International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 07 Issue: 05 | May - 2023 SJIF 2023: 8.176 ISSN: 2582-3930

Tracing IP Address Behind VPN/Proxy Servers

Meghashyam Y[1], Pappu Saicharan[2] , P Rajeshwari[3] , R Dhanush[4] Students,Dayananda Sagar Academy of Technology & Management, Bengaluru, India
D.r Rahmi Amardeep[5], Assistant Professor , Dayananda Sagar Academy of Tech & MGMT, Bengaluru, India
shyamsj001@gmail.com[1] , saicharanpappu208@gmail.com[2] , podamalarajeswari07@gmail.com [3] ,dhanushramesh6@gmail.com[4] , dr.rashmi-is@dsatm.edu.in[5]

ABSTRACT

To strengthen their anonymity, cybercriminals frequently utilize pseudonymous IP addresses to conceal genuine IP addresses. To address this, we intend to develop a tool that can determine if an IP address is genuine or a proxy or VPN IP. The solution should also be able to track the VPN user's actual IP address and offer location data. It is more difficult for authorities to identify and bring to justice offenders when hackers utilize a range of tools and tactics to conceal their digital tracks. One of the better ways is through a "proxy" or VPN server, which effectively serves as a layer between the target computer and the target computer and allows access to the target computer without going directly through it.

One of the better methods is to connect to the target's computer via a "proxy" or VPN server rather than directly, which effectively creates a layer between the target computer and the target computer. It only observes requests coming from the target computer's name server or VPN server. This solution's primary goal is to discover the genuine IP address of cybercriminals who are hiding it behind the IP address of a server or VPN (if utilized). a system that can use an IP address as a login and distinguish between a VPN service provider and a "proxy". This information must be given if a "proxy" or VPN service provider is being utilized. The remedy can also identify the actual IP address that is. Additionally, it makes use of (optional) sophisticated heuristic methods that can aid in the discovery of new risks (like malware).

Keywords

VPN, Honey Pots, Canary Tokens.

1. INTRODUCTION

False IP addresses are regularly used by cybercriminals to hide their real IP addresses and maintain their anonymity. The major goal of our work is to identify the cybercriminals operating behind a name by tracking their real IP address or, if they are using a VPN, their VPN IP address. Hackers use a variety of techniques to conceal their online actions, making it difficult for law authorities to capture and indict them. Typically, they utilize a proxy server or VPN server, which serves as an intermediate layer between their device and the desired target computer, rather than directly contacting it. Entering an IP address to check whether it belongs to a proxy or a VPN service might be one way to solve this problem. This project's goal is to safeguard. This project aims to defend against hackers by tracking and ultimately apprehending harmful individuals who attempt to compromise our system or access hostile websites. The location of the malicious user who was using a VPN will be made known together with the person's genuine IP address. Verify the actual IP address of unauthorised users. via way of the VPN server. The concept behind this is that by developing a honeypot security system, we may draw in unauthorised users. By doing this, we may persuade the attacker that we would deliver a Trojan with the honey information we want him to take. When our Trojan successfully infiltrates the attacker's system, it will transmit the attacker's system's true IP Address, data, logs, and files. With the use of this information, we can determine the attacker's location. Using canary tokens is an easy approach to tripwire events. They are an outdated idea that, although they are simple to use and extremely helpful, they need some supporting infrastructure to function. We give you access to this infrastructure, allowing you to quickly deploy tokens and reap their benefits . You may be acquainted with tracking pixels, which are translucent 1x1 pictures included in emails and which monitor a person after they are opened. These operate by watching incoming GET requests and inserting a certain URL in the image tag of a page . Imagine implementing something similar for database searches, process executions, log file patterns, or file reads. All of this and more is possible using Canary tokens, which let you to insert traps into your production systems rather than erecting separate honeypots.

