|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ | | | | | | | | | | | | | | | | | | | | |
| Федеральное государственное автономное образовательное  учреждение высшего образования | | | | | | | | | | | | | | | | | | | | |
| **Дальневосточный федеральный университет** | | | | | | | | | | | | | | | | | | | | |
|  | | | | | | | | | | | | | | | | | | | | |
|  | | | | | | | | | | | | | | | | | | | | |
|  | | | | | | | | | | | | | | | | | | | | |
| **ШКОЛА ЕСТЕСТВЕННЫХ НАУК** | | | | | | | | | | | | | | | | | | | | |
|  | | | | | | | | | | | | | | | | | | | | |
|  | | | | | | | | | | | | | | | | | | | | |
| **Кафедра информационной безопасности** | | | | | | | | | | | | | | | | | | | | |
|  | | | | | | | | | | | | | | | | | | | | |
|  | | | | | | | | | | | | | | | | | | | | |
|  | | | | | | | | | | | | | | | | | | | | |
| **О Т Ч Е Т** | | | | | | | | | | | | | | | | | | | | |
| о прохождении учебной практики (учебно-лабораторного практикума) | | | | | | | | | | | | | | | | | | | | |
|  | | | | | | | | | | | | | | | | | | | | |
|  | | | | | | | | | | | | | | | | | | | | |
|  | | | | | | | | | | | | | | | | | | | | |
|  | | | | | | | | | |  |  | Выполнил студент  гр. С8117-10.05.01ммзи | | | | | | | | |
|  |  |  | | | | | | Красников А.Д. | | |
|  | | | | | | | | | |  |  | (подпись) | | | | | |  | | |
|  | | | | | | | | | | | | | | | | | | | | |
| Отчет защищен с оценкой | | | | | | | | | |  |  | Руководитель практики | | | | | | |  | |
|  | | | | | | | | | |  |  | Старший преподаватель кафедры информационной безопасности ШЕН | | | | | | | | |
|  | | | |  | С.С. Зотов | | | | |  |  |  | | | | |  | С.С. Зотов | | |
| (подпись) | | | |  | (И.О. Фамилия) | | | | |  |  | (подпись) | | | | |  | (И.О. Фамилия) | | |
| « | 26 | » | июня | | | | | | 2021 г. |  |  |  | | | | | | | | |
|  | | | | | | | | | | | | | | | | | | | | |
| Регистрационный № | | | | | | | |  | |  |  | Практика пройдена в срок | | | | | | | | |
| « | 26 | » | июня | | | | | | 2021 г. |  |  | с | « | 22 | » | февраля | | | | 2021 г. |
|  | | | | | | | | | |  |  | по | « | 26 | » | июня | | | | 2021 г. |
|  | | | | | |  | Е.В. Третьяк | | |  |  | на предприятии | | | | | | | | |
| (подпись) | | | | | |  | (И.О. Фамилия) | | |  |  |
|  | | | | | | | | | |  |  | Кафедра информационной | | | | | | | | |
|  | | | | | | | | | |  |  | безопасности ШЕН ДВФУ | | | | | | | | |
|  | | | | | | | | | |  |  |  | | | | | | | | |
|  | | | | | | | | | | | | | | | | | | | | |
|  | | | | | | | | | | | | | | | | | | | | |
|  | | | | | | | | | | | | | | | | | | | | |
|  | | | | | | | | | | | | | | | | | | | | |
|  | | | | | | | | | | | | | | | | | | | | |
| г. Владивосток | | | | | | | | | | | | | | | | | | | | |
| 2021 | | | | | | | | | | | | | | | | | | | | |

**Содержание**

Задание на практику 3

Введение 4

Разработка программы для детектирования аномалий с помощью машинного обучения 5

Заключение 10

Список использованных источников 11

**Задание на практику**

- Проведение исследования в области защиты от взлома программных средств

- Написание отчета по практике о проделанной работе.

**Введение**

Учебная практика (учебно-лабораторный практикум) проходил на кафедре информационной безопасности ШЕН ДВФУ в период с 22 февраля 2021 года по 26 июня 2021 года.

