## MAJOR PROJECT G-29

## MALICIOUS WEBSITE DETECTION AND BLOCKING SYSTEM USING EBPF

The project utilizes eBPF for traffic filtering, while first performing deep packet inspection (DPI) to analyze the content. This combination allows for efficient, real-time traffic monitoring and filtering based on packet data, enhancing network security and performance by identifying and mitigating threats before applying filtering rules.

NETWORK PACKET PASSES
KERNEL INITIALLY AND GOES
THROUGH DPI

DPI TELLS EBPF WHETHER
TO BLOCK OR ALLOW
FURTHER CONNECTIONS TO
THE WEBSITE

ALLOWED TRAFFIC IS
MONITORED BASED ON USER'S
IP,APPLICATION. AMOUT OF
DATA USED IS NOTED



MALICIOUS TRAFFIC IS
BLOCKED IN KERNEL USING
EBPF, AND NEVER REACHES
USER SPACE

## **OBJECTIVES**

**Objective 1:** 

**Objective 2:** 

**Objective 3:** 

To detect websites

To log website

To block websites

based on Deep

traffic to a database. using eBPF

Packet Inspection

Made By: Amrinder Singh URN: 2104066

Made By: Ravinder Kaur

URN: 2104168

Made By: Ranbir Singh URN: 2104166