FINAL REPORT

Technology stack: AI for cyber security with IBM Qradar

Project Title: Strengthening Web Server Security: Proactive Measures Against Threats

Team ID: LTVIP2024TMID11381

Team no.: 5

Team Members: 5

1. Kambala durga prasad
2. Jagi Ganesh kumar
3. Burada upendra
4. Palla Charan raj
5. Marpu kanvith

COLLEGE: DR LANKAPALLI BULLAYYA COLLEGE VISHAKHAPATNAM

Index

INTRODUCTION

Web server security is the security of any server that is deployed on a Worldwide Web domain or the Internet. It is implemented through several methods and in layers, typically, including the base operating system (OS) security layer, hosted application security layer and network security layer. OS security, which ensures access to authorized users only, operates a Web server's critical components and services. Application layer security ensures control over the content and services hosted on the Web server. Network security provides protection against Internet-based security exploits, viruses and attacks. The Web Server Security Service Module (SSM) provides an environmental binding between the WebLogic Enterprise Security infrastructure and IIS and Apache web servers. The WebLogic Enterprise Security infrastructure provides six distinct services: Registry, Authentication, Authorization, Auditing, Role Mapping, and Credential Mapping. Each of these services is expressed in a way that is understandable to applications running within a web server that is protected by the WebLogic Enterprise Security infrastructure. Therefore, the SSM can be used to configured and enforce security for web server applications and resources.

The Web Server SSM makes access control decisions for the web server to which it is bound. The security configuration on which the access control decisions are based is defined and deployed by the Administration Server via the Security Control Module.

You can tailor the Web Server SSM to meet your specific needs. Using templates provided as part of the product, security developers can customize the look and feel of authentication pages and configure parameters that allow fine tuning for a particular installation. Web applications can have information added to the HTTP request by the security framework, such as roles and response attributes. Additionally, the Web Server SSM enables security administrators and web developers to perform security tasks for applications running on a web

Secure Sockets Layer (SSL) certificates, HTTP Secure protocol and firewalling are several tools and technologies used to implement Web server security.

ABSTRACT

Web applications are active websites which are composition of server based programs serving user interaction and various other functionalities. Web Server security is thus an important aspect for any organisation having web server connectivity with the internet and also to ensure customers using their websites, for a secure online portal. In this age of digital revolution, there has been a rise in demand of web developers who can produce user friendly web platforms such as mobile applications, web applications. The user base for online web applications is on a rise too. We have seen a huge emphasis on creating visual and catchy web applications but with large amount of sensitive user data at stake there should be more focus on providing web security to the applications developed. website managers, and web content owners who manage IU-owned IT resources must do so in accordance with applicable IT policy and published guidance to promote the security of these resources. The information here details existing policies and other resources that apply to web servers, web server administrators, and web content owners, and explains them in the context of web server administration.

Hosted content must be managed in a manner commensurate with its value as an information asset and to promote appropriate use of information.

As the use of the cloud and web applications expands, it is important to remember that all existing IT policies also apply to new and emerging technologies. These policy requirements for IU web server administrators, outlined in greater detail below, protect the university community by mitigating the risk of malicious attacks, intrusions of privacy, and data breaches. These are divided into categories based on the type of requirement.

Web server administrators must be familiar with IU's information technology policies, and must ensure that their staff are as well.

STAGE-1

Title of the Project: Strengthening Web Server Security Proactive

Measures Against Threats Overview:

A distributed denial-of-service (DDoS) attack is a malicious attempt to disrupt the normal traffic of a targeted server, service or network by overwhelming the target or its surrounding infrastructure with a flood of Internet traffic. here the attacks are withheld on the server

DDoS attacks achieve effectiveness by utilizing multiple compromised computer systems as sources of attack traffic. Exploited machines can include computers and other networked resources such as IoT devices. From a high level, a DDoS attack is like an unexpected traffic jam clogging up the highway, preventing regular traffic from arriving at its destination

DDoS attacks are carried out with networks of Internet-connected machines

These networks consist of computers and other devices (such as IoT devices) which have been infected with malware, allowing them to be controlled remotely by an attacker. These individual devices are referred to as bots (or virus), and a group of bots is called a botnet.

Once a botnet has been established, the attacker is able to direct an attack by sending remote instructions to each bot

When a victim's server or network is targeted by the botnet, each bot sends requests to the target's IP address, potentially causing the server or network to become overwhelmed, resulting in a denial-of-service to normal traffic.

AS WE PERFORM ON XAMPP AND THE FOX NEWS SITE

There are 3 types of DDoS Attacks:

- Volume-based attacks,
- Protocol attacks, and • Application layer attacks.

Low and slow attack tools:

As the name implies, these types of attack tools use a low volume of data and operate very slowly. Designed to send small amounts of data across multiple connections in order to keep ports on a targeted server open as long as possible, these tools continue to take up the server's resources until it is unable to maintain additional connections. Uniquely, low and slow attacks may at times be effective even when not using a distributed system such as a botnet and are commonly used by a single machine.

Application layer (L7) attack tools:

These tools target layer 7 of the OSI model, where Internet-based requests such as HTTP occur. Using an HTTP flood attack to overwhelm a target with HTTP GET and POST requests, a malicious actor can launch attack traffic that is difficult to distinguish from normal requests made by actual visitors.

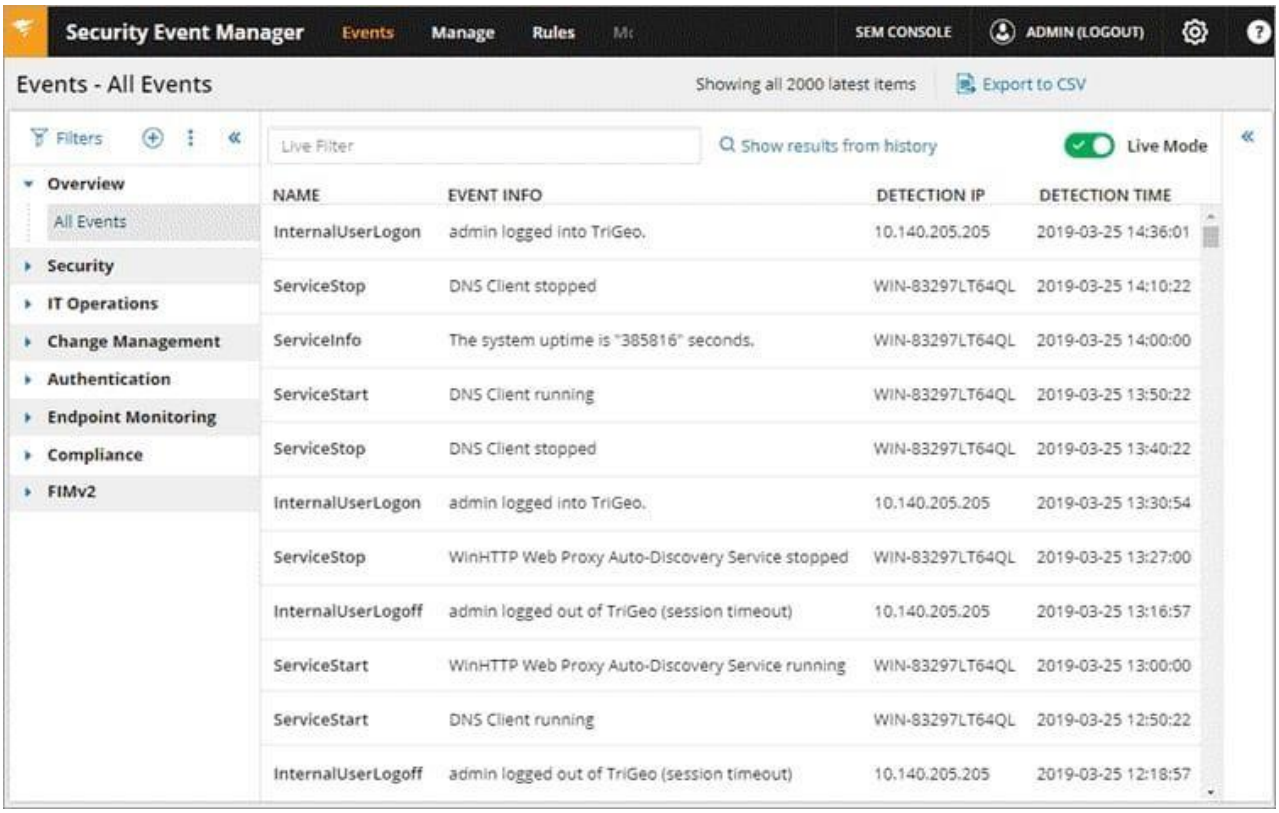
Protocol and transport layer (L3/L4) attack tools :