Целью прохождения практики является приобретение практических и теоретических навыков по специальности, а также навыков оформления проведенного исследования в отчетной форме.

Задачи практики:

1. Теоретическое ознакомление с существующими вредоносными программами.
2. Применить полученные знания в создании аномальных ивентов безопасности Windows
3. На основе полученных знаний написать отчет по практике о проделанной работе.

**Разработка программы для детектирования аномалий с помощью машинного обучения**

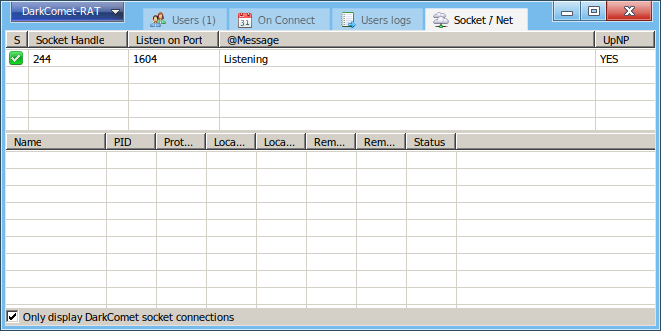
Для создания программы по детектированию аномалий необходимо собрать данные, на которых будет учится модель. Этими данными будут записи журналов событий Windows, взятых после подозрительной активности, которая будет внесена искусственно с помощью различных эксплойтов и вирусов. В качестве системы, которая подвергается атакам была выбрана Windows7(x64). Для формирования подозрительной активности использовались: DarkComet, созданные с помощью msfvenom бекдоры и различные троянские программы. Далее будет описан процесс создания подозрительной активности в атакуемой машине и сбор данных, которые будут впоследствии использоваться для кластеризации.

**DarkComet**

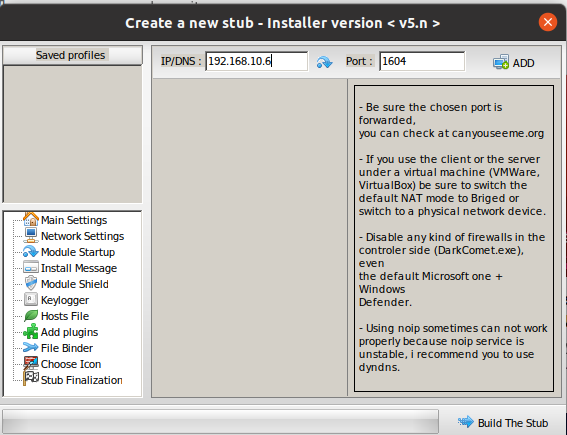
DarkComet — троянская программа, позволяющий получить удалённый доступ к компьютеру жертвы. Изначально использовался как программа для удалённого администрирования, но из-за широкого арсенала возможностей стал излюбленным средством злоумышленников.

Процесс создания подозрительной активности с использованием DarkComet:

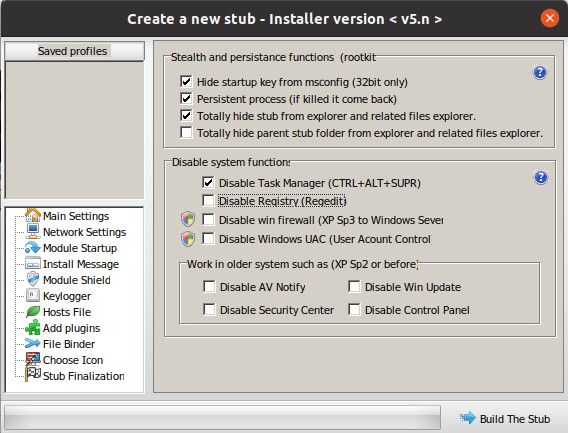
1. Запустим DarkComet на системе, с которой будем выполнять атаку, в рамках данной практики использовалась Ubuntu 20.04
2. Во вкладке Socket задаём порт для прослушивания



