DLINE JOURNALS

Journal of Information Security Research

Print ISSN: 0976-4143
Online ISSN: 0976-4151

JISR 2024; 15 (1)
https://doi.org/10.6025/jisr/2024/15/1/23-29

An Efficient Security Framework for Cloud Computing

Farhan Nisar[1] Samad Baseer[2] Arshad khan[3]
[1,3]Department of Computer Science and Information Technology
Qurtaba University

[2]Department of Engineering & Technology
University of Engineering & Technology, Peshawar
Pakistan

{farhansnisar@yahoo.com}
{Drsamadbaseer@uetpeshawar.edu.pk}
{Arshidkhan1991@gmail.com}

ABSTRACT

Many organisations have been established due to the rapid development of cloud in business environments. Today, our scenario related to cloud attacks on computer networks has increased because of security vernal ability and breaches in establishments. Many attack spenetrate our edge network device; some of the most prone attacks are ICMP attacks, CDP attacks and port security attacks, leading to a denial of service. In this paper, we analyze different mechanisms to provide network security by using different policies and rules on edge network devices to protect the network devices. We can be tested in Lab in Lab by using the GNS3 simulator. We are implementing these mechanisms to protect internal and external networks from attacks like ICMP, CDP, and Port Security.

Received: 27 August 2023
Revised: 20 November 2023
Accepted: 30 November 2023

Keywords: Attacks, Security, Network, DoS, ICMP, CDP, Port Security

1. Introduction

With the rapid increase in the use of networks for storing and sharing data, security attacks on computer networks have also increased [1] at an alarming rate. Even inside attacks have increased in the past few years. In an annual survey on cyber security, not only large organizations but also small organization businesses have been targeted by 63%. [2][3]. DOS Attack is an attack where the attacker shows him an authorized user and wants to access the service. The DOS attack may be attempted on a single machine but may be carried out by different computer attacks and Distributed Denial of service attacks. CDP attacks will control the network device, and local events can be impacted and lead to network instability, resulting in a loss of connection and data. Security will be solved by encryption and decryption of data and policies that enforce the data. Resources will be allocated to memory and the secure algorithm for security [4].

Finally, they can find data mining techniques for security, but they cannot be solved. In clouds many types of attacks can happen on cloud data centres, like random, strong and weak attacks. (i.e. criminal or terrorism). The cloud service is on web pages, and most data is on it, and hackers can target Amazon and Microsoft. It also explains the security and cybercrimes. If exceeded, the data store limit will cause such types of attacks. Cloud applications are concerned with data, and data must be reliable, and most threads are based on network layer distributed attacks. Denial of service attacks are related to network flooding of packets and hardware failure in the clouds.

2. Types of Different Attacks

There are many types of DOS attacks. Some major attacks can be classified as follows:

• ***Distributed Attacks:*** *They can be attempted by online applications like trades, banking, and e-commerce. A specific host can target a particular application or be a small or large network with many hosts.*

• ***Insider Attacks:*** *A trusted person inside the organization does the attacks. These types of attacks are difficult to detect because the attacker knows the policies and rules of the network organisation, and the attacker can misuse information.*

• ***Active Attacks:*** *These can be initiated from a single PC and compromise many PCs around the globe connected to the internet with a low level of Security.*

• ***Close-in-Attacks:*** *Attackers analyzed traffic using Homeport to initiate the attack and tried to exploit them by sending emails and obtaining confidential information about the account, etc.*

• ***DOS Attacks:*** *DoS attack from a single source and compromised source with spoofed IP. Those attacks are huge in volume and paralyzed the network. The attacker tries to find out the vulnerability of the network and target to some specific service and consist of many hosts of small/extensive networks.*

3. Types of Dos Attacks

The first attack was attempted on 2 November 1988[6]. This attack was self-propagating and stopped 15% of the system of the network, which was infected. There are several attacks of DoS, the popular as follows:

- *Port Security Attacks*
- *ICMP Attacks*
- *CDP Attacks*
- *DHCP Attacks*

• ***Port Security Attacks:*** *A Port security attack is one of the most important attacks. Confidential information will be lost and damaged when any intruder inside an organization has easy access to the server.[5] If the port is shut down, it will not be implemented easily. It can simulate in Gns3 how to prevent port security attacks. We can see in this diagram that two users are connected to the network, and the remaining ports are empty. Then, a port security attack should be implemented.*

• ***ICMP Attacks:*** *Ping causes the remote system to hang, reboot or crash. The attacker will exploit the internet control message protocol, which enables the user to send an echo message to check whether it is alive. During a Dos attack, many ICMP_ECHO_Reply packets use ping messages [6]. These packets request and reply from unauthorized users and are the result of the bandwidth of the victim network connection. The attacker mostly sends ping commands to the router and checks whether the router gives any response or not.*

• ***CDP Attacks:*** *Before launching the Cisco Discovery Protocol flooding attack, it shows how it*

affects our topology. The CPU utilization of the switch before the attack is 5%. The steps in OS that should be performed during the Cisco Discovery Packet attack are the following:

Go to Launch attack → Cisco Discovery Packet → Flooding CDP Table → OK.

After launching the attack and running for a few minutes, the CPU utilization of the switch is increased to 59%. If the attack runs a bit longer, the switch will drop packets because it will become too busy.

• ***DHCP Attacks:*** *Before launching an attack, the following steps allow the practical execution of a DHCP attack using GNS3.*

Create a network sub-interface on the machine as the default gateway to route our rogue DHCP client. Set an IP on the new Ethernet 0/1 interface to another unused IP address. Allow IP forwarding on your machine. Set the default gateway and default route on the Ethernet interface 0/1 sub-interface. Show the route table. Launch the DHCP module and show the optional and required options that have to be set to run a rogue DHCP server. In another terminal window, launch the DHCP attack. Start the Rogue DHCP server from the console. When a new user connects to the network and IP address, he gets assigned from the DHCP server; now, the default gateway is actually the IP address of the running machine. The attacker is now in the middle of the communication between the DHCP server and the User.

4. Control Mechanism

Many mechanisms are available for network security, and a few will be discussed briefly.

• ***Firewall:*** *The firewall is a type of security that will control intrusion and monitor the incoming and outgoing traffic of the network in cloud Computing.*

• ***IDS System:*** *IDS stand for intrusion detection system, and it will protect the network from application-level attacks. It will identify the attempts, alert the system to maintain each user's log, and block and stop it.*

• ***ISP edge Router:*** *The edge device will accept traffic only from the source and monitor traffic between the sender and receiver on both sides.*

• ***Reactive Mechanism:*** *The mechanism will reduce attack and is also called an early working system, which responds to an attack immediately.*

In this paper, we apply some mechanisms on edge networks and test these policies by simulating them in a GNS3 network simulator.

