Intercepter-NG
absolute capture

Инструкция

v.01

Предисловие

Данный мануал должен отсеять большинство вопросов, связанных с использованием Intercepter-NG, однако надо понимать, что возникающие трудности в большей степени могут зависеть от личного непонимания технических особенностей реализации и применения различных сетевых атак. Программа бесполезна для школьников и "мамкиных хакиров". Столь позднее появление мануала, лишь на десятом году существования проекта, обусловлено постоянно изменяющимся функционалом и частичным изменением интерфейса и ряда настроек. Так или иначе, текущая версия Intercepter-NG находится в более или менее законченном виде, и любые последующие изменения не должны внести кардинальных перемен.

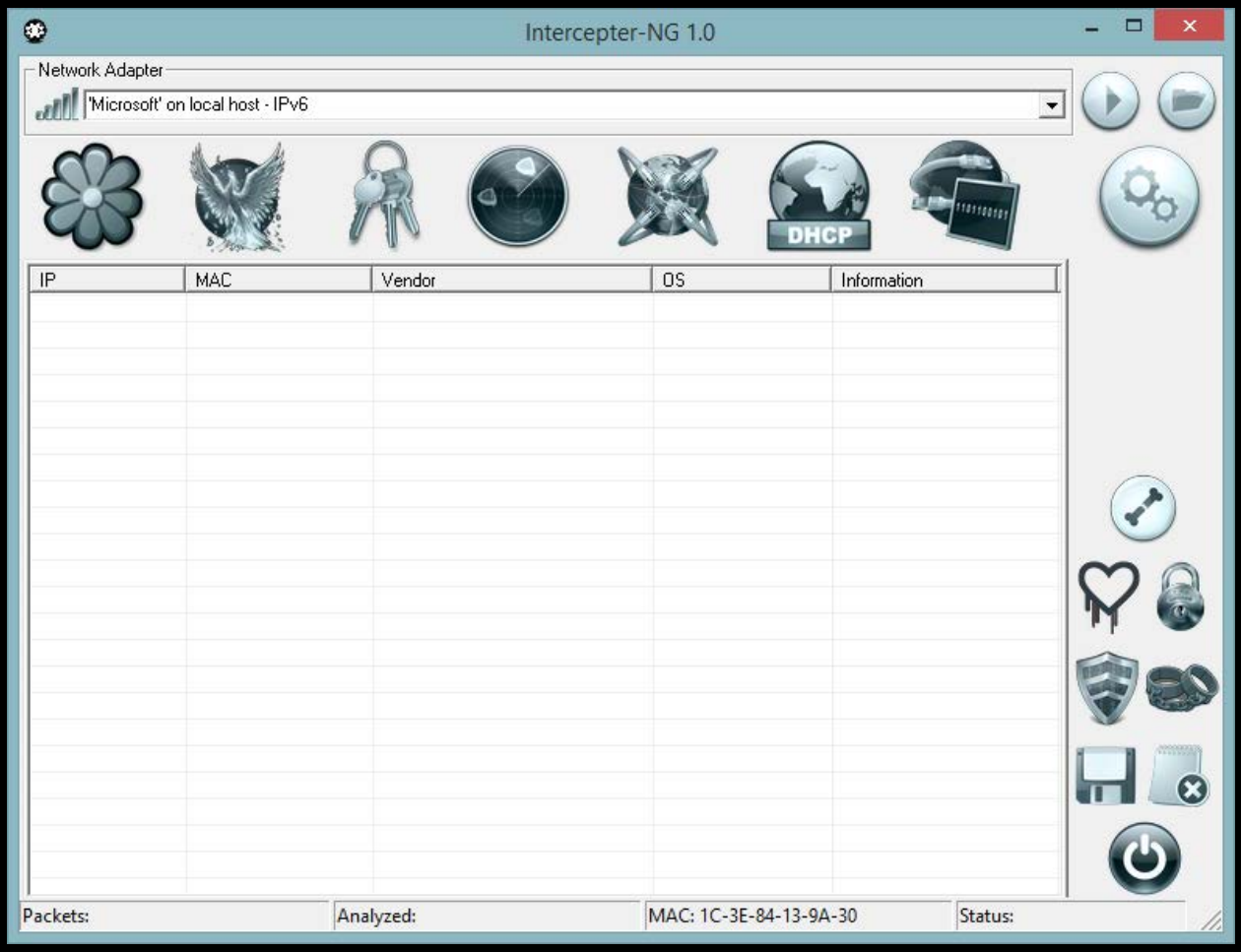
Итак, Intercepter-NG это мультифункциональный сетевой инструмент, предназначенный для администраторов, программистов и специалистов по информационной безопасности. Двумя базовыми функциями инструмента являются:

1. Восстановление данных из трафика, таких как пароли, файлы, переписка и т.п.

