Министерство образования и науки Российской Федерации

Санкт-Петербургский Политехнический Университет Петра Великого

—

Институт компьютерных наук и кибербезопасности

ЛАБОРАТОРНАЯ РАБОТА № 4

«Исследование принципов функционирования сетевых компонентов операционной системы Microsoft Windows с использованием методов обратной разработки»

1. по дисциплине «Технологии реверс-инжиниринга программного обеспечения»
2. Выполнил
3. студент гр. 5151004/10101 Веремейчук Я.Ю.

<подпись>

1. Проверил
2. преподаватель Овасапян Т.Д.

<подпись>

1. Санкт-Петербург
2. 2023
3. Цель работы

Практическое освоение методов обратной разработки системного программного обеспечения и изучение принципов функционирования сетевых компонентов операционной системы.

1. Ход работы

IKEEXT – это служба Windows, которая предоставляет услуги обмена ключами Интернета (IKE) и IPSec. Он используется для создания безопасных соединений между двумя компьютерами через Интернет. Это важный компонент операционной системы Windows и необходим для безопасной связи между двумя компьютерами.

Служба IKEEXT отвечает за согласование и установление безопасных соединений между двумя компьютерами. Она используется для аутентификации двух компьютеров и шифрования данных, которые передаются между ними. Она также используется для проверки подлинности двух компьютеров и для обеспечения того, чтобы данные не были подделаны во время передачи.

Основные шаги, описывающие общий принцип работы службы IKEEXT:

1. Инициация соединения. Когда два узла (например, компьютеры или устройства) решают установить безопасное соединение, они сначала инициируют процесс обмена ключами.
2. Предложение параметров. Каждый узел отправляет предложение с параметрами безопасности, такими как методы шифрования, методы аутентификации и другие параметры.
3. Переговоры и выбор параметров. Узлы взаимодействуют, согласовывают и выбирают общие параметры для безопасного соединения. Это включает в себя выбор алгоритмов шифрования, аутентификации и обмена ключами.
4. Обмен ключами. С использованием протокола обмена ключами, обычно IKE (Internet Key Exchange), узлы генерируют общий секретный ключ, который будет использоваться для шифрования данных во время передачи.
5. Установка безопасного соединения. После успешного обмена ключами узлы могут установить безопасное соединение, используя общий ключ для шифрования и аутентификации данных.
6. Управление и обслуживание. IKEEXT заботится об управлении ключами, обновлении параметров безопасности и обслуживании безопасных соединений в процессе их использования.

Процесс svchost.exe -k netsvcs -p -s IKEEXT:

-k netsvcs: svchost.exe выполняет несколько служб, связанных с сетевыми сервисами "netsvcs" (Network Services).

-p: svchost.exe должен создавать новый процесс для каждой группы служб. Это улучшает стабильность, так как одна служба, вызывающая ошибку, не повлияет на другие службы, выполняемые в других процессах.

-s IKEEXT: среди служб, управляемых данным экземпляром svchost.exe, присутствует служба с(Internet Key Exchange).

Была произведена проверка в “Службах”, работает ли IKEEXT.

Изображение выглядит как текст, электроника, снимок экрана, программное обеспечение

Автоматически созданное описание

Рисунок – Служба выполняется

Был использован Process Hacker для поиска сетевого порта, который используется системой для определенной службы. Осуществлен поиск по названию службы и найдены процессы, которые связаны с ней.