5. Main Contribution of Our Work

Analyze the different types of security as

• *Studying different types of DoS attacks.*

• *Enhance different types of security mechanisms on edge network router*

• *GNS3 network to protect our network, like*

• *CDP, DHCP, ICMP and Port Security Attacks*

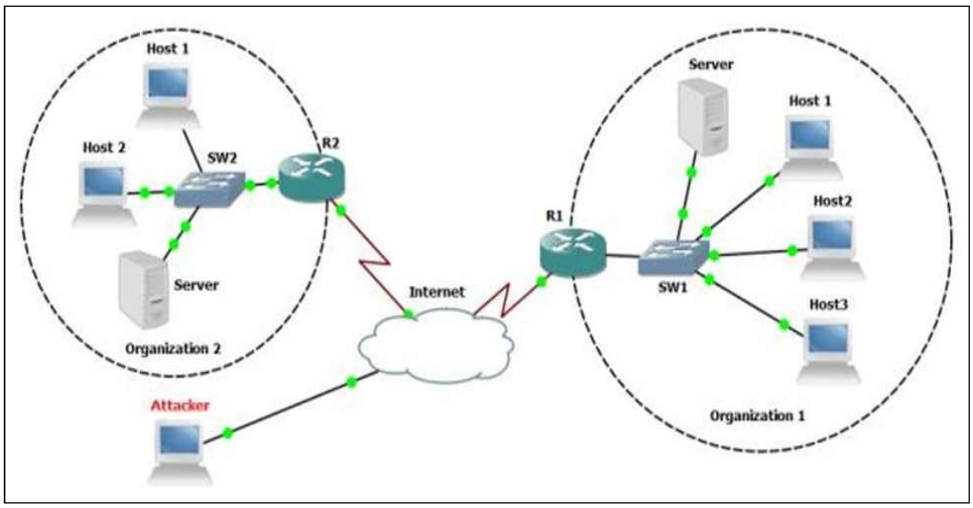
6. Simulation and Experimentation

1. *For the Port, from the network, Port security is used for inside organization security because the attack ratio will be random and communication from source to destination will be random. When any attacker or intruder connects the port, it is necessary to disconnect the interface automatically*

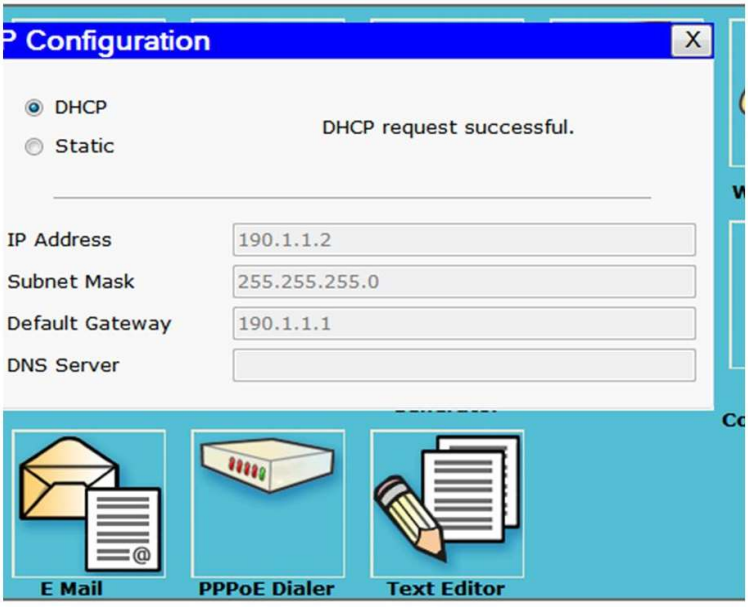
by using this command.

The above result shows the result more clearly about the status of the packets dropped. When the packet increases, drops of packets will increase, and the attack must decrease at an optimal level.[7]

We apply policies on all router edges, switch off all interfaces when unused, and disable the ping command.



2. *There are several ways of preventing a DHCP attack with a rogue server for the DHCP attack. DHCP snooping is also used for these attacks. It provides network security by filtering un-trusted DHCP messages and maintains DHCP snooping in the table. Ports must be trusted and un-trusted. Un-trusted ports can be source requests only, and trusted ports contain all DHCP messages. After enabling DHCP spoofing using the command IP DHCP snooping, IP DHCP snooping vlan1 Attacker cannot be performed successfully. The command can be implemented in routers.*



3. *For the CDP Attack, the only easy step to prevent a CDP flooding attack in GNS3 is to command disable CDP features on all the ports, and it will never share neighbour information and the attack*

of DOS is prevented.

Before disabling the CDP, it will show the neighbour information, as shown in the figure.

```
Office-R1#
Office-R1#
Office-R1#sh cdp nei
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone
Device ID       Local Intrfce Holdtme Capability Platform Port ID
```

The figure shows that the router and switch are connected to the internet with an interface connected to the network.
The command is run in the GNS3 simulator, as shown. When simulating in Gns3, it will never share information with any other router, and many organizations have disabled CDP.

