



SWINBURNE
UNIVERSITY OF
TECHNOLOGY

Swinburne University of Technology
Faculty of Science, Engineering and Technology

ASSIGNMENT AND PROJECT COVER SHEET

Unit Code: COS30015 Unit Title: IT Security

Assignment number and title: No. 2 - Practical Project Due date: 06/08/2023

Lab group: Group 2 Tutor: Dr. Anh Ngoc Le Lecturer: Dr. Anh Ngoc Le

Family name: Trac Duc Anh Luong Identity no: 103488117

Other names: _____

To be completed if this is an INDIVIDUAL ASSIGNMENT

I declare that this assignment is my individual work. I have not worked collaboratively, nor have I copied from any other student's work or from any other source except where due acknowledgment is made explicitly in the text, nor has any part been written for me by another person.

Signature: Trac Duc Anh Luong

To be completed if this is a GROUP ASSIGNMENT

We declare that this is a group assignment and that no part of this submission has been copied from any other student's work or from any other source except where due acknowledgment is made explicitly in the text, nor has any part been written for us by another person.

ID Number	Name	Signature
_____	_____	_____
_____	_____	_____

Marker's comments:

Total Mark: _____

Extension certification:

This assignment has been given an extension and is now due on _____

Signature of Convener: _____ Date: _____ / 2022

COS30015 - IT Security

Assignment 2: Practical Project

Denial of Service Attack on IoT Devices and Prevention Method

Author: Trac Duc Anh Luong

Submission Date: 06/08/2023

Abstract

The increase in Internet of Things (IoT) devices has brought unprecedented convenience and connectivity to various domains and introduced new security challenges. Among the most significant threats IoT devices face is Denial of Service (DoS) attacks. In this research, we experimented to assess the efficacy of DoS attack tools and defence mechanisms on IoT devices. The DoS attack simulation used the nping tool to generate a TCP SYN flood directed towards an IoT edge device. The results demonstrated the susceptibility of IoT devices to DoS attacks, with a high failure rate in establishing connections, leading to resource exhaustion and service disruptions. To counteract DoS attacks, we implemented Cloudflare Web Application Firewall (WAF) as a defence mechanism. Cloudflare WAF proactively inspects and filters incoming traffic, blocking malicious requests before reaching the IoT device. The defence mechanism successfully mitigated the impact of the DoS attack, safeguarding the IoT device's integrity and availability. Overall, this research highlights the importance of bolstering IoT device security to defend against evolving cyber threats. By adopting advanced security solutions like Cloudflare WAF, organisations can ensure the resilience of their IoT devices and maintain network integrity. The findings dedicate to a broader understanding of IoT device security and provide practical recommendations to enhance protection against DoS attacks and other cyber threats in the IoT ecosystem.

Introduction

The rapid growth and integration of Internet of Things (IoT) devices have revolutionised various industries and transformed our everyday lives (Sisinni et al., 2018). However, this rapid expansion also brings new challenges, particularly concerning cybersecurity. One of the most concerning threats IoT devices face is Denial of Service (DoS) attacks.

DoS attacks happen when hostile actors try to flood a target network or system with unwanted traffic or requests. These attacks can quickly exhaust the resources of the targeted IoT device, rendering it unresponsive to legitimate users and services. Compromised IoT devices are frequently harnessed to form botnets, amplifying the scale and impact of DoS attacks. Botnets composed of IoT devices can launch massive and coordinated attacks on targets, overwhelming even well-protected networks. In addition to the potential for network disruption, DoS attacks on IoT devices can lead to data breaches and privacy violations. Many IoT devices collect and process sensitive data, such as personal information or operational data, in industrial settings (Chow, 2017). If an attacker successfully takes control of these devices, people and organisations could suffer greatly.

The experiment conducted for this research aims to assess the effectiveness of DoS attack tools and defence mechanisms on a set of IoT devices. Using a well-known DoS attack tool like nping, we seek to gain insights into their functionalities and understand how they can overload and disrupt IoT devices. To counteract the DoS attack, we implemented Cloudflare Web Application Firewall (WAF), a highly advanced security solution designed to protect responsive web applications and high-traffic APIs from various threats, including DDoS attacks. Cloudflare WAF intelligently inspects and filters incoming traffic, blocking malicious requests before they reach the origin server, ensuring robust protection against DoS and other cyber threats, and providing a fortified defence for a safer and more resilient web environment (developers.cloudflare.com, 2023).

The outcomes of this experiment will contribute to the broader understanding of IoT device security and the measures needed to protect these devices from evolving cyber threats. With the knowledge gained from the evaluation, we can provide practical recommendations to enhance the security of IoT devices, fortify network infrastructure, and mitigate the risk of DoS attacks.

Planning and Justification

DoS Attack

Cyber attacks known as Denial of Service (DoS) overwhelm a target system with excessive traffic, rendering it unavailable to legitimate users (Zhang et al., 2016). With the rise of IoT devices, DoS attacks have become a significant threat, as IoT devices often lack robust security measures (Liang et al., 2016). Attackers use various methods, including volumetric attacks, TCP state exhaustion, and application layer attacks, to disrupt services and networks. DoS attacks pose serious risks, leading to service disruptions, financial losses, and reputational damage.

For IoT devices, the implications are even more dire, as these attacks can lead to critical service disruptions, such as disabling essential functions in smart homes, healthcare devices, or critical infrastructure (Sinha and G, 2021). Moreover, compromised data integrity resulting from a successful DoS attack can lead to data breaches, privacy violations, and potentially life-threatening situations. Therefore, it is of utmost importance for IoT device manufacturers, service providers, and users to prioritise cybersecurity efforts. Implementing robust security measures, including device authentication, encryption, and regular software updates, is vital to fortify IoT devices against potential DoS attacks (Huraj, Simon and Horák, 2018). Additionally, continuous monitoring and timely detection of suspicious activities can help identify and mitigate threats promptly, safeguarding IoT ecosystems from the devastating impact of DoS attacks. By collectively addressing these challenges, we can create a safer and more resilient IoT

environment, enabling the full potential of IoT technology while minimising the risks posed by cyber threats.

Framework Implementation

Attacking Framework

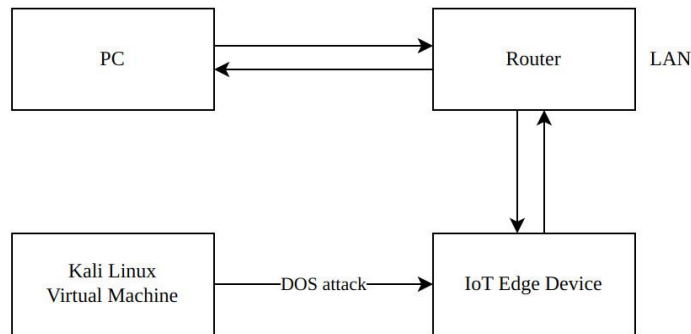


Figure 1: Attack framework for the project

This section will describe the attack framework implemented for conducting the DoS attack on an IoT edge device using Kali Linux Virtual Machine. The attack framework involves the following components:

- **Kali Linux Virtual Machine (Attacker):** Kali Linux is a specialised penetration testing platform known for its extensive collection of security tools. In our framework, Kali Linux is the attacker, running the DoS attack tool (nping) to generate malicious traffic and overwhelm the IoT edge device.
- **IoT Edge Device (Victim):** The IoT edge device represents a typical IoT device with limited computing resources. It is the target of the DoS attack, and its performance and functionality will be monitored during the experiment.
- **Router (LAN):** The router is the gateway between the IoT edge device and the local area network (LAN). It facilitates communication between the IoT device and other devices on the network.
- **Personal Computer (PC):** The personal computer is used to monitor the experiment, capture network traffic, and analyse the results of the DoS attack.

Defending Framework

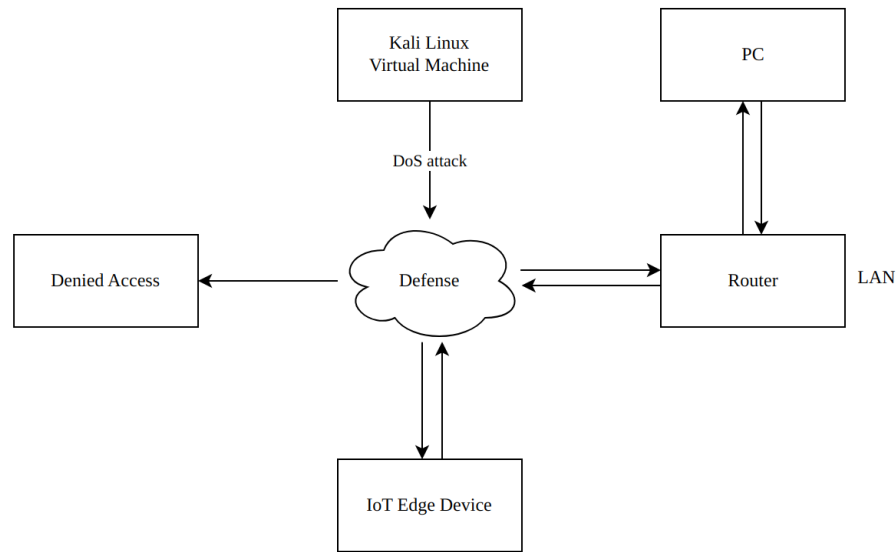


Figure 2: Defense framework for the project

We must deploy a new component in our IoT Edge Device, Cloudflare WAF, for the defence mechanism framework. The defence framework involves the following components:

- **Kali Linux Virtual Machine (Attacker):** Kali Linux is the attacking platform, launching a Denial of Service (DoS) attack on the network's vulnerable IoT Edge Device. It generates a high volume of network traffic to overwhelm the target.
- **IoT Edge Device:** The IoT Edge Device is the target of the DoS attack. As a part of the Internet of Things (IoT) network, it may need more robust defence mechanisms against such attacks.
- **Cloudflare WAF (Defender):** Cloudflare Web Application Firewall (WAF) is the defence mechanism in the framework, protecting the IoT Edge Device. As a robust security solution, Cloudflare WAF blocks malicious requests in real-time, preventing DoS attacks from reaching the IoT Edge Device. Proactive filtering at Cloudflare's edge servers ensures a secure and resilient defence, safeguarding the IoT device and maintaining network integrity.
- **Router (LAN):** The Router is the gateway connecting the IoT Edge Device to the LAN. It routes incoming traffic, including the DoS attack, and manages communication within the local network.
- **Personal Computer (PC):** The PC represents a regular user or a device on the same LAN. While not the direct target of the DoS attack, it may be indirectly affected if sharing resources with the IoT Edge Device.

