DDOS\_Tools

프로그램 제작

Land,flooding(TCP,UDP,ICMP),Slowloris,Rudy,Teardrop,Slowread

공격문실행 및 결과 보고서 작성

ㅇ

팀명:진훈태주

프로젝트 기간:

12월14 ~ 12월 30일

한국 IT직업전문학교

한국 IT직업전문학교

목차

[개요 2](#_Toc60142452)

[기사 2](#_Toc60142453)

[**구성원** 3](#_Toc60142454)

[내용 4](#_Toc60142455)

[구성도 4](#_Toc60142456)

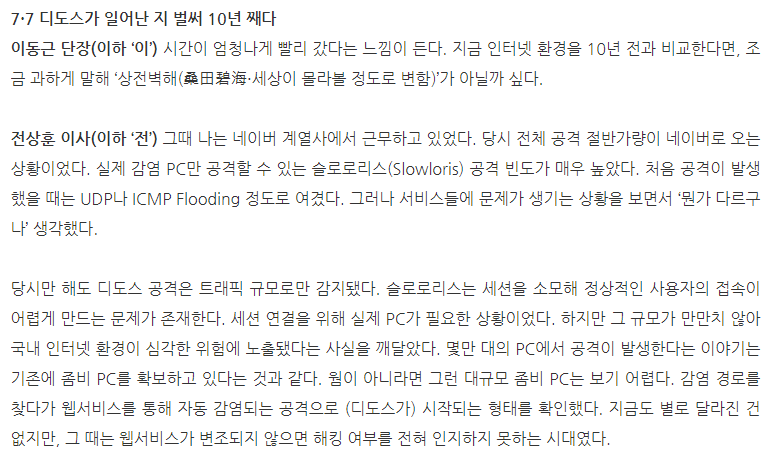
[주요공격문 5](#_Toc60142457)

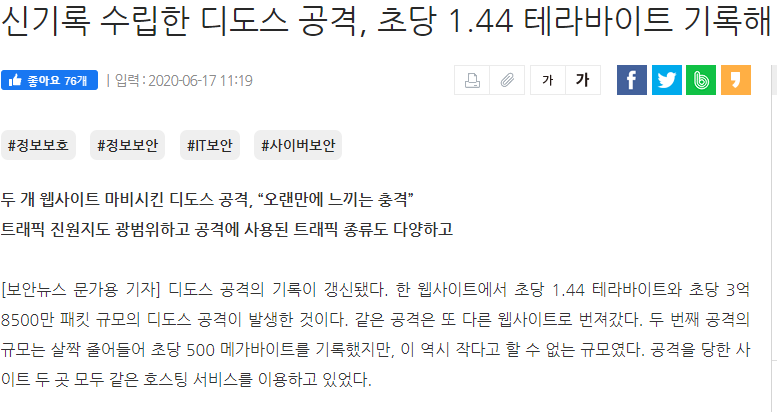
[UI 6](#_Toc60142458)

[결론 7](#_Toc60142459)

# 개요

### 기사





구성원 유주환(팀장, 소스코드작성)

이태서(UI, 소스코드작성)

정재훈(코드분석, 소스코드작성)

김진(소스코드작성)

