DDOS DETECTION USING ML

BY
Raed Hermessi

Introduction

Distributed Denial of Service (DDoS) attacks are very common nowadays. It is evident that the current industry solutions, such as completely relying on the **Internet Service Provider (ISP)** or setting up a DDoS defense infrastructure, are not sufficient in detecting and mitigating DDoS attacks, hence consistent research is needed. In this article we're gonna first try to understand how DDoS attacks happen, then we're gonna to discuss a way to detect DDoS attacks using machine learning tools.

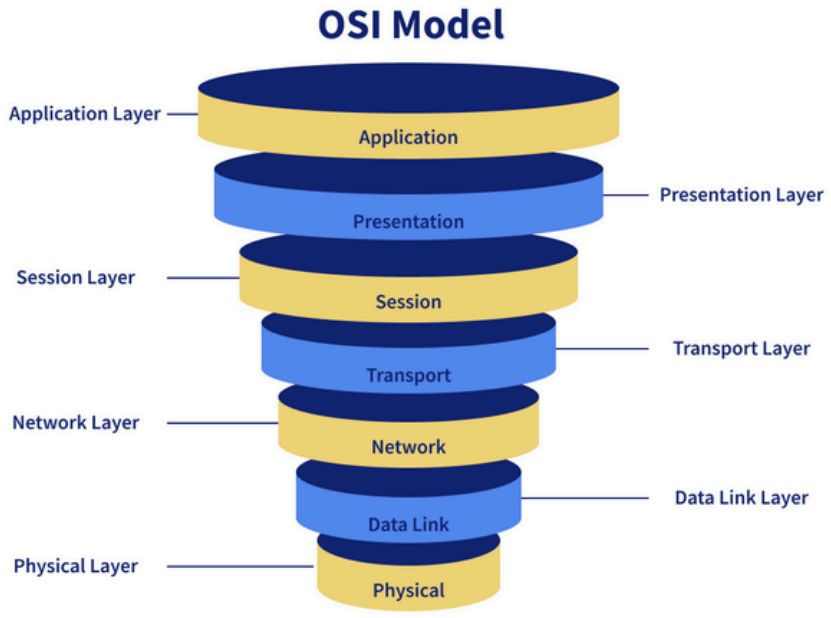
Contents

1.1 what is DDOS attack ?

A Distributed Denial of Service (DDoS) attack is a way to jam a host network or its resources with a large number of data packets or connections, so that the host becomes disabled.

1.2 some common types of DDoS attacks

Different types of DDoS attacks target varying components of a network connection. In order to understand how different DDoS attacks work, it is necessary to know how a network connection is made.
A network connection on the Internet is composed of many different components or “layers”. Like building a house from the ground up, each layer in the model has a different purpose.
The OSI model, shown below, is a conceptual framework used to describe network connectivity in 7 distinct layers



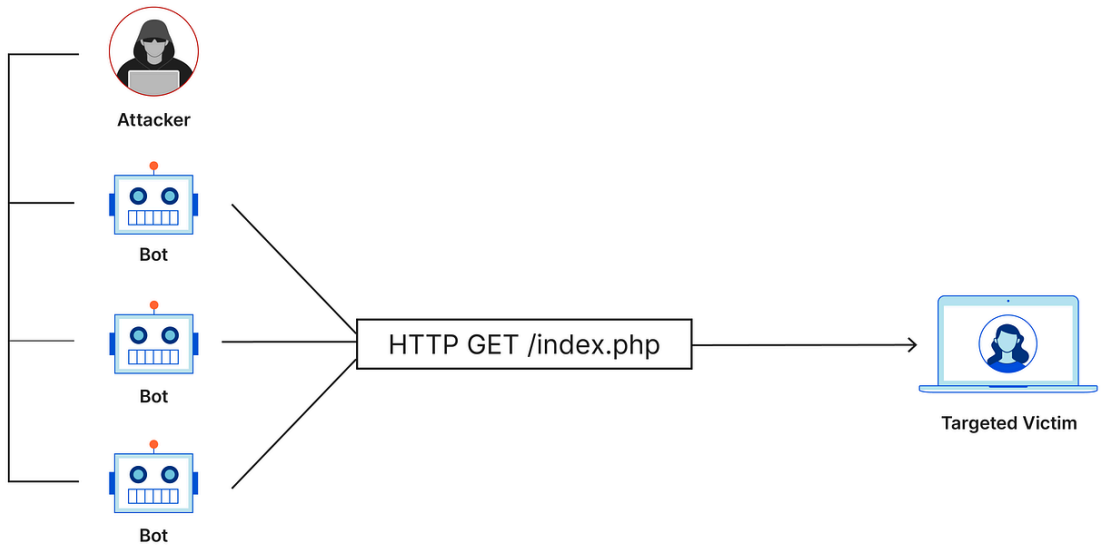
While nearly all DDoS attacks involve overwhelming a target device or network with traffic, attacks can be divided into three categories. An attacker may use one or more different attack vectors, or cycle attack vectors in response to counter measures taken by the target.

