**HIDDENEYE**

**MCA REGULAR SEMINAR REPORT**

**Submitted in partial fulfilment of requirements for the**

**Award of the Degree in**

**Regular Master of Computer Application**

**By**

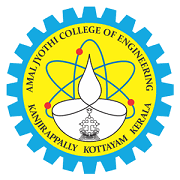
**TINTU KL**

**Reg No:LAJC17MCA043**

**Under the Guidance of**

**Mr.TJ Jobin**

**Assistant Professor,MCA**

****

**Department of Computer Application**

**Amal Jyothi College of Engineering**

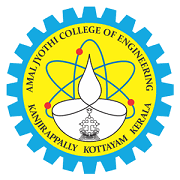
**Kanjirappally,Kerala**

**November 2019**

**DEPARTMENT OF COMPUTER APPLICATIONS**

**AMAL JYOTHI COLLEGE OF ENGINEERING**

**KANJIRAPPALLY**

****

**CERTIFICATE**

This is certify that the seminar report “**HIDDENEYE**” tool in kali linux is the bonafide work of **TINTU KL** (Reg no: LAJC17MCA043) in partial fulfilment of the requirements for the award of the Master of Computer Application Regular under Kalam Technical University during the year 2019.

**Mr.TJ Jobin Ms.Shelly Shiju George**

**Internal Guide Coordinator**

**Fr.Rubin Thottupuram**

**Head of Department**

**ACKNOWLEDGEMENT**

First and foremost, I thank God almighty for his eternal love and protection throughout the seminar, I take this opportunity to express my gratitude to all who helped me in completing this seminar successfully. It has been said that gratitude is the memory of heart. I wish to express my sincere gratitude to our Manager **Rev. Fr. Dr. Mathew Paikatt** and our Principal **Dr. Z. V. Lakaparambil** for providing good faculty for guidance.

I owe a great depth of gratitude towards our Head of the Computer Application Department **Fr. Rubin** **Thottupuram**  for helping me. I extend my whole hearted thanks to the Seminar Coordinator **Ms. Shelly Shiju** **George** for her valuable suggestions and for overwhelming concern and guidance from the beginning to the end of the Seminar. I would also like to express sincere gratitude to my Guide**, Mr. TJ Jobin** for his inspiration and helping hand.

I thank to our beloved teachers for their corporation and suggestions that helped me throughout the seminar. I express my thanks to all my friends and classmates for their interest ,dedication, and encouragement shown towards the seminar. I convey my family for the moral support ,suggestions, and encouragement to make this venture a success.

**Tintu KL**

**CONTENTS**

**1.INTRODUCTION………………………………………………………………5**

**1.1 KALI LINUX ………………………………………………………………5**

**1.2 PENETRATING TESING …………………………………………………6**

**1.3 ETHICKAL HACKING…………………………………………………....7**

**2. HIDDENEYE……………………………………………………………………..9**

**2.1 INTRODUCTION TO HIDDENEYE……………………………………..9**

**2.2 FEATURES OF HIDDENEYE…………………………………………....9**

**3.WORKING OF HIDDENEYE…………………………………………………..11**

**4. HOW TO PREVENT PHISHING ATTACK………………………………….17**

**5. CONCLUSION…………………………………………………………………..20**

**5. REFERENCES…………………………………………………………………...21**

**1.INTRODUCTION**

* 1. **Kali Linux**

[Kali Linux](https://www.kali.org/) is a Debian-based Linux distribution aimed at advanced Penetration Testing and Security Auditing. Kali contains several hundred tools which are geared towards various information security tasks, such as Penetration Testing, Security research, Computer Forensics and Reverse Engineering. It was developed by Mati Aharoni and Devon Kearns of offensive security through the rewrite of Backtrack, their previous information security testing Linux distribution based on Knoppix. The third core developer Raphael Hertzog joined them as a Debian expert. Kali Linux was released on the 13th march, 2013 as a complete ,top to bottom. Rebuild of Backtrack Linux, adhering completely to Debian development standards.

Kali Linux is one of the best open-source security packages of an ethical hacker, containing a set of tools divided by categories. Kali Linux can be installed in a machine as an Operating System. Installing Kali Linux is a practical option as it provides more options to work and combine the tools.