Going further down the protocol stack, these tools utilize protocols like UDP to send large volumes of traffic to a targeted server, such as during a UDP flood. While often ineffective individually, these attacks are typically found in the form of DDoS attacks where the benefit of additional attacking machines increases the effect.

1) SolarWinds Security Event Manager (SEM)

SolarWinds Security Event Manager
SolarWinds provides a Security Event Manager that is effective mitigation and prevention software to stop the DDoS Attack. It will monitor the event logs from a wide range of sources for detecting and preventing DDoS activities.
SEM will identify interactions with potential command and control servers by taking advantage of community-sourced lists of known bad actors. For this, it consolidates, normalizes, and reviews logs from various sources like IDS/IPs, firewalls, servers, etc. SolarWinds is committed to taking our customers security and privacy concerns seriously and makes it a priority. We strive to implement and maintain security processes, procedures, standards, and take all reasonable care to prevent unauthorized access to our customer data. We apply appropriate administrative, operational, and technical security controls to help ensure that our customer data is handled and processed in a responsible and secure manner.

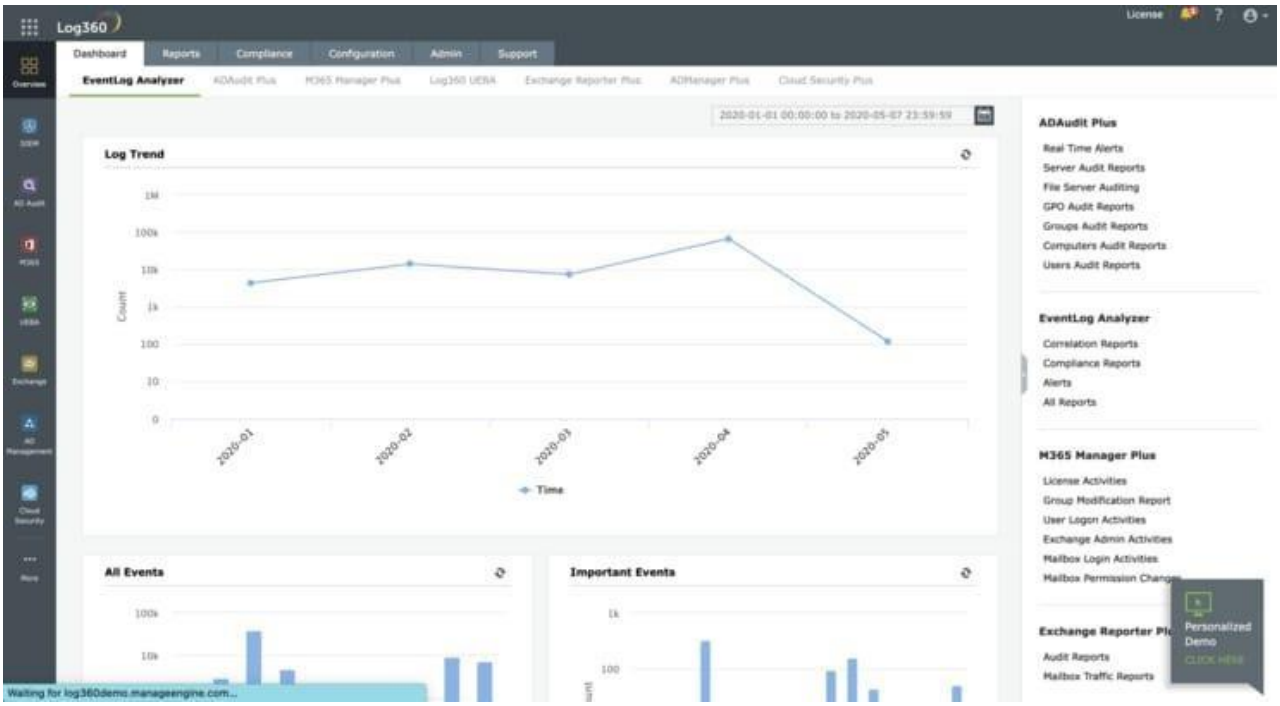
Our security strategy covers all aspects of our business, including:



ManageEngine

ManageEngine Log360 is a comprehensive SIEM solution that allows you to stay one step ahead of threats like DDoS attacks. The platform can help detect shadow apps in your network and take command over sensitive data. The platform also gives you complete visibility into your network.

Thanks to Log360's powerful correlation engine, you get alerted to the existence of a threat in real time. As suc byh, the platform is ideal for facilitating an efficient incident response process. It can quickly identify external threats by leveraging a global intelligent threat database.



HULK

stands for HTTP Unbearable Load King. It is a DoS attack tool for the web server. It is created for research purposes.

Features:

It can bypass the cache engine.

It can generate unique and obscure traffic.

It generates a great volume of traffic at the web server.

Slowloris

tool is used to make a DDoS attack. It is used to make the server down

Features:

It sends authorized HTTP traffic to the server.

It doesn't affect other services and ports on the target network.

This attack tries to keep the maximum connection engaged with those that are open.

It achieves this by sending a partial request.

It tries to hold the connections as long as possible.

As the server keeps the false connection open, this will overflow the connection pool and will deny the request to the true connections

LOIC

stands for Low Orbit Ion Cannon. It is a free and popular tool that is available for the DDoS attack

Features:

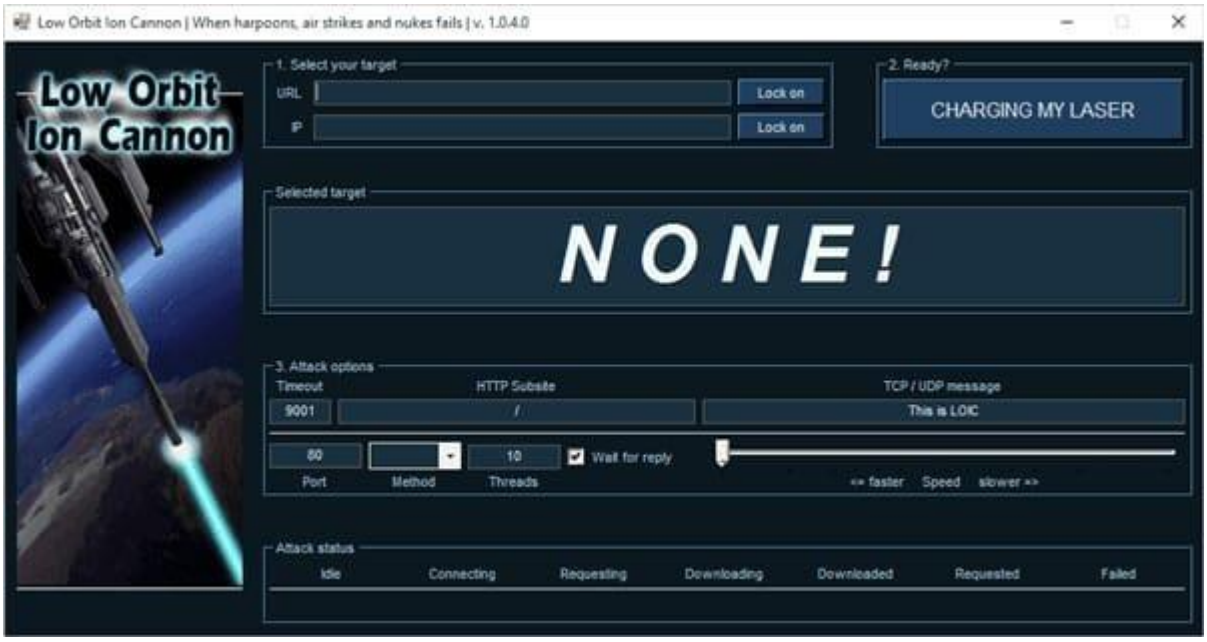
It is easy to use.

It sends UDP, TCP, and HTTP requests to the server.

It can do the attack based on the URL or IP address of the server.

Within seconds, the website will be down and it will stop responding to the actual requests.

It will NOT HIDE your IP address. Even using the proxy server will not work. Because in that case, it will make the proxy server a target.



Stage -2

(attack on the main site) Description:

Having DVWA on XAMPP server on our Windows 8 and using a software to implement brute force attack on DVWA. detect this brute force attack log on XAMPP? Or generally other attacks (e.g. sqli, xss)! xamppbrute-force

find patterns in your Apache access logs (Apache is a part of XAMPP). During a typical "brute force" attack the access logs will find multiple POST requests to a specific log-in page. Have a look at you access log while/after your running a brute force attack

Typically, the access logs wil include multiple login attempts from the same IP address. More advanced, distributed brute forces will connect using various IP's.

A way of preventing these attacks is by limiting the amount of possible logins

How are DoS/DDoS attack tools categorized?

A number of tools exist that can be adapted to launch DoS/DDoS attacks, or are explicitly designed for that purpose. The former category are often ““stressors”” — tools with the stated purpose of helping security

researchers and network engineers perform stress tests against their own networks, but which can also be used to perform genuine attacks.

Some are specialized and only focus on a particular layer of the OSI model, while others are designed to allow for multiple attack vectors. Categories of attack tools include:

The attacking web site is the xampp which is used when even if it is refreshed we don't get the site

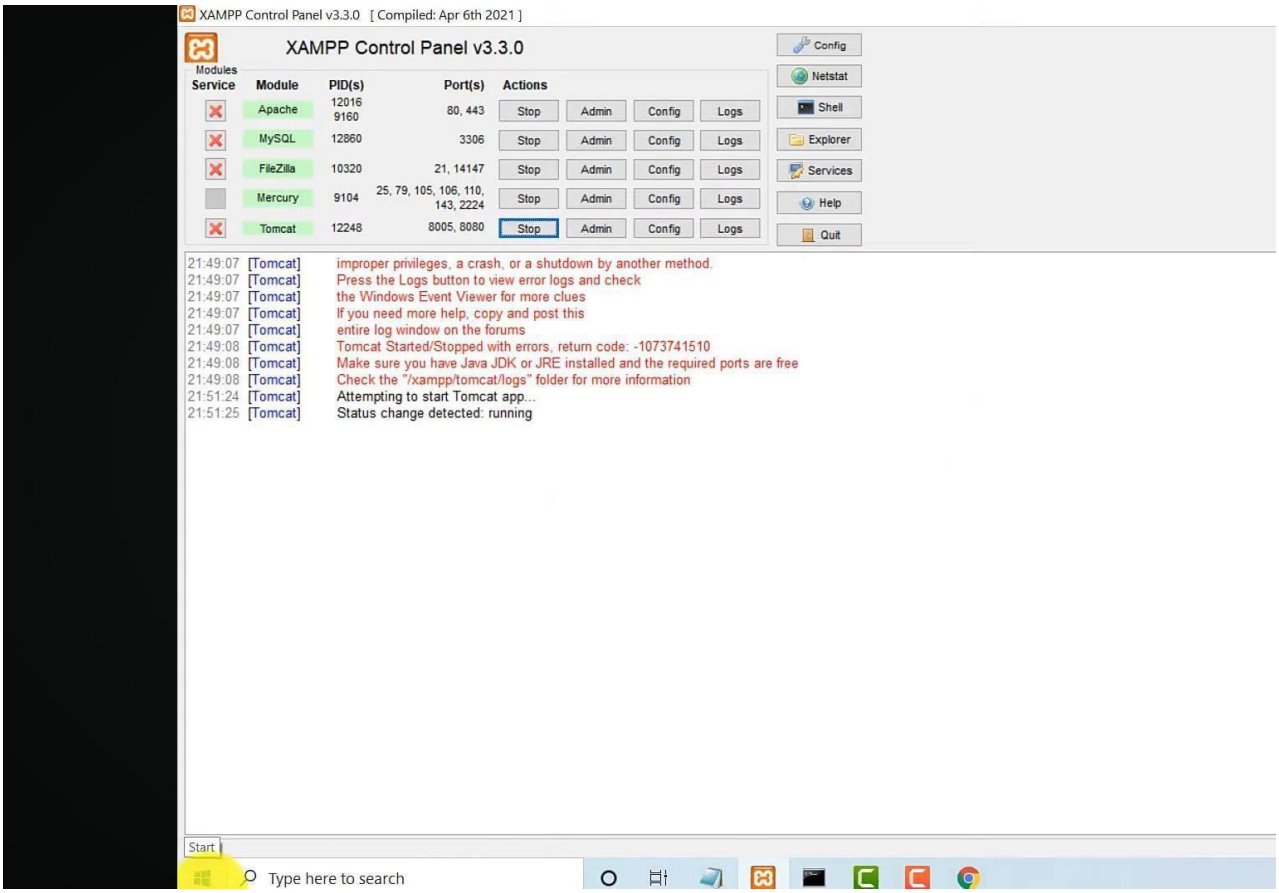
As working

Step 1 : open the

xampp

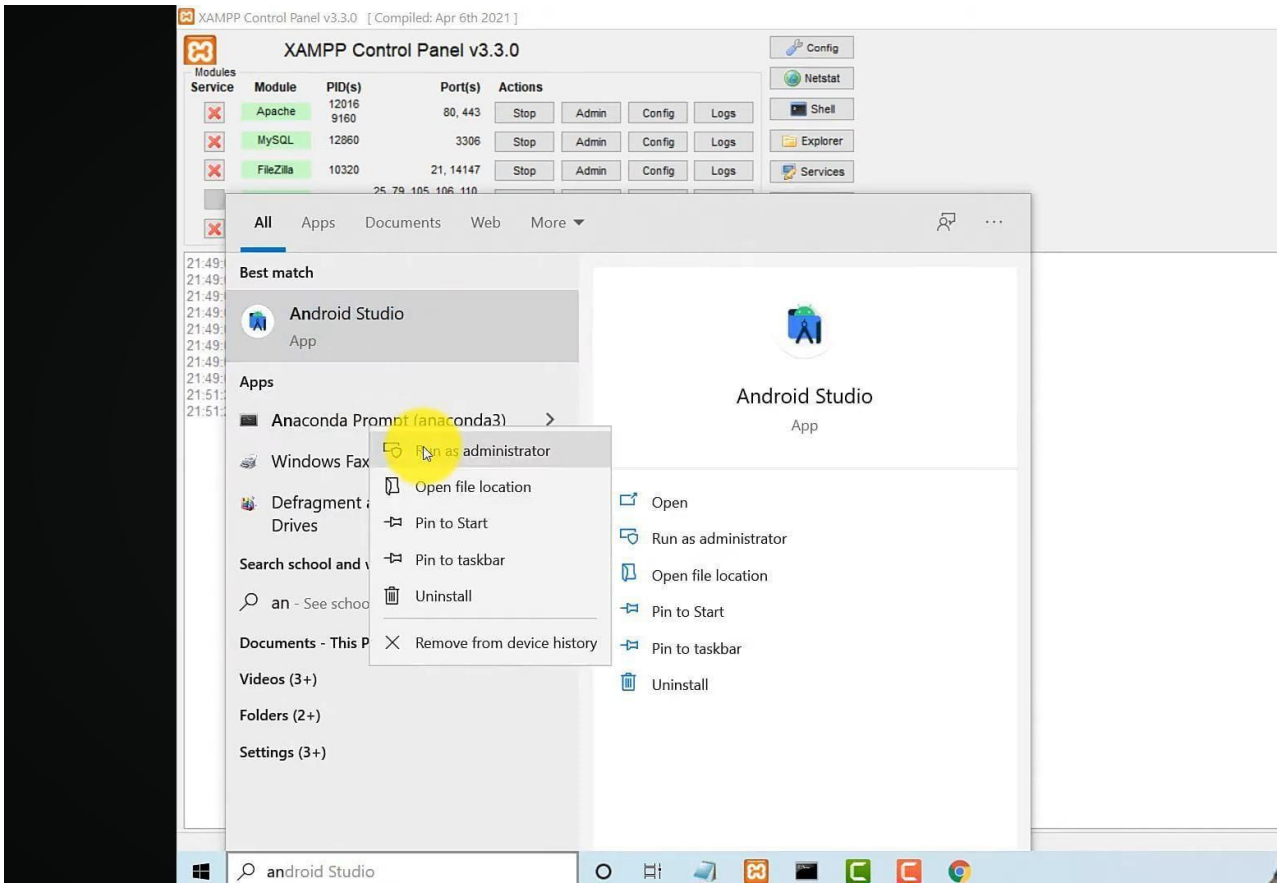
Local host ip address : 127.0.0.1 Step 2:

As we get into the xampp there we appear the search engines we have in our system



Step 3 :

As we enter into the all controls of the xampp we appear the anaconda prompt then we need to make it as the pin as administrator then we can perform the dos attack the anaconda is nothing but the slowris tool.



Step 4 :

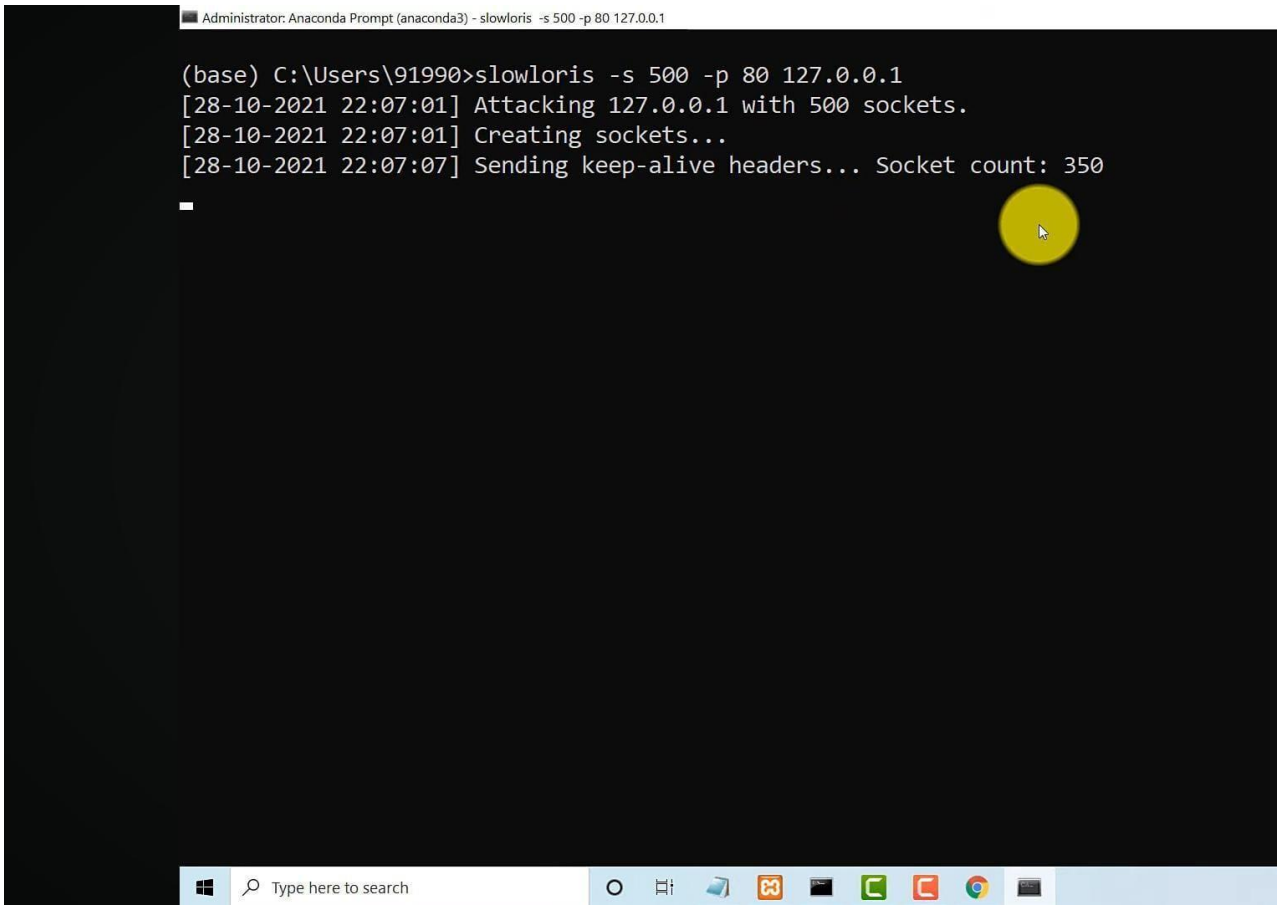
The slowloris attack on the pasted site that as the

Slowloris -s 500 -p 80 127.0.0.1

And this should be pasted on the xampp web site

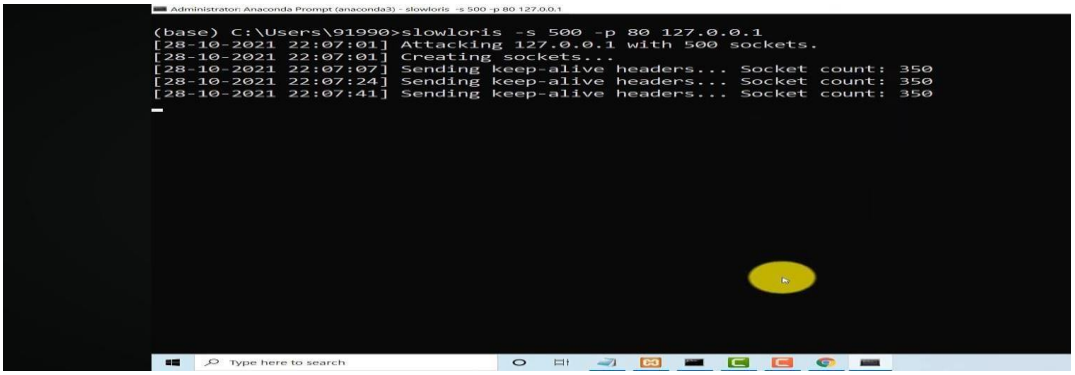
And press enter

Then the we send the request that to more than the 350 requests then the site will give the site cannot be requestd after even the refresh .

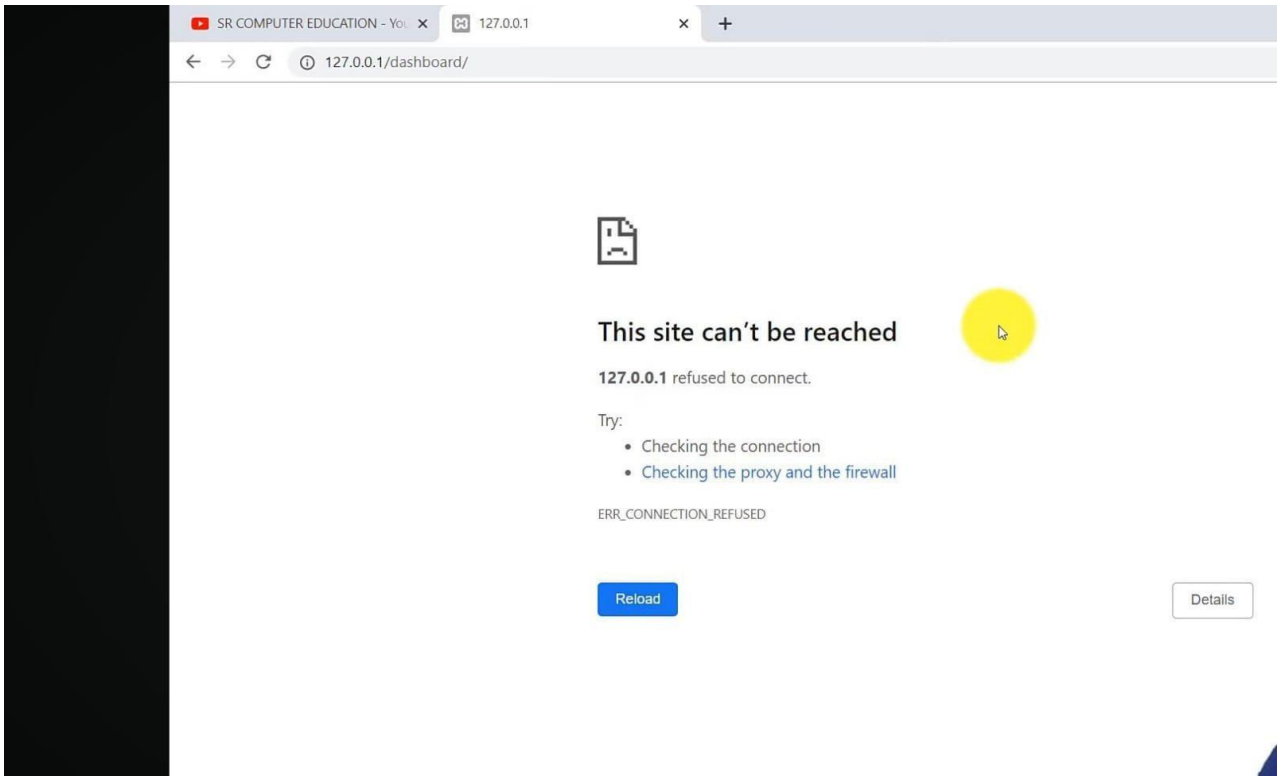


step 5

Has the 500 times as we perform the image is below the image occur the within site not reacheable



The site cant be reached as we request so many times even after refresh multiple times.



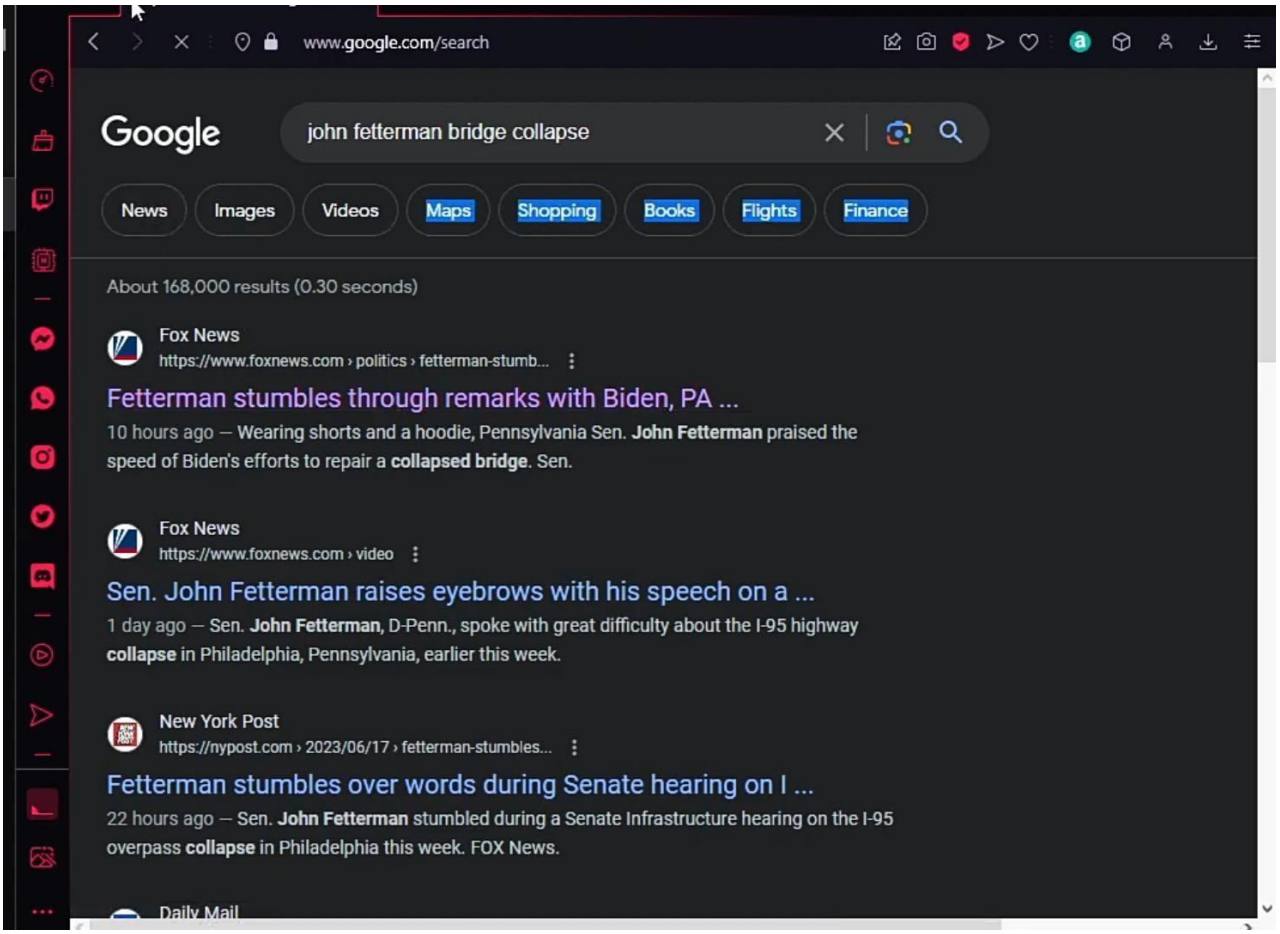
Stage : 3

REPORT ON MAIN WEBSITE

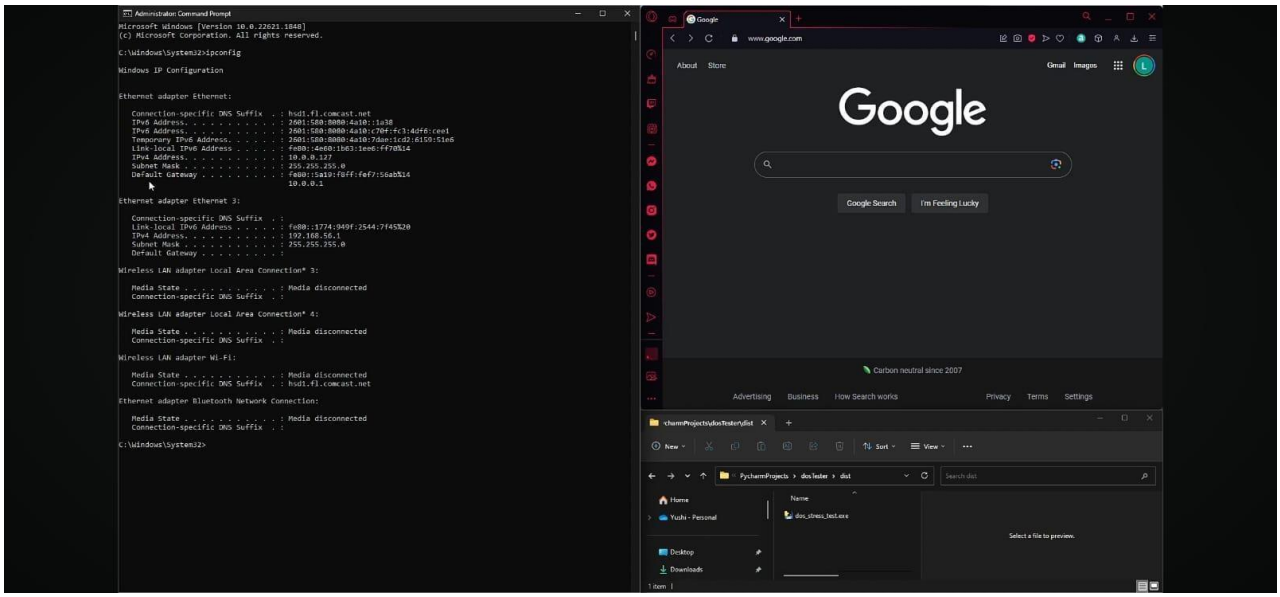
Chosen Website : http://www.foxnews.com **Step**

1 :

As we choose the foxweb site that to perform the dos attack the tool that used here is the flood and spoofing For ip address ;10.0.0.1



Step 2 let we should go to the command prompt and then we will select the if configuration as we select the required if configuration then we get the image shown below

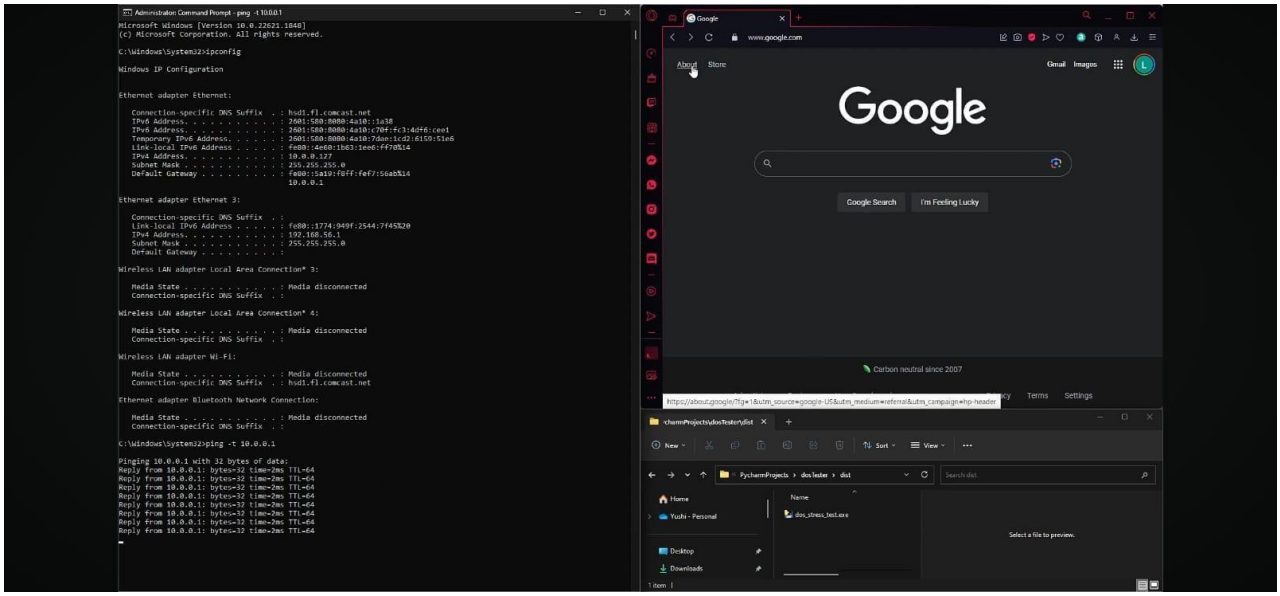


Step 3

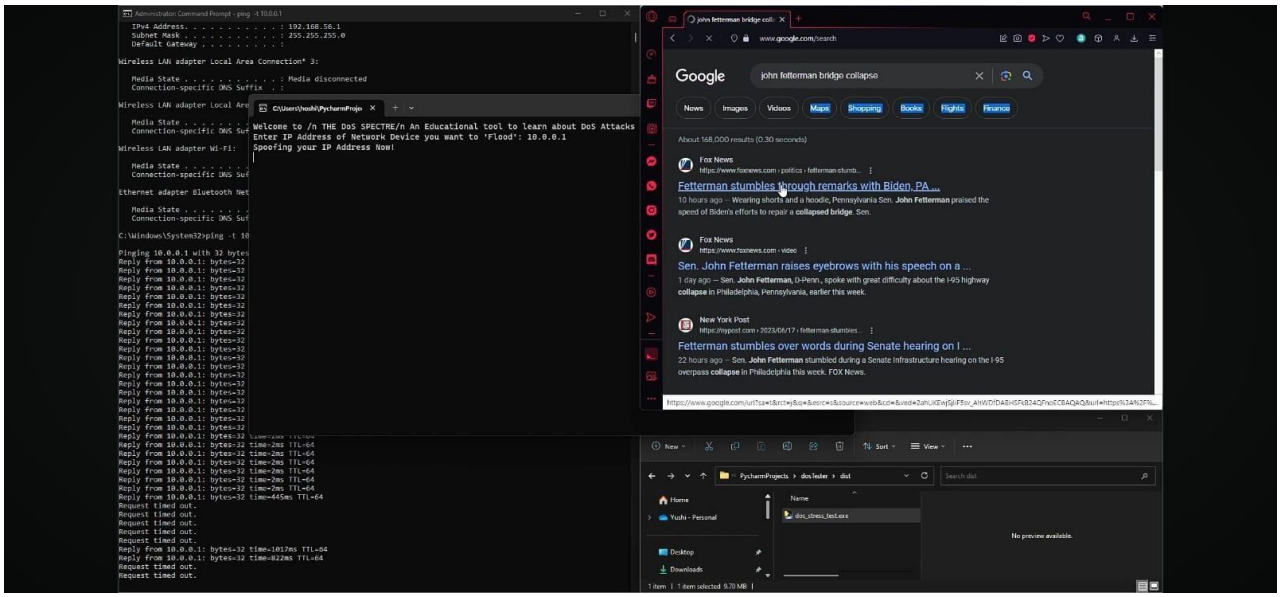
Pinging10.0.0.1 with 32 bytes of data

C:|\windows \system32>ping -t 10.0.0.1

Let paste this command to the website network



Sterp4



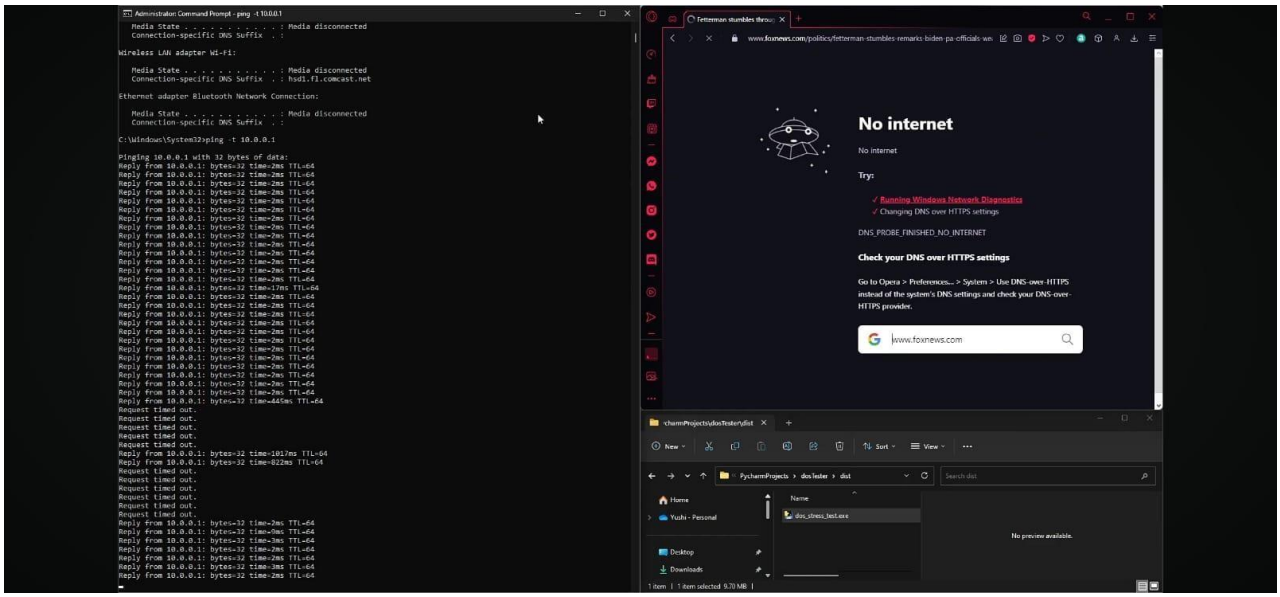
As we refresh the site is getting still buffer

Step 5

As we still refresh the site the gives us the not reacheable.

Thus the dos attack was performed

127.0.0.1 refused to connect



Prevention method of the dos attack

Preventing DDoS attacks can be challenging, particularly during high-traffic periods or across a vast and distributed network architecture. A truly proactive DDoS threat defense hinges on several key factors: attack surface reduction, threat monitoring, and scalable DDoS mitigation tools.

DDoS prevention methods

malicious requests, protocols, and IP blocks. Attack surface reduction: Limiting attack surface exposure can help minimize the effect of a DDoS attack. Several methods for reducing this exposure include restricting traffic to specific locations, implementing a load balancer, and blocking

communication from outdated or unused ports, protocols, and applications.

