# Выявление вредоносного программного обеспечения, внедренного в ядро Linux

Выполнил: Михаил Клементьев
Руководитель: Роман Бажин, Digital Security

23 июня 2017 г.

Цель выпускной квалификационной работы – разработка методов выявления вредоносного программного обеспечения, внедренного в ядро Linux.

Цель выпускной квалификационной работы – разработка методов выявления вредоносного программного обеспечения, внедренного в ядро Linux.

Решаемые задачи:

Цель выпускной квалификационной работы – разработка методов выявления вредоносного программного обеспечения, внедренного в ядро Linux.

Решаемые задачи:

- Анализ существующих методов обнаружения руткитов;

Цель выпускной квалификационной работы – разработка методов выявления вредоносного программного обеспечения, внедренного в ядро Linux.

Решаемые задачи:

- Анализ существующих методов обнаружения руткитов;
- Разработка новых методов обнаружения руткитов.

# Проблема

- Руткит – это программа или набор программ для сокрытия следов присутствия злоумышленника

# Проблема

- Руткит – это программа или набор программ для сокрытия следов присутствия злоумышленника
  - Подмена системных файлов

# Проблема

- Руткит – это программа или набор программ для сокрытия следов присутствия злоумышленника
  - Подмена системных файлов
  - Изменение системных журналов

# Проблема

- Руткит – это программа или набор программ для сокрытия следов присутствия злоумышленника
  - Подмена системных файлов
  - Изменение системных журналов
  - Скрытие процессов ОС

# Проблема

- Руткит – это программа или набор программ для сокрытия следов присутствия злоумышленника
  - Подмена системных файлов
  - Изменение системных журналов
  - Скрытие процессов ОС
  - Скрытие сетевых соединений