2. Перехват трафика посредством MiTM атак.

Кроме этого, Intercepter-NG предоставляет широкий спектр различных функций, о которых будет сказано в дальнейшем.

Изначально Intercepter-NG разрабатывался под ОС Windows, и максимальный функционал представлен именно в этой версии. Также серьезное внимание было уделено версии под Android. Существует консольная версия, собранная под Linux\BSD и Mac (OS X), но на данный момент разработка этой версии практически приостановлена. Windows-версия может быть запущена с ограниченным функционалом под Wine.



В верхней части окна находится выпадающий список обнаруженных сетевых интерфейсов. Если по какой-то причине вашей сетевой карты нет в списке, это означает, что она не поддерживается WinPcap, хотя это очень редкая ситуация. Также имейте в виду, что при наличии сетевого драйвера от Microsoft, карта может не иметь ожидаемого названия - в этом случае она будет называться просто "Microsoft", поэтому нужно обращать внимание на IP адрес, а не название интерфейса. Естественно сетевой интерфейс должен иметь настроенный адрес. Запуск анализа пакетов происходит нажатием кнопки "Play", а справа от нее находится кнопка открытия .pcap файлов. Допускается выбор нескольких файлов - в этом случае файлы будут обрабатываться по очереди. Обработку .pcap файла можно осуществить перетаскиванием файла на рабочую область экрана (drag & drop), но это работает только для одного файла.

Ниже находится кнопка настроек.

Password Mode

Поддерживаемые протоколы для восстановления паролей:

Plain Text: **PPTP\PPPoE PAP, Oracle, MS-SQL, PostgreSQL, NNTP, CVS, WWW Basic, HTTP, SOCKSv5, MRA, FTP, DC++, POP3, SMTP AUTH-PLAIN\AUTH-LOGIN, IMAP, LDAP, AIM, IRC**.

Hashes: **PPTP\PPPoE CHAP-MD5\MS-CHAP\MS-CHAPv2, Kerberos, RADIUS, Oracle DES\AES128, MongoDB, MySQL SHA1, VNC, MRA MD5, SMTP\POP3 CRAM-MD5, POP3 APOP-MD5, POP3 NTLM-SSP, IMAP CRAM-MD5, ICQ MD5, SMB NTLM**.

MiTM-атаки дополнительно позволяют перехватить учетные данные протоколов HTTPS, IMAPS, SMTPS, POP3S.

Для некоторых хешей предусмотрен контекстный брутфорс непосредственно из приложения. Для этого необходимо скачать john the ripper с jumbo-патчем в папку Intercepter-NG. Все исполняемые файлы должны находиться в каталоге john. Брутфорс запускается правой кнопкой мыши по хешу выбором пункта «Brute It!».

Обработчик HTTP, помимо встроенного списка полей, использует эвристический метод для обнаружения авторизации. Non-ASCII символы в именах пользователя или паролях, кодируемые как %XX (URL-encoding), автоматически конвертируются. Имеется поддержка интернациональных доменных имен. Опционально включается отображение cookie, которые можно открыть через IE, и получить доступ к сессии. Для протоколов Telnet\Rsh\Rlogin осуществляется полное логирование сессий.

Messengers Mode

Поддерживаемые мессенджеры для восстановления переписки: **ICQ\AIM, JABBER, YAHOO, MSN, IRC, MRA**. Естественно при условии, что отсутствует шифрование.

Resurrection Mode

Протоколы, для которых реализовано восстановление файлов: HTTP, FTP, IMAP, POP3, SMTP, SMB, TFTP. Восстановлению подлежат только законченные цепочки фреймов, неполные файлы на диск не сохраняются. В данном режиме имеется несколько фильтров, например минимальный и максимальный размер файлов, а также отсеивание текстовых файлов из HTTP трафика.

Scan Mode

Режим сканирования является активным по умолчанию после запуска инструмента. Основная задача данного режима заключается в ARP сканировании с целью выявления других участников сети (компьютеры, телефоны, прочее сетевое оборудование), для чего необходимо запустить ARP Scanning. Кроме обычного ARP сканирования имеется Promisc Detection, который позволяет найти с определенной точностью сетевые устройства, находящиеся в promiscuous-mode, т.е. в неразборчивом режиме, который является потенциальным признаком наличия сниффера. Надо помнить, что некоторые сетевые карты (3com) могут реагировать на данное сканирование даже при отключенном неразборчивом режиме. DHCP Discovering позволяет найти действующие DHCP сервера в сети. Gateway Discovering обнаруживает действующие интернет-шлюзы; обнаружение происходит отсылкой tcp-syn пакета на 8.8.8.8:53.

Для более точного сканирования сети с плохой связью (WiFi) или при наличии большого количества активных хостов может понадобиться увеличение параметра ARP Scan Timeout.

Основной функцией данного режима является «Smart Scan», которая комбинирует в себе целый ряд подфункций, и автоматизирует заполнение некоторых параметров для проведения MiTM атак. При выполнении "умного сканирования" сперва выполняется обычное ARP сканирование, после чего найденные хосты подвергаются более глубокому анализу. В зависимости от условий определяется приблизительная версия операционной системы, NETBIOS имя хоста, а так же имя Apple устройств (Bonjour). Автоматически происходит поиск сетевых шлюзов, и заполняются поля Gateway и Stealth в MiTM режиме. Важно помнить, что в некоторых сетях может быть несколько шлюзов, и за корректную конфигурацию сетевых параметров режима MiTM отвечает пользователь. Автоматизация лишь служит помощником в небольших и простых сетях. Параметр Stealth необходим для корректной работы сложных MiTM атак. Это должен быть свободный незадействованный IP-адрес с выходом в интернет. Желательно перепроверить, что автоматически подобранный адрес действительно свободен и не принадлежит другому участнику сети, который по каким-либо причинам не был обнаружен во время сканирования.

DHCP Mode

Это обычный DHCP сервер, который можно использовать как по прямому назначению, так и для захвата dhcp клиентов в свою подсеть с целью проведения MiTM атаки. Для корректной работы требуется предварительная настройка MiTM режима. По умолчанию указана подсеть 1.1.1.X, клиенты которой будут автоматически маршрутизироваться в действующую сеть. На этапе трансляции можно провести атаки типа SSL Strip, SSL MiTM и ряд других. Старт сервера автоматически включает функцию NAT. Можно

настроить whitelist, в котором указать IP адреса для конкретных MAC адресов, например 00-11-22-33-44-55:1.2.3.4.

RAW Mode

"Сырой" режим является классическим пакетным анализатором визуально напоминающим Wireshark. Несмотря на то, что функционал встроенного анализатора Intercepter-NG гораздо меньше, он вполне достаточен для выполнения базовых задач. Основной обработчик пакетов, который используется и для восстановления данных, и для "сырого" режима, поддерживает большое количество инкапсуляций, в том числе IPv6. Кроме отображения основных TCP\UDP сведений в RAW режиме выводится дополнительная информация по ряду протоколов, например ARP\DNS\NETBIOS запросы. При включении фильтра "Show Only Data" пакеты с нулевым размером данных будут игнорироваться. "Copy as Hex C-Array" копирует в буфер обмена весь фрейм в виде шестнадцатеричной последовательности в формате Си массива. Функция "Follow TCP Stream" позволяет отфильтровать конкретную TCP сессию. В этом режиме присутствует Pcap Filter, который позволяет задать правила фильтрации для всего приложения, а не только для Raw Mode. Синтаксис pcap-фильтра можно найти в интернете, например для захвата TCP или UDP пакетов можно задать "tcp" или "udp" соответственно, а для захвата только HTTP протокола - "tcp port 80".

