Infection Monkey

Information Security Inc.

iSEC
information security inc.

Contents

- About Infection Monkey
- Architecture
- Requirements
- Testing Setup
- Installing Infection Monkey
- Running Infection Monkey
- References

About Infection Monkey

- The Infection Monkey is an open source security tool for testing a data center's resiliency to perimeter breaches and internal server infection
- The Monkey uses various methods to self propagate across a data center and reports success to a centralized Command and Control(C&C) server

Architecture

- Monkey - A tool which infects other machines and propagates to them
- Monkey Island - A C&C server with a dedicated UI to visualize the Chaos Monkey's progress inside the data center

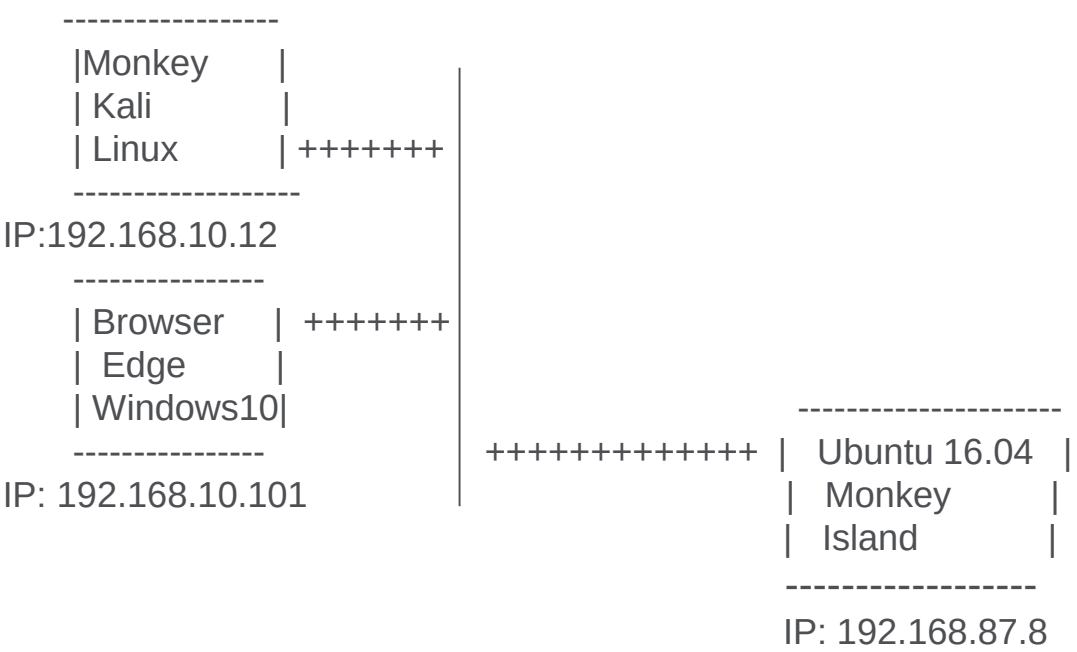
Architecture

- The monkey is composed of three separate parts
- * The Infection Monkey itself - PyInstaller compressed python archives
- * Sambacry binaries - Two linux binaries, 32/64 bit
- * Mimikatz binaries - Two windows binaries, 32/64 bit

Requirements

- The C&C Server has been tested on Ubuntu 14.04,15.04 and 16.04
- The Monkey itself has been tested on Windows XP, 7, 8.1 and 10
- The Linux build has been tested on Ubuntu server (multiple versions)

