энциклопедия антиотладочных приемов — россыпи головоломок выпуск #00h (пилотный)

крис касперски, ака мыщъх, a.k.a nezumi, a.k.a souriz, a.k.a elraton, no-email

за бытность своей кодокопательской жизни мыщъх нарыл обширную (и достаточно полную) коллекцию антиотладочных приемов, надерганных из протекторов, вирусов, crack-me'сов плюс собственные идеи и разработки. систематизировав разрозненные факты и разложив их по полочкам, мыщъх решил разделить заначки своей норы с хакерским миром. вот так и возникла идея рубрики "антиотладка", главным образом посвященной NT- и UNIX-подобным операционным системам (W2K, XP, Vista, Linux, BSD) и x86-платформе. Виртуальные машины JVM и .NET так же как и 64-разрядные архитектуры пока еще находятся в исследовательской стадии, но мыщъх доберется и до них!

введение

Антиоладочными приемами называются способы противостояния отладчику от простого детеката до захвата ресурсов жизненно необходимых отладчику для работы. Все это затрудняет реконструкцию подопытной программы и хотя отладчик — не единственный хакерский инструмент (другой популярный инструмент — дизассемблер) — нельзя объять необъятное и мы решили сосредоточиться исключительно на антиотладке.

Об антиотладке написано много, настолько много, что в этом ворохе беспорядочной информации нетрудно и утонуть, причем большинство статей охватывает лишь малый круг антиотладочных приемов, часть из которых несовместима с современными операционными системами, а часть автоматически распознается современными же отладчиками и потому уже совершенно неактуальна.

Мыщъх поставил перед собой задачу: систематизировать всю имеющуюся информацию, протестировать каждый антиотладочный прием под десятком популярных отладчиков, показав каким образом и с помощью каких плагинов его можно обойти, как распознать эти плагины и нейтрализовать их. Вот такая рекурсивная тема получается: отладка -> анти-отладка -> анти-анти-отладка -> анти-анти-анти-отладка… И рекурсивный спуск на этом не останавливается, а продолжает падать вглубь — ведь количество приставок "анти-" ничем не ограничено!

Рисунок 1 мыщъх собственной персоной

боевой арсенал

В качестве базовой операционной системы для проведения экспериментов выбрана W2K SP0 и Knoppix 4.7 (Debian-based Linux с ядром 2.4.x). Отличия остальных осей будут упоминаться по ходу (если в этом возникнет необходимость).

Отладчики — самые последние на момент публикации _текущего_ выпуска "антиотладки", при этом мыщъх считает допустим использовать внутренние билды, не выложенные в паблик-доступ, естественно, явным образом оговаривая отличительные особенности их поведения (как правило, эти просто текущие фиксы ошибок, и в паблик они попадают вместе со следующим релизом).

Список подопытных отладчиков с их кратным описанием и указаниям версий приведен ниже:

Olly Debugger 1.10

Самый продвинутый ring-3 отладчик из всех имеющихся на сегодняшний день, к тому же бесплатный (в просторечии Ольга или Олли). Основное преимущество — огромное количество плагинов, способных решить практически любую задачу и обломать рога даже крутым защитам. Недостаток — "движок" отладчика работает через MS Debugging API,

страдающим кучей врожденных ограничений, оставляющим за собой множество трудноудаляемых следов и представляющим легкую мишень для анти-отладочных технологий, для борьбы с которыми приходится писать довольно сложные плагины, зачастую работающие на уровне нулевого кольца (т. е. устанавливающие свой собственный драйвер). Другой недостаток — графический интерфейс, причем часть действий выполняется _только_ мышью ненавистной хакерам старого поколения, предпочитающих консоль и клаву.

