смертельная схватка: Open BSD vs. Server 2003 – битва за безопасность

крис касперски, no-email

OpenBSD – самая защищенная операционная система, Server 2003 – самая распространенная (речь, разумеется, идет о серверной нише), поэтому, представляет интерес сравнить двух лидеров на предмет (не)безопасности, проанализировав их устойчивость как к удаленным, так и к локальным атакам, поскольку инсайдеры представляют ничуть не меньшую угрозу, чем хакеры, находящие периметром охраняемой зоны

введение

Главным образом мы будем говорить о Microsoft Server 2003 SP2 и OpenBSD 4.2. Важно отметить, что "девственно чистый" Server 2003 без установленных пакетов обновлений очень слабо защищен и совершенно непригоден для "промышленной" эксплуатации, поскольку, будучи подключенным к глобальной Сети, мгновенно превращается в рассадник вирусов, червей и прочей заразы, чего нельзя сказать о OpenBSD, выбор версии которой в общем-то некритичен и даже древние дистрибутивы уверенно держат удар, а вредоносные программы под них либо вообще отсутствуют, либо носят "лабораторный" характер, совершенно нежизнеспособный в условиях "дикой" сети.

общее количество дыр — броня крепка и танки быстры

По данным компании Secunia (http://secunia.com/) за период 2003 — 2008 г. в OpenBSD было обнаружено всего 10 дыр, из которых только две — критические. Количество дыр в Server 2003 за тоже самое время перевалило за полторы сотни и свыше половины из них — критические (см. рис. 1). Комментарии, как говориться, излишни. Цифры отличаются на пару порядков и никакие оправдания не спасут Server 2003 от позора.

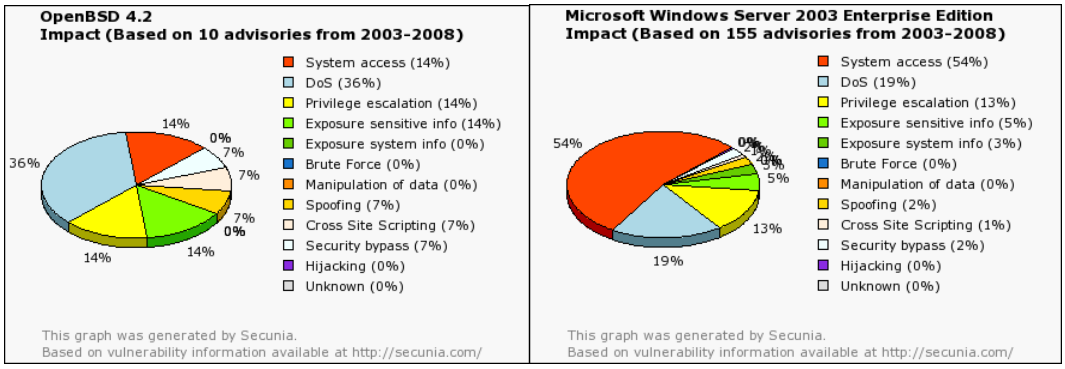

Рисунок 1 кол-во дыр в OpenBSD (слева) и Server 2003 (справа) за период 2003 – 2008 г. по данным компании Secunia

безопасность ядра — на урановых рудниках

Кто контролирует ядро — тот контролирует систему. Ядро — это своеобразная Мекка, в которую каждый уважающий себя хакер должен совершить хадж, засадив туда rootkit или другую нехорошую программу, активно сопротивляющуюся своему обнаружению и удалению из системы.

Ни в OpenBSD, ни в Server 2003 целостность ядра не проверяется. Почему? В x86/x86-64 процессорах нет адекватных аппаратных средств, позволяющих реализовать такую проверку без значительного падения производительности. И хотя в x86-64 редакции Server 2008 появился механизм PatchGuard, периодически проверяющий критические ядерные структуры, его _насколько_ просто обойти, что это не сделает только ленивый. Если говорить кратко: PatchGuard — компонент ядра, запускающийся приблизительно раз в секунду, следовательно, у зловредного кода имеется предостаточно времени для его "нейтрализации" путем прямой

модификации памяти ядра с ядерного уровня, запрещенной по умолчанию запрещена, но "отмыкаемой" всего тремя машинными командами!

С другой стороны, разработчики OpenBSD предприняли ряд шагов, существенно затрудняющих атаку на ядро. Скомпилировав монолитное ядро (без возможности загрузки модулей или, в терминологии Windows, драйверов) и запретив модификацию ядерной памяти с прикладного уровня, администратор предотвратит вторжение зловредного кода в область ядра (и хотя ошибки в ядерных компонентах, например, TCP/IP драйверах, позволяют атаковать систему, подобные дыры затыкаются в оперативном порядке, а вот не безопасность Windows носит _концептуальный_ характер, существенно исправленный в Server 2008, но все равно остающийся порочным и уязвимым).

безопасность прикладного кода — Билл не играет в кости

Нерелигиозные люди хаджей не совершают, в ядро не стремятся и вполне комфортно чувствуют себя на прикладном уровне, преимущественно используя для атаки ошибки переполнения буферов, которые в языке Си носят фундаментальный характер и потому вездесущи. Разработчики UNIX- и Windows-компиляторов предпринимают определенные усилия для предотвращения атак, но это относится только к вновь создаваемым программ, собранными новейшими компиляторами со всеми ключами безопасности. Но, как показывает статистика, даже программы, выпущенные за последние несколько лет, не используют этих возможностей, и потому приходится надеяться только на операционную систему — сумеет ли она постоять за себя или нет?

