of a social engineering test.	https://github.com/Dionach/PhEmail
phoss	0.1.13	Sniffer designed to find HTTP, FTP, LDAP, Telnet, IMAP4, VNC and POP3 logins.	http://www.phenoelit.org/fr/tools.html
php-mt-seed	3.2	PHP mt_rand() seed cracker	http://www.openwall.com/php_mt_seed/
php-rfi-payload-decoder	30.bd42caa	Decode and analyze RFI payloads developed in PHP.	https://github.com/bwall/PHP-RFI-Payload-Decoder
php-vulnerability-hunter	1.4.0.20	An whitebox fuzz testing tool capable of detected several classes of vulnerabilities in PHP web applications.	https://phpvulnhunter.codeplex.com/
phpsploit	650.df68e79	Незаметный фреймворк последующей эксплуатации.	https://github.com/nil0x42/phpsploit
phpstress	5.f987a7e	A PHP denial of service / stress test for Web Servers running PHP-FPM or PHP-CGI.	https://github.com/nightlionsecurity/phpstress
phrasendrescher	1.2.2	A modular and multi processing pass phrase cracking tool	http://www.leidecker.info/projects/phrasendrescher/
pip3line	80.2e926b0	The Swiss army knife of byte manipulation.	https://github.com/nccgroup/pip3line
pipal	1.1	A password analyser	http://www.digininja.org/projects/pipal.php
pipeline	17.468a058	Создан для содействия в целенаправленных атаках на взлом паролей грубой силой.	https://github.com/hirnschallsebastian/Pipeline2
pirana	0.3.1	Exploitation framework that tests the security of a email content filter.	http://www.guay-leroux.com/projects.html
pkcrack	1.2.2	Взломщик шифрования PkZip.	https://www.unix-ag.uni-kl.de/~conrad/krypto/pkcrack/download1.html
plcscan	0.1	This is a tool written in Python that will scan for PLC devices over s7comm or modbus protocols.	http://packetstormsecurity.com/files/119726/PLC-Device-Scanner.html
plecost	87.07409aa	Wordpress finger printer Tool.	https://github.com/iniqua/plecost
plown	13.ccf998c	A security scanner for Plone CMS.	https://github.com/unweb/plown
pmap	1.10	Пассивно обнаруживает, сканирует и снимает отпечатки у связанных локально пиров по фоновому шуму, который они генерируют (например по их широковещательному и многоадресному трафику).	http://www.hellfiresecurity.com/tools.htm
pmcma	1.00	Automated exploitation of invalid memory writes (being them the consequences of an overflow in a writable section, of a missing format string, integer overflow, variable misuse, or any other type of memory corruption).	http://packetstormsecurity.com/files/104724/Post-Memory-Corruption-Memory-Analyzer.00.html
pnscan	1.11	A parallel network scanner that can be used to	http://www.lysator.liu.se/~pen/pnscan/

Имя	Версия	Описание	Домашняя страница
		survey TCP network services.	
poison	1.5.41	A fast, asynchronous syn and udp scanner.	http://nologin.org/main.pl?action=codeList&
pompem	85.a2dc2bb	A python exploit tool finder.	https://github.com/rfunix/Pompem
portmanteau	1.0	An experimental unix driver IOCTL security tool that is useful for fuzzing and discovering device driver attack surface.	https://packetstormsecurity.com/files/134230/Portmanteau-Unix-Driver-IOCTL-Security-Tool.html
portspoof	100.70b6bf2	This program's primary goal is to enhance OS security through a set of new techniques.	http://portspoof.org/
posttester	0.1	A jar file that will send POST requests to servers in order to test for the hash collision vulnerability discussed at the Chaos Communication Congress in Berlin.	http://packetstormsecurity.com/files/109010/MagicHash-Collision-Testing-Tool.html
powerfuzzer	1_beta	Powerfuzzer is a highly automated web fuzzer based on many other Open Source fuzzers available (incl. cfuzzer, fuzzled, fuzzer.pl, jbrofuzz, webscarab, wapiti, Socket Fuzzer). It can detect XSS, Injections (SQL, LDAP, commands, code, XPATH) and others.	http://www.powerfuzzer.com
powersploit	318.2a813fa	Фреймвок последующей эксплуатации PowerShell.	https://github.com/mattifestation/PowerSploit
pr0cks	16.e1fb6f7	Скрипт на python, поднимает прозрачный прокси для перенаправления всего TCP и DNS трафика через SOCKS / SOCKS5 или HTTP(CONNECT) прокси, используя цель iptables -j REDIRECT.	https://github.com/n1nj4sec/pr0cks
prads	1124.dabcaa2	Is a "Passive Real-time Asset Detection System".	http://gamelinux.github.io/prads/
praeda	37.093d1c0	An automated data/information harvesting tool designed to gather critical information from various embedded devices.	https://github.com/percx/Praeda
princeprocessor	115.26cefc9	Standalone password candidate generator using the PRINCE algorithm.	https://github.com/jsteube/princeprocessor/
procyon	0.5.30	A suite of Java metaprogramming tools focused on code generation and analysis.	https://bitbucket.org/mstrobel/procyon/
prometheus	176.a316d66	A Firewall analyzer written in ruby	https://github.com/averagesecurityguy/prometheus
propecia	2	A fast class scanner that scans for a specified open port with banner grabbing	http://www.redlevel.org
protos-sip	2	SIP test suite.	https://www.ee.oulu.fi/research/ouspg/PROTOS_Test-Suite_c07-sip
proxenet	589.3e07775	THE REAL hacker friendly proxy for web application pentests.	https://github.com/hugsy/proxenet
proxmark	1434.d889dac	Мощный инструмент общего назначения RFID (радиочастотной идентификации), размером с колоду карт, прибор предназначен для подглядывания, подслушивания и подражания всему, с низкой частоты (125kHz) до высокой частоты (13.56MHz).	https://github.com/Proxmark/proxmark3
proxychains-ng	4.11	Предварительно загружаемый хук, который позволяет перенаправлять TCP трафик существующих динамично подключаемых программ через один или более SOCKS или HTTP прокси.	https://github.com/rofl0r/proxychains
proxycheck	0.1	This is a simple proxy tool that checks for the HTTP CONNECT method and grabs verbose output from a webserver.	http://packetstormsecurity.com/files/61864/proxycheck.pl.txt.html

Имя	Версия	Описание	Домашняя страница
proxyp	2013	Small multithreaded Perl script written to enumerate latency, port numbers, server names, & geolocations of proxy IP addresses.	http://sourceforge.net/projects/proxyp/
proxyscan	0.3	A security penetration testing tool to scan for hosts and ports through a Web proxy server.	http://packetstormsecurity.com/files/69778/proxyScan.3.tgz.html
proxytunnel	1.9.0	a program that connects stdin and stdout to a server somewhere on the network, through a standard HTTPS proxy	http://proxytunnel.sourceforge.net
pscan	1.3	A limited problem scanner for C source files	http://deployingradius.com/pscan/
pshitt	23.dae7931	A lightweight fake SSH server designed to collect authentication data sent by intruders.	https://github.com/regit/pshitt
pstoreview	1.0	Lists the contents of the Protected Storage.	http://www.ntsecurity.nu/toolbox/pstoreview/
ptf	434.a4105a8	Фреймворк тестеров на проникновения - устанавливает в неспециализированные дистрибутивы программы для тестирования на проникновение.	https://github.com/trustedsec/ptf
ptunnel	0.72	A tool for reliably tunneling TCP connections over ICMP echo request and reply packets	http://www.cs.uit.no/~daniels/PingTunnel/#download
pwd-hash	2.0	A password hashing tool that use the crypt function to generate the hash of a string given on standard input.	http://vladz.devzero.fr/pwd-hash.php
pwdump	7.1	Extracts the binary SAM and SYSTEM file from the filesystem and then the hashes.	http://www.tarasco.org/security/pwdump_7/index.html
pwnat	9.1d07c2e	A tool that allows any number of clients behind NATs to communicate with a server behind a separate NAT with *no* port forwarding and *no* DMZ setup on any routers in order to directly communicate with each other.	http://samy.pl/pwnat/
pwntools	2.2.0	The CTF framework used by #Gallopsled in every CTF.	https://github.com/Gallopsled/pwntools
pyersinia	47.e59812b	Network attack tool like yersinia but written in Python.	https://github.com/nottinghamprisateam/pyersinia
pyew	100.2d086a1	A python tool to analyse malware.	https://code.google.com/p/pyew/
pyexfil	36.978ec43	A couple of beta stage tools for data exfiltration.	https://github.com/ytisf/PyExfil
pyfiscan	1481.e76be65	Бесплатный сканер уязвимостей и версий веб-приложений.	https://github.com/fgeek/pyfiscan
pyinstaller	3.1.1	Программа, которая конвертирует (пакеты) программ Python в самостоятельные исполнимые файлы, на Windows, Linux, Mac OS X, Solaris и AIX.	http://www.pyinstaller.org/
pyminifakedns	0.1	Minimal DNS server written in Python; it always replies with a 127.0.0.1 A-record	http://code.activestate.com/recipes/491264/
pyrasite	2.0	Code injection and introspection of running Python processes.	http://pyrasite.com/
pyrit	0.4.0	WPA/WPA2-PSK attacking with gpu and cluster	https://code.google.com/p/pyrit
pytacle	alpha2	Automates the task of sniffing GSM frames	http://packetstormsecurity.com/files/124299/pytacle-alpha2.tar.gz
pytbull	2.0	A python based flexible IDS/IPS testing framework shipped with more than 300 tests	http://pytbull.sourceforge.net/
python-capstone	3.0.4	A lightweight multi-platform, multi-architecture disassembly framework	http://www.capstone-engine.org/index.html
python-utidylib	0.2	Python bindings for Tidy HTML parser/cleaner.	http://utidylib.berlios.de
python2-	0.4.0	Ultra-lightweight pure Python package to check	https://github.com/audreyr/binaryornot