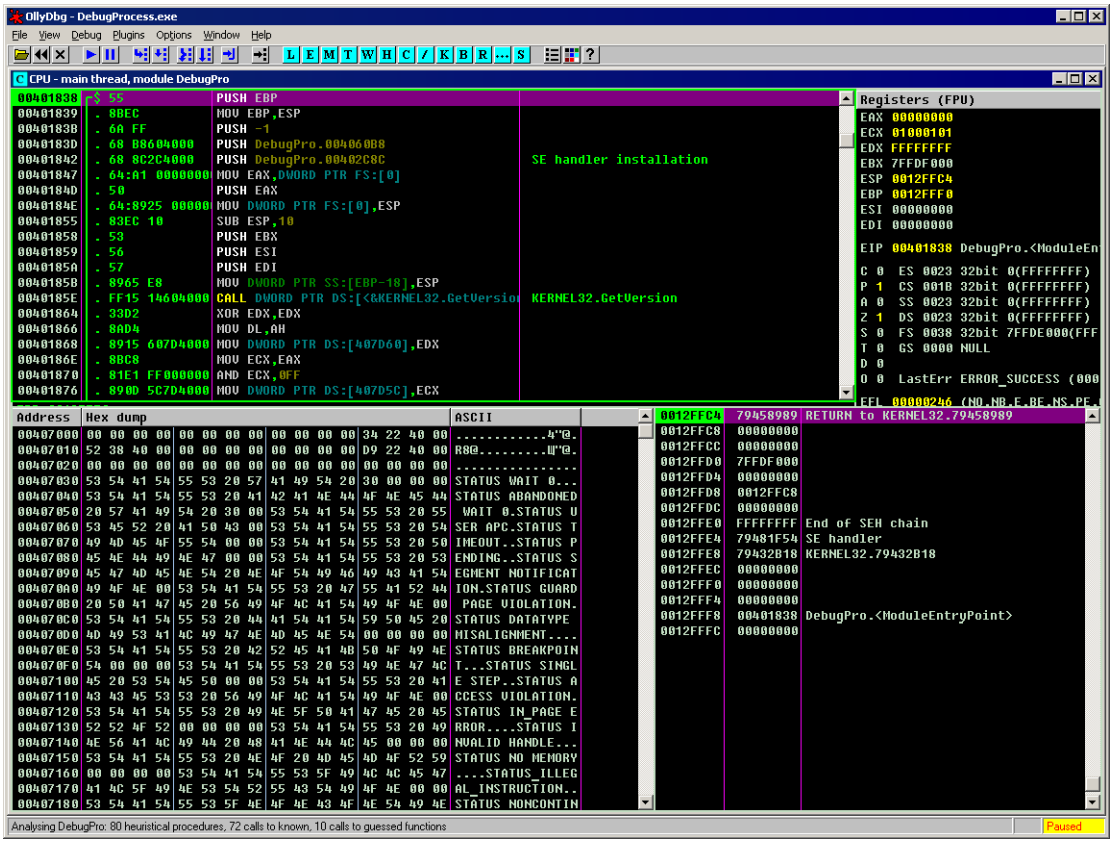

Рисунок 2 внешний вид Olly Debugger

Olly Debugger 2.00c pre-alpha 3

Экспериментальный отладчик с полностью переписанным debug engine и жестоко урезанным функционалом (по сравнению с версией 1.10). Тем не менее, debug engine по прежнему использует MS Debugging API и это по-прежнему ring-3 отладчик, со всеми вытекающими отсюда ограничениями.

IDA Pro Advanced 5.2

Включает в себя довольно примитивный ring-3 отладчик работающий через MS Debugging API (в NT) и через библиотеку ptrace (в UNIX), что делает ее легкой добычей для защитных механизмов, причем, готовых анти-антиоладочных плагинов под ИДУ раз два и обчелся, тем не менее, при наличии SDK, всегда можно написать свой собственный, только вместе с этим еще придется писать кучу недостающего функционала, уже реализованного у конкурентов. Пожалуй, единственное преимущество интегрированного отладчика — возможность отладки подопытного кода прямо "на месте" (just in the place), без выхода из дизассемблера. Поддерживаются как графические, так и консольные режимы (в UNIX – только консоль).