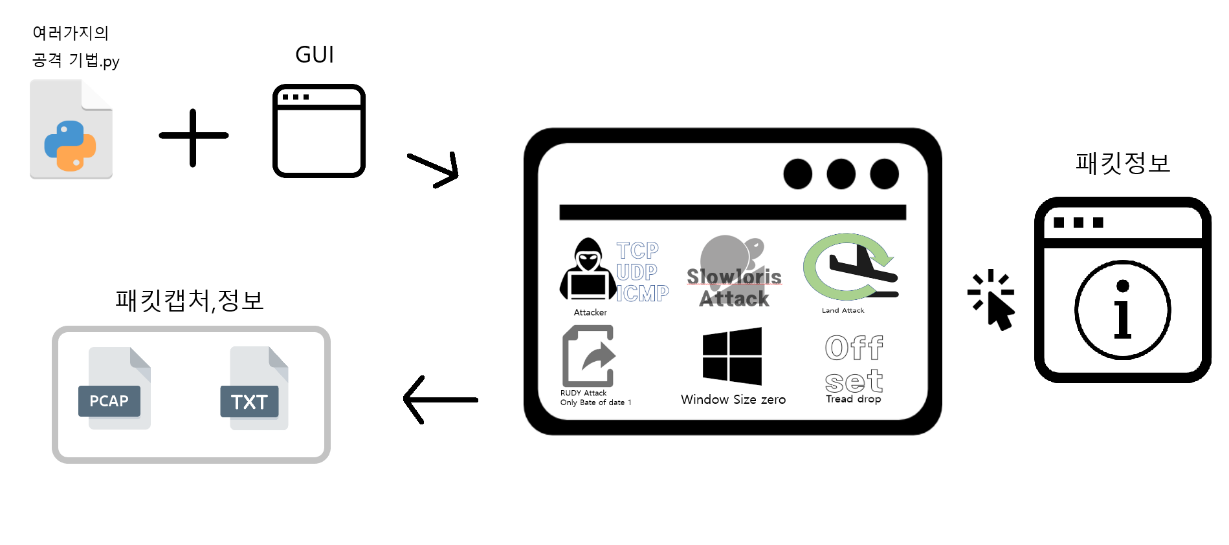
개발환경 파이썬3.7

환경 pycharm

# 내용

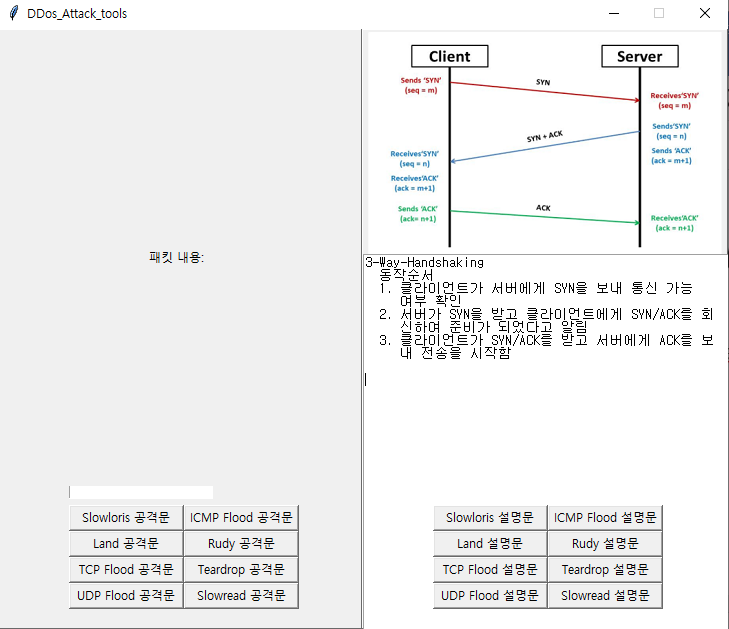
### 구성도

Python의 공격문을 window의 UI를 통해서 8개의 공격문을 가지고 패킷정보와 패킷캡처정보를 한눈에 확인하고 공격문에 대한 설명을 확인 할 수 있도록 설계하였습니다.



|  |
| --- |
| 라이브러리  File :파일생성 및 읽기  Scapy : 패킷을 수정 및 변조  Pyinstaller : exe파일을 만들 때 사용  Treading : 프로세스를 원활하게 이용시 사용  Tkinter : window환경에서 필요한 UI를 완성을  Socket :소켓을 생성을 통해 웹사이트와 연결  Sys : file처리를 위한 라이브러리 |
|
|
|
|
|
|
|