1.2.a Application layer attacks :

The goal of the attack:

Layer 7 DDoS attacks, often referred to in connection with the 7th layer of the OSI model, aim to deplete a target's resources, leading to a denial-of-service. These attacks specifically focus on the layer responsible for generating web pages on the server and responding to HTTP requests. While a single HTTP request is relatively inexpensive for the client, the server's response can be resource-intensive, involving the loading of multiple files and execution of database queries to construct a web page. Defending against Layer 7 attacks proves challenging, as distinguishing malicious traffic from legitimate traffic can be complex.

Application Layer attack example :



HTTP flood:

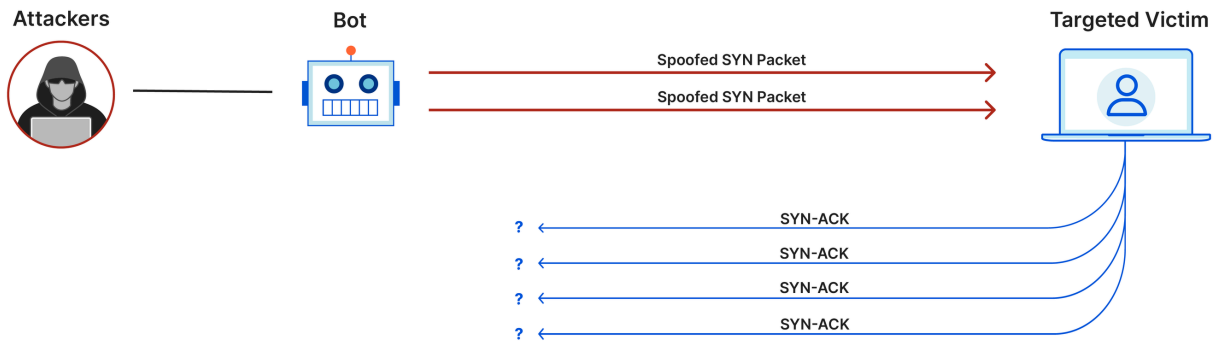
An HTTP flood attack is like repeatedly hitting the refresh button on a web page, but from many different computers all at once. This overwhelms the server with a huge number of requests, causing it to stop working properly.
There are simpler versions of this attack where a group of computers all access the same web page using the same tricks. More complex versions involve many computers targeting different parts of a website with different tactics to make it even harder to defend against.

1.2.b Protocol attacks :

The goal of the attack:

Protocol attacks, also known as a state-exhaustion attacks, cause a service disruption by over-consuming server resources and/or the resources of network equipment like firewalls and load balancers.
Protocol attacks utilize weaknesses in layer 3 and layer 4 of the protocol stack to render the target inaccessible.

Protocol attack example:



SYN flood Attack:

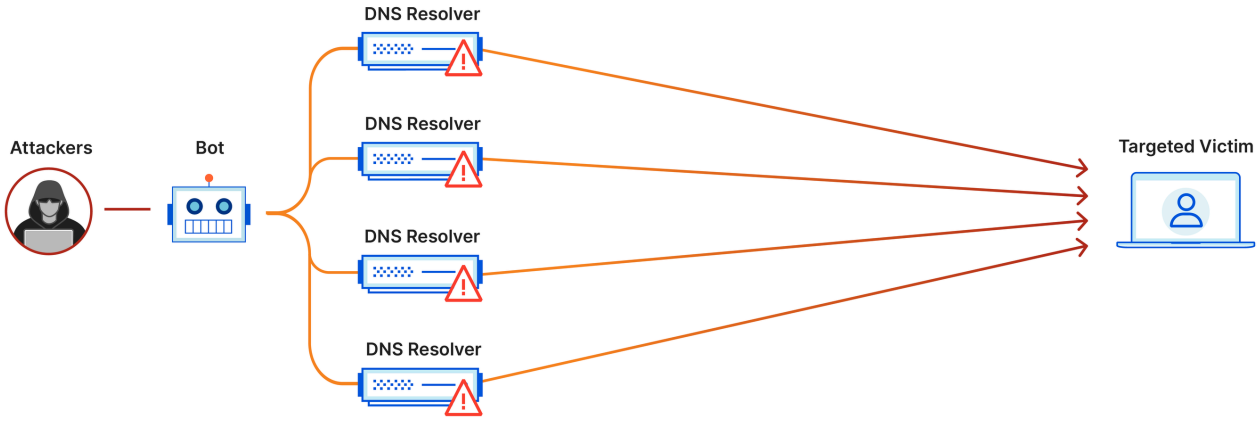
A SYN flood attack is a type of TCP State-Exhaustion Attack that attempts to consume the connection state tables present in many infrastructure components, such as load balancers, firewalls, Intrusion Prevention Systems (IPS), and the application servers themselves. This type of DDoS attack can take down even high-capacity devices capable of maintaining millions of connections.