IDA Pro – коммерческий продукт, причем большинство "варезных" версий, гуляющих в сети, работают крайне нестабильно и постоянно падают, поэтому, имеет смысл остановится на бесплатной (и, естественно, нереально урезанной) версии 4.9.

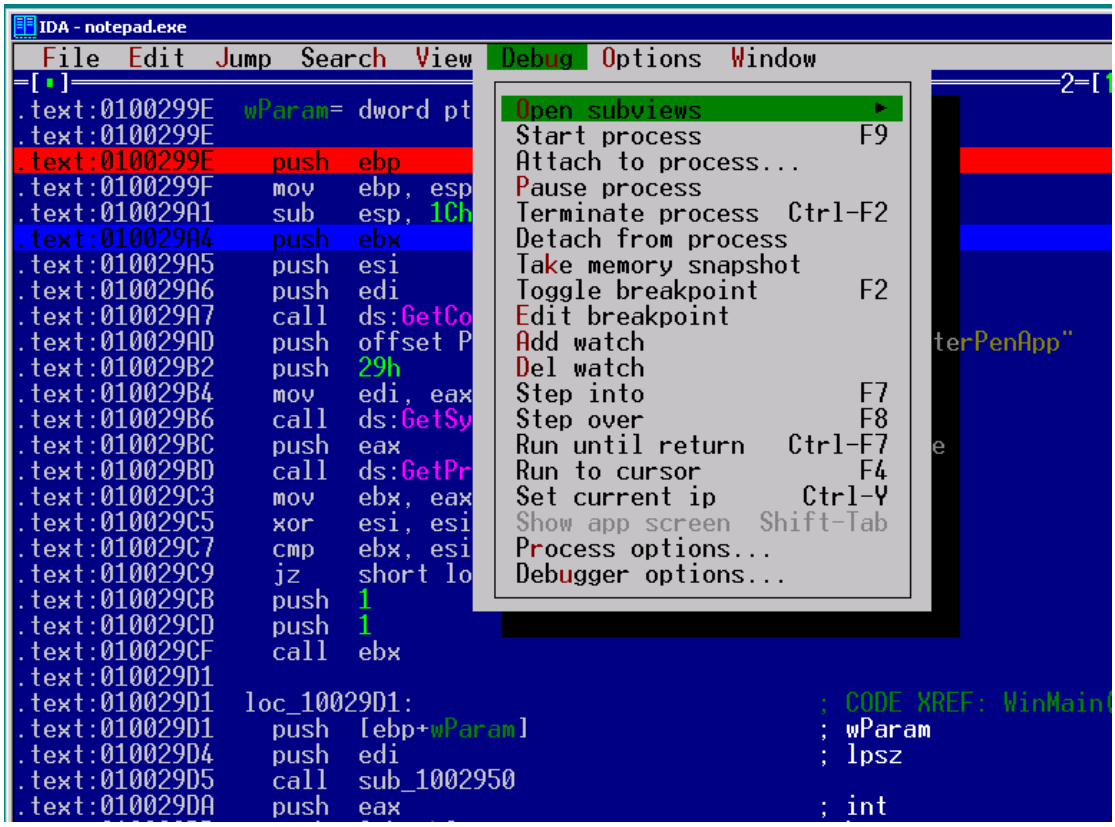

Рисунок 3 отладчик, интегрированный в IDA Pro (консольная редакция)

Microsoft Debugger 6.8.4.0

Входит в состав WDK (Windows Driver Kit — бывший Driver Development Kit или DDK), а так же в комплект Debugging Tools. Оба они бесплатны, но WDK намного больше по объему и требует предварительной регистрации для получения Windows Live ID (проверка валидности Windows при этом _не_ осуществляется), в то время как Debugging Tools раздается без регистрации вместе с SDK, в которую входит документация, заголовочные файлы, библиотеки и пара примеров как надо писать плагины. К сожалению, сторонних плагинов под Microsoft Debugger очень немного.