Testing Setup



Installing Infection Monkey

- Installing the InfectionMonkey on Linux
- Downloading Infection Monkey

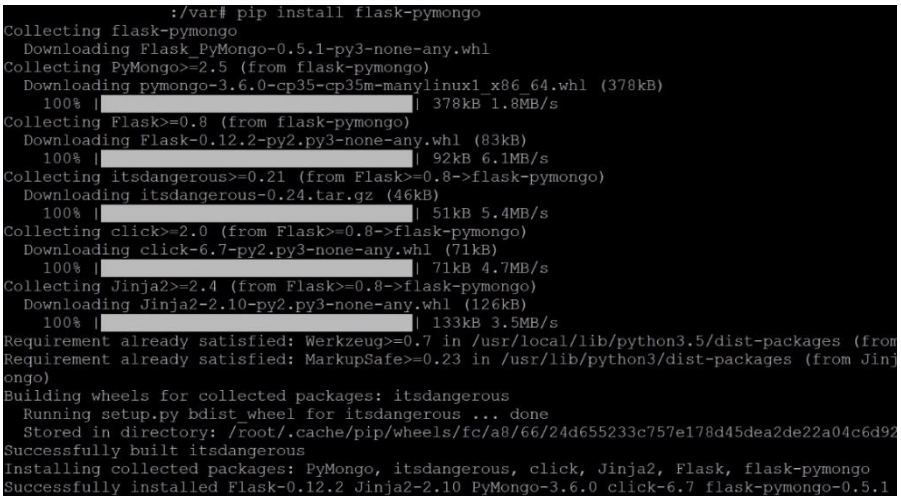
Installing Infection Monkey

- Installing the InfectionMonkey on Linux
- Unpacking the tarball

```
                :~/Monkey# tar -xf infection_monkey.tgz
                :~/Monkey# ls -lah
total 112M
drwxr-xr-x  2 root root 4.0K Feb 12 19:26 .
drwx------ 57 root root  16K Feb 12 19:26 ..
-rwxr-xr-x  1 root root 2.5K Sep  7  2016 example.conf
-rw-r--r--  1 root root  56M Feb 12 19:26 infection_monkey.tgz
-rw-r--r--  1 root root  56M Sep  7  2016 monkey_island.deb
-rwxr-xr-x  1 root root  11K Sep  7  2016 README.md
```

