**Важнейшие инструменты для тестирования в сети**

*[Этичный Хакер](http://t.me/hack_less" \t "_blank)August 18, 2023*



Инструменты сетевой безопасности для тестирования на проникновение чаще используются в сфере безопасности для проверки уязвимостей в сети и приложениях.

Здесь вы можете найти список комплексных инструментов сетевой безопасности, который охватывает выполнение операции тестирования на проникновение во всей среде.

**Инструменты сетевой безопасности**

**Сканирование/пентестинг**

* **OpenVAS** — представляет собой набор из нескольких сервисов и инструментов, предлагающих комплексное и мощное решение для сканирования и управления уязвимостями.
* **Metasploit** **Framework** — один из лучших инструментов сетевой безопасности для разработки и выполнения кода эксплойта на удаленной целевой машине. Другие важные подпроекты включают базу данных Opcode, архив шелл-кода и соответствующие исследования.
* **Kali** **Linux** — это производный от Debian дистрибутив Linux, предназначенный для цифровой криминалистики и тестирования на проникновение. В Kali Linux предустановлено множество программ для тестирования на проникновение, включая nmap (сканер портов), Wireshark (анализатор пакетов), John the Ripper (взломщик паролей) и Aircrack-ng (программный пакет для тестирования беспроводных локальных сетей на проникновение). .
* pig — инструмент для создания пакетов Linux.
* Scapy: интерактивная программа и библиотека для работы с пакетами на основе Python.
* Pompem — это инструмент сетевой безопасности с открытым исходным кодом, предназначенный для автоматизации поиска эксплойтов в основных базах данных. Разработан на Python, имеет систему расширенного поиска, что облегчает работу пентестеров и этичных хакеров. В текущей версии выполняет поиск в базах данных: Exploit-db, 1337day, Packetstorm Security…
* Nmap — бесплатная утилита с открытым исходным кодом для обнаружения сети и аудита безопасности.

**Мониторинг/регистрация**

* Justniffer — это анализатор сетевых протоколов, который фиксирует сетевой трафик и создает журналы в индивидуальном порядке, может эмулировать файлы журналов веб-сервера Apache, отслеживать время отклика и извлекать все «перехваченные» файлы из HTTP-трафика.
* httpry —  это специализированный анализатор пакетов, предназначенный для отображения и регистрации HTTP-трафика. Он предназначен не для выполнения самого анализа, а для захвата, анализа и регистрации трафика для последующего анализа. Его можно запустить в режиме реального времени, отображая трафик по мере его анализа, или как процесс-демон, который записывает данные в выходной файл. Он написан максимально легким и гибким, чтобы его можно было легко адаптировать к различным приложениям.
* ngrep — стремится предоставить большинство общих функций GNU grep, применяя их на сетевом уровне. ngrep — это инструмент с поддержкой pcap, который позволит вам указать расширенные регулярные или шестнадцатеричные выражения для сопоставления с полезными данными пакетов. В настоящее время он распознает IPv4/6, TCP, UDP, ICMPv4/6, IGMP и Raw через Ethernet, PPP, SLIP, FDDI, Token Ring и нулевые интерфейсы и понимает логику фильтрации BPF так же, как более распространенные инструменты анализа пакетов, такие как как tcpdump и snoop.
* passivedns — один из лучших инструментов сетевой безопасности для пассивного сбора записей DNS для помощи в обработке инцидентов, мониторинге сетевой безопасности (NSM) и общей цифровой криминалистике. PassiveDNS перехватывает трафик с интерфейса или читает pcap-файл и выводит ответы DNS-сервера в лог-файл. PassiveDNS может кэшировать/агрегировать дубликаты ответов DNS в памяти, ограничивая объем данных в файле журнала без потери сути ответа DNS.
* Sagan использует движок и правила, похожие на Snort, для анализа журналов (syslog/журнал событий/snmptrap/netflow/и т. д.).
* Node Security Platform — набор функций, аналогичный Snyk, но в большинстве случаев бесплатный и очень дешевый для других.
* Ntopng — это проверка сетевого трафика, которая показывает использование сети, аналогично тому, что делает популярная команда top Unix.
* Fibratus — это инструмент для исследования и отслеживания ядра Windows. Он способен захватывать большую часть активности ядра Windows — создание и завершение процесса/потока, ввод-вывод файловой системы, реестр, сетевую активность, загрузку/выгрузку DLL и многое другое. Fibratus имеет очень простой интерфейс командной строки, который инкапсулирует механизмы для запуска сборщика потока событий ядра, установки фильтров событий ядра или запуска облегченных модулей Python, называемых филаментами.

