Три миллиарда человек во всем мире, то есть около 40% населения, пользуются социальными сетями в интернете. Мы тратим на них в среднем два часа ежедневно: публикуем заметки, обмениваемся фото, реагируем на посты друзей.

Каждую минуту пользователи соцсетей отправляют почти полмиллиона твитов и фотографий в Snapchat.

Если социальные медиа играют в нашей жизни такую большую роль, то очень важно понимать, как они влияют на нас.

Именно поэтому спецслужбы имеют доступ к нашим социальным сетям.

Автоматические сканеры уязвимостей

Айтишники, как известно, стремятся все автоматизировать, и хакеры в этом не отстают. Существуют автоматические сканеры уязвимостей — чтобы можно было запустить, откинуться на спинку кресла и потягивать кофе (или пивко), пока они сделают целую гору работы. Поиск уязвимостей с их использованием сводится к тому, чтобы отдать сканеру адрес цели и нажать большую кнопку Start, ну или Enter, если ты любитель терминала.

При этом понятно, что сканер найдет только типовые уязвимости и, чтобы пойти дальше, нужно уметь не только нажимать на кнопку. Но почему бы не сэкономить немного сил? Во многих случаях это вполне оправданно.

Категории и методы

Универсальных инструментов не существует, и сканеры уязвимостей не стали исключением из этого правила. Они обычно нацелены на уязвимости какого-то определенного рода. В этой статье мы рассмотрим следующие виды сканеров.

- WVS (Web Vulnerability Scanner) — сканеры веб-уязвимостей. У меня это самая многочисленная категория. Сюда входят как общеизвестные OWASP ZAP и sqlmap, так и менее известные, но не менее полезные, вроде Vega.
- Анализаторы мобильных приложений. Тут очень мало достойных продуктов, и мы остановимся на самых ярких из них.

- Полууниверсальные сканеры для локальной сети предприятия или дома. Это уже не просто сканеры, а целые комбайны для анализа и учета оборудования в сети. Многие из них заодно ищут уязвимости.
- Всякие узкоспециализированные сканеры типа анализа исходного кода, Git/SVN-репозиториев и других сложных для ручной обработки массивов данных.

Сканеры бывают со свободной лицензией и коммерческие. Если с опенсорсом все понятно, то для использования коммерческих придется выложить весьма приличную сумму. К сожалению, ни редакция «Хакера», ни автор не настолько богаты, чтобы покупать их для обзора. Поэтому для всех коммерческих сканеров была использована официальная пробная версия, если не оговорено иное.

Само тестирование тоже бывает разным: Black Box либо White Box. При первом типе пентестер или его инструмент должны работать с сервисом через те же интерфейсы, через которые с ним взаимодействуют пользователи. Например, если для тестирования методом Black Box тебе дан сайт, то ты можешь проверять его только как посетитель, без какого-либо специального доступа к исходному коду или привилегированным аккаунтам. Если это приложение, то подразумевается, что у тебя нет доступа к исходникам: ковыряй сам, если сможешь. В общем, Black Box значит, что у тебя нет ничего, чего бы не было у всех.

При тестировании методом White Box пентестер (или хакер) имеет доступ ко всем потрохам целевого объекта. Если это сайт — у тебя есть его код. Если это сервер — у тебя есть доступ к его внутренностям вроде версии ОС и установленного софта или к некоторым файлам. В этом случае возможности куда шире и ты можешь найти проблему, которую способен эксплуатировать только продвинутый злоумышленник.

Sn1per

Цена: Community edition — бесплатно, Professional edition — от 150 долларов

Sn1per — мощный фреймворк для автоматического анализа безопасности цели. Разработан небезызвестным 1N3, основателем компании XeroSecurity. Из других его известных инструментов — Findsploit (для быстрого поиска эксплоитов к уязвимости) и PrivEst — для поиска локальных багов EoP.

Sn1per поставляется в двух вариантах. Есть версия Community «для всех и даром» и Sn1per Professional, лицензия на который стоит от 150 зеленых американских

рублей.

В бесплатном варианте сканер умеет собирать базовую информацию (IP цели, ping, whois, DNS); запускает Nmap для поиска открытых портов и определения сервисов, в том числе и с помощью NSE; ищет часто встречающиеся уязвимости и автоматически эксплуатирует их; пробует получить доступ ко всем файловым шарам (FTP, NFS, Samba); запускает Nikto, WPScan и Arachni для всех найденных веб-приложений и многое другое. Поддерживает интеграцию с Hunter.io, OpenVAS, Burp Suite, Shodan, Censys и Metasploit.