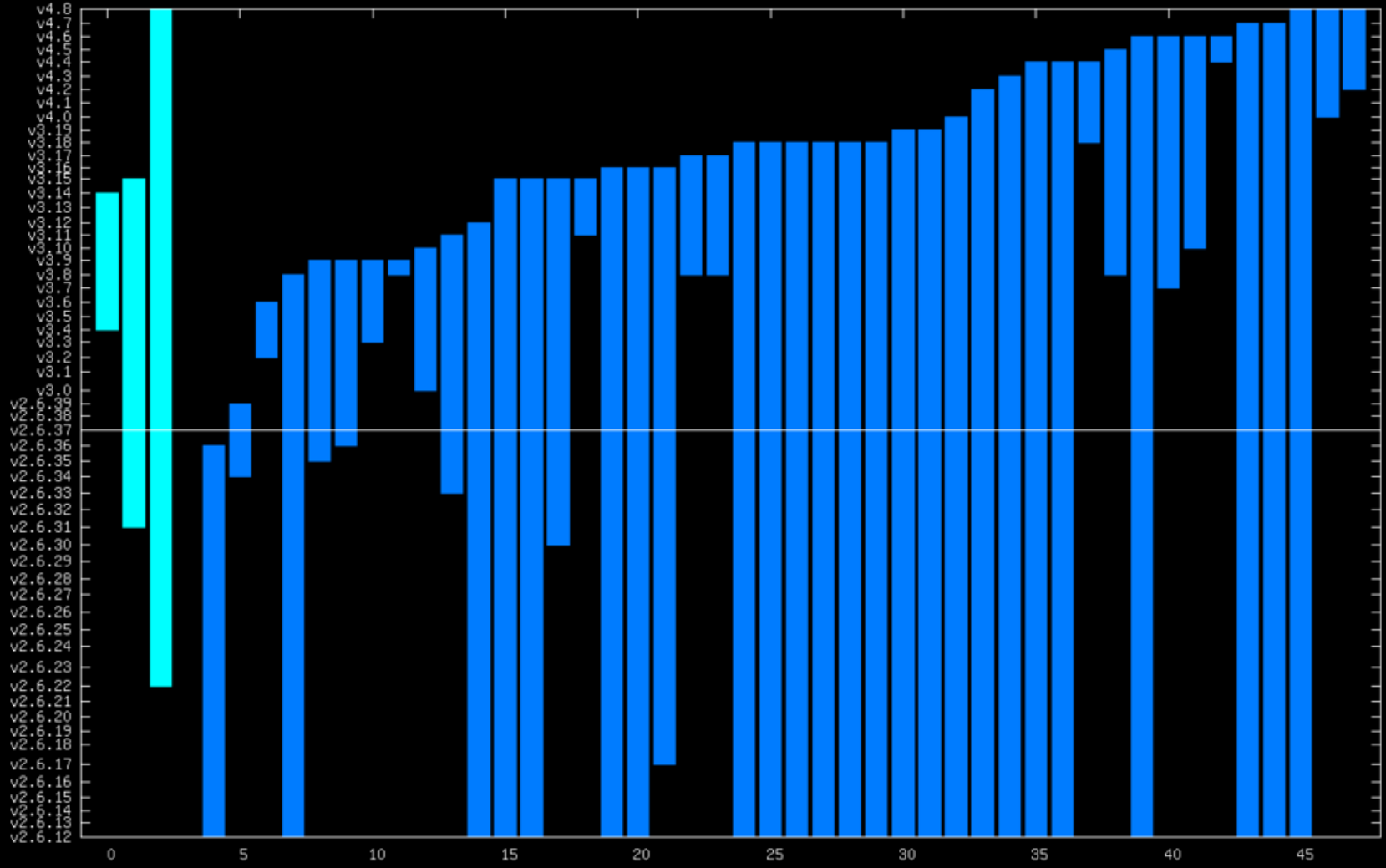
# Проблема

- Руткит – это программа или набор программ для сокрытия следов присутствия злоумышленника
  - Подмена системных файлов
  - Изменение системных журналов
  - Скрытие процессов ОС
  - Скрытие сетевых соединений
  - Скрытие объектов ФС

