**ABSTRACT**

The primary objective of this project is to find the firewall vulnerability using Wireshark. The firewall is a critical component of network security, designed to filter the incoming and outgoing traffic based on predefined security rules. The firewall is most important in real life it is used in many companies, instates, different sector and many more. Wireshark, a powerful network protocol analyzed, is widely used to monitor and analysers network traffic, providing valuable insights into potential firewall vulnerabilities.

Firewall vulnerabilities pose significant risk to network security. If firewall is not present there will be a different option to attack like Inside attacks, DDos attacks, poorly implemented controls, Lax firewall update, Poor documentation and awareness, Inadequate inspection tools, Misconfiguration. There will be more problem if there is no firewall present. Wireshark is essential tool network administrator and security professionals. Wireshark is the tool that is used to captures and analyses network traffic in real-time, helping to identify unusual pattens and potential threads. Key features include the ability to filter traffic by IP, address, port, and protocol, as well as detect SYN packets and failed connection. Nmap is used to detect the firewall is present or not. It will send the number of packets to detect the ports of the system.

The flow of project is, first we send the packets to the firewall using the Nmap, and we will monitor the traffic of network using Wireshark. By using Wireshark. we can find the vulnerability of firewall. Wireshark is an industry network protocol analysis tool. It allows you to capture and view the data travelling back and forth on your network, providing the ability to drill down and read the content of each packet.

Wireshark provide a robust solution for identifying and addressing firewall vulnerabilities. Its comprehensive traffic analysis capabilities enable the detection of misconfigurations, outdated software, and insufficient logging practices. By regularly monitoring network traffic and applying Wireshark’s analytical tools, security professionals can mitigate potential threats and enhance the overall security posture of their network. Continuous vigilance and proactive management of firewall configurations are essential for safeguarding against cyber threats.