**IDS / IPS / Host IDS / Host IPS**

* Snort — это бесплатная система предотвращения сетевых вторжений (NIPS) и система обнаружения сетевых вторжений (NIDS) с открытым исходным кодом, созданная Мартином Решем в 1998 году. В настоящее время Snort разрабатывается компанией Sourcefire, основателем и техническим директором которой является Роеш. В 2009 году Snort вошел в Зал славы открытого исходного кода InfoWorld как один из «величайших [предметов] программного обеспечения с открытым исходным кодом всех времен».
* Bro — это мощная структура сетевого анализа, которая сильно отличается от типичных IDS, которые вы, возможно, знаете.
* OSSEC — всеобъемлющий HIDS с открытым исходным кодом. Не для слабонервных. Требуется немного, чтобы понять, как это работает. Выполняет анализ журнала, проверку целостности файлов, мониторинг политик, обнаружение руткитов, оповещение в реальном времени и активное реагирование. Он работает в большинстве операционных систем, включая Linux, MacOS, Solaris, HP-UX, AIX и Windows. Много адекватной документации. Оптимальное место занимают средние и крупные развертывания.
* Suricata — это высокопроизводительный механизм Network IDS, IPS и Network Security Monitoring. Открытый исходный код и принадлежит некоммерческому фонду, управляемому сообществом, Open Information Security Foundation (OISF). Suricata разработана OISF и поддерживающими его поставщиками.
* Security Onion — это дистрибутив Linux для обнаружения вторжений, мониторинга сетевой безопасности и управления журналами. Он основан на Ubuntu и содержит Snort, Suricata, Bro, OSSEC, Sguil, Squert, Snorby, ELSA, Xplico, NetworkMiner и многие другие инструменты безопасности. Простой в использовании мастер установки позволяет за считанные минуты создать целую армию распределенных датчиков для вашего предприятия!
* sshwatch — IPS для SSH, аналогичный DenyHosts, написанный на Python. Он также может собирать информацию о злоумышленнике во время атаки в журнале.
* Stealth — проверка целостности файлов, практически не оставляющая осадка. Контроллер запускается с другой машины, из-за чего злоумышленнику трудно понять, что файловая система проверяется через определенные псевдослучайные интервалы через SSH. Настоятельно рекомендуется для малых и средних развертываний.
* AIEngine — это интерактивный/программируемый механизм проверки пакетов Python/Ruby/Java/Lua следующего поколения с возможностями обучения без вмешательства человека, функциями NIDS (Система обнаружения сетевых вторжений), классификацией доменов DNS, сетевым сборщиком, сетевой криминалистикой и многими другими функциями. другие.
* Denyhosts — предотвращает атаки SSH на основе словаря и атаки грубой силы.
* Fail2Ban — сканирует файлы журналов и принимает меры в отношении IP-адресов, демонстрирующих вредоносное поведение.
* SSHGuard - программное обеспечение для защиты сервисов в дополнение к SSH, написанное на C.
* Lynis — инструмент аудита безопасности с открытым исходным кодом для Linux/Unix.

