Nation-State Cyber Threat Simulation (Demo Preview)

**By Piyush Goyel**

*Cybersecurity Specialist | MERN Stack Developer | Offensive Security Enthusiast*

# Introduction

This document provides a preview into a comprehensive 240+ page Nation-State Threat Simulation Report. It covers the simulation of sophisticated cyberattacks against Android devices, web applications, Windows/Linux systems, and network infrastructures. The report features real-world techniques, screenshots, payload executions, and red vs blue team strategies.

# Technologies and Tools Used

- Metasploit Framework (Payloads and Exploitation)

- SQLMap (Automated SQL Injection Testing)

- John the Ripper (Password Cracking)

- Hydra (Brute Force Attack Automation)

- Bettercap (MITM Attack Toolkit)

- Wireshark (Network Traffic Analysis)

- Suricata and Wazuh (Threat Detection and SIEM)

# Attack Scenarios Simulated

• Android Remote Payload Deployment and Shell Access

• SQL Injection on E-commerce and Education Portals

• Windows/Linux Password Dumping and Cracking

• ARP Spoofing, SSL Stripping, and Session Hijacking

• Social Engineering Attacks (Phishing Campaigns)

# Defense and Monitoring Setup

- Suricata custom rules for SQLi detection

- Wazuh monitoring for unauthorized access attempts

- Kibana dashboards for real-time attack visualization

# Sample Attack Visuals

[Screenshot Placeholder] - SQL Injection database dump

[Screenshot Placeholder] - Successful Android payload session

[Screenshot Placeholder] - Wireshark ARP Spoof capture

# Explore the Full Report!

Curious to explore real payload sessions, screenshots, full attack logs, and blue team defenses?

*👉 Access the complete 240+ page Nation-State Threat Simulation Report here: [Insert GitHub/Drive Link]*