УДК: 004.492.3

Сканер уязвимости Web-серверов NIKTO

Ларчиков Д.Э., Госуниверситет-УНПК группа 11-ИБ

Nikto — open source сканер, который осуществляет всеобъемлющее тестирование веб-серверов на уязвимости, в том числе проверяет наличие более 6500 потенциально опасных файлов и CGI, определяет устаревшие версии более 1250 различных веб-серверов, а также отображает специфические проблемы для более чем 270 версий серверов. Сканер также определяет типичные ошибки в конфигурации веб-сервера, в том числе наличие нескольких индексных файлов, опции HTTP-сервера, после чего пытается составить максимально полный список версий программ и модулей на сервере. Список сканируемых объектов в Nikto реализован в виде подключаемых плагинов и часто обновляется (эти плагины не являются open source).

Сканер Nikto спроектирован для работы в скрытном режиме: он осуществляет сканирование максимально быстро, записывая результаты в лог. Версия 2.1.5 содержит исправления нескольких багов, а также новые функции и новые виды проверок . Среди самого важного — распознавание IP в HTTP-заголовках, автоматическая проверка доступных файлов после парсинга robots.txt, проверка иконок в <link>, проверка уязвимостей с crossdomain.xml и clientaccesspolicy.xml. Среди новых опций программы — установка максимального времени сканирования хоста (в секундах) для маскировки сканирования, повтор сохранённых JSON-запросов с помощью replay.pl, поддержка SSL-сертификатов на стороне клиента, более продвинутое тестирование за счёт автоматического добавления переменных в db_variables после парсинга robots.txt или других страниц.

Для чего нужен Nikto. Web-серверы - одни из самых уязвимых сервисов, так как нередко их сложно правильно настроить и

администраторы настраивают их по принципу «лишь бы работало». Поистине, множество уязвимостей Web-серверов связано с их неправильной настройкой, а не ошибками в программе.

Сервер Apache - один из наиболее защищенных Web-серверов, но все старания разработчиков пропадают впустую, потому что администраторы размещают некоторые CGI-сценариев в каталоге cgi-bin.

Рассмотрим сканер уязвимостей Web-сервера - программу Nikto, в базе данных которой содержатся сведений о более чем 3500 уязвимостях для 900 различных серверов и версии специфических проблем о более чем 250 серверов. Эта утилита чрезвычайно полезна не только для хакеров, но и для администраторов Web-сервера.

Основные функции программы:

- Поддержка плагинов, что позволяет пользователям расширять возможности программы, добавляя новые типы сканирования.
- "Обход" IDS (Intrusion Detection System, система обнаружения вторжения).
- Поддержка SSL (Secure Sockets Layer).
- Поддержка прокси.
- Вывод в форматах: текст, HTML, CSV (Comma Separated Values).
- Находит Web-сервера, расположенные на нестандартных портах.
- Проверка огромного числа уязвимостей.

Чтобы запустить Nikto ваша система должна иметь базовую поддержку Perl. Самой программе нужны два модуля: LibWhisker и Net::SSLeay. Также в системе должна быть поддержка OpenSSL и установлен сканер уязвимостей nmap.

Параметры обхода IDS. Наиболее интересная функция программы Nikto - это IDS-обход системы обнаружения вторжений, который позволяет «обойти» большинство известных IDS, то есть просканировать сервер так,

что IDS этого не заметит.

Параметры IDS устанавливаются в командной строке с помощью опции -e:

- Произвольное URL-кодирование (не-UTF8).
- Добавление "ссылки" каталога (/./).
- Преждевременное завершение URL.
- Присоединение длинных случайных строк к запросу.
- Использование в запросах TAB вместо пробела.
- Использование разделителя пути MS Windows (\) вместо (/).
- Случайный выбор регистра.

Можно устанавливать несколько опций, например, -e 25 означает, что были выбраны опции 2 и 5.

Кроме опции -e, можно использовать опции:

- -Cgidirs — указывает каталог /cgi-bin.
- -cookies - выводит полученные во время сканирования Cookies.
- -generic - запускает полное сканирование.

