INTERNATIONAL RESEARCH JOURNAL ON ADVANCED SCIENCE HUB
e-ISSN : 2582 - 4376
Open Access
RSP SCIENCE HUB
(The Hub of Research Ideas)
Available online at www.rspsciencehub.com

Identification of DOS Attack by implementing SYN Flood Attack and considering CPU Load Analysis.

Ms. Sona D Solanki[1]*, Mrs. Asha D Solanki*[2]

[1]*PG Student, Department of Electronics and Communication Engineering, Babaria Institute of Technology, Vadodara, India.*

[2]*Department of Arts, B. K. Arts and Science College, Palanpur, India.*

solankisona28@gmail.com[1]

Abstract

The stupendous utilization of the web and its entrepreneurial inclination is growing the prevalence to enhance cyber threats occurrence. The absolute identification of virtual-harassment plays a critical role in safeguarding computer systems. Assessment of safety concerns when recognizing a convergence between internet-security and network equipment is vital. To construct a robust infrastructure, the requisite of a cyber-safety methodology is integral. For example, if efficacious cyber-threat takes place then it significantly enhances the power usage of the database and solely impacts its hardware elements. This article provides a glimpse into a DOS intrusion and its stronger links between CPU utilization and absorbed resources, which is one of the most critical admonitions and intimidate features of the machine. DOS threat loads the network with congestion by implementing perilous data that will disrupt the machine by incorporating an estimated excessive energy usage imbibed by a Processor. According to the elevated mechanism, the identification of the SYN flood intrusion is addressed, which is the utmost prevalent DOS attack. In this methodology, this prominent attack is identified by incorporating Wireshark tools. The surveilling and sorting online flood vulnerabilities like SYN by extending a precise intrusion detection model for the safeguarding of data as well as cybersecurity to make the structure sustainable is implemented.

Keywords: Cyber-attacks, DOS, SYN, SYN Flood, Energy consumption.

1. Introduction

A cyber threat associates with identifying fraud, intended extortion, loss of critical information such as family photographs. It seeks to influence and demolish sensitive data, extorts user cash and disrupts their regular business operations. In today's interconnected culture, everybody profits from innovative data security strategies. Cyber threat relates to the body of techniques, procedures and strategies designed to avoid malicious access to the systems, computers and software's [1]. Incorporating efficient security protocols is exceptionally difficult today as there are numerous computer systems than humans and hackers have become more inventive.

A substantial chunk of the information could be confidential detail, be it personal capital, financial records, private details or other data forms for which security breach or disclosure may have negative repercussions [3]. In the course of business operations, companies transfer classified information through networks and to various machines and cyber safety encompasses the practice devoted to securing that data and the devices used to analyze and manage that content. When the frequency and complexity of cyber-threats increase, businesses and organizations, particularly those dealing with data protection associated with nationwide protection, healthcare, or banking data, need to intervene to safeguard their classified company and personal records.

This article addresses the identification of the DOS attack that is a denial of service invasion. The DOS threats are a prominent kind of cyber-threat that is designed to reduce the database access and restricting the client access to systems. This can be tackled with the utilization of the CPU load management and Wireshark monitoring tool within the framework for malware detection.

2. Motivation

The gargantuan utilization of the web and its monetary behavior increases the vulnerability of cyber threats. Cyber infliction mitigation plays a critical part in enhancing computer security. DOS intrusions are amongst the renowned data breaches, as well as the most directed intrusion to the safeguarding of the system. This article is a tremendous internet security prognosis for identifying dos invasions. The inclination to publish this academic paper reared when numerous amounts of data breaches occurred in multiple services across the globe including India like the Facebook and WhatsApp data breach by North Korean hackers during the epidemic. The site of the IRCTC was exploited in 2020. As addressed earlier in this thread, the amount of cyber-attack occurrences in India is a reminder to all people as well as corporations that are yet susceptible to hacker-extortion [13]. At the commencement of 2020, information fissures reflect 8.1 billion data. Noticing heaps of recent events, I have comprehended the shortfall of such an adequate research paper. The primary goal of this research article is to examine the DOS intrusion within the risk assessment framework that will be beneficial to experts in the domain. I portrayed the overarching classification of cybersecurity, SYN Flood intrusions by implementing the Wireshark tool to monitor them and interpret the outcome by CPU Load evaluation. In cyber-invasion, the SYN Flood Attack identification is implemented including practical simulation outcomes. I used entire course material to analyze and enhance this research article to incorporate a systematic, rigorous and thorough cyber-safety assessment.