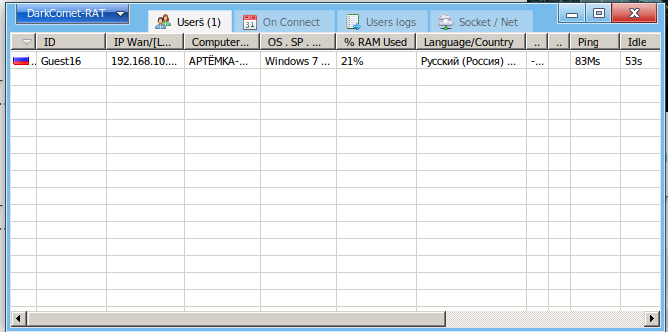
1. В настройках сервера задаём ip атакующей машины и порт для прослушивания



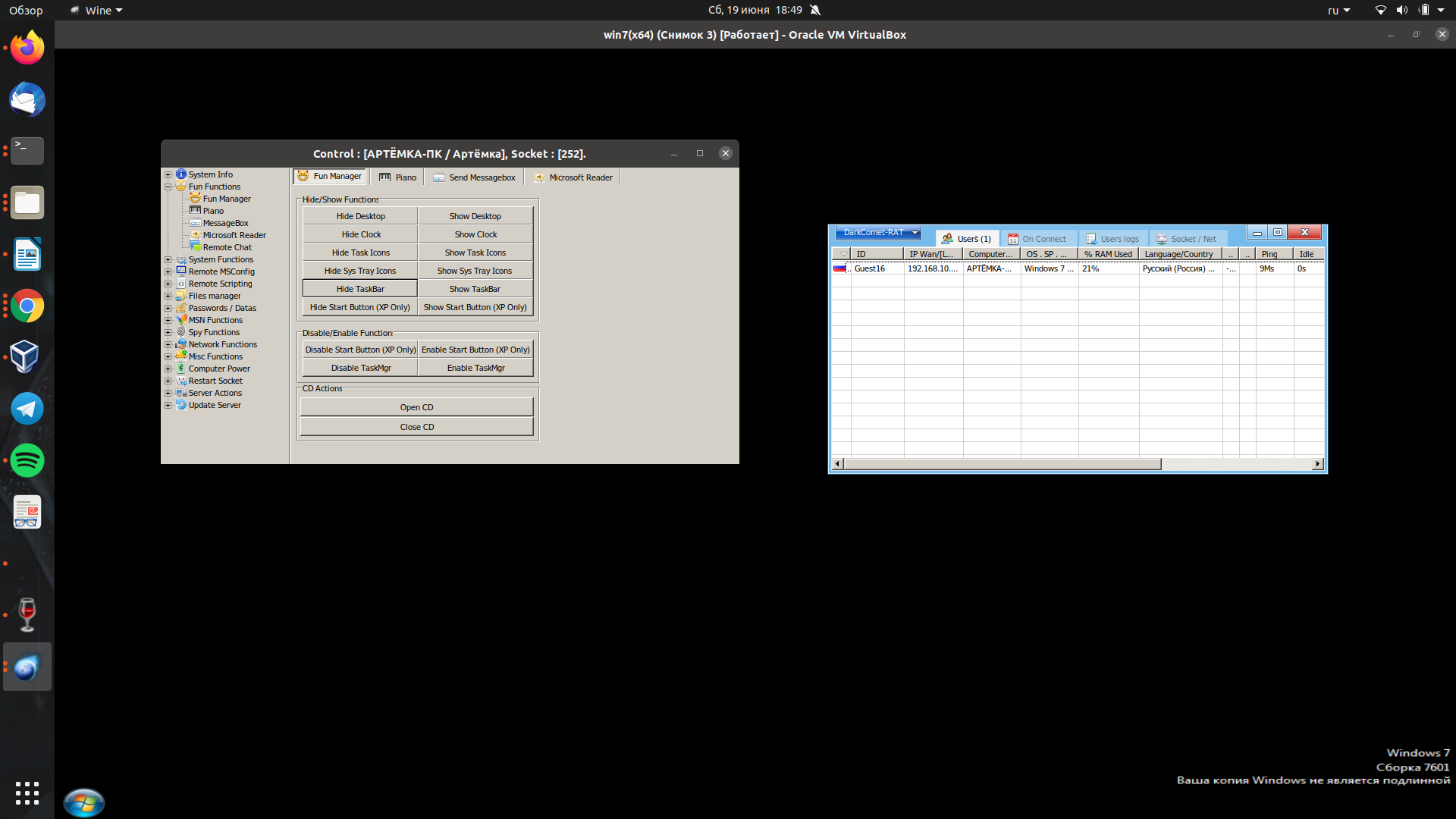
1. Можно задать различные функции препятствующие обнаружению будущего бекдора