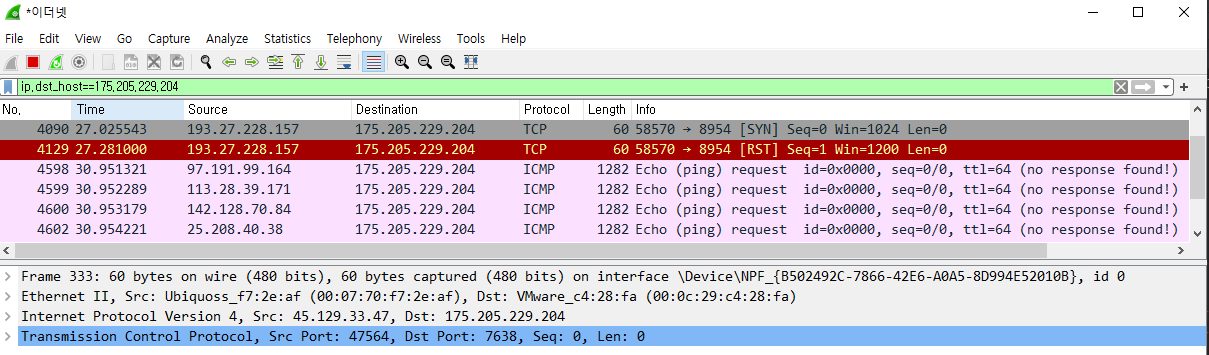
|  |
| --- |
| 주요공격문 Flooding  TCP,UDP,ICMP 대량의 TCP,UDP,ICMP패킷을 보내서 대상의 호스트에 네트워크자원을 소모시키는 공격을 말한다. |
| Slowloris : 지속적인 세션연결패킷을 여러 개보내서 자원고갈 시키는 공격입니다. |
| Land :송신자와 수신자의 ip를 똑같이 하여 보내 패킷이 피해자에게 순환되도록하는 공격입니다. |
| RUDY : 많은 데이터를 보낼꺼라고 컴퓨터를 속인후 1byte씩 단위로 발송하여 지연시키는 공격입니다. |
| Slowread :window size를 조작하여 응답을 천천히 읽어 TCP연결을 지연시키는 공격입니다. |
| Teardrop : TCP/IP 통신에서 데이터 패킷을 전송할 경우 패킷은 네트워크 전송크기(MTU) 에 맞게 단편화(fragment)가 되고 재조합 된다.  그리고 단편화된 각 패킷들은 IP헤더 내 재조합 순서를 가르키는 fragment offset 값을 가진다.  이러한 기능을 이용하여 공격자가 단편화된 패킷 조각의 fragment offset 값이 겹치거나 빈 공간이 생기게 만들어 보내면  시스템은 단편화 된 패킷의 재조합(reassemble)이 꼬이고 처리하지 못해 장애가 발생하게 된다. |

UI

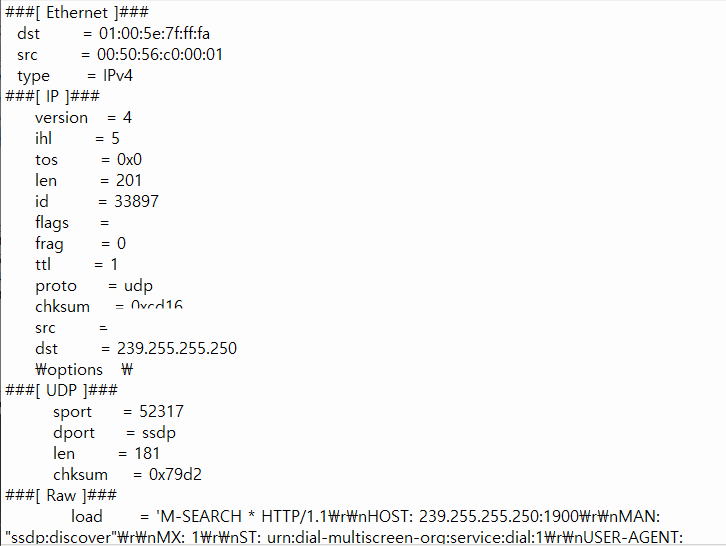
기본적인 UI는 textbox형식을 통해 원하는 ip를 결정하고 그 ip를 통해서 공격문을 실행하는 방식으로 설계하였습니다.

패킷내용은 왼쪽상단에 표시하도록 하였습니다.

공격시 발생되는 패킷값(ICMP예시)



공격시 생성되는 파일에 대한 정보값(ICMP)



# 결론

의사소통방법은 카카오톡통해서 시간표와 계획등을 이야기하였고 계획 중 zoom을 통해서 화면공유 및 시연결과 보고 그리고 소스를 공유하였습니다. discord로는 화면공유 및 의사소통 편리성을 위해서 사용하였습니다.

참고자료 :youtube , <http://blog.naver.com/stop2y> 을 보고 참고 해서 기본적인 틀을 완성하려 했습니다.

기사1<https://www.boannews.com/media/view.asp?idx=81348>

기사2<https://www.boannews.com/media/view.asp?idx=89014>