# 2020.12. 14 / 융보1B \_5조/유주환

# **서비스 거부 공격 도구 구현**

# 프로젝트 목적 및 배경

DDOS 공격이 난무한 요즘 그 공격원리를 이해하기 위하여 이 프로젝트를 결정하였습니다.

Python 언어가 간단 명료하여 이 언어로 빠른 시일내에 툴 제작을 하기로 하였습니다.

Python 의 입지가 넓어지는 현재 라이브러리들을 최대한 이용하여 작성하기로 하였습니다..

개발 환경

python

(공격자)툴 사용자, (피해자)Ubuntu\_Web\_server

슬로우 리스 공격 , tcp/udp 플러딩 공격 , land 공격

1. 프로젝트 기간 : 2020.12.14 ~ 2020.12.30
2. 주요 기능
   1. land공격으로 dos 공격을 수행할수 있으며, tcp/udp 플러딩 공격을 통하여 서버부하를 일으킬수 있으며, 슬로우리스 공격으로 http 패킷 변조를 수행할 수 있다.

프로젝트 개요

python으로 간단 명료하게 라이브러리를 이용하여 툴을 빠른 시일내에 제작하여 학습하는곳에 의의를 두고 있습니다.

프로젝트 목적 및 배경  
DDOS 공격이 난무한 요즘 그 공격기법의 원리를 알아 막아낼수 있기 위하여 이 프로젝트를 수행한다

**공격기법의 해결 방안**

프로젝트 배경

DDOS 공격 피해

1. 금융권을 노린 DDOS 공격
   1. 원격 근무가 시행된 코로나시대에 금융권또한 원격근무를 하는 요즘 DDOS 공격이 잦고있습니다. 한국거래소의 경우 지난 8월에 이어 최근에도 디도스 공격을 받아 공시사이트 접속이 지연되는 등 홈페이지 운영에 차질을 빚었다. 최근에는 적은 양의 트래픽을 사용해 서버를 다운시키는 `슬로우로리스(Slowloris)` 공격, 금전을 요구하는 `랜섬 디도스` 공격 형태로 진화하고 있어 체계적인 보안 전략으로 대응해야 한다는 조언이다.

2020년 12월4일 카이스트는 교직원과 학생들의 개인정보가 유출되는 사고가 발생하였다.

**DOS, DDOS공격에 위험성**

이런 공격들은 원격근무를 하는 요즘 급증하고 있다. 피해규모는 상상을 초월하며 더 큰 피해를 입기전에 막하야한다

**이러한 공격들을 대비하기 위해 이러한 공격들은 사전에 학습한다.**

본문 내용은 스타일의 ‘본문’을 적용합니다. (본문1)

개발 IDE : PyCharm

개발 기간 : Python 을 활용하여 DOS, DDOS 공격문을 작성하는 기간 ( 1주일 )  
 Tkinter를 활용하여 GUI를 생성한 뒤 이벤트를 발생시켜 동작시킨다. (1주일)

툴 GUI CLI

|  |  |  |
| --- | --- | --- |
| **표** | **CLI** | **GUI** |
| **사용자 편의성** | 사용자가 어떤기능을 하는지 알아야 사용할 수 있다. | 사용자가 어떤 기능인지 몰라도 클리과 입력만으로 사용할 수 있다. |
| **기능성** | CLI를 기반으로한다면 좀더 많은 기능들을 수행할 수 있다. | 기능들이 간편화 되어있고 보기쉽게 정렬되어있다. |
| **OS** | 리눅스, 윈도우 | 윈도우(PE파일) |

## 본 프로젝트는 이러한 이유들을 종합하고 의논해본결과 사용자들에게 편의성을 주는 GUI를 결정하였습니다

공격 기법의 해결방안

DDOS, DOS 공격의 해결방안

1. 공격 기법들 마다 해결방안이 다르다. 하지만 같다는건 한가지 있다. 네트워크의 트래픽이 급증하다는거다. 네트워크 장비로 여러 개 걸쳐서 통과하게 할 수 있다. 각 프로토콜의 취약점을 이용한 공격들도 있고 방어책을 연구하고자 본 프로젝트를 하였습니다.

이 프로젝트의 중점

DOS, DDOS의 원리를 알고 해결방안을 모색하는 것이다.

이 프로젝트의 중점

Python 이라는 언어를 통하여 GUI 프로그래밍언어와 수많은 라이브러리들을 통하여 파이썬 언어의 효율성과 네트워크 프로그래밍을 함으로써 python언어에 이해도와 네트워크에 대한 이해력을 키운다.