Project's equipment

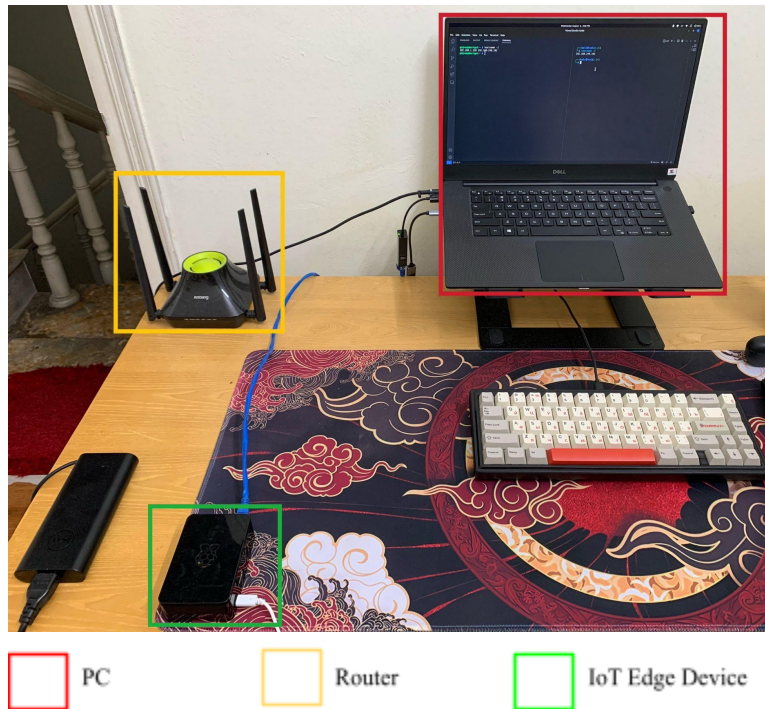


Figure 3: Equipments for the project

The red box highlights our PC, which hosts our Kali Linux Virtual Machine. The green box highlights our IoT Edge Device, the Raspberry Pi. The yellow box highlights our router. The PC and the IoT Edge Device are connected to the LAN via the router.

Implemented Softwares and Commands

In this research, we utilise a set of software tools and commands divided into three sections: Attacking Tool, Defending Tool, and Other Supporting Tools, to conduct our experiments.

Attacking Tool

Nping, a powerful tool within the Nmap suite, is a versatile packet generator that allows us to send a wide range of network packets with fine-grained control (Gordon Fyodor Lyon, 2008). This flexibility enables us to precisely tailor our attack scenarios and simulate various Denial of Service (DoS) attacks. By customising the packet content, timing, and frequency, we can generate a high traffic volume directed towards the IoT device, effectively overwhelming its resources and testing its resilience under different attack scenarios. Nping's ability to manipulate packet headers and payloads give insight into how the target device responds to different types of network traffic and helps us identify potential vulnerabilities and weak points in its defence mechanisms. By analysing the impact of nping-generated traffic on the IoT device, we can better

understand its susceptibility to DoS attacks and evaluate the effectiveness of our defence mechanisms in safeguarding against such threats.

Defending Tool

We will leverage Cloudflare Web Application Firewall (WAF) for the Defence Mechanism. As a robust and sophisticated security solution, Cloudflare WAF is the first line of defence for the IoT Edge Device. It intelligently analyses incoming HTTP/HTTPS traffic, utilising a wide range of predefined rules and custom configurations to detect and block malicious requests in real-time. This proactive approach effectively mitigates DoS attacks and various cyber threats. Cloudflare WAF maintains an extensive database of known malicious domains and continuously updates it to stay ahead of emerging threats. When a malicious request is detected, Cloudflare WAF promptly blocks it at the edge servers, preventing it from reaching the IoT Edge Device. The mitigation ensures a secure and resilient defence, safeguarding the integrity and availability of the IoT device and maintaining a robust network environment.

Other Supporting Tools

In addition to the main tools, we use several supporting software to monitor, access, and capture data during the experiment:

1. **top**: This system monitoring tool enables us to observe the Raspberry Pi's resource utilisation, such as CPU and memory usage, during the DoS attacks. It helps us assess the impact on the IoT device's performance.
1. **ssh**: Secure Shell (SSH) allows us to securely access both the attacker (Kali Linux Virtual Machine) and the victim (IoT edge device) using our personal computer. SSH ensures encrypted communication and secure remote access.
2. **Virtualbox**: We use Virtualbox as the hosting system for the Kali Linux Virtual Machine, providing a virtualised environment to run the attacking tools safely.
3. **Wireshark**: This network packet analyser captures and analyses packets sent and received from the Kali Linux machine during the DoS attack. Wireshark helps us examine the attack traffic and understand the attack patterns (Sandhya et al., 2017).