MiTM Mode

Переименован из NAT в MiTM. Изначально представлял собой классический симметричный NAT с трансляцией ICMP\TCP\UDP пакетов и поддержкой FTP Active mode. Именно с этим было связано наличие в предыдущих версиях выбора двух сетевых карт: Internal и External. В этом режиме представлено большинство MiTM атак, которые будут рассмотрены позднее.

В поле Gateway в большинстве случаев необходимо указывать действующий Интернет-шлюз. В Stealth, как было сказано ранее, свободный IP адрес в сети с выходом в Интернет (без блока на шлюзе). В Targets соответственно адреса клиентов-целей. Кнопка "Play" запускает работу NAT, а соседняя "радиация" запускает ARP Poison.

Settings

Раздел содержит ряд глобальных настроек и некоторые специфичные опции.

Resolve Hosts – определение имени узла по IP адресу в режиме паролей. При анализе .pcap дампов его необходимо отключить для ускорения обработки.

Lock on Tray - при сворачивании приложения в tray и последующем восстановлении будет запрошен пароль. По умолчанию пароль 4553. Его можно сменить вручную в файле settings.cfg, пароль хранится в base64 кодировке.

Save Session - сохранение пакетов в .pcap файл.

Promiscuous - перевод сетевой карты в неразборчивый режим. В редких случаях требует отключения.

Unique Data - фильтрация дублей в режиме паролей.

Autosave - автоматическое сохранение текстового лога собранной информации.

Grid View - вывод данных в виде таблицы в режиме паролей. При отключении будет показан старый режим в виде простого текста. Требуется в редких случаях, например при перехвате ICQ MD5.

eXtreme Mode - проверка всех пакетов всеми обработчиками, независимо от сетевых портов. Может помочь в перехвате служб на нестандартных портах. Не рекомендуется для постоянного использования.

Capture Only – опция, работающая совместно с Save Session. Никакой анализ не проводится, Intercepter-NG просто собирает данные в .pcap файл.

Resurrection - отвечает за восстановление файлов из сетевого трафика.

Spoof IP\MAC - отвечает за подмену IP и MAC адреса, при обычном ARP Poison обеспечивает полную скрытную работу. При сложных MiTM атаках скрытность обеспечивается только для стороны жертвы.

iOS Killer - см. раздел про атаки.

Kerberos Downgrade - понижение с aes-256-cts-hmac-sha1-96 до rc4-hmac в AS-REQ пакетах.

HSTS Spoofing - см. раздел про атаки.

IP Forward - классический IP форвардинг, позволяет осуществить ARP Poison в случае, когда невозможно использовать Stealth IP. Сложные MiTM атаки не работают.

Cookie Killer - см. раздел про атаки.

Extra SSL Port - установка SSL MiTM на любой дополнительный порт. Можно указать список через запятую.

Remote Capture - настройка на удаленный захват при помощи rpcapd-демона. В правиле not host необходимо указать свой же IP адрес для игнорирования служебного трафика.

PCAP Over IP - другой способ удаленного захвата. С любого удаленного хоста можно направить трафик непосредственно на Intercepter-NG. Для этого необходимо запустить tcpdump, и перенаправить его вывод в netcat. Пример использования:

#cat log.cap | nc IP PORT

#tcpdump -i face -w - not port PORT| nc IP PORT

#dumpcap -i face -P -w - | nc IP PORT

IP - адрес Intercepter, PORT - значение указанное в настройках, по умолчанию 2002.

WPAD Configuration - настройка конфигурации для WPAD MiTM. Возможно использование встроенного proxy-сервера.

В настройках присутствует экспертный режим, который будет рассмотрен позже.

В правом нижнем углу находятся несколько дополнительных режимов. Кроме них присутствует кнопка сохранения данных (дискета) и очистки логов (блокнот). Сохранять можно как в текстовом виде, так и в HTML. При сохранении в RAW режиме можно сохранить .pcap файл.

HeartBleed

Это эксплойт уязвимости SSL HeartBleed, позволяет получить произвольный кусок памяти на уязвимом сервере.

ARP Watch

Функция слежения за состоянием ARP таблицы: в случае подмены в разделе NAT появится надпись с предупреждением.

ARP Cage

ARP Клетка позволяет изолировать один хост от другого.