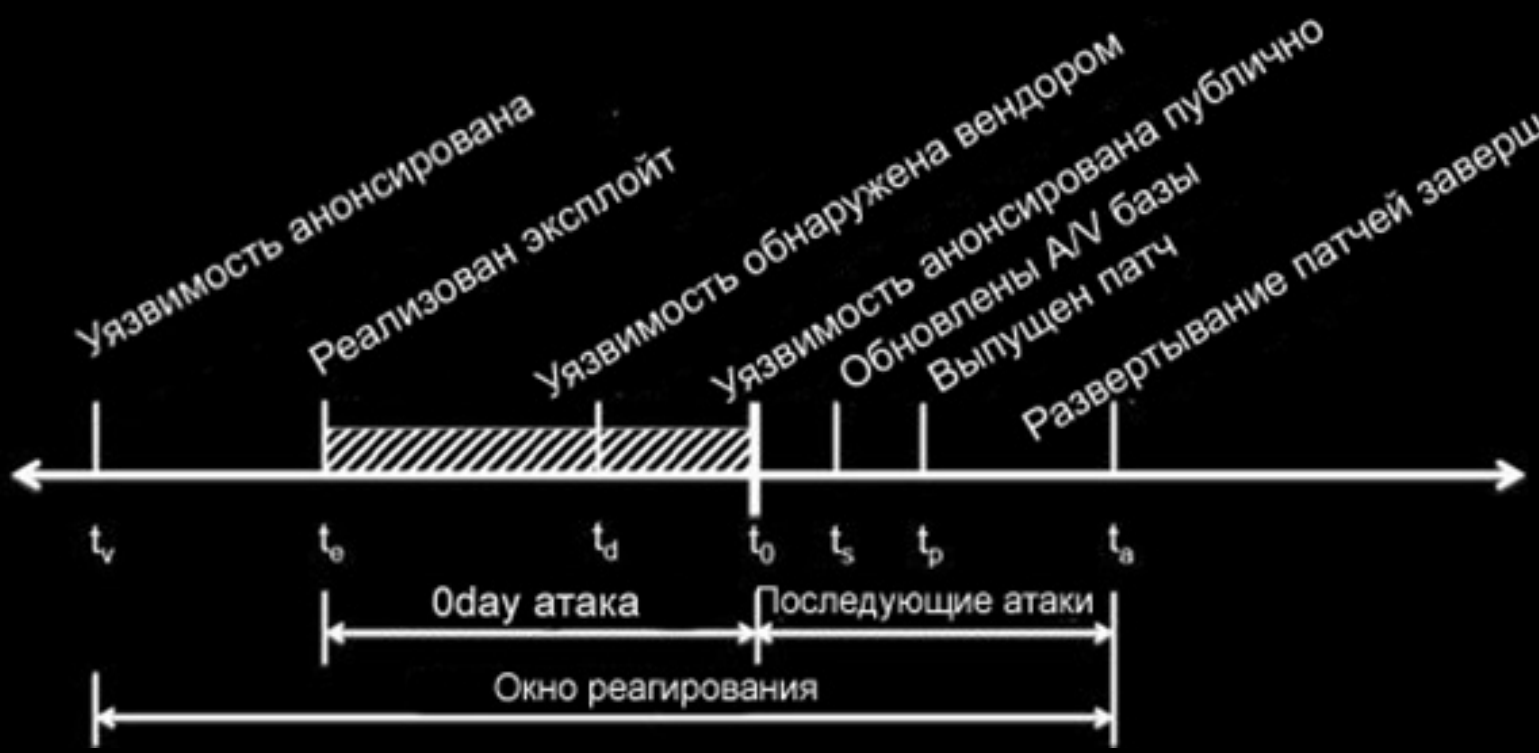
# Проблема

- Руткит – это программа или набор программ для сокрытия следов присутствия злоумышленника
  - Подмена системных файлов
  - Изменение системных журналов
  - Скрытие процессов ОС
  - Скрытие сетевых соединений
  - Скрытие объектов ФС
  - Защита от обнаружения

# Уязвимости ядра Linux



# Жизненный цикл уязвимости



# Существующие методы

- Поиск нарушений консистентности предоставляемой ядром информации

# Существующие методы

- Поиск нарушений консистентности предоставляемой ядром информации
- Поиск конкретных файлов известных руткитов

# Существующие методы

- Поиск нарушений консистентности предоставляемой ядром информации
- Поиск конкретных файлов известных руткитов
- Проверка целостности

# Существующие методы

- Поиск нарушений консистентности предоставляемой ядром информации
- Поиск конкретных файлов известных руткитов
- Проверка целостности
- Перебор идентификаторов процесса

# Существующие методы

- Поиск нарушений консистентности предоставляемой ядром информации
- Поиск конкретных файлов известных руткитов
- Проверка целостности
- Перебор идентификаторов процесса
- Исследование памяти

# Недостатки существующего программное обеспечение

- Устаревшие индикаторы компрометации

# Недостатки существующего программное обеспечение

- Устаревшие индикаторы компрометации
- Все поддерживаемые средства работают в пространстве пользователя

# Недостатки существующего программное обеспечение

- Устаревшие индикаторы компрометации
- Все поддерживаемые средства работают в пространстве пользователя
- Небольшое покрытие версий ядра в случае реализации со стороны ядра

# Недостатки существующего программное обеспечение

- Устаревшие индикаторы компрометации
- Все поддерживаемые средства работают в пространстве пользователя
- Небольшое покрытие версий ядра в случае реализации со стороны ядра
- Почти не развиваются

# Недостатки существующего программное обеспечение

- Устаревшие индикаторы компрометации
- Все поддерживаемые средства работают в пространстве пользователя
- Небольшое покрытие версий ядра в случае реализации со стороны ядра
- Почти не развиваются
- Не учитывают противодействие со стороны вредоносного ПО

# Недостатки существующего программное обеспечение

- Устаревшие индикаторы компрометации
- Все поддерживаемые средства работают в пространстве пользователя
- Небольшое покрытие версий ядра в случае реализации со стороны ядра
- Почти не развиваются
- Не учитывают противодействие со стороны вредоносного ПО
- Почти не применимы в противодействии реальному вредоносному ПО

# Сформированные требования

- Работа в пространстве ядра

# Сформированные требования

- Работа в пространстве ядра
- Только детерминированные методы

# Сформированные требования

- Работа в пространстве ядра
- Только детерминированные методы
- Без индикаторов компрометации

# Сформированные требования

- Работа в пространстве ядра
- Только детерминированные методы
- Без индикаторов компрометации
- Выявление исходя из действий:

# Сформированные требования

- Работа в пространстве ядра
- Только детерминированные методы
- Без индикаторов компрометации
- Выявление исходя из действий:
  - Планировщик процессов

# Сформированные требования

- Работа в пространстве ядра
- Только детерминированные методы
- Без индикаторов компрометации
- Выявление исходя из действий:
  - Планировщик процессов
  - Сетевой стек

# Сформированные требования

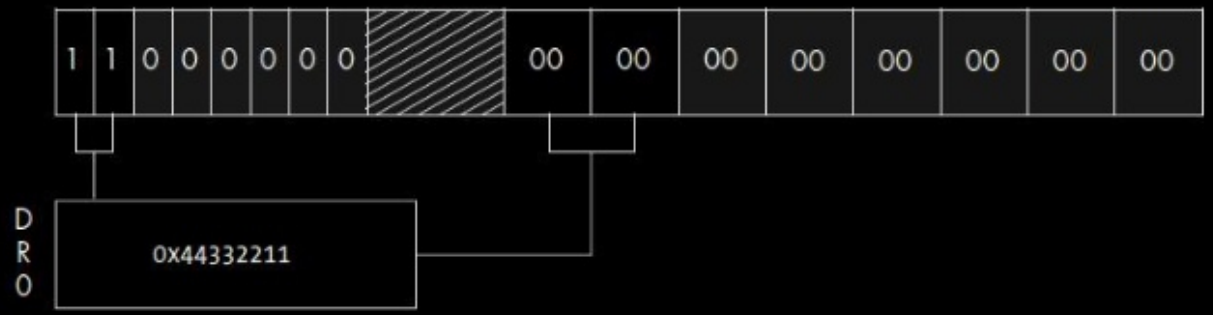
- Работа в пространстве ядра
- Только детерминированные методы
- Без индикаторов компрометации
- Выявление исходя из действий:
  - Планировщик процессов
  - Сетевой стек
  - Файловые системы