**Honeypot tools**

* HoneyPy — это приманка с низким и средним уровнем взаимодействия. Он предназначен для простого развертывания, расширения функциональности с помощью подключаемых модулей и применения пользовательских конфигураций.
* Dionaea задуман как преемник nepenthes, встраивающий python в качестве языка сценариев, использующий libemu для обнаружения шелл-кодов, поддерживающий ipv6 и tls.
* Conpot – ICS/SCADA Honeypot. Conpot — это малоинтерактивная приманка промышленных систем управления на стороне сервера, которую легко развертывать, модифицировать и расширять. Предоставляя ряд общих промышленных протоколов управления, мы создали основу для создания собственной системы, способной эмулировать сложные инфраструктуры, чтобы убедить противника, что он только что нашел огромный промышленный комплекс.
* Amun - Honeypot с низким уровнем взаимодействия на основе Amun Python.
* Glastopf — это приманка, которая эмулирует тысячи уязвимостей для сбора данных об атаках, направленных на веб-приложения. Принцип очень прост: дайте правильный ответ злоумышленнику, использующему веб-приложение.
* Kippo — это приманка SSH со средним уровнем взаимодействия, предназначенная для регистрации атак грубой силы и, что наиболее важно, всего взаимодействия с оболочкой, выполняемого злоумышленником.
* Kojoney — это приманка низкого уровня взаимодействия, которая эмулирует сервер SSH. Демон написан на Python с использованием библиотек Twisted Conch.
* HonSSH — это решение Honey Pot с высоким уровнем взаимодействия. HonSSH будет располагаться между злоумышленником и приманкой, создавая между ними два отдельных соединения SSH.
* Bifrozt — это устройство NAT с DHCP-сервером, которое обычно развернуто с одной сетевой картой, подключенной непосредственно к Интернету, и одной сетевой картой, подключенной к внутренней сети. Что отличает Bifrozt от других стандартных устройств NAT, так это его способность работать в качестве прозрачного прокси-сервера SSHv2 между злоумышленником и вашей приманкой.
* HoneyDrive — лучший дистрибутив Linux-приманки. Это виртуальное устройство (OVA) с установленной версией Xubuntu Desktop 12.04.4 LTS. Он содержит более 10 предустановленных и предварительно настроенных программных пакетов-приманок, таких как приманка Kippo SSH, вредоносные приманки Dionaea и Amun, приманка Honeyd с низким уровнем взаимодействия, веб-приманка Glastopf и Wordpot, приманка Conpot SCADA/ICS, приманки Thug и PhoneyC и многое другое. .
* Cuckoo Sandbox — это программное обеспечение с открытым исходным кодом для автоматизации анализа подозрительных файлов. Для этого он использует специальные компоненты, которые отслеживают поведение вредоносных процессов во время работы в изолированной среде.

**Захват и анализ пакетов**

* tcpflow — это программа, которая захватывает данные, передаваемые в рамках TCP-соединений (потоков), и сохраняет данные в виде, удобном для анализа и отладки протокола.
* Xplico. Целью Xplico является извлечение из интернет-трафика содержащихся данных приложений. Например, из файла pcap Xplico извлекает каждое электронное письмо (протоколы POP, IMAP и SMTP), все содержимое HTTP, каждый вызов VoIP (SIP), FTP, TFTP и т. д. Xplico не является анализатором сетевых протоколов. Xplico — это инструмент сетевого криминалистического анализа (NFAT) с открытым исходным кодом.
* Moloch — это крупномасштабная система захвата пакетов IPv4 (PCAP), индексации и базы данных с открытым исходным кодом. Для просмотра, поиска и экспорта PCAP предусмотрен простой веб-интерфейс. Доступны API-интерфейсы, которые позволяют напрямую загружать данные PCAP и данные сеанса в формате JSON. Простая безопасность реализуется за счет поддержки дайджест-паролей HTTPS и HTTP или использования apache впереди. Moloch не предназначен для замены механизмов IDS, а вместо этого работает вместе с ними для хранения и индексации всего сетевого трафика в стандартном формате PCAP, обеспечивая быстрый доступ. Moloch создан для развертывания во многих системах и может масштабироваться для обработки трафика в несколько гигабит в секунду.
* OpenFPC — это набор инструментов, которые в совокупности обеспечивают облегченную полнофункциональную систему записи сетевого трафика и буферизации. Цель его разработки — позволить пользователям, не являющимся экспертами, развертывать распределенный регистратор сетевого трафика на оборудовании COTS, одновременно интегрируя его в существующие средства управления предупреждениями и журналами.
* Dshell — это фреймворк для судебного анализа сети. Обеспечивает быструю разработку подключаемых модулей для поддержки разбора перехваченных сетевых пакетов.
* stenographer — решение для захвата пакетов, предназначенное для быстрой буферизации всех пакетов на диск, а затем для обеспечения простого и быстрого доступа к подмножествам этих пакетов.

**Инструменты сетевой безопасности на основе сниффера**

* Wireshark — это бесплатный анализатор пакетов с открытым исходным кодом. Он используется для устранения неполадок в сети, анализа, разработки программного обеспечения и протоколов связи, а также для обучения. Wireshark очень похож на tcpdump, но имеет графический интерфейс, а также некоторые встроенные параметры сортировки и фильтрации.
* netsniff-ng — это бесплатный сетевой инструментарий для Linux, швейцарский армейский нож для ежедневного подключения к сети Linux, если хотите. Прирост производительности достигается за счет механизмов нулевого копирования, так что при приеме и передаче пакетов ядру не нужно копировать пакеты из пространства ядра в пространство пользователя и наоборот.
* Заголовки HTTP в реальном времени. Заголовки HTTP в реальном времени — это бесплатное дополнение Firefox, позволяющее просматривать запросы вашего браузера в режиме реального времени. Он показывает полные заголовки запросов и может использоваться для поиска лазеек в безопасности в реализациях.