2. LITERETURE SURVEY

Si.No	Literature	Author	Year of publication	Description
1.	Tracking and Tracing proxy enabled system	Vipasha Chaudhary, Dr. Purushottam Sharma, Dr Vinod Kr Shukla, Vikasdeep Vipasha Chaudhary, Dr. Purus	2021	They have developed a system that determines whether a given IP address is a proxy or not and takes into account the country and region as well as IPv4 and IPv6. The proxy's region, not the host's actual IP address, was detected
2.	Voyager: Trackingwith a Click	Samuel Decanioa, Michael Soltysa, Kimo Hildreth. KES International	2020	In order to lure the hacker into clicking on an image or thumbnail that would reveal the hacker's IP address, a clickbait system was developed. VPN and proxy use are not detected by this system.
3.	Honeypots: Approach and Implementation	Kumar Shridhar, Mayank Jain	2018	Honeypots can be connected to the production network to check the network vulnerabilities. If the attack is on the honeypot in the production network.
4.	The Vital Role of Virtual Private Network (VPN) in Making Secure Connection Over Internet World	Yogesh Kumar Sharma, Chamandeep Kaur	2020	VPNs enable users and companies to communicate over the public internet to remote servers, branches or the business while retaining secure communication.
5.	Research on Network Security of VPN technology	JIE NI.	2021	VPNs enable users and companies to communicate over the public internet to remote servers, branches or the business while retaining secure communication
6.	RADITIONAL TECHNOLOGIES IN WEB DEVELOPMENT	Pratiksha D Dutonde, Shivani S Mamidwar	2017	The goal is to development a technique that may add structure to a extremely unstructured drawback to help within the development and success of net services

3. PROPOSED FRAMEWORK

We need to determine the unauthorized user's precise IP address who accesses the VPN server. For that, IDEA: We can include unauthorized users by developing a honeypot security technique. By doing so, we are able to attract the attacker, and when he attempts to take our bogus data, we are able to transmit our Trojan with it. Our Trojan will provide the attacker's system's true IP address, data, logs, and files after it has successfully entered the attacker's system.We may use this information to determine the attacker's location.

Techniques used in the proposed system are:

Honeypot: A honeypot is a computer system that's created to seem exactly like a real computer system, replete with real-looking data and apps, to trick hackers into believing it's a legitimate target. It's not a problem-specific solution like an antivirus programme or a firewall. Instead it acts as a tool for information that may help you identify present hazardsto your company and spot emerging ones.

Choose a suitable e-commerce platform: Choose an appropriate e-commerce platform among the numerous options available, including WooCommerce, Shopify, Magento, and many more. Pick a platform that works for your needs and skill set.

Set up the honeypot website: After deciding on an e-commerce platform, you must create a honeypot website that looks exactly like a real e-commerce site. You can use fictitious goods, pictures, and descriptions as long as they appearauthentic and well-done.

Implement security measures: Since the honeypot website is intended to draw attackers, you must put security measures in place to prevent actual consumers from unintentionally visiting the honeypot.

Monitor the honeypot: You must keep a tight eye on the honeypot after it is set up for any indications of an attack. Several tools, including web application firewalls, intrusion detection systems, and log analysis tools, can be used for this.

Analyze the data: The data gathered from the honeypot must be analyzed in order to learn more about the strategies and methods employed by attackers. This might aid in creating stronger security protocols and enhancing the general safety of e-commerce websites.

Action and response: This stage involves taking appropriate action based on the analysis of the data, such as blocking IP addresses, implementing new security measures, or reporting attacks to law enforcement.

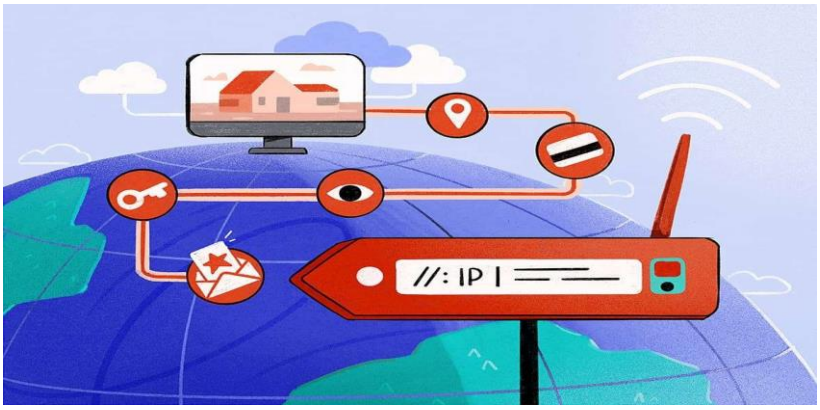


Fig. Proposed system Architecture

The first step in tracking an IP address behind a VPN is to collect as much information about the VPN provider and the individual VPN connection as feasible. This information may include the network architecture of the VPN provider, the VPN protocol being used, the client software used to create the connection, and any records or metadata that are accessible

3.1 Architecture

The architecture of "Tracing IP address behind VPN or proxy networks using honey pots" involves setting up a system of honeypots that are designed to attract and capture malicious traffic. A honeypot is a computer system that is designed to simulate the behavior of a vulnerable or valuable system in order to attract attackers and monitor their activity:
The system consists of several components, including:

Honeypots: The honeypots are set up to simulate vulnerable systems and services that attackers are likely to target. These honeypots are designed to capture the IP addresses of attackers and the methods they use to attempt to compromise the system.

Monitoring system: The monitoring system is responsible for collecting and analyzing the data captured by the honeypots. This system is designed to detect patterns of malicious behavior and to identify the IP addresses of attackers.

VPN or Proxy Detection: The system includes tools and algorithms to detect the use of VPNs or proxies by attackers. These tools can analyze traffic patterns and behavior to determine if an attacker is using a VPN or proxy to hide their true IP address.

Tracing and Tracking: The system is designed to trace and track the IP addresses of attackers, even if they are using VPNs or proxies. This is done by analyzing the traffic and behavior of attackers and using advanced algorithms to tracetheir true IP address.
Canary Tokens: When an attacker or unauthorized user attempts to access the canary token, either intentionally or inadvertently, the token is triggered and sends an alert to the system administrator or security team. The alert can be customized to include information such as the IP address or location of the attempted access, allowing security personnel to quickly investigate and respond to the potential threat.

Overall, the architecture of "Tracing IP address behind VPN or proxy networks using honey pots" is designed to capture and analyze the behavior of attackers, even if they are using VPNs or proxies to hide their true IP addresses. By using a combination of honeypots, monitoring systems, and advanced algorithms, the system can accurately trace and track the IP addresses of attackers, allowing security teams to take action to prevent further attacks.

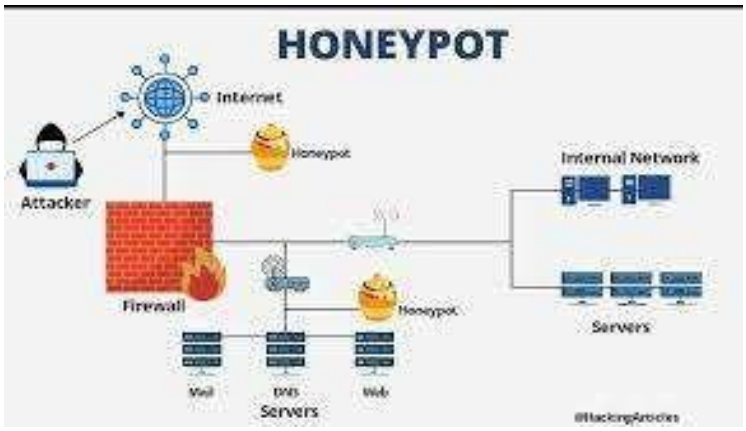
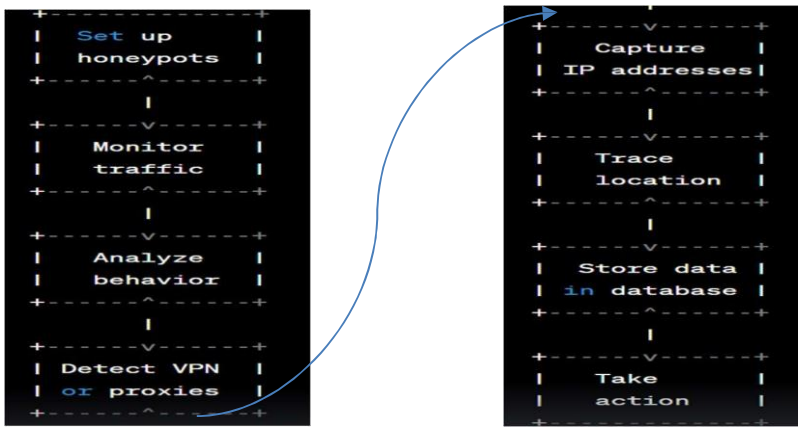


Fig.1 The current system architecture used for Content Based Systems

1.1 Flowchart

Set up honeypots to simulate vulnerable systems and services:

1. Monitor honeypots for incoming traffic and analyze the behavior of attackers.
2. Detect the use of VPNs or proxies by analyzing traffic patterns and behavior.
3. Capture the IP address of attackers and trace their true location using advanced algorithms.
4. Store IP addresses and other relevant data in a database for further analysis.
5. Take appropriate action to prevent further attacks based on the analysis of the data.



Working Flow :

- **USER LOGIN**
  - Create a User Login web page that requires authorized Credential to access the data from theserver

- **ATTACKER SIDE**
  - Attacker should access the server using a VPN to hide his IP address.

- **HONEYPOT SERVER**
  - This service will contain a website having featured login authentication. This website will help us to pretend our honeypot is a server. On the same system, we will set up our Canary Tokens API which isgoing to help in deploying the payload certainty information.
  - When the attacker will access server and having that file downloaded to his system, the file when opened will bring the original IP Address of the attacker so we have to check this address as DNS leak

- **FILE ACCESS ALERT**
  - When the attacker will access server and having that file downloaded to his system, the file whenopened will bring the original IP Address of the attacker so we have to check this address as DNS leak

- **GEO LOCATION**
  - Get the actual geo-location of the attacker which includes the latitude and longitude of the attacker's IP Address. As well as it will bring us the ISP details from that we can identify the actual user and take that information to the respected authority. In this way, we will go to find out the actual IP of the attacker eventhough they are using a VPN /proxy.

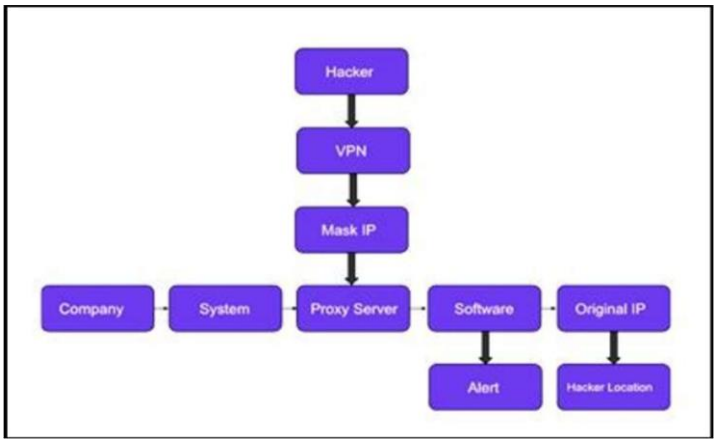


Fig.2 flow chart of working architecture

4. RESULTS

The results of "Tracing IP address behind VPN or proxy networks using honey pots" can vary depending on the specific implementation and the sophistication of the attackers being targeted. However, some potential results of this approach include:

Identification of attackers: By tracing the true location of attackers, security teams can identify individuals or organizations responsible for attacks.

Prevention of further attacks: By taking appropriate action based on the analysis of data, security teams can prevent further attacks from the same source.

Improved threat intelligence: The data collected from honeypots can provide valuable insight into the behavior of attackers, which can be used to improve threat intelligence and develop better defense strategies.

Mitigation of risk: By identifying vulnerabilities in systems and services, security teams can take steps to mitigate the risk of future attacks.

