



МІНІСТЕРСТВО ОСВІТИ І НАУКИ, МОЛОДІ ТА СПОРТУ УКРАЇНИ

НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ

«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ ІМЕНІ ІГОРЯ

СІКОРСЬКОГО»

ФІЗИКО-ТЕХНІЧНИЙ ІНСТИТУТ

Кафедра Інформаційної Безпеки

Аналіз та моніторинг кібербезпеки

Практичне завдання №7

Симуляція діяльності зловмисника

Перевірив:

Козленко О. В.

Виконав:

студент IV курсу

групи ФБ-01

Сахній Н. Р.

Київ 2024

Мета: Аналіз стану кібербезпеки об'єкту за допомогою пен-тестингу.

Завдання: Провести симуляцію діяльності зловмисника при атаці на систему за допомогою утиліти [Infection Monkey](#).

- Завантажимо та автентифікуємось на власний **Infection Monkey** сервер:

```
(nazar@snz24) ~/Завантажене
$ chmod u+x InfectionMonkey-v2.3.0.AppImage

(nazar@snz24) ~/Завантажене
$ ./InfectionMonkey-v2.3.0.AppImage
2024-03-07 13:09:52,820 - DEBUG - __init__.py:449 - __getattr__() - loaded lazy attr 'SafeConfigParser': <class 'configparser.ConfigParser'>
2024-03-07 13:09:52,821 - DEBUG - __init__.py:449 - __getattr__() - loaded lazy attr 'NativeStringIO': <class '_io.StringIO'>
2024-03-07 13:09:52,821 - DEBUG - __init__.py:449 - __getattr__() - loaded lazy attr 'BytesIO': <class '_io.BytesIO'>
2024-03-07 13:09:52,894 - DEBUG - __init__.py:449 - __getattr__() - loaded lazy attr 'UnicodeIO': <class '_io.StringIO'>
2024-03-07 13:09:52,917 - DEBUG - registry.py:296 - register_crypt_handler() - registered 'pbkdf2_sha256' handler: <class 'passlib.handlers.pbkdf2.pbkdf2_sha256'>
2024-03-07 13:09:53,399 - INFO - config_setup.py:31 - update_config_from_file() - Server config updated from /tmp/.mount_InfectxSsAKk/usr/src/monkey_island/c
2024-03-07 13:09:53,400 - INFO - data_dir.py:19 - setup_data_dir() - Setting up data directory at /home/nazar/.monkey_island.
2024-03-07 13:09:53,403 - INFO - data_dir.py:25 - setup_data_dir() - Data directory set up in /home/nazar/.monkey_island.
2024-03-07 13:09:53,406 - INFO - server_setup.py:105 - _collect_system_info() - Monkey Island deployment: Deployment.APPIMAGE
2024-03-07 13:09:53,424 - INFO - server_setup.py:108 - _collect_system_info() - Monkey Island version: 2.3.0
2024-03-07 13:09:53,427 - INFO - mongo_setup.py:34 - _create_db_dir() - Database content directory: /home/nazar/.monkey_island/db.
2024-03-07 13:09:53,428 - INFO - mongo_db_process.py:23 - start() - Starting MongoDB process.
2024-03-07 13:09:53,428 - DEBUG - mongo_db_process.py:24 - start() - MongoDB will be launched with command: /tmp/.mount_InfectxSsAKk/usr/src/monkey_island/bin/
2024-03-07 13:09:53,428 - INFO - mongo_db_process.py:25 - start() - MongoDB log will be available at /home/nazar/.monkey_island/mongodb.log.
2024-03-07 13:09:53,435 - DEBUG - connectionpool.py:1014 - _new_conn() - Starting new HTTPS connection (1): njf01cuupf.execute-api.us-east-1.amazonaws.com:443
2024-03-07 13:09:53,533 - DEBUG - connectionpool.py:1014 - _new_conn() - Starting new HTTPS connection (1): m15mjynko3.execute-api.us-east-1.amazonaws.com:443
2024-03-07 13:09:53,560 - INFO - mongo_db_process.py:32 - start() - MongoDB has been launched!
```



