Министерство образования Республики Беларусь

Учреждение образования

«Брестский государственный технический университет»

Кафедра ИИТ

Лабораторная работа №4

По дисциплине: «Безопасность компьютерных систем и сетей»

Тема: «Работа с антивирусными программами»

Выполнил:

Студент 4 курса

Группы ПО-7

Комиссаров А.Е.

Проверил:

Самолюк О.Ю.

2023

**Цель работы:** работа с антивирусными программами

1. Создать 2 виртуальные машины с ОС Windows и ОС Linux
2. Заразить обе системы вирусным ПО.

Ход работы:

Заражать будем виртуальные машины VirtualBox на Windows 7, Windows 10 и Ubuntu. После заражения некоторыми вирусами требуется откат до прошлого состояния из-за отсутствия возможности исцеления (потеря управления).

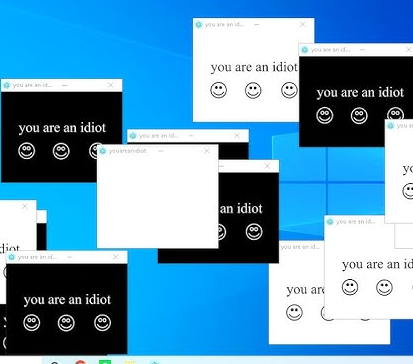
1. Начнём с установки вируса Coffin32. Данный вирус является отсылкой на известный мем где скачут парни из африки вместе с гробом в руках, при этом экран становится разноцветным и мышь тоже скачет в разные стороны под каждый прыжок гроба.



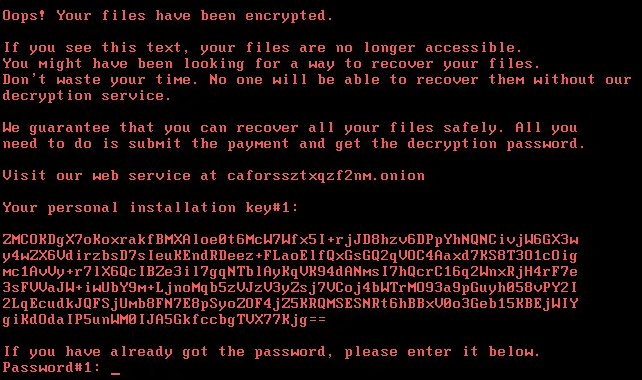
1. Следующим возьмём вирус WannaCry, нашумевший в 2017 году который заразил порядка 300 тысяч компьютеров по всему миру. Вирус распространялся автоматически, используя эксплоит EternalBlue. Файлы компьютера кодируются и вирус просит денег за разблокировку.



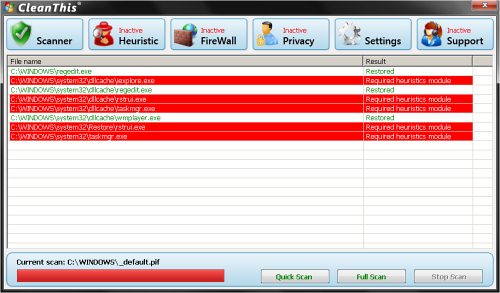
3. Возьмём вирус YouAreAnIdiot, что переводится буквально как ВыИдиОт. При запуске вируса появляется окно с трёмя смайликами и играет музыка. Если попытаться закрыть окно вирус открывает новые окна и делает это пока не истратит все ресурсы системы. После перезагрузки вирус пропадает



4. BadRabbit.exe. Данный вирус также шифрует все данные в системе и просит оплаты криптовалютой на кошелёк мошенника, при этом также распространяясь по локальной сети перехватывая логины и пароли админ-пользователей используя эксплоиты ОС Windows.



5. CleanThis.exe. Этот вирус выглядит как безобидная программа-очиститель ненужных файлов по типу CCleaner, однако после запуска компьютер начинает жить своей жизнью. Сам запускает программы, удаляет файлы, драйвера и так далее.



**Вирусы на Linux**

Вирусы на таких системах тоже существуют. Например, каждый раз когда происходит взлом какого-либо сайта, скорее всего был запущен вирус в Linux-систему так как веб-сервера работают преимущественно на таких ОС. Также можно взять Mirai ботнет, который заразил в 2016 году порядка 150 тысяч компьютеров, в основном используя в качестве жертв IoT-сектор. Были заражены холодильники, кофемашины, роутеры, камеры и другие вещи использующие интернет и запущенные на Linux – подобных системах.