Anycast network diffusion: An Anycast network helps increase the surface area of an organization's network, so that it can more easily absorb volumetric traffic spikes (and prevent outages) by dispersing traffic across multiple distributed servers.

Real-time, adaptive threat monitoring: Log monitoring can help pinpoint potential threats by analyzing network traffic patterns, monitoring traffic spikes or other unusual activity, and adapting to defend against anomalous or

Caching: A cache stores copies of requested content so that fewer requests are serviced by origin servers. Using a content delivery network (CDN) to cache resources can reduce the strain on an organization's servers and make it more difficult for them to become overloaded by both legitimate and malicious requests.

Rate limiting: Rate limiting restricts the volume of network traffic over a specific time period, essentially preventing web servers from getting overwhelmed by requests from specific IP addresses. Rate limiting can be used to prevent DDoS attacks that use botnets to spam an endpoint with an abnormal amount of requests at once. DDoS prevention tools

Web application firewall (WAF): A WAF helps block attacks by using customizable policies to filter, inspect, and block malicious HTTP traffic between web applications and the Internet. With a WAF, organizations can enforce a positive and negative security model that controls incoming traffic from specific locations and IP addresses.

Always-on DDoS mitigation: A DDoS mitigation provider can help prevent DDoS attacks by continuously analyzing network traffic, implementing policy changes in response to emerging attack patterns, and providing an expansive and reliable network of data centers. When evaluating cloud-based DDoS mitigation services, look for a provider that offers adaptive, scalable, and always-on threat protection against sophisticated and volumetric attacks

Report :

The overall firepower of DDoS threat actors has increased significantly. A clear example is the recent attack on Google Cloud in October, which was over seven times more powerful than any previous, reaching 398 million RPS. This escalation in attack power has had a major impact on businesses globally

Compared to 2022, the total number of DDoS attacks worldwide in 2023 went up by 63%. Geopolitical factors were a major driver of this increase. The influence of these factors grew throughout the year and was especially pronounced in the fourth quarter, aligning with the start of the conflict between Israel and Palestine in October.

In terms of industries affected, finance was the most targeted, accounting for 26% of the attacks. This was followed by government services at 21% and retail at 14%.

Advantage ：

Few things are as catastrophic in modern life as not being able to use the Internet. Social media outages are headline news even when they last for a matter of minutes, so integral are they to how we communicate. For a

business, losing your website for any extended period not only means losing sales, but also losing some of the trust of your clients or customers.

This is the terrifying prospect behind a Denial of Service attack. These common and easily executed attacks can knock our websites and critical systems for minutes or hours at a time. While they pose less of a security risk than some other cyber attacks, they are harder to stop – meaning that your security has to be proactive to prevent them.

A Denial of Service (DoS) attack is a cyberattack that is designed to shut down the connectivity of a machine or network, making it inaccessible to its intended users. This is usually done by flooding the targeted machine or network with traffic (known as a Flood Attack), or by sending information across that

triggers a crash (referred to as a Crash Attack).

Unlike the majority of other cyber threats covered in typical security training modules, DoS attacks are unlikely to result in a data breach, although they can expose vulnerabilities which could be exploited. However, they can end up being very costly for organisations, as they may require a great deal of time and money to resolve.

In recent years, Distributed Denial of Service (DDoS) attacks have become increasingly common. These types of attack occur when multiple systems carry out synchronised DoS attacks on a single target. In these cases, the key difference is that the target ends up being attacked from various different locations at once, increasing the amount of traffic or data that is being sent.

DDoS attacks provide a number of advantages for the cyber criminal over traditional denial of service attacks, or indeed other forms of cyber attacks. These include:

By using more than just one machine in a combined attack, the attack is far more powerful, and can overload the victim machine or network much quicker.

Because the locations of the attacking systems are often spread across a wider area, it is much more difficult to locate and identify the attacker.

It is significantly harder to shut down multiple machines rather than just stopping one.

While DDoS attacks themselves do not pose the risk of a data breach, the irony is that they often require such data breaches to operate. Many DDoS attacks originate from computers which have been compromised and hijacked

by malware, often without the knowledge of their owner. This allows the attackers to coordinate computers around the world, and means that they do not actually have to own the hardware themselves

Conclusion :

As we have seen, distributed DoS attacks are a genuine threat that cause serious damage to many Internet users. The losses being suffered have escalated from being merely annoying to actually being debilitating and disastrous for some users. There is every reason to believe that the rate and seriousness of DDoS attacks will increase. The current limited level of losses caused by DDoS is probably not due to successes in defending against them, difficulties in perpetrating the attacks, or lack of attractive targets to attack. Rather, the level of loss is related more to the motivations and desires of those who are perpetrating the attacks. As more unprincipled and dissatisfied users of the Internet observe the success of Vulnerabilities in web applications can allow attackers to exhaust available

resources and thereby deny access to legitimate users. Companies that rely on web applications to provide critical business functions are therefore at risk from attackers wishing to disrupt these functions by exploiting application-level vulnerabilities.

Application based DoS attacks require considerably less resource in terms of processing power and bandwidth on the part of the attacker, and therefore present a higher risk to business as the number of possible threat-agents is much greater.

The possibility of a denial-of-service attack should be considered when designing, implementing and providing applications, and appropriate strategies and mitigation techniques put in place within the application.

Future scope

In the ever-changing digital battlefield, Distributed Denial-of-Service (DDoS) attacks continue to be a formidable weapon for cybercriminals and disruptors. As technology advances, so do the tactics employed in DDoS attacks, necessitating organisations to stay one step ahead with adaptive prevention strategies. Let's

take a peek into the future of DDoS threats and explore how organisations can prepare for what lies ahead.

Emerging Trends in DDoS Attacks

1. Increased Complexity and Sophistication

Future DDoS attacks are likely to become more complex by employing multi-vector approaches. Attackers may combine different techniques to overload both network and application layers simultaneously, making mitigation more challenging.

2. Rise of IoT-Based Botnets

The proliferation of vulnerable Internet of Things (IoT) devices creates a vast potential for botnets. Future attacks might leverage these compromised devices, amplifying the scale and impact of DDoS incidents.

3. Weaponised AI and Machine Learning

Attackers are expected to leverage Artificial Intelligence (AI) and Machine Learning (ML) to develop adaptive

attack schemes. This could bypass traditional signature-based detection methods, requiring more sophisticated defence mechanisms.

4. Focus on Disruption and Data Theft

DDoS attacks may increasingly serve as a smokescreen for more sophisticated cybercrimes. Beyond causing service disruptions, attackers may aim to steal sensitive data or disrupt critical infrastructure during DDoS incidents.

References

https://hackerlists.com/hacking-sites/ https://www.hacking-lab.com/index.html

https://securityscorecard.com/blog/best-practices-to-prevent-ddosattacks/

an introduction to DDos attack and defence mechanisum {BB guptha author]

https://www.researchgate.net/publication/216573214_An_Introduction_to_DDoS_Attacks_and_Defense_Mechanisms_An_Analyst's_Handbook