1. Создаём бекдор кликом на кнопку Bild The Stub
2. Доставляем бекдор на атакуемую машину
3. Запускаем троян на машине жертвы и на атакующей машине во вкладке Users появляется компьютер, подвергшейся атаке



1. Кликнув на соответствующие поле получаем контроль на компьютером жертвы



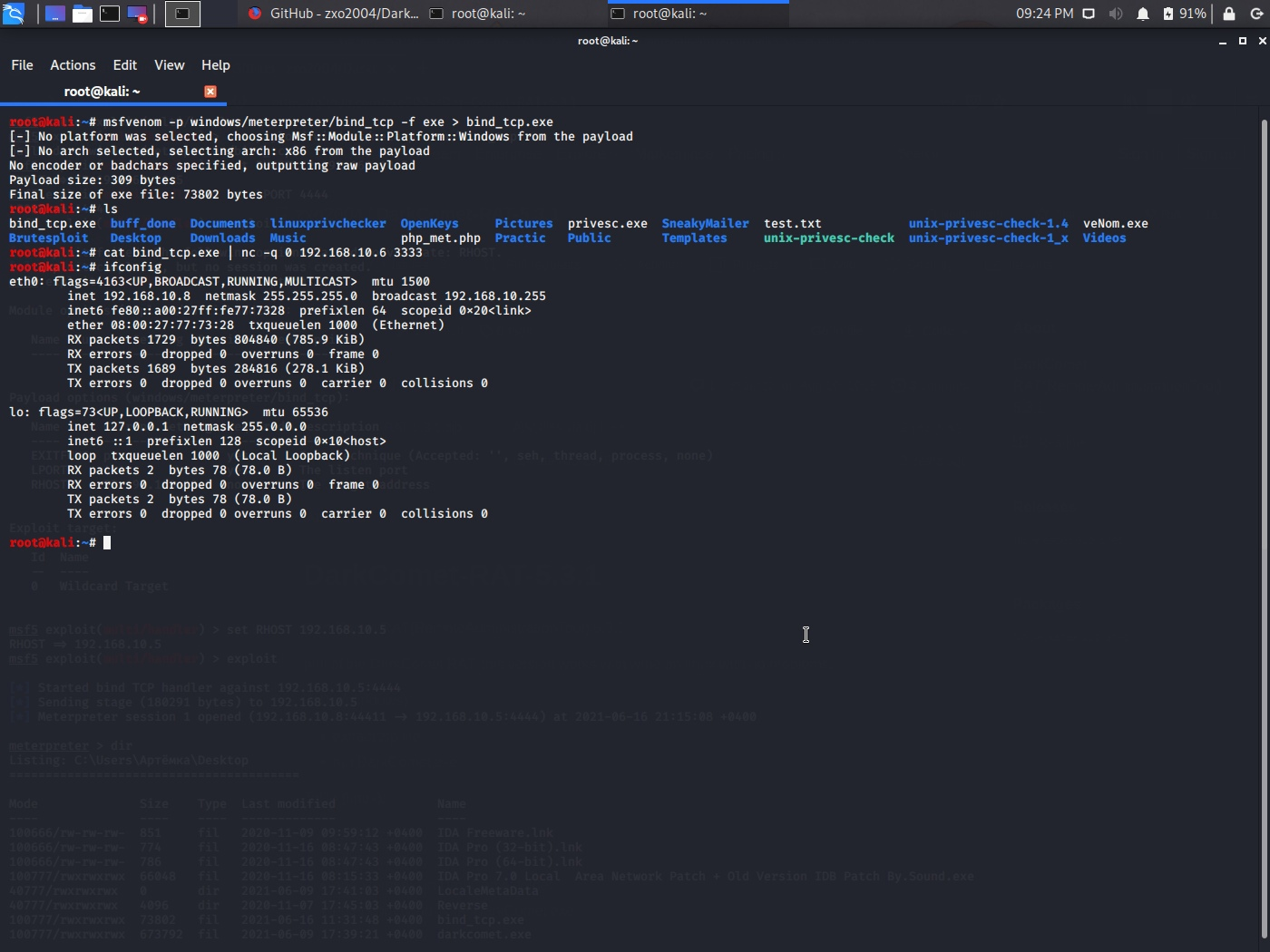
**msfvenom**

msfvenom **-** инструмент командной строки из пакета