Legal action: In some cases, the identification of attackers can lead to legal action being taken against them, which can serve as a deterrent for future attacks.

5. CONCLUSION AND FUTURE WORK

In conclusion, "Tracing IP address behind VPN or proxy networks using honey pots" is a useful technique for identifying and preventing cyberattacks. By using honeypots to simulate vulnerable systems and services, security teams can monitor incoming traffic and analyze the behavior of attackers. By tracing the true location of attackers, security teams can identify individuals or organizations responsible for attacks, prevent further attacks, improve threat intelligence, mitigaterisk, and even take legal action in some cases.

However, there are limitations to this approach. Sophisticated attackers may be able to evade detection, and tracing IP addresses may not always provide conclusive evidence of the true identity of the attacker. Additionally, there is a risk of false positives, where legitimate users are mistakenly identified as attackers.

Future work in this area could include improving the accuracy and reliability of the techniques used to detect VPNs and proxies, developing more sophisticated algorithms for tracing IP addresses, and integrating the data collected from honeypots with other security tools and techniques to provide a more comprehensive approach to cyber defense

6. REFERENCES

[1] Vipasha Chaudhary, Dr. Purushottam Sharma, Dr Vinod Kr Shukla, Vikasdeep. "Tracking and Tracing proxy enabledsystem" (ICRITO) Amity University, Noida, India. Sep 3-4, 2021

[2] hane Miller, Kevin Curran,Tom Lunney "Detection of Anonymising Proxies Using Machine Learning" S. International Journal of Digital Crime and ForensicsVolume 13 • Issue 6, 2021.

[3] Samuel Decanioa, Michael Soltysa, Kimo Hildreth "Voyager: Tracking with a Click" KES International. 10.1016/j.procs.2020.08.11.

[4] Ankith Rai, Jovita Dsouza, Edison.C.Saldanha. "Secure +, An Intrusion Detection System" International Journal of Innovative Science and Research Technology Volume 4, Issue 5, May– 2019.

[5] hou-Hsuan Stephen Huang, Zechun Cao. "Detecting Malicious Users Behind Circuit-Based Anonymity Networks" S IEEE access Dec 1 2020
[6] Mr. Saurabh Alva, Mr. Rahul Madhyan, Mr. Anoop Madan "Implementation of Honeypot" International Journal of Engineering and Technical Research (IJETR) August 2015.

[7] Zhi Fu, S. Felix Wu, He Huang, Kung Loh, Fengmin Gong, "IPSec/VPN Security Policy Correctness, Conflict Detection, and Resolution" International Workshop on Policies for Distributed Systems and Networks.

[8] Rajashree, S., Soman, K. S., & Shah, P. G. (2018, September). Security with IP address assignment and spoofing for smart IOT devices. In 2018 international conference on advances in computing, communications and informatics (ICACCI) (pp. 1914-1918). IEEE.

[9] Gondaliya, H., Sankaran, G. C., & Sivalingam, K. M. (2020, December). Comparative evaluation of IP address anti- spoofing mechanisms using a P4/NetFPGA-based switch. In Proceedings of the 3rd P4 Workshop in Europe (pp. 1-6).

[10] Ezra, P. J., Misra, S., Agrawal, A., Oluranti, J., Maskeliunas, R., & Damasevicius, R. (2022). Secured communication using virtual private network (VPN). Cyber Security and Digital Forensics, 309-319.

[11] Tambe, A., Aung, Y. L., Sridharan, R., Ochoa, M., Tippenhauer, N. O., Shabtai, A., & Elovici, Y. (2019, March). Detection of threats to IoT devices using scalable VPN-forwarded honeypots. In Proceedings of the Ninth ACM Conference on Data and Application Security and Privacy (pp. 85-96).

[12] Kim, I., Kim, D., Cho, S., & Jeon, B. (2021). A Method for Original IP Detection of VPN Accessor. The Journal of the Institute of Internet, Broadcasting and Communication, 21(3), 91-98.

[13] Goel, A., Kashyap, A., Reddy, B. D., Kaushik, R., Nagasundari, S., & Honnavali, P. B. (2022, February).