4. *We apply policies called ICMP protocol, which will work in parameters like access group, bandwidth burst size, etc.*

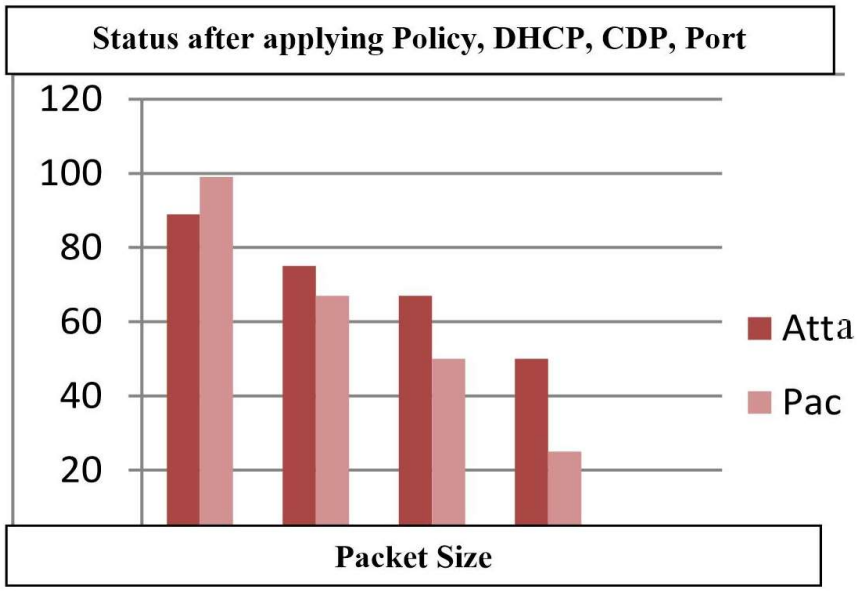
Before we apply the policy, the success rate is high, and in time intervals, the attack is generated successfully up to 100%. We also sent different sizes of packets sent and reached up to the host network. It indicates a successful percentage of up to 99%.

Before we apply any policy in the GNS3 lab, we must check the success rate of attacks of different sizes of packets with different time intervals. The attack is generated and successful up to 100%. The outside attacker should ping the server user within the organization, and there is another problem inside the organization. If an authorized person becomes unfaithful, then he tries to destroy the network or give confidential information to another one, then it will be very unfaithful. So, we implement security for this type of attack. The diagram shows that the server will respond to the attack and then implement such a security mechanism for the attackers.

The table shows the result obtained after applying policies on edge and considering different parameters like packet size and repetition, and different values will be obtained. We see a gradual decrease in packets from 99% to 89% and reaching 0% status. The mechanism must be implemented in the organization, and the third party will also trust that your security will be secure and the success rate of attack is dropped concerning more packet size and taking readings at different time intervals.[8] If we apply the proper countermeasures mechanism, large and small organizations can be protected by applying policies like routers, web servers, firewalls, etc., and protect them to the maximum level. We implement such types of attacks with higher success rates and efficiency.

ICMP, DHCP, Port Security Attack with Policy Mechanism			
ICMP echo	**Packet Size**	**Attack success**	**Packet drops**
100	250	98%	2
100	500	91%	9
100	750	70%	30
100	1000	67%	33
100	1500	0%	100

The graph will show the existing work with the new work after applying such types of security for it. They will show the new techniques are reliable for cloud users.



The Graph shows the above result more clearly and checks the packet's status dropped. The size of the packet increases, then more impact on attack success, and the drop rate of the packet increases. The attack must be decreased optimally by applying such a policy for internal and external edges on the network. It is more successful as packet size increases and packet dropped rate increases, and even reaches the maximum level.

7. Reltad Work

Many researchers have done lots of work on security and establishing the network; a few papers related to our work are:

In 2012 [4], Bellovin implemented a mechanism on the routers and provided a pushback mechanism for the flooding attacks, but he discussed only countermeasures.

Rao Kompella, in 2007 [5], proposed a novel data structure called a partial completion filter that can detect claim and hold attacks in the network. Still, he demonstrated the low false positive and false negative probability of the network.

Katerina and David in 2009 [6] presented Active Internet Traffic filtering based on internet Bandwidth flooding Attacks but provided scalable deployment solutions for the bandwidth flooding attack.

Xin Liu in 2010 [7] presents a novel mechanism to enable robust congestion policing feedback inside the network. It can used to unsecure traffic. They are using ns2 simulation and theoretical analysis for the DoS solution. Mitko and Risteski, in 2011 [8],sent bogus packets to the router and disrupted and intercepted communication from the wireless access point. They approach the ICMP Ping flood attack and provide different types of countermeasures. Simulation results affect the link failure recovery mechanism against this type of attack.[10]

8. Comparative Analysis

In Katrina's 2009 paper, they present Active internet Traffic filtering for flooding attacks. They have shown that:

***1.** It allows the receiver to preserve, on average, 80%, and its tail circuit of Syn-flooding attack has ten times the rate of its capacity.*

2. *Each participating ISP need thousands of filters and a few megabytes of Dynamic RAM per client; the per-client cost is not expected to increase unless bot net size outpaces Moore's law.*

These two active internet traffic filters enable networks to maintain their communication during the flooding attack, and the path between them cannot be compromised.

Mitko and Risteski 2011 discussed the behaviour of wireless networks under different numbers of attackers and ping packet sizes; they found QoS parameters can be reduced under these types of flooding attacks. During their work, they simulated the same scenarios when a firewall and fast recovery of filtering of ICMP ECHO massage is used. In all these situation results, they intend to continue exploring the possibility of setting an optimal threshold for successor and recovery mechanism if an active large number of packets or greater size ICMP packet was received.

Our approach in this paper has the following aspects.

1) *Our approach is straightforward to implement.*

2) *The result clearly shows the packet size increased and decreased, reaching up to 99%.*

3) *There is no effect related to time. These policy, CDP, and DHCP mechanisms will be successful for the Local area networks. Still, there are many areas of effective inputs that could be referred from the work by earlier research.*

9. Conclusion and Future Work

This research identifies the attack attempts and shows that security testing can be challenged and met. They show several security issues and how specific processes can solve them. Security is related to protecting our information, and we must have issues of availability and how to prevent DoS attacks in cloud computing. It is vital to protect our office network from newly evolved attacks. Recently, a survey has revealed that attacks on smaller organizations are to a great extent. Our simulation results show that policy, DHCP, CDP and Port Security mechanism success rate becomes high and packet drops rate and reach to maximum level. Furthermore, investigating a high level of monitoring is necessary to know attacks and their signature, which an edge router can implement to counter the maximum types of attacks with a higher success rate and efficiency.

References

[1] Harshita. (2013). A survey of different types of security threats and its countermeasures.

[2] Computerweekly.com.

[3] Ponemon Institute/Symantic.com.

[4] Ionanidis, J., Bellovin, S. (2012). Implementing PushBack: Router-based Defense Against DDoS Attacks.

[5] Rao, R. (2007). On Scalable Attack Detection in the Network.

[6] Karerna., David. (2009). Scalable Network-Layer Defense Mechanism against Internet Bandwidth Flooding Attack.

[7] Lui, X. (2010). Preventing Internet Denial of Service from Inside Out.

[8] Bogdanoshi, M. (2011). Wireless Network Behavior under ICMP Flood DoS Attack and Mitigation Techniques.

[9] TELELINK. (2013). Corporate WAN Threats, IT Threats – Control Plane Attack.

[10] CSA, Security Guidance. (2014). Construction of digital campus security based cloud computing.