By utilising this diverse set of software tools and commands, we can comprehensively evaluate DoS attacks on IoT edge devices and assess the effectiveness of defence mechanisms in safeguarding these devices from potential threats.

Application of Tools and Methods

Preparation for experiment

The PC, virtual machine, and sensor nodes are all given IP addresses by the router, which also connects them to the local area network (LAN). Finding out the IP addresses of various components should come first. Table I lists the components along with their IP addresses.

Device	System Information	Role	IP Address	MAC Address
PC	Linux mint 5.15.0-78-generic	Hosting Server	192.168.249.244	3c:9c:0f:08:e9:4a
Virtual Machine	Linux kali 6.3.0-kali1-amd64	Attacker	192.168.249.164	b8:27:eb:3d:35:bc
Raspberry Pi 3B+	Linux raspberrypi 5.15.32-v7+	Victim	192.168.249.102	08:00:27:53:0c:ba
Antbang Router	ANTBANG_A3_V2	Local Network Gateway	192.168.249.1	00:1c:a3:0b:8b:3b

Table 1: IP and MAC address of the experiment's components

After setting up the devices, we must test our connection via the ping command. Other statuses of the Raspberry Pi were also recorded, including the CPU(s) and the Memory utility.

Status	CPU(s) idling (%)	Memory used (MiB)	Average response time (ms)
Initial status	99.8	179.1	0
Status when testing connection with ping command	96.1	179.3	41.079

Table 2: Result from connection test using the ping command

The data shows that the CPU and Memory resources are mostly free, with a sub-second response time from the Kali Linux and the Raspberry Pi, indicating the unrestricted connection between these two devices.

Attacking Results

To bolster the IoT Edge Device's resilience against potential Denial of Service (DoS) attacks, we opted for nping as our chosen tool for conducting the attack. nping serves as a potent and versatile packet generator, empowering us to simulate various types of DoS attacks with fine-grained control over the network traffic. Through nping's capabilities, we can precisely craft attack scenarios, test the IoT device's susceptibility to different attack vectors, and gain valuable insights into its defence mechanisms.

The command used for nping is

nping -tcp-connect -p 80 -rate=100000 -c 100000 -q 192.168.249.102

Explanation of the parameters:

Parameter	Functionality
-tcp-connect	Unprivileged TCP connect probe mode.
-p	Set destination port(s).
-rate	Set the number of packets per second.
-c	Set the number of rounds to stop.
-q	Decrease verbosity level by one.

Table 3: Explanation of parameters used for nping

After launching the attack, we can see the returned results from the Kali Linux machine.

- TCP connection attempts: 100000
- Successful connections: 30460 (30.46%)
- Failed connections 69540 (69.54%)
- Time taken: 52.98s

During the attack, the victim's resources registered **87.4%** of the CPU idling, with **185.1 MiB** in memory resources used.

For this project, we also set up a sample social media page hosted locally using Apache HTTP Server on port 80 of the Raspberry Pi, featuring a login.php page that would be susceptible to a DoS attack.

My Friends System Log in Page

Email

Password

[Home](#)

Figure 4: Sample login.php page hosted on the victim.

Service Unavailable

HTTP Error 503. The service is unavailable.

Figure 5: Returned error from successful DoS attack

During the attack, the web was not accessible and returned error code 503, “Service Temporarily Unavailable”.

8481...	505.277195048	192.168.249.164	192.168.249.102	TCP	66 35118 → 80 [ACK] Seq=2
8481...	505.277028809	192.168.249.102	192.168.249.164	TCP	66 80 → 35476 [FIN, ACK] :
8481...	505.277258806	192.168.249.164	192.168.249.102	TCP	66 35476 → 80 [ACK] Seq=2
8481...	505.277028963	192.168.249.102	192.168.249.164	TCP	66 80 → 36248 [FIN, ACK] :
8481...	505.277288786	192.168.249.164	192.168.249.102	TCP	66 36248 → 80 [ACK] Seq=2
8481...	505.277029056	192.168.249.102	192.168.249.164	TCP	66 80 → 42202 [FIN, ACK] :
8481...	505.277325234	192.168.249.164	192.168.249.102	TCP	66 42202 → 80 [ACK] Seq=2
8481...	505.277359124	192.168.249.102	192.168.249.164	TCP	66 80 → 41656 [FIN, ACK] :
8481...	505.277367622	192.168.249.164	192.168.249.102	TCP	66 41656 → 80 [ACK] Seq=2
8481...	505.277359236	192.168.249.102	192.168.249.164	TCP	66 80 → 43304 [FIN, ACK] :
8481...	505.277394361	192.168.249.164	192.168.249.102	TCP	66 43304 → 80 [ACK] Seq=2
8481...	505.277359344	192.168.249.102	192.168.249.164	TCP	66 80 → 42332 [FIN, ACK] :
8481...	505.277417144	192.168.249.164	192.168.249.102	TCP	66 42332 → 80 [ACK] Seq=2
8481...	505.277359439	192.168.249.102	192.168.249.164	TCP	66 80 → 46578 [FIN, ACK] :
8481...	505.277439264	192.168.249.164	192.168.249.102	TCP	66 46578 → 80 [ACK] Seq=2
8481...	505.277359534	192.168.249.102	192.168.249.164	TCP	66 80 → 40332 [FIN, ACK] :
8481...	505.277471940	192.168.249.164	192.168.249.102	TCP	66 40332 → 80 [ACK] Seq=2
8481...	505.277359631	192.168.249.102	192.168.249.164	TCP	66 80 → 44816 [FIN, ACK] :
8481...	505.277498946	192.168.249.164	192.168.249.102	TCP	66 44816 → 80 [ACK] Seq=2
8481...	505.277359724	192.168.249.102	192.168.249.164	TCP	66 80 → 40000 [FIN, ACK] :
8481...	505.277523565	192.168.249.164	192.168.249.102	TCP	66 40000 → 80 [ACK] Seq=2
8481...	505.277359821	192.168.249.102	192.168.249.164	TCP	66 80 → 42482 [FIN, ACK] :
8481...	505.277546956	192.168.249.164	192.168.249.102	TCP	66 42482 → 80 [ACK] Seq=2