1. ZipWorm.zip. Безобидный Linux-вирус, добавляющий свои копии к ZIP-архивам. Заражает архивы только в текущем каталоге. При заражении вирус не использует внешние утилиты работы с ZIP-файлами, а самостоятельно обрабатывает внутренний формат архива. Копии вируса в архивах имеют одно из пяти возможных имен:

Ten motives why linux sux!

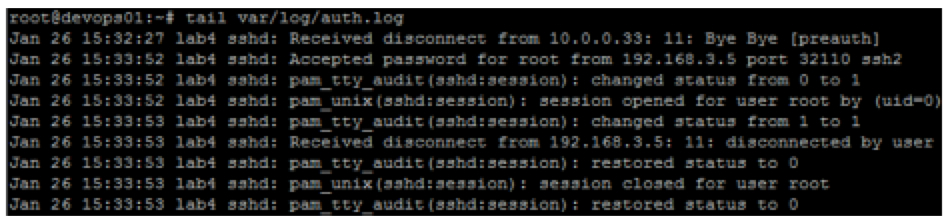
Why Windows is superior to Linux!

Is Linux for you? Never!

Is Linux immune to virus? NO!

zipworm!

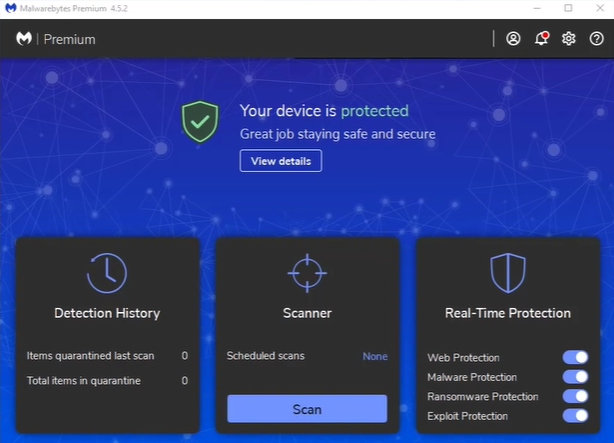
1. Xor DDoS. Вирус сканирует компьютеры поблизости и заставляет их скачивать самого себя для дальнейшего распространения. При получении команды извне позволяет выполнять бот-атаки. Больше всего применяется в азии. Из-за отсутствия интернет-соединения в виртуальной машине он бездействует. В рабочем состоянии мы бы увидели следующую картину:



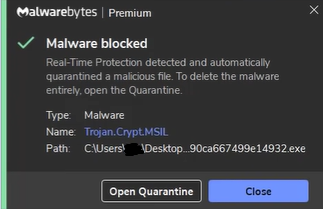
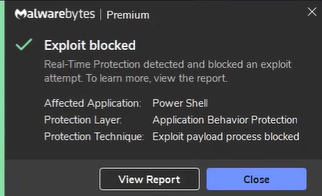
Постоянные переподключения по ssh могут сигнализировать о наличии вируса по типу ботнет в системе Linux.

1. Провести анализ доступного ПО на рынке и выбрать антивирус для защиты своей системы.

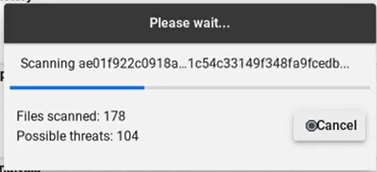
По своему личному и удачному опыту борьбы с вирусами на ОС Windows была использована утилита под названием Malwarebytes Anti-malware. Этот антивирус довольно прост – устанавливаем, запускаем проверку, удаляем заражённые файлы. Но главное что он бесплатный.



При попытке запуска вируса-блокировщика с установленным антивирусом выходит ошибка и вирус блокируется:



Среди антивирусов на Linux популярным является ClamAV. После установки в систему Mirai – ботнета, антивирус успешно определяет заражённые файлы и предлагает различные действия с файлами – удалить, карантин, либо ничего не делать:





После удаления антивирус больше не обнаруживает никаких угроз.

**Вывод:** в ходе работы узнал, как могут повлиять вирусы на мою систему и как предотвратить их появление.