УДК 004.258

СПОСОБЫ ВЫЯВЛЕНИЯ СКРЫТЫХ КАНАЛОВ ПО ПАМЯТИ

Худяков Юрий Андреевич, Кручинин Александр Владимирович
ГВУЗ «Национальный горный университет», http://bit.nmu.org.ua, yurokaz@mail.ru

Рассмотрена классификация скрытых каналов утечки информации. Выполнен анализ реализации требований критерия КО-1 в операционных системах семейства Windows при выделении оперативной памяти для процессов в системе. Обоснован выбор инструментов для анализа. Сделано обследование ОС Windows 7 и Windows XP на выполнение критерия КО-1.

Ключевые слова – срытые каналы утечки информации, критерий повторного использования, функциональные услуги безопасности.

ВВЕДЕНИЕ

Скрытые каналы – это простые, однако очень эффективные механизмы, позволяющие передавать неавторизованную информацию с помощью методов, считающихся авторизованными.

Однако были выделены два типа скрытых каналов – это скрытые каналы по времени (covert timing channel) и скрытые каналы по памяти (covert storage channel).

Наиболее распространенным является скрытый канал по памяти, так при работе вычислительных систем с одним и тем же хранилищем данных может возникнуть скрытый канал.

Во время проведения экспертизы КСЗИ должен затрагиваться вопрос о возможных скрытых каналах утечки информации, но как такового плана проведения анализа оперативной памяти на возможные утечки не существует. Поэтому стал вопрос о работе в данном направлении.

ФУНКЦИОНАЛЬНАЯ УСЛУГА «ПОВТОРНОЕ ИСПОЛЬЗОВАНИЕ ОБЬЕКТОВ»

Услуга "Повторное использование объектов" позволяет обеспечить корректность повторного использования разделяемых ресурсов, гарантируя, что в случае, если разделяемый ресурс выделяется новому пользователю или процессу, он не содержит информации, оставшейся от предыдущего пользователя или процесса.

Исходя из этого после завершения работы с программой, данные, используемые в работе процессом должны быть освобождены из оперативной памяти. Условие выполнения критерия КО-1 является необходимым для реализации ряда других критериев.

ВЫБОР ИНСТРУМЕНТОВ ДЛЯ АНАЛИЗА

Для проведения испытаний по поиску скрытого канала утечки информации в виде не соблюдения критерия о «повторном использовании обьектов» будем использовать программные продукты, которые работают непосредственно с оперативной памятью автоматизированной системы и дают возможность наглядно установить факт наличия скрытого канала. Такими программными комплексами могу выступать: специализированные программы из сферы компьютерной криминалистики, специальные отладчики, используемые разработчиками для выявления ошибок в программных продуктах.

После проведенного подбора были выбраны такие программные отладчики:

- OllyDBG (Win7, WinXP, Win2003,Win2000);
- Visual DuxDebagger (Win7).

СРЕДА ДЛЯ АНАЛИЗА

Средой для анализа были избранны ОС Windows 7 и Windows XP как наиболее распространенные в настоящее время. Программами, взаимодействующими с оперативной памятью и работающими под управлением выше указанных ОС, выступили текстовые редакторы, так как огромную долю обработки конфиденциальной информации возлагается на данные программные продукты. Из огромного числа текстовых редакторов были выбраны наиболее популярные, а именно такие как:

- NotePad;
- WordPad;
- Word из пакета офисных программ Mircrosoft.

АНАЛИЗ ВЫПОЛНЕНИЯ ФУНКЦИОНАЛЬНОЙ УСЛУГИ «ПОВТОРНОЕ ИСПОЛЬЗОВАНИЕ ОБЬЕКТОВ»

В исследовании был использован отладчик Visual DuxDebagger и текстовый редактор NotePad.

Сканирование оперативной памяти на данные процесса проводилось в трех случаях:

1. Проверка возможности доступа к тестовой текстовой информации во время выполнения процесса.
2. Содержания тестовой текстовой информации в оперативной памяти после завершения процесса.
3. Содержания тестовой текстовой информации в оперативной памяти после завершения процесса и повторного запуска процесса того же программного обеспечения.

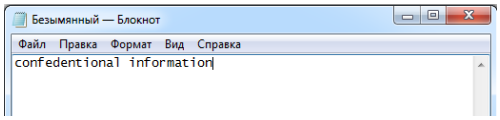

Рисунок 1. Окно текстового редактора NotePad с тестовой информацией

Во время выполнения данного процесса был запущен отладчик и просканирована оперативная

память, используемая текстовым редактором, на наличие в ней слова «information»

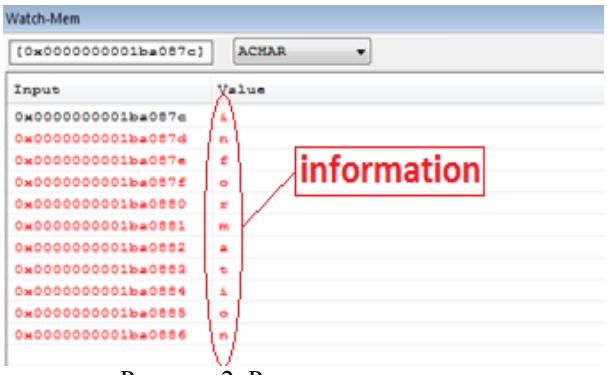

Рисунок 2. Результат сканирования

Далее был проведен эксперимент по остальным двум сценариям.

Во всех трех случаях данные, хранимые в оперативной памяти, не меняли своего местоположения и не видоизменялись, что напрямую указывает на то, что критерий КО-1 в операционных системах Windows 7 и Windows XP не выполняется.

ВЫВОД

Как видно из эксперимента функциональная услуга «Повторное использование объектов» не выполняется и требует систематизации хода экспертизы с выведением основных действий по подтверждению наличия скрытого канала. Так же необходимы дальнейшие исследование данного направления, но при использовании комплексных систем защиты, которые в теории могут решить проблему повторного использования. Результатом данной работы будет служить четко составленный план хода экспертизы системы обработки информации на выполнение функциональной услуги КО-1, что существенно облегчит общую экспертизу объекта и даст возможность привлекать к экспертизе менее квалифицированные кадры, что экономически выгодно.

СПИСОК ИСПОЛЬЗУЕМЫХ ИСТОЧНИКОВ

1. Спитцнер Л. Honeynet Project: ловушка для хакеров // Открытые системы, № 07–08, 2003.

2. Лукацкий А. В. Обнаружение атак. СПб.: БХВ-Петербург, 2003.

3. Котенко И. В., Степашкин М. В. Прототип ложной информационной системы // XI Российская научно-техническая конференция (по Северо-западному региону) “Методы и технические средства обеспечения безопасности информации”: Тезисы докладов. СПб.: Из-дательство СПбГПУ, 2003.

4. Cohen F. A Note on the Role of Deception in Information Protection // Computers and Security 1999.

5. НД ТЗІ 2.7 -009-09 Адміністрація Державної служби спеціального зв’язку та захисту інформації України, Киев, 2009