**DDoS and DoS Report**

**Report for DDos Dos Attack Testing**

Khai Phan (100901164), Marco Rico (111708178),

Carlianz Pura (104375167), Andriy Yevseytsev (131845158)

Information Security (BTN710 - NAA)

Professor Navid Esfahani

Summer Semester, 2020

Table of Content

[**Section 1 - The Exploit (Summary)**](#_3gj20vgsfu7y) **3**

[**Section 2 - The Attack**](#_9a16j5vqb2jt) **4**

[**Section 3 - Security Policy**](#_vebagap2t1wa) **7**

[**Bibliography**](#_tk0nwutux1xl) **9**

# Section 1 - The Exploit (Summary)

There are two ways to do DDoS attacks, direct and indirect. The direct method will be the attacker sending a script to the botnet and let it execute to the target. The indirect attack will log into another computer, like a chain-of-attack, and use that to assign the scripts to the botnet. The indirect way will be hard for the victim to trace back to find the attacker, although the attacker might lose some power through the chain of the computer accessing. The direct way, however, will allow the attacker to intervene if there is an issue and be able to control the script without any interruption. In this testing scenario, we will use the direct way to attack the host target.

The environment we will test our attack is Windows 10 with no specific version. Since this is just small testing, the windows version doesn’t really matter.

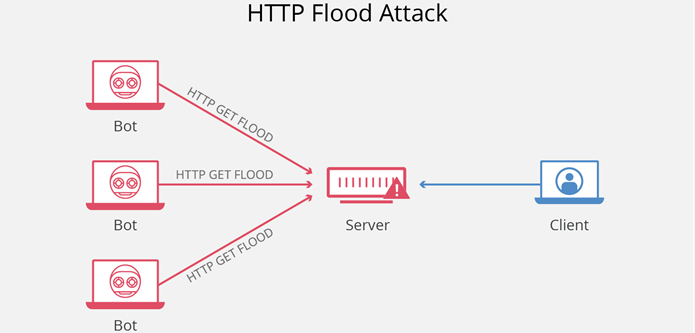
In the real environment, botnets are illegal in some countries. Consider that botnet is a chain of infected computers (can be malware, hidden virus, etc.) used in an Internet attack created by the attackers. However, those are not free. To set up testing that doesn’t cost much, we will use one of the free software and that software can only use the resources from the attacker to pursue an attack.

The application we will use for this attack is HULK (Http Unbearable Load King). So far, there is only one version of the program, so version/numbers and patch level are not applicable. HULK will take any address that you want to attack and send the request to the target. Since it is a free version, it cannot make any massive attack like 1GB/s bandwidth and above to websites like Facebook or Google (those targets are built to stand any attack above 100GB/s bandwidth or even more). What HULK will do is send requests to the target. At first, the target will be able to resolve the connection. However, as more requests are generated, the server will have a long queue of connections waiting to resolve. At some point, the website will be down because there are too many requests.

As we only have the free version, it isn’t sufficient to attack any hosted website since it would require a lot of bandwidth and hosts to join the attack simultaneously (like botnet). Therefore, we will be doing DoS instead of DDoS (single attack) and plan to host it locally. The same method and logic would apply the same for DDoS, as DoS is a DDoS subset.

There are many different variants to carry with this attack. Traditionally, attackers will generate all of the resources they have and shut down the target as fast as possible. Some attackers prefer to take it slow to convey the message to the victim. However, it can’t be too slow that the victim has enough time to stop the attacker. For this report, we will mainly use HULK, as it is easy to test with a fixed amount of attack requests per second and amount of bandwidth usage. If possible and time permits, we would like to carry out a different tester, which allows us to modify the bandwidth usage and delay between each attack. The program is called hping3. As to remember, the software we use will use our resources to handle the attack, and it will be a matter if we use too many resources as our devices will not be able to handle the attack.