* Provides More than 600 penetrating testing tools.
* OS Family –Unix Like
* Working State- Active
* Platform –x86,x86-64,armel,armhf
* Kernel Type-Monolithic kernel (Linux)
* Default UI –GNOME3
  1. **PENETRATION TESTING**

Penetration testing, also called pen testing or ethical hacking, is the practice of testing a computer system, network or web application to find security vulnerabilities that an attacker could exploit. Penetration testing can be automated with software applications or performed manually. Either way, the process involves gathering information about the target before the test, identifying possible entry points, attempting to break in -- either virtually or for real -- and reporting back the findings.

The main objective of penetration testing is to identify security weaknesses. Penetration testing can also be used to test an organization's [security policy](https://searchsecurity.techtarget.com/definition/security-policy), its adherence to [compliance](https://searchdatamanagement.techtarget.com/definition/compliance) requirements, its employees' security awareness and the organization's ability to identify and respond to security incidents. Penetration tests are also sometimes called [white hat](https://searchsecurity.techtarget.com/definition/white-hat) attacks because in a pen test, the good guys are attempting to break in.

**Purpose of penetration testing**

The primary goal of a pen test is to identify weak spots in an organization's security posture, as well as measure the compliance of its security policy, test the staff's awareness of security issues and determine whether -- and how -- the organization would be subject to security disasters.

**Penetration test strategies**

Targeted Testing – Testing team working together.

External Testing – Targets externally visible servers or devices.

Internal Testing- Attack behind the firewall.

Blind Testing- Simulates the actions of a real attacker.

**Targeted testing** is performed by the organization's IT team and the penetration testing team working together. It's sometimes referred to as a "lights turned on" approach because everyone can see the test being carried out.

**External testing**targets a company's externally visible servers or devices including domain name servers, email servers, web servers or firewalls. The objective is to find out if an outside attacker can get in and how far they can get in once they've gained access.

**Internal testing** mimics an inside attack behind the firewall by an authorized user with standard access privileges. This kind of test is useful for estimating how much damage a disgruntled employee could cause.

**Blind testing**simulates the actions and procedures of a real attacker by severely limiting the information given to the person or team performing the test beforehand. Typically, the pen testers may only be given the name of the company. Because this type of test can require a considerable amount of time for reconnaissance, it can be expensive.

**Benefit of Penetration Testing**

Intelligently manage vulnerabilities.

Avoid the cost of network downtime.

Meet regulatory requirements and avoid fines.

Preserve corporate image and customer loyalty.

* 1. **ETHICAL HACKING**

An ethical hacker, also referred to as a [white hat](https://searchsecurity.techtarget.com/definition/white-hat) hacker, is an information security expert who systematically attempts to penetrate a computer system, network, application or other computing resource on behalf of its owners -- and with their permission -- to find security vulnerabilities that a malicious hacker could potentially exploit.

The purpose of ethical hacking is to evaluate the security of and identify vulnerabilities in systems, networks or system infrastructure. It includes finding and attempting to exploit any vulnerabilities to determine whether unauthorized access or other malicious activities are possible.

**Uses of Ethical Hacking**

There are a number of ways ethical hackers can help organizations, including:

**Finding vulnerabilities**. Ethical hackers help companies determine which of their IT security measures are effective, which need to be updated and which contain vulnerabilities that can be exploited. When ethical hackers finish evaluating organizations' systems, they report back to company leaders about those vulnerable areas, for instance, a lack of sufficient password encryption, insecure applications or exposed systems running unpatched software. Organizations can use the data from these tests to make informed decisions about where and how to improve their security posture to prevent cyberattacks.

**Helping prepare for a cyberattack**. Cyberattacks can cripple or destroy a business, especially a small business. However, most companies are completely unprepared for cyberattacks. Ethical hackers understand how threat actors operate and they know how these bad actors will use new information and techniques to attack systems. Security professionals who work with ethical hackers are better able to prepare for future attacks because they can better react to the constantly changing nature of online threats.

**2.HIDDENEYE**

**2.1 INTRODUCTION TO HIDDENEYE**

Phishing is a type of social engineering attack often used to steal user data, including login credentials and credit card numbers.It occurs when an attacker, masquerading as a trusted entity , dupes a victim into opening an email, instant message or text message. The recipient is then tricked into clicking a malicious link, which can lead to the installation of malware, the freezing of the system as part of a ransom ware attack or the revealing of sensitive information.

