

Эксплойт

Материал из Википедии — свободной энциклопедии

Экспл^бйт (англ. *exploit*, эксплуатировать) — компьютерная программа, фрагмент программного кода или последовательность команд, использующие уязвимости в программном обеспечении и применяемые для проведения атаки на вычислительную систему. Целью атаки может быть как захват контроля над системой (повышение привилегий), так и нарушение её функционирования (DoS-атака).

Содержание

Классификация

Виды эксплойтов

Как выглядит эксплойт?

Актуальность

Связки (набор эксплойтов, exploit kit)

Примечания

Ссылки

См. также

Классификация

В зависимости от метода получения доступа к уязвимому программному обеспечению эксплойты подразделяются на удалённые (англ. *remote*) и локальные (англ. *local*).

- *Удалённый эксплойт* работает через сеть и использует уязвимость в защите без какого-либо предварительного доступа к уязвимой системе;
- *Локальный эксплойт* запускается непосредственно в уязвимой системе, требуя предварительного доступа к ней. Обычно используется для получения взломщиком прав суперпользователя.

Атака эксплойта может быть нацелена на различные компоненты вычислительной системы — серверные приложения, клиентские приложения или модули операционной системы. Для использования серверной уязвимости эксплойту достаточно сформировать и послать серверу запрос, содержащий вредоносный код. Использовать уязвимость клиента немного сложнее — требуется убедить пользователя в необходимости подключения к поддельному серверу (перехода по ссылке в случае если уязвимый клиент является браузером).

Виды эксплойтов

Эксплойты фактически предназначены для выполнения сторонних действий на уязвимой системе и могут быть разделены между собой следующим образом:

1. Эксплойты для операционных систем.
2. Эксплойты для прикладного ПО (музыкальные проигрыватели, офисные пакеты и т. д.).
3. Эксплойты для браузеров (Internet Explorer, Mozilla Firefox, Opera и другие).
4. Эксплойты для интернет-продуктов (IPB, WordPress, VBulletin, phpBB).
5. Эксплойты для интернет-сайтов (facebook.com, hi5.com, livejournal.com).
6. Другие эксплойты.

Как выглядит эксплойт?

Эксплойт может распространяться в виде исходных текстов, исполняемых модулей или словесного описания использования уязвимости. Он может быть написан на любом языке программирования (наиболее часто использующиеся: C/C++, Perl, Python, PHP, HTML+JavaScript)^[1].

Эксплойты могут быть классифицированы также по типу используемой ими уязвимости, такой как: переполнение буфера, внедрение SQL-кода, межсайтовый скриптинг, подделка межсайтовых запросов и т. д.

Актуальность

Информация, полученная в результате обнаружения уязвимости, может быть использована как для написания эксплойта, так и для устранения уязвимости. Поэтому в ней одинаково заинтересованы обе стороны — и взломщик, и производитель взламываемого программного обеспечения. Характер распространения этой информации определяет время, которое требуется разработчику до выпуска заплатки.

После закрытия уязвимости производителем шанс успешного применения эксплойта начинает стремительно уменьшаться. Поэтому особой популярностью среди хакеров пользуются так называемые 0day-эксплойты, использующие недавно появившиеся уязвимости, которые ещё не стали общеизвестны^[2].

Связки (набор эксплойтов, exploit kit)

Связки эксплойтов представляют собой пакет эксплойтов сразу под несколько программ (версий) и/или под разные уязвимости в них. В последних версиях связок производится выбор эксплойта именно под конкретную программу пользователя.


В большинстве случаев эксплойт-киты применяются для атак, использующих уязвимости браузеров или их дополнений (частыми целями, к примеру, являются Java, Flash и PDF)^[3].

Также существуют наборы локальных эксплойтов для поднятия привилегий в атакованной системе. Фактически подобные наборы тоже являются связками, но в хакерской среде таковыми не считаются и не называются.

Примечания

1. *ReanimatoR*. Что такое эксплойт? (<http://xakepam.ru/article/a-4.html>) (недоступная ссылка). xakepam.ru (22 августа 2008). Дата обращения: 31 августа 2009. Архивировано (<https://web.archive.org>)

[e.org/web/20120208231208/http://xakepam.ru/article/a-4.html](http://xakepam.ru/article/a-4.html)) 8 февраля 2012 года.

2. *Catherine Engelke*. What is zero-day exploit? (http://searchsecurity.techtarget.com/sDefinition/0,,sid14_gci955554,00.html) (англ.) (недоступная ссылка). SearchSecurity.com (4 июня 2007). Дата обращения: 31 августа 2009. Архивировано (https://web.archive.org/web/20101003180515/http://searchsecurity.techtarget.com/sDefinition/0,,sid14_gci955554,00.html) 3 октября 2010 года.
3. <https://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-evolution-of-exploit-kits.pdf> 

Ссылки

- *jonse*. Новости и описания Эксплойтов (<http://exploit.in>) (недоступная ссылка). Exploit.IN (9 марта 2010). Дата обращения: 9 марта 2010. Архивировано (<https://web.archive.org/web/20100216135506/http://www.exploit.in/>) 16 февраля 2010 года.
- *Mik*. Сетевые эксплойты (<http://www.netsecret.by/index.php?type=review&area=1&p=articles&id=8>). netsecret.by (11 октября 2007). Дата обращения: 31 августа 2009. (недоступная ссылка)
- *хеоп*. Эксплойты (<http://exploit.in.ua>) (недоступная ссылка). Exploit.In.UA (18 февраля 2010). Дата обращения: 18 февраля 2010. Архивировано (<https://web.archive.org/web/20090914150504/http://exploit.in.ua/>) 14 сентября 2009 года.
- Архив эксплоитов с 2001 года (<http://www.securitylab.ru/pos/>) (недоступная ссылка). securitylab.ru (25 февраля 2010). Дата обращения: 25 февраля 2010. Архивировано (<https://web.archive.org/web/20110104023521/http://www.securitylab.ru/pos/>) 4 января 2011 года.
- База данных эксплоитов и уязвимостей (<https://0day.today>)

См. также

- [DoublePulsar](#)
 - [EternalBlue](#)
 - [Буткит](#)
 - [Бэкдор](#)
 - [Уязвимость нулевого дня](#)
-

Источник — <https://ru.wikipedia.org/w/index.php?title=Эксплойт&oldid=111654954>

Эта страница в последний раз была отредактирована 11 января 2021 в 10:34.

Текст доступен по лицензии Creative Commons Attribution-ShareAlike; в отдельных случаях могут действовать дополнительные условия.

Wikipedia® — зарегистрированный товарный знак некоммерческой организации Wikimedia Foundation, Inc.