3. Types Of Cyber Attack

3.1 Man-in-the-Middle Attack (MITM)

It arises if anybody sits among host devices and retrieve traffic by pilfering pertinent data. A hacker incorporates an open-source software and collects entire packets passed among systems, then evaluate device-to-device interactions and determine possibly beneficial transmitted content.

3.2 TCP Session Hijacking

It is a pivotal intrusion against a user's browser over a secured infrastructure. IP spoofing is the greatest popular cause of session sabotage, in which an intruder utilizes client-routed data packets to induce instructions into an ongoing interaction between two entities on a system and disguise themselves among the authorized personnel.

3.3 Sniffing and Eavesdropping

It signifies evaluating entire packets, while eavesdropping identifies inadequate packets instead of accurate ones. Eavesdropping is an automated invasion in which digital interaction is intercepted by an undestined entity.

3.4DNS Poisoning

It is recognized as DNS spoofing, is a form of intrusion that compromises domain name system (DNS) security breaches to redirect network traffic far from authorized databases and towards bogus systems. It is hazardous because it can migrate among various DNS databases. Figure 1. Demonstrates the malicious attacks performed by the hacker

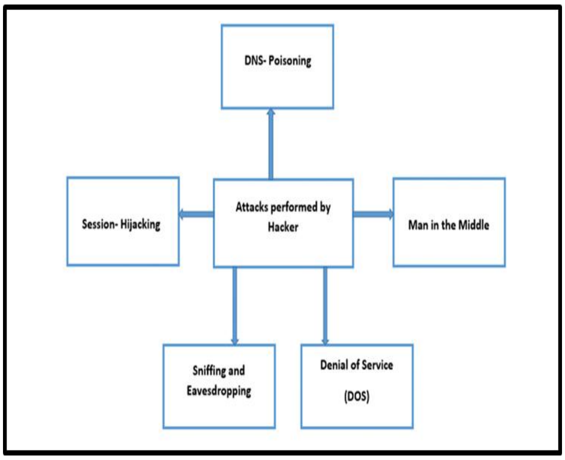


Fig1. Hacker performing Malicious Attacks.

4. DOS Attack

DOS Attack prohibits authorized customers to recourse system resources such as accessing a webpage, system, electronic mail etc. This intrusion is enforced by repeatedly striking the target tool, such as an internet server with numerous requests simultaneously [2]. This leads the database to collapse to reply to all of the queries. The impact of this can be either malfunction or failure of the database and make an internet connection inaccessible. The host that is linked to the web is generally disrupted permanently. These threats usually aim services that are deployed on critical operational web applications such as financial firms, gateways for bill payments. Figure 2. indicates the impact of DOS Attack on Intruder and Authorized User.

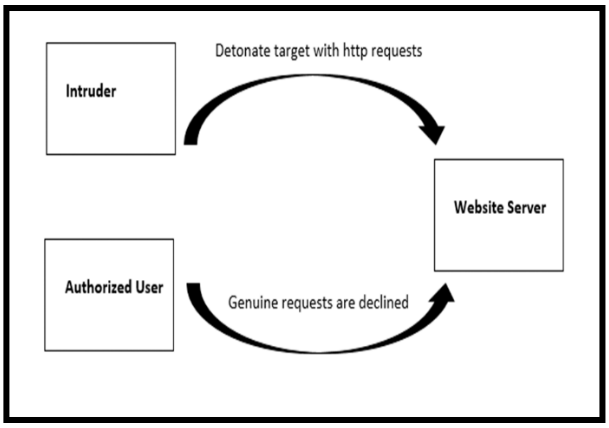

Intruder
Detonate target with http requests
Website Server
Authorized User
Genuine requests are declined

Fig 2. Impact of DOS Attack on Intruder and Authorized User

4.1 Sidelines of DOS Attack

- Extraordinarily sluggish network implementation.
- Specific site is inaccessible.
- Unable to connect any of the websites.
- Raising the quantity of junk mail received significantly.
- Prolonged interruption of internet connectivity or certain online services.

Usually, DOS interventions take one of two classifications. They either deluge online services or collapse them.

4.2Flooding Threats

1. SYN Flood Attack

A SYN Flood Attack is an alteration that targets system vulnerability in the series of the TCP connections. This is termed as the three-way handshake interaction between the client and the database.

2.ICMP Flood Attack

An ICMP flood identified as a ping flood is a form of DOS intrusion that transfers spoofed data streams that strike every device in a specified network, benefitting from malfunctioned network machines.

5.Three-Way Handshake in TCP SYN

A three-way handshake is a technique implemented to establish a connection within a host computer and a database in a TCP / IP network. It is a three-step process proposed for the client-server interaction. It starts after the virtual correlation has been constructed. The client begins a communication by requesting access for SYN (synchronization) to the database, and then the database replies by returning SYN / ACK, which is an acknowledgment of the customer's original request for SYN. It ensures that both sender and the recipient interchange SYN and ACK data until the real information transmission starts. Figure 3. shows a Three-way handshake methodology in the Client-Server TCP SYN.

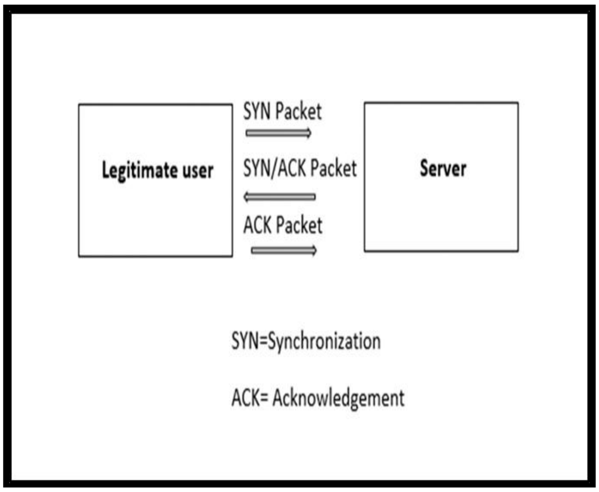


Fig 3. Three-Way Handshake Technique.

6. SYN Flood Attack

A SYN intrusion is defined as a TCP SYN threat or a SYN flood. It is a form of Denial-of-Service

(DOS) invasion where a hacker exploits the Network data transmission, TCP / IP, to strike a victim machine with an original request (a SYN). Presuming it as a genuine request, the database replies with SYN / ACK, but rarely gets a final (an ACK) from the intruder and they probably would not reply. Eventually working closely with the processor system resources through half-open TCP connections, it would stay for a pre-specified frame level to reject the demand for communication that ultimately corresponds declining the valid requests for the link, inevitably being exhausted and uncommunicative. Figure4.Presents performance of SYN Flood Attack.

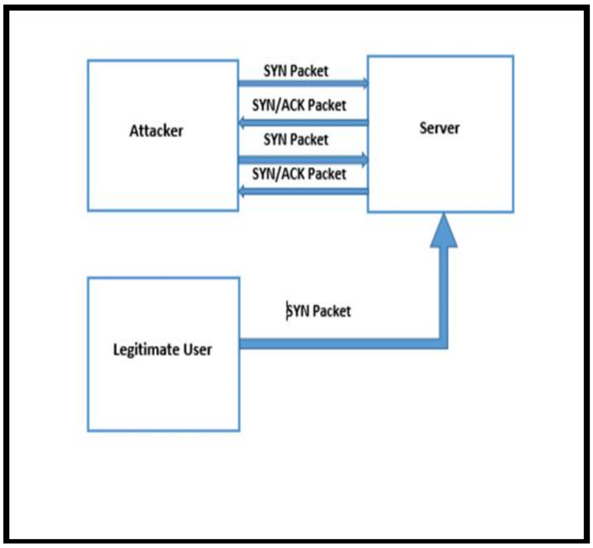


Fig.4. SYN Flood Attack

7. Results and Discussion

7.1 Enhancement in Strategy by Deploying Wireshark – Software.

The enhanced strategy is an online breach identification framework where SYN Flood intrusion diagnosis and sorting are achievable. Since our technique is innovative, the methodology and further tasks are being illustrated with the aid of the flowchart provided below. The mitigation of the above hazardous cyber threat can be achieved in the long term and eventually render the mechanism automatically by constructing a script and insinuating the individual when an attack occurs. Figure 5. demonstrates a Flow Chart of the enhanced strategy describing the technique and further work.

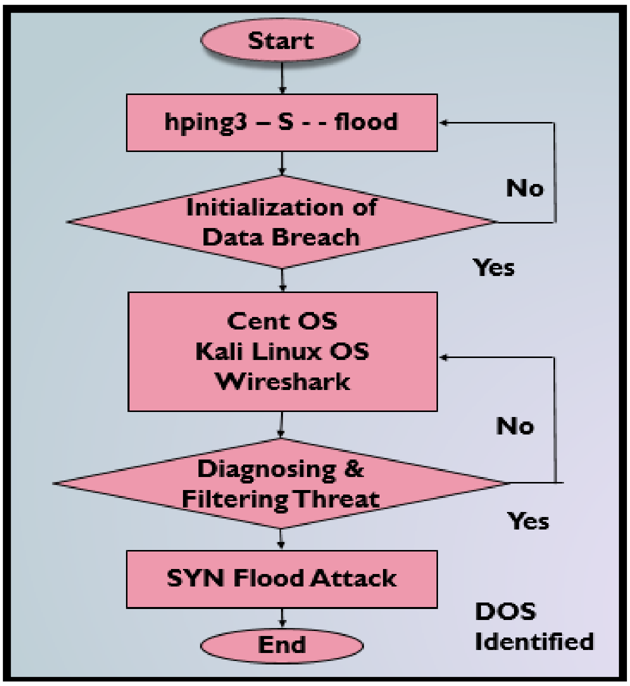
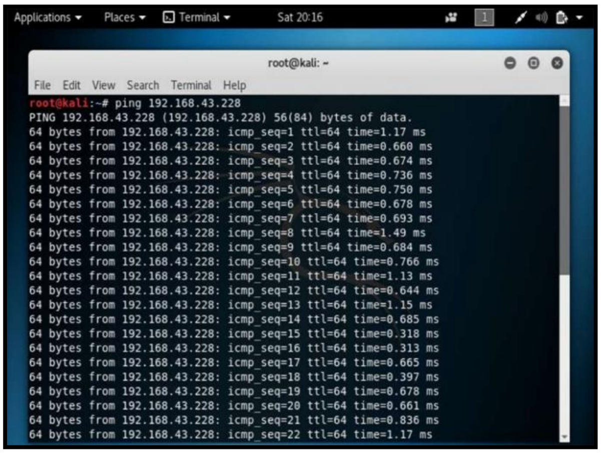


Fig.5. Flow Chart of the Enhanced Strategy.

7.2 Manual Supervision Of Threats

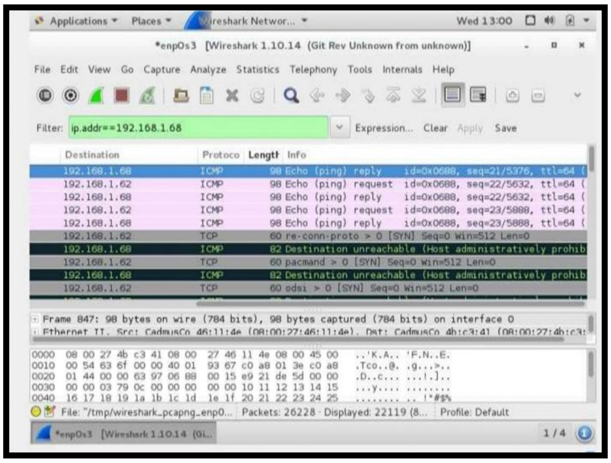
1. **TCP SYN**

In SYN, the "three-way handshake" is the methodology through which two machines establish an event of interaction. After this data transmitting and receiving, the sequence is effective and the TCP connection is established and is authorized for information interchange and sharing. In Figure 6, the framework connection is analyzed utilizing instruction ping 192.168.43.228, which is the target IP address by employing Kali Linux OS and the outcome of standardized traffic is inspected through Wireshark software in Figure 7, respectively.



```
root@kali:~# ping 192.168.43.228
PING 192.168.43.228 (192.168.43.228) 56(84) bytes of data.
64 bytes from 192.168.43.228: icmp_seq=1 ttl=64 time=1.17 ms
64 bytes from 192.168.43.228: icmp_seq=2 ttl=64 time=0.660 ms
64 bytes from 192.168.43.228: icmp_seq=3 ttl=64 time=0.674 ms
64 bytes from 192.168.43.228: icmp_seq=4 ttl=64 time=0.736 ms
64 bytes from 192.168.43.228: icmp_seq=5 ttl=64 time=0.750 ms
64 bytes from 192.168.43.228: icmp_seq=6 ttl=64 time=0.678 ms
64 bytes from 192.168.43.228: icmp_seq=7 ttl=64 time=0.693 ms
64 bytes from 192.168.43.228: icmp_seq=8 ttl=64 time=1.49 ms
64 bytes from 192.168.43.228: icmp_seq=9 ttl=64 time=0.684 ms
64 bytes from 192.168.43.228: icmp_seq=10 ttl=64 time=0.766 ms
64 bytes from 192.168.43.228: icmp_seq=11 ttl=64 time=1.13 ms
64 bytes from 192.168.43.228: icmp_seq=12 ttl=64 time=0.644 ms
64 bytes from 192.168.43.228: icmp_seq=13 ttl=64 time=1.15 ms
64 bytes from 192.168.43.228: icmp_seq=14 ttl=64 time=0.685 ms
64 bytes from 192.168.43.228: icmp_seq=15 ttl=64 time=0.318 ms
64 bytes from 192.168.43.228: icmp_seq=16 ttl=64 time=0.313 ms
64 bytes from 192.168.43.228: icmp_seq=17 ttl=64 time=0.665 ms
64 bytes from 192.168.43.228: icmp_seq=18 ttl=64 time=0.397 ms
64 bytes from 192.168.43.228: icmp_seq=19 ttl=64 time=0.678 ms
64 bytes from 192.168.43.228: icmp_seq=20 ttl=64 time=0.661 ms
64 bytes from 192.168.43.228: icmp_seq=21 ttl=64 time=0.836 ms
64 bytes from 192.168.43.228: icmp_seq=22 ttl=64 time=1.17 ms
```

Fig.6.Connectivity Evaluation using Kali OS

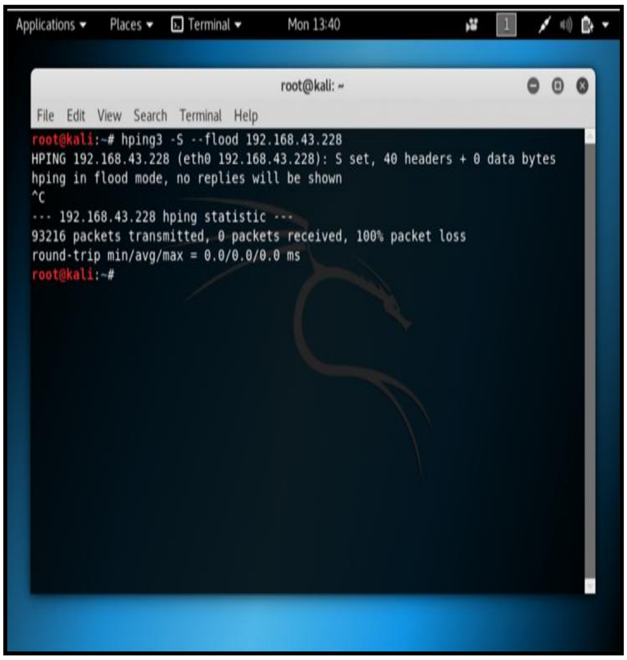

Applications
Places
Wireshark Networ...
Wed 13:00
*enp0s3 [Wireshark 1.10.14 (Git Rev Unknown from unknown)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter: ip.addr==192.168.1.68
Expression... Clear Apply Save

```
Destination          Protoco Lengtt Info
192.168.1.68         ICMP    98 Echo (ping) reply    id=0x0688, seq=21/5376, ttl=64 (
192.168.1.62         ICMP    98 Echo (ping) request  id=0x0688, seq=22/5632, ttl=64 (
192.168.1.68         ICMP    98 Echo (ping) reply    id=0x0688, seq=22/5632, ttl=64 (
192.168.1.62         ICMP    98 Echo (ping) request  id=0x0688, seq=23/5888, ttl=64 (
192.168.1.68         ICMP    98 Echo (ping) reply    id=0x0688, seq=23/5888, ttl=64 (
192.168.1.62         TCP     60 re-conn-proto > 0 [SYN] Seq=0 Win=512 Len=0
192.168.1.68         ICMP    82 Destination unreachable (Host administratively prohib
192.168.1.62         TCP     60 pacmand > 0 [SYN] Seq=0 Win=512 Len=0
192.168.1.68         ICMP    82 Destination unreachable (Host administratively prohib
192.168.1.62         TCP     60 odsi > 0 [SYN] Seq=0 Win=512 Len=0

Frame 847: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface 0
Ethernet II, Src: CadmusCo_46:11:4e (08:00:27:46:11:4e), Dst: CadmusCo_4b:c3:41 (08:00:27:4b:c3:

0000  08 00 27 4b c3 41 08 00  27 46 11 4e 08 00 45 00   ..'K.A.. 'F.N..E.
0010  00 54 63 6f 00 00 40 01  93 67 c0 a8 01 3e c0 a8   .Tco..@. .g...>..
0020  01 44 00 00 63 97 06 88  00 15 e9 21 de 5d 00 00   .D..c... ...!.]..
0030  00 00 03 79 0c 00 00 00  00 00 10 11 12 13 14 15   ...y.... ........
0040  16 17 18 19 1a 1b 1c 1d  1e 1f 20 21 22 23 24 25   ........ .. !"#$%

File: "/tmp/wireshark_pcapng_enp0...  Packets: 26228 · Displayed: 22119 (8...  Profile: Default
```

Fig 7. Inspecting Standa rd Traffic using Wireshark Software.