Имя	Версия	Описание	Домашняя страница
binaryornot		if a file is binary or text.	
python2-capstone	3.0.4	A lightweight multi-platform, multi-architecture disassembly framework	http://www.capstone-engine.org/index.html
python2-yara	3.4.0	Tool aimed at helping malware researchers to identify and classify malware samples	https://plusvic.github.io/yara/
qark	9.96fc6db	Tool to look for several security related Android application vulnerabilities.	https://github.com/linkedin/qark
quickrecon	0.3.2	A python script for simple information gathering. It attempts to find subdomain names, perform zone transfers and gathers emails from Google and Bing.	http://packetstormsecurity.com/files/104314/QuickRecon.3.2.html
radamsa	0.4	General purpose data fuzzer.	https://github.com/aoh/radamsa
radare2	0.10.1	Инструмент с открытым исходным кодом для дизассемблирования, отладки, анализа и манипулирования бинарными файлами.	http://radare.org
radiography	2	A forensic tool which grabs as much information as possible from a Windows system.	http://www.security-projects.com/?RadioGraPhy
rainbowcrack	1.6	Password cracker based on the faster time-memory trade-off. With MySQL and Cisco PIX Algorithm patches.	http://project-rainbowcrack.com/
ranger-scanner	108.0c70888	Инструмент для поддержания профессионалов по безопасности в доступе и взаимодействию с удалёнными системами на основе Microsoft Windows.	https://github.com/funkandwagnalls/ranger
rarcrack	0.2	This program uses bruteforce algorithm to find correct password (rar, 7z, zip).	http://rarcrack.sourceforge.net/
ratproxy	1.58	A passive web application security assessment tool	http://code.google.com/p/ratproxy/
rawr	71.f9a4f40	Быстрая оценка веб-ресурсов. Веб-перечислитель.	https://bitbucket.org/al14s/rawr/wiki/Home
rcracki-mt	0.7.0	A tool to perform rainbow table attacks on password hashes. It is intended for indexed/perfected rainbow tables, mainly generated by the distributed project www.freerainbowtables.com	http://rcracki.sourceforge.net/
rdesktop-brute	1.5.0	It connects to windows terminal servers - Bruteforce patch included.	http://www.rdesktop.org/
reaver	1.4	Brute force attack against Wifi Protected Setup	http://code.google.com/p/reaver-wps/
rebind	0.3.4	DNS Rebinding Tool	http://code.google.com/p/rebind/
recon-ng	4.7.3	Полнофункциональный фреймворк веб-разведки, написан на Python.	https://bitbucket.org/LaNMaSteR53/recon-ng
recoverjpeg	2.6	Recover jpegs from damaged devices.	http://www.rfc1149.net/devel/recoverjpeg
recstudio	4.0_20130717	Cross platform interactive decompiler	http://www.backerstreet.com/rec/rec.htm
redfang	2.5	Finds non-discoverable Bluetooth devices by brute-forcing the last six bytes of the devices' Bluetooth addresses and calling read_remote_name().	http://packetstormsecurity.com/files/31864/redfang.2.5.tar.gz.html
redirectpoison	1.1	A tool to poison a targeted issuer of SIP INVITE requests with 301 (i.e. Moved Permanently) redirection responses.	http://www.hackingexposedvoip.com/
redpoint	123.23ef36b	Digital Bond's ICS Enumeration Tools.	https://github.com/digitalbond/Redpoint3
regeorg	28.0ead547	Преемник reDuh, создаёт SOCKS прокси через DMZ.	https://github.com/sensepost/reGeorg
reglookup	1.0.1	Command line utility for reading and querying	http://projects.sentinelchicken.org/regloo

Имя	Версия	Описание	Домашняя страница
		Windows NT registries	kup
relay-scanner	1.7	An SMTP relay scanner.	http://www.cirt.dk
replayproxy	1.1	Forensic tool to replay web-based attacks (and also general HTTP traffic) that were captured in a pcap file.	https://code.google.com/p/replayproxy/
responder	157.4906e7d	Травильщик LLMNR и NBT-NS со встроенным мошенническим сервером HTTP/SMB/MSSQL/FTP/LDAP аутентификации, поддерживающим NTLMv1/NTLMv2/LMv2, Extended Security NTLMSSP и базовую HTTP аутентификацию.	https://github.com/SpiderLabs/Responder/
reverse	659.1e79d9e	Инструмент обратной инженерии для x86/ARM/MIPS. Генерирует отформатированный псевдо-C код с цветной подсветкой синтаксиса.	https://github.com/joelpx/reverse
revipd	5.2aaacfb	A simple reverse IP domain scanner.	https://github.com/PypeRanger/revipd
rext	40.43ca8f6	Router EXploitation Toolkit (инструмент эксплуатации роутеров) - маленький набор инструментов для простого создания и использования различных скриптов на python, которые работают со встроенным оборудованием.	https://github.com/j91321/rext
rfcat	150225	RF ChipCon-based Attack Toolset.	http://code.google.com/p/rfcat
rfdump	1.6	A back-end GPL tool to directly inter-operate with any RFID ISO-Reader to make the contents stored on RFID tags accessible	http://www.rfdump.org
rfidiot	71.ed1732f	An open source python library for exploring RFID devices.	http://rfidiot.org/
rfidtool	0.01	A opensource tool to read / write rfid tags	http://www.bindshell.net/tools/rfidtool.html
ridenum	40.a50ea22	A null session RID cycle attack for brute forcing domain controllers.	https://github.com/trustedsec/ridenum
rifiuti2	0.6.1	A rewrite of rifiuti, a great tool from Foundstone folks for analyzing Windows Recycle Bin INFO2 file.	https://code.google.com/p/rifiuti2/
rinetd	0.62	internet redirection server	http://www.boutell.com/rinetd
ripdc	0.2	A script which maps domains related to an given ip address or domainname.	http://nullsecurity.net/tools/scanner
rkhunter	1.4.2	Checks machines for the presence of rootkits and other unwanted tools.	http://rkhunter.sourceforge.net/
rlogin-scanner	0.2	Multithreaded rlogin scanner. Tested on Linux, OpenBSD and Solaris.	http://wayreth.eu.org/old_page/
rootbrute	0.1	Local root account bruteforcer.	http://www.packetstormsecurity.org/
ropeadope	1.1	A linux log cleaner.	http://www.highhacksociety.com/
ropeme	1.0	ROPME is a set of python scripts to generate ROP gadgets and payload.	http://www.vnsecurity.net/2010/08/ropeme-rop-exploit-made-easy/
ropgadget	5.4	Lets you search your gadgets on your binaries (ELF format) to facilitate your ROP exploitation.	https://github.com/JonathanSalwan/ROPgadget
ropper	1.7.3	Show information about binary files and find gadgets to build rop chains for different architectures	https://github.com/sashs/Ropper
roputils	189.07fc123	A Return-oriented Programming toolkit.	https://github.com/inaz2/roputils
routerhunter	19.0c9cb3c	Инструмент используется для поиска в Интернете уязвимых роутеров и устройств и выполнения тестов.	https://github.com/jh00nbr/Routerhunter-2.0

Имя	Версия	Описание	Домашняя страница
rp	136.5f0841c	A full-cpp written tool that aims to find ROP sequences in PE/Elf/Mach-O x86/x64 binaries.	https://github.com/0vercl0k/rp
rpcsniffer	7.9fab095	Sniffs WINDOWS RPC messages in a given RPC server process.	https://github.com/AdiKo/RPCSniffer
rpdscan	2.a71b0f3	Remmina Password Decoder and scanner.	https://github.com/freakyclown/RPDscan
rrs	1.70	A reverse (connecting) remote shell. Instead of listening for incoming connections it will connect out to a listener (rrs in listen mode). With tty support and more.	http://www.cycom.se/dl/rrs
rsakeyfind	1.0	A tool to find RSA key in RAM.	http://citp.princeton.edu/memory/code/
rsmangler	1.4	rsmangler takes a wordlist and mangle it	http://www.randomstorm.com/rsmangler-security-tool.php
rspet	40.c76dae2	Основанная на Python обратная оболочка, снабжённая функциональностью, которая помогает в сценарии последующей эксплуатации.	https://github.com/panagiks/RSPET
rtlamr	197.03369d1	An rtl-sdr receiver for smart meters operating in the 900MHz ISM band.	https://github.com/bemasher/rtlamr/
rtlizer	35.5614163	Simple spectrum analyzer.	https://github.com/csete/rtlizer
rtlsdr-scanner	930.51ea2b9	Кроссплатформенный (на Python) графический интерфейс сканера частот OsmoSDR rtl-sdr библиотеки.	https://github.com/EarToEarOak/RTLSDR-Scanner
rtp-flood	1.0	RTP flooder	http://www.hackingexposedvoip.com/
rtpbreak	1.3a	Detects, reconstructs and analyzes any RTP session	http://xenion.antifork.org/rtpbreak/
rubilyn	0.0.1	64bit Mac OS-X kernel rootkit that uses no hardcoded address to hook the BSD subsystem in all OS-X Lion & below. It uses a combination of syscall hooking and DKOM to hide activity on a host.	http://nullsecurity.net/tools/backdoor.html
ruby-msgpack	0.7.0	MessagePack, a binary-based efficient data interchange format.	http://msgpack.org/
rww-attack	0.9.2	The Remote Web Workplace Attack tool will perform a dictionary attack against a live Microsoft Windows Small Business Server's 'Remote Web Workplace' portal. It currently supports both SBS 2003 and SBS 2008 and includes features to avoid account lock out.	http://packetstormsecurity.com/files/79021/Remote-Web-Workplace-Attack-Tool.html
safecopy	1.7	A disk data recovery tool to extract data from damaged media.	http://safecopy.sourceforge.net/
sagan	1.0.0	A snort-like log analysis engine.	https://quadrantsec.com/sagan_log_analysis_engine/
sakis3g	0.2.0e	An all-in-one script for connecting with 3G	http://www.sakis3g.org/
sambascan	0.5.0	Allows you to search an entire network or a number of hosts for SMB shares. It will also list the contents of all public shares that it finds.	http://sourceforge.net/projects/sambascan2/
samdump2	3.0.0	Dump password hashes from a Windows NT/2k/XP installation	http://sourceforge.net/projects/ophcrack/files/samdump2/
samydeluxe	2.2ed1bac	Automatic samdump creation script.	http://github.com/jensp/samydeluxe
sandy	6.531ab16	An open-source Samsung phone encryption assessment framework	https://github.com/donctl/sandy
saruman	1.1a8e77d	ELF anti-forensics exec, for injecting full dynamic executables into process image (With thread injection).	https://github.com/elfmaster/saruman
sasm	3.2.0	A simple crossplatform IDE for NASM, MASM, GAS and FASM assembly languages.	https://github.com/Dman95/SASM

