CMP3750M Assessment 1
Brandon Broadway
18685301

# How does the tool operate?

## Installation

1. If you do not already have a python environment set up, please download Python 3.X and visual studio community. Also download the DDOSDetector (Named CMP3750M)
2. After you have installed these, open CMP3750M.sln file and click on “Manage Packages” and click “install pip” then type win10toast, then click “Pip install win10toast”
3. After these steps press F5 or the run button to run the program.
4. After the initial setup you will only need to open the CMP3750M.sln file and run it

## Operation Details

The program uses the system function in the os module to send a packet to a target server which is decided by the user while the program is running. If the server returns a response the program will inform the user of ICMP vulnerabilities and wait five minutes before sending another ping, if the server does not respond it will inform the user that there is a potential DDOS attack using a push notification from the win10toast module..

## Code

```
import os
from win10toast import ToastNotifier
import time
#initialisation
ICMPWarning = "\nThis network is vulnerable to ICMP attacks, please disable ICMP unless it is
needed"
notif = ToastNotifier()
running = 1
#get hostname
print("Enter a hostname:\nEG: youtube.com")
hostname = input()

while running == 1: #loop forever
    response = os.system("ping " + hostname)#ping hostname

    if response == 0:
        print(ICMPWarning)#warn user about ICMP vulnerabilities
        time.sleep(300) #wait 5 mins
    else:
        notif.show_toast("Server Downtime detected!","Potential DDOS attack")#notify user of
downtime
```

# What are DDOS attacks?

DDOS attacks are a significant threat to any network or business, these attacks take advantage of security flaws that are very difficult to prevent (Wilde, 2015). Volumetric attacks flood the open ports on a target network until the target machine is overwhelmed and unable to function. This happens using two main protocols: User Datagram protocol (UDP) is a high-speed data transmission protocol that does not check the data it receives (Cloudfare, C, 2017), this makes it extremely vulnerable to a threat actor targeting a network (Dobran, 2018). Internet control

message protocol (ICMP) is used in the “flood” style of DDOS attack, when a device sends a ping to a target server the target server is forced to send a reply to the sender, so by sending many ping requests you can overwhelm a server. (Cloudflare, A, 2017)  IMCP can also be used in a “Ping of death attack” this is where a attacker will send a packet over 110,000 bytes to the target server which will cause the target to freeze, crash or reboot. This works because the normal maximum size is 65,538 bytes and are not prepared to deal with packets larger than this (Cloudflare, B, 2017). ICMP attacks can be mitigated by either disabling ICMP on a router (Cloudflare, A, 2017) or creating a large memory buffer which can handle larger than normal packets. There are also other less common methods of DDOS attacks

## Why is the tool important for the business?

Being aware of when a DDOS attack could be occurring is a vital tool to be able to diagnose downtime and can be used to help identify if a network is vulnerable to ICMP attacks. If an attack was to go undetected it could have significant financial repercussions and could cause the airline to lose customers and gain a bad reputation for being unreliable.

## Impact of a DDoS attack

A DDOS attack could have large, potentially extremely expensive consequences. Website downtime could negatively affect your SEO ranking which could mean losing out on potential business, if the website is not quickly protected. (McCollin, 2020). A DDOS attack could also open other vulnerabilities, particularly with WordPress. A breach like this could be potentially catastrophic as the airline could lose customer data, or their whole website, to a malicious actor. DDOS threats can also create a terrible user experience, for example during Christmas 2014, the XBOX and PlayStation servers were taken offline during an attack from the Blackhat “Lizard Squad” hacking group. This prevented hundreds of thousands of game consoles from being set up, which had large financial repercussions for both Microsoft, Sony and the consumer, who lost time on subscription services they purchased while the attacks were occurring, for example Xbox live Gold or PlayStation Plus which could drive the customer to use an alternative service (Ingram, 2019).

If the airline was to be targeted by a DDOS attack they would lose on average £10,958.90 a day based on their £4 million profit figure. This figure does not account for peak times or seasons, however it still represents the huge amount of money they could potentially lose to a competitor during site outages. It could also lead to loss of revenue in bookings that needed to be adjusted but could not be due to the DDOS attack. The average DDOS attack lasts for 4 hours which would make the airline lose approximately £1800. However, some DDOS attacks have been reported to have lasted over 10 days which could potentially cost over £110,000 (Cook, 2021).

CMP3750M Assessment 1
Brandon Broadway
18685301

# How will the tool help to protect the business?

By identifying if ICMP is enabled, this tool helps to prevent a variety of attacks, including CVE-2016-10142, in which a threat actor could trick a router into dropping legitimate traffic, or CVE-2015-3913 where a forged ICMP packet can force some Huawei switches to reset . These vulnerabilities are not limited to DDOS attacks however, CVE-2014-8533 allows a malicious user to execute arbitrary code through ICMP packets through an old version of McAffe Network Data Loss Protection (Mitre, 2020). This attack could cause a potentially unrecoverable amount of damage to the airline. An attack like this could be prevented by disabling ICMP entirely and relying on protocols that use the transport layer such as TCP and UDP.

DDOS attacks often go commonly undetected until a customer informs the websites owners to the attack, so having a tool that can run in the background and detect when a DDOS attack occurs is a useful tool in reducing downtime, which will allow the user to respond to attacks as fast as possible.

# References

B, Dobran. (2018) 7 Tactics To Prevent DDoS Attacks & Keep Your Website Safe. 10 September. Available from: https://phoenixnap.com/blog/prevent-ddos-attacks [Accessed 17 March 2021]

Cloudfare A (2017) Ping (ICMP) Flood DDoS Attack. Available from: https://www.cloudflare.com/en-gb/learning/ddos/ping-icmp-flood-ddos-attack/ [Accessed 17 March 2021]

Cloudfare B (2017) Ping of Death DDoS attack. Available from: https://www.cloudflare.com/en-gb/learning/ddos/ping-of-death-ddos-attack/ [Accessed 17 March 2021]

Cloudfare C (2017) Ping of Death DDoS attack Available from: https://www.cloudflare.com/en-gb/learning/ddos/glossary/user-datagram-protocol-udp/ [Accessed 17 March 2021]

R. McCollin (2020) DDoS Attacks Explained: Causes, Effects, and How to Protect Your Site. 26 October. Available from: https://kinsta.com/blog/what-is-a-ddos-attack/ [Accessed 17 March 2021]

D, Ingram (2019) How Christmas became one of the biggest days of the year for hackers. December 24. Available from: https://www.nbcnews.com/tech/tech-news/how-christmas-became-one-biggest-days-year-hackers-n1106451 [Accessed 17 March 2021]

Mitre (2020) CVE Database. Available from: https://cve.mitre.org/cve/search_cve_list.html [Accessed 17 March 2021]

S, Cook. (2021) DDoS attack statistics and facts for 2018-2021. 10 February. Available from: https://www.comparitech.com/blog/information-security/ddos-statistics-facts/ [Accessed 17 March 2021]

T, Wilde (2015) Why are DDoS attacks so hard to stop? 3 February. Available from: https://www.pcgamer.com/uk/why-are-ddos-attacks-so-hard-to-stop/ Accessed 17 March 2021]