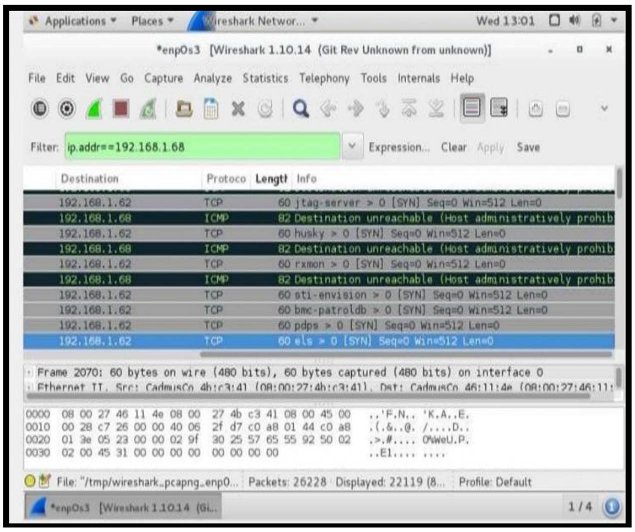
2. SYN Flood Attack

A SYN (synchronize) flood attack is a category of DOS threat that drains entire existing database resources and renders a server inaccessible for authorized traffic. In Figure 8, the SYN Flood invasion is performed utilizing the instruction hping3 -S--flood 192.168.43.228 by transferring a huge amount of malicious packets to the target's device through Kali Linux OS, and in Figure 9, the outcome of fraudulent traffic is evaluated and screened using the command ip.addr = = 192.168.1.68 through Wireshark software.



```
root@kali:~# hping3 -S --flood 192.168.43.228
HPING 192.168.43.228 (eth0 192.168.43.228): S set, 40 headers + 0 data bytes
hping in flood mode, no replies will be shown
^C
--- 192.168.43.228 hping statistic ---
93216 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
root@kali:~#
```

Fig. 8. Conducting SYN Flood Attack using Kali OS.

