Social Engineering Attack on Creating Fake Webpage in Social Media

Dr. T. Arumuga Maria Devi
Associate Professor[1]
Centre For Information Technology Engineering
Manomaniyam Sundaranar University,
Tirunelveli, India

R. Arun Bothagar
PG Scholar[2]
Centre For Information Technology Engineering
Manomaniyam Sundaranar University,
Tirunelveli, India

M. Divya Magesh
PG Scholar[3]
Centre For Information Technology Engineering
Manomaniyam Sundaranar University,
Tirunelveli, India

***Abstract*— A Social engineering is a network type attack where To trick an internet user into disclosing personal information, the attacker fabricates a replica of an existing webpage. This review's main goal is to conduct a literature evaluation on social engineering attacks. This paper addresses hypothetically how social engineering assaults and phishing scams effect people's daily life. Phishing is the practise of employing both technological and social engineering approaches to persuade a user to give personal information. Phishing is frequently done through instant chat or email spoofing. It mostly targets users who are ignorant In social engineering techniques and online safety, such as those who neglect to protect the privacy of their Facebook, Gmail, Twitter, credit card, and other financial account information.**

Keywords—VM ware, kali Linux, SET TOOL KIT, URL

INTRODUCTION

Mobile phones & Computers are becoming major part of people’s everyday life, since they are connected with friends, family, Business, Can use any time anyplace & anywhere. Phishing is an example of Social Engineering. Phishing is primarily utilised in email hacking, where the hacker sends a link to the recipient via email in exchange for, say, some bank information other personal information. During the COVID-19 Pandemic, phishing attacks had a great deal of victims. [1] According to statistics on cyber security for 2021, social engineering was used in 98% of cyberattacks, and 43% of IT workers had fallen victim to similar attacks the year before. [2]

I. RELATED WORK

The most common type of social engineering, phishing, has an increasing number of victims. Phishing entails meticulously designing websites and emails to look exactly like the authentic ones. The user is deceived into supplying personal data via Phishing attacks can also be carried out via phone calls, text messages, or even social media, while email phishing is still the most common type. A highly specialized method of phishing known as spear-phishing or website attack targets victims or prominent targets in a company.[3] By tricking the user into clicking a link or an attachment, the attacker can gain access to the targeted system by opening a backdoor.[4] The attacker will now be able to steal everything from the user, including financial information, personnel information, important passwords, and corporate credentials.[5]

II SOFTWARE USED FOR PROPOSED SYSTEM

An open-source operating system is Kali Linux. In this Linux are distribution allowing cyber security professionals and ethical hackers to perform penetration testing and security audits against internal and remote networks. Freely available to access the users. In order to run different operating systems on a single physical host computer, x86 and x86-64 PCs can use the virtual machine software called VM ware Workstation. Each virtual machine can run a single instance of any operating system (Windows, Linux, etc.) simultaneously.

Dave Kennedy, the founder of Trusted Sec, developed and wrote the Social-Engineer Toolkit (SET).It is an open-source Python programme designed to perform penetration tests on Social-Engineering systems.

A website tool included in SET turns your Kali server into a web server equipped with a variety of exploits that can compromise the majority of browsers. Sending your target a link that takes them to your website and then directly to the exploit's download and execution page is the idea. In order to make the exploit appear more convincing, you can even use the pre-built templates in SET to copy an actual website. A number of well-known websites, including Facebook, Twitter, Google, and Yahoo, include pre-formatted phishing pages.

III. METHODOLOGY

The purpose of this study is to determine social networking site users' understanding of the hazards involved, identify privacy settings that are vulnerable, and assess the risks.

SOCIAL MEDIA ANALYSIS

In 2021, 91.2% of the 81 respondents said they use Facebook frequently.13.6% acknowledged using other social media sites, while 59% named twitter, 81.6% LinkedIn, and 71%

Instagram. This suggested that a significant portion of the respondents expressed their opinions on a variety of social media sites. In response to the question about how long respondents had been using social media, 43% said they had been using it for more than six years, 22% said they had been using it for between four and six years, and 20% said they had been using it for between two and four years. The fact that 9% of users were under the age of two is particularly significant because it shows that they have only recently started using social media as a means of self-expression.