# Реализация: аппаратные точки останова

Layout of DR7 Register

| | L DR0 | G DR0 | L DR1 | G DR1 | L DR2 | G DR2 | L DR3 | G DR3 | | Type DR0 | Len DR0 | Type DR1 | Len DR1 | Type DR2 | Len DR2 | Type DR3 | Len DR3 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Bits | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 – 15 | 16 17 | 18 19 | 20 21 | 22 23 | 24 25 | 26 27 | 28 29 | 30 31 |

DR7 with 1-byte Execution Breakpoint Set at 0x44332211




DR7 with Additional 2-byte Read/Write Breakpoint at 0x55667788

# Экспериментальные исследования

- Запуск руткита на целевой системе

# Экспериментальные исследования

- Запуск руткита на целевой системе
- Настройка руткита с целью скрытия процессов, файлов и сетевых соединений

# Экспериментальные исследования

- Запуск руткита на целевой системе
- Настройка руткита с целью скрытия процессов, файлов и сетевых соединений
- Запуск антируткита на целевой системе

# Экспериментальные исследования

- Запуск руткита на целевой системе
- Настройка руткита с целью скрытия процессов, файлов и сетевых соединений
- Запуск антируткита на целевой системе
- Анализ отчета сервисной утилиты

# Результаты экспериментального исследования

Обнаружение всех доступных для исследования руткитов

# Результаты экспериментального исследования

Обнаружение всех доступных для исследования руткитов

Успешно обнаруживает:

# Результаты экспериментального исследования

Обнаружение всех доступных для исследования руткитов

Успешно обнаруживает:

- Diamorphine;

# Результаты экспериментального исследования

Обнаружение всех доступных для исследования руткитов

Успешно обнаруживает:

- Diamorphine;
- ivyl rootkit;

# Результаты экспериментального исследования

Обнаружение всех доступных для исследования руткитов

Успешно обнаруживает:

- Diamorphine;
- ivyl rootkit;
- nurupo rootkit;

# Результаты экспериментального исследования

Обнаружение всех доступных для исследования руткитов

Успешно обнаруживает:

- Diamorphine;
- ivyl rootkit;
- nurupo rootkit;
- NoviceLive research-rootkit;

# Результаты экспериментального исследования

Обнаружение всех доступных для исследования руткитов

Успешно обнаруживает:

- Diamorphine;
- ivyl rootkit;
- nurupo rootkit;
- NoviceLive research-rootkit;
- И другие.

# Демонстрация

# Результаты ВКР

- Разработаны эффективные методы обнаружения руткитов

# Результаты ВКР

- Разработаны эффективные методы обнаружения руткитов
- Программная реализация методов показывает работоспособность в реальной среде

# Результаты ВКР

- Разработаны эффективные методы обнаружения руткитов
- Программная реализация методов показывает работоспособность в реальной среде
- По теме ВКР

# Результаты ВКР

- Разработаны эффективные методы обнаружения руткитов
- Программная реализация методов показывает работоспособность в реальной среде
- По теме ВКР
  - Выступления на DEFCON Russia и SECON 2017

# Результаты ВКР

- Разработаны эффективные методы обнаружения руткитов
- Программная реализация методов показывает работоспособность в реальной среде
- По теме ВКР
  - Выступления на DEFCON Russia и SECON 2017
  - Статья в сборнике трудов конференции ПАУТС 2017

# Результаты ВКР

- Разработаны эффективные методы обнаружения руткитов
- Программная реализация методов показывает работоспособность в реальной среде
- По теме ВКР
  - Выступления на DEFCON Russia и SECON 2017
  - Статья в сборнике трудов конференции ПАУТС 2017
  - Акт о внедрении результатов исследования

# Выявление вредоносного программного обеспечения, внедренного в ядро Linux

Выполнил: Михаил Клементьев
Руководитель: Роман Бажин, Digital Security

23 июня 2017 г.