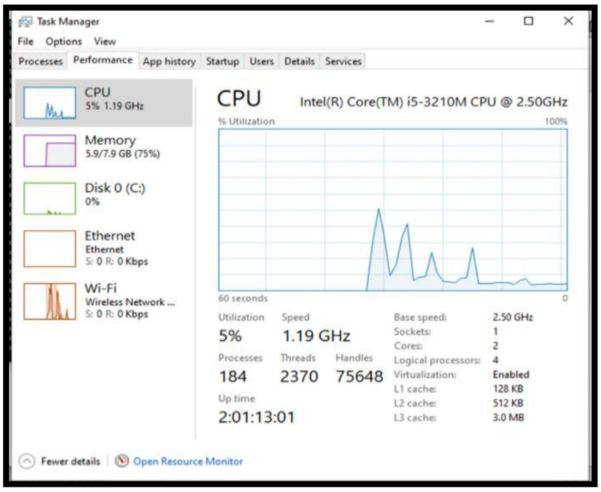

Applications
Places
Wireshark Networ...
Wed 13:01
*enp0s3 [Wireshark 1.10.14 (Git Rev Unknown from unknown)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter: ip.addr==192.168.1.68
Expression... Clear Apply Save

```
Destination          Protoco Lengtt Info
192.168.1.62         TCP     60 jtag-server > 0 [SYN] Seq=0 Win=512 Len=0
192.168.1.68         ICMP    82 Destination unreachable (Host administratively prohib
192.168.1.62         TCP     60 husky > 0 [SYN] Seq=0 Win=512 Len=0
192.168.1.68         ICMP    82 Destination unreachable (Host administratively prohib
192.168.1.62         TCP     60 rxmon > 0 [SYN] Seq=0 Win=512 Len=0
192.168.1.68         ICMP    82 Destination unreachable (Host administratively prohib
192.168.1.62         TCP     60 sti-envision > 0 [SYN] Seq=0 Win=512 Len=0
192.168.1.62         TCP     60 bmc-patroldb > 0 [SYN] Seq=0 Win=512 Len=0
192.168.1.62         TCP     60 pdps > 0 [SYN] Seq=0 Win=512 Len=0
192.168.1.62         TCP     60 els > 0 [SYN] Seq=0 Win=512 Len=0

Frame 2070: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0
Ethernet II, Src: CadmusCo_4b:c3:41 (08:00:27:4b:c3:41), Dst: CadmusCo_46:11:4e (08:00:27:46:11:

0000  08 00 27 46 11 4e 08 00  27 4b c3 41 08 00 45 00   ..'F.N.. 'K.A..E.
0010  00 28 c7 26 00 00 40 06  2f d7 c0 a8 01 44 c0 a8   .(.&..@. /....D..
0020  01 3e 05 23 00 00 02 9f  30 25 57 65 55 92 50 02   .>.#.... 0%WeU.P.
0030  02 00 45 31 00 00 00 00  00 00 00 00               ..E1.... ....

File: "/tmp/wireshark_pcapng_enp0...  Packets: 26228 · Displayed: 22119 (8...  Profile: Default
```

Fig 9. Inspecting and Filtering Malicious Traffic using Wireshark Software.

7.3 Alliance between CPU and Data Breach.

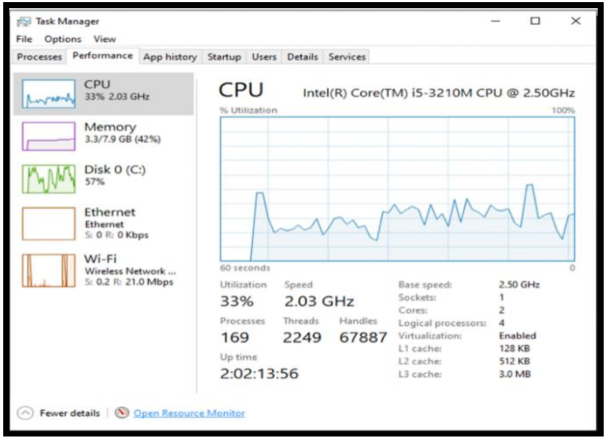
The efficiency of the devices is quantified regarding CPU utilization until intrusion and throughout a flood invasion with TCP SYN. DOS threat uses a strategy called coercive rendering to absorb system resources such as the Processor and memory of the victim's device. These are the vital components from the efficiency perspective because the essence of the drives is evident in the entire server. The aggregate surplus energy utilization introduced by a CPU-based DOS invasion determines the necessary power by consolidating the strong relationship between Processor implementation and cyber-threat.


Task Manager
File Options View
Processes Performance App history Startup Users Details Services
CPU
Intel(R) Core(TM) i5-3210M CPU @ 2.50GHz
% Utilization
100%
60 seconds
0
Fewer details
Open Resource Monitor

CPU 5% 1.19 GHz
Memory 5.9/7.9 GB (75%)
Disk 0 (C:) 0%
Ethernet Ethernet S: 0 R: 0 Kbps
Wi-Fi Wireless Network ... S: 0 R: 0 Kbps

Utilization	Speed		Base speed:	2.50 GHz
5%	1.19 GHz		Sockets:	1
Processes	Threads	Handles	Cores:	2
184	2370	75648	Logical processors:	4
Up time			Virtualization:	Enabled
2:01:13:01			L1 cache:	128 KB
			L2 cache:	512 KB
			L3 cache:	3.0 MB

Fig.10. Utilization of CPU before ata Breach.



CPU 33% 2.03 GHz
Memory 3.3/7.9 GB (42%)
Disk 0 (C:) 57%
Ethernet Ethernet S: 0 R: 0 Kbps
Wi-Fi Wireless Network ... S: 0.2 R: 21.0 Mbps

CPU Intel(R) Core(TM) i5-3210M CPU @ 2.50GHz

Utilization 33%
Speed 2.03 GHz
Processes 169
Threads 2249
Handles 67887
Up time 2:02:13:56

Base speed: 2.50 GHz
Sockets: 1
Cores: 2
Logical processors: 4
Virtualization: Enabled
L1 cache: 128 KB
L2 cache: 512 KB
L3 cache: 3.0 MB

Fig.11. Utilization of CPU after the Data Breach.

