РАЗРАБОТКА МЕТОДА ГЕНЕРАЦИИ ОТЛАДОЧНЫХ ДАМПОВ ГОСТЕВОЙ ОС WINDOWS ПОД ГИПЕРВИЗОРОМ QEMU/KVM

Прутьянов В.В. viktor.prutyanov@phystech.edu

В настоящее время рабочая нагрузка многих серверов, особенно в облачной инфраструктуре, выполняется с использованием технологии гипервизорной виртуализации. Один из популярных гипервизоров – QEMU/KVM – используется в том числе для запуска Windows в качестве гостевой ОС.

Во время работы ОС внутри виртуальных машин зачастую возникают проблемы, такие как аварийные завершения и зависания. Один из методов анализа проблем, возникающих при работе ОС Windows, — снятие снимка состояния системы, называемого дампом, и его анализ отладчиком Microsoft WinDbg. Этот метод используется при анализе проблем на физических машинах — ОС Windows может автоматически создать дамп при аварийном завершении. Но такой способ, во-первых, требует специальной настройки гостевой ОС, а во-вторых, не позволяет создать дамп работающей системы. Кроме того, при работе ОС внутри виртуальной машины дамп может быть сгенерирован на стороне гипервизора без участия гостевой ОС. Однако, в силу особенностей подсистемы создания дампов в ОС Windows с ядром 6.2 и новее, до недавнего времени все способы создания дампов на стороне гипервизора либо опирались на предоставленные гостевой ОС данные, либо полагались на эвристические методы и не всегда давали результат. QEMU позволяет сделать дамп виртуальной машины в формате ELF и сохранить в нем данные из физической памяти и регистров виртуальных процессоров, но для отладки Windows этого недостаточно.

Рассматривается метод создания полного дампа памяти (Complete Memory Dump) 64-разрядной ОС Windows с ядром 6.1 и новее, работающей внутри виртуальной машины под управлением QEMU/KVM, который не требует никаких действий внутри гостевой ОС.

Метод реализован в виде утилиты elf2dmp, которая поставляется вместе с QEMU и конвертирует дамп из формата ELF в формат DMP, понятный WinDbg. Алгоритм работы утилиты состоит из нескольких частей. Сначала происходит определение физического адреса корня таблицы страничной трансляции либо из регистра CR3 виртуального процессора, занятого системным потоком, либо из области памяти с данными для обработчика прерываний, если все процессоры заняты

пользовательскими задачами, что определяется по доступности виртуального адреса структуры PRCB.

После восстановления страничного преобразования становится доступным обращение к памяти по виртуальным адресам и сканирование виртуальной памяти на предмет сигнатуры загруженного образа ядра ОС Windows. В качестве стартового адреса для поиска сигнатуры используется адрес из первой записи таблицы дескрипторов прерываний IDT, которая находится по адресу из регистра IDTR виртуального процессора.

Далее виртуальная память сканируется в сторону уменьшения адресов, пока не будет обнаружен заголовок PE-образа ядра ntoskrnl.exe, по данным из которого можно автоматически подобрать PDB-файл с отладочной информацией и загрузить его из хранилища PDB-файлов на сайте Microsoft. Данные из PDB-файла позволяют найти в памяти виртуальной машины и расшифровать структуру KdDebuggerDataBlock, на основе которой генерируется сперва 8Кб заголовка дампа, а затем и весь дамп.

Таким образом, был разработан и реализован как часть проекта QEMU способ генерации отладочных дампов гостевой ОС Windows, не требующий кооперации со стороны гостевой ОС.

Литература

1. Prosek L. Extracting Windows VM crash dumps, 2017. https://ladipro.wordpress.com/2017/01/06/extracting-windows-vm-crash-dumps/
2. Volatility Labs The Secret to 64-bit Windows 8 and 2012 Raw Memory Dump Forensics, 2014. https://volatility-labs.blogspot.com/2014/01/the-secret-to-64-bit-windows-8-and-2012.html
3. Соломон Д. Руссинович М. Внутреннее устройство Microsoft Windows. 6-е изд. СПб.: Питер, 2013. 800 с.
4. Gu Y., Lin Z. Derandomizing kernel address space layout for memory introspection and forensics // Proceedings of the Sixth ACM Conference on Data and Application Security and Privacy. ACM, 2016. С. 62-72.