1.2.c Volumetric attacks :

The goal of the attack:

This category of attacks attempts to create congestion by consuming all available bandwidth between the target and the larger Internet. Large amounts of data are sent to a target by using a form of amplification or another means of creating massive traffic, such as requests from a botnet.

Amplification example:



DNS Amplification:

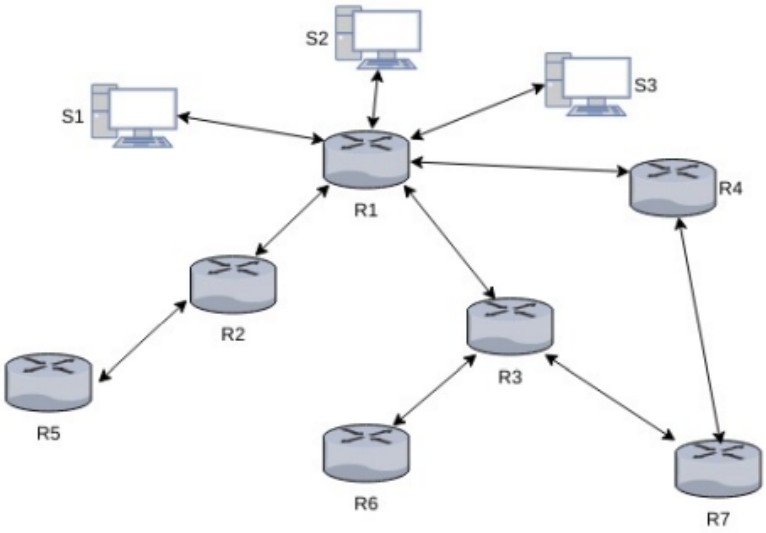
A DNS amplification attack is like making lots of phone calls to a friend using a speakerphone. You ask your friend to repeat what you say, but you use many speakerphones at once. This makes your friend's voice really loud and overwhelms them. In the same way, attackers send requests to a bunch of computers, pretending to be someone else, and those computers respond with much more data than the attacker asked for. This floods the target with a huge amount of unnecessary information, causing a problem

1.3 DDOS attack detection and mitigation

A DDoS attack detection and mitigation A DDoS attack can be detected by checking if there is any anomalous behavior in the network traffic, such as, a sudden increase in the number of packets going to a destination. Detection can occur at the server by observing all of the incoming traffic or it can be done by observing all of the outgoing/incoming traffic at the ISP or at every router. The attack can be mitigated if the anomalous packets are blocked from reaching their destination.

2.1 Network functioning

A switch creates a network and a router connects those networks. A router links a computer to the Internet through other routers. Routers are the backbone of the network that helps to forward packets from one point to another point on the Internet. Every packet traveling on the Internet goes through a router . A router knows the destination of a packet, hence it could serve as a first point of knowledge about the change in the packet flow information for a destination. Each router has interfaces to which hosts or other networks are connected. So, a router is aware to what it is connected. It uses protocols to communicate among other routers and by that it gathers knowledge about other routers on the Internet. Internet Control Message Protocol (ICMP) is one of the most frequently used protocol by routers for sharing operational information



Network example

In the above figure we can see that three computers (S1, S2, and S3) are connected to a main hub (R1), acting like a traffic controller. This hub is connected to the Internet through three other hubs (R2, R3, and R4). When data goes to computer S2, it passes through one of these three hubs. These hubs are in different places on the map. Most websites are designed for specific areas, like a town, state, or country (except for global sites). So, when you visit a website, the data often comes from a hub in that same region.

As the article title suggests, 'DDOS attack using ML,' we need to delve further into machine learning concepts. In this section, we will explore machine learning algorithms and conclude by examining their use in detecting DDOS attacks

3. Machine Learning ? never heard of it !

3.1 what is machine learning ? :

Machine learning is a field of study in artificial intelligence concerned with the development and study of statistical algorithms that can learn from data and generalize to unseen data, and thus perform tasks without explicit instructions.