Microsoft Debugger может работать как в на прикладном уровне (ring-3), так и на уровне ядра. Вплоть до XP ядерная отладка требовала как минимум двух машин, соединенных COM-шнурком, но теперь достаточно и одной.

Поставляется в двух редакциях: windbg.exe – графический интерфейс и cdb.exe — интерфейс командой строки. Но все они являются лишь тонкими обертками вокруг dbgeng.dll, в которой, собственно, и реализован основной отладочный "движок", протокол обмена с которым документирован и потому dbgeng.dll можно использовать в качестве "фундамента" при написании универсальных распаковщиков исполняемых файлов (чтобы в очередной раз не писать трассер с нуля).

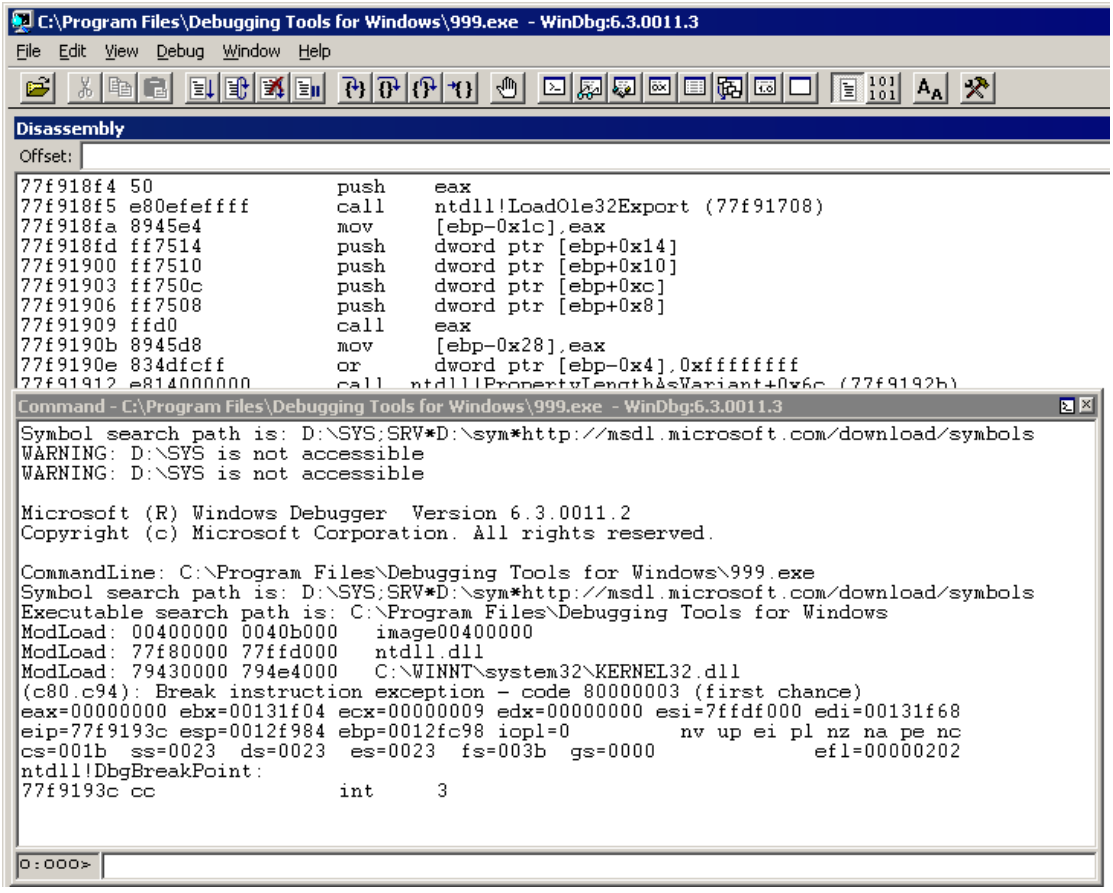

Рисунок 4 Microsoft Debugger (графическая версия)

Soft-Ice 2.6.0 (Build 336)

Легендарный отладчик ядерного уровня всех времен и народов. Работает в обход MS Debugging API, что значительно усложняет антиотладку, однако, учитывая, что для разработчиков защит soft-ice – враг номер один, практически все протекторы легко распознают присутствие soft-ice в системе и без специальных расширений (которые мы будем упоминать по ходу дела) никак не обойтись.

Обозначенная версия не является последней, но зато стабильной и хорошо совместимой с хакерскими плагинами, "вгрызающихся" в отладчик без всякого API (путем bit-hack'a). С более новыми версиями хакерские плагины несовместимы. С другой стороны, Soft-Ice поддерживает плагины, написанные для MS Debugger, а вот обратной совместимости, увы, не наблюдается.

В настоящее время поддержка soft-ice прекращена и продукт похоронен. Он еще совместим с XP и Server 2003 (хотя на многоядерных процессорах уже наблюдаются серьезные проблемы), но в долгосрочной перспективе soft-ice обречен и необходимо искать ему замену. Причем, чем скорее, тем лучше.

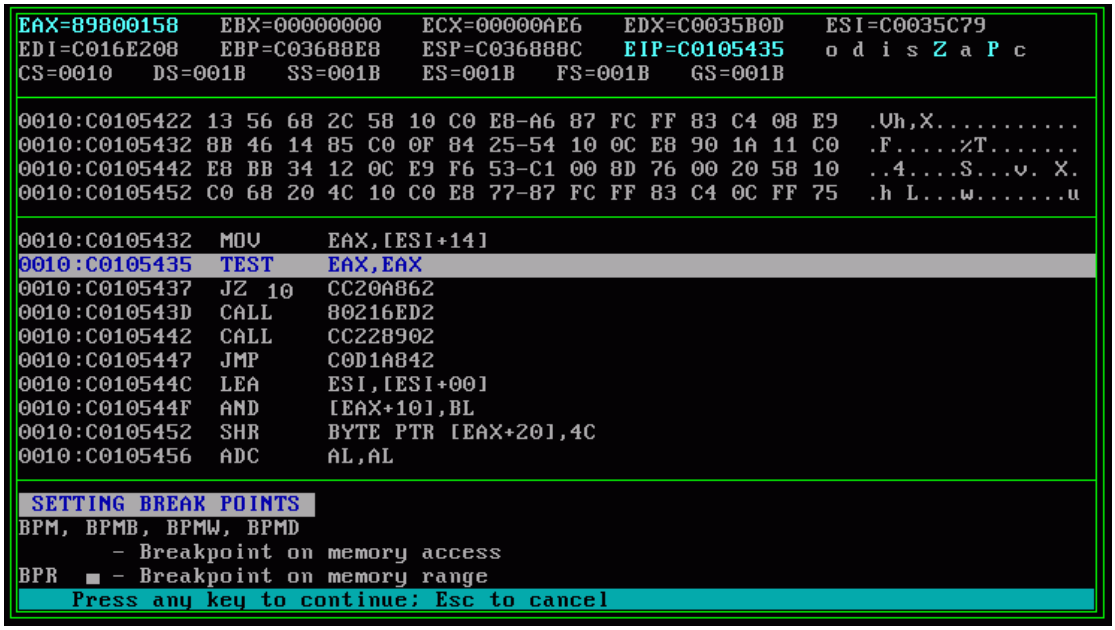

Рисунок 5 легендарный мягкий лед

>>> врезка знаете ли вы что…

…название "soft-ice" позаимствовано из фантастического романа Вильяма Гибсона "Нейроматик" (William Gibson: "Neuromantic"). В образе льда там выступали защитные механизмы, которые хакерам приходилось рубить, соответственно, soft-ice – дословно "мягкий лед" — легкий хакинг.

