



All



ADVANCED SEARCH

Conferences > 2023 International Conference... ?

Detection of Denial of Service Attacks Using SNMP-MIB in Internet of Things Environment

Publisher: IEEE

Cite This

PDF

R. Vijayarangan ; Sumathi Loganathan ; V. Thirumurugan ; I Poonguzhali ; A C Ramachandra All Authors



93 Full Text Views

Alerts

Manage Content Alerts Add to Citation Alerts

Abstract

Document Sections

- I. Introduction
- II. Related Works
- III. Methodology
- IV. Result and Discussions
- V. Conclusions

Authors

Figures

References

Keywords

Metrics



Download PDF

Abstract:

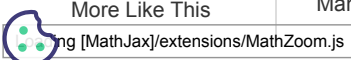
The Internet is a vast system of interconnected networks that provide a variety of services. More than a million people join the World Wide Webs every day, making it a po... **View more**

Metadata

Abstract:

The Internet is a vast system of interconnected networks that provide a variety of services. More than a million people join the World Wide Webs every day, making it a powerful force. Approximately 70% of businesses are considering making the switch to cloud services due to the many benefits and pay-as-you-go structure of cloud computing. DoS attacks, which interrupt internet services, are a common kind of cybercrime. Distributed DoS assaults (or DDoS for short) happen when the same DoS comes in from several different places at once. DoS severely destroys the availability limitation of online services, hence early detection is crucial. The DoS attack type known as TCPSYN causes the TCP protocol's connection setup procedure to fail, leading to partially open connections. TCP-SYN is used to force a web server to crash by using up all of its resources. Despite ongoing efforts at repair, attacks against TCP-SYN continue to increase in frequency and sophistication. Therefore, in today's digital environment, it is envisaged that the solution would completely mitigate such threats. A multi-level detection strategy that integrates SNMP and incoming request analysis is offered as a means to early detection and cost-effectiveness. The basic goal of SNMP is to achieve maximum effectiveness in distinguishing TCP-SYN from valid traffic in a shorter time span. Using the SNMP Management Information Base (MIB) variables, a TCP-SYN attack may be spotted in two stages. Theoretical validation

More Like This



is used to determine which MIBs should be used, and feature selection approaches have been verified using the prediction and accuracy metrics of linear regression.

Published in: 2023 International Conference on Applied Intelligence and Sustainable Computing (ICAISC)

Date of Conference: 16-17 June 2023

DOI: 10.1109/ICAISC58445.2023.10199348

Date Added to IEEE Xplore: 09 August 2023

Publisher: IEEE

► ISBN Information:

Conference Location: Dharwad, India

 Contents

I. Introduction

Rapid advancements in data storage, processing power, and lower prices have made IT more accessible and commonplace. As computational power continues to expand rapidly, new security vulnerabilities are opening up as a result of these developments in technology [1]. The cyberspace is the internet-connected environment, which has infinite access points and thus presents inherent vulnerabilities that cannot be eliminated. Risk variables such as sector interdependence, exposure point proliferation, and asset concentration are monitored and controlled in the present context. The economy, public safety, and national security all depend on these services being available and undamaged. There has been a rise in both the frequency and complexity of attacks on internet services. If an assault is successful, it will have a devastating effect on any services that rely on the internet. The financial, legal, and reputational repercussions of a security breach touch every industry [2]. To disrupt the service or information stored in a computer system, infrastructure, crucial network, or personal computer, an offensive manoeuvre known as a security assault may be undertaken against an individual or organisation. The goal of the assault is to corrupt, steal from, or otherwise interfere with the targeted internet services. Common security vulnerabilities include compromises to online services' confidentiality, integrity, and availability (CIA) (Stallings, 2006). A denial-of-service (DoS) assault is one kind of cyberattack that often occurs. The goal of a denial-of-service (DoS) attack is to temporarily or permanently interrupt an online service, rendering the targeted computer system or network resource inaccessible to its intended users. It works by overwhelming the targeted system with so much traffic that it either slows down or crashes [3]. Data on Dos Attacks are shown in Fig. 1.

Authors	▼
Figures	▼
References	▼
Keywords	▼
Metrics	▼

More Like This

A thrust force characteristics measurement of the planar switched reluctance motor using flux linkage characteristics
2014 17th International Conference on Electrical Machines and Systems (ICEMS)
Published: 2014

Measurement of ion parameters during a forced switching off of current in vacuum
IEEE Transactions on Plasma Science
Published: 1997

Show More

IEEE Personal Account

CHANGE
USERNAME/PASSWORD

Purchase Details

PAYMENT OPTIONS
VIEW PURCHASED
DOCUMENTS

Profile Information

COMMUNICATIONS
PREFERENCES
PROFESSION AND
EDUCATION
TECHNICAL INTERESTS


Need Help?

US & CANADA: +1 800
678 4333
WORLDWIDE: +1 732
981 0060
CONTACT & SUPPORT

Follow



Loading [MathJax]/extensions/MathZoom.js

[About IEEE Xplore](#) | [Contact Us](#) | [Help](#) | [Accessibility](#) | [Terms of Use](#) | [Nondiscrimination Policy](#) | [IEEE Ethics Reporting](#)  | [Sitemap](#) | [IEEE Privacy Policy](#)

A not-for-profit organization, IEEE is the world's largest technical professional organization dedicated to advancing technology for the benefit of humanity.

© Copyright 2024 IEEE - All rights reserved, including rights for text and data mining and training of artificial intelligence and similar technologies.

IEEE Account

- » [Change Username/Password](#)
- » [Update Address](#)

Purchase Details

- » [Payment Options](#)
- » [Order History](#)
- » [View Purchased Documents](#)

Profile Information

- » [Communications Preferences](#)
- » [Profession and Education](#)
- » [Technical Interests](#)

Need Help?

- » **US & Canada:** +1 800 678 4333
- » **Worldwide:** +1 732 981 0060
- » [Contact & Support](#)

[About IEEE Xplore](#) | [Contact Us](#) | [Help](#) | [Accessibility](#) | [Terms of Use](#) | [Nondiscrimination Policy](#) | [Sitemap](#) | [Privacy & Opting Out of Cookies](#)

A not-for-profit organization, IEEE is the world's largest technical professional organization dedicated to advancing technology for the benefit of humanity.

© Copyright 2024 IEEE - All rights reserved. Use of this web site signifies your agreement to the terms and conditions.