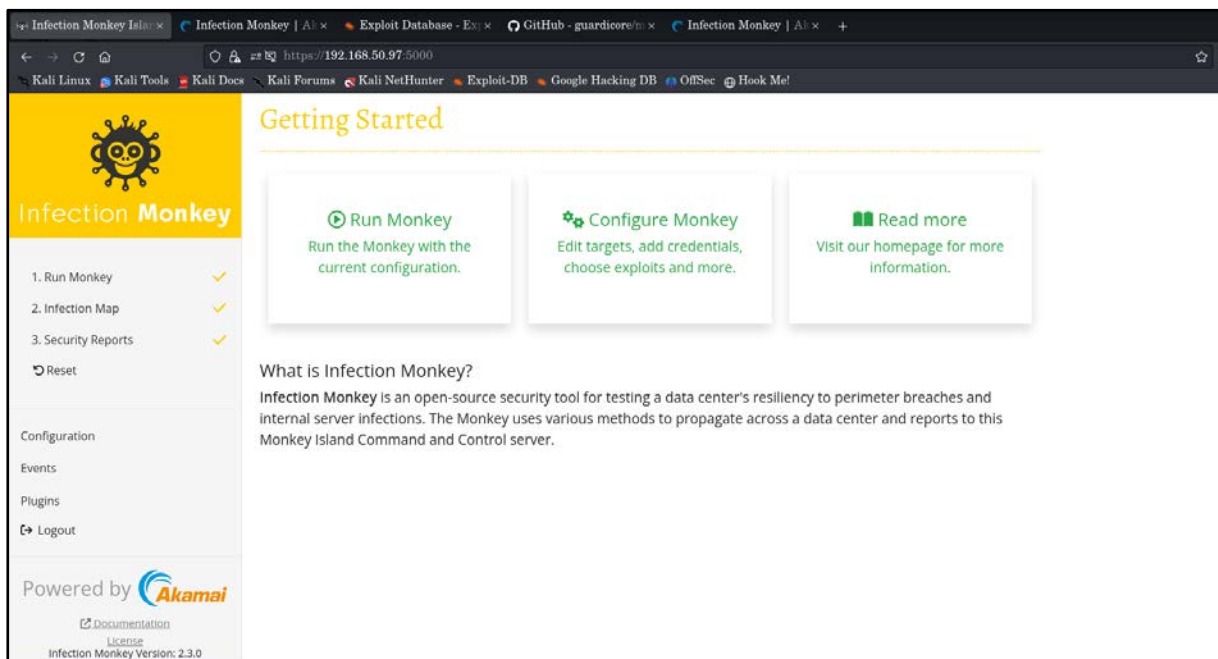
- Використаємо вразливу машину **metasploitable 2** для її пентестування:

```
metasploitable 2 (Before Monkey) [Запущено] - Oracle VM VirtualBox
Файл Машина Перегляд Введення Пристрої Довідка

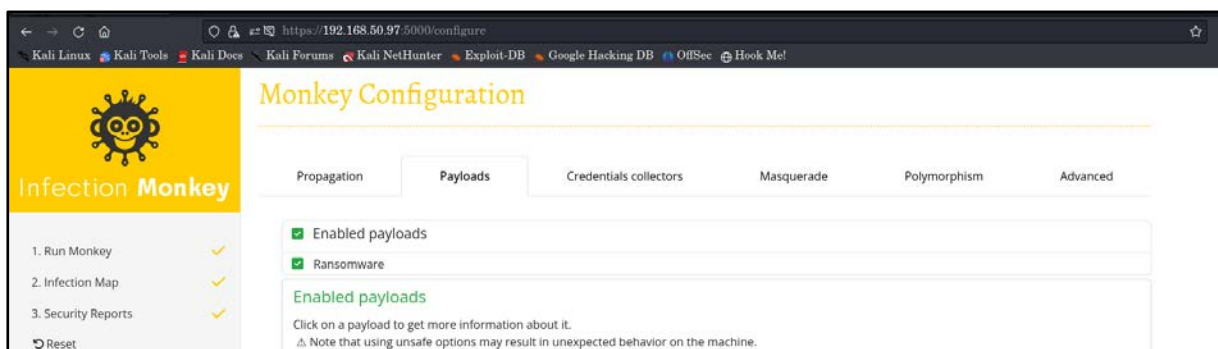
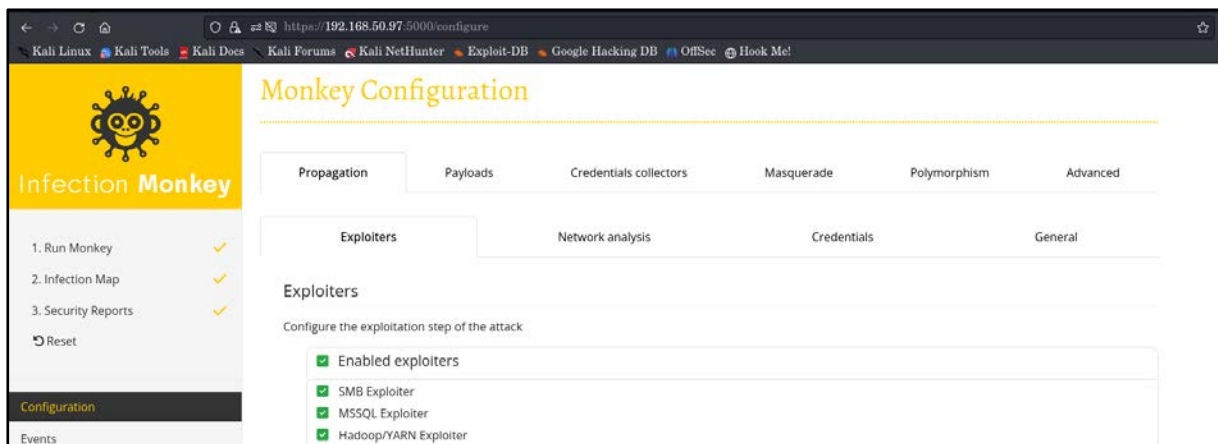
To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ ifconfig
eth0
    Link encap:Ethernet  HWaddr 08:00:27:a2:2c:cf
    inet addr:192.168.50.205  Bcast:192.168.50.255  Mask:255.255.255.0
    inet6 addr: fe80::a00:27ff:fea2:2ccf/64 Scope:Link
    UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
    RX packets:997 errors:0 dropped:0 overruns:0 frame:0
    TX packets:85 errors:0 dropped:0 overruns:0 carrier:0
    collisions:0 txqueuelen:1000
    RX bytes:66110 (64.5 KB)  TX bytes:8014 (7.8 KB)
    Base address:0xd020  Memory:f0200000-f0220000

lo
    Link encap:Local Loopback
    inet addr:127.0.0.1  Mask:255.0.0.0
```

