IDENTIFYING NETWORKS VULNERABLE TO IP SPOOFING

A PROJECT REPORT

Submitted by

112818104024	JOTHIKA A
112818104028	KARTHIKA K S
112818104038	SREE DIVYA NARRA

In partial fulfilment for the award of the degree of

BACHELOR OF ENGINEERING

IN

COMPUTER SCIENCE AND ENGINEERING

T.J.S ENGINEERING COLLEGE

PERUVOYAL (NEAR KAVARAIPETTAI)

GUMMIDIPOONDI TALUK

THIRUVALLUR DISTRICT – 601206

Approved by AICTE and Affiliated to Anna University, Chennai

ANNA UNIVERSITY: CHENNAI 600 025

JUNE 2022

PRINCIPAL
T.J.S. ENGINEERING COLLEGE
Peruvoyal, Kavaraipettai,
Gummidipoondi Taluk,
Thiruvallur Dist - 601 206.

ANNA UNIVERSITY: CHENNAI 600 025

BONAFIDE CERTIFICATE

Certificate that this project report **"IDENTIFYING NETWORKS VULNERABLE TO IP SPOOFING"** is the bonafide work of the following students.

112818104024	JOTHIKA A
112818104028	KARTHIKA K S
112818104038	SREE DIVYA NARRA

SIGNATURE

Dr.S.Anbu,M.E.,Ph.D.,

Professor & Head of the department

Department of CSE

SIGNATURE

Mr.T.A.Vinayagam,M.Tech.,

Associate Professor & Supervisor

Department of CSE

T.J.S ENGINEERING COLLEGE

PERUVOYAL (NEAR KAVARAIPETTAI)

GUMMIDIPOONDI TALUK

THIRUVALLUR DISTRICT – 601206

Submitted for viva voce held on 22-6-22 at T.J.S Engineering College, Peruvoyal.

INTERNAL EXAMINER

EXTERNAL EXAMINER

PRINCIPAL
T.J.S. ENGINEERING COLLEGE
Peruvoyal, Kavaraipettai,
Gummidipoondi Taluk,
Thiruvallur Dist - 601 206.

ABSTRACT

This aims in refining any organization's security policy due to identification of vulnerabilities, and guarantees that the security measures taken actually gives the protection that the organization expects and requires. Administrator needs to perform vulnerability which helps them to uncover shortcomings of network security that can lead to device or information being compromised or destroyed by exploits. These outputs are typically heterogeneous which makes the further analysis a challenging task. Normal user network may give the way to unauthorized people to access as a authorized agents. Whenever, users step into online networks, without knowing them third party or any other harmful person monitoring their behaviour. Provide the protection from malicious activity, admin or authorized person also check the user networks such as IP address and email. In this project, we explore how a network can manipulate this information source the peering link where traffic ingresses a network-to more precisely locate sources of spoofed traffic. Our key observation is that the routes are partially under an origin network's control, and so the network receiving the spoofed traffic has some ability to impact on which link it receives traffic, instead of relying on routers that are not under its control. We propose techniques that are fundamentally different from existing trace back approaches and can be used today, requiring no changes to deployed equipment nor cooperation from other networks. Our techniques work best when the spoofed traffic originates from few sources, as is common in amplification DOS attacks.

PRINCIPAL
T.J.S. ENGINEERING COLLEGE
Peruvoyal, Kavaraipettai,
Gummidipoondi Taluk,
Thiruvallur Dist - 601 206.

CS8792 CRYPTOGRAPHY AND NETWORK SECURITY

OBJECTIVES:

- To understand Cryptography Theories, Algorithms and Systems.
- To understand necessary Approaches and Techniques to build protection mechanisms in order to secure computer networks.

UNIT I INTRODUCTION 9

Security trends - Legal, Ethical and Professional Aspects of Security, Need for Security atMultiple levels, Security Policies - Model of network security – Security attacks, services and mechanisms — OSI security architecture — Classical encryption techniques: substitution techniques, transposition techniques, steganography- Foundations of modern cryptography: perfect security – Information theory – product cryptosystem – cryptanalysis.

UNIT II SYMMETRIC KEY CRYPTOGRAPHY 9

MATHEMATICS OF SYMMETRIC KEY CRYPTOGRAPHY: Algebraic structures - Modular arithmetic-Euclid"s algorithm- Congruence and matrices - Groups, Rings, Fields- Finite fields- SYMMETRIC KEY CIPHERS: SDES – Block cipher Principles of DES – Strength ofDES – Differential and linear cryptanalysis - Block cipher design principles – Block cipher mode of operation – Evaluation criteria for AES – Advanced Encryption Standard - RC4 – Key distribution.

UNIT III PUBLIC KEY CRYPTOGRAPHY 9

MATHEMATICS OF ASYMMETRIC KEY CRYPTOGRAPHY: Primes – Primality Testing –Factorization – Euler's totient function, Fermat's and Euler's Theorem - Chinese Remainder Theorem — Exponentiation and logarithm - ASYMMETRIC KEY CIPHERS: RSA cryptosystem — Key distribution — Key management — Diffie Hellman key exchange - ElGamal cryptosystem – Elliptic curve arithmetic-Elliptic curve cryptography.

UNIT IV MESSAGE AUTHENTICATION AND INTEGRITY 9

Authentication requirement – Authentication function – MAC – Hash function – Security of hash function and MAC – SHA –Digital signature and authentication protocols – DSS- Entity Authentication: Biometrics, Passwords, Challenge Response protocols- Authentication applications - Kerberos, X.509

UNIT V SECURITY PRACTICE AND SYSTEM SECURITY 9

Electronic Mail security — PGP, S/MIME — IP security — Web Security - SYSTEM SECURITY: Intruders – Malicious software – viruses – Firewalls.

TOTAL 45 PERIODS

OUTCOMES:

At the end of the course, the student should be able to:

- Understand the fundamentals of networks security, security architecture, threats andvulnerabilities
- Apply the different cryptographic operations of symmetric cryptographic algorithms
- Apply the different cryptographic operations of public key cryptography
- Apply the various Authentication schemes to simulate different applications.
- Understand various Security practices and System security standards

TEXT BOOK:

1. William Stallings, Cryptography and Network Security: Principles and Practice, PHI3rd Edition, 2006.

REFERENCES:

1. C K Shyamala, N Harini and Dr. T R Padmanabhan: Cryptography and Network Security, Wiley India Pvt.Ltd