3.2 ML algorithms :

KNN :

K-Nearest Neighbor (K-NN) is one of the simplest Supervised Machine Learning algorithms which presumes the similarity between existing data and new data and put the new case into the category that is most like the available ones. It classifies a new data point based on the similarity of stored available data i.e., when any new data appears then it can be easily classified into a well-suited category by using K- NN algorithm. The KNN classifier has the ability to effectively detect invasive attacks as well as achieve a low fall-out ratio. It can distinguish between the normal and abnormal behavior of the system and is used to classify the status of networks to each phase of DDoS attack.

Support Vector Machines :

Support Vector Machines (SVM) is one of the most favored ML algorithms for many applications, such as pattern recognition, spam filtering and intrusion detection. There are several SVM formulations for regression, classification, and distribution estimation. It is derived from linearly separable and the most optimal classification hyperplane. There is a training set D = {(X1, y1), (X2, y2) .... (Xn, yn)}, where Xi is the characteristic vector of the training sample and yi is the associated class label. takes +1 or −1 (y belongs to {+1, -1}) indicating that the vector belongs to this class or not. It is said to be linearly separable if there exists a linear function that can separate the two categories completely; otherwise, it is nonlinearly separable. As DDoS attack detection is equivalent to that of a binary classification problem, we can use the characteristics of SVM algorithm collect data to extract the characteristic values to train, find the optimal classification hyperplane between the legitimate traffic and DDoS attack traffic, and then use the test data to test our model and get the classification results

Random Forest :

The Random Forest classifier makes use of ensemble learning technique as it constitutes of many decision trees. All the individual trees present as a part of random forest provide a class prediction. Subsequently, the class with the highest number of votes becomes the prediction of the entire model. The core idea of the classifier is to have a significant number of trees which operate together as a whole to outperform any of the individual constituent models. The key is low correlation between the models. Uncorrelated models have the capability to produce more accurate models than any of the individual predictions. The main reason is that the trees protect one another from individual errors. While some trees might be wrong, if many other trees are right, then, the group of trees would be able to move towards the right direction. The classifier makes use of feature randomness and bagging to build each individual tree to create an uncorrelated forest of trees.

4. Approach

The implementation of machine learning (ML) to detect Distributed Denial of Service (DDOS) attacks involves several key steps. Initially, a robust dataset representing normal network behavior is collected and used to train the ML model. This dataset encompasses a variety of network attributes, such as packet sizes, request rates, and traffic patterns during regular operation.

The ML model employs various algorithms, including but not limited to decision trees, support vector machines, or neural networks, to learn patterns and relationships within the dataset. This training phase is crucial as it enables the model to differentiate between normal and potentially malicious network behavior.

Once the model is trained, it is deployed to analyze real-time network traffic. The ML system continuously monitors incoming data, comparing it to the learned patterns. Any deviation or anomaly that surpasses a predefined threshold is flagged as a potential DDOS attack. The model adapts over time, continuously learning from new data to stay attuned to evolving attack strategies.

Key features considered during the analysis include the frequency and intensity of requests, geographical origin of traffic, and the diversity of devices generating requests. ML algorithms excel at identifying subtle, complex patterns that may be indicative of a DDOS attack, even when the attack methods evolve.

An added advantage of ML-based DDOS detection is its ability to minimize false positives. As the model becomes more refined through ongoing training, it becomes adept at distinguishing between benign traffic fluctuations and genuine threats. This capability reduces the likelihood of disrupting legitimate user access while efficiently identifying and mitigating DDOS attacks.

5. Conclusion

In summary, ML for DDOS detection involves training algorithms on diverse datasets, deploying them to analyze real-time network traffic, and continuously refining their capabilities to adapt to emerging threats. This approach provides a proactive and dynamic defense against DDOS attacks, enhancing the overall resilience of network infrastructure.

6. References

- https://data.mendeley.com/datasets/jxpfjc64kr/1
- https://www.cloudflare.com/learning/ddos/what-is-a-ddos-attack/
- https://rucore.libraries.rutgers.edu/rutgers-lib/57074/PDF/1/play/
- https://github.com/ReubenJoe/DDoS-Detection/tree/main/DDoS-Detection-main

BONUS: DDOS Attack Simulation

- Step 1 - Attacker System (running Kali Linux) and Target system (running Windows 10 or 7) set up in Oracle VirtualBox.
- Step 2 - Both systems placed in the same subnet - 192.168.100.0/24 (IP address of the attacker system - 192.168.100.4, IP address of the target system - 192.168.100.5
- Step 3 - Connectivity verified using the Ping command.
- Step 4 - List open ports on the target system obtained using Nmap (Command used : **nmap -Pn 192.168.100.5**)
- Step 5 - DDos attack against port 135 of the target system initiated using **Hping3** (Command used : **hping3 -S --flood --rand-source 192.168.100.5 -p 135**