Имя	Версия	Описание	Домашняя страница
sawef	28.e65dc9f	Инструмент для анализа веб-сайтов, особое внимание уделено сбору информации о веб-формах, сбору адресов эл.почты, ссылок.	https://github.com/danilovazb/sawef
sb0x	19.04f40fe	A simple and Lightweight framework for Penetration testing.	https://github.com/levi0x0/sb0x-project
sbd	1.36	Netcat-clone, portable, offers strong encryption - features AES-CBC + HMAC-SHA1 encryption, program execution (-e), choosing source port, continuous reconnection with delay + more	http://www2.packetstormsecurity.org/cgi-bin/search/search.cgi?searchvalue=sbd
scalpel	2.0	A frugal, high performance file carver	http://www.digitalforensicssolutions.com/Scalpel/
scanmem	0.15.6	Сканер памяти, предназначенный для изоляции адреса произвольной величины в выполняемой программе.	https://github.com/scanmem/scanmem
scanssh	2.1	Fast SSH server and open proxy scanner.	http://www.monkey.org/~provos/scanssh/
scapy	2.3.2	Мощная программа интерактивного манипулирования пакетами, написанная на Python	http://www.secdev.org/projects/scapy/
schnappi-dhcp	0.1	schnappi can fuck network with no DHCP	http://www.emanuelegentili.eu/
scout2	453.a616215	Security auditing tool for AWS environments.	http://isecpartners.github.io/Scout2/
scrape-dns	58.3df392f	Searches for interesting cached DNS entries.	https://github.com/304GEEK/Scrape-DNS
scrapy	1.0.5	Быстрый высокоуровневый фреймворк для обхода и извлечения нужных данных с веб-сайта.	http://scrapy.org
scrounge-ntfs	0.9	Data recovery program for NTFS file systems	http://memberwebs.com/stef/software/scrounge/
sctpscan	34.4d44706	A network scanner for discovery and security.	http://www.p1sec.com/
sdn-toolkit	1.01	Discover, Identify, and Manipulate SDN-Based Networks	http://www.hellfiresecurity.com/tools.htm
search1337	12.0887770	Онлайн сканнер эксплойтов 1337Day.	https://github.com/b3mb4m/Search1337
seat	0.3	Next generation information digging application geared toward the needs of security professionals. It uses information stored in search engine databases, cache repositories, and other public resources to scan web sites for potential vulnerabilities.	http://thesprawl.org/projects/search-engine-assessment-tool/
secscan	1.5	Web Apps Scanner and Much more utilities.	http://code.google.com/p/secscan-py/
secure-delete	3.1	Secure file, disk, swap, memory erasure utilities.	http://www.thc.org/
sees	67.cd741aa	Increase the success rate of phishing attacks by sending emails to company users as if they are coming from the very same company's domain.	https://github.com/galkan/sees/
sergio-proxy	0.2.1	A multi-threaded transparent HTTP proxy for manipulating web traffic	https://github.com/darkoperator/dnsrecon
sessionlist	1.0	Sniffer that intents to sniff HTTP packets and attempts to reconstruct interesting authentication data from websites that do not employ proper secure cookie auth.	http://www.0xrage.com/
set	6.5.9	Social-engineer toolkit. Aimed at penetration testing around Social-Engineering.	https://www.trustedsec.com/downloads/social-engineer-toolkit
sfuzz	0.7.0	A simple fuzzer.	http://aconole.brad-x.com/programs/sfuzz.html
shareenum	46.3bfa81d	Tool to enumerate shares from Windows hosts.	https://github.com/CroweCybersecurity/shareenum

Имя	Версия	Описание	Домашняя страница
shellcodecs	0.1	A collection of shellcode, loaders, sources, and generators provided with documentation designed to ease the exploitation and shellcode programming process.	http://www.blackhatlibrary.net/Shellcodecs
shellme	3.8c7919d	Because sometimes you just need shellcode and opcodes quickly. This essentially just wraps some nasm/objdump calls into a neat script.	https://github.com/hatRiot/shellme
shellnoob	2.1	A toolkit that eases the writing and debugging of shellcode	https://github.com/reyammer/shellnoob
shellsploit-framework	203.33e195e	Набор разработчика эксплойтов нового поколения.	https://github.com/b3mb4m/shellsploit-framework
sherlocked	1.f190c2b	Universal script packer-- transforms any type of script into a protected ELF executable, encrypted with anti-debugging.	https://github.com/elfmaster/sherlocked
shitflood	12.9b49c80	Флудер клонов Socks5 для протокола Internet Relay Chat (IRC).	https://github.com/acidvegas/shitflood
shocker	54.f5e7886	A tool to find and exploit servers vulnerable to Shellshock.	https://github.com/nccgroup/shocker
shodan	1.4.8	Библиотека на Python для Shodan (https://developer.shodan.io).	http://github.com/achillean/shodan-python
shortfuzzy	0.1	A web fuzzing script written in perl.	http://packetstormsecurity.com/files/104872/Short-Fuzzy-Rat-Scanner.html
sidguesser	1.0.5	Guesses sids/instances against an Oracle database according to a predefined dictionary file.	http://www.cqure.net/wp/tools/database/sidguesser/
siege	4.0.0	Утилита тестирования регрессий http, а также замера бенчмарков.	http://www.joedog.org/JoeDog/Siege
silk	3.11.0.1	A collection of traffic analysis tools developed by the CERT NetSA to facilitate security analysis of large networks.	https://tools.netsa.cert.org/silk/
simple-ducky	1.1.1	A payload generator.	https://code.google.com/p/simple-ducky-payload-generator
simple-lan-scan	1.0	A simple python script that leverages scapy for discovering live hosts on a network.	http://packetstormsecurity.com/files/97353/Simple-LAN-Scanner.0.html
simplyemail	241.b065fdb	Разведка Email сделалась быстрой и простой вместе с фреймворком сделанном на http://CyberSyndicates.com.	https://github.com/killswitch-GUI/SimplyEmail
sinfp	1.22	A full operating system stack fingerprinting suite.	http://www.networecon.com/tools/sinfp/
siparmyknife	11232011	A small command line tool for developers and administrators of Session Initiation Protocol (SIP) applications.	http://packetstormsecurity.com/files/107301/sipArmyKnife_11232011.pl.txt
sipbrute	11.5be2fdd	Утилита для выполнения атаки по словарю против хеша регистрации VoIP SIP.	https://github.com/packetassailant/sipbrute
sipcrack	0.2	A SIP protocol login cracker.	http://www.remote-exploit.org/codes_sipcrack.html
sipffer	27.f818593	Сниффер командной строки для протокола SIP.	https://github.com/xenomuta/SIPffer
sipp	3.3	A free Open Source test tool / traffic generator for the SIP protocol.	http://sipp.sourceforge.net/
sipsak	0.9.6	A small command line tool for developers and administrators of Session Initiation Protocol (SIP) applications.	http://sipsak.org
sipscan	0.1	A sip scanner.	http://www.hackingvoip.com/sec_tools.html
sipshock	6.1d636ab	A scanner for SIP proxies vulnerable to	https://github.com/zaf/sipshock

