International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

IP Detection using Different Methodologies behind VPN/Proxy

[1]Tathagat Gaikwad, [2]Manoj Padvi, [3]Gaurav Patil, [4]Dr. M. T. Jagtap

[1,2,3] PVGCOE & SSDIOM Nashik, India

[4]Project Guide, PVGCOE & SSDIOM Nashik, India

Abstract ---

Cyber-attacks are increasing day by day and since the pandemic of Covid-19, the world has recorded the most cyber-attacks ever. This attack is generally performed by attackers to steal personal information or by doing financial fraud. As seen, data is the next currency for the upcoming future. So, confidentiality matters the most. Detecting unauthorized users can be problematic as the attacker are using hiding tools such as anonymizing proxies or Virtual Private Networks (VPN). It is one model to detect usage of the network in which way that it can be categorized/identified and tracked using method. The attacker uses SSH and HTTP to launch attacks by taking advantage of these services to hide their identities. This approach can be applied to other applications meeting the same criteria. Data breaches can happen the most which causes too much loss to companies. An attacker may be anyone, who attacks the server of the websites. Generally, to gather user information and to take down that website or to do some inappropriate runtime changes in the website. To track-down, down this, cyberpunk or crackers will use a honeypot and will manage to get their IP address. After getting this IP address it will track their geo- location and have the latitude and longitude of the attacker. Even though they are using a proxy or VPN it can get their exact IP address. This approach will help in finding the attacker and their system logs and other related stuff will be accessible. Hence, it can track IP behind VPN/Proxy and get information about the attacker.

Keywords*: Cyberpunk, Honeypot, VPN/proxy, IP address, data breach, SSH and HTTP.*

I. INTRODUCTION

In today's era, we face more online threats as compared to the old days. So, to overcome this kind of problem we have implemented one approach to find out what is the real IP of an attacker. Cyberattacks are increasing day by day and since the pandemic of Covid-19, the world has recorded the most cyberattacks ever. This attack is generally performed by attackers to steal personal information or by doing financial fraud. So, we will be including a honeypot as a primary weapon to lure the attacker or hacker to get his real IP. Since every transaction is recorded and publicly verified. The transaction is registered and checked publicly.

II. LITERATURE SURVEY

Various methods have been implemented for tracking the real IP address of an attacker. Various algorithms and hardware equipment were used for the same. This section provides a comparison- information about such findings. In this module the issue of detecting intruders from hiding behind hidden networks. Some of the freely available proxy services are Tor and SOCKS are popular tools that provide circuit-based anonymous connections to network users. However, recent security breaches reveal and HTTPS have been used to launch attacks by malicious users by taking advantage of these services to hide their identities.[2] Internet users are facing an unprecedentedly high risk of being tracked and monitored. However, the use of an anonymity network to protect a user's privacy comes with a cost. Since the global pandemic of Covid-19, there have been reports of economic espionage against many medical centres, universities, and pharmaceutical companies. Furthermore, hackers have used anonymity technologies to hide their identities in numerous attacks. Various types of applications are becoming more widespread. In edge computing, existing network agents, NAT, IP tunnelling technologies, and rapidly evolving anonymous communication systems provide convenience for attackers to hide real IP. The attacker also creates a "stepping" chain by breaching many intermediate edges computing network services. Network flow refers to a sequence of unidirectional data packets or frames transmitted between any different nodes in the network over some time. It is also named as communication data flow or packet flow. The network flow watermarking model mainly includes the original network flow, watermark, watermark carrier, embedded function, extracting function, and comparison function.[3] Virtualization is an emerging approach utilizing resources effectively in a cloud computing environment. Virtualization has an intellectual abstraction layer that hides the complexity of essential hardware or software. Virtualization technology is not a novel technology possessing security issues that can be inherited in a cloud environment. In a cloud environment, the virtualization method plays a vital role by providing several services for several users using with different VMs. Before virtualization, the machine is a single OS image with tightly coupled Hardware and Software. Hereafter OS runs multiple applications on the same machine by utilizing all the hardware resources like CPU, memory, NIC, and disk. [4] The investigation of a proxy detection methodology and efforts to implement such technology into a business solution with the sole purpose of eliminating the majority of fraudulent transaction attempts. The approach described identifies multiple proxy connectivity methods, and implements a multi- tiered detection technique. When

we use any Internet-related application or service, we become potential targets for cybercriminals who utilize techniques such as social engineering, phishing, and scamming to exploit system vulnerabilities for personal gain. They might act on our behalf to seize our valuable property or secretly exercise our privileges or rights.

III. METHODOLOGIES

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

IV. TECHNOLOGIES

Virtualization: The best way to think of virtualization is to imagine five physical computers, each running their own isolated operating systems and software services. Each device can work separately on different tasks, but through virtualization, you are able to unlink each operating system (OS) and its software from each terminal and combine them into one single entity, or 'host computer.' This can maintain separate software packages and run individual devices if it must.

Honeypot: This network-attached system set up as a decoy to lure cyber attackers and detect, deflect, and study hacking attempts to gain unauthorized access to information systems. A honeypot's purpose is to pose as a prospective target for attackers on the internet, typically a server or other high-value asset, collect data, and alert defenders to any unauthorized user tries to access the honeypot.

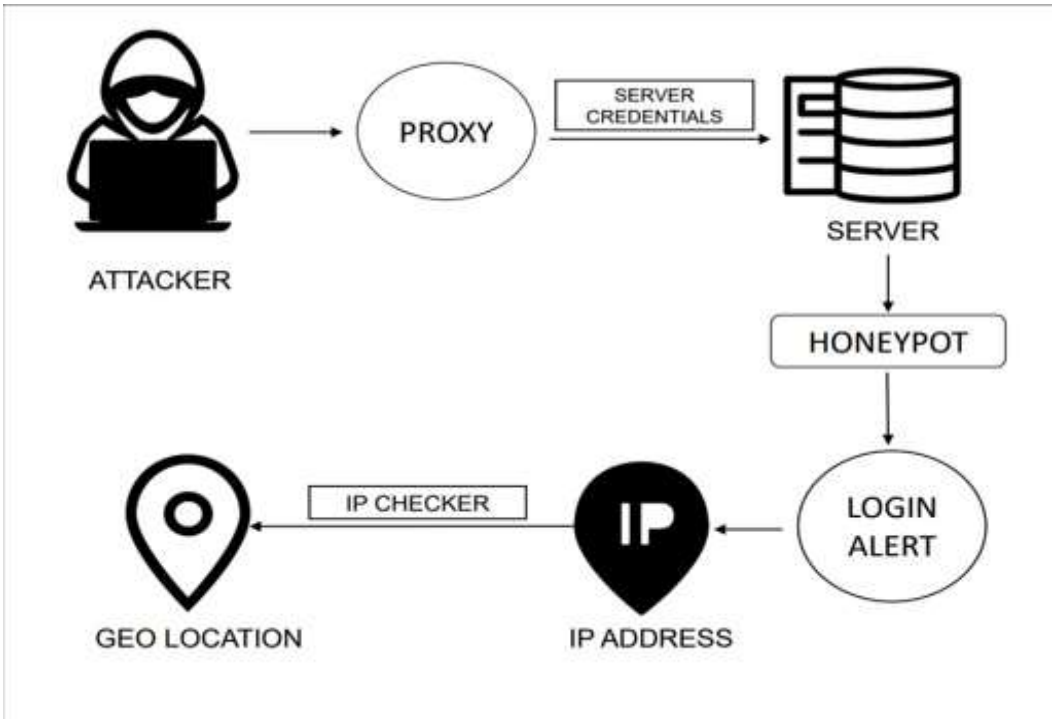

Fig. 1 Block Diagram of IP Detection using different Methodologies behind VPN/Proxy.

Working of Proposed System:

The system which we are trying to implement is an approach to deal with the live environment. A system that is developed is created to work under a certain environment. And this will vary when we try to implement the same and the live event. Our approach consists of a set of tools as well as steps that are required to follow to achieve the end goal. For this purpose, we are setting a honeypot on the server. This service will contain a website having featured login authentication and the same Scenario based tasks. Such as an e-commerce website. 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 is going 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 Website to 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 even though they are using a VPN /proxy.

V. CONCLUSION

Similar connections have many types and protocols, and with different software and technique configurations, it can be difficult to uncover a proxy connection. Although there are numerous ways to find a proxy connection right now, each one has its own shortcomings. It is our goal to create a tool that can identify the real IP Address of the attacker.

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/9583403 6.c ms