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

T.J.S. ENGINEERING COLLEGE
T.J.S.E.C.
PERUVOYAL, KAVARAIPETTAI

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

ANNA UNIVERSITY: CHENNAI 600 025

JUNE 2022

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

22/6/22

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.

J.

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