Bruteforce Mode

Сетевой переборщик паролей. Поддерживаемые протоколы: FTP, POP3 (TLS), SMTP (TLS), IMAP, SSH, HTTP Basic/POST, LDAP, SMB, TELNET, VNC, VMWARE, RDP.

Кнопка Test Password позволяет проверить произвольный пароль. Heuristic Bruteforce генерирует ряд вариаций на основе введенного слова. Single Mode устанавливает правило: один коннект - одна попытка. Максимальное количество эффективных тредов зависит индивидуально от удаленного сервиса, подбирается эмпирическим путем.

X-Scan

Сетевой сканер безопасности, способен на следующее:

1. Сканировать открытые порты и эвристически определять следующие протоколы: SSH, Telnet, HTTP\Proxy, Socks4\5, VNC, RDP.

2. Определять наличие SSL на открытом порту, читать баннеры и различные web заголовки.

3. При обнаружении прокси или сокса, проверять их открытость наружу.

4. Проверять беспарольный доступ к VNC серверам, проверять SSL на HeartBleed. Читать version.bind у DNS.

5. Проверять по базе наличие скриптов на веб-сервере, потенциально уязвимых к ShellShock. Проверять по базе список директорий и файлов на 200 OK, а так же список директорий из robots.txt.

6. Определять версию ОС через SMB. При наличии анонимного доступа получать локальное время, uptime, список общих ресурсов и локальных пользователей. Для найденных пользователей запускается автоматический перебор паролей.

7. Определять по встроенному списку пользователей SSH через замер времени отклика. Для найденных пользователей запускается автоматический перебор паролей. Если энумерация не дала результата (работает не на всех версиях), перебор запускается только для root.

8. Автоматический брутфорс для HTTP Basic и Telnet. Учитывая особенности telnet протокола возможны ложные срабатывания.

Сканировать можно любые цели, как в локальной сети так и в интернете. Можно указывать список портов для скана: 192.168.1.1:80,443 или диапазон 192.168.1.1:100-200. Можно указывать диапазон адресов для скана: 192.168.1.1-192.168.3.255. При установленной опции Scan ICMP Alive Only сканирование портов будет происходить только "живых" хостов, ответивших на ping. По умолчанию сканируются наиболее распространенные порты, для сканирования всех портов есть опция Scan All Ports. Custom userlist позволяет загрузить свой список пользователей, для которых будет запускаться автоматический перебор паролей. Режимы сканирования Reliable\Normal\Fast регулируют целый ряд параметров работы сканера, влияющих на точность и скорость определения состояния портов и запущенных служб. В локальных сетях с хорошей связью между компьютерами допускается применение режима Fast, для более точного результата рекомендуется режим Reliable.

MiTM Атаки

В Intercepter-NG все MiTM атаки можно разделить на две группы: транспортные и прикладные. К транспортным атакам относятся ARP Poison, DNS Over ICMP MiTM и DHCP MiTM. Перечисленные типы атак в первую очередь служат для захвата чужого трафика. Прикладные атаки (или так называемые "сложные MiTM") позволяют изменять трафик и вытаскивать информацию из защищенных протоколов. К таким атакам можно отнести: SSL MiTM, SSL Strip, SSH MiTM, SMB Hijacking, Group Policy Hijacking, LDAP Relay, MySQL LOAD DATA Injection, HTTP Injections. Несколько особняком стоят: Spoofing Mode, Traffic Changer, WPAD MiTM. Основная последовательность действий для запуска атак сводится к следующему: выбрать цели из режима сканирования или внести их вручную в MiTM Mode, настроить поля Gateway и Stealth и запустить ARP Poison. Некоторые "сложные митмы" имеют свои особенности конфигурации. Все нюансы применения MiTM атак продемонстрированы в серии обзорных видео роликов на Youtube канале проекта.

SSL MiTM

Классический SSL MiTM с подменой сертификатов. Поддерживаемые протоколы: HTTPS, POP3S, SMTPS, IMAPS. Любой другой протокол можно подключить через Extra SSL Port в настройках. SSL трафик в чистом виде пишется в лог файл. Функция iOS Killer, совместно с SSL MiTM, позволяет перехватить авторизацию iCloud, Instagram, VK, а функция Cookier Killer поможет сбросить сессию мобильного приложения Facebook.

