**A MAJOR PROJECT REPORT ON**

# **Exploring Tools For Vulnerability Management**

Submitted to JNTUH in the partial fulfillment of the Academic Requirements for the award of the degree of

**BACHELOR OF TECHNOLOGY**

IN

**ELECTRONICS AND COMMUNICATION ENGINEERING**

**BY**

**AMBATI BHARGAV 18QM1A0406**

**UNDER THE GUIDANCE OF**

**Dr. B. Vandana**

**ASSOCIATE PROFESSOR**

****

**ELECTRONICS AND COMMUNICATION ENGINEERING**

# **KG REDDY COLLEGE OF ENGINEERING AND TECHNOLOGY**

**(Accredited by NAAC, Approved by AICTE, New Delhi, Affiliated to JNTUH, Hyderabad)**

# **Chilkur (Village), Moinabad (Mandal), R. R Dist, TS-501504**

2021-22

**DEPARTMENT OF ELECTRONICS AND COMMUNICATION ENGINEERING**

# **KG REDDY COLLEGE OF ENGINEERING AND TECHNOLOGY**

**(Accredited by NAAC, Approved by AICTE, New Delhi, Affiliated to JNTUH, Hyderabad)**

**Chilkur (Village), Moinabad (Mandal), R. R Dist, TS-501504**

****

**CERTIFICATE**

This is to certify that the Project report on “**Exploring Tools For Vulnerability Management**” is a bonafide record work carried out by **AMBATI BHARGAV (18QM1A0406),** in partial fulfillment for the requirement for the award of degree of **BACHELOR OF TECHNOLOGY** in “**ELECTRONICS AND COMMUNICATION ENGINEERING”, JNTUH,** Hyderabad during the year 2021-2022.

**Internal Guide**  **Head of the department**

Dr. D. Vandana Dr. M.N. Narsaiah

ASSOCIATE PROFESSOR ASSOCIATE PROFESSOR

**External Examiner**

i

**ACKNOWLEDGEMENT**

We wish to thank the Management, Sri. **Ln. K. Krishna Reddy, CHAIRMAN** of KG Reddy College of Engineering and Technology for providing the facilities to complete our project work.

We would also especially like to express our extreme gratitude and sincere thanks to our beloved **Director**, **Dr. Rohit Kandakatla**, KG Reddy College of Engineering and Technology, who encouraged and gave support to complete the project successfully.

At the very outset, we wish to place on record our sincere thanks and gratitude to our beloved head of the Institution, **Dr. R.S. Jahagirdar, Principal**, KG Reddy College of Engineering and Technology, who allowed us to complete this endeavor successfully.

We would like to express our sincere deep sense of gratitude and indebtedness to **Dr. M N Narsaiah, HOD**, Department of Electronics and Communication Engineering, for his significant suggestions and help in every respect to accomplish the project work. His persisting encouragement, everlasting patience and keen interest in discussions have benefited us to the extent that cannot be spanned by words. He has been the continuous source of inspiration for us throughout the work.

We would like to sincerely thank our Major **Project coordinator, Dr. B Vandana, Associate Professor** who stimulated many thoughts for this project and Staff-Members of the Department of Electronics and Communication Engineering Department for their goodwill gestures towards us.

We would especially like to express our extreme gratitude and sincere thanks to our project guide **Dr. B Vandana, Associate Professor,** Department ofElectronics and Communication Engineering for his enthusiastic and innovative guidance and support.

Last but not least we would also like to thank teaching and non-teaching staff and also all my family, friends without whose support this project work would remain unfulfilled.

| **AMBATI BHARGAV** | **18QM1A0406** |
| --- | --- |
|  |  |

ii

**ABSTRACT**

Digital security plays an important role in the world of data innovation. In today’s world, data security is arguably the most difficult task to complete. When it comes to network security, the word ”cybercrime” comes to mind first, and it’s on the rise at an alarming rate. Different governments and groups are adopting a variety of strategies to combat cybercrime. Despite considerable advancements, network security remains a major concern for some people. The difficulties that digital protection faces in the cutting-edge time are the focus of this research. It also contains the most up-to-date information on network security techniques, ethics, and patterns that are transforming the face of network security.