metasploit для создания полезной нагрузки. Для создания подозрительной активности создадим с помощью msfvenom бекдор схемы bind shell.

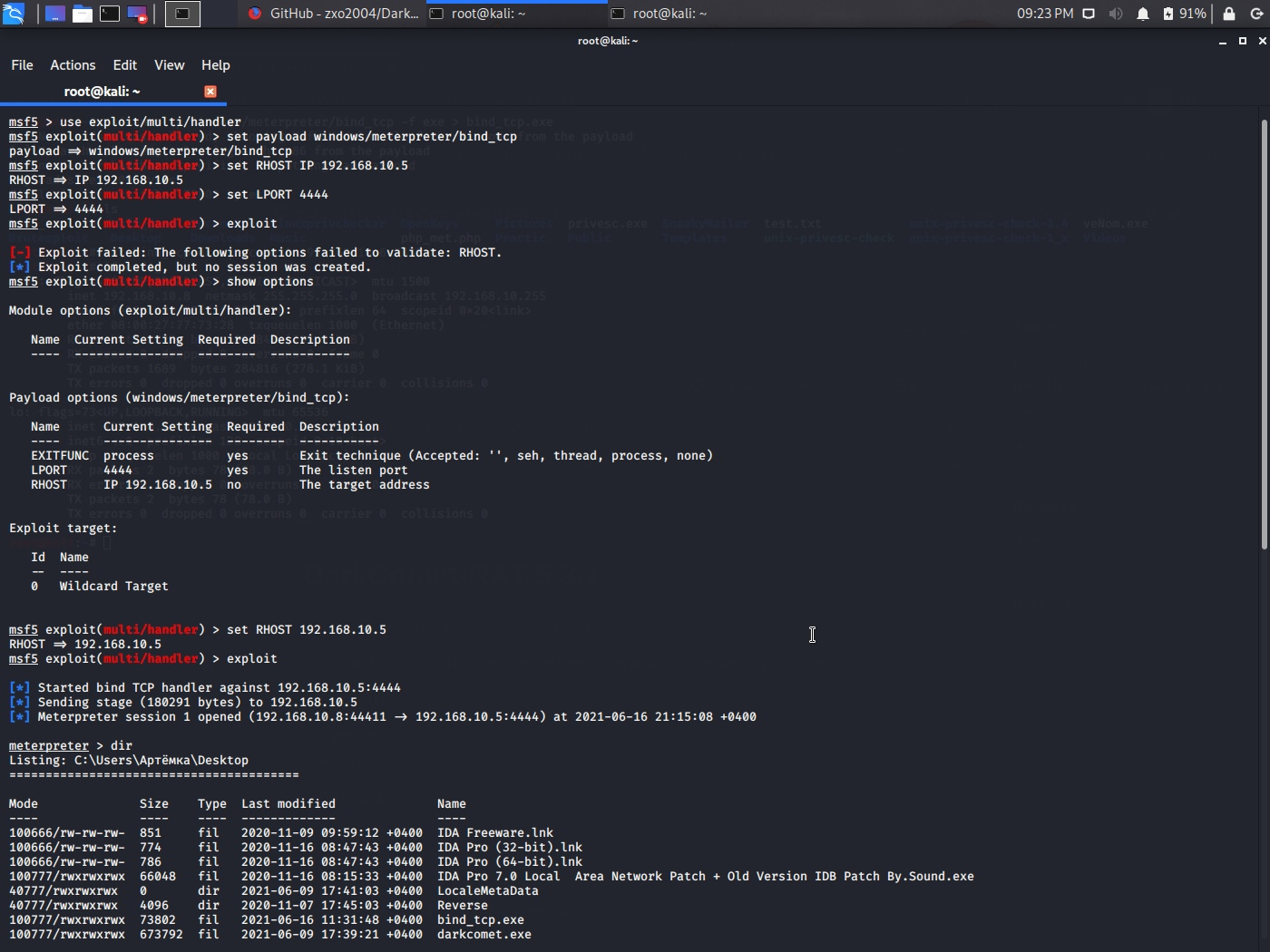
Bind shell — это схема взаимодействия с удалённой консолью, при которой на целевом компьютере запускается сервис, к которому может подключиться атакующий. Фактически, речь идёт о прямом подключении к атакуемому компьютеру.

