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 Reverse Shell Payload Deployment

• SQL Injection on Live Websites (Database Dumping)

• Windows/Linux Password Dumping and Cracking

• MITM Attacks (ARP Spoofing, Cookie Hijacking)

• Social Engineering Campaigns (Phishing Simulations)

# Defense and Monitoring Setup

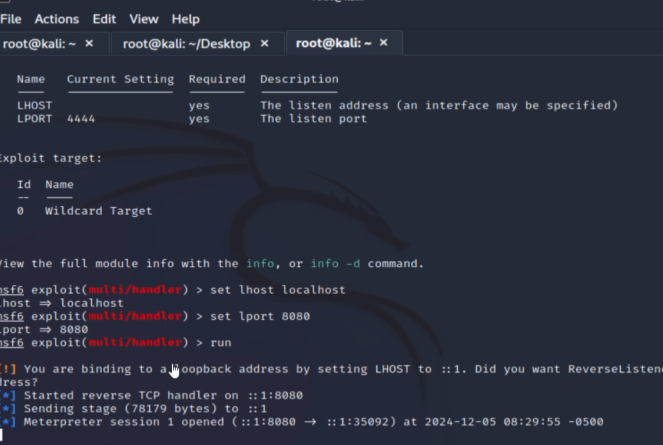
- Suricata custom IDS rules for SQL Injection detection

- Wazuh SIEM alerts for brute force and unauthorized login attempts

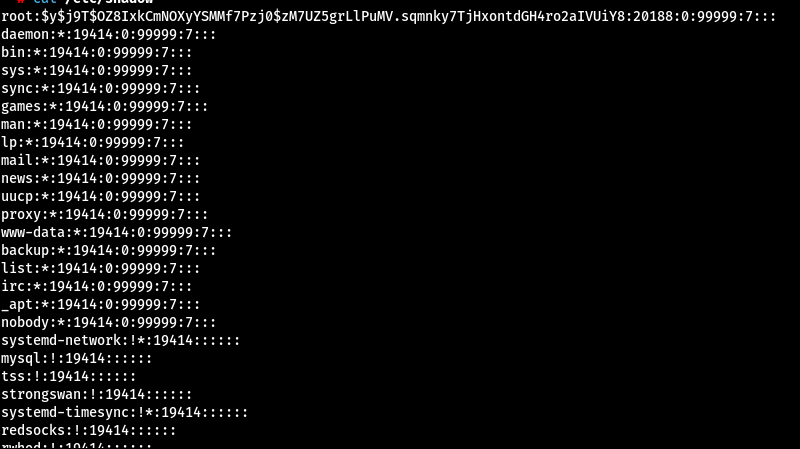
- Visualization and correlation in Kibana dashboards

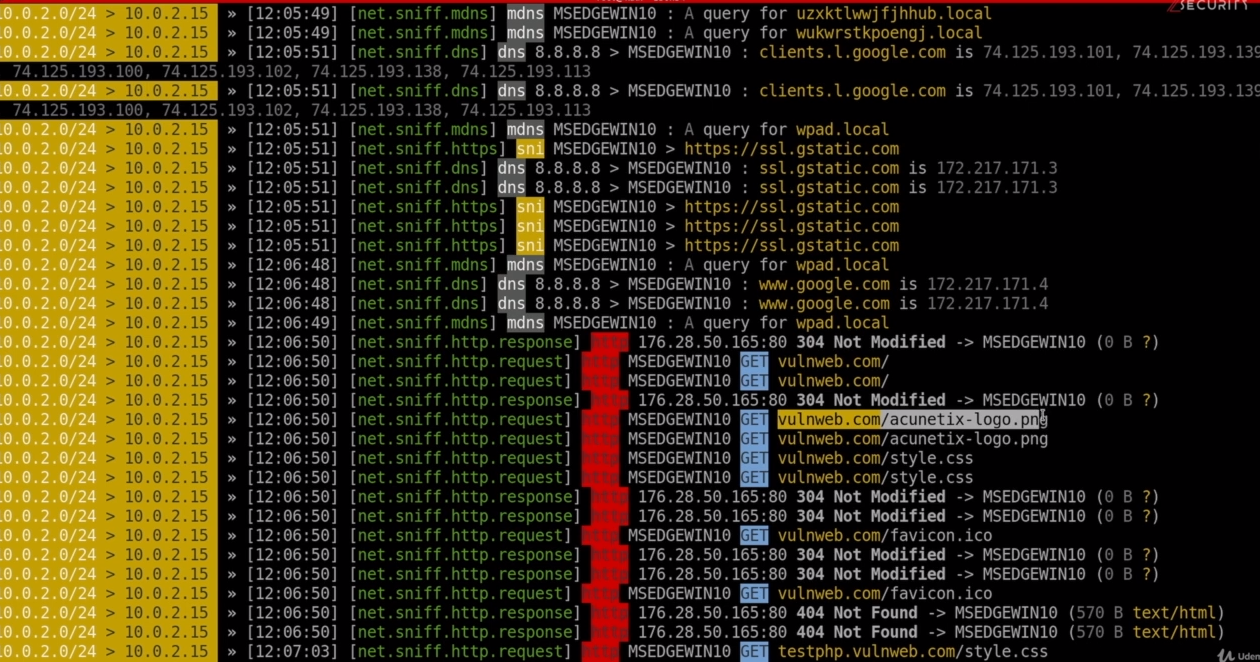
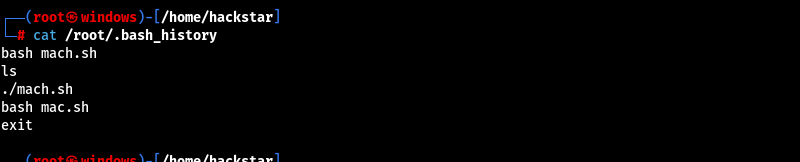
# Sample Attack Visuals

**▼ Android Payload Session Established (Meterpreter Shell)**

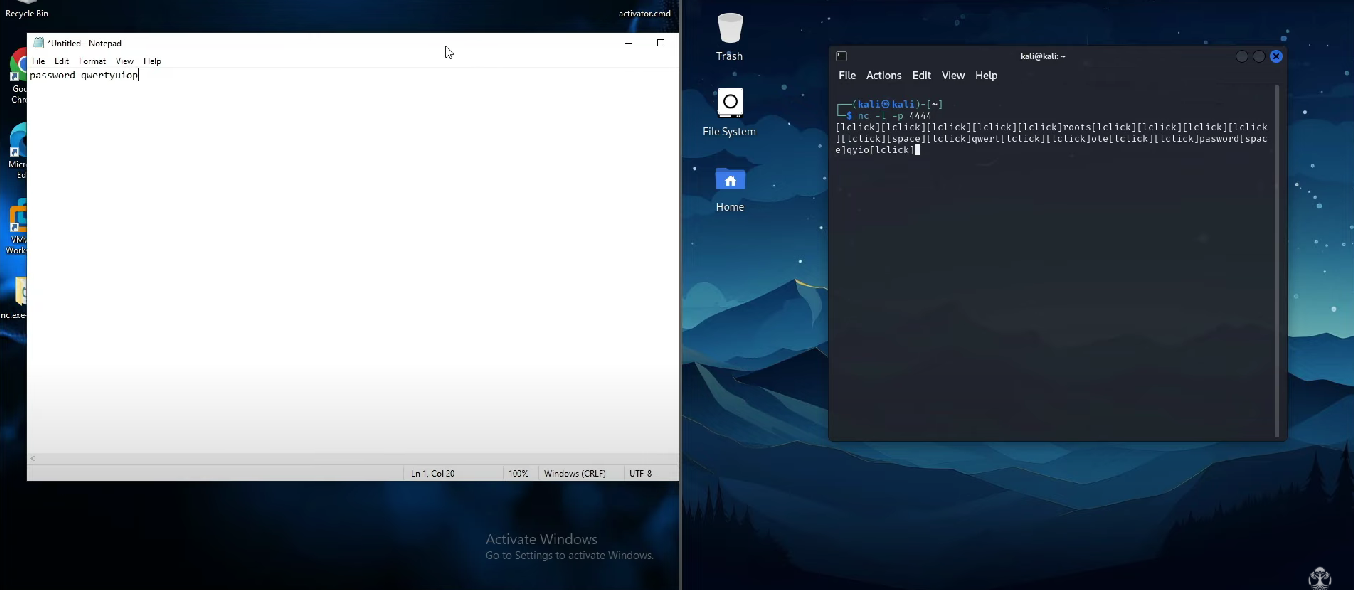


**▼ SQL Injection Attack Result - Database Dump**

**▼ MITM Attack - Wireshark Capture (ARP Spoofing)**



**▼ Windows remote keylogger**

Explore the Full Report!

Curious to explore real payload sessions, screenshots, full attack logs, red vs blue exercises, and detailed recommendations from a simulated nation-state threat actor perspective?

*👉 Access the complete 240+ page Nation-State Threat Simulation Report here:* [*nation-state-threat-simulation-report/ at main · hackcrackboy/nation-state-threat-simulation-report*](https://github.com/hackcrackboy/nation-state-threat-simulation-report/tree/main)