**SIEM — инструменты сетевой безопасности**

* Prelude — Prelude — это универсальная система управления информацией и событиями безопасности (SIEM). Prelude собирает, нормализует, сортирует, объединяет, сопоставляет и сообщает обо всех событиях, связанных с безопасностью, независимо от марки продукта или лицензии, вызвавших такие события; Прелюдия «без агента».
* OSSIM — OSSIM предоставляет все функции, необходимые специалисту по безопасности в предложении SIEM, — сбор событий, нормализацию и корреляцию.
* FIR — Fast Incident Response, платформа управления инцидентами кибербезопасности.

**VPN**

* OpenVPN — OpenVPN — это программное приложение с открытым исходным кодом, которое реализует методы виртуальной частной сети (VPN) для создания безопасных соединений «точка-точка» или «сеть-сеть» в маршрутизируемых или мостовых конфигурациях и средствах удаленного доступа. Он использует собственный протокол безопасности, использующий SSL/TLS для обмена ключами.

**Быстрая обработка пакетов**

* DPDK — DPDK представляет собой набор библиотек и драйверов для быстрой обработки пакетов.
* PFQ — PFQ — это функциональная сетевая структура, разработанная для операционной системы Linux, которая обеспечивает эффективный захват/передачу пакетов (10G и выше), функциональную обработку в ядре и управление пакетами через сокеты/конечные точки.
* PF\_RING — PF\_RING — это новый тип сетевого сокета, который значительно повышает скорость захвата пакетов.
* PF\_RING ZC (Zero Copy) — PF\_RING ZC (Zero Copy) — это гибкая структура обработки пакетов, позволяющая достичь скорости обработки пакетов 1/10 Гбит (как RX, так и TX) при любом размере пакета. Он реализует операции с нулевым копированием, включая шаблоны для взаимодействия между процессами и между виртуальными машинами (KVM).
* PACKET\_MMAP/TPACKET/AF\_PACKET — можно использовать PACKET\_MMAP для повышения производительности процесса захвата и передачи в Linux.
* netmap — netmap — это фреймворк для высокоскоростного пакетного ввода-вывода. Вместе со своим сопутствующим программным переключателем VALE он реализован как единый модуль ядра и доступен для FreeBSD, Linux, а теперь и для Windows.

**Инструменты сетевой безопасности на основе брандмауэра**

* pfSense — дистрибутив FreeBSD для брандмауэра и маршрутизатора.
* OPNsense — это открытый исходный код, простой в использовании и простой в сборке брандмауэр и платформа маршрутизации на основе FreeBSD. OPNsense включает в себя большинство функций, доступных в дорогих коммерческих брандмауэрах, а во многих случаях даже больше. Он предлагает богатый набор функций коммерческих предложений с преимуществами открытых и проверенных источников.
* fwknop — защищает порты с помощью однопакетной авторизации в вашем брандмауэре.

**Анти-Спам**

* SpamAssassin — мощный и популярный фильтр спама в электронной почте, использующий различные методы обнаружения.

**Образы Docker для тестирования на проникновение**

* docker pull kalilinux/kali-linux-docker Официальный Кали Линукс
* docker pull owasp/zap2docker-stable– Официальный OWASP ZAP
* docker pull wpscanteam/wpscan- Официальный WPScan
* docker pull remnux/metasploit— Докер-метасплоит
* docker pull citizenstig/dvwa– Чертовски уязвимое веб-приложение (DVWA)
* docker pull wpscanteam/vulnerablewordpress– Уязвимый WordPress
* docker pull hmlio/vaas-cve-2014-6271– Уязвимость: Shellshock
* docker pull hmlio/vaas-cve-2014-0160– Уязвимость: Heartbleed
* docker pull opendns/security-ninjas- Ниндзя-безопасность
* docker pull diogomonica/docker-bench-security– Docker Bench для безопасности
* docker pull ismisepaul/securityshepherd– пастырь безопасности OWASP
* docker pull danmx/docker-owasp-webgoat– Образ докера проекта OWASP WebGoat.
* docker-compose build && docker-compose up– OWASP NodeGoat
* docker pull citizenstig/nowasp– Приложение OWASP Mutillidae II для веб-тестирования на проникновение