Syser 1.95.19000.0894

Достойная альтернатива умирающему soft-ice. Ядерный отладчик, поддерживающий многопроцессорные машины и всю линейку NT-подобных систем по Вислу включительно. Это коммерческий продукт, написанный двумя китайскими хакерами: Wu YanFeng и Chen JunHao, предоставляющими всего лишь семидневный бесплатный триал, что оскорбительно мало, однако, поскольку, мыщъх вливается в Syser team, то рассказывать о том, как ломать его — не собирается (хотя ломается он легко). С другой стороны, в настоящий момент готовится книжка "техника отладки II" с полной версий Syser'a на компакт диске, осталось лишь немного подождать, чтобы заполучить это чудо.

Нас ждет графический интерфейс к которому поначалу очень трудно привыкнуть, но в остальном — это все тот же самый soft-ice, во всяком случае с точки зрения синтаксиса команд. Другое преимущество — будучи в team'e мыщъх плотно работает вместе с разработчиками над усилением обороноспособности отладчика в смысле стойкости к антиотладке. Плюс возможность подключения внешних плагинов (правда, плагины для Syser'a мыщъху не известны, кроме пары штук, написанных им самим, да и то в порядке эксперимента).

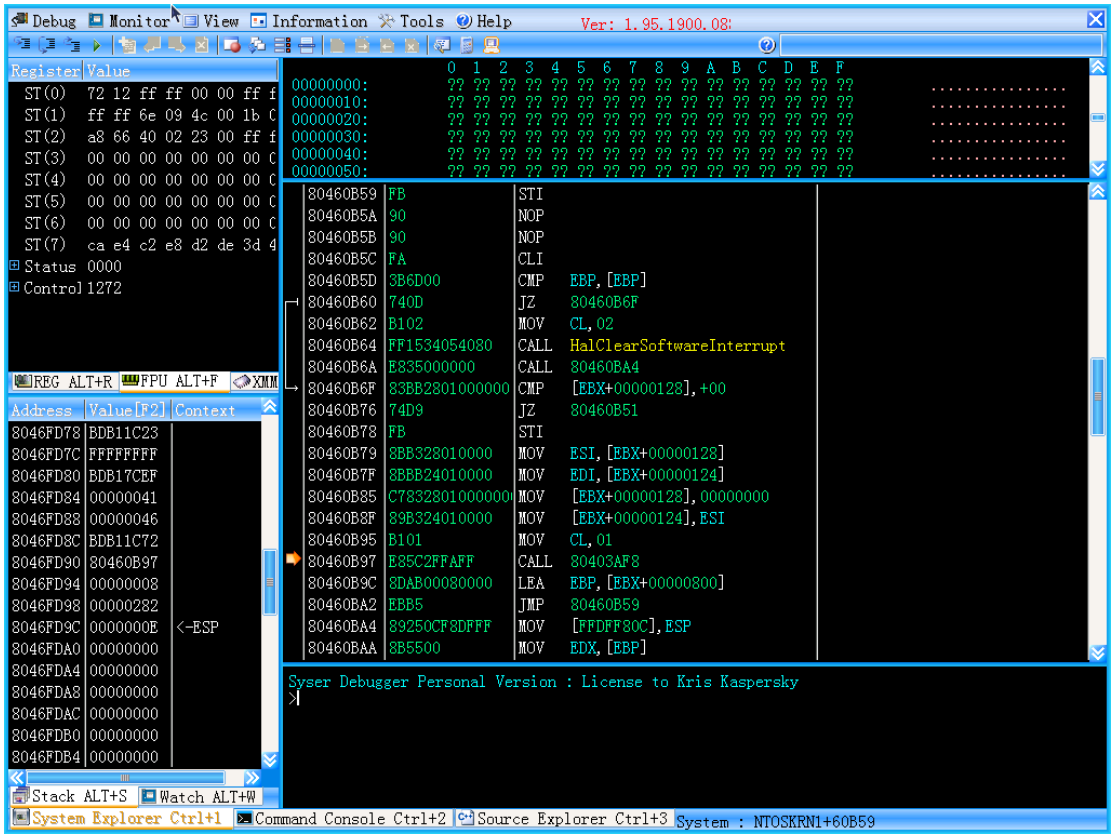

Рисунок 6 Syser за работой

GDB 6.1

