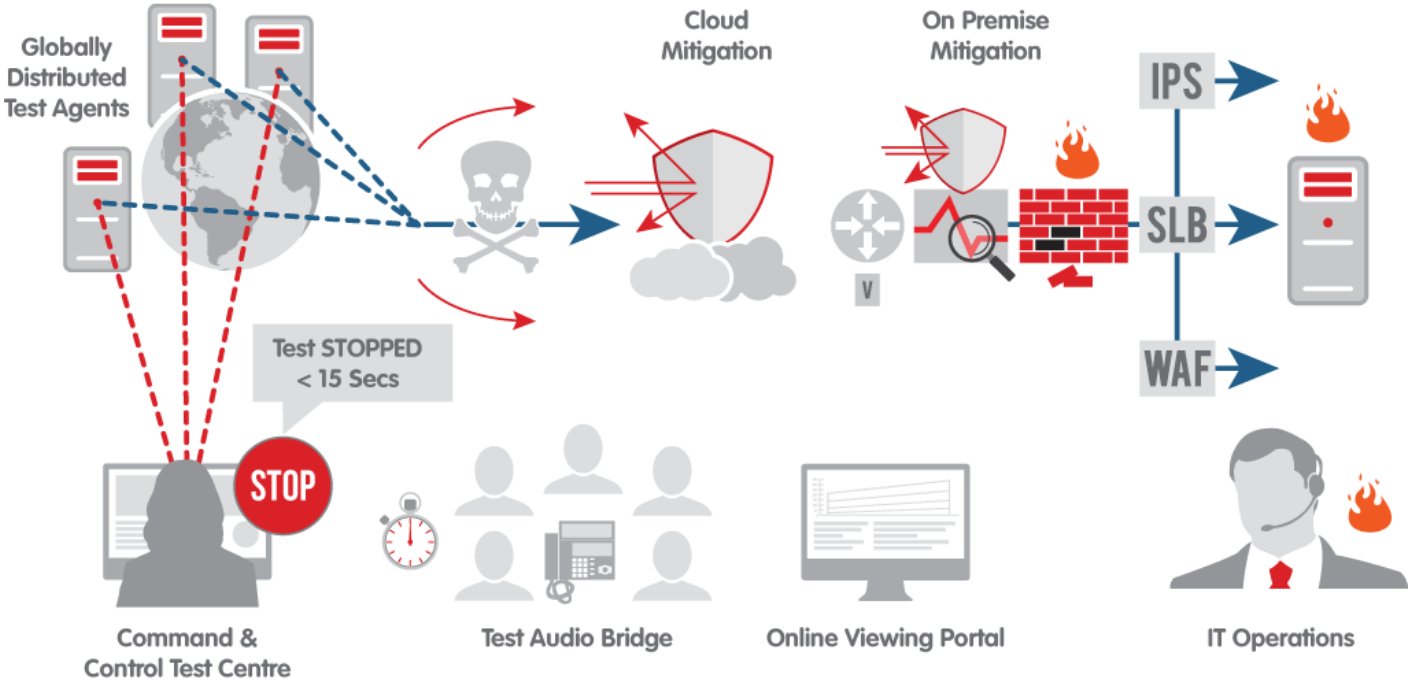
ITEC442 IOT & Cyber Security

Week 5-6 - DoS Attack

What is Denial of Service (DoS) Attack?

A Denial of Service (DoS) attack is a type of cyberattack that is designed to make a computer or network resource unavailable to its intended users by overwhelming it with traffic or requests for resources. DoS attacks can be performed using a single device or multiple devices, and can target a specific service, such as a website or a network connection, or the entire network. DoS attacks can be very disruptive and can cause serious damage to a business or organization, as they can prevent users from accessing the resources they need to do their jobs or conduct their daily activities. It is important to protect against DoS attacks by implementing security measures such as firewalls, intrusion detection and prevention systems, and load balancers.

Simulating DDoS Attack:



How to DDoS someone, cybercriminal style

There's more than one way of carrying out a denial-of-service attack. Some methods are easier to execute than others, but not as powerful. Other times, the attacker might want to go the extra mile, to really be sure the victim gets the message, so he can hire a dedicated botnet to carry out the attack..

Botnets

A botnet is a collection of computers or other Internet-connected devices that have been infected with malware, and now respond to the orders and commands of a central computer, called the Command and Control center.

The big botnets have a web of millions of devices, and most of the owners have no clue their devices are compromised.

Usually, botnets are used for a wide variety of illegal activities, such as pushing out spam emails, phishing or cryptocurrency mining.

Some, however, are available to rent for the highest bidder, who can use them in whatever way seems fit. Oftentimes, this means a DDoS attack.

DDoS programs and tools

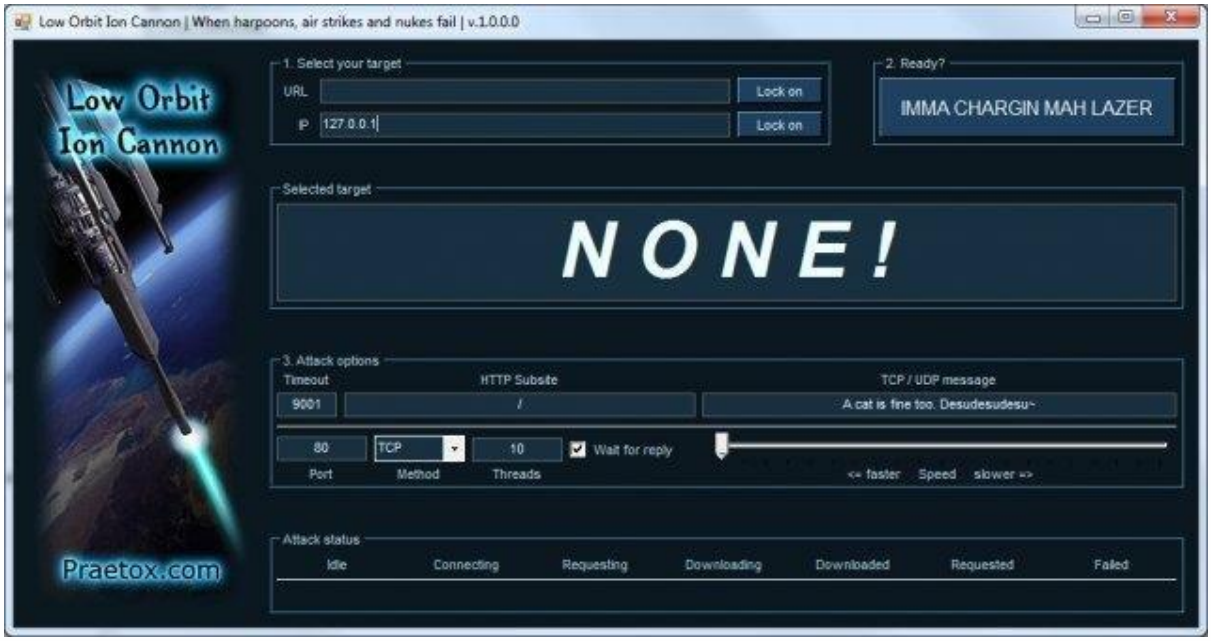
Small scale hackers who don't have access to botnets, have to rely on their own computers. This means using specialized tools, that can direct Internet traffic to a certain target.

Of course, the amount of traffic an individual computer can send is small, but crowdsource a few hundreds or thousands of users, and things suddenly grow in scope.

This particular tactic has been successfully employed by Anonymous. In short, they send a call to their followers, asking them to download a particular tool, and be active on messaging boards, such as IRC, at a particular time. They then simultaneously attack the target website or service, bringing it down.