# Section 2 - The Attack

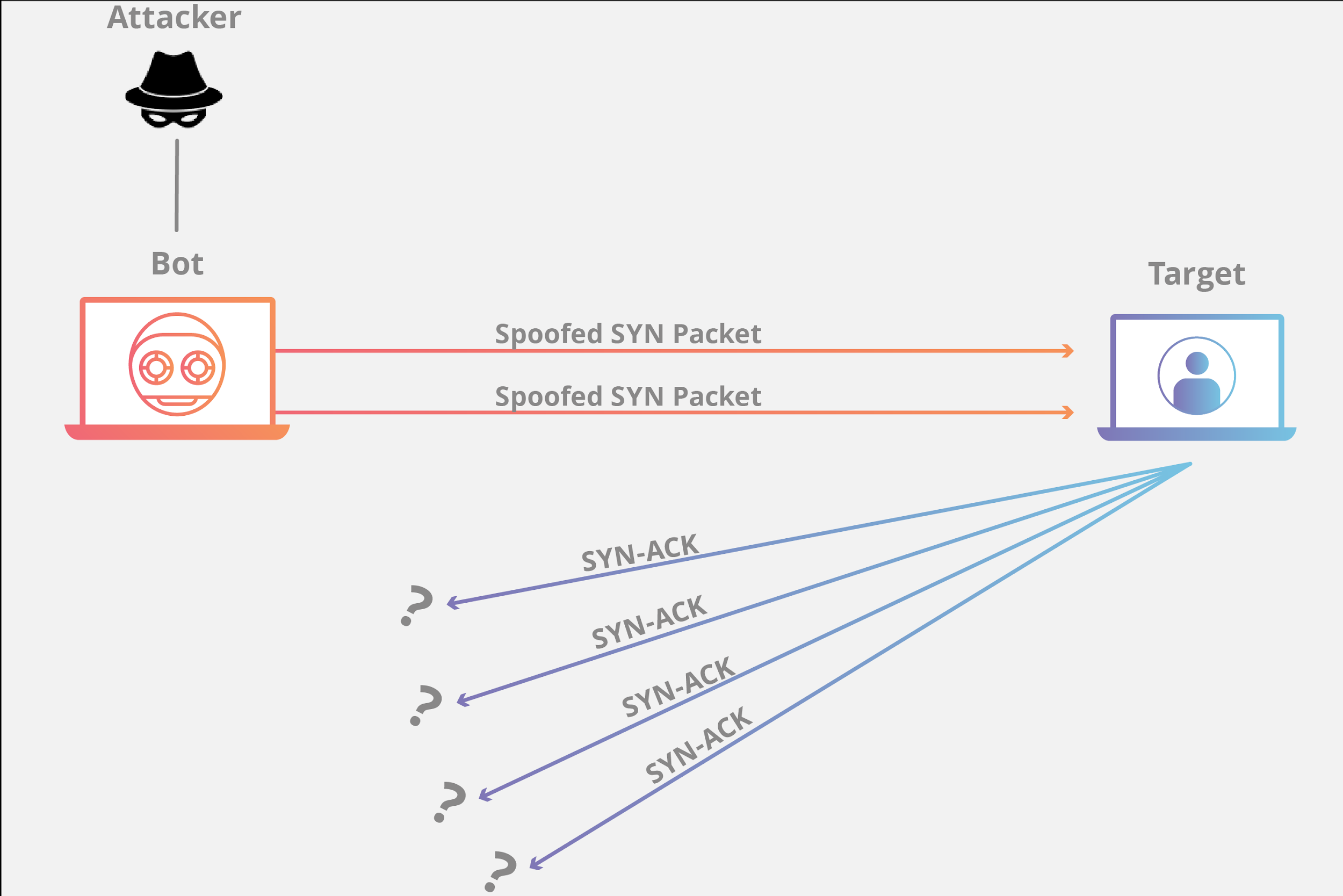


An HTTP flood attack is considered as a “layer 7” DDoS attack where the application layer of the OSI model is affected. To achieve maximum efficacy, attackers usually utilize or create botnets to drastically overwhelm a web server with HTTP requests. Additionally, this type of attack is most effective when it forces the server or application to allocate the most amount of resources to every single request. The attack tool we are using is HULK (HTTP Unbearable Load King is a web server DoS attack tool and is designed to generate large amounts of unique and obscure traffic to a web server (*HTTP Flood DDoS Attack*, n.d.).