В OpenBSD запрещено исполнение кода в стеке и куче, причем целостность кучи тщательно проверяется и хакер может воздействовать лишь на указатели на функции, расположенные в памяти процесса, посредством подмены которых можно, в частности, отключить защиту от исполнения кода, и, чтобы этого не произошло, адресное пространство процесса рандомизировано — т.е. хакер заранее не знает по каким адресам окажутся расположены интересующие его функции, а потому атаки на переполняющие буфера в OpenBSD не выходят за рамки лабораторных экспериментов.

А что мы имеем в Windows? Запрет на исполнение кода появился только в Server 2003 SP1, рандомизация — в Server 2008 (точнее, некоторая пародия на рандомизацию). А сама по себе защита стека/кучи от исполнения кода без рандомизации элементарно обходится классической атакой return2libc и ни от чего не спасает, к тому же целостность кучи реально никак не проверяется и что самое противное — обработчики структурных исключений (SEH) находятся в стеке и могут быть легко атакованы. Механизм SafeSEH, призванный предотвратить атаку на SEH, остается уязвимым даже в Server 2008. Операционная система OpenBSD использует совсем другой механизм обработки исключений, не подверженный подобным угрозам.

криптография без секретов — иллюзия полета

UNIX-подобные операционные системы издавна поддерживают множество шифрованных файловых систем, существенно затрудняющих атаку даже при физическом доступе к компьютеру. В Server 2003 так же имеется что-то подобное, но… увы… приносящее больше вреда, чем пользы. Microsoft Encrypted File System, во-первых, легко взламывается при наличии достаточных вычислительных мощностей, во-вторых, ключи шифрования хранятся в пользовательском профиле, откуда их легко "вытащить" зловредной программе, а, в-третьих, эти ключи генерируются системой самостоятельно и при утере пользовательского профиля (например, в результате сбоя), теряется доступ и ко всем зашифрованным данным, а механизмы резервирования ключей появились только в Server 2008 и все еще слишком сырые и создающие много проблем при попытке их использования.

К тому же, ряд файлов (например, системный реестр или файл подкачки) вообще не могут быть зашифрованы, что существенно ослабляет безопасность. А вот OpenBSD шифрует все подряд — от системных файлов, до подкачки.

безопасность сети — глушим рыбу динамитом

В любую UNIX-подобную систему изначально входит надежный брандмауэр, вполне устраивающий подавляющее подавляюще большинство администраторов. В Server 2003 имеется что-то подобное, но уж слишком функционально ущемленное, поэтому, приходится приобретать продукты сторонних разработчиков, что, в принципе, не создает проблемы.

Проблема в другом — разработчики Server 2003 сделали все возможное, чтобы администратор _не_ мог удалить не нужные ему протоколы, а поскольку TCP/IP стек — грандиозное сооружение, содержащее миллионы строк кода — ошибки там неизбежны и обнаруживаются с завидной регулярностью. Причем, Server 2003 использует предсказуемые идентификаторы в IP/RPC-заголовках и DNS-запросах, существенно упрощая многие виды удаленных атак. В OpenBSD для этих целей используются надежные генераторы псевдослучайных чисел, оставляющих лишь теоретическую возможность атаки.

заключение

Как мы видим, Server 2003 – катастрофически небезопасная система, причем, большинство дефектов носит фундаментальный характер, требующий для своего исправления радикального редизайна ядра и потому Server 2008 в этом плане не сильно лучше. Все это — соломенные домики, разваливающийся при маленьком дуновении ветерка.

OpenBSD – напоминает неприступную крепость, стойкую ко всем погодным явлениям (включая даже такие стихийные бедствия как землетрясения и цунами), но означает ли это, что всем нам нужно немедленно сносить Server 2003 и мигрировать на OpenBSD?! Ответ отрицательный. Перенос сложившейся инфраструктуры даже небольшого предприятия с Server 2003 на OpenBSD требует существенных финансовых вложений, а вероятность пасть жертвой атаки, сидя под Server 2003, не так уж и велика…

Другими словами, переход с Server 2003 на OpenBSD в общем случае нецелесообразен. Бесплатность дистрибутива OpenBSD еще не означает бесплатности _владения_ им.

>> врезка сводная таблица

	OpenBSD	**Server 2003**
проверка целостности ядра	не поддерживается	не поддерживается
запрет загрузки модулей ядра	поддерживается	не поддерживается
удаление символьной информации о ядре	поддерживается	не поддерживается
отключение защиты памяти ядра от записи	не поддерживается	поддерживается
запрет модификации памяти ядра с прикладного уровня	поддерживается	поддерживается начиная с SP1
"люки" к ядру с прикладного режима	отсутствуют	имеются в изобилии
запрет на исполнение кода в стеке и куче	поддерживается	поддерживается начиная с SP1
контроль целостности кучи	поддерживается	не реализован должным образом
рандомизация адресного пространства	поддерживается	не поддерживается
защита обработчиков исключений	поддерживается	не реализована должным образом
шифрованная ФС	поддерживается	не реализован должным образом
автоматическое затирание удаляемых файлов	поддерживается	не поддерживается
шифрование файла подкачки	поддерживается	не поддерживается
системный диск только на чтение	поддерживается	не поддерживается
встроенный брандмауэр	поддерживается	не реализован должным образом
рандомизация ID в IP,RPC,DNS…	поддерживается	не поддерживается
загрузка в однопользовательском режиме	поддерживается	не поддерживается

Таблица 1 сравнительные характеристики основных параметров безопасности OpenBSD и Server 2003