Journal of Cyber Security
DOI:10.32604/jcs.2021.024614
Article

Linux Kali for Social Media User Location: A Target-Oriented Social Media Software Vulnerability Detection

Adnan Alam Khan[1,2,*] and Qamar-ul-Arfeen[1]

[1]Sindh Madressatul Islam University, Karachi, Pakistan
[2]DHA Suffa University, Karachi, Pakistan
[*]Corresponding Author: Adnan Alam Khan. Email: write2adnanalamkhan@gmail.com
Received: 23 October 2021; Accepted: 21 December 2021

Abstract: Technology is expanding like a mushroom, there are various benefits of technology, in contrary users are facing serious losses by this technology. Furthermore, people lost their lives, their loved ones, brain-related diseases, etc. The industry is eager to get one technology that can secure their finance-related matters, personal videos or pictures, precious contact numbers, and their current location. Things are going worst because every software has some sort of legacy, deficiency, and shortcomings through which exploiters gain access to any software. There are various ways to get illegitimate access but on the top is Linux Kali with QRLjacker by user grabber command. This study recapitulates the impacts of the said technology and related avoidance. Detail contemplation depicts social media users like WhatsApp users can take a long sigh of relief when they will adopt the recommended methods. The problem is breaching of legitimate social media real-time location by an illegitimate user through Linux Kali, for this reason, end-user has no knowledge to spoof their IP to protect their real-time location. This paper will address the solution to the said problem.

Keywords: Cyber security; defensive tools; Linux Kali; WhatsApp; IP address; Artificial Intelligence; social media security

1 Introduction

Criminals or exploiters can easily be located, once Law enforcement agencies (LEAs) send WhatsApp messages to the suspect, the communication channel provides suspect details to the LEAs, their real-time location by inspecting the packet and grabbing his IP address assigned by WhatsApp. Later this IP will provide its longitude and latitude instantly. For the analysis, part LEA can use any PST as mentioned above to get its real IP. There are main types of protocols responsible for message and voice communication from one end to another a) Basic is (XMPP) Extensible Messaging and Presence Protocol b) Session Traversal Utilities for NAT (STUN) protocol works on IP address, related port, UDP/TCP data packets. Furthermore, it listens to UDP on 3478, and TCP/TLS is on 5349 port number. In curtail combination of PST provides STUN and STUN ports provide IP packet information, which will be utilized in Whois, which is an IP's database provides details of the person, further this research will locate this criminal by using IPtolocation. Software whose core duty is to intercept ongoing network packets, compose logs for traffic analysis generated by sender and receiver is generally known as Packet sniffing tool (PST) [1]. There are various types of PST windows based and Linux based, etc. The top five PST are as follows:

1. SolarWinds Network Performance Monitor (SNPM)
2. Paessler PRTG Network Monitor (PPNM)
3. ManageEngine NetFlow Analyzer (MeNA)

4. Savvius Omnipeek (SOp)
5. tcpdump (Td) CLI based program
6. WinDump (Wd)
7. Wireshark (Ws)
8. Telerik Fiddler (TF)
9. NETRESEC NetworkMiner (NNM)
10. Colasoft Capsa (CC)

Motivation factors of illegitimate social media exploiter.

1. Quick money is on the top because the motivation behind this act is greed to get a handsome amount of money in the nick of time.

S*olution,* is two-tier WhatsApp security, cloud strong password with encrypted storage file in it.

2. Impersonation, accessing data of other users for fun or sale. The motive is to access others' data and sell the user information to a third party for money.

Solution, frequency of password change is the best way to protect your account. Two-tier authentication is now implemented to secure your account, do remember password recovery option will be adopted in two ways secret question & answer and mobile recovery option.

3. Business data must be saved on various locations/clouds to save the organization from the attacker.

Solution, do not forget your data on the aforementioned location for a long duration, it will be vulnerable with time.

4. User precious data can be accessed if the user public channel, taking control of such stuff would be easy.

Solution, do not use a public network, use an enterprise firewall, and design VPN groups of users.

5. If services are not depicting normal then go for SOP provided by your IT team.

Solution, follow the SOP, mirror your server, change the password, run antivirus, and check system logs.

6. Most attractive part is credit card information, tax return info, summer visits or family holidays, airline tickets, medical receipts, medical reports, grocery item payments, shoulder surfing, wireless credit card, etc.

Solution, protect your belongings, do not give your cellphone to anyone, do not type a password in a public place, install mobile vision-protected screens, or obscure the screen by an external filter.

7. Attractive advertisement on social media or press the link to watch the full video.

Solution, this is a honey pot scheme by the exploiter to the end-user, in which the end-user will lose all his information.

8. Think thrice before clicking any link.

Solution, social media awareness means a lot of training or experience to overcome these issues.

9. Say no to fake callers from WhatsApp, Skype, Telegram, etc.

Solution, just tell them I will visit the branch to overcome this issue.

Which type of data do they want to hack? User login Name, User Email address, user physical location, user Data of Birth, user cast/Ethnicity/nationality/religion/Race, Gender, targeted user National ID# and (SSN) Social security number, user Passport details, and Visa related information, user Driving license #, and locomotive information, any user disability report, real-time user location, user nature of attended events, Marital Status, user private life information, user research projects and patents, user family novelty, social media activist or famous social media celebrity, etc.

Law enforcement agencies are doing hot escape to the criminals 24 * 7 and there are various methods so far like packet sniffing, protocol analysis, and contemplation of attached payload in any message or email. This way is time-consuming and requires a huge amount of patience and computation [1].

Mobile tower tracking is one of the most pleasant ways to know the accurate location of your loved ones. For this reason pattern, behavior, and characteristics of a person are observed through this technique to determine the personality of the said person [2].

Delhi policing has adopted a new scheme through which they recognize a person through a call graph in a very short interval of time [3].

Artificial Intelligence is the first line of defense against any crime, it is flexible, robust, adaptable, can take an online decision, and hinders any type of threat [4,5].

Bigdata utilizes Teradata or more than tera-data to analyze any crime-related pattern to guard against cybercriminals, this technique can take an online decision against any threat [6,7].

2 Related Work

1. Social media does not reveal its user location so far, for the sake of security but a user can share its location with others. This is legitimate in every aspect and the examples are online taxis like Uber, Karim, etc.

2. CLI or Linux Kali interface provides one unique and powerful command which is NETSAT which means networks and statistics with switch AN, whereas provides remote user IP address and -n depicts port numbers and numeric address.

3. Windows operating system provides the same option with DOS command NETSTAT with switch “a”, “n”, “o”. The logic is quite simple in the sense to go to the command prompt, write the said command and see the list which depicts the latest internet connectivity like TCP, UDP with three types of messages “Listening”, “Time wait” and “Established”.

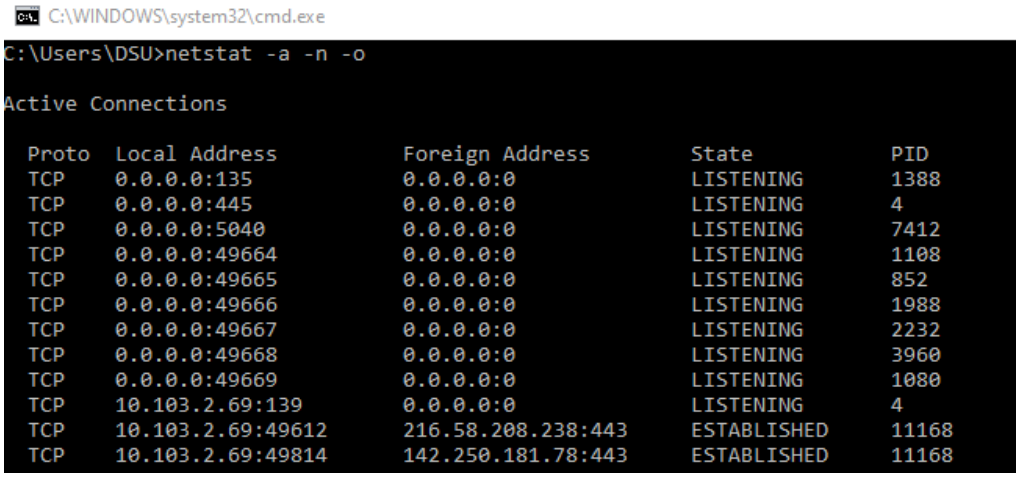
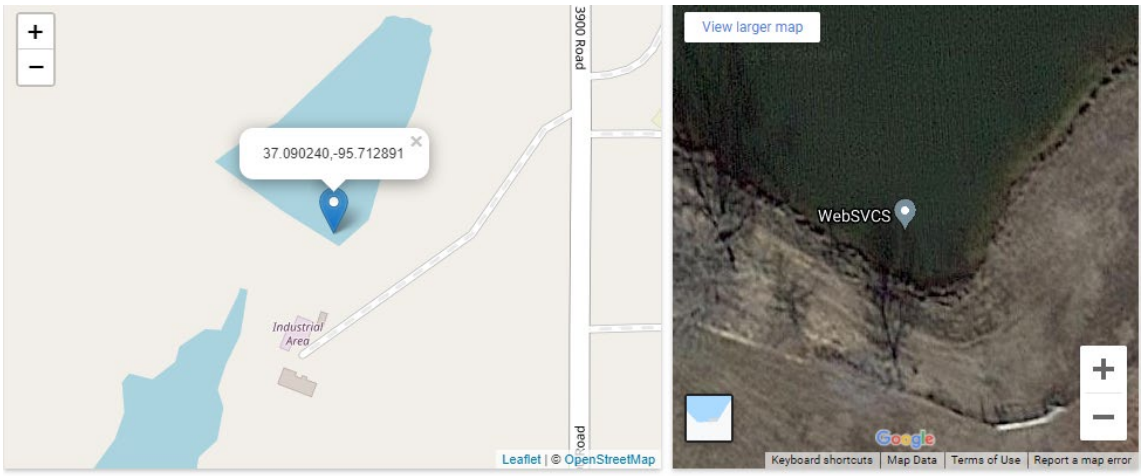


Figure 1: Foreign IP address

In Fig. 1, close the unnecessary connections and take its print screen using “PrtSc”. Now connect social media like WhatsApp on the website, you may see a new addition in the list is WhatsApp data and the list is something like it. The first attribute is “Proto” or protocol, “Local Address”, “Foreign Address”, “State” means listening, established or time wait, and Process ID or “PID”.

4. Choose the new row, copy a foreign address, and put it into IP to loc servers like “IP Logger”, “ip-adress.com”, and “ip2location.com”, etc. The end-user will get the following results.



Lat Long	GPS Coordinates
(37.090240, -95.712891)	37° 5' 24.864" N

Figure 2: Longitude and Latitude of the tacked IP address

In Fig. 2, details of the web service are easily visible to end-users like its name, country, longitude and latitude, domain name, and date with time. This type of activity can be provided to any user in any country. The Fig. 3 will provide complete details:

Permalink	https://www.ip2location.com/172.217.19.3
IP Address	172.217.19.3
Country	United States of America [US]
Region	California
City	Mountain View
Coordinates of City	37.405992, -122.078515 (37°24'22"N 122°4'43"W)
ISP	Google LLC
Local Time	07 Jul, 2021 04:26 AM (UTC -07:00)
Domain	google.com

Figure 3: Details about the remote user

Algorithm. Social Media breaching Algorithm for White Hat KALI LINUX users

while perform chat with remote user
stop other internet connections
Load LINUX KALI
Apply netstat –a –n
Check the list
Condition is false **do for** $i = 1$ *to n*
Do
if *f* (netstat -an *Send message*[*i*]) < *f* (*netstat Send video message*[*i*])
then *List*[*i*] = *Foreign List S*[*i*]
end if
end for
Apply List[i]= iptoloc{n}
Check longitude and latitude {m,n}
end if
end for

Results: The study has depicted the possibilities of network vulnerabilities in any social media platform like WhatsApp, Twitter, and Facebook, etc. To hinder this gap this study has highlighted the facts through which one can overcome the highlighted problem. In the first phase, this study highlighted the proposed algorithm that can open a new cyber security way for user data protection.

Funding Statement: The authors received no specific funding for this study.

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

[1] F. C. Tsai, E. C. Chang and D. Y. Kao, "WhatsApp network forensics: Discovering the communication payloads behind cybercriminals," in *2018 20th Int. Conf. on Advanced Communication Technology (ICACT)*, IEEE, pp. 679–684, 2018.

[2] N. Walfield, J. L. Griffin and C. Grothoff, "A quantitative analysis of Cell tower trace data for understanding human mobility and mobile networks," in *6th Int. Workshop on Mobile Entity Localization, Tracking, and Analysis (MELT)*, 2016.

[3] A. Joshi, O. Madan and B. Ranjan, "Analyzing CDR/IPDR data to find people network from encrypted messaging services," in *2018 IEEE 4th Int. Conf. on Collaboration and Internet Computing (CIC)*, IEEE, pp. 480–486, 2018.

[4] S. Dilek, H. Çakır and M. Aydın, "Applications of Artificial Intelligence techniques to combating cyber crimes: A review," *arXiv preprint arXiv:1502.03552*, 2015.

[5] M. C. Feng, J. B. Zheng, J. C. Ren, A. Hussain, X. X. Li *et al.,* "Big data analytics and mining for effective visualization and trends forecasting of crime data," *IEEE Access*, vol. 7, pp. 106111–106123, 2019.

[6] P. Stalidis, T. Semertzidis and P. Daras, "Examining deep learning architectures for crime classification and prediction," *arXiv preprint arXiv:1812.00602*, 2018.

[7] M. A. B. Bella, J. H. P. Eloff and M. S. Olivier, "Using the Internet Protocol Detail Record standard for Next-Generation Network billing and fraud detection," Pretoria, South Africa, 2005.