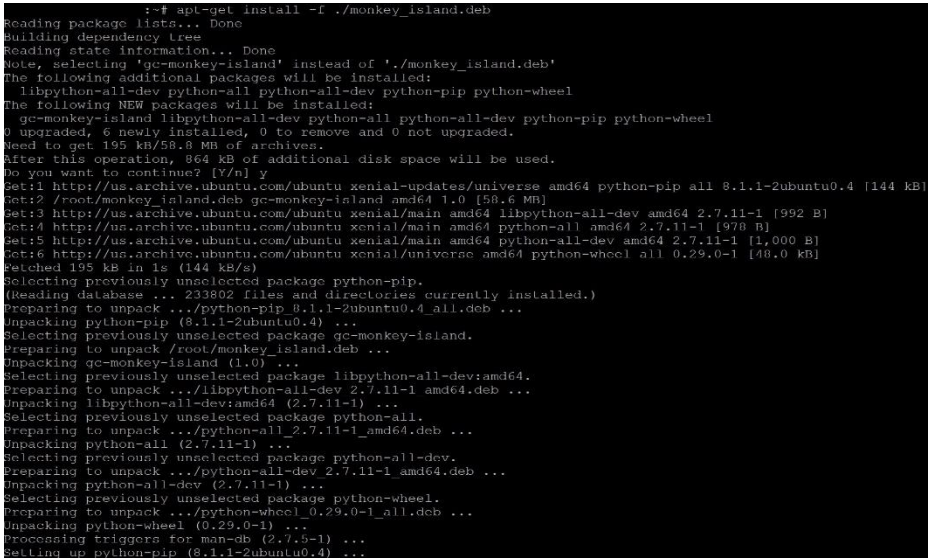
Installing Infection Monkey

- Installing the InfectionMonkey on Linux
- Installing Flask-pymongo



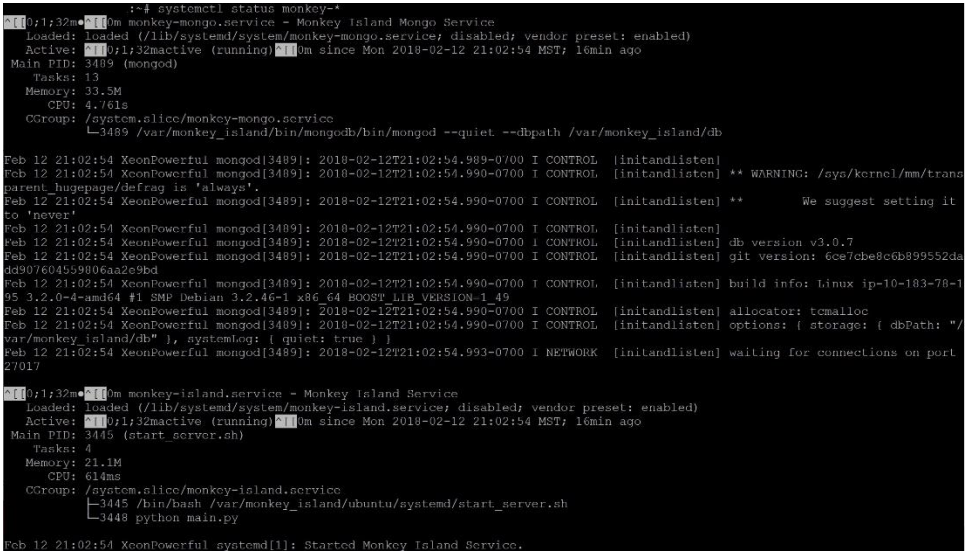
Installing Infection Monkey

- Installing the Monkey on Linux
- Installing the Monkey Island



Installing Infection Monkey

- Installing the Monkey on Linux
- Verify the Monkey service is functional



Installing Infection Monkey

- Installing the Monkey on Linux
- Verify the Monkey service is functional

```
root@XeonPowerful:~# netstat -anepl | less
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       User       Inode      PID/Program name
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN      0          16165      3040/sshd
tcp        0      0 127.0.0.1:631           0.0.0.0:*               LISTEN      0          29603      4975/cupsd
tcp        0      0 0.0.0.0:443             0.0.0.0:*               LISTEN      0          28619      4482/vmware-hostd
tcp        0      0 0.0.0.0:445             0.0.0.0:*               LISTEN      0          28541      4447/smbd
tcp        0      0 0.0.0.0:902             0.0.0.0:*               LISTEN      0          25969      3488/vmware-authdla
tcp        0      0 0.0.0.0:5000            0.0.0.0:*               LISTEN      0          264961     3448/python
tcp        0      0 0.0.0.0:27017           0.0.0.0:*               LISTEN      0          265579     3489/mongod
```

Installing Infection Monkey

- Access the Monkey's Island GUI by browsing to https://192.168.87.8:5000/admin/index.html

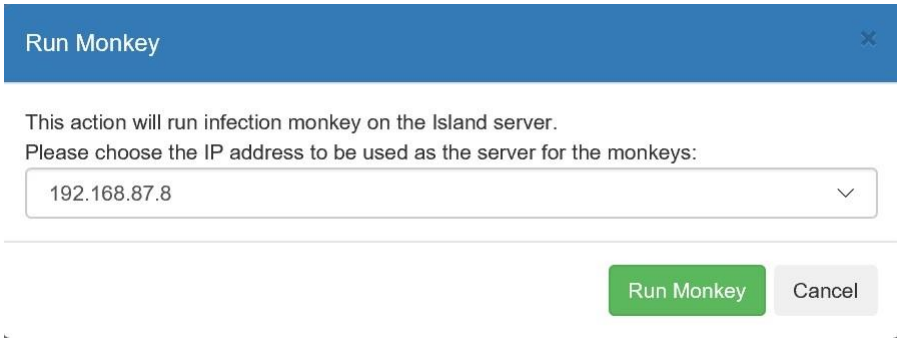
Running Infection Monkey

- The Monkey can be run in two ways =>

1) With the Monkey Island as the initial attacker. This will use the Monkey Island server as a starting position for the Monkey, from which it will expand based on the configuration

Running Infection Monkey

1) With the Monkey Island as the initial attacker. This will use the Monkey Island server as a starting position for the Monkey, from which it will expand based on the configuration

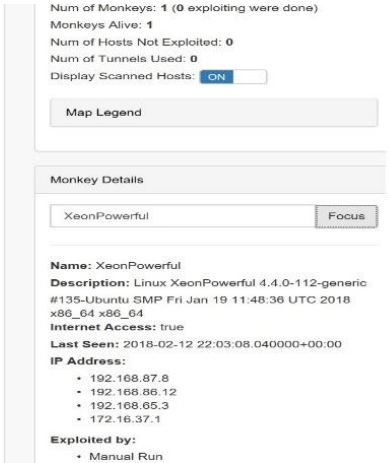


Running Infection Monkey

1) With the Monkey Island as the initial attacker. This will use the Monkey Island server as a starting position for the Monkey, from which it will expand based on the configuration

Running Infection Monkey

1) With the Monkey Island as the initial attacker. This will use the Monkey Island server as a starting position for the Monkey, from which it will expand based on the configuration