SSL Strip

Преобразует https ссылки в http, тем самым заставляя цель отправлять данные в открытом виде. Самостоятельно проксирует соединения до оригинального https ресурса. Подмена происходит только в открытом трафике. В настройках можно включить HSTS Spoofing. Эффективность не очень высокая, и требуется предварительная настройка misc\hsts.txt.

SSH MiTM

Перехват авторизации и сессии SSH протокола версии 2.0. Поддерживает два механизма аутентификации: password и keyboard-interactive. Подробности в статье "MiTM атака на SSH".

WPAD MiTM

WPAD - Web Proxy Auto-Discovery Protocol. Отвечает на llmnr\nbns запросы имени WPAD, и выдает настройки proxy сервера. Позволяет перехватить web трафик. При использовании встроенного proxy сервера можно получить NETNTLM хеши, автоматически пересылаемые браузером при определенных условиях. Подробности в статье "Перехват WEB трафика через протокол WPAD при помощи Intercepter-NG".

SMB Hijacking

Аналог атаки SMBRelay. Работает в современных сетях. Подробности в статье "SMB Hijacking. Kerberos is defeated" и "SMB Hijacking. Kerberos не помеха". В экспертных настройках можно переключить вариант атаки с smb hijack на классический smb relay, поддерживающий NTLMv2.

GP Hijacking

Позволяет получить SYSTEM shell практически на любой цели в доменной сети. Подробности в статье "Group Policy Hijacking" и "Обзор нового Intercepter-NG 0.9.10".

LDAP Relay

Позволяет получить права Domain Admin при NTLM Relay атаке на действующего администратора сети. Подробности в статье "Ldap Relay. NTLM strikes back again" и "Реинкарнация NTLM-relay или как стать администратором домена за 1 минуту".

DNS Over ICMP MiTM

Получение контроля над частью исходящего трафика через ICMP редиректы. Подробности в статье "Снифер + MITM-атаки = 0x4553-Intercepter".

FATE

Режим FATE совмещает в себе две функции: FAke siTE и FAke updaTE.

Ключевой целью FAke siTE является получение авторизационных данных с любого веб ресурса, в обход SSL и других механизмов защиты. Достигается это клонированием страницы авторизации и созданием шаблона, который будет размещаться на встроенном псевдо-веб сервере.

Fake updaTE эксплуатирует механизм автоматического обновления, которое выполняется без открытым способом, без ssl и дополнительных проверок. При желании можно добавлять софт самостоятельно, структуру шаблонов можно посмотреть в misc\FATE\updates.

Traffic Changer

Режим замены данных в сетевых пакетах. Длина данных **до** и **после** должна быть одинаковой. Менять можно как текстовые данные так и бинарные, синтаксис для бинарных паттернов как в Си — "\x01\x02\x03". Если требуется подмена в HTTP трафике, то в настройках необходимо включить опцию «Disable HTTP gzip encoding».

Spoofing Mode

Классический спуфинг для протоколов DNS, LLMNR, NBNS.

HTTP Injection

Позволяет добавлять правила замены данных в веб трафике. В поле Pattern вводится шаблон для замены, это может быть расширение файлов или конкретное имя, например .jpg или manual.doc. В Content-Type соответствующий тип данных, в Count количество производимых замен, в User-Agent можно указать конкретный UA для целевого применения. При нажатии кнопки Add будет предложено выбрать файл, которым будет заменен запрашиваемый файл согласно шаблону. Если в Pattern мы ввели .jpg, то при запросе GET /photo.jpg картинка будет заменена той, что была выбрана пользователем. Кнопка Update служит для обновления полей в имеющейся записи, в основном это требуется для увеличения поля Count. Кроме этого в данном режиме присутствует 4 Inject функции.

Inject Java Backdoor - внедряет в веб трафик java аплет. При низком уровне безопасности Java и запуске со стороны пользователя - произойдет обратное соединение на shell обработчик.

Inject Plugin Detector - внедряет специальный java скрипт, который соберет информацию об установленных расширениях браузера и отправит ее атакующему.

Inject Forced Download - принудительная закачка файла на стороне цели как если бы закачка была инициирована ручным нажатием ссылки.

Inject Reverse Shell - принудительная закачка back connect пейлоада. При запуске будет предоставлен шелл доступ.

to be continued...