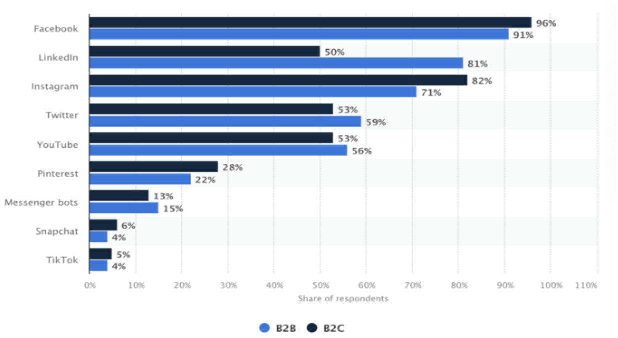


Figure:1

SOCIAL MEDIA USAGE

Only 20% of respondents said they normally attempt to avoid posting, while the majority of respondents (77%) said they frequently share their own photographs and videos on social media Of the respondents (70%) who said they also post photos of friends and family, 57% said they would publish the location. Despite the fact that 54% of respondents said they post personal contact information on their profiles, 42% of the respondents said they do not share personal information.

According to the study, 73% of users acknowledged to sharing personal information on social media, while only 23.5% said they often don't.83% of people who responded to the question about social media awareness of social security said they are aware of social dangers.15% of them said that they were ignorant about social media information security. While 88% of the respondents said they don't disclose their usernames or passwords with friends or family members who use their accounts, 9% said they do. This shows that consumers are generally aware of the value of security, however there are weaknesses due to users exchanging information.

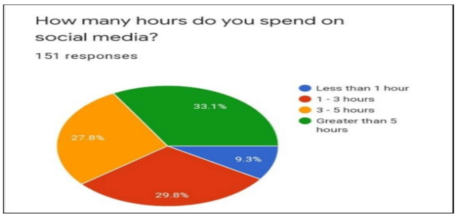


Figure:2

IV. PROPOSED SYSTEM

You can open SET in Kali Linux by going to Applications > Kali Linux > Exploitation Tools > Social Engineering Toolkit | toolkit or by entering **Set toolkit** as a shell prompt. The aim of the attack is getting the "User name" and "password" of victims in mobile phones pcs and IP address. Now we launch the social engineering tool kits. And it has implemented this tool using the command like https://github.com/trustedsec/ptf After this command the kali Linux will make a directory for this clone document. Now we launch the social engineering tool kit dialogue box will appear. They can 'n' number of attacks using in this tool. Now we can select the Social Engineering attack vectors to switch on web attack modes. Then set our Localhost IP address which is example:(10.0.2.15) And Enter fake URL website to clone Finally, we can configure the clone Templates.

IMPLEMENTATION STEPS

- Step1:VMware Workstation 16 Player Version 15.0.2
- Step2: Configure a Kali Linux in VM workstation
- Step3: Open Kali Linux Terminal
- Step4: Cloning the GitHub in Trusted Tool
- Step5: Social Engineering Toolkit Dialog Box Open
- Step6: Select >1st phase social Engineering attack
- Step7: Select the 2nd Menu of Website Attack Vectors
- Step8: And select Credential harvester Attack Method
- Step9: Then Enter the host IP Address.
- Step10: When Copy the URL/IP Send email to Victim

PREVENTION IN SOCIAL ENGINEERING ATTACK

Attacks using social engineering pose serious security threats, so enterprises and organisations should include prevention in their risk management plans. Businesses should commit to fostering a culture of security have an awareness among their workforce. Numerous strategies have been suggested to identify and stop these attacks.

Encouragement of security education and training, increased social awareness of social engineering attacks, provision of necessary tools to detect and prevent these attacks, instruction on how to protect confidential information, reporting any suspected activity to the security service, organisation of security orientations for new hires, and dissemination of sensitization emails and known fraudulent email to all employees social engineering attacks.

1. Avoid opening Fake Email & Attachments
2. Avoid Sharing personal Information
3. Be Careful of the Tempting offers
4. Use Multi factor Authentication
5. Install an Anti-malware and keep it updated

V RESULTS

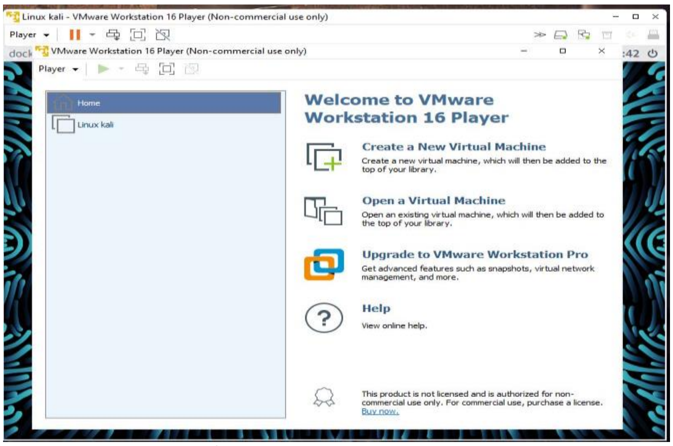

Linux kali - VMware Workstation 16 Player (Non-commercial use only)
VMware Workstation 16 Player (Non-commercial use only)
Player
Home
Linux kali
Welcome to VMware Workstation 16 Player
Create a New Virtual Machine
Create a new virtual machine, which will then be added to the top of your library.
Open a Virtual Machine
Open an existing virtual machine, which will then be added to the top of your library.
Upgrade to VMware Workstation Pro
Get advanced features such as snapshots, virtual network management, and more.
Help
View online help.
This product is not licensed and is authorized for non-commercial use only. For commercial use, purchase a license. Buy now.

Figure (4) Configure a Kali Linux in VMware Workstation

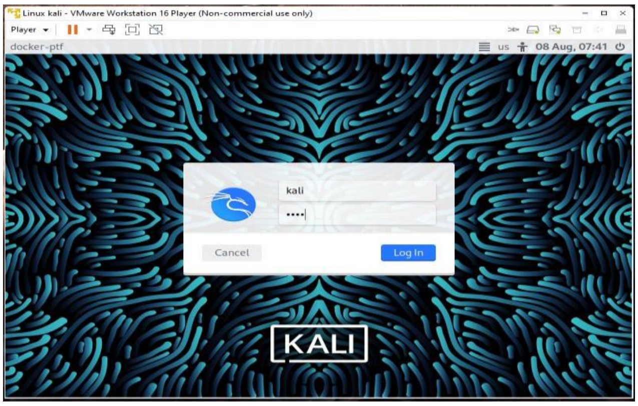

Linux kali - VMware Workstation 16 Player (Non-commercial use only)
Player
docker-ptf
us
08 Aug, 07:41
kali
Cancel
Log In
KALI

Figure (5) The user name and password will appear on Kali Linux's login page once configuration is finished.

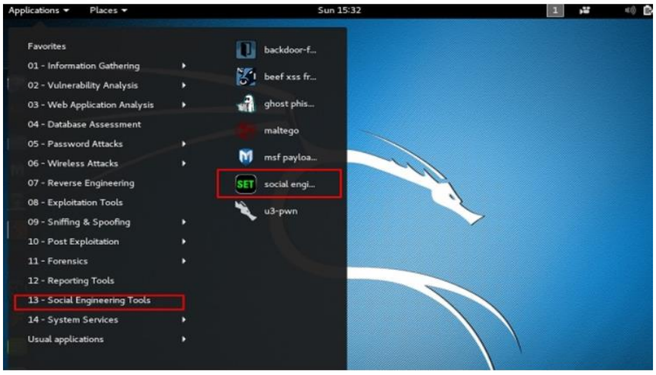
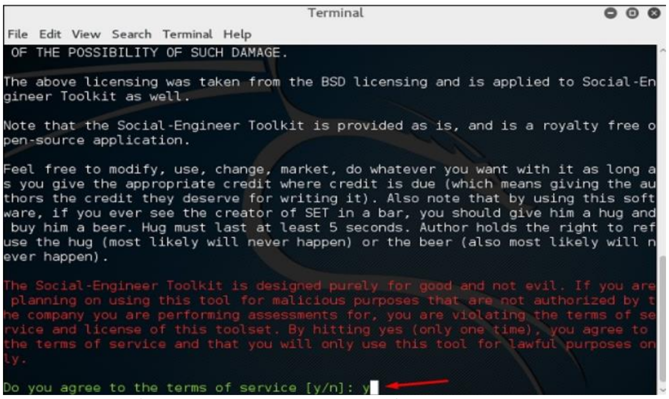
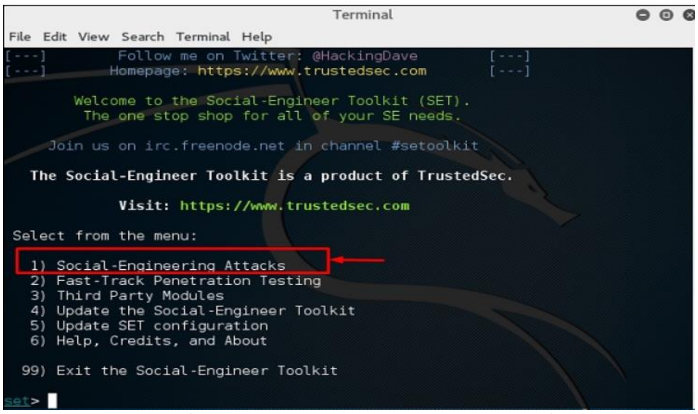


Figure (6) Go to Applications Social Engineering Tools to launch SET. Social engineering tool: click "SET."



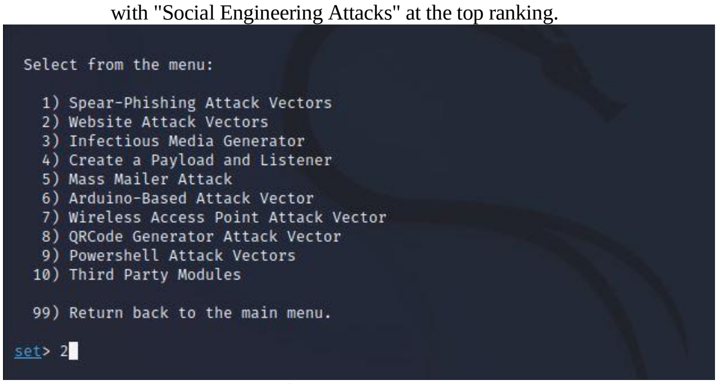
```
 OF THE POSSIBILITY OF SUCH DAMAGE.

The above licensing was taken from the BSD licensing and is applied to Social-En
gineer Toolkit as well.

Note that the Social-Engineer Toolkit is provided as is, and is a royalty free o
pen-source application.

Feel free to modify, use, change, market, do whatever you want with it as long a
s you give the appropriate credit where credit is due (which means giving the au
thors the credit they deserve for writing it). Also note that by using this soft
ware, if you ever see the creator of SET in a bar, you should give him a hug and
 buy him a beer. Hug must last at least 5 seconds. Author holds the right to ref
use the hug (most likely will never happen) or the beer (also most likely will n
ever happen).

The Social-Engineer Toolkit is designed purely for good and not evil. If you are
 planning on using this tool for malicious purposes that are not authorized by t
he company you are performing assessments for, you are violating the terms of se
rvice and license of this toolset. By hitting yes (only one time), you agree to
the terms of service and that you will only use this tool for lawful purposes on
ly.

Do you agree to the terms of service [y/n]: y
```

Figure(7) If you agree to the conditions of usage, it will ask you.Input "y" as seen in the screenshot below.



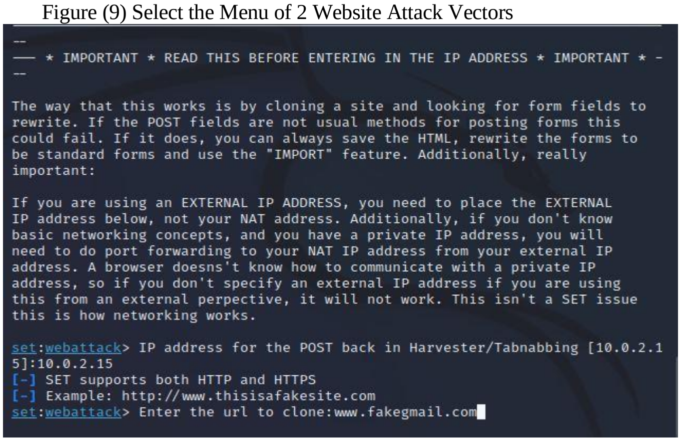
```
[---]        Follow me on Twitter: @HackingDave        [---]
[---]       Homepage: https://www.trustedsec.com       [---]

        Welcome to the Social-Engineer Toolkit (SET).
         The one stop shop for all of your SE needs.

     Join us on irc.freenode.net in channel #setoolkit

   The Social-Engineer Toolkit is a product of TrustedSec.

           Visit: https://www.trustedsec.com

 Select from the menu:

   1) Social-Engineering Attacks
   2) Fast-Track Penetration Testing
   3) Third Party Modules
   4) Update the Social-Engineer Toolkit
   5) Update SET configuration
   6) Help, Credits, and About

  99) Exit the Social-Engineer Toolkit

set>
```

Figure(8) The most of the menus in the screenshot below are self-explanatory, with "Social Engineering Attacks" at the top ranking.



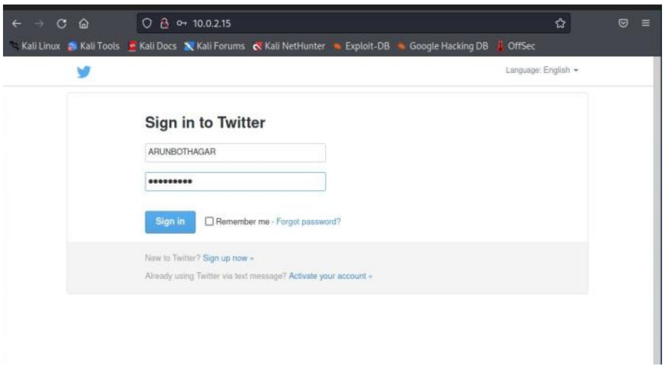
```
 Select from the menu:

   1) Spear-Phishing Attack Vectors
   2) Website Attack Vectors
   3) Infectious Media Generator
   4) Create a Payload and Listener
   5) Mass Mailer Attack
   6) Arduino-Based Attack Vector
   7) Wireless Access Point Attack Vector
   8) QRCode Generator Attack Vector
   9) Powershell Attack Vectors
  10) Third Party Modules

  99) Return back to the main menu.

set> 2
```

Figure (9) Select the Menu of 2 Website Attack Vectors



```
--
—— * IMPORTANT * READ THIS BEFORE ENTERING IN THE IP ADDRESS * IMPORTANT * -
--

The way that this works is by cloning a site and looking for form fields to
rewrite. If the POST fields are not usual methods for posting forms this
could fail. If it does, you can always save the HTML, rewrite the forms to
be standard forms and use the "IMPORT" feature. Additionally, really
important:

If you are using an EXTERNAL IP ADDRESS, you need to place the EXTERNAL
IP address below, not your NAT address. Additionally, if you don't know
basic networking concepts, and you have a private IP address, you will
need to do port forwarding to your NAT IP address from your external IP
address. A browser doesns't know how to communicate with a private IP
address, so if you don't specify an external IP address if you are using
this from an external perpective, it will not work. This isn't a SET issue
this is how networking works.

set:webattack> IP address for the POST back in Harvester/Tabnabbing [10.0.2.1
5]:10.0.2.15
[-] SET supports both HTTP and HTTPS
[-] Example: http://www.thisisafakesite.com
set:webattack> Enter the url to clone:www.fakegmail.com
```

Figure (10) This attack technique has the ability to make a malicious copy of a web platform in an effort to gather login information from a targeted victim. The IP address of the computer used for the attack, in this case Kali Linux (10.0.2.15), and the URL of the website to be cloned, which, for this demonstration, is a well-known social network website, such as Facebook, Twitter, or Gmail Accounts are needed to execute this exploit.



Sign in to Twitter

ARUNBOTHAGAR

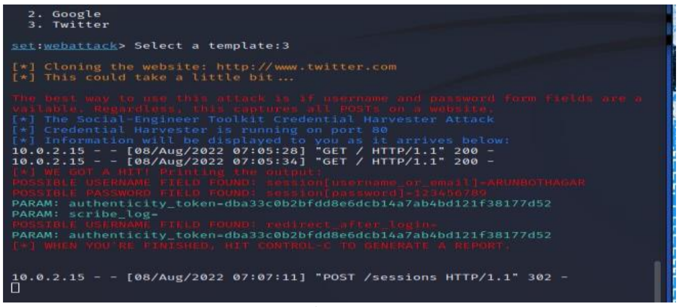
••••••••••

Sign in □ Remember me · Forgot password?

New to Twitter? Sign up now »

Already using Twitter via text message? Activate your account »

Figure (11) By using social engineering techniques, the perpetrator tricks the victim into providing the wrong credentials. The victim clicks the link, types their username and password, and the login information is then forwarded to the Kali Linux server.



```
  2. Google
  3. Twitter

set:webattack> Select a template:3

[*] Cloning the website: http://www.twitter.com
[*] This could take a little bit...

The best way to use this attack is if username and password form fields are a
vailable. Regardless, this captures all POSTs on a website.
[*] The Social-Engineer Toolkit Credential Harvester Attack
[*] Credential Harvester is running on port 80
[*] Information will be displayed to you as it arrives below:
10.0.2.15 - - [08/Aug/2022 07:05:28] "GET / HTTP/1.1" 200 -
10.0.2.15 - - [08/Aug/2022 07:05:34] "GET / HTTP/1.1" 200 -
[*] WE GOT A HIT! Printing the output:
POSSIBLE USERNAME FIELD FOUND: session[username_or_email]=ARUNBOTHAGAR
POSSIBLE PASSWORD FIELD FOUND: session[password]=123456789
PARAM: authenticity_token=dba33c0b2bfdd8e6dcb14a7ab4bd121f38177d52
PARAM: scribe_log=
POSSIBLE USERNAME FIELD FOUND: redirect_after_login=
PARAM: authenticity_token=dba33c0b2bfdd8e6dcb14a7ab4bd121f38177d52
[*] WHEN YOU'RE FINISHED, HIT CONTROL-C TO GENERATE A REPORT.


10.0.2.15 - - [08/Aug/2022 07:07:11] "POST /sessions HTTP/1.1" 302 -
□
```

Figure (12) credentials for the victim on the terminal

CONCLUSION

The Real time case study of Social Engineering Attack WE can gathering a lot of information about impact of phishing. Also a various Social Engineering Techniques Like smishing, spear phishing, Whaling, Baiting, Vishing can be used for people that are interested in such purposes. This instance demonstrates how social engineering and phishing are attacks that prey on human frailties. We practically learn about the tools and techniques that are required to perform the fake social media web page attack. These attacks are harmful to stolen the victim sensitive information like (user name and password). So hence it can implement the proper security measures in order to avoid the fake web pages for social Engineering attacks.

REFERENCES

[1] "Kali Linux", https://www.kali.org/. [Online; accessed on December 21 2016].

[2] "Social-engineer toolkit", https://www.trustedsec.com/. [Online; accessed on December 21 2016]

[3] Mika Kontio et al, "Social engineering", pp.101, 2016.

[4] Chewae, M., Hayikader, S., Hasan, M.H., Ibrahim J. (2015). How Much Privacy We Still Have on Social Network. International Journal of Scientific and Research Publications, 5(1), 1.

[5] Rahul Singh Patel, "Kali Linux Social Engineering", Packt Publishing Ltd, 2013..

[6] Parthy P. P, Rajendran G. Identification and prevention of social engineering attacks on an enterprise. 2019; pp 1–5.

[7] https://en.wikipedia.org/wiki/Social_engineering_(security)"
Social engineering (security)".

AUTHOR'S PROFILE

Dr. T. Arumuga Maria Devi Associate Professor, Received B.E. degree in Electronics & Communication Engineering from Manonmaniam Sundaranar University, Tirunelveli, Tamil Nadu, India, in 2003, M.Tech degree in Computer & Information Technology from Manonmaniam Sundaranar University, Tirunelveli, Tamil Nadu, India, in 2005, also received Ph.D degree in Information Technology—Computer Science and Engineering, from Manonmaniam Sundaranar University, Tirunelveli, Tamil Nadu, India, in 2012 and also the Associate Professor of Center for Information Technology and Engineering of Manonmaniam Sundara nar University since November 2005 onwards. Her research includes Signal Processing, Remote Communication, Multime- dia and Mobile Computing.

ArunBothagar. R, Msc CyberSecurity, Centre for Information Technology & Engineering, Manonmaniam Sundaranar University, Abishekapatti, Tirunelveli - 627012, Tamil Nādu, India. .He received Bachelor of Networking in Subbulakshmi Lakshmipathi College of Science ,Madurai-2021.His Research includes Social Enfineering.Ethical Hacking Using Linux Platform.

M. Divya Magesh, MSc Data Analytics, Centre for Information Technology & Engineering, Manonmaniam Sundaranar University, Abishekapatti, Tirunelveli - 627012, Tamilnadu, India. She received her in Bachelor of Mathematics in Sri GVG Vishalakshi College for Womens,Udumalpet.Her Research includes Machine learning,Natural Language Processing.