Шелл-код

Материал из Википедии — свободной энциклопедии

Шелл-код (англ. *shellcode*, код запуска оболочки) — это двоичный исполняемый код, который обычно передаёт управление командному процессору, например '/bin/sh' в Unix shell, 'command.com' в MS-DOS и 'cmd.exe' в операционных системах Microsoft Windows. Шелл-код может быть использован как полезная нагрузка эксплойта, обеспечивающая взломщику доступ к командной оболочке (англ. *shell*) в компьютерной системе.

При эксплуатации удаленной уязвимости шелл-код может открывать заранее заданный порт TCP уязвимого компьютера, через который будет осуществляться дальнейший доступ к командной оболочке, такой код называется привязывающим к порту (англ. *port binding shellcode*). Если шелл-код осуществляет подключение к порту компьютера атакующего, что производится с целью обхода брандмауэра или NAT, то такой код называется обратной оболочкой (англ. *reverse shell shellcode*).

Содержание

Принцип работы

Шелл-код обычно внедряется в память эксплуатируемой программы, после чего на него передается управление путём переполнения стека, или при переполнении буфера в куче, или используя атаки форматной строки. Передача управления шелл-коду осуществляется перезаписью адреса возврата в стеке адресом внедрённого шелл-кода, перезаписью адресов вызываемых функций или изменением обработчиков прерываний. Результатом этого является выполнение шелл-кода, который открывает командную строку для использования взломщиком.

Обнаружение

Взломщики пишут шелл-коды, часто используя приёмы, скрывающие их атаку. Они часто пытаются выяснить, как системы обнаружения вторжений (СОВ) распознают любую входящую атаку. Типичная СОВ обычно просматривает все входящие пакеты в поисках структуры, специфичной для шелл-кода (часто большой массив мусорных кодов, в простейшем случае NOP-ов); если она находит такую структуру, пакет уничтожается до того, как он достигнет своей цели. Слабая позиция СОВ в данном случае состоит в том, что она не осуществляет действительно хороший поиск, иначе он займёт слишком много времени и, таким образом, замедлит соединение с интернетом.

Шелл-код почти всегда содержит строку с именем оболочки. Все входящие пакеты, содержащие такую строку, всегда рассматриваются как подозрительные в глазах СОВ. Также некоторые приложения не принимают неалфавитно-цифровой ввод (они не принимают символов, выходящих за рамки набора a-z, A-Z, 0-9 и нескольких других символов.)

Для прохождения через все эти меры, направленные против вторжения, взломщики используют шифрование, самомодифицирующийся код, полиморфный код и алфавитно-цифровой код.

См. также

- Переполнение буфера
- Переполнение кучи
- Информационная безопасность
- Язык ассемблера
- Heap spraying

Ссылки

- *Steve Hanna.* Shellcoding for Linux and Windows Tutorial with example windows and linux shellcode (http://www.vividmachines.com/shellcode/shellcode.html) (англ.) (недоступная ссылка) (2004). Дата обращения: 30 сентября 2007. Архивировано (https://web.archive.org/web/20050728094519/http://www.vividmachines.com/shellcode/shellcode.html) 28 июля 2005 года.
- Designing Shellcode Demystified (http://www.enderunix.org/docs/en/sc-en.txt) (англ.) (недоступная ссылка). Дата обращения: 28 июля 2005. Архивировано (https://web.archive.org/web/20050829191606/http://www.enderunix.org/docs/en/sc-en.txt) 29 августа 2005 года.