Процесс создания подозрительной активности с использованием msfvenom:

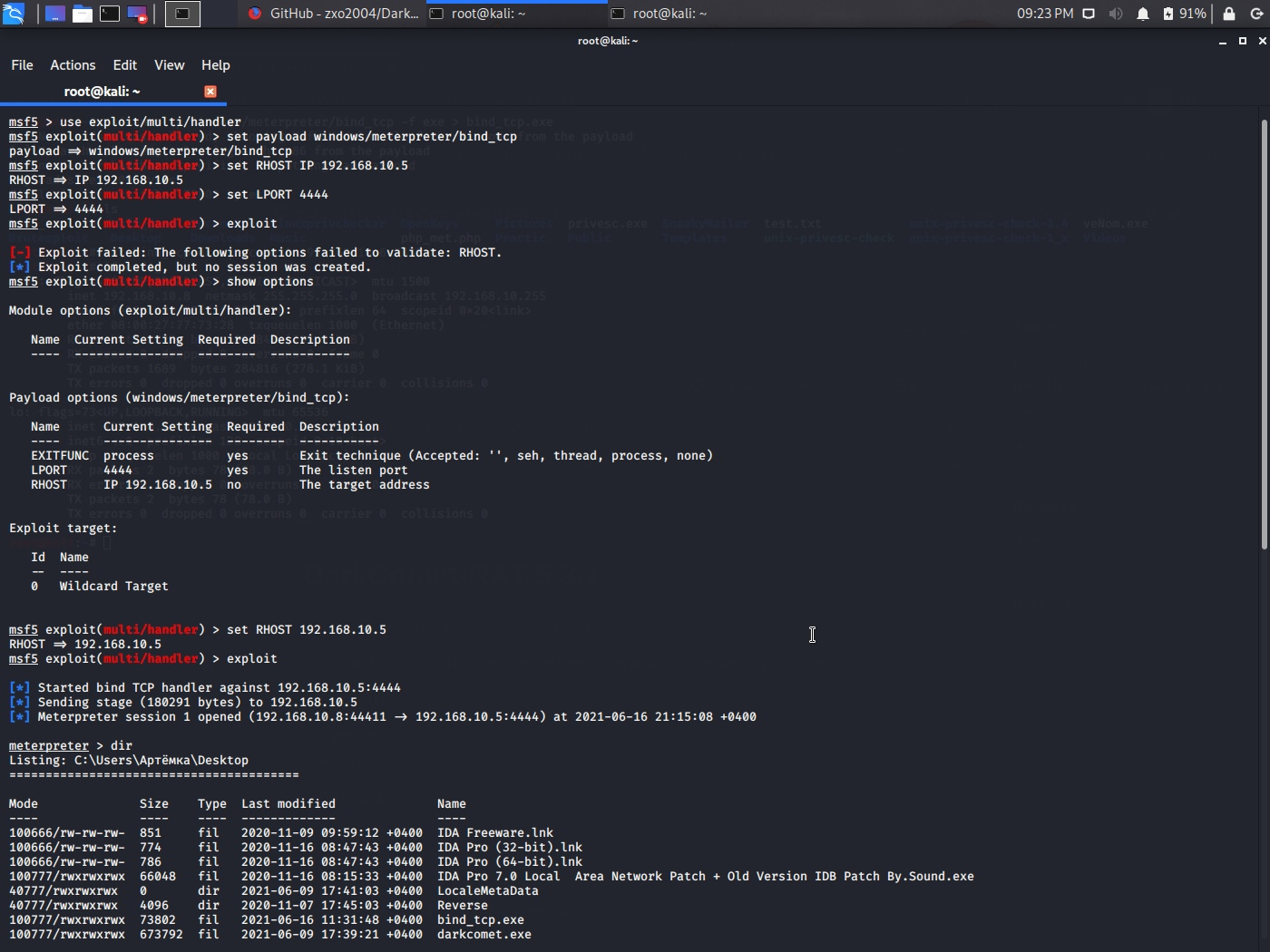
1. Атакующей машиной будет Kali Linux. Создаём payload с помощью msfvenom