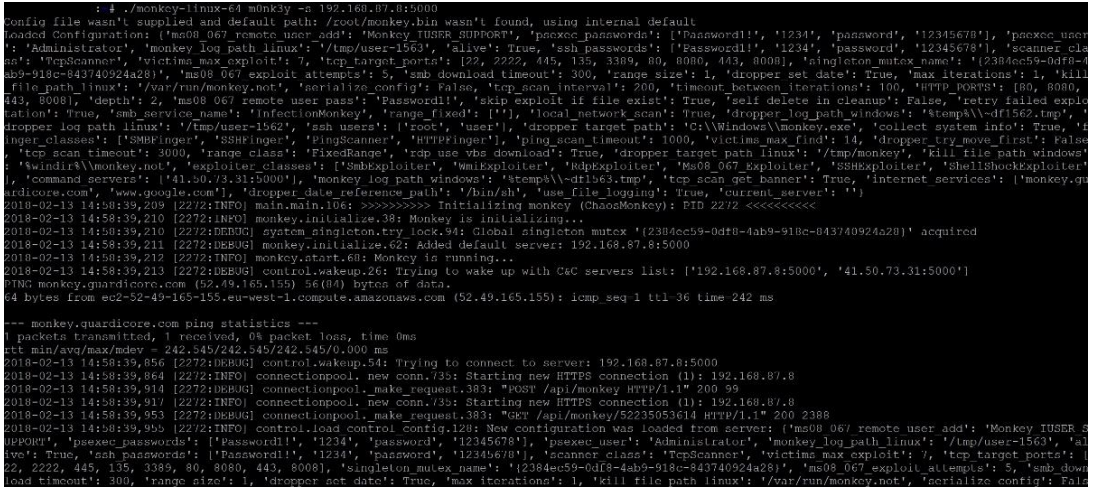


Running Infection Monkey

2) Running the Monkey from a machine elsewhere network
Download the appropriate Monkey executable (Linux/Windows and matching 32/64 bitness) using the following path [https://192.168.87.8:5000/api/monkey/download/[binaryToDownload]](https://192.168.87.8:5000/api/monkey/download/[binaryToDownload]) (monkey-windows-32.exe, monkey-windows-64.exe, monkey-linux-32, monkey-linux-64)

Running Infection Monkey

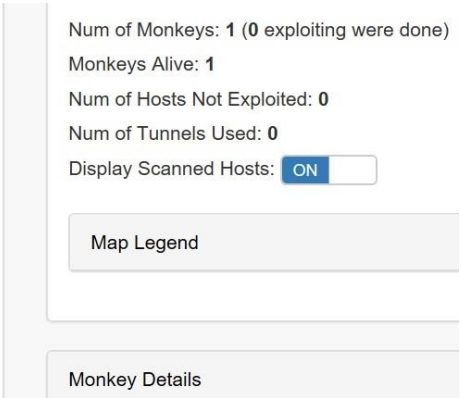
- Execute the Monkey from the console, passing the server address as a parameter and the magic keyword for execution
- Example “./monkey m0nk3y -s 192.168.87.8:5000”



Running Infection Monkey

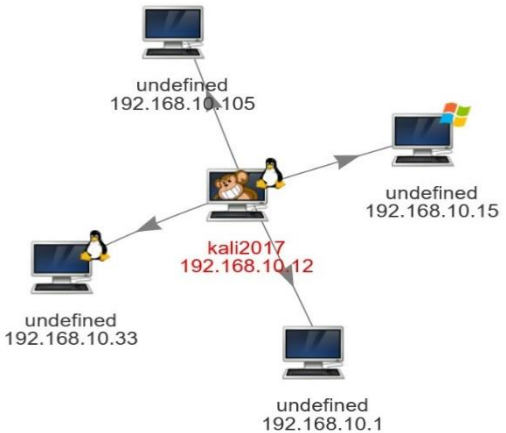
- Execute the Monkey from the console, passing the server address as a parameter and the magic keyword for execution
- Example “./monkey-linux-64 m0nk3y -s 192.168.87.8:5000”

kali2017
192.168.10.12



Running Infection Monkey

- 2) Execute the Monkey from the console, passing the server address as a parameter and the magic keyword for execution
- Example “./monkey-linux-64 m0nk3y -s 192.168.87.8:5000”



References

- Official website
https://www.guardicore.com/infectionmonkey/

- Github
https://github.com/guardicore/monkey