Изображение выглядит как текст, снимок экрана, программное обеспечение

Автоматически созданное описание

Рисунок – Поиск процесса

Изображение выглядит как текст, снимок экрана, число, программное обеспечение

Автоматически созданное описание

Рисунок – Свойства модуля IKEEXT.DLL

Изображение выглядит как текст, число, Шрифт, программное обеспечение

Автоматически созданное описание

Рисунок – Используемая память

Информация о службе во вкладке “Services” процесса svchost.exe:

Служба IKEEXT содержит модули для работы с ключами в Интернете (IKE) и по протоколу IP с проверкой подлинности (AuthIP). Эти модули для работы с ключами используются при проверке подлинности и обмене ключами в протоколе безопасности IP (IPsec). Остановка или отключение службы IKEEXT ведет к отключению обмена ключами IKE и AuthIP с другими компьютерами. Как правило, IPsec настроен на использование IKE или AuthIP; таким образом, остановка или отключение службы IKEEXT может привести к сбою в работе IPsec и поставить под угрозу безопасность системы. Настоятельно рекомендуется, чтобы служба IKEEXT была включена.

Были найдены зависимости службы IKEEXT.

Изображение выглядит как текст, снимок экрана, программное обеспечение, веб-страница

Автоматически созданное описание

Рисунок – Службы, от которых зависит служба IKEEXT

А также сервис, зависящий от IKEEXT.

Изображение выглядит как текст, снимок экрана, программное обеспечение, Значок на компьютере

Автоматически созданное описание

Рисунок – Служба, которая зависит от IKEEXT

Во вкладке Network были найдены порты, используемые в системе исследуемой службой: 500 и 4500.

Изображение выглядит как текст, снимок экрана, Шрифт, число

Автоматически созданное описание

Рисунок – Порты службы IKEEXT

Затем был произведен поиск информации об известных уязвимостях рассматриваемого сервиса.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **№** | **Тип уязвимости** | **Уязвимые компоненты** | **Описание уязвимости** | **Идентификатор уязвимости (CVE) и исправления (MSXX-012)** | **Ссылки** |
| 1 | DLL-инъекция и эксплуатация службы IKEEXT | Служба IKEEXT (IKE and AuthIP IPsec Keyring Modules) в операционных системах Windows Vista, 7, 8, Server 2008, Server 2008 R2 и Server 2012. | Уязвимость заключается в недостаточной проверке безопасности в службе IKEEXT, которая позволяет аутентифицированным пользователям в определенных условиях повысить свои привилегии до системных. Проблема связана с попыткой службой загрузить DLL-файл (wlbsctrl.dll), отсутствующий в системе. Если одна из папок в переменной среды PATH настроена с недостаточными правами, злоумышленник может внедрить зловредный DLL, что позволит выполнить код от имени системы. | Уязвимость не имеет явного идентификатора CVE в предоставленной информации. Важно отметить, что, согласно тексту, уязвимость была закрыта в Windows 8.1 и более новых версиях. Таким образом, пользователи рекомендуются перейти на более новые версии операционной системы, где проблема была устранена. | <https://github.com/securycore/Ikeext-Privesc>  <https://xploitlab.com/ikeext-privesc-windows-dll-hijacking-and-exploit-tool/>  <https://infosecwriteups.com/ikeext-dll-hijacking-3aefe4dde7f5> |

Был проведен анализ кода IKEEXT.DLL с помощью IDA Pro. Необходимо найти этот файл на виртуальной машине и перенести его на хост. И открыть его на IDA на хосте.

В импортируемых функциях были найдены функции, которые осуществляют принятие сетевых пакетов.

Изображение выглядит как текст, снимок экрана, Шрифт, число

Автоматически созданное описание

Рисунок – Функции работы с пакетами

Изображение выглядит как текст, снимок экрана, Шрифт, программное обеспечение

Автоматически созданное описание

Рисунок – Функции работы с пакетами

Нажав “X”, можно получить список функций, из которых вызывается искомая функция.

Изображение выглядит как текст, снимок экрана, программное обеспечение, Шрифт

Автоматически созданное описание

Рисунок – Функции, из которых вызывается функция \_\_imp\_WSAStartup

Изображение выглядит как текст, электроника, снимок экрана, дисплей

Автоматически созданное описание

Рисунок – Часть кода функции IkeInitSockets, которая вызывает \_\_imp\_WSAStartup

Нажав F5, можно перейти к псевдокоду функции.