GNU Debugger – основной отладчик под UNIX, ориентированный на совершенно иной тип мышления, чем все вышеперечисленные отладчики. Это не просто интерактивный отладчик, скорее, это станок с программным управлением, невероятно гибкий и мощный (в плане интерфейса). Отлаживать "честные" программы — одно удовольствие, а вот в плане анти-отладки GDB даже и не пытается сопротивляться и работает через библиотеку ptrace, которая на самом деле никакая не библиотека, а системный вызов. Но это не важно. Важно другое — GDB принципиально неспособен отлаживать программы, которые не хотят, чтобы их отлаживали. И такие программы мало-помалу уже начинают появляться (взять хотя бы упаковщик исполняемых файлов от Shiva).

Обозначенная версия GDB собрана в 2004 году и к новым билдам, очевидно, не относится, однако, поскольку, основной debug engine реализован не в GDB, а сосредоточен в ядре системы, то версия GDB решающего значения не имеет.

Естественно, помимо GDB существуют и другие отладчики, например, Lin-Ice, но… поскольку, антиотладочные технологии под UNIX только-только начинают развиваться, для наших экспериментов вполне сгодиться и GDB.

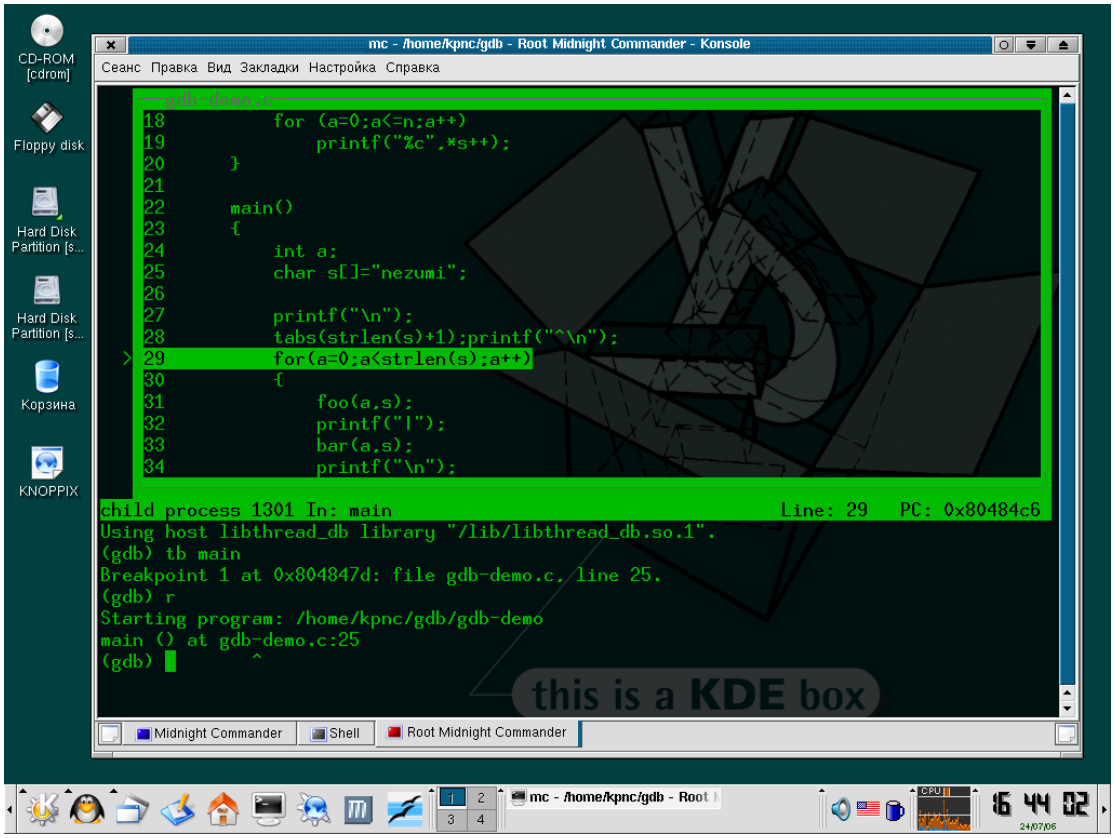

Рисунок 7 GDB (консольная версия с tui-интерфейсом)