Установка довольно проста и поддерживает Docker, что сводит ее к двум командам:

dockerpullxerosecurity/sn1perdocker run -it xerosecurity/sn1per /bin/bash

Для сканирования выполни

sniper -t [TARGET]

Чтобы задействовать все возможности Sn1per, понадобятся дополнительные ключи:

o — использует движок OSINT;

- -re — разведка;
- -fp — полностью проработать все порты;
- -m stealth — старательно скрывает сканер, чтобы цель не поняла, что ее сканируют;
- -m webscan — Sn1per будет работать как обычный сканер WVS;
- -b — использовать брутфорс при необходимости;
- -f [FILE] — сканировать сразу несколько целей, которые перечислены в файле [FILE];
- -m nuke — «ядерный» режим сканирования. Включает в себя брутфорс, обработку всех портов, OSINT, разведку и сохранение всех находок (loot);
- -m massvulnscan — очень мощная функция в сочетании с -f. Массово сканирует на многие известные уязвимости все заданные цели. Если в тестируемой компании много хостов, эта опция будет весьма полезна;
- -m discover — опция поиска всех хостов в заданной подсети и запуск сканирования на каждый из найденных. Если ты даже не знаешь всех возможных целей, это будет очень полезно.

Wapiti3

Цена: бесплатно

Wapiti — подвид американских оленей полностью бесплатный сканер веб-уязвимостей. На момент написания статьи последняя версия была 3.0.3, выпущенная 20 февраля этого года, то есть проект живой. Несмотря на скромные размеры сканера (всего 2,3 Мбайт в распакованном виде), набор функций у него довольно обширный. По официальному заявлению, сканер умеет обнаруживать следующие баги:

- раскрытие содержимого файла (local file inclusion), в том числе бэкапов и исходного кода сайта;
- SQL-инъекции и внедрение кода PHP/ASP/JSP;
- отраженные и хранимые XSS;
- инъекции команд ОС;
- XXE Injection;
- неудачные конфигурации .htaccess;
- Open Redirect.

Wapiti3 поддерживает прокси, аутентификацию на целевом сайте, умеет не кричать на самопальные сертификаты SSL и может вставлять в запросы любые заголовки (в том числе кастомный User-Agent).

Использование инструмента весьма тривиально. После установки выполни в терминале (да, это консольное приложение) такую команду:

wapiti -u [URL]

Wapiti просканирует весь сайт и выдаст соответствующий отчет. Чтобы исключить ненужные адреса (например, logout), добавь параметр -x [URL], а для авторизованного сканирования требуются куки. Для их использования сначала сгенерируй JSON-файл с помощью специального скрипта. Он лежит в bin/wapiti-getcookie и запускается следующим образом:

wapiti-getcookie -u [LOGIN_URL] -c cookies.json -d "username=[USER]&password=[PASS]"

[LOGIN_URL] — это адрес страницы логина, а [USER] и [PASS] — логин и пароль соответственно. Затем подключаем готовый файл к сканеру:

wapiti -u [URL] -x [EXCLUDE] -c cookies.json

Вот и все. Отчет генерируется в HTML и сохраняется в /home/[USER]/.wapiti/generated_report/[TARGET_HOST]_[DATE]_[ID].html, где [USER] — твой логин, [TARGET_HOST] — целевой сайт, [DATE] — дата сканирования и [ID]— четыре цифры. Можно открыть в браузере и посмотреть.

MobSF

Цена: бесплатно

Последний в этой статье, но не последний по ценности и наворотам сканер, который будет отлично смотреться в арсенале пентестера. Это еще один статический анализатор мобильных приложений, тоже написанный на Python, но работающий только в Windows.

Загружаем туда APK или IPA (да, приложения для iOS тоже поддерживаются) и ждем окончания анализа. После этого видим весьма обширный отчет о найденных багах с указанием возможности эксплуатации. Цветовая индикация серьезности тоже присутствует, и в целом интерфейс весьма дружественный, не хватает только поддержки русского.

Сканер умеет анализировать код, сертификат, которым подписано приложение, его манифест и позволяет выгрузить декомпилированный код для последующего анализа в других программах. Анализ выполняется как статически (декомпиляция и анализ полученного кода), так и динамически (запуск в виртуальном окружении).

Можно скачать инструмент на GitHub или установить по инструкции ниже.

Для начала нам нужен Python с pip. Далее установи rsa следующей командой:

python -m pip install rsa

Скачай скрипт установки и выполни. Отвечай на вопросы (установщик интерактивный) — и пользуйся на здоровье.

Можно также основную часть инструмента запустить на одной машине (это может быть Linux), а сервер для статического анализа — на другой (тут нужна Windows). Чтобы выключить эту возможность, поправь MobSF/settings.py, указав в WINDOWS_VM_IP адрес твоей виртуальной машины с RPC-сервером.

В целом инструмент очень хороший и удобный. Правда, лично у меня установка вызвала некоторые проблемы — из-за битых зависимостей.

Заключение

Многие люди против слежки за ними в соц. сетях, он именно благодаря этому слежению, соц. службы могут предотвратить многие теракты суициды запланированные всевозможные сходки пьянки и т. д.

Но отслеживать все до мелкого шага тоже нехорошо, каждый человек имеет право на личную жизнь и сохранение каких-либо секретов.

Лично против досконального отслеживания в интернете.

Список литературы

1. https://zen.yandex.ru/media/id/5e79af0605140c7f02909152/hak-v-odin-klik-skanery-uiazvimostei-5ea1bfa365d5b620781f37a2
2. https://www.bbc.com/ukrainian/vert-fut-russian-42694015