Изображение выглядит как текст, Шрифт, линия, число

Автоматически созданное описание

Рисунок – Псевдокод

Для дальнейшей работы необходимо спинговать хост и гостевую систему. Сначала пинг не получалось сделать. На обеих системах был отключен брандмауэр.

Изображение выглядит как текст, снимок экрана, программное обеспечение, веб-страница

Автоматически созданное описание

Рисунок – Отключение брандмауэра на виртуальной машине

Изображение выглядит как текст, программное обеспечение, Шрифт, веб-страница

Автоматически созданное описание

Рисунок – Отключение брандмауэра на хосте

Но это не помогало. Были изменены настройки сети на виртуальной машине.

Изображение выглядит как текст, снимок экрана, программное обеспечение, Мультимедийное программное обеспечение

Автоматически созданное описание

Рисунок – Настройка сети

Изображение выглядит как текст, снимок экрана, Веб-сайт, веб-страница

Автоматически созданное описание

Рисунок – Изменившиеся настройки сети виртуальной машины

Теперь системы пингуются.

Изображение выглядит как текст, снимок экрана, Шрифт

Автоматически созданное описание

Рисунок – Успешный пинг

Далее необходимо запустить отладочный сервер win64\_remote64.exe (IDA\dbgsrv\). Для этого необходимо установить PsExec64.exe на гостевую систему.

Изображение выглядит как текст, снимок экрана, Шрифт

Автоматически созданное описание

Рисунок – Запуск отладочного сервера win64\_remote64.exe на виртуальной машине

Далее на хосте необходимо запустить IDA Pro (в режиме “Go”).

Изображение выглядит как текст, электроника, снимок экрана, программное обеспечение

Автоматически созданное описание

Рисунок – Выбор необходимой опции

Далее необходимо задать IP-адрес виртуальной машины.

Изображение выглядит как текст, снимок экрана, дисплей, Шрифт

Автоматически созданное описание

Необходимо проверить, что на гостевой системе служба запущена, и найти ID процесса (432 в данном случае).

Изображение выглядит как текст, снимок экрана, программное обеспечение, число

Автоматически созданное описание

Рисунок – Служба работает

Далее на хосте можно также увидеть этот процесс с ID 432.

Изображение выглядит как текст, электроника, снимок экрана, программное обеспечение

Автоматически созданное описание

Рисунок – Поиск рассматриваемого процесса

Дважды нажав на процесс, можно подключиться к нему.

Изображение выглядит как текст, снимок экрана, программное обеспечение, Значок на компьютере

Автоматически созданное описание

Рисунок – Подключение к процессу (на точке останова)

Для того чтобы в отладке найти вызов функции \_\_imp\_WSAStartup, необходимо правильно рассчитать ее адрес. Так как база отлаживаемой программы не совпадает с базой программы в статике, необходимо к базе в отладке прибавить смещение в статике.

Необходимо в Модулях найти рассматриваемую DLL и увидеть там базовый адрес.

Изображение выглядит как текст, снимок экрана, программное обеспечение, число

Автоматически созданное описание

Рисунок – Поиск базового адреса

Далее в IDA, куда загружалась DLL, необходимо перейти к функции, которая была найдена на этапе Рисунок 10. Отобразив код в текстовом формате (необходимо правой кнопкой мыши нажать на пустое поле и выбрать соответствующее отображение), необходимо скопировать оффсет (адрес функции, не зависящий от базового адреса 0x0000000180000000).

Изображение выглядит как текст, снимок экрана, Шрифт, линия

Автоматически созданное описание

Рисунок – Оффсет

Далее на IDA-отладчике (который подключался к процессу на виртуальной машине) необходимо нажать “G”, ввести базовый адрес + адрес оффсета.

Изображение выглядит как текст, снимок экрана, программное обеспечение, дисплей

Автоматически созданное описание

Рисунок – Прыжок

Далее будет совершен прыжок на полученный адрес.

Изображение выглядит как текст, снимок экрана, программное обеспечение, дисплей

Автоматически созданное описание

Рисунок – Прыжок на полученный адрес

Нажав на 48h, а затем на клавишу “C”, можно будет увидеть искомую команду call. Остальные команды также должны совпадать со статиком.

Изображение выглядит как текст, снимок экрана, программное обеспечение, число

Автоматически созданное описание

Рисунок – Сравнение кода

Далее необходимо установить ncat на хост. С помощью него можно подключаться к службе и посылать сообщения. Так как служба IKEEXT работает по протоколу UDP, необходим флаг -u для работы ncat (для служб с протоколом TCP флаги не нужны).

Также были рассмотрены и другие функции, например, использующие библиотеку cryptsp.dll. Cryptsp.dll (Cryptographic Service Provider API) – это библиотека динамической загрузки (DLL) в операционной системе Windows, отвечающая за криптографические функции и службы. Она предоставляет интерфейс для криптографических провайдеров (CSP), которые, в свою очередь, предоставляют реализацию криптографических алгоритмов для шифрования, подписи, хэширования и других операций безопасности.

Изображение выглядит как текст, снимок экрана, Шрифт, число

Автоматически созданное описание

Рисунок – Функции cryptsp.dll

Изображение выглядит как текст, снимок экрана, Шрифт, документ

Автоматически созданное описание

Рисунок – Функции cryptsp.dll

Изображение выглядит как текст, снимок экрана, линия, диаграмма

Автоматически созданное описание

Рисунок – Переход к функции

Можно заметить, что для шифрования используется алгоритм RSA.

Изображение выглядит как текст, электроника, снимок экрана, программное обеспечение

Автоматически созданное описание

Рисунок – Использование функции

Как было выяснено выше, данный сервис зависит от сервиса nsi. Эта служба отправляет сетевые уведомления (например, о добавлении или удалении интерфейса и т. п.) клиентам пользовательских режимов. Остановка этой службы вызовет отключение от сети. Если данная служба отключена, все явно зависящие от нее службы запустить не удастся.

Поэтому в коде IKEEXT.DLL были найдены компоненты, участвующие в обработке сетевых данных.

Изображение выглядит как текст, линия, Шрифт, число

Автоматически созданное описание

Рисунок – Компоненты, участвующие в обработке сетевых данных

Функция NsiGetParameter используется для получения значений сетевых параметров. Когда вызывается NsiGetParameter, она запросит значение определенного параметра сети. Эти параметры могут включать в себя информацию о сетевых интерфейсах, конфигурации IP, статусе соединения и других аспектах сетевой конфигурации.

Функция NsiSetParameter, напротив, предназначена для установки значений сетевых параметров. Она позволяет изменять конфигурацию сетевых параметров в соответствии с требованиями. Например, это может быть использовано для изменения IP-адреса или других параметров настройки сетевого интерфейса.

Изображение выглядит как текст, снимок экрана, Шрифт, линия

Автоматически созданное описание

Рисунок – Вызов функции NsiGetParameter

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| № | Исполняемый файл | Функция | Вызывается из… | Вызывает… |
| 1 | Модули ключей IPsec для обмена ключами в Интернете и протокола IP с проверкой подлинности | Используются при проверке подлинности и обмене ключами в протоколе безопасности IP (IPsec). | При загрузке системы | svchost.exe  IKEEXT.DLL |
| 2 | svchost.exe | Обеспечивает многопоточность и изоляцию служб | IKEEXT | - |
| 3 | IKEEXT.DLL | Функциональность, связанную с расширением протокола IKE в контексте IPsec. | IKEEXT | BFE  nsi |

1. Выводы

В ходе работы были освоены методы обратной разработки системного программного обеспечения и изучены принципы функционирования сетевых компонентов операционной системы.