Использование Nikto. Базовое сканирование. Например, просканировать внутренний Web-сервер:

perl nikto.pl -h 192.168.0.1

Можно указать определенный порт (например, порт 443), или даже протокол, который будет проверяться (например, https://), или проверку порта 443 с использованием ssl:

perl nikto.pl -h 192.168.0.1 -p 443

perl nikto.pl -h https://192.168.0.1:443/

perl nikto.pl -h 192.168.0.1 -p 443 -ssl

Nikto поддерживает сканирование с использованием нескольких портов, например:

perl nikto.pl -h 192.168.0.1 -p 80,88,443

Также эта программа умеет работать через прокси. Для этого нужно

установить значение переменой системы PROXY. Используется следующая команда:

perl nikto.pl -h 192.168.0.1 -p 80 -u

Для автоматизации сканирования предусмотрено сканирование нескольких web-серверов за один раз. Для этого нужно создать текстовый файл (web.txt) такого вида:

192.168.0.2:80

192.168.0.2:443

192.168.2.30:8000

И передать его программе Nikto:

perl nikto.pl -h web.txt

Если в файле не указать номер порта, то по умолчанию будет использоваться порт 80.

При выводе отчета о сканировании Nikto выводит версии Apache и PHP и сообщает, что, если они содержат уязвимости, их нужно обновить.

Конфигурационный файл Nikto.

В дополнение к опциям командной строки Nikto для удобства поддерживает текстовый файл конфигурации - config.txt. Все параметры в этом файле хорошо прокомментированы, следовательно, можно самостоятельно с ними разобраться. Рассмотрим некоторые опции для примера:

- CGIDIRS — список каталогов (разделенный пробелами), в котором нужно производить поиск CGI-сценариев. Для администратора: использование нестандартного имени каталога для CGI-файлов не остановит хакера.
- ADMINDIR — список каталогов администратора.
- USERS — имена пользователей, которые будут использоваться при попытке установить домашние каталоги пользователей или при подборе паролей, когда будет достигнута защищенная паролем область Web-сервера.

Параметры запуска.

Прежде всего следует обратить внимание на синтаксис параметров. Все они регистрозависимые — при наборе необходимо учитывать прописные и строчные буквы.

Параметр -config.Данный параметр позволяет задать другой конфигурационный файл и не использовать тот, который находится в корне директории nikto.

Параметр -findonly.Данный параметр указывает сканеру на неполное сканирование исследуемого сервера — лишь на обнаружение открытых HTTP/HTTPS-портов.

Параметр -host.Данным параметром задается имя исследуемого компьютера или его IP-адрес. В случае если параметр -nolookup указан, необходимо задавать IP-адрес, а не DNS-имя компьютера.

Параметр -id.Опция -id позволяет задать имя пользователя и пароль для входа на web-сервер, который требует предварительной авторизации. Пример работы этой команды следующий:

./nikto.pl –id login:password –host testserver, где login — имя пользователя; password — пароль; testserver — название исследуемого компьютера.

Параметр -port.Настоящая опция позволяет вручную указать порт, который использует исследуемый web-сервер. По умолчанию этот параметр имеет значение 80. Однако если сканер обнаружил и другие открытые стандартные порты, то он будет их применять в процессе сканирования.

Параметр -ssl.Данная опция отключает сканирование web-сервера по HTTPS-протоколу. В основном она необходима потому, что очень многие серверы требуют дополнительной аутентификации и в любом случае сканирование не осуществится.

Параметр -useproxy.Данная опция включает режим работы через прокси-сервер, который указывается в конфигурационном файле config.txt.

Работа через прокси-сервер более корректна с точки зрения защиты от обнаружения сканирования удаленным компьютером.

В заключение отметим, что сканер Nikto является отличным подспорьем и для системного администратора, и для web-программиста, поскольку позволяет определять уязвимости не только серверного программного обеспечения (Apache и др.), но и самих скриптов. Базы данных, поставляемые в комплекте со сканером, содержат записи о тысячах уязвимостей, которые ранее были найдены в популярных скриптах (форумах, голосованиях, CMS).

На официальном сайте также говорится о возможности интеграции сканера уязвимостей Nikto со сканером Nessus.

Список литературы:

1. NIKTO сканер уязвимости Web-серверов.Личный блог Suvan'a.http://suvan.ru/page/nikto.html Дата посещения 25.10.2012
2. FAQ и релизы.Nikto-сканер уязвимости Web-серверов.http://www.xaker.name/forvb/showthread.php?t=16257 Дата посещения 15.11.2012
3. Журнал КомпьютерПресс #6 2008 года (http://www.compress.ru/article.aspx?id=19161&iid=889) Дата посещения 12.12.12