StarSentinel :

Space Systems Cybersecurity Toolkit

Presented By : Upasana Manoj Solanki
Soham Shrikant Ghaware

How is cybersecurity is connected to StarSentinel?

STARSentinel is designed as a cybersecurity toolkit for space systems, focusing on threats that can impact satellite operations. It targets three key areas: GNSS spoofing, SatCom vulnerabilities, and orbital spoofing —all of which are real-world cybersecurity risks.

The toolkit simulates these attacks to help researchers and students understand how software-based exploits can affect critical infrastructure in space. For example, it can detect fake GPS signals, scan for insecure satellite communication setups, and model spoofed satellites that might cause orbital collisions.

By providing hands-on tools for ethical hacking and vulnerability testing, STARSentinel bridges the gap between traditional cybersecurity and cyber-physical threats in aerospace—making it highly relevant for space-focused cybersecurity education, training, and research.

INTRODUCTION

STARSentinel is a modular, Python-based toolkit developed to simulate and detect cybersecurity threats in modern space systems.

As satellite-based infrastructure becomes essential for navigation, communication, and space traffic management, these systems face growing risks from cyber-attacks.
This toolkit was created as part of a cybersecurity internship project to address these threats through simulation and analysis in a safe, educational environment.
It focuses on three main vectors of attack:

- GNSS Spoofing – manipulating GPS data to mislead receivers
- Satellite Communication Vulnerabilities – exploiting insecure SatCom configurations
- Orbital Spoofing – faking satellite positions to simulate collisions

STARSentinel enables ethical hacking, red-teaming, and research training in space systems cybersecurity.

What is StarSentinel?

STARSentinel is a multi-vector cybersecurity toolkit designed to simulate and detect threats in satellite-based space systems.

Developed in Python, it provides a hands-on platform to study how cyber attacks could affect space infrastructure.

◆ Purpose:

To raise awareness and provide training in detecting vulnerabilities in systems like GNSS (Global Navigation Satellite Systems), satellite communication (SatCom), and orbital tracking.

◆ Key Features:

- Simulates realistic space cybersecurity threats
- Detects anomalies in satellite data
- Provides ethical, controlled environments for testing
- Modular design – each threat type is a separate module

◆ Users:

- Cybersecurity students and researchers
- Aerospace engineers
- Ethical hackers focused on critical infrastructure

STARSentinel bridges the gap between theory and real-world application in the emerging field of space cybersecurity.

CORE MODULES :

STARSentinel is divided into three specialized modules, each addressing a distinct space cybersecurity threat:

- 1. GNSS Spoofing Detector

Detects sudden jumps in location or time from GPS logs, which may indicate spoofed signals.

- 2. SatCom Security Scanner

Simulates port scans and configuration checks on mock satellite IPs to find vulnerabilities like open ports or default credentials.

- 3. Space Traffic Simulator

Loads real satellite data (TLEs), injects spoofed satellites, and flags potential collisions if two objects come dangerously close (<50 km).

Each module is designed for simulation, ethical analysis, and training, allowing independent testing and learning.

GNSS SPOOFING DETECTON

🛰️ Module Overview

This module analyzes GPS logs to identify signs of spoofed signals in Global Navigation Satellite Systems (GNSS).

🧩 Key Functions:

- Parses GPS logs in NMEA format
- Monitors signal consistency over time
- Detects sudden jumps in position or timestamp

🚨 Spoofing Detection Logic:

- If distance between points > 500m
- Or time gap > 10 seconds
- → Flagged as potential spoofing

✅ Purpose:

To help researchers and trainees identify malicious GPS signal manipulation in a controlled, ethical test environment.

GNSS SPOOFING: How it works?

This module reads a GPS log file and checks if the movement data is realistic. It works in three simple steps:
Reads GPS data from a file in NMEA format using a GPS-parsing library called pynmea2.
Calculates distance between each GPS point using a math formula (Haversine) to check how far the object moved.

Checks for jumps:
If the distance jumped is more than 500 meters or the time gap is more than 10 seconds, it assumes the signal might be fake and flags it as spoofing.
At the end, the tool shows when and where the spoofing might have happened. It helps detect suspicious or manipulated GPS signals.

OUTPUT

127.0.0.1:5000/run

STARSentinel Toolkit

Run GNSS Detector | Run SatCom Scanner | Run Space Traffic Simulator

Output:

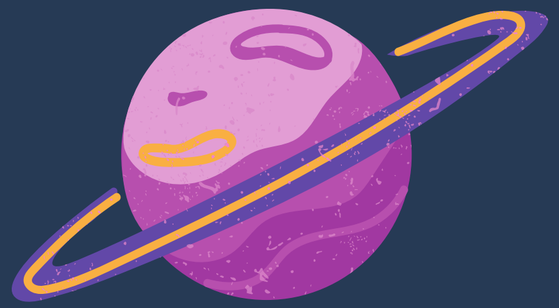
```
GNSS Spoofing Detector Started
Parsed: $GPRMC,120000,A,3751.65,N,12218.45,W,000.0,360.0,280425,015.5,E*60
Parsed: $GPRMC,120005,A,3751.66,N,12218.46,W,000.0,360.0,280425,015.5,E*65
Parsed: $GPRMC,120010,A,3751.67,N,12218.47,W,000.0,360.0,280425,015.5,E*61
Parsed: $GPRMC,120015,A,3751.68,N,12218.48,W,000.0,360.0,280425,015.5,E*64
Parsed: $GPRMC,120020,A,3751.69,N,12218.49,W,000.0,360.0,280425,015.5,E*62
Parsed: $GPRMC,120025,A,3751.70,N,12218.50,W,000.0,360.0,280425,015.