Имя	Версия	Описание	Домашняя страница
		Shellshock.	
sipvicious	0.2.8	Tools for auditing SIP devices	http://blog.sipvicious.org
skipfish	2.10b	A fully automated, active web application security reconnaissance tool	http://code.google.com/p/skipfish/
skul	4.846c091	Рабочий концепт для брутфорса Linux реализации Cryptsetup спецификации шифрования дисков (LUKS).	https://github.com/cryptcoffee/skul
skyjack	8.8b0a57c	Перехватывает дроны Parrot, деаутентифицирует их истинных владельцев и захватывает контроль, превращая из в дронов-зомби под вашим собственным контролем.	https://github.com/samyk/skyjack
skype-dump	0.1	This is a tool that demonstrates dumping MD5 password hashes from the configuration file in Skype.	http://packetstormsecurity.com/files/119155/Skype-Hash-Dumper.0.html
skypefreak	33.9347a65	Кроссплатформенный криминалистический фреймворк для Skype.	http://osandamalith.github.io/SkypeFreak/
sleuthkit	4.2.0	File system and media management forensic analysis tools	http://www.sleuthkit.org/sleuthkit
sloth-fuzzer	39.9f7f59a	Умный файловый фаззер	https://github.com/mfontanini/sloth-fuzzer
slowhttptest	1.6	A highly configurable tool that simulates application layer denial of service attacks.	http://code.google.com/p/slowhttptest
slowloris	0.7	A tool which is written in perl to test http-server vulnerabilites for connection exhaustion denial of service (DoS) attacks so you can enhance the security of your webserver.	http://ha.ckers.org/slowloris/
smali	2.1.1	An assembler/disassembler for Android's dex format	https://github.com/JesusFreke/smali
smartphone-pentest-framework	104.fc45347	Repository for the Smartphone Pentest Framework (SPF).	https://github.com/georgiaw/Smartphone-Pentest-Framework
smbbf	0.9.1	SMB password bruteforcer.	http://packetstormsecurity.com/files/25381/smbbf.9.1.tar.gz.html
smbexec	148.7827616	A rapid psexec style attack with samba tools.	https://github.com/pentestgeek/smbexec
smbmap	54.57b0176	A handy SMB enumeration tool.	https://github.com/ShawnDEvans/smbmap
smbrelay	3	SMB / HTTP to SMB replay attack toolkit.	http://www.tarasco.org/security/smbrelay/
smbspider	10.7db9323	A lightweight python utility for searching SMB/CIFS/Samba file shares.	https://github.com/T-S-A/smbspider
smikims-arpspoof	14.7fd3021	Performs an ARP spoofing attack using the Linux kernel's raw sockets.	https://github.com/smikims/arpspoof
smod	27.7679302	Модульный фреймворк с любого рода диагностическими и наступательными функциями, которые вам только могут понадобиться для пентеста протокола modbus.	https://github.com/enddo/smod
smtp-fuzz	1.0	Simple smtp fuzzer	none
smtp-test	3.acbe743	Automated testing of SMTP servers for penetration testing.	https://github.com/isaudits/smtp-test
smtp-user-enum	1.2	Username guessing tool primarily for use against the default Solaris SMTP service. Can use either EXPN, VRFY or RCPT TO.	http://pentestmonkey.net/tools/user-enumeration/smtp-user-enum
smtp-vrfy	1.0	An SMTP Protocol Hacker.	
smtpmap	0.8.234_BET	Tool to identify the running smtp software on a	http://www.projectiwear.org/~plasmahh/s

Имя	Версия	Описание	Домашняя страница
	A	given host.	oftware.html
smtpscan	0.5	An SMTP scanner	http://packetstormsecurity.com/files/31102/smtpscan.5.tar.gz.html
smtptx	1.0	A very simple tool used for sending simple email and do some basic email testing from a pentester perspective.	http://www.0x90.se/
sn00p	0.8	A modular tool written in bourne shell and designed to chain and automate security tools and tests.	http://www.nullsecurity.net/tools/automation.html
sn1per	61.5ab69c3	Автоматизированный разведывательный сканер пентестера.	https://github.com/1N3/Sn1per
snapception	8.c156f9e	Intercept and decrypt all snapchats received over your network.	https://github.com/thebradbain/snapception
snarf-mitm	40.49cc8cb	SMB Man in the Middle Attack Engine / relay suite.	https://github.com/purpleteam/snarf
sniffjoke	0.4.1	Injects packets in the transmission flow that are able to seriously disturb passive analysis like sniffing, interception and low level information theft.	http://www.delirandom.net/sniffjoke/
snmp-brute	15.64ec0ce	SNMP brute force, enumeration, CISCO config downloader and password cracking script.	https://github.com/SECFORCE/SNMP-Brute
snmp-fuzzer	0.1.1	SNMP fuzzer uses Protos test cases with an entirely new engine written in Perl.	http://www.arhont.com/en/category/resources/tools-utilities/
snmpattack	1.8	SNMP scanner and attacking tool.	http://www.c0decafe.de/
snmpcheck	1.8	A free open source utility to get information via SNMP protocols.	http://www.nothink.org/perl/snmpcheck/
snmpenum	1.7	snmp enumerator	http://www.filip.waeytens.easynet.be/
snmpscan	0.1	A free, multi-processes SNMP scanner	http://www.nothink.org/perl/snmpscan/index.php
snoopbrute	17.589fbe6	Multithreaded DNS recursive host brute-force tool.	https://github.com/m57/snoopbrute
snoopy-ng	128.eac73f5	A distributed, sensor, data collection, interception, analysis, and visualization framework.	https://github.com/sensepost/snoopy-ng
snort	2.9.8.0	Легковесная система выявления сетевых вторжений.	http://www.snort.org
snow	20130616	Steganography program for concealing messages in text files.	http://darkside.com.au/snow/index.html
snscan	1.05	A Windows based SNMP detection utility that can quickly and accurately identify SNMP enabled devices on a network.	http://www.mcafee.com/uk/downloads/free-tools/snscan.aspx
socat	1.7.3.1	Многоцелевой ретранслятор.	http://www.dest-unreach.org/socat/
sockstat	0.3	A tool to let you view information about open connections. It is similar to the tool of the same name that is included in FreeBSD, trying to faithfully reproduce as much functionality as is possible.	https://packages.debian.org/unstable/main/sockstat
soot	2.5.0	A Java Bytecode Analysis and Transformation Framework.	http://www.sable.mcgill.ca/soot
spade	114	A general-purpose Internet utility package, with some extra features to help in tracing the source of spam and other forms of Internet harassment.	http://www.hoobie.net/brutus/
spaf	11.671a976	Static Php Analysis and Fuzzer.	https://github.com/Ganapati/spaf
sparta	17.bdbf244	Python GUI application which simplifies network infrastructure penetration testing by	http://sparta.secforce.com/

Имя	Версия	Описание	Домашняя страница
		aiding the penetration tester in the scanning and enumeration phase.	
sparty	0.1	An open source tool written in python to audit web applications using sharepoint and frontpage architecture.	http://sparty.secniche.org/
spectools	2010_04_R1	Spectrum-Tools is a set of utilities for using the Wi-Spy USB spectrum analyzer hardware. Stable version.	http://www.kismetwireless.net/spectools/
speedpwn	8.3dd2793	An active WPA/2 Bruteforcer, original created to prove weak standard key generation in different ISP labeled routers without a client is connected.	https://gitorious.org/speedpwn/
spf	62.959d3e9	A python tool designed to allow for quick recon and deployment of simple social engineering phishing exercises.	https://github.com/tatanus/SPF
spiderfoot	2.6.1	The Open Source Footprinting Tool.	http://spiderfoot.net/
spiderpig-pdffuzzer	0.1	A javascript pdf fuzzer	https://code.google.com/p/spiderpig-pdffuzzer/
spiga	383.4b6f802	Настраиваемый сканер веб-ресурсов.	https://github.com/getdual/scripts-n-tools/blob/master/spiga.py
spike	2.9	IMMUNITYsec's fuzzer creation kit in C	http://www.immunitysec.com/resources-freesoftware.shtml
spike-proxy	148	A Proxy for detecting vulnerabilities in web applications	http://www.immunitysec.com/resources-freesoftware.shtml
spiped	1.5.0	A utility for creating symmetrically encrypted and authenticated pipes between socket addresses.	https://www.tarsnap.com/spiped.html
spipscan	69.4ad3235	SPIP (CMS) scanner for penetration testing purpose written in Python.	https://github.com/PaulSec/SPIPScan
splint	3.1.2	A tool for statically checking C programs for security vulnerabilities and coding mistakes	http://www.splint.org/
sploitctl	47.e6f9e15	Fetch, install and search exploit archives from exploit sites like exploit-db and packetstorm.	https://github.com/BlackArch/sploitctl
sploitego	153.d9568dc	Maltego Penetration Testing Transforms.	https://github.com/allfro/sploitego
spooftooph	0.5.2	Designed to automate spoofing or cloning Bluetooth device Name, Class, and Address. Cloning this information effectively allows Bluetooth device to hide in plain sight	http://www.hackfromacave.com/projects/spooftooph.html
sps	4.3	A Linux packet crafting tool. Supports IPv4, IPv6 including extension headers, and tunneling IPv6 over IPv4.	https://sites.google.com/site/simplepacketsender/
sqid	0.3	A SQL injection digger.	http://sqid.rubyforge.org/
sqlbrute	1.0	Brute forces data out of databases using blind SQL injection.	http://www.justinclarke.com/archives/2006/03/sqlbrute.html
sqlmap	1.0.3	Мощнейший инструмент по обнаружению и эксплуатации SQL инъекций.	http://sqlmap.org/
sqlninja	0.2.999	A tool targeted to exploit SQL Injection vulnerabilities on a web application that uses Microsoft SQL Server as its back-end.	http://sqlninja.sourceforge.net/
sqlpat	1.0.1	This tool should be used to audit the strength of Microsoft SQL Server passwords offline.	http://www.cqure.net/wp/sqlpat/
sqlping	4	SQL Server scanning tool that also checks for weak passwords using wordlists.	http://www.sqlsecurity.com/downloads
sqlsus	0.7.2	An open source MySQL injection and takeover tool, written in perl	http://sqlsus.sourceforge.net/
ssdp-scanner	1.0	SSDP amplification scanner written in Python.	http://packetstormsecurity.com/files/1279