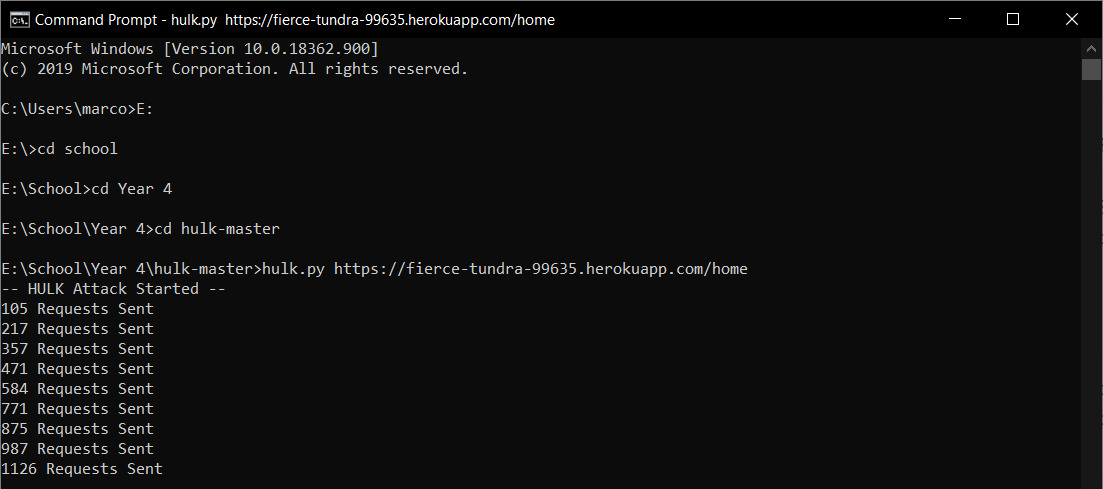
Web servers that utilize Hypertext Transfer Protocol are easily exploited to denial-of-service attacks. HTTP is the basis for loading web pages and used to transfer data over the web. When a client initiates an HTTP GET request to a server a TCP connection must be established in order for a client to obtain a web server response. The first process in an HTTP GET request requires a web server to listen to an incoming connection. Next, a socket queue is assigned to serve the request. The socket queue is responsible for holding the HTTP GET request until a dedicated thread is assigned. Then, request queue processes and responds to individual requests and then the web server sends an HTTP response. Web servers do not have a filtering mechanism to determine authentic HTTP GET requests and therefore during a flood attack, a web server will continuously receive and process these requests. As a result, request queues become flooded and drops incoming requests from authentic users (“What Is an HTTP Flood” n.d.).

Also, outline each stage of an attack, including reconnaissance, scanning, exploiting the system (gaining access, elevating access, application-level access and/or denial of service). For each stage, provide details of the steps you performed, the commands that you typed, the tools that you used, and why each step was performed. Use as many screenshots as possible to document the process. Your documentation should be so clear that someone could take your report and reproduce the attack.

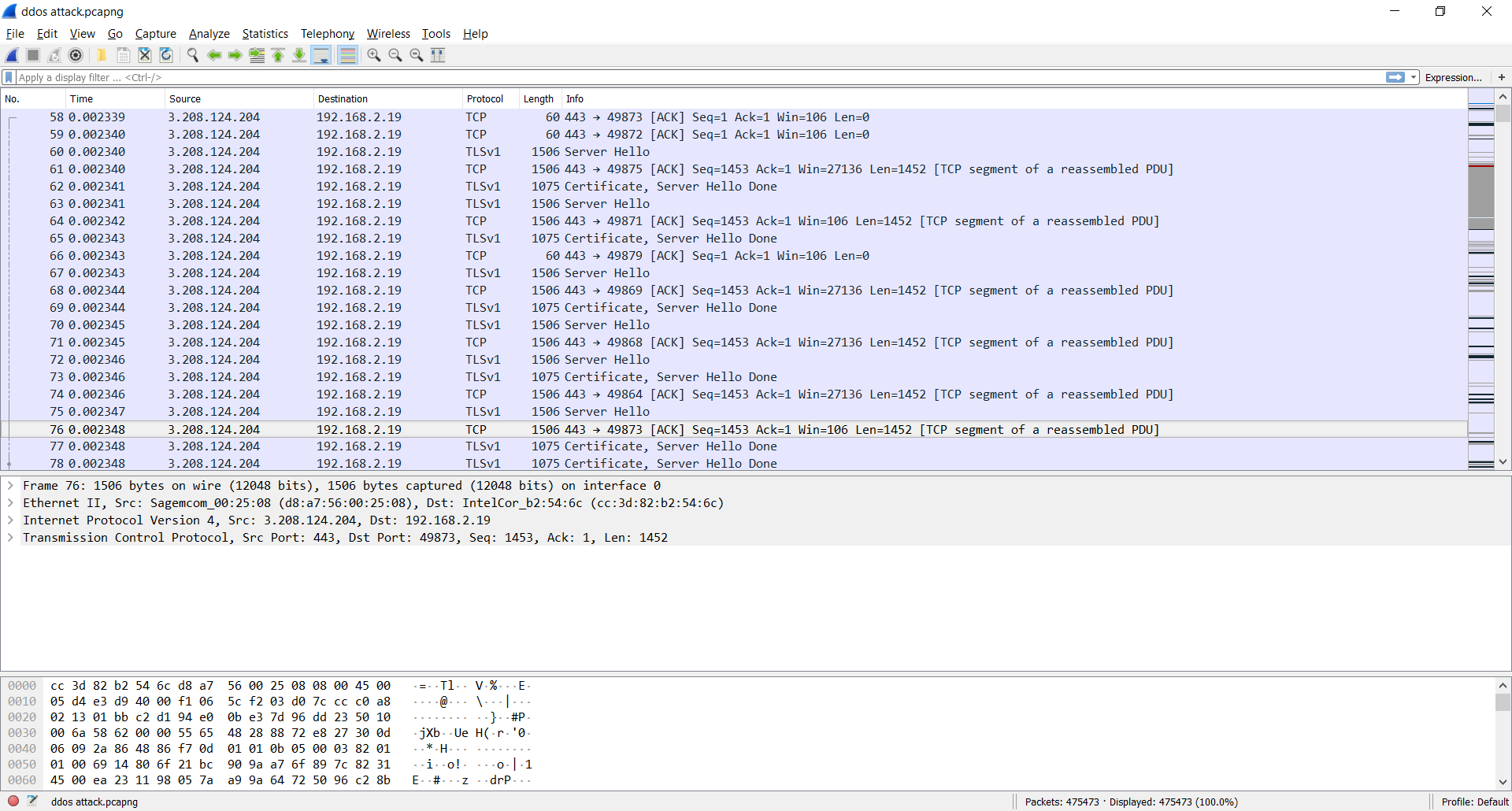
The protocols at the application layer have many vulnerabilities to HTTP flood DDoS attacks. The main reason for this vulnerability is because HTTP flooding attacks are hard to distinguish. The HTTP protocol uses TCP and UDP connections to operate and thus makes it difficult to differentiate from valid traffic. Also, this attack requires less bandwidth than other attacks and can often remain undetected while carrying out attacks (*What Is an HTTP Flooding Attack?* n.d.).