>>> врезка знаете ли вы, что…

…ядро NT включает в себя интегрированный отладчик, способный устанавливать точки останова, вести мониторинг множества системных событий, причем с прикладного режима его активность запеленговать невозможно! Функции эти недокументированны, но открыто экспортируется ядром NTOSKRNL.EXE и начинаются с префикса Kd*. Их прототипы описаны в NTDDK, а в независимых ресурсах типа ReactOS, ORS.com, wine еще можно нарыть и краткое описание, что делает каждая из них. Стоит только начать курить в сторону KdEnableDebugger/KdDisableDebugger как все остальное приходит само.

>>> врезка знаете ли вы, что…

…для запуска soft-ice под VM Ware необходимо добавить в конфигурационный файл виртуальной машины (*.vmx) следующие строки (остальные отладчики запускаются на ней и без этого):

- svga.maxFullscreenRefreshTick = "2";
- vmmouse.present = "FALSE";
- paevm = TRUE;
- processor1.use = FALSE;

>>> врезка знаете ли вы, что…

…если soft-ice и Syser не запускаются, то причина, возможно, кроется в конфликте с драйвером stpd.sys, который устанавливает копировщик CD/DVD дисков Alcohol и его младший собрат Daemon Tools для предотвращения обнаружения виртуальных CD/DVD-дисков, создаваемых эмулятором, причем, поведение драйвера stpd.sys столь агрессивно, что отладчики с ним не живут и это никак не лечится — либо stpd.sys, либо отладчики, но никак не то и другое сразу!

>>> врезка быть или не быть

Категорически не рекомендуется использовать антиотладочные приемы в своих собственных программах (равно как и задействовать опции протектора, отвечающие за это), поскольку, "честных" антиотладочных приемов существует немного и все они легко обходятся отладчиками, а нечестные конфликтуют с операционной системой, различными сторожевыми программами, новыми типами процессоров и виртуальными машинами, в результате чего отдел поддержки взрывается тысячей звонков недовольных пользователей, что крайне отрицательно сказывается как на имидже фирме, так и на кривой продаж. А хакеры… ну взломают они программу не за час, так за полтора, пускай даже за неделю. Да, это задержит их, но какой ценой?!

>>> врезка ссылки на отладчики, упомянутые в статье

- **Olly-Debugger 1.10:**
  - http://www.ollydbg.de/odbg110.zip;
- **Olly-Debugger 2.00c pre-alpha 3:**
  - http://www.ollydbg.de/odbg200c.zip;
- **IDA Pro 5.2 (commercial_**:
  - http://www.datarescue.com/idabase;
- **IDA Pro 4.9 Freeware:**
  - http://www.hex-rays.com/idapro/idadownfreeware.htm;
- **Microsoft Debugging Tools for Windows:**
  - http://msdl.microsoft.com/download/symbols/debuggers/dbg_x86_6.8.4.0.msi;
- **Windows Driver Kit (WDK) для всех систем по Вислу включительно:**
  - http://www.microsoft.com/whdc/DevTools/default.mspx (требует регистрации);
- **Windows Server 2003 SP1 DDK:**
  - http://www.microsoft.com/whdc/devtools/ddk/default.mspx;
- **Soft-Ice**:
  - www.google.com ;-)
- **Syser 1.95.19000.0894**:
  - http://www.sysersoft.com/download/download.php;
- **GDB**:
  - http://sourceware.org/gdb/download/;