Имя	Версия	Описание	Домашняя страница
		Makes use of Scapy.	94/SSDP-Amplification-Scanner.html
ssh-privkey-crack	0.4	A SSH private key cracker.	https://code.google.com/p/lusas/
ssh-user-enum	5.3d83131	SSH User Enumeration Script in Python Using The Timing Attack.	https://github.com/nccgroup/ssh-user-enum
sshatter	1.2	Password bruteforcer for SSH.	http://www.nth-dimension.org.uk/downloads.php?id=34
sshscan	1.0	A horizontal SSH scanner that scans large swaths of IPv4 space for a single SSH user and pass.	https://github.com/getdual/scripts-n-tools/blob/master/sshscan.py
sshtrix	0.0.2	A very fast multithreaded SSH login cracker.	http://nullsecurity.net/tools/cracker.html
sshuttle	0.77.2	Прозрачный прокси сервер, который перенаправляет все TCP через ssh.	https://github.com/sshuttle/sshuttle
ssl-hostname-resolver	1	CN (Common Name) grabber on X.509 Certificates over HTTPS.	http://packetstormsecurity.com/files/120634/Common-Name-Grabber-Script.html
ssl-phuck3r	2.0	All in one script for Man-In-The-Middle attacks.	https://github.com/zombiesam/ssl_phuck3r
sslcat	1.0	SSLCat is a simple Unix utility that reads and writes data across an SSL enable network connection.	http://www.bindshell.net/tools/sslcat
sslcaudit	524.f218b9b	Утилита для выполнения аудита безопасности SSL/TLS клиентов.	https://github.com/grwl/sslcaudit
ssldump	0.9b3	an SSLv3/TLS network protocol analyzer	http://www.rtfm.com/ssldump/
sslh	1.17	SSL/SSH/OpenVPN/XMPP/tinc port multiplexer	http://www.rutschle.net/tech/sslh.shtml
ssllabs-scan	1.2.0	Command-line client for the SSL Labs APIs	https://github.com/ssllabs/ssllabs-scan
sslmap	0.2.0	A lightweight TLS/SSL cipher suite scanner.	http://thesprawl.org/projects/latest/
sslnuke	5.c5faeaa	Transparent proxy that decrypts SSL traffic and prints out IRC messages.	https://github.com/jtripper/sslnuke
sslscan	1.10.2	A fast tools to scan SSL services, such as HTTPS to determine the ciphers that are supported	https://github.com/DinoTools/sslscan/
sslsniff	0.8	A tool to MITM all SSL connections on a LAN and dynamically generate certs for the domains that are being accessed on the fly	http://www.thoughtcrime.org/software/sslsniff/
sslyze	0.12	Python tool for analyzing the configuration of SSL servers and for identifying misconfigurations.	https://github.com/nabla-c0d3/sslyze/
ssrf-proxy	72.a01a2fe	Facilitates tunneling HTTP communications through servers vulnerable to Server-Side Request Forgery.	https://github.com/bcoles/ssrf_proxy
stackflow	2.2af525d	Universal stack-based buffer overfow exploitation tool.	https://github.com/d4rkcat/stackflow
starttls-mitm	7.b257756	A mitm proxy that will transparently proxy and dump both plaintext and TLS traffic.	https://github.com/ipopov/starttls-mitm
statsprocessor	0.11	A high-performance word-generator based on per-position Markov-attack.	http://hashcat.net/wiki/doku.php?id=statsprocessor
steghide	0.5.1	Embeds a message in a file by replacing some of the least significant bits	http://steghide.sourceforge.net
stegolego	8.85354f6	Simple program for using stegonography to hide data within BMP images.	https://github.com/razc411/StegoLeggo
stenographer	414.7b68b6d	Программа по захвату пакетов для выявления вторжений. Создана для работы с ОЧЕНЬ большими потоками данных.	https://github.com/google/stenographer
stompy	0.0.4	An advanced utility to test the quality of WWW session identifiers and other tokens that are meant to be unpredictable.	http://lcamtuf.coredump.cx/
storm-ring	0.1	This simple tool is useful to test a PABX with	http://packetstormsecurity.com/files/1158

Имя	Версия	Описание	Домашняя страница
		"allow guest" parameter set to "yes" (in this scenario an anonymous caller could place a call).	52/Storm-Ringing-PABX-Test-Tool.html
striptls	30.9ba887f	Рабочий прототип реализации атак раскрытия STARTTLS	https://github.com/tintinweb/striptls
strutscan	4.8712c12	Сканер уязвимости Apache Struts2, написан на Perl.	https://github.com/riusksk/StrutScan
stunnel	5.31	Программа позволяет вам зашифровать произвольные TCP подключения внутри SSL	http://www.stunnel.org
subbrute	1.2.1	A DNS meta-query spider that enumerates DNS records and subdomains	https://github.com/TheRook/subbrute
subdomainer	1.2	A tool designed for obtaining subdomain names from public sources.	http://www.edge-security.com/subdomainer.php
subterfuge	5.0	Automated Man-in-the-Middle Attack Framework	http://kinozoa.com
sucrack	1.2.3	A multi-threaded Linux/UNIX tool for brute-force cracking local user accounts via su	http://labs.portcullis.co.uk/application/sucrack
sulley	1.0.3bce87a	A pure-python fully automated and unattended fuzzing framework.	https://github.com/OpenRCE/sulley/
superscan	4.1	Powerful TCP port scanner, pinger, resolver.	http://www.foundstone.com/us/resources/proddesc/superscan.htm
suricata	3.0	Движок нового покаления обнаружения и предотвращения вторжений с открытым исходным кодом.	http://openinfosecfoundation.org/index.php/download-suricata
svn-extractor	32.a3d4677	Простой скрипт для извлечения всех веб ресурсов с помощью папки .SVN открытой в сети.	https://github.com/anantshri/svn-extractor
swaks	20130209.0	Swiss Army Knife SMTP; Command line SMTP testing, including TLS and AUTH	http://jetmore.org/john/code/swaks/
swfintruder	0.9.1	First tool for testing security in Flash movies. A runtime analyzer for SWF external movies. It helps to find flaws in Flash.	http://code.google.com/p/swfintruder/
swftools	0.9.2	A collection of SWF manipulation and creation utilities	http://www.swftools.org/
synflood	0.1	A very simply script to illustrate DoS SYN Flooding attack.	http://thesprawl.org/projects/syn-flooder/
synner	1.1	A custom eth->ip->tcp packet generator (spoofer) for testing firewalls and dos attacks.	http://packetstormsecurity.com/files/69802/synner.c.html
synscan	5.02	fast asynchronous half-open TCP portscanner	http://www.digit-labs.org/files/tools/synscan/
syringe	1.9786f35	A General Purpose DLL & Code Injection Utility.	https://github.com/securestate/syringe
sysdig	0.8.0	Инструмент с открытым исходным кодом, для исследования и решения проблем уровня системы.	http://www.sysdig.org/
sysinternals-suite	1.7	Sysinternals tools suite.	http://sysinternals.com/
t50	5.5	Experimental Multi-protocol Packet Injector Tool.	http://t50.sourceforge.net/
taof	0.3.2	Taof is a GUI cross-platform Python generic network protocol fuzzer.	http://taof.sf.net
tbear	1.5	Transient Bluetooth Environment Auditor includes an ncurses-based Bluetooth scanner (a bit similar to kismet), a Bluetooth DoS tool, and a Bluetooth hidden device locator.	http://freshmeat.net/projects/t-bear
tcgetkey	0.1	A set of tools that deal with acquiring physical	http://packetstormsecurity.com/files/1191

Имя	Версия	Описание	Домашняя страница
		memory dumps via FireWire and then scan the memory dump to locate TrueCrypt keys and finally decrypt the encrypted TrueCrypt container using the keys.	46/tcgetkey.1.html
tckfc	21.a32167e	TrueCrypt key file cracker.	https://github.com/Octosec/tckfc
tcpcontrol-fuzzer	0.1	2^6 TCP control bit fuzzer (no ECN or CWR).	https://www.ee.oulu.fi/research/ouspg/tcpcontrol-fuzzer
tcpdump	4.7.4	A tool for network monitoring and data acquisition	http://www.tcpdump.org
tcpextract	1.1	Extracts files from captured TCP sessions. Support live streams and pcap files.	https://pypi.python.org/pypi/tcpextract/1.1
tcpflow	1.4.5	Captures data transmitted as part of TCP connections then stores the data conveniently	https://github.com/simsong/tcpflow
tcpick	0.2.1	TCP stream sniffer and connection tracker	http://tcpick.sourceforge.net/
tcpjunk	2.9.03	A general tcp protocols testing and hacking utility.	http://code.google.com/p/tcpjunk
tcpreplay	4.1.0	Gives the ability to replay previously captured traffic in a libpcap format	http://tcpreplay.appneta.com
tcptraceroute	1.5beta7	A traceroute implementation using TCP packets.	http://michael.toren.net/code/tcptraceroute/
tcpwatch	1.3.1	A utility written in Python that lets you monitor forwarded TCP connections or HTTP proxy connections.	http://hathawaymix.org/Software/TCPWatch
tcpxtract	1.0.1	A tool for extracting files from network traffic.	http://tcpxtract.sourceforge.net
teardown	1.0	Command line tool to send a BYE request to tear down a call.	http://www.hackingexposedvoip.com/
tekdefense-automater	86.6c916fd	Анализ IP URL и MD5 OSINT	https://github.com/1aN0rmus/TekDefense-Automater
termineter	0.1.0	Smart meter testing framework	https://code.google.com/p/termineter/
testssl	2.6	Testing TLS/SSL encryption.	https://github.com/drwetter/testssl.sh
tftp-bruteforce	0.1	TFTP-bruteforcer is a fast TFTP filename bruteforcer written in perl.	http://www.hackingexposedcisco.com/
tftp-fuzz	1337	Master TFTP fuzzing script as part of the ftools series of fuzzers.	http://nullsecurity.net/tools/fuzzer.html
tftp-proxy	0.1	This tool accepts connection on tftp and reloads requested content from an upstream tftp server. Meanwhile modifications to the content can be done by pluggable modules. So this one's nice if your mitm with some embedded devices.	http://www.c0decafe.de/
thc-keyfinder	1.0	Finds crypto keys, encrypted data and compressed data in files by analyzing the entropy of parts of the file.	https://www.thc.org/releases.php
thc-pptp-bruter	0.1.4	A brute force program that works against pptp vpn endpoints (tcp port 1723).	http://www.thc.org
thc-smartbrute	1.0	This tool finds undocumented and secret commands implemented in a smartcard.	https://www.thc.org/thc-smartbrute/
thc-ssl-dos	1.4	A tool to verify the performance of SSL. To be used in your authorized and legitimate area ONLY. You need to accept this to make use of it, no use for bad intentions, you have been warned!	http://www.thc.org/thc-ssl-dos/
theharvester	46.ec7f8be	Инструмент на Python для сбора e-mail аккаунтов и имёт поддоменов из различных публичных источников (поисковых машин, серверов ключей pgp).	http://www.edge-security.com/theHarvester.php
themole	0.3	Automatic SQL injection exploitation tool.	http://sourceforge.net/projects/themole/