Here's a sample list of tools that malicious hackers use to carry out denial of service attacks:

- Low Orbit Ion Cannon, shortened to LOIC.
- XOIC.
- HULK (HTTP Unbearable Load King).
- DDOSIM – Layer 7 DDoS Simulator
- R-U-Dead-Yet.
- Tor's Hammer.



How to DDoS an IP using cmd

One of the most basic and rudimentary denial-of-service methods is called the “ping of death”, and uses the Command Prompt to flood an Internet Protocol address with data packets.

Because of its small scale and basic nature, ping of death attacks usually work best against smaller targets. For instance, the attacker can target:

a) A single computer. However, in order for this to be successful, the malicious hacker must first find out the IP address of the device.

b) A wireless router. Flooding the router with data packets will prevent it from sending out Internet traffic to all other devices connected to it. In effect, this cuts the Internet access of any device that used the router.

In order to launch a ping denial-of-service attack, the malicious hacker first needs to find out the IP of the victim’s computer or device. This is a **relatively straightforward task**, however.

A ping of death is small in scale, and fairly basic, so it’s mostly efficient against particular devices. However, if multiple computers come together, it’s possible for a handful of these to bring down a smallish website without the proper infrastructure to deal with this threat.

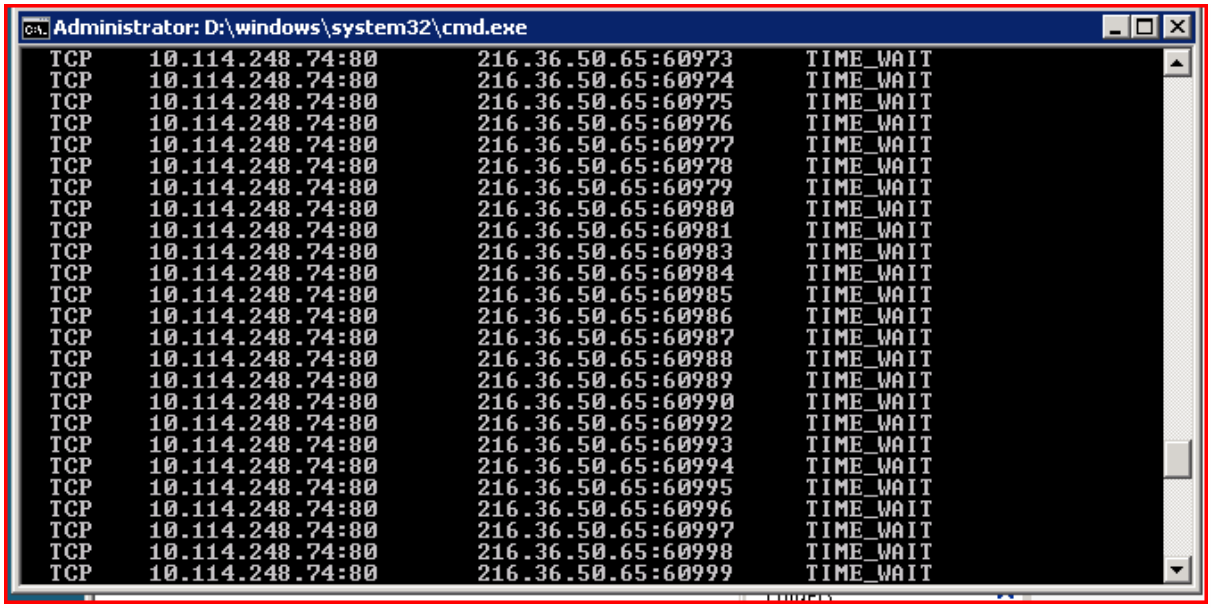
```
Administrator: Command Prompt
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Users\[redacted]>ping -t -l 65500 127.0.0.1

Pinging 127.0.0.1 with 65500 bytes of data:
Reply from 127.0.0.1: bytes=65500 time<1ms TTL=128
Reply from 127.0.0.1: bytes=65500 time<1ms TTL=128
Reply from 127.0.0.1: bytes=65500 time<1ms TTL=128
Reply from 127.0.0.1: bytes=65500 time<1ms TTL=128
Reply from 127.0.0.1: bytes=65500 time<1ms TTL=128
Reply from 127.0.0.1: bytes=65500 time<1ms TTL=128
Reply from 127.0.0.1: bytes=65500 time<1ms TTL=128
Reply from 127.0.0.1: bytes=65500 time<1ms TTL=128
Reply from 127.0.0.1: bytes=65500 time<1ms TTL=128
Reply from 127.0.0.1: bytes=65500 time<1ms TTL=128
Reply from 127.0.0.1: bytes=65500 time<1ms TTL=128
Reply from 127.0.0.1: bytes=65500 time<1ms TTL=128
Reply from 127.0.0.1: bytes=65500 time<1ms TTL=128

Ping statistics for 127.0.0.1:
    Packets: Sent = 13, Received = 13, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
Control-C
```