Figure 5: TCP SYN flood from nping

Figure 5 shows that Wireshark captured TCP SYN packets, revealing the attacker's and the victim's interaction. The sender initiates a series of SYN packets to establish connections, while the target responds with SYN-ACK packets to acknowledge the requests. However, due to the high packet transmission rate, some SYN-ACK packets may be lost or dropped, leading to TCP retransmissions. These retransmissions and their corresponding ACK packets can be observed in the captured data. The analysis provides insights into the success rate of connection establishment and potential network congestion during the nping DoS attack simulation.

Defending Results

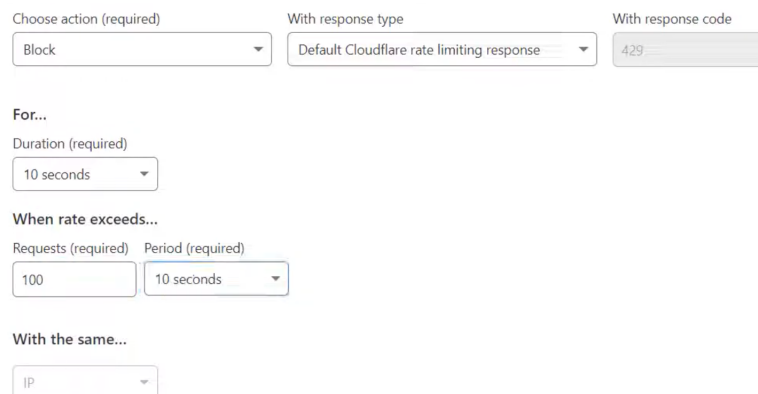
To enhance the security of the IoT Edge Device against potential Denial of Service (DoS) attacks, we implemented Cloudflare Web Application Firewall (WAF) as a robust defence mechanism. Cloudflare WAF is a sophisticated security solution designed to combat various cyber threats, including DoS attacks.

The first step in the configuration process involved setting up Cloudflare WAF through the Cloudflare platform. We accessed the "Security" section and then navigated to "WAF."

Subsequently, we created a limiting rule named "antidos," specifically tailored to counteract DoS attacks effectively. The rule was designed to trigger when incoming requests did not match the condition of an "Empty URI Path" being "/login.php". This condition was indicated by the expression preview "not http.request.uri.path in {"/login.php"}."

To take action against malicious requests, we selected the "Block" action for this rule and set the duration to 10 seconds. This configuration meant that any requests exceeding the limit of 100 within a 10-second interval would be blocked for 10 seconds.

Leveraging Cloudflare's rate-limiting feature, the rule was triggered when a user's requests exceeded 100 within a 10-second timeframe. Rate limiting was applied based on the user's IP address.



The screenshot displays the configuration for a Cloudflare WAF rule. At the top, there are three fields: "Choose action (required)" set to "Block", "With response type" set to "Default Cloudflare rate limiting response", and "With response code" set to "429". Below these, the "For..." section shows "Duration (required)" set to "10 seconds". The "When rate exceeds..." section has "Requests (required)" set to "100" and "Period (required)" set to "10 seconds". At the bottom, the "With the same..." section is set to "IP".

Figure 6: Cloudflare WAF settings

The impact of this defence mechanism was significant. When the Cloudflare WAF rule was activated, any user attempting to surpass the threshold of 100 requests in 10 seconds would be temporarily blocked. Cloudflare displayed the error message "Error 1015: You are being rate-limited" to the blocked user. After the 10-second block period, the user regained access to the server.

Error 1015

You are being rate limited

What happened?

The owner of this website has banned you temporarily from accessing this website.