Keywords: *Cyber Forensics, Malicious, Tor Browser, Machine learning, Cybercrime, Cyber Security, Network Security*

iii

**Contents**

**Certificate…….……………………………………….. i**

**Acknowledgement ……………………………………. ii**

**Abstract……………………………………………….. iii**

**Page No**

**Chapter1: Introduction ………………………………………………… 01 1.0.What is ML………………………………………………… 01**

**1.1.Why Is Machine Learning Important?.............................. 01**

**1.2.Machine Learning Use Cases…………………………….. 01**

**1.3.What does Prediction mean in Machine Learning?......... 02**

**1.4.Why are Predictions Important?........................................ 02**

**1.5.Classification Model……………………………………… 02**

**1.5.1.Clustering Model……………………………………… 02**

**1.5.2.Forecast Model………………………………………… 03**

**1.5.3.Outliers Model………………………………………… 03**

**1.5.4.Time Series Model…………………………………….. 03**

**1.6.Common Predictive Algorithms…………………………. 04**

**1.6.1.Random Forest………………………………………… 04**

**1.6.2.Generalised Linear Model (GLM) for Two Values…. 06**

**1.6.3.Gradient Boosted Model (GBM).................................. 06**

**1.6.4.K-Means………………………………………………. 07**

**1.6.5. Linear Regression…………………………………….. 08**

**1.6.6.Logistic Regression…………………………………… 09**

**1.6.7.Linear Discriminant Analysis……………………….. 10**

**1.6.8.Classification and Regression Trees………………… 10**

**1.6.9.K-Nearest Neighbours……………………………….. 10**

**1.6.10.Learning Vector Quantization……………………… 11**

**1.7.What is Cyber Security………………………………….. 12**

**1.8.Types of cyber threats…………………………………….. 14**

**1.8.1.Malware……………………………………………….. 14**

**1.8.2.Virus** …………………………………………………… 14

**1.8.3.Trojans…………………………………………………. 15**

**1.8.4.Spyware………………………………………………… 15**

**1.8.5.Ransomware…………………………………………… 15**

**1.8..6.Adware……………………………………………….. 15**

**1.8.7.Botnets………………………………………………… 16**

**1.8.8.SQL injection………………………………………… 16**

**1.8.9.Phishing………………………………………………. 16**

**1.8.10.Man-in-the-middle attack………………………….. 16**

**1.8.11.Denial-of-service attack…………………………….. 17**

**1.9..Latest cyber threats……………………………………… 17**

**1.10.Dridex malware…………………………………………. 17**

**1.11.Romance scams………………………………………….. 18**

**1.12.Emotet malware…………………………………………. 18**

**1.13.Cyber safety tips - protect yourself against cyberattacks 18**

**1.14.What is Cybercrime ?........................................................ 19**

**1.15.Cyberterrorism…………………………………………… 19**

**1.16.Cyber Extortion………………………………………….. 19**

**1.17.Cyber Warfare…………………………………………… 20**

**Chapter 2: Literature survey ……………………………………………... 21**

**Chapter 3: Methodology …………………………………………………... 26**

**3.1.Detecting Malicious URLs using Machine Learning …… 26**

**3.1.1.Data Preprocessing…………………………………….. 27**

**3.1.2.Data Visualization …………………………………….. 27**

**3.2.Algorithm and Predication ………………………………. 27**

**3.2.1.** **Logistic Regression…………………………………… 27**

**3.2.2.Decision Trees ………………………………………….. 28**

**3.2.3.Random Forest…………………………………………. 29**

**Chapter 4: Design/Coding/Simulation/Experimental investigations ……. 31**

**Chapter 5: Results and discussions ………………………………………... 57 5.1.NMAP……………………………………………………….. 57**

**5.2.Harvester……………………………………………………. 58**

**5.3.Nikto………………………………………………………… 58**

**5.4.Metasploit………………………………………………….. 59**

**5.5.Red Hawk…………………………………………………… 59**

**Chapter 6: Conclusions ……………………………………………………... 61**

**References……………………………………………………….. 62**

# **List of Figure**

# 

# **Figure No Name of the Figure Page No**

# Figure 1 Random Forest working flow chart 05

# Figure 2 Gradient Boosted Model working flow chart 07

# Figure 3K-means working flow chart 08

# Figure 4 Linear Regression Variable Graph 28

# Figure 5 Decision Tree Flowchart 29

# Figure 6Random Forest 30

# Figure 7 NMAP 57

# Figure 8 Harvester 58

# Figure 9 Nikto 58

# Figure 10 Metasploit 59

# Figure 11 Red Hawk 60

# 

**Acronyms**

**S.No Abbreviation Acronym**

1.Natural Language Processing NLP

2. Computer Vision CV

3.Generalized Linear Model GLM

4.Gradient Boosted Model GBM

6.Linear Discriminant Analysis LDA

7.K-Nearest Neighbours KNN

8.Learning Vector Quantization LVQ

9.Operations security OPSEC

10.Structured Language Query SQL

11.Man in the Middle MITM

12.Denial-of-Service DoS

13.Department of Justice DoJ

14.Federal Bureau of Investigation FBI

15.Central Intelligence Agency CIA

16.Information technology IT

17.Advanced Encryption Standard's AES

18.Uniform Resource Locator URL

19.Network Mapper NMAP

20.Open Source Intelligence OSINT

21.Hypertext Preprocessor PHP

22.Internet Protocol IP

23.Domain Name System DNS

24.Content Management System CMS

25.Hypertext Transfer Protocol Secure HTTPS