1. Доставляем его на машину жертвы
2. Жертва запускает файл
3. На атакующей машине запускаем metasploit, выбираем модуль multi/handler и настраиваем его( задаём полезную нагрузку, ip машины жертвы и порт атакующей машины)



1. Создаём метерпретер сессию и получаем доступ к атакуемой машине



**Троянские программы**

Троянские программы- вредоносные программы, которые распространяются под видом легитимного программного обеспечения. Троянские программы осуществляют различные неподтверждённые пользователем действия, которые зачастую вредят пользователю. В рамках данной практики для получения данных использовались 3 вида троянских программ: загрузчики, поисковик электронных адресов и поисковик паролей. Загрузчики качают зараженные исполняемые файлы (скрипты, файлы с разрешением exe) с заранее прописанных в коде злоумышленником доменов. Поисковики электронных адресов ищут адресные книги (например, для Outlook) на хосте и считывают из них почтовые адреса пользователей (например, для рассылки спама в дальнейшем). Поисковики паролей ищут пароли на компьютере жертвы и отправляют их злоумышленнику.

Процесс создания подозрительной активности с использованием троянских программ типов указанных выше сводится к доставке исполняемого файла на компьютер жертвы и запуск жертвой самих троянских программ.

**Заключение**

Для достижения данной цели, в процессе прохождения учебной практики (учебно-лабораторного практикума) Теоретическое ознакомился с существующими вредоносными программами. Применил полученные знания в создании аномальных ивентов безопасности Windows.

Также были изучены требования к написанию отчета по практике. В результате прохождения практики был составлен отчет по практике, соответствующий предъявленным требованиям.

В ходе прохождения практики все задачи были выполнены, а цель достигнута.

**Список используемых источников**

1) MSFVENOM — инструмент для создания payload в metasploit [Электронный ресурс]. Режим доступа : https://cryptoworld.su/msfvenom-инструмент-для-создания-payload-в-metasploit/ (дата обращения: 25.05.2021).

2) О создании пэйлоадов для разных платформ с помощью msfvenom [Электронный ресурс]. – Режим доступа : https://habr.com/ru/company/ruvds/blog/343612/ (дата обращения: 26.05.2021).

3) How to setup DarkComet RAT for Easy Access to a Target Computer –Режим доступа : https://tamilhackersgroup.blogspot.com/2014/01/how-to-setup-darkcomet-rat-for-easy.html (дата обращения: 30.05.2021).