Figure 7: Returned error from failed DoS attack

5671..	345.990206788	192.168.249.102	192.168.249.164	TCP	60 49223 → 47962 [RST, ACK]
5671..	345.990206839	192.168.249.102	192.168.249.164	TCP	60 4086 → 47962 [RST, ACK]
5671..	345.990206893	192.168.249.102	192.168.249.164	TCP	60 40647 → 47962 [RST, ACK]
5671..	345.990206949	192.168.249.102	192.168.249.164	TCP	60 53414 → 47962 [RST, ACK]
5671..	345.990238670	192.168.249.102	192.168.249.164	TCP	60 25879 → 47962 [RST, ACK]
5671..	345.990238739	192.168.249.102	192.168.249.164	TCP	60 53253 → 47962 [RST, ACK]
5671..	345.990238799	192.168.249.102	192.168.249.164	TCP	60 3690 → 47962 [RST, ACK]
5671..	345.990238855	192.168.249.102	192.168.249.164	TCP	60 52627 → 47962 [RST, ACK]
5671..	345.990238916	192.168.249.102	192.168.249.164	TCP	60 60900 → 47962 [RST, ACK]
5671..	345.990238978	192.168.249.102	192.168.249.164	TCP	60 36369 → 47962 [RST, ACK]
5671..	345.990239020	192.168.249.102	192.168.249.164	TCP	60 51770 → 47962 [RST, ACK]
5671..	345.990239092	192.168.249.102	192.168.249.164	TCP	60 43677 → 47962 [RST, ACK]
5671..	345.990314007	192.168.249.102	192.168.249.164	TCP	60 10214 → 47962 [RST, ACK]
5671..	345.990314069	192.168.249.102	192.168.249.164	TCP	60 55121 → 47962 [RST, ACK]
5671..	345.990314135	192.168.249.102	192.168.249.164	TCP	60 20860 → 47962 [RST, ACK]
5671..	345.990314195	192.168.249.102	192.168.249.164	TCP	60 50994 → 47962 [RST, ACK]
5671..	345.990314262	192.168.249.102	192.168.249.164	TCP	60 29949 → 47962 [RST, ACK]
5671..	345.990314321	192.168.249.102	192.168.249.164	TCP	60 26850 → 47962 [RST, ACK]
5671..	345.990314377	192.168.249.102	192.168.249.164	TCP	60 51082 → 47962 [RST, ACK]
5671..	345.990314438	192.168.249.102	192.168.249.164	TCP	60 22589 → 47962 [RST, ACK]
5671..	345.990340942	192.168.249.102	192.168.249.164	TCP	60 1367 → 47962 [RST, ACK]
5671..	345.990341010	192.168.249.102	192.168.249.164	TCP	60 27484 → 47962 [RST, ACK]
5671..	345.990341069	192.168.249.102	192.168.249.164	TCP	60 20887 → 47962 [RST, ACK]

Figure 8: Denied TCP SYN packets captured in Wireshark

During the DoS attack simulation, Cloudflare WAF effectively mitigated the impact on the IoT Edge Device. It dynamically blocked excessive requests from potentially malicious sources, substantially bolstering the device's security and ensuring a stable and resilient network environment.

Throughout the experiment, the implemented Cloudflare WAF rule successfully defended against the DoS attack, preventing malicious requests from reaching the IoT Edge Device's origin server. This proactive approach significantly reduced the device's exposure to attacks and maintained its availability and integrity. The successful evaluation of Cloudflare WAF emphasises the importance of advanced security solutions in safeguarding IoT devices from evolving cyber threats.

Analysis of Results

Attacking Method

The Denial of Service (DoS) attack conducted using the nping tool on the IoT Edge Device aimed to assess the effectiveness of the attack tool and its impact on the target system. The nping attack simulated a TCP SYN flood, where the attacker generated massive network traffic directed towards the victim's IoT device. This attack aimed to overwhelm the device's resources and disrupt its normal operations, rendering it unresponsive to legitimate users and services.

During the DoS attack, nping was configured to launch 100,000 TCP connection attempts on the IoT Edge Device. The results showed that only 30.46% of these attempts were successful, while 69.54% of the connections failed. The high failure rate indicated that the IoT device's resources were overwhelmed by the continuous barrage of malicious traffic. As a result, the device struggled to process incoming requests, leading to delays, timeouts, and, in some cases, complete unresponsiveness.

Wireshark packet analysis during the nping attack provided further visibility into the attack patterns. The captured data revealed many TCP SYN packets being sent by the attacker to initiate connections with the IoT device. In response, the victim IoT device sent SYN-ACK packets to acknowledge the connection requests. However, some SYN-ACK packets were lost or dropped due to the attack's intensity and the IoT device's limited resources. These dropped packets resulted in TCP retransmissions, adding to the device's workload and exacerbating resource exhaustion.

The high resource utilisation during the attack was also observed using the 'top' system monitoring tool. The IoT device's CPU utilisation was significantly impacted, with only 12.6% of the CPU idle during the attack, compared to 99.8% in the initial state.

Additionally, the device's memory usage increased to 185.1 MiB from 179.3 MiB during the attack, indicating a considerable strain on its computing resources.

Overall, the results of the DoS attack using nping highlighted the vulnerability of IoT devices to such attacks. Without adequate protection and mitigation measures, a malicious actor could easily disrupt the functionality of IoT devices, leading to service disruptions, financial losses, and reputational damage.

Defending Method

Analysing the defence mechanism implemented through Cloudflare Web Application Firewall (WAF) demonstrated its effectiveness in mitigating the DoS attack and providing robust protection for the IoT Edge Device. Cloudflare WAF, as a sophisticated security solution, proactively inspects incoming HTTP/HTTPS traffic and intelligently detects and blocks malicious requests in real-time. This proactive approach prevents malicious traffic, including DoS attacks, from reaching the IoT device's origin server, ensuring its security and availability.