To open the tool, write **cmd** in the Start menu search bar, and then type in **netstat –an**. This will take you to a screen showing your own internal IP in the left-hand column, while the right-hand column holds all of the external IPs connected to your device.

```
Command Prompt
Microsoft Windows [Version 10.0.15063]
(c) 2017 Microsoft Corporation. All rights reserved.

C:\Users\Cristina>netstat -an

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    0.0.0.0:135            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:445            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:2869           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:5357           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49664          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49665          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49666          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49667          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49668          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49677          0.0.0.0:0              LISTENING
  TCP    192.168.1.243:80       0.0.0.0:0              LISTENING
  TCP    192.168.1.243:139      0.0.0.0:0              LISTENING
  TCP    192.168.1.243:443      0.0.0.0:0              LISTENING
  TCP    192.168.1.243:5127     0.0.0.0:0              LISTENING
  TCP    192.168.1.243:54361    157.55.235.150:40005   ESTABLISHED
  TCP    192.168.1.243:54362    40.77.226.192:443      ESTABLISHED
  TCP    192.168.1.243:54363    91.190.219.41:12350    ESTABLISHED
  TCP    192.168.1.243:54368    34.252.56.31:443       ESTABLISHED
  TCP    192.168.1.243:54418    13.74.136.47:443       ESTABLISHED
  TCP    192.168.1.243:54569    64.233.184.188:5228    ESTABLISHED
  TCP    192.168.1.243:54584    38.127.167.13:443      ESTABLISHED
  TCP    192.168.1.243:54776    40.77.229.8:443        ESTABLISHED
  TCP    192.168.1.243:54873    151.101.12.249:443     ESTABLISHED
  TCP    192.168.1.243:54883    52.4.57.32:443         ESTABLISHED
  TCP    192.168.1.243:54899    185.12.82.1:443        CLOSE_WAIT
  TCP    192.168.1.243:54922    104.16.205.165:443     ESTABLISHED
  TCP    192.168.1.243:54945    192.0.77.32:443        CLOSE_WAIT
  TCP    192.168.1.243:54946    192.0.77.32:443        CLOSE_WAIT
  TCP    192.168.1.243:54947    192.0.77.32:443        CLOSE_WAIT
  TCP    192.168.1.243:54948    192.0.77.32:443        CLOSE_WAIT
  TCP    192.168.1.243:54949    192.0.77.32:443        CLOSE_WAIT
```

The screenshot above is for a normal connection. In it, you can see a few other IPs that communicate normally with the device.

Now, here’s how a DDoS attack would look like:



On the right hand side, you can see that a single external IP repeatedly tries to connect to your own device. While not always indicative of a DDoS, this is a sign that something fishy is going, and warrants further investigation.

References:

https://heimdalsecurity.com/blog/how-to-ddos/

https://www.cloudflare.com/learning/ddos/ddos-attack-tools/how-to-ddos/