Имя	Версия	Описание	Домашняя страница
tiger	3.2.3	A security scanner, that checks computer for known problems. Can also use tripwire, aide and chkrootkit.	http://www.nongnu.org/tiger/
tilt	90.2bc2ef2	An easy and simple tool implemented in Python for ip reconnaissance, with reverse ip lookup.	https://github.com/AeonDave/tilt
timegen	0.4	This program generates a *.wav file to "send" an own time signal to DCF77 compatible devices.	http://bastianborn.de/radio-clock-hack/
tinc	1.0.26	VPN (Virtual Private Network) daemon	http://www.tinc-vpn.org/
tinfoleak	3.6469eb3	Get detailed information about a Twitter user activity.	https://github.com/technoskald/tinfoleak/
tinyproxy	1.8.4	A light-weight HTTP proxy daemon for POSIX operating systems.	https://banu.com/tinyproxy/
tlsenum	77.b60e2c8	A command line tool to enumerate TLS cipher-suites supported by a server.	https://github.com/Ayrx/tlsenum
tlspretense	0.6.2	SSL/TLS client testing framework	https://github.com/iSECPartners/tlspretense
tlssled	1.3	A Linux shell script whose purpose is to evaluate the security of a target SSL/TLS (HTTPS) web server implementation.	http://blog.taddong.com/2011/05/tlssled-v10.html
tnscmd	1.3	a lame tool to prod the oracle tnslsnr process (1521/tcp)	http://www.jammed.com/~jwa/hacks/security/tnscmd/
topera	19.3e230fd	An IPv6 security analysis toolkit, with the particularity that their attacks can't be detected by Snort.	https://github.com/toperaproject/topera
tor	0.2.7.6	Anonymizing overlay network.	http://www.torproject.org/
tor-autocircuit	0.2	Tor Autocircuit was developed to give users a finer control over Tor circuit creation. The tool exposes the functionality of TorCtl library which allows its users to control circuit length, speed, geolocation, and other parameters.	http://www.thesprawl.org/projects/tor-autocircuit/
tor-browser-en	5.5.3	Связка Tor браузера для анонимного браузинга с использованием Firefox и Tor.	https://www.torproject.org/projects/torbrowser.html.en
torshammer	1.0	A slow POST Denial of Service testing tool written in Python.	http://sourceforge.net/projects/torshammer/
torsocks	2.1.0	Wrapper to safely torify applications	https://gitweb.torproject.org/torsocks.git/
tpcat	latest	TPCAT is based upon pcapdiff by the EFF. TPCAT will analyze two packet captures (taken on each side of the firewall as an example) and report any packets that were seen on the source capture but didn’t make it to the dest.	http://sourceforge.net/projects/tpcat/
traceroute	2.0.21	Tracks the route taken by packets over an IP network	http://traceroute.sourceforge.net/
treasure	6.a91d52b	Hunt for sensitive information through githubs code search.	https://github.com/GuerrillaWarfare/Treasure
trid	2.20	An utility designed to identify file types from their binary signatures.	http://mark0.net/soft-trid-e.html
trinity	4501.1f5b0cc	Файзер системных запросов Linux.	http://codemonkey.org.uk/projects/trinity/
trixd00r	0.0.1	An advanced and invisible userland backdoor based on TCP/IP for UNIX systems.	http://nullsecurity.net/tools/backdoor.html
truecrack	35	Password cracking for truecrypt(c) volumes.	http://code.google.com/p/truecrack/
truecrypt	7.1a	Free open-source cross-platform disk encryption software	http://www.truecrypt.org/
tsh	0.6	An open-source UNIX backdoor that compiles on all variants, has full pty support, and uses strong crypto for communication.	http://packetstormsecurity.com/search/?q=tsh

Имя	Версия	Описание	Домашняя страница
tsh-sctp	2.850a2da	An open-source UNIX backdoor.	https://github.com/infodox/tsh-sctp
tunna	19.f8c1881	a set of tools which will wrap and tunnel any TCP communication over HTTP. It can be used to bypass network restrictions in fully firewalled environments.	https://github.com/SECFORCE/Tunna
tuxcut	5.1	Netcut-like program for Linux written in PyQt.	http://bitbucket.org/a_atalla/tuxcut/
twofi	2.0	Twitter Words of Interest.	http://www.digininja.org/projects/twofi.php
u3-pwn	2.0	A tool designed to automate injecting executables to Sandisk smart usb devices with default U3 software install.	http://www.nullsecurity.net/tools/backdoor.html
uatester	1.06	User Agent String Tester	http://code.google.com/p/ua-tester/
ubertooth	2015.10.R1	A 2.4 GHz wireless development board suitable for Bluetooth experimentation. Open source hardware and software. Tools only.	https://github.com/greatscottgadgets/ubertooth/releases
ubitack	0.3	Tool, which automates some of the tasks you might need on a (wireless) penetration test or while you are on the go.	https://code.google.com/p/ubitack/
udis86	1.7.2	A minimalistic disassembler library	http://udis86.sourceforge.net/
udptunnel	19	Tunnels TCP over UDP packets.	http://code.google.com/p/udptunnel/
uefi-firmware-parser	136.e6f122a	Разбирает связанные с BIOS/Intel ME/UEFI прошивками структуры: тома, файловые системы, файлы и т.д.	https://github.com/theopolis/uefi-firmware-parser
ufo-wardriving	4	Allows you to test the security of wireless networks by detecting their passwords based on the router model	http://www.ufo-wardriving.com/
ufonet	19.0287655	Инструмент создан для запуска DDoS атак против цели, используя вектор 'Open Redirect' на сторонних приложениях, как botnet.	https://github.com/epsylon/ufonet
umap	25.3ad8121	The USB host security assessment tool.	https://github.com/nccgroup/umap
umit	1.0	A powerful nmap frontend.	http://www.umitproject.org/
unhide	20130526	A forensic tool to find processes hidden by rootkits, LKMs or by other techniques.	http://sourceforge.net/projects/unhide/
unibrute	1.b3fb4b7	Multithreaded SQL union bruteforcer.	https://github.com/GDSSecurity/Unibrute
unicorn	30.783adda	A simple tool for using a PowerShell downgrade attack and inject shellcode straight into memory.	https://github.com/trustedsec/unicorn
unicornscan	0.4.7	A new information gathering and correlation engine.	http://www.unicornscan.org/
uniofuzz	1337	The universal fuzzing tool for browsers, web services, files, programs and network services/ports	http://nullsecurity.net/tools/fuzzer.html
uniscan	6.2	A simple Remote File Include, Local File Include and Remote Command Execution vulnerability scanner.	http://sourceforge.net/projects/uniscan/
unix-privesc-check	1.4	Tries to find misconfigurations that could allow local unprivilged users to escalate privileges to other users or to access local apps (e.g. databases)	http://pentestmonkey.net/tools/audit/unix-privesc-check
unsecure	1.2	Bruteforces network login masks.	http://www.sniperx.net/
upnp-pentest-toolkit	1.1	UPnP Pentest Toolkit for Windows.	https://github.com/nccgroup/UPnP-Pentest-Toolkit
upnpscan	0.4	Scans the LAN or a given address range for UPnP capable devices.	http://www.cqure.net/wp/upnpscan/
upx	3.91	Ultimate executable compressor.	http://upx.sourceforge.net/

Имя	Версия	Описание	Домашняя страница
urlcrazy	0.5	Generate and test domain typos and variations to detect and perform typo squatting, URL hijacking, phishing, and corporate espionage.	http://www.morningstarsecurity.com/research/urlcrazy
urldigger	02c	A python tool to extract URL addresses from different HOT sources and/or detect SPAM and malicious code	https://code.google.com/p/urldigger/
urlview	0.9	A curses URL parser for text files.	http://packages.qa.debian.org/u/urlview.html
username-anarchy	0.2	Tools for generating usernames when penetration testing.	http://www.morningstarsecurity.com/research/username-anarchy
usernamer	7.813139d	Pentest Tool to generate usernames/logins based on supplied names.	https://github.com/jseidl/usernamer
uw-loveimap	0.1	Multi threaded imap bounce scanner.	http://uberwall.org/bin/download/45/UWloveimap.tgz
uw-offish	0.1	Clear-text protocol simulator.	http://uberwall.org/bin/download/42/UW_offish.1.tar.gz
uw-udpscan	0.1	Multi threaded udp scanner.	http://uberwall.org/bin/download/44/UWudpscan.tar.gz
uw-zone	0.1	Multi threaded, randomized IP zoner.	http://uberwall.org/bin/download/43/UWzone.tgz
v3n0m	77.ce17555	Инструмент автоматического массивного сканирования дорков SQLi и уязвимостей Metasploit.	https://github.com/v3n0m-Scanner/V3n0M-Scanner
valabind	0.10.0	Инструмент для парсинга файлов vala или vapi для их трансформации в файлы интерфейса swig, C++, NodeJS-ffi или GIR	http://radare.org
valgrind	3.11.0	A tool to help find memory-management problems in programs	http://valgrind.org/
vane	1855.6a47cd8	A vulnerability scanner which checks the security of WordPress installations using a black box approach.	https://github.com/delvelabs/vane
vanguard	0.1	A comprehensive web penetration testing tool written in Perl thatidentifies vulnerabilities in web applications.	http://packetstormsecurity.com/files/110603/Vanguard-Pentesting-Scanner.html
vbrute	1.11dda8b	Virtual hosts brute forcer.	https://github.com/nccgroup/vbrute
vbscan	4.abbaed3	Сканер уязвимостей vBulletin по принципу чёрного ящика, написан на perl.	https://github.com/rezasp/vbscan
vega	1.0	An open source platform to test the security of web applications	https://github.com/subgraph/Vega/wiki
veil	513.e345b01	Инструмент создан для генерации рабочей нагрузки metasploit, которая обходит популярные антивирусные решения.	https://github.com/veil-evasion/Veil
veracrypt	1.17	Бесплатное программное обеспечение для шифрования диска, форк TrueCrypt.	http://veracrypt.codeplex.com/
vfeed	49.c8cf0ec	Open Source Cross Linked and Aggregated Local Vulnerability Database main repository.	http://www.toolswatch.org/vfeed
vidalia	0.2.21	Controller GUI for Tor.	https://www.torproject.org/vidalia
videosnarf	0.63	A new security assessment tool for pcap analysis	http://ucsniff.sourceforge.net/videosnarf.html
vinetto	0.07beta	A forensics tool to examine Thumbs.db files	http://vinetto.sourceforge.net
viper	1050.563de66	Фреймворк анализа бинарных файлов.	https://github.com/botherder/viper
viproy-voipkit	2.99.1	VoIP Pen-Test Kit for Metasploit Framework	http://viproy.com/
virustotal	4.9aea023	Command-line utility to automatically lookup on VirusTotal all files recursively contained in a	https://github.com/botherder/virustotal