Implementing rate-limiting rules on Cloudflare WAF was crucial in handling the DoS attack. The defence mechanism dynamically blocked excessive requests from specific IP addresses, efficiently defending against the attack and mitigating its impact on the IoT Edge Device's resources. When the attack threshold was surpassed, users attempting to access the IoT Edge Device received the "Error 1015: You are being rate-limited" message, indicating a temporary block for 10 seconds. After the block period, the server became accessible again, ensuring that legitimate users could continue to access the device while malicious traffic was effectively filtered out.

Cloudflare WAF's ability to detect and block DoS attacks in real-time ensured the stability and resilience of the IoT device during the experiment. By maintaining an extensive database of known malicious domains and continuously updating its threat intelligence, Cloudflare WAF stayed ahead of emerging threats and provided proactive protection against new attack vectors.

The effectiveness of the defence mechanism was also evident in the Wireshark packet analysis during the attack. The captured data showed that Cloudflare WAF successfully blocked malicious traffic before reaching the IoT device, as indicated by the absence of certain malicious packets. This proactive filtering at Cloudflare's edge servers significantly reduced the device's exposure to attacks and ensured a secure and resilient defence.

Overall, the successful analysis of Cloudflare WAF as a defence mechanism underscores the importance of incorporating advanced security solutions to protect IoT devices from the growing threat landscape. The experiment's results provide practical insights into the efficiency of Cloudflare WAF in countering DoS attacks and highlight its role in fortifying the security posture of IoT devices. Organisations can effectively safeguard their IoT devices, maintain network integrity, and protect sensitive data from potential cyber threats by deploying robust defence mechanisms like Cloudflare WAF.

Evaluation

This research report aims to provide a thorough and insightful perspective on Denial of Service (DoS) attacks on IoT devices and the implementation of Cloudflare Web Application Firewall (WAF) as a defence mechanism. We have effectively addressed the increase in IoT devices and the resulting security challenges, particularly the significant threat of DoS attacks. Through the nping tool, the study successfully demonstrates the vulnerability of IoT devices to DoS attacks, with a high failure rate in establishing connections, leading to resource exhaustion and service disruptions. This finding highlights the urgent need for robust security measures to protect IoT devices from evolving cyber threats (Roukounaki et al., 2019).

The implementation of Cloudflare Web Application Firewall (WAF) as a defence mechanism is critically evaluated, showcasing its proactive approach in inspecting and filtering incoming traffic to block malicious requests before reaching the IoT device. The Cloudflare WAF successfully mitigated the impact of the DoS attack, ensuring the integrity and availability of the IoT device during the experiment. The mitigation highlights Cloudflare WAF as an advanced security solution capable of defending against various cyber threats, including DoS attacks. The research implementation recognises the significance of such defence mechanisms in safeguarding IoT devices from potential threats and maintaining network integrity.

The experiment provides a contrasting perspective by comparing the research with current and future factors in the cybersecurity landscape. It acknowledges the rapid growth of IoT devices and the increasing need to address their security vulnerabilities (Iqbal et al., 2020). Organisations can protect their IoT devices from the growing threat landscape by adopting advanced security solutions like Cloudflare WAF. The research emphasises the importance of continuous integration and update of security measures to stay ahead of emerging threats, acknowledging the dynamic nature of the cybersecurity landscape.

Based on the research findings, practical recommendations are offered, providing insights into enhancing IoT device security. The research underscores the need for robust defence mechanisms and continuous research to ensure the resilience of IoT devices against cyber threats. Organisations can effectively safeguard their IoT devices and maintain a secure and resilient network environment by implementing innovative security solutions like Cloudflare WAF and proactively monitoring network traffic.

Furthermore, the research delves into the potential implications of the findings in the broader security landscape. It highlights the growing significance of IoT devices in various industries and everyday life, leading to an increased attack surface for malicious actors. The research findings underscore the pressing need for organisations to prioritise IoT device security and adopt comprehensive defence mechanisms to counteract sophisticated cyber threats like DoS attacks.

This research also considers the potential challenges and limitations faced during the experiment. While nping proved a powerful tool for conducting DoS attack simulations, it may only partially represent the vast array of attack vectors that real-world attackers can employ. The research experiment was also shown in a controlled environment, which may not accurately mirror the complexities and variations in network environments. As such, the research evaluation emphasises the importance of continuous research and real-world testing to understand better and address the evolving landscape of IoT device security.

The research evaluation provides a forward-looking perspective by discussing the implications of the research findings for future IoT security measures. It recognises that the security landscape will continue to evolve, with attackers becoming dangerous and IoT devices becoming even more pervasive (Kumar and Paidi Raja Ramesh, 2018). This evaluation calls for a proactive approach to developing and deploying security solutions that can adapt to new and emerging threats. Moreover, the review highlights the need for collaboration among industry stakeholders, researchers, and policymakers to establish comprehensive security standards and best practices for IoT devices (Zuo et al., 2020).

The practical recommendations presented in this evaluation provide actionable insights for organisations seeking to enhance their IoT device security. Organisations can effectively detect and mitigate potential DoS attacks and other cyber threats by adopting advanced security tools like Cloudflare WAF and investing in continuous monitoring and threat intelligence. Additionally, this evaluation emphasises the importance of educating end-users and IoT device manufacturers about the risks and best practices for ensuring secure IoT deployments (Shin and Seto, 2020).