HiddenEye is a tool for perform phishing attacks. It work just like other phishing framework, simply it takes credentials from users when they type confidential information like usernames, passwords, credit card-numbers and take that inputs and show you on terminal. .It is the advanced phishing tool with 34 phishing pages such as Instagram,Facebook, Snapchat, Twitter, Github, Google, Spotify, NetFlix, paypal, Origin, steam ,Yahoo , LinkedIn, Protonmail, Wordpress, Microsoft, IGFollowers, eBay, Pintrest , CryptoCurrency, Verizon, Dropbox, Adobe, Shopify, Messenger , Git Hub, Twitch ,MySpace,Badoo, VK, Yandex, iCloud,GitLab devianART. HiddenEye also provides the information of victim such as IP address,Country, State City Location , Geolocation, ISP.

HiddenEye uses ngrok ,where ngrok is a cross-platform application that enables developers to expose a local development server to the internet with minimal effort.

**Requiements**

Installed Kali Linux on your system.

Basic knowledge on kali Linux.

Downloading link of HiddenEye tool.

Python 3

Internet connection.

sudo

* 1. **FEATURES OF HIDDENEYE**
* Live information about the victims such as : IP ADDRESS, Geolocation, ISP, Country, & many more.
* All the sites are mobile compatible.
* Ability to capture all the keystokes of victim.
* **Large collection of phishing pages are added.**

**Downloading HiddenEeye**

Download HiddenEye using the following URL:

https://github.com/DarkSecDevelopers/HiddenEye.git

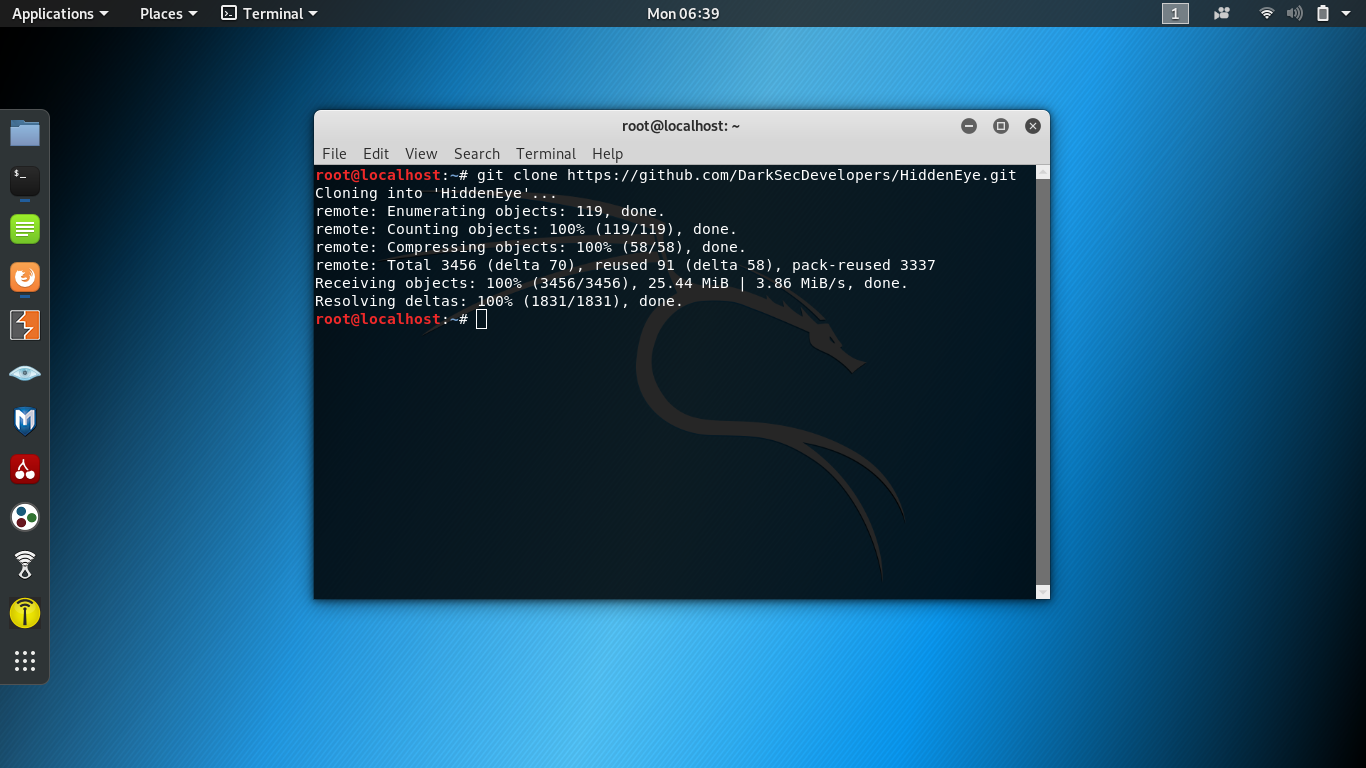
To clone the following command is used

git clone https://github.com/DarkSecDevelopers/HiddenEye.git

**3.STEPS FOR PHISHING USING HIDDENEYE**

Step 1:

Download the link from GitHub and clone the link to get access to the sub folders of HiddenEye

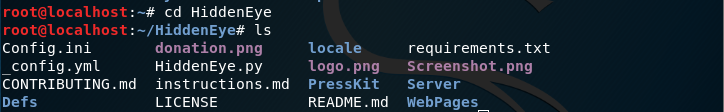


Step 2:

After the HiddenEye Downloaded ,got a new folder ‘HiddenEye’. To access this directory ,the following command is used:

cd HiddenEye.

List the folder ‘HiddenEye’ ,it contains a file ‘HiddenEye.py’.

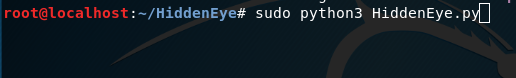


Step 3:

Execute the following command, it will open a new terminal.

Pip3 install –r requirements.txt ,Sudo python3 HiddenEye.py

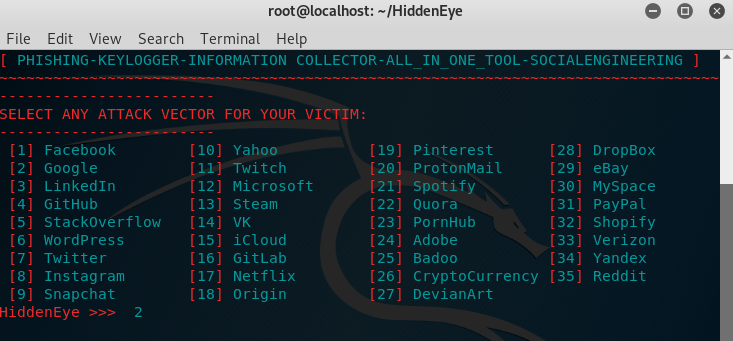




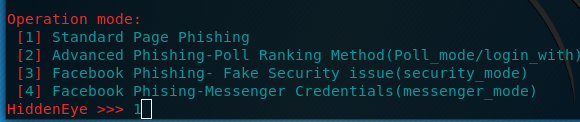
Step 4:

Choose an option for phishing

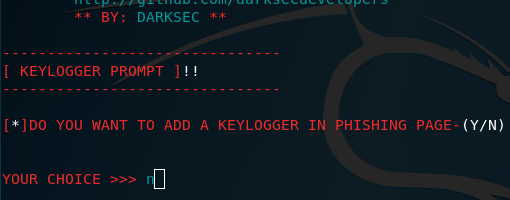
After entering the number of the site you wish to create, press enter.



Next we have to select the operation mode



Then it generate a key logger prompt. Here we have to specify the key logger.

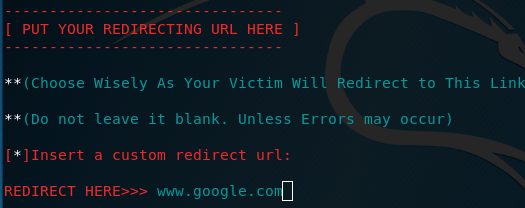


Specify Cloudfare protection option by pressing yes/no.



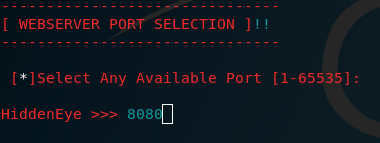
Step 5:

Enter the custom redirect url.



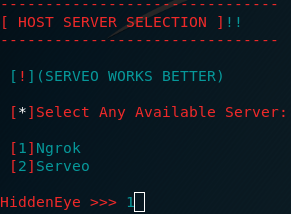
Step 6:

Select a port number.