For our attack, we are planning to locally host our website (we cannot find a host willing to let us DDoS it) and use tools to launch an attack on it inside of the local network. This diagram shows what one of the computers will be doing on the network, and that will be flooding packet requests. We will have multiple machines doing this towards the target. 

For our attack, we are planning to use a few tools to do the attack on our website. The main tool we are using is called Hulk. Hulk (Http Unbearable Load King) is an open-source DDoS attacking tool that has the ability to bypass the website caching and hit a website's back-end servers with continuous and high volumes of unique and confusing traffic to the system. With this tool, we are planning to use it as the tool to overload our website’s server with packets for the attack. The tool will also let us know when the website starts to return 503 errors because it was successful in its attack.



This was a test done on a past Heroku website project. Once the specified URL link is inserted, the program gets to work and launches the attack, it then displays how many request packets have been sent to the website every few seconds. Now, looking at this example and using Wireshark, we can see the packets being sent.



As seen in the capture using Wireshark, Hulk creates a unique packet every time for sending to help keep the host system from knowing it is an attack (More on this in the next section).

With a DDoS attack, there is nothing left on the affected system as with a DDoS attack, we are just overloading the system with packets, these packets do not leave a trace in the system. This attack also does not have a signature that could really be traced. For starters, a system manager is going to have a hard time distinguishing if there is a DDoS attack going on or just an uptick in traffic to the server. Also, with some changes to packets, packets can be completely unique and not have similarities between them causing systems to have trouble creating a pattern to help distinguish real user packets from attacker packets.

Since HTTP flood attacks are hard to distinguish from real incoming traffic, the most effective mitigation techniques involve a combination of traffic profiling methods. One technique involves establishing an IP reputation database to identify and deny the suspicious activity. Additionally, implementing security challenges such as JavaScript computation challenges can be used to test if a bot is being used and thus mitigating the attack (Jaafar et al., 2019).

# Section 3 - Security Policy

The main goal of hackers is to make the attacked resource inaccessible to the user, to do this, a huge number of false requests are sent to the server, which the server is not able to process, and as a result, the website "drops itself" and instead of the usual page, the user sees a static page with an error message. To generate malicious traffic (which is a DDoS attack), most often a large number of devices are infected with a special code and these devices are combined into botnets that send requests to the attacked address.