Conclusion

In conclusion, the rapid expansion of the Internet of Things (IoT) devices has brought about new challenges in terms of cybersecurity, with Denial of Service (DoS) attacks being a significant concern. This research aimed to assess the effectiveness of DoS attack tools and defence mechanisms on IoT devices.

The DoS attack simulation using the nping tool revealed the vulnerability of IoT devices to such attacks. The experiment successfully overwhelmed the target IoT edge device, causing resource exhaustion and service disruptions. The analysis of the attack patterns and impact on the IoT device highlighted the need for robust security measures to safeguard these devices from potential threats.

In response to this vulnerability, Cloudflare Web Application Firewall (WAF) was implemented as a proactive defence mechanism. Cloudflare WAF demonstrated its efficiency in the real-time detection and mitigation of DoS attacks. Cloudflare WAF effectively protected the IoT Edge Device from the simulated DoS attack by dynamically blocking excessive requests from potentially malicious sources.

Overall, this research provided valuable insights into the significance of securing IoT devices against DoS attacks. By adopting advanced security solutions like Cloudflare WAF, organisations can ensure their IoT devices' integrity, availability, and resilience. The findings of this experiment contribute to a better understanding of IoT device security and offer practical recommendations to enhance protection against evolving cyber threats. With the continuous evolution of technology, strengthening IoT device security remains a critical priority to foster a safer and more connected future.

References

- Sisinni, E., Saifullah, A., Han, S., Jennehag, U. and Gidlund, M. (2018). Industrial Internet of Things: Challenges, Opportunities, and Directions. *IEEE Transactions on Industrial Informatics*, 14(11), pp.4724–4734. doi:<https://doi.org/10.1109/tii.2018.2852491>.
- Chow, R. (2017). The Last Mile for IoT Privacy. *IEEE Security & Privacy*, 15(6), pp.73–76. doi:<https://doi.org/10.1109/msp.2017.4251118>.
- developers.cloudflare.com. (2023). *Cloudflare Web Application Firewall · Cloudflare Web Application Firewall (WAF) docs*. [online] Available at: <https://developers.cloudflare.com/waf/#cloudflare-web-application-firewall> [Accessed 5 Aug. 2023].
- Zhang, H., Cheng, P., Shi, L. and Chen, J. (2016). Optimal DoS Attack Scheduling in Wireless Networked Control System. *IEEE Transactions on Control Systems Technology*, 24(3), pp.843–852. doi:<https://doi.org/10.1109/tcst.2015.2462741>.
- Liang, L., Zheng, K., Sheng, Q. and Huang, X. (2016). *A Denial of Service Attack Method for an IoT System*. [online] IEEE Xplore. doi:<https://doi.org/10.1109/ITME.2016.0087>.

Gordon Fyodor Lyon (2008). *Nmap network scanning: official Nmap project guide to network discovery and security scanning*. Sunnyvale, Ca: Insecure.com, Llc.

Sandhya, S., Purkayastha, S., Joshua, E. and Deep, A. (2017). *Assessment of website security by penetration testing using Wireshark*. [online] IEEE Xplore.

doi:<https://doi.org/10.1109/ICACCS.2017.8014711>.

Roukounaki, A., Efremidis, S., Soldatos, J., Neises, J., Walloschke, T. and Kefalakis, N. (2019). *Scalable and Configurable End-to-End Collection and Analysis of IoT Security Data: Towards End-to-End Security in IoT Systems*. [online] IEEE Xplore.

doi:<https://doi.org/10.1109/GIOTS.2019.8766407>.

Shin, S. and Seto, Y. (2020). *Development of IoT Security Exercise Contents for Cyber Security Exercise System*. [online] IEEE Xplore. doi:<https://doi.org/10.1109/HSI49210.2020.9142678>.

Sinha, S. and G, Kruthi. (2021). *Network layer DoS Attack on IoT System and location identification of the attacker*. [online] IEEE Xplore.

doi:<https://doi.org/10.1109/ICIRCA51532.2021.9545071>.

Huraj, L., Simon, M. and Horák, T. (2018). *IoT Measuring of UDP-Based Distributed Reflective DoS Attack*. [online] IEEE Xplore. doi:<https://doi.org/10.1109/SISY.2018.8524703>.

Iqbal, W., Abbas, H., Daneshmand, M., Rauf, B. and Abbas, Y. (2020). An In-Depth Analysis of IoT Security Requirements, Challenges and their Countermeasures via Software Defined Security. *IEEE Internet of Things Journal*, 7(10), pp.1–1.

doi:<https://doi.org/10.1109/jiot.2020.2997651>.

Kumar, J. and Paidi Raja Ramesh (2018). Low Cost Energy Efficient Smart Security System with Information Stamping for IoT Networks. doi:<https://doi.org/10.1109/iot-siu.2018.8519875>.

Zuo, X., Pang, X., Zhang, P., Zhang, J., Dong, T. and Zhang, P. (2020). A Security-aware Software-defined IoT Network Architecture.

doi:<https://doi.org/10.1109/comcomap51192.2020.9398887>.