Имя	Версия	Описание	Домашняя страница
		directory.	
vivisect	456.6e6287a	Фреймворк на Python, базирующийся на статичном анализе и обратной инженерии, Vdb - это основанный на Python, фокусирующийся на исследовании/ревёрсинге и API программной отладки от invisigoth of kenshoto	http://visi.kenshoto.com/
vlan-hopping	16.a2959fe	Easy 802.1Q VLAN Hopping	https://github.com/nccgroup/vlan-hopping
vmcloak	0.3.6	Automated Virtual Machine Generation and Cloaking for Cuckoo Sandbox.	https://github.com/jbremer/vmcloak
vnak	1.cf0fda7	Aim is to be the one tool a user needs to attack multiple VoIP protocols.	https://www.isecpartners.com/vnak.html
vnc-bypauth	0.0.1	Multi-threaded bypass authentication scanner for VNC servers <= 4.1.1.	http://pentester.fr/resources/tools/techno/VNC/VNC_bypauth/
vncrack	1.21	What it looks like: crack VNC.	http://phenoelit-us.org/vncrack
voiper	0.07	A VoIP security testing toolkit incorporating several VoIP fuzzers and auxilliary tools to assist the auditor.	http://voiper.sourceforge.net/
voiphopper	2.04	A security validation tool that tests to see if a PC can mimic the behavior of an IP Phone. It rapidly automates a VLAN Hop into the Voice VLAN.	http://voiphopper.sourceforge.net/
voipong	2.0	A utility which detects all Voice Over IP calls on a pipeline, and for those which are G711 encoded, dumps actual conversation to seperate wave files.	http://www.enderunix.org/voipong/
vscan	10.da4e47e	Сканер HTTPS / уязвимостей	https://github.com/pasjtene/Vscan
vstt	0.5.0	VSTT is a multi-protocol tunneling tool. It accepts input by TCP stream sockets and FIFOs, and can send data via TCP, POP3, and ICMP tunneling.	http://www.wendzel.de/dr.org/files/Projects/vstt/
vsvbp	6.241a7ab	Black box tool for Vulnerability detection in web applications.	https://github.com/varunjammula/VSVBP
vulscan	2.0	A module which enhances nmap to a vulnerability scanner	http://www.computec.ch/projekte/vulscan/
w3af	1.6.49	Web Application Attack and Audit Framework.	http://w3af.sourceforge.net/
waffit	39	A set of security tools to identify and fingerprint Web Application Firewall/WAF products protecting a website.	http://code.google.com/p/waffit/
wafp	0.01_26c3	An easy to use Web Application Finger Printing tool written in ruby using sqlite3 databases for storing the fingerprints.	http://packetstormsecurity.com/files/84468/Web-Application-Finger-Printer.01-26c3.html
waidps	16.ff8d270	Wireless Auditing, Intrusion Detection & Prevention System.	https://github.com/SYWorks/waidps
waldo	28.a33de7a	A lightweight and multithreaded directory and subdomain bruteforcer implemented in Python.	https://github.com/red-team-labs/waldo
wapiti	2.3.0	A vulnerability scanner for web applications. It currently search vulnerabilities like XSS, SQL and XPath injections, file inclusions, command execution, LDAP injections, CRLF injections…	http://wapiti.sourceforge.net/
wavemon	0.8.0	Ncurses-based monitoring application for wireless network devices	http://eden-feed.erg.abdn.ac.uk/wavemon/
web-soul	2	A plugin based scanner for attacking and data mining web sites written in Perl.	http://packetstormsecurity.com/files/122064/Web-Soul-Scanner.html
webacoo	0.2.3	Web Backdoor Cookie Script-Kit.	https://bechtsoudis.com/webacoo/
webenum	0.1	Tool to enumerate http responses using	http://code.google.com/p/webenum/

Имя	Версия	Описание	Домашняя страница
		dynamically generated queries and more. Useful for penetration tests against web servers.	
webexploitationtool	63.8245aea	Крассплатформенный набор инструментов эксплуатации веб-приложений.	https://github.com/AutoSecTools/WebExploitationTool
webhandler	324.047dddf	A handler for PHP system functions & also an alternative 'netcat' handler.	https://github.com/lnxg33k/webhandler
webpwn3r	35.3fb27bb	A python based Web Applications Security Scanner.	https://github.com/zigoo0/webpwn3r
webrute	3.3	Web server directory brute forcer.	https://github.com/BlackArch/webrute
webscarab	20120422.001828	Framework for analysing applications that communicate using the HTTP and HTTPS protocols	http://www.owasp.org/index.php/Category:OWASP_WebScarab_Project
websearch	1.cce2384	Search vhost names given a host range. Powered by Bing..	https://github.com/PentesterES/WebSearch
webshag	1.10	A multi-threaded, multi-platform web server audit tool.	http://www.scrt.ch/en/attack/downloads/webshag
webshells	14.112ea8c	Вэб бэкдоры.	https://github.com/BlackArch/webshells
webslayer	5	A tool designed for brute forcing Web Applications.	https://code.google.com/p/webslayer/
websockify	0.7.0	WebSocket to TCP proxy/bridge.	http://github.com/kanaka/websockify
webspa	0.8	A web knocking tool, sending a single HTTP/S to run O/S commands.	http://sourceforge.net/projects/webspa/
websploit	3.0.0	An Open Source Project For, Social Engineering Works, Scan, Crawler & Analysis Web, Automatic Exploiter, Support Network Attacks	http://code.google.com/p/websploit/
webxploiter	20.41a11d1	An OWASP Top 10 Security scanner.	https://github.com/xionsec/WebXploiter
weeman	75.f1f4642	HTTP сервер на Python для фишинга.	https://github.com/Hypsurus/weeman
weevely	670.7d7dfc9	Военизированный веб-шэлл	http://epinna.github.io/Weevely/
wepbuster	1.0_beta_0.7	script for automating aircrack-ng	http://code.google.com/p/wepbuster/
wfuzz	37.574caa5	Utility to bruteforce web applications to find their not linked resources.	https://github.com/xmendez/wfuzz
whatportis	34.66a04b2	Программа для поиска информации о программах, которые обычно прослушивают какой-либо порт, а также информации о порте, который обычно прослушивается конкретной программой.	https://github.com/ncrocfer/whatportis
whatweb	4071.c489fbd	Next generation web scanner that identifies what websites are running.	http://www.morningstarsecurity.com/research/whatweb
wi-feye	1.1	An automated wireless penetration testing tool written in python, its designed to simplify common attacks that can be performed on wifi networks so that they can be executed quickly and easily.	http://wi-feye.za1d.com/download.php
wifi-honey	1.0	A management tool for wifi honeypots	http://www.digininja.org/projects/wifi_honey.php
wifi-monitor	24.33b682e	Prints the IPs on your local network that're sending the most packets.	https://github.com/DanMcInerney/wifi-monitor
wifi-pumpkin	60.784cacf	Фреймворк для атаки фальшивой точкой доступа Wi-Fi	https://github.com/P0cL4bs/WiFi-Pumpkin
wificurse	0.3.9	WiFi jamming tool.	https://github.com/oblique/wificurse
wifijammer	64.27fe50d	Скрипт на python для непрерывного глушения wifi клиентов в пределах досягаемости.	https://github.com/DanMcInerney/wifijammer
wifiphisher	167.91cf3c0	Быстрые автоматизированные фишинговые атаки в отношении сетей WPA.	https://github.com/sophron/wifiphisher
wifitap	2b16088	WiFi injection tool through tun/tap device.	https://github.com/GDSSecurity/wifitap

Имя	Версия	Описание	Домашняя страница
wifite	2.28fc5cd	A tool to attack multiple WEP and WPA encrypted networks at the same time.	http://code.google.com/p/wifite/
wig	522.eeaab12	Сборщик информации по веб-приложениям.	https://github.com/jekyc/wig
wikigen	8.348aa99	A script to generate wordlists out of wikipedia pages.	https://github.com/zombiesam/wikigen
wildpwn	9.379f0da	Unix wildcard attacks.	https://github.com/localh0t/wildpwn
windows-privesc-check	181.9f304fd	Standalone Executable to Check for Simple Privilege Escalation Vectors on Windows Systems.	https://github.com/pentestmonkey/windows-privesc-check
winexe	1.00	Remotely execute commands on Windows NT/2000/XP/2003 systems.	http://sourceforge.net/projects/winexe/
winfo	2.0	Uses null sessions to remotely try to retrieve lists of and information about user accounts, workstation/interdomain/server trust accounts, shares (also hidden), sessions, logged in users, and password/lockout policy, from Windows NT/2000/XP.	http://www.ntsecurity.nu/toolbox/winfo/
wireless-ids	24.b132071	Ability to detect suspicious activity such as (WEP/WPA/WPS) attack by sniffing the air for wireless packets.	https://github.com/SYWorks/wireless-ids
wireshark-cli	2.0.2	Бесплатный анализатор сетевого протокола для Unix/Linux и Windows - версия командной строки	http://www.wireshark.org/
wireshark-gtk	2.0.2	Бесплатный анализатор сетевого протокола для Unix/Linux и Windows - версия с графическим интерфейсом	http://www.wireshark.org/
wirouter-keyrec	1.1.2	A powerful and platform independent software to recover the default WPA passphrases of the supported router models (Telecom Italia Alice AGPF, Fastweb Pirelli, Fastweb Tesley, Eircom Netopia, Pirelli TeleTu/Tele 2).	http://www.salvatorefresta.net/tools/
witchxtool	1.1	A perl script that consists of a port scanner, LFI scanner, MD5 bruteforcer, dork SQL injection scanner, fresh proxy scanner, and a dork LFI scanner.	http://packetstormsecurity.com/files/97465/Witchxtool-Port-LFI-SQL-Scanner-And-MD5-Bruteforcing-Tool.1.html
wlan2eth	1.3	Re-writes 802.11 captures into standard Ethernet frames.	http://www.willhackforsushi.com/?page_id=79
wmat	0.1	Automatic tool for testing webmail accounts.	http://netsec.rs/70/tools.html
wnmap	0.1	A shell script written with the purpose to automate and chain scans via nmap. You can run nmap with a custom mode written by user and create directories for every mode with the xml/nmap files inside.	http://nullsecurity.net/tools/automation.html
wol-e	2.0	A suite of tools for the Wake on LAN feature of network attached computers.	http://code.google.com/p/wol-e/
wordbrutepress	28.8061c52	Python script that performs brute forcing against WordPress installs using a wordlist.	http://www.homelab.it/index.php/2014/11/03/wordpress-brute-force-multithreading/
wordpot	38.ca12cb5	A WordPress Honeypot.	https://github.com/gbrindisi/wordpot
wpa-bruteforcer	4.d5f8586	Attacking WPA/WPA encrypted access point without client.	https://github.com/SYWorks/wpa-bruteforcer
wpa2-halfhandshake-crack	26.84fa6be	A POC to show it is possible to capture enough of a handshake with a user from a fake AP to crack a WPA2 network without knowing the passphrase of the actual AP.	https://github.com/dxa4481/WPA2-HalfHandshake-Crack
wpbf	7.11b6ac1	Multithreaded WordPress brute forcer.	https://github.com/dejanlevaja/wpbf

Имя	Версия	Описание	Домашняя страница
wpbrute-rpc	3.e7d8145	Tool for amplified bruteforce attacks on wordpress based website via xmlrcp API.	https://github.com/zendoctor/wpbrute-rpc
wpscan	2017.b328dc4	Сканер уязвимостей, который проверяет безопасность WordPress, использует метод чёрного ящика.	http://wpscan.org
ws-attacker	1.7	A modular framework for web services penetration testing.	http://ws-attacker.sourceforge.net/
wsfuzzer	1.9.5	A Python tool written to automate SOAP pentesting of web services.	https://www.owasp.org/index.php/Category:OWASP_WSFuzzer_Project
wsuspect-proxy	22.0f79a2f	Инструмент для атаки человек-посередине MITM небезопасных соединений службы обновлений Widnows (WSUS).	https://github.com/ctxis/wsuspect-proxy
wyd	0.2	Gets keywords from personal files. IT security/forensic tool.	http://www.remote-exploit.org/?page_id=418
x-scan	3.3	A general network vulnerabilities scanner for scanning network vulnerabilities for specific IP address scope or stand-alone computer by multi-threading method, plug-ins are supportable.	http://www.xfocus.org/
xcat	0.7.1	Инструмент командной строки для автоматизированной эксплуатации узяхвимостей слепых инъекций XPath.	https://github.com/orf/xcat
xcavator	5.bd9e2d8	Man-In-The-Middle and phishing attack tool that steals the victim's credentials of some web services like Facebook.	https://github.com/nccgroup/xcavator
xcname	9.08942ae	A tool for enumerating expired domains in CNAME records.	https://github.com/mandatoryprogrammer/xcname
xorbruteforcer	0.1	Script that implements a XOR bruteforcing of a given file, although a specific key can be used too.	http://eternal-todo.com/category/bruteforce
xorsearch	1.11.1	Program to search for a given string in an XOR, ROL or ROT encoded binary file.	http://blog.didierstevens.com/programs/xorsearch/
xortool	0.96	A tool to analyze multi-byte xor cipher.	https://github.com/hellman/xortool/
xpire-crossdomain-scanner	1.0cb8d3b	Scans crossdomain.xml policies for expired domain names.	https://github.com/mandatoryprogrammer/xpire-crossdomain-scanner
xpl-search	42.d4dbc97	Поиск эксплойтов по множеству базам данных эксплойтов!.	https://github.com/CoderPirata/XPL-SEARCH
xplico	33.0f6d8bc	Internet Traffic Decoder. Network Forensic Analysis Tool (NFAT).	http://www.xplico.org/
xprobe2	0.3	An active OS fingerprinting tool.	http://sourceforge.net/apps/mediawiki/xprobe/index.php?title=Main_Page
xspy	1.0c	A utility for monitoring keypresses on remote X servers	http://www.freshports.org/security/xspy/
xsser	1.7	Инструмент для тестирования на проникновение для выявления и эксплуатации уязвимостей XSS.	https://xsser.03c8.net/
xssless	35.9eee648	An automated XSS payload generator written in python.	https://github.com/mandatoryprogrammer/xssless
xsss	0.40b	A brute force cross site scripting scanner.	http://www.sven.de/xsss/
xssscan	17.7f1ea90	Command line tool for detection of XSS attacks in URLs. Based on ModSecurity rules from OWASP CRS.	https://github.com/gwroblew/detectXSSlib
xsssniper	0.9	An automatic XSS discovery tool	https://github.com/gbrindisi/xsssniper
xsstracer	5.f2ed21a	Скрипт на Python, который проверяет удалённые веб-сервера на Кликджекинг,	https://github.com/1N3/XSSTracer

Имя	Версия	Описание	Домашняя страница
		кросс-сайтовый скриптинг, кросс-сайтовый трэкинг и инъекцию заголовка хоста.	
xssya	12.abe1aec	A Cross Site Scripting Scanner & Vulnerability Confirmation.	https://github.com/yehia-mamdouh/XSSYA
xxeinjector	50.a76fac9	Инструмент для автоматизированной эксплуатации уязвимости XXE, используя прямой и различные вне групповые методы.	https://github.com/enjoiz/XXEinjector
yaaf	7.4d6273a	Yet Another Admin Finder.	https://github.com/Plasticoo/YAAF
yaf	2.7.1	Yet Another Flowmeter.	http://tools.netsa.cert.org/yaf/
yara	3.4.0	Tool aimed at helping malware researchers to identify and classify malware samples	https://plusvic.github.io/yara/
yasat	839	Yet Another Stupid Audit Tool.	http://yasat.sourceforge.net/
yasca	2.1	Набор инструментов статичного анализа кода множества языков.	http://www.scovetta.com/yasca.html
yasuo	105.29ef967	Скрипт на ruby, который сканирует на уязвимости и эксплуатируемость веб-приложения в сети.	https://github.com/0xsauby/yasuo
ycrawler	0.1	A web crawler that is useful for grabbing all user supplied input related to a given website and will save the output. It has proxy and log file support.	http://packetstormsecurity.com/files/98546/yCrawler-Web-Crawling-Utility.html
yersinia	0.7.3	A network tool designed to take advantage of some weakness in different network protocols.	http://www.yersinia.net/
yinjector	0.1	A MySQL injection penetration tool. It has multiple features, proxy support, and multiple exploitation methods.	http://packetstormsecurity.com/files/98359/yInjector-MySQL-Injection-Tool.html
ysoserial	0.0.2	Рабочий концепт для генерации рабочей нагрузки, которая эксплуатирует небезопасную десериализацию объектов Java.	https://github.com/frohoff/ysoserial
zackattack	5.1f96c14	A new tool set to do NTLM Authentication relaying unlike any other tool currently out there.	https://github.com/urbanesec/ZackAttack/
zaproxy	2.4.3	Integrated penetration testing tool for finding vulnerabilities in web applications	https://www.owasp.org/index.php/ZAP
zarp	0.1.7	A network attack tool centered around the exploitation of local networks.	https://defense.ballastsecurity.net/wiki/index.php/Zarp
zerowine	0.0.2	Malware Analysis Tool - research project to dynamically analyze the behavior of malware	http://zerowine.sf.net/
zgrab	418.1870438	Собирает банеры (может и через TLS).	https://github.com/zmap/zgrab
zizzania	115.a063e6c	Автоматизированный захват рукопожатий с использованием атаки деаутентификация	https://github.com/cyrus-and/zizzania
zmap	2.1.1	Fast network scanner designed for Internet-wide network surveys	https://zmap.io/
zulu	0.1	A light weight 802.11 wireless frame generation tool to enable fast and easy debugging and probing of 802.11 networks.	http://sourceforge.net/projects/zulu-wireless/
zykeys	0.1	Demonstrates how default wireless settings are derived on some models of ZyXEL routers.	http://packetstormsecurity.com/files/119156/Zykeys-Wireless-Tool.html
zzuf	0.14	Transparent application input fuzzer.	http://sam.zoy.org/zzuf/