BUBT
Committed to Academic Excellence

BANGLADESH UNIVERSITY OF BUSINESS AND TECHNOLOGY

Assignment On

Course Code: CSE 413

Course Title: Cyber Security and Digital forensic

Submitted to:

Name: Dr. Shekh Abdullah-Al-Musa Ahmed

Lecturer

Department of Computer Science & Engineering

at Bangladesh University of Business and Technology.

Submitted by:

Name: Syeda Nowshin Ibnat

ID: 17183103020

Intake: 39

Section: 01

Program: B.Sc. in CSE

Semester: Fall 2021-2022

Date of Submission: 1-02-2022

Title: Towards the Qualitative Analysis of Slow Read Dos Attacks in an Educational Institute.

1.Introduction: Nowadays, with the ever-growing number of Internet users and the expanding range of Internet services, the demands on the security of users' data, services, and privacy are also growing. One type of cyber-attack is the DoS (denial-of-service) attack. A slow read DoS attack involves an attacker sending an appropriate HTTP request to a server, but then reading the response at a very slow speed, if at all. By reading the response slowly – sometimes as slow as one byte at a time – the attacker prevents the server from incurring an idle connection timeout. Slow Read Attack doesn't stop the server; Cloud flare doesn't provide protection. SlowHTTPTest (slow http read) is a highly configurable tool that simulates some Application Layer Denial of Service attacks. It implements most common low-bandwidth Application Layer DoS attacks, such as slowloris, Slow HTTP POST, Slow Read attack (based on TCP persist timer exploit) by draining concurrent connections pool, as well as Apache Range Header attack by causing very significant memory and CPU usage on the server.

As education institutions across the world moved to online learning, cyber threat disruptions have amplified more than ever. Malware, vulnerability exploits, denial-of-service (DoS), phishing attacks have all struck this sector, increasing in frequency over the past two months. It is that time, when students of educational institutions attending classes virtually. This requirement alone will vastly increase the overall traffic that will be flowing through an institutes network which in turn increases opportunities for bad actors to attack those institutes systems' networks to bring them down. Hard at work behind the scenes are the computers, servers, and infrastructure that support all of the applications that teachers, administrators, and students depend on. Another reason of DoS attack is today many educational institutions are using older networks and legacy hardware and software systems that make it easy to hack. Unlike corporations with trade secrets and data to protect, many educational institutions have set up systems to make connectivity even easier. By providing free Wi-Fi in buildings, these institutions are presenting thousands of opportunities for a hacker to gain access to network.