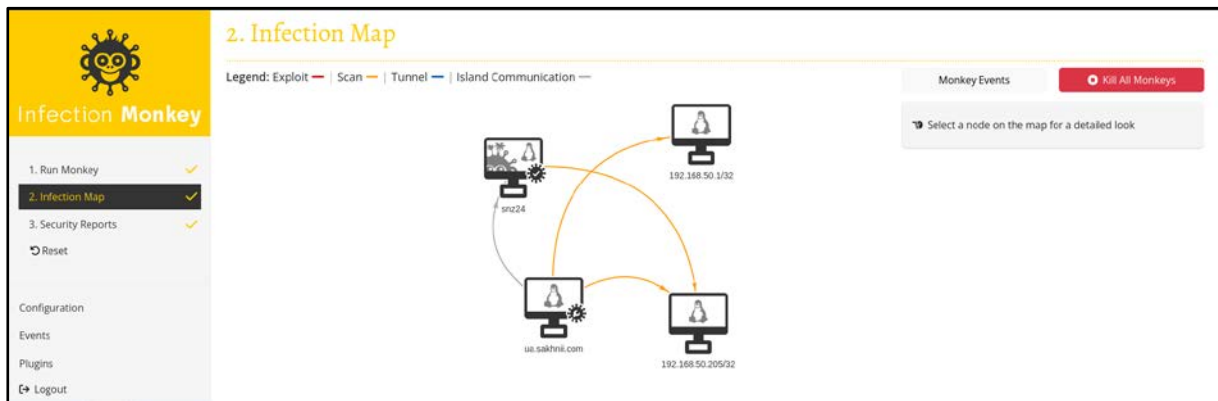
- Отже, розпочнемо попереднє конфігурування “мавпочки із гранатою”:



- Увімкнемо всі можливі експлойти, пейлоади та збирачі облікових даних:



- Перейдемо до перегляду мережевої мапи інфікованих хостів:



- Аналізуючи отриманий звіт, бачимо, що були знайдені відкриті сервіси:

3. Security Reports

Security report

Ransomware report

Print Report

Security Report

Infection Monkey

Overview

✓ No critical security issues were detected.

▲ To improve Infection Monkey's detection rates, try adding credentials under Propagation - Credentials and updating network settings under Propagation - Network analysis.

The first Infection Monkey Agent ran on 3/7/2024, 1:14:03 PM. After 51 minutes and 47 seconds, all Agents finished propagation attempts.

Infection Monkey started propagating from the following machines where it was manually installed:

- snz24
- ua.sakhnii.com

1. Run Monkey ✓

2. Infection Map ✓

3. Security Reports ✓

Reset

Configuration

Events

Plugins

Logout

Powered by Akamai

Documentation

License

Infection Monkey Version: 2.3.0

Configured exploitation methods:

- SMB Exploiter
- MSSQL Exploiter
- Hadcop/YARN Exploiter
- Log4Shell Exploiter
- PowerShell Exploiter
- RDP Exploiter
- SNMP Exploiter
- SSH Exploiter
- WMI Exploiter

Configured IPs to scan:

- 192.168.50.205

The Network from Infection Monkey's Eyes

Infection Monkey discovered 2 machines and successfully breached 0 of them.

0% of scanned machines exploited

Infection Monkey discovered 5 open services on 2 machines:

Machine	Services found
(192.168.50.205/32)	192.168.50.205:22 - ssh 192.168.50.205:80 - http 192.168.50.205:445 - smb
(192.168.50.1/32)	192.168.50.205:3306 - unknown 192.168.50.1:80 - http