Servers imbibe optimum energy during the same interval of time that is calculated by their particular energy usage and standard of energy performance, which is also facilitated by a relative structure that induces power absorption associated with original operating capacity. Data breaches significantly affect the CPU and the entire foundation. CPU and whole structure become relatively slow because it incorporates supplemental bandwidth compared to regular traffic. The device becomes overloaded by extraneous requests to control the computer infrastructure and eliminates authorized users. Furthermore, the proposed paradigm is disrupted by security vulnerabilities that impede its consistency and robustness and enhance the load. Figure 10, indicates that the overall CPU utilizes 5% of the load preceding data infringement and Figure 11, demonstrates that Processor consumption enhances from 5% to 33% post data infringement.

Conclusion

As per preceding research and findings, the emergence of a DOS invasion is imminent. DOS invasion transfers umpteen falsified packets to the victim that occupies the resources of the victim and creates disruptions in database processes and computing resources. A perceptual correlation between cybersecurity and system is conducted to assess the absorption of resources of servers and communication hardware.

This article concentrates on the DOS flood vulnerability in the infrastructure by employing an on-line infringement identification strategy where a specific DOS intrusion like SYN flood is regarded and the technique of scanning and filtration of system packets for the threat is implemented. Subsequently, the significant correlation between Processor utilization and used resources is presented where the excessive cumulative use of energy generated by a CPU-based DOS invasion decides the cyber hazard.

ACKNOWLEDGEMENT

I reverence and glorify the Supreme Lord for the spiritual inspiration, the most benevolent and accommodating for my research methodology task to accomplish this article. I would like to articulate my wholehearted gratitude to my grandmother **Shardaba**, my parents: **Dansinh and Asha Solanki** and the entire members of my family for their pertinent motivation and virtuous assistance towards my higher education Master of Engineering (Electronics & Communication) and for supplying indispensable direction throughout this document.

Reference

[1]. Benamar Bouyeddou, Fouzi Harrou, Ying Sun and Benamar Kadri. "Detecting SYN Flood Attacks via Statistical Monitoring Charts: A Comparative Study." In The 5th International Conference on Electrical Engineering (ICEE-B), pp. 5386-6869. IEEE, Boumerdes, Algeria, 2017.

[2]. Poonam Jagannath Shinde and Madhumita Chatterjee. "A Novel Approach for Classification and Detection of DOS Attacks." In International Conference on Smart City and Emerging Technology (ICSCET), pp. 1109-8537. IEEE, 2018.

[3]. Neha G. Relan and Prof. Dharmaraj R. Patil. "Implementation of Network Intrusion Detection System using Variant of Decision Tree Algorithm." In International Conference on Nascent Technologies in the Engineering Field (ICNTE), pp. 4799-7263. IEEE, 2015.

[4]. Wentao Liu. "Research on DOS Attack and Detection Programming." In Third International Symposium on Intelligent Information Technology Application (ISIITA), pp. 7695-3859. IEEE, 2009.

[5]. Ivan Burmaka, Stanislav Zlobin, Svitlana Lytvyn and Valentin Nekhai. "Detecting Flood Attacks and Abnormal System Usage with Artificial Immune System." International Scientific-Practical Conference on Mathematical Modeling and Simulation of Systems (MODS), pp. 131–143. Springer, 2020.

[6]. Bo Li, Minghui Gao, Li Ma, Ye Liang and Guifeng Chen. "Web Application-

[7]. Layer DDOS Attack Detection Based on Generalized Jaccard Similarity and Information Entropy." In International Conference on Artificial Intelligence and Security (ICAIS), pp. 576-585. Springer, 2019.

[8]. K. Munivara Prasad, A. Rama Mohan Reddy and K.Venugopal Rao."DOS and DDOS Attacks: Defense, Detection and Traceback Mechanisms -A Survey." In Global Journal of Computer Science and Technology: E Network, Web & Security, Vol.14, no.7, pp. 10975-4172. Global Journals, 2014.

[9]. Deepak Kshirsagar, Suraj Sawant, Amit Rathod and Sachin Wathore. "CPU Load Analysis & Minimization for TCP SYN Flood Detection." In International Conference on Computational Modeling and Security (CMS 2016), pp.1877-0509. Elsevier, 2016.

[10]. Miroslav Dulik jr. "Network attack using TCP protocol for performing DOS and DDOS attacks." In International Scientific Conference. IEEE, 2019.

[11]. Robert Shimonsk, "Certified Ethical Hacker Version 9 Study Guide", 2016.

[12]. Ramon Base, "Computer Networking Hacking", July 26, 2019.