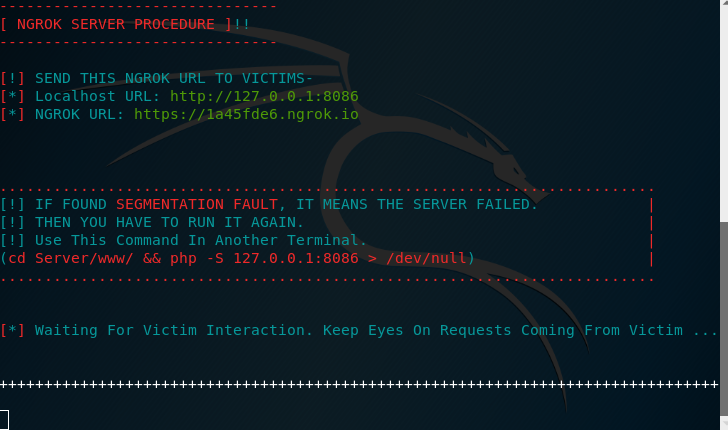


Step 7:

Select available Host Server.

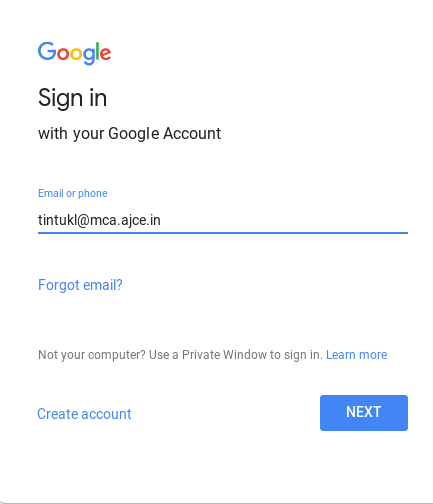


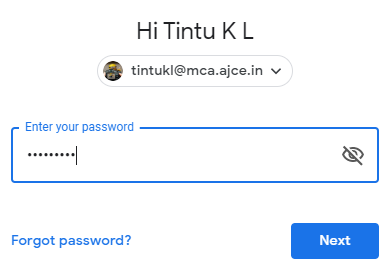
It will create a NGROK URL.



Copy this url and paste it on another browser window. When the victim clicks on the link, victim will redirect to the phishing page. If the victim enters any secret credentials on the page, the information will display on the HiddenEye terminal.

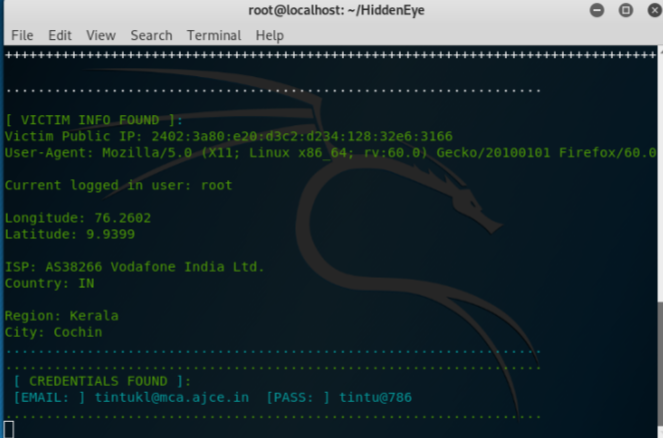
Step 8: Victim enter the login credentials.





Step 9:

Login credentials and some device information of the victim are displayed.



**4. HOW TO PREVENT PHISHING ATTACK**

Phishing attacks are one of the most common security challenges that both individuals and companies face in keeping their information secure. Whether it's getting access to passwords, credit cards, or other sensitive information, hackers are using email, social media, phone calls, and any form of communication they can to steal valuable data. Businesses, of course, are a particularly worthwhile target.

**1. Keep Informed About Phishing Techniques** – New phishing scams are being developed all the time. Without staying on top of these new phishing techniques, you could inadvertently fall prey to one. Keep your eyes peeled for news about new phishing scams. By finding out about them as early as possible, you will be at much lower risk of getting snared by one. For IT administrators, ongoing [security awareness training](https://www.knowbe4.com/?hsLang=en) and simulated phishing for all users is highly recommended in keeping security top of mind throughout the organization.   
  