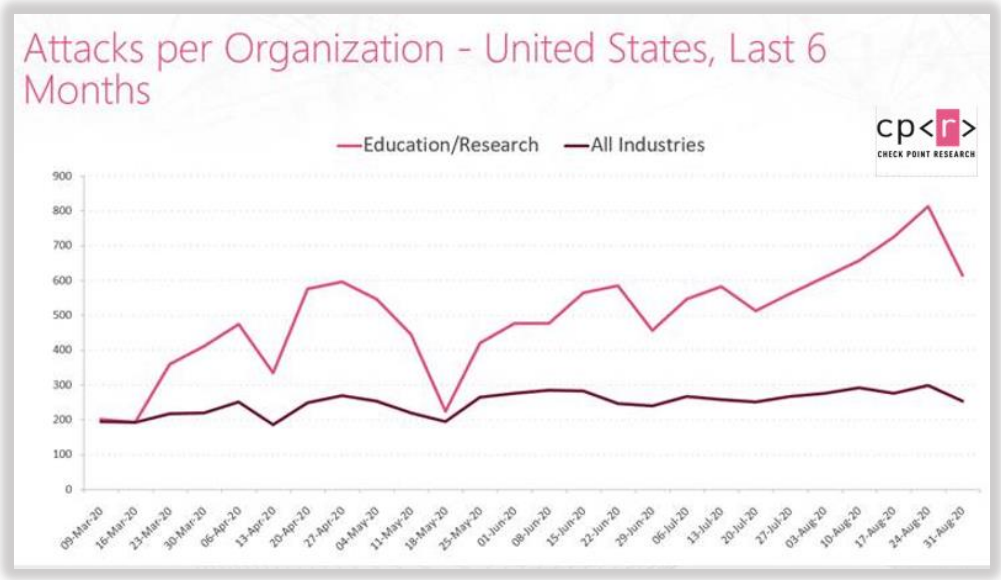

Figure Source: Check Point

Data from cybersecurity company Check Point shows that attackers have adopted different methods and tactics when targeting the education and research sectors in the U.S., Europe, and Asia. Most of the attacks targeted institutions in the U.S., with an average weekly increase of 30% during July and August 2020 in the academic sector.

2. Objectives:

1. The main goal of slow read DoS attack is to make the target Internet service unavailable to other users, or, at least, to degrade the quality and speed of the service. Most often, DoS attacks are targeted on web servers to prevent users from accessing web content. The primary targets of DoS attacks include web, mail, database, file, and domain system servers, and remote access services.

2. DoS attacks, typically deployed by hacktivists. Sometimes, though, behind the disruption are students trying out dedicated tools freely available online.

3. Sometimes the motivation of the student has generally been focused on taking down a server during exams where a student had not prepared or to see and potentially change grades or to show off for classmates.

3.Literature Review:

Aspects	Paper #1
Title	A Slow Read Attack Using Cloud.
Objectives	Show how slow read DoS attack happens using a cloud platform could not be detected by previous techniques. And Present a tricky solution based on the cloud as well.
Methodology/ Theory	Suggest incorporating multiple Web servers by implementing a failure-isolation zone to provide high availability and redundancy in a Cloud environment. This improves performance because several servers can answer user requests simultaneously depending on the traffic.
Software Tools	Virtual Machine.
Conclusion	Present an approach to prohibit the slow read attack which uses cloud environment.
Obstacles/ Challenges	The first one is the difficulty to detect such attack when they are highly distributed. And the second challenge is to detect such attacks without creating false alarm.
Terminology	Slow Read attack, distributed denial-of service, Cloud computing, Security, Virtual IP address.
Review Judgment	This article provides a method of how we can get read of Slow Read DoS attack.
Review Outcome	In this article, a clear discussion of slow read DoS attack as well as the use of cloud environment to prohibit Slow Read DoS attack is given.

4.Methodology: Slow Read Attack doesn't stop the server; Cloud flare doesn't provide protection.

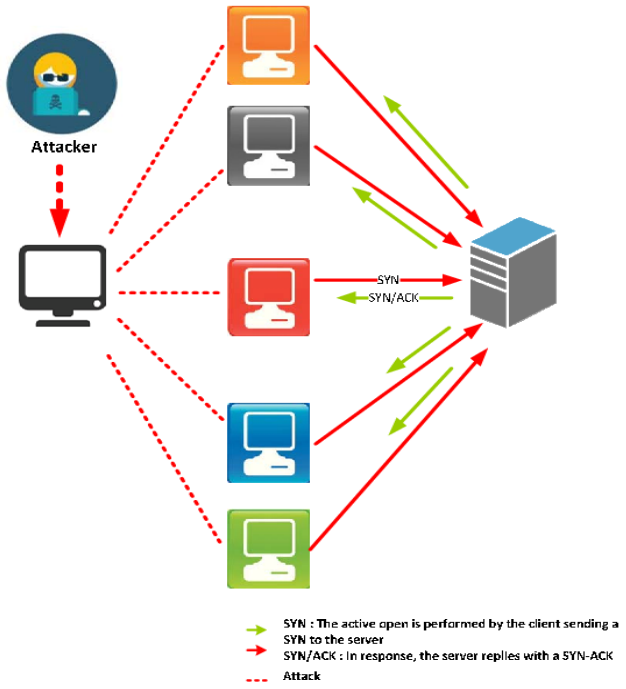

Figure 1: The Slow Read attack

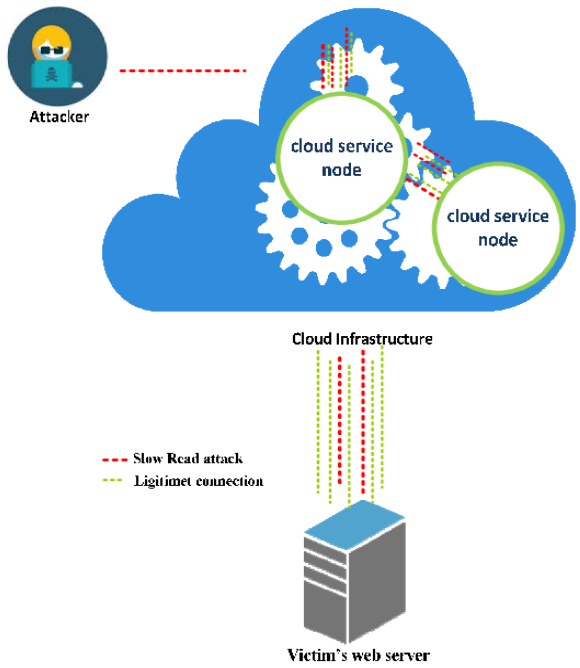

Figure 2: A Slow Read DoS attack using cloud

Figure 2 shows how slow read DoS attack happens. A hacker can launch several connection requests from the same virtual machine and using different virtual IP address (an IP address assigned to multiple domain names or servers that share an IP address). Virtual IP addresses are allocated to virtual private servers, websites or any other application residing on a single server.

Figure 2 shows the scenario of a Slow Read attack for Denial of Services-DoS using a Cloud environment. In this scenario, the attacker sends a set of HTTP requests to a Web server using a program installed on a virtual machine on the cloud. Then, the attacker sets the window size to the smallest acceptable value to make the HTTP response operation slow down. If the number reaches the limit of maximum clients of the web server, the web server cannot accept new legitimate connections and cannot disconnect actual connections. Thus, it becomes inactive and unavailable

5. Socio-economic Impact: Social and economic impact of slow read denial of service attack-

1. **Public Services:** The denial of service of public services on a national basis or on an agency basis (administrative services, social services, water, air traffic, waste management, financial payments), have wide ranging consequences where the indirect impact encompasses prejudice caused to citizens.
2. **Company Products and Services:** In this case, the applicable methodology to the data collection is the one used for corporate liability insurance assessment. This includes loss of capabilities (physical raw material and service related).
3. **Loss of shared infrastructure:** Lost revenues by infrastructure operator including claims payable to customers under contract terms, of verifiable loss and damage by individual and institutional users, and moreover of social costs to the same.
4. **Technology Providers:** Some well know technology providers in such areas as communications, software, control systems, transport technologies, biomedical devices, etc. may be liable to claims by their customers for vulnerabilities in their products.

6.Conclusion: Education institutions across the world moved to online learning, cyber threat disruptions have amplified more than ever. Attacks like slow read DoS are happening. A Slow Read DoS attack will result in the connection staying open for a long time. If the attacker establishes multiple connections, for example by using a DoS Botnet, he/she will be able to fill up the connection tables, resulting in legitimate users not being able to access the services. The indicators will be that the server has large amount of connections, but very little traffic is sent or received.

7.Reference:

[1] https://www.tandfonline.com/doi/full/10.1080/21642583.2016.1241193

[2] https://edtechmagazine.com/higher/article/2021/05/easy-and-inexpensive-ddos-attacks-surge-higher-ed

[3] https://www.netscout.com/what-is-ddos/slow-read-attacks

[4] https://www.ncbi.nlm.nih.gov/pmc/articles/PMC8401215/

[5] https://arxiv.org/pdf/1308.3693