There is a solution - it is both independent and professional protection against DDoS, including services of specialized companies. But it is important to understand that universal protection measures against DDoS attacks do not exist, hackers are constantly finding new vulnerabilities and ways to trick security systems.

Here are the most popular protection methods against DDoS attacks that should be included in the policy:

1. A firewall is a filter system that helps protect the site from junk traffic before it even gets to the site. The main function of the firewall is the fight against viruses. It also protects against DDoS somehow, but for weak attacks, it is enough. Moreover, it will cost less than a fully equipped Anti-DDoS.
2. Anti-DDoS is more flexible and intelligent than a regular Firewall. The system automatically arranges filters depending on the type and power of the attack and is able to conduct additional manipulations with traffic. This Anti-DDoS ​​service is offered by hosters whose servers are already connected to the protection system. Advantages of Anti-DDoS: one common bill for all services from the hoster and the fact that all settings are performed by the provider’s specialists.
3. Protected IP transit through a virtual tunnel. This service is suitable for projects with large volumes of traffic, to protect against the junk traffic of the entire autonomous system at once. This is an expensive service used by data centers, hosting providers, domain name registrars, telecom operators that do not have their own filtering stations.

There are also preventive some measures that can help you:

1. Do not save money on hardware. Spend a little more money on a more expensive hosting and server. Pay attention to the channel width and the number of CPUs. As a rule, these resources are "destroyed" during DDoS. This will not save you from large and planned attacks, but it will definitely protect you from an inexperienced hacker. You can still be saved using the cloud hosting service, with its help you can add the missing resources at any time.
2. Configure the software on your server. Use traffic distribution between two web servers. (For example Apache and Nginx proxy).
3. Optimize the queries. Try to avoid heavy queries by refactoring the code, adding the missing indexes to the databases, and more. When there are too many of them, the probability of server failure is high, even without a DDoS attack.
4. Track the number of requests per second. Look at the number of requests per second. They grow if a massive botnet arrives, and fall if a botnet leaves that crashes the site, making it completely inaccessible to legitimate users. But we are talking about severe changes in website indicators.

# Bibliography

**Exploit Host:** <https://fierce-tundra-99635.herokuapp.com/home>

Blog, R. (2019, January 7). 3 Tools to Test Denial of Service Vulnerability. Retrieved July 11, 2020,

from <https://www.redlegg.com/blog/3-tools-to-test-denial-of-service-vulnerability>

Cucu, P. (2019, October 04). How to DDoS Like an Ethical Hacker. Retrieved July 11, 2020, from

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

E. (n.d.). HULK - Web Server DoS (Denial of Service) Tool. Retrieved July 11, 2020, from

<http://www.effecthacking.com/2017/11/hulk-web-server-dos-tool.html>

*HTTP Flood DDoS Attack*. (n.d.). Cloudflare. Retrieved July 9, 2020, from<https://www.cloudflare.com/learning/ddos/http-flood-ddos-attack/>

I. (2019, December 29). DDoS for Hire: Booter, Stresser and DDoSer: Imperva. Retrieved

July 11, 2020, from https://www.imperva.com/learn/application-security/booters-stressers-ddosers/

Jaafar, G. A., Abdullah, S. M., & Ismail, S. (2019, January 10). *Review of Recent Detection Methods for HTTP DDoS Attack* [Review Article]. Journal of Computer Networks and Communications; Hindawi.<https://doi.org/10.1155/2019/1283472>

What is an HTTP Flood | DDoS Attack Glossary | Imperva? (n.d.). *Learning Center*. Retrieved July 9, 2020, from<https://www.imperva.com/learn/application-security/http-flood/>

*What is an HTTP Flooding Attack?* (n.d.). NETSCOUT. Retrieved July 9, 2020, from<https://www.netscout.com/what-is-ddos/http-flood-attacks>

What is a DDoS Attack? Retrieved July 9, 2020, from

<https://aws.amazon.com/shield/ddos-attack-protection/>

7 Tips for Defending Your Network against DDoS Attacks Retrieved July 9, 2020, from

<https://www.corero.com/blog/7-tips-for-defending-your-network-against-ddos-attacks/>

How to Prevent DDoS Attacks: 6 Tips to Keep Your Website Safe Retrieved July 9, 2020, from

<https://www.esecurityplanet.com/network-security/how-to-prevent-ddos-attacks.html>

Six Steps to Defend Against DDoS Attacks Retrieved July 9, 2020, from

<https://www.a10networks.com/blog/how-defend-against-ddos-attacks-six-steps/>