iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 11 **Issue:** V **Month of publication:** May 2023

DOI: https://doi.org/10.22214/ijraset.2023.52592

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 11 Issue V May 2023- Available at www.ijraset.com

Proxified IP Detection in Networks for Security Enhancement

Tathagat Gaikwad[1], Gaurav Patil[2], Manoj Padvi[3], Dr. M. T. Jagtap[4]
[1, 2, 3, 4]*Computer Engineering, PVGCOE & SSDIOM, Nashik*

Abstract: ***The number of cyberattacks worldwide since the Covid-19 epidemic has reached an all-time high as they continue to rise day by day. This assault is typically carried out by criminals who want to steal personal data or commit financial fraud. As can be seen, data is the new kind of currency. Therefore, maintaining privacy is crucial. Since the attackers utilise techniques for concealment, such as anonymizing proxies or Virtual Private Networks (VPN), spotting unauthorised users might be challenging. There is a model to identify how network consumption can be categorised, detected, and tracked using that manner. Using these services to conceal their identity, the attacker launches attacks using SSH and HTTP. Other applications with the same criteria can use this strategy. The most frequent data breaches result in too much loss for businesses. Any person who hits a website's server is considered an attacker. typically to collect user data, shut down the website, or make inappropriate runtime changes to the website. Cyberpunks or crackers will employ a honeypot to find this and will be able to obtain their IP address. Once it has the IP address, it can follow the attacker's geolocation and determine their latitude and longitude. Even though they are utilising a proxy or VPN. This strategy will aid in locating the attacker, allowing access to their system logs and other pertinent information. As a result, it may monitor IP hidden behind VPN or a proxy and learn more about the attacker.***
Keywords: Data breach, IP address, VPN/proxy, honeypot, SSH, and HTTP.

I. INTRODUCTION

Compared to earlier times, we now confront greater online hazards. So, in order to solve this kind of issue, we put into practice a method for determining an attacker's actual IP address. Since the Covid-19 pandemic, the world has seen the most cyberattacks ever, and they are growing daily. Attackers typically carry out this attack in order to steal personal data or commit financial fraud. Therefore, we will use a honeypot as our main weapon to entice the attacker or hacker into giving up his true IP. since each transaction is documented and openly checked. The transaction is recorded and publicly verified.

II. LITERATURE SURVEY

Many techniques have been used to find an attacker's actual IP address. For the same, a variety of hardware tools and algorithms were employed. Information regarding such findings is provided in this part through comparison. This module addresses the problem of spotting intruders who hide behind covert networks. Tor and SOCKS are two widely used applications that offer network users circuit-based anonymous connections as examples of publicly available proxy services. But as previous security lapses have shown, malevolent users have utilised HTTPS and other services to launch attacks while hiding their identities.[2] Users of the internet are at an unprecedentedly high danger of being followed and watched. However, using an anonymity network to safeguard a user's privacy has a price. Since the global Covid-19 pandemic, there have been allegations of economic espionage against numerous hospitals, colleges, and pharmaceutical firms. Additionally, in several instances, hackers have concealed their identities by using anonymity tools. Applications of all kinds are spreading more widely. With the use of already-built network agents, NAT, IP tunnelling technologies, and swiftly emerging anonymous communication systems, attackers can mask genuine IP in edge computing. Additionally, the hacker breaks into numerous intermediate edges computing network services to build a "stepping" chain. The term "network flow" describes a series of unidirectional data packets or frames sent over a period of time between any two network nodes. Additional names for it include communication data flow and packet flow. The primary components of the network flow watermarking model are the original network flow, the watermark, the carrier for the watermark, the embedded function, the extracting function, and the comparison function.[3] A new strategy for efficiently using resources in a cloud computing environment is virtualization. The intellectual abstraction layer of virtualization conceals the complexity of necessary hardware or software. Virtualization technology is not a new invention, but it does have security flaws that can transfer to cloud environments.

The virtualization technique plays a crucial part in a cloud environment by offering a variety of services for numerous customers using various VMs. The machine is a single OS image with tightly connected Hardware and Software prior to virtualization. Following this, OS runs several apps simultaneously on a single computer while utilising all available hardware, including the CPU, memory, NIC, and disc. [4] The research into a proxy identification approach and endeavours to incorporate such technology into a commercial solution with the express objective of obviating most fraudulent transaction attempts. The method outlined provides a multi-tiered detection mechanism and recognises various proxy connectivity options. When we use any Internet-related application or service, we put ourselves at risk of being targeted by cybercriminals who use scamming, phishing, and social engineering to take advantage of system flaws and make money. They might act on our behalf to grab our priceless belongings or covertly use our privileges or rights.

III. METHODOLOGIES

1) USER LOGIN
2) ATTACKER SIDE
3) HONEYPOT SERVER
4) LOGIN ALERT
5) GEO LOCATION

A. Technologies

Virtualization: To understand virtualization, picture five physical computers, each of which is running a separate operating system and set of software services. Through virtualization, you may detach each operating system (OS) and its associated software from each terminal and combine them into a single entity, or "host computer," allowing each device to perform independently on distinct tasks. If necessary, this can manage several software packages and manage various devices.

Network-attached machine known as a "honeypot" that is used as a ruse to entice online attackers to detect, block, and research efforts to hack into information systems without authorization. A honeypot's function is to impersonate a potential target for attackers online, usually a server or other high-value asset, gather data, and notify defenders when an unauthorised user attempts to access the honeypot.

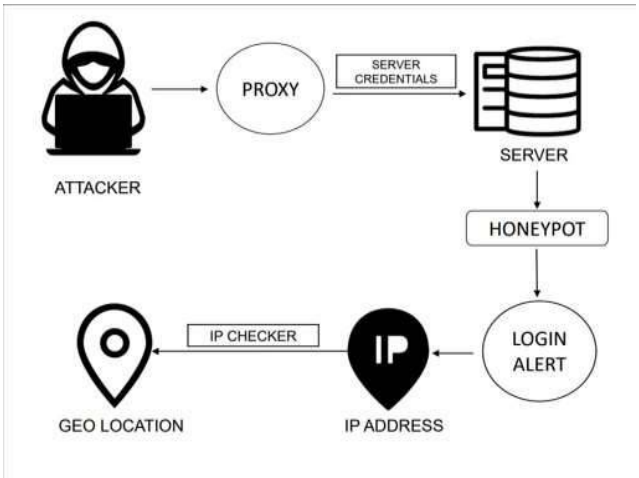


Fig. 1 Block Diagram of IP Detection using different Methodologies behind VPN/Proxy.

B. Ngrok

Ngrok is a well-liked programme that enables programmers to safely reveal a local web server to the public internet. Without deploying them to a public server, developers can use ngrok to test their web applications or APIs in actual use cases.

In order for Ngrok to function, a secure tunnel must be built between a developer's local computer and the internet. It gives the local web server a public URL so that it can be accessible from anywhere in the world. Ngrok offers a variety of capabilities to developers, such as configurable subdomains, password security, and HTTPS support.

C. Working of Proposed System

The system we are attempting to develop is a method for coping with the real world. A system is constructed to function in a certain context. And when we attempt to execute the same and the actual event, this will change. Our strategy consists of a number of instruments and instructions that must be followed in order to accomplish the final objective. We're installing a honeypot on the server for this reason. A website with featured login authentication and the similar scenario-based chores will be part of this service. like an online store, for example. We may use this website to make our honeypot appear to be a server. We will set up our Canary Tokens API, which will assist with distributing the payload certainty data, on the same server. The attacker will access the server and download the file to his computer. When the file is opened, the attacker's original IP address will be displayed, so we must check this address on a website for DNS leaks to determine the attacker's precise geolocation, which includes latitude and longitude of the attacker's IP address. In addition, it will provide us with the ISP details, which we can utilise to identify the real user and present that information to the appropriate government. This will enable us to track down the attacker's real IP address

IV. CONCLUSIONS

Due to the range of proxy connection types and protocols, as well as the numerous software and technique installations, it might be difficult to recognize a proxy connection. Even while there are currently several techniques to find a proxy connection, each one has drawbacks of its own. Our goal is to create a tool that can find the actual IP address of the attacker.

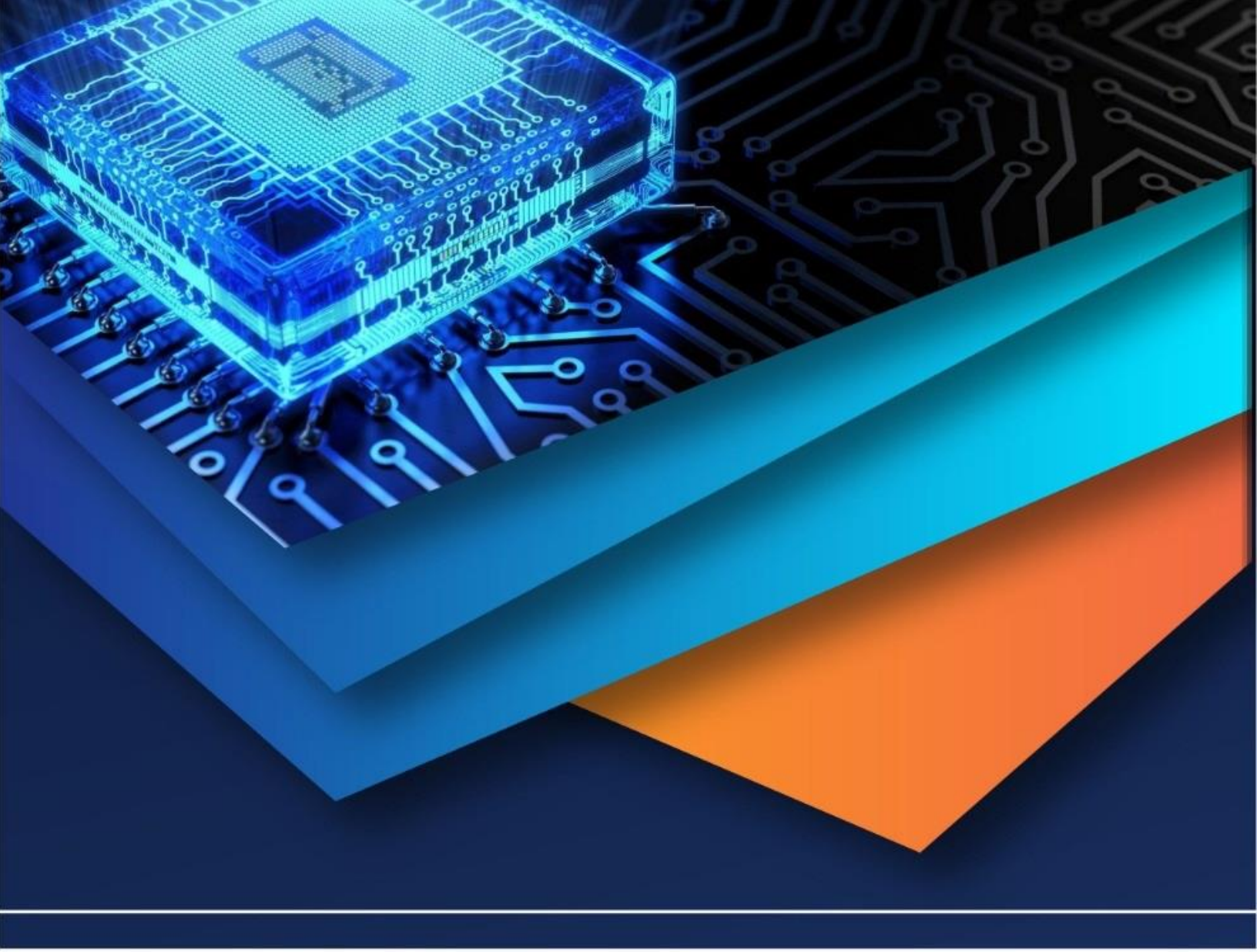
In the expanding number of cyberattacks, attackers commonly use anonymizing proxies or VPNs to mask their identities and locations. This makes it difficult to find and identify them. With the aid of honeypots and other monitoring tools, it is still possible to find and follow an attacker's IP address even if they are using a VPN or proxy. The attacker's identity and their system logs can be discovered by following their IP address. The attack can be investigated, future assaults can be stopped, and the attacker can be prosecuted using this knowledge. In order to increase internet security and defend against cyberattacks, this project is a crucial first step. We can all benefit from a safer internet by creating tools and techniques to locate and identify attackers. It is crucial to keep investigating and developing these strategies since attackers will keep developing their tactics and strategies to avoid discovery. This initiative has the potential to greatly enhance internet safety and defend against online dangers.

V. ACKNOWLEDGMENT

One benefit of doing this project report is that it enables you to collaborate and test ideas with teachers and fellow students. We owe a debt of thanks to each person on this team who helped make this project successful. We are appreciative of the chance to convey our sincere gratitude. We appreciate the project guide for this department's inspiration and priceless advice. Appreciate the project guide's insightful recommendations. Last but not least, we want to thank everyone who helped the project succeed, whether they were directly involved or not. Each project is the outcome of careful planning, ongoing work, and well-coordinated efforts. The culmination of all of them is this piece.

REFERENCES

[1] K. M. Babu and P. S. Kiran, "A secure virtualized cloud environment with pseudo- hypervisor IP based technology," 2016 2nd International Conference on Next Generation Computing Technologies (NGCT), 2016, pp. 626-630, DOI: 10.1109/NGCT.2016.7877488.
[2] M. Pannu, B. Gill, R. Bird, K. Yang, and B. Farrel, "Exploring proxy detection methodology," 2016 IEEE International Conference on Cybercrime and Computer Forensic (ICCCF), 2016, pp. 1-6, DOI: 10.1109/ICCCF.2016.7740438.
[3] J. Hou, Q. Li, R. Tan, S. Meng, H. Zhang, and S. Zhang, "An Intrusion Tracking Watermarking Scheme," in IEEE Access, vol. 7, pp. 141438- 141455, 2019, DOI: 10.1109/ACCESS.2019.2943493.
[4] O. Fediushyn, V. Ruzhentsev, I. Fedorov and K. Moskvin, "Honeypot Data Storage and Analysis Software to Prevent Intrusions," 2021 IEEE 8th International Conference on Problems of Infocommunications, Science and Technology (PIC S&T), 2021, pp. 169-173, DOI: 10.1109/PICST54195.2021.9772139.
[5] Ruei-Min Lin, Yi-Chun Chou, and Kuan- Ta Chen, "Stepping stone detection at the server side," 2011 IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS), 2011, pp. 964- 969, DOI: 10.1109/INFCOMW.2011.5928952.
[6] M. Ligh, S. Adair, B. Hartstein, and M. Richard, "Malware Analyst's Cookbook and DVD: Tools and Techniques for Fighting Malicious Code," John Wiley & Sons, 2010, pp. 11-15.
[7] TorGuard.net, "Anonymous VPN, Proxy & Anonymous Proxy Services," 2016. [Online]. Available: https://torguard.net.
[8] BBC News. Coronavirus: Cyber-Attacks Hit Hospital Construction Companies. Accessed: May 13, 2020. [Online].
[9] https://timesofindia.indiatimes.com/gadgets-news/aiims-server-down-hackers-demand-rs-200-croreincryptocurrency/articleshow/95834036.c ms
[10] https://timesofindia.indiatimes.com/india/why-we-need-to-worry-about-the-aiims-cyber-attack/articleshow/95976398.cms
[11] O. Fediushyn; Victor Ruzhentsev; Illia Fedorov; Kostiantyn Moskvi, "Honeypot Data Storage and Analysis Software to Prevent Intrusions"



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY