NOVEL APPROACH FOR LOCATION TRACKING

Shinu Francis
Department of Computer Applications
Amal Jyothi College of Engineering
Kanjirappally
shinufrancis@mca.ajce.in

Blaze Mathew
Department of Computer Applications
Amal Jyothi College of Engineering
Kanjirappally
blazemathew@mca.ajce.in

Aparna Manesh
Department of Computer Applications
Amal Jyothi College of Engineering
Kanjirappally
aparnamanesh@mca.ajce.in

Ms. Grace Joseph
Assistant Professor
Amal Jyothi College of Engineering
Kanjirappally
gracejoseph@amaljyothi.ac.in

Abstract— **In this fast era, Location Tracking is an essential technology required for tracking objects or people. A very helpful technique for parents to get updates about children without their knowledge when they are away from home. By using the penetration testing tool TrackURL and the deception method SET we are creating a URL and sending it to the victim which asks location access. When the victim allows location access, the victim's current location latitude and longitude are received by the sender. From the received URL we can track the current location with the help of Google Map.**

Keywords—TrackUrl, Location, Victim, SET

I. INTRODUCTION

TrackUrl is a penetration testing tool that is used to track the exact location of the victim. Deception is the method used to attack a victim by using SET which is a Social Engineering Toolkit. As a result, TrackUrl helps in the creation of Url, then sends it to the victim's email by using the SET Toolkit. It asks the victim to allow location when the victim gives access to the location we get the exact latitude and longitude of the victim. If we paste it in google map, we get a clear view of the victim's location.

PENETRATION TESTING

Penetration testing which is also called pen testing is referred to the process of testing a computer system, network or Web application to find vulnerabilities that an attacker could exploit and make use of it. Pen tests can be performed on applications. The most target of penetration testing is to determine security weaknesses.

Benefits of Penetration Testing

- Intelligently manage vulnerabilities.

- Avoid the cost of network downtime.

- Meet regulatory requirements and avoid fines.

- Preserve corporate image and customer loyalty.

II. LITERATURE REVIEW

V. Santhi, Dr. K. Raja Kumar, B. L. V. Vinay Kumar et al. [1] mentioned that Penetration Testing lets you protect a computer system, network or web application that allows you to obtain high-security issues that also helps find vulnerabilities that could be exploited by an attacker. This paper discusses various penetration testing techniques in Kali Linux, how to deploy them and how to use them to perform different types of attacks including methodologies.

Ahmed Mohammd Al-tarawneh & Alaa H Al-Hamami et al. [2] in Social Engineering attack using SET Toolkit packages in Kali Linux – IP address approach, depicts the social engineering attacks, with an associate experiment on Kali Linux software exploitation the Set package from the SET Toolkit, Social Engineering is that the art of manipulating individuals and build them to administer up counseling. SET may be a social engineering tool that in the main concentrates on the offensive the human part of security. Social Engineering Toolkit (SET) package to implement one in every of the social engineering attacks on Gmail accounts. Here it discusses the ways(attacks) of the Social Engineering on the social media platforms as (Facebook, twitter and Malicious software) like email, passwords or some personal information throw social media platforms.

Nikola Pavkovic, Luka Perkov et al. [3] in Social Engineering Toolkit – A systematic approach to Social Engineering, here it presents Social Engineering techniques, exploiting humans as data systems security weakest link, area unit principally the initial attack vectors at intervals larger intrusions and knowledge system compromises. Social Engineering Toolkit (SET) is an integrated set of tools designed specifically to perform advanced attacks against the human part and is that the most advanced, if not the sole toolkit of such kind that's publically accessible as open-supply computer code. This paper provides a quick introduction to the Social Engineering Toolkit computer code design and provides a summary of supported attack vectors.

DaneshIrani, Marco Balduzzi, DavideBalzarotti, EnginKirda, Calton Pu et al. [4] in Reverse Social Engineering Attacks in Online Social Networks. In this paper, it mentioned as in, a reverse social engineering attack, the attacker does not initiate contact with the victim. The victim is tricked into contacting the attacker herself. The attacker establishes a high degree of trust between the victim. When the attacker has established a friendly relationship with the victim then launch a wide range of attacks such as persuading victims to click on malicious links, phishing.

III. TRACKURL

TrackUrl is a powerful tool that can track someone's exact location, this tool run on Kali Linux is a bash/JS script for tracking locations. TrackUrl is a tool that will create a URL when your victim Visit that URL then it will ask your victim to allow location. When the victim allows the location you will get the exact latitude and longitude of the victim.

FEATURES

- Automated Tool
- Track Exact Location
- Easily Edit the TrackUrl Program
- Easy to use

IV. SET

Social Engineering is the art of manipulating people and make them give up confidential information. SET is a Social Engineering Tool which mainly concentrates on attacking the human element of security.

 FEATURES

- Fast penetration testing
- Integration with third-party modules
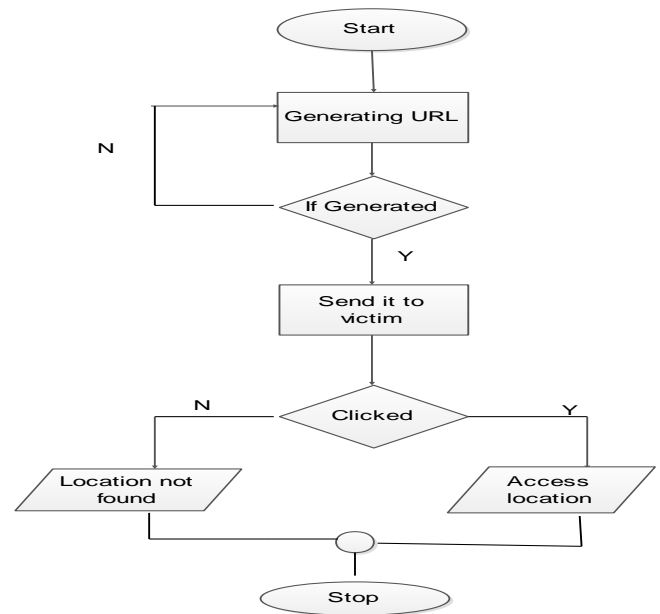- Phishing attack generator

Fig 1: Flowchart

V. IMPLEMENTATION

Step 1: We need to clone the TrackUrl from GitHub. To do that, you need to type this command:

git clone https://www.github.com/Mauladen/TrackUrl

Step 2: Change the Directory to TrackUrl by using the command cd TrackUrl. Now, you have to get in the TrackUrl, just by typing: ./TrackUrl.sh.

Step 3: Now, you have to get in the TrackUrl, just by typing: ./TrackUrl.sh.

Step 4: Then we will get two terminals one is the Xterm terminal and the other is our main terminal.

Step 5: From the X-term terminal copy the link with "https" in it and paste it in the main terminal. (fig.2)
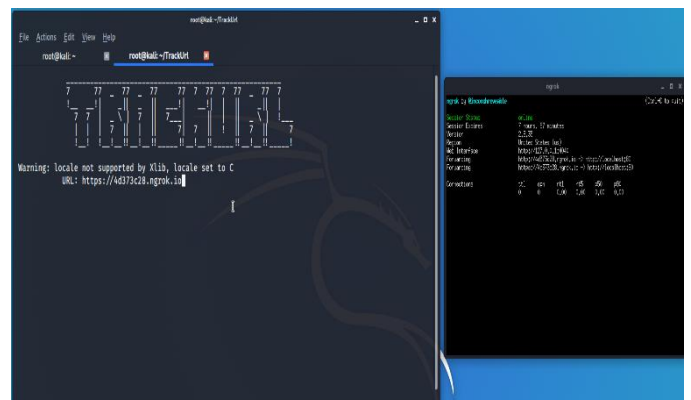

Fig 2

Step 6: The attacker sends the link to the victim by email using the Mass Mailer Attack which is an email option available in the SET toolkit. The victim trust that it is not a malicious site. When the victim opened the email and click on the link, a new phishing page appears and asks the victim to allow location. When the victim allows location access, the victim location can be traced. (fig.3)
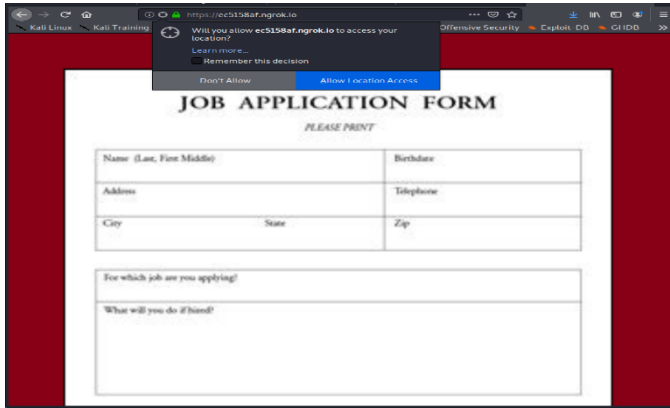

Fig 3

Step 7: The tail terminal on the attacker, there will be a bunch of sentences. Choose the number which is at the bottom and which after "/log me/" and behind "http/1.1/".

Step 8: Go to Google Maps and paste the numbers and search, we will get the victim's location. (fig.4)
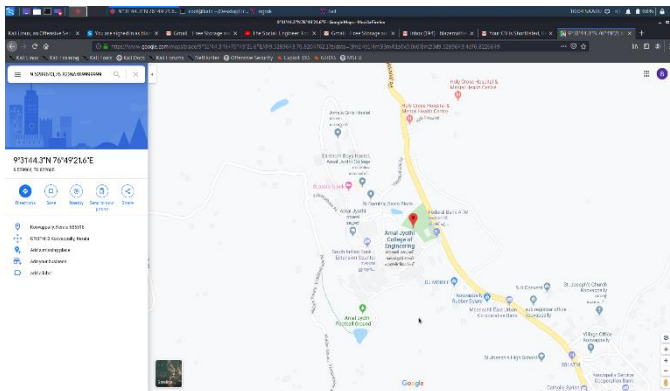

Fig 4

TECHNIQUE EMPLOYED -NGROK

Ngrok is multiplatform tunneling, opposite proxy software program that establishes comfy tunnels from a public endpoint inclusive of the net to a regionally jogging community provider at the same time as taking pictures all site visitors for distinctive inspection and replay. The second element:8080 means connect with port 8080 of that internet address. If you don't specify it, your net browser will connect to the default webserver port, that's port eighty. Port eighty is the port quantity assigned to generally used internet verbal exchange protocol, hypertext transfer protocol secure (https). It's miles the port from which a pc sends and gets net customer based conversation and messages from a web server and is used to ship and acquire Html pages or information.

VI. CONCLUSION

TrackUrl is a very helpful tool to track the exact location of the victim integrating with the SET Toolkit. We can send phishing emails to the targeted victim and thus we get the targeted victim location by clicking the link. In the future, we can focus on the improved tracking method which helps to track the victim effectively.

REFERENCES

[1] V. Santhi, Dr. K. Raja Kumar, B. L. V. Vinay Kumar: Penetration Testing using Linux Tools: Attacks and Defense Strategies.

[2] Ahmed Mohammd Al-tarawneh & Alaa H Al-Hamami: Social Engineering attack using setoolkit packages in Kali Linux – IP address approach.

[3] Nikola Pavković, Luka Perkov: Social Engineering Toolkit – A systematic approach to social engineering.

[4] Danesh Irani, Marco Balduzzi, Davide Balzarotti, Engin Kirda, Calton Pu: Reverse Social Engineering Attacks in Online Social Networks.