**2. Think Before You Click!** – It’s fine to click on links when you’re on trusted sites. Clicking on links that appear in random emails and instant messages, however, isn’t such a smart move. Hover over links that you are unsure of before clicking on them. Do they lead where they are supposed to lead? A phishing email may claim to be from a legitimate company and when you click the link to the website, it may look exactly like the real website. The email may ask you to fill in the information but the email may not contain your name. Most phishing emails will start with “Dear Customer” so you should be alert when you come across these emails. When in doubt, go directly to the source rather than clicking a potentially dangerous link.   
  
**3. Install an Anti-Phishing Toolbar** – Most popular Internet browsers can be customized with anti-phishing toolbars. Such toolbars run quick checks on the sites that you are visiting and compare them to lists of known phishing sites. If you stumble upon a malicious site, the toolbar will alert you about it. This is just one more layer of protection against phishing scams, and it is completely free.   
  
**4. Verify a Site’s Security –**It’s natural to be a little wary about supplying sensitive financial information online. As long as you are on a secure website, however, you shouldn’t run into any trouble. Before submitting any information, make sure the site’s URL begins with “https” and there should be a closed lock icon near the address bar. Check for the site’s security certificate as well. If you get a message stating a certain website may contain malicious files, do not open the website. Never download files from suspicious emails or websites. Even search engines may show certain links which may lead users to a phishing webpage which offers low cost products. If the user makes purchases at such a website, the credit card details will be accessed by cybercriminals.   
  
**5. Check Your Online Accounts Regularly** – If you don’t visit an online account for a while, someone could be having a field day with it. Even if you don’t technically need to, check in with each of your online accounts on a regular basis. Get into the habit of changing your passwords regularly too. To prevent bank phishing and credit card phishing scams, you should personally check your statements regularly. Get monthly statements for your financial accounts and check each and every entry carefully to ensure no fraudulent transactions have been made without your knowledge.   
  
**6. Keep Your Browser Up to Date** – Security patches are released for popular browsers all the time. They are released in response to the security loopholes that phishers and other hackers inevitably discover and exploit. If you typically ignore messages about updating your browsers, stop. The minute an update is available, download and install it.   
  
**7. Use Firewalls** – High-quality firewalls act as buffers between you, your computer and outside intruders. You should use two different kinds: a desktop firewall and a network firewall. The first option is a type of software, and the second option is a type of hardware. When used together, they drastically reduce the odds of hackers and phishers infiltrating your computer or your network.   
  
**8. Be Wary of Pop-Ups** – Pop-up windows often masquerade as legitimate components of a website. All too often, though, they are phishing attempts. Many popular browsers allow you to block pop-ups; you can allow them on a case-by-case basis. If one manages to slip through the cracks, don’t click on the “cancel” button; such buttons often lead to phishing sites. Instead, click the small “x” in the upper corner of the window.   
  
**9. Never Give Out Personal Information** – As a general rule, you should never share personal or financially sensitive information over the Internet. This rule spans all the way back to the days of America Online, when users had to be warned constantly due to the success of early phishing scams. When in doubt, go visit the main website of the company in question, get their number and give them a call. Most of the phishing emails will direct you to pages where entries for financial or personal information are required. An Internet user should never make confidential entries through the links provided in the emails. Never send an email with sensitive information to anyone. Make it a habit to check the address of the website. A secure website always starts with “https”.   
  
**10. Use Antivirus Software** – There are plenty of reasons to use antivirus software. Special signatures that are included with antivirus software guard against known technology workarounds and loopholes. Just be sure to keep your software up to date. New definitions are added all the time because new scams are also being dreamed up all the time. Anti-spyware and firewall settings should be used to prevent phishing attacks and users should update the programs regularly. Firewall protection prevents access to malicious files by blocking the attacks. Antivirus software scans every file which comes through the Internet to your computer. It helps to prevent damage to your system.

You don’t have to live in fear of phishing scams. By keeping the preceding tips in mind, you should be able to enjoy a worry-free online experience.

**5.CONCLUSION**

Phishing is a growing crime and one that we must be aware of and HiddenEye is the most complete phishing tool. Although laws have been enacted, education is the best defense against phishing. Being a bit suspicious of all electronic communication and websites is recommended. Look out for the common characteristics- sense of urgency , request for verification , and grammar and spelling errors. Also , get in the habit of comparing the provided URL with an independent search for the company’s website.

**6.REFERENCES**

<https://github.com/DarkSecDevelopers/HiddenEye>

<https://youtu.be/aOJPwYQZn34?t=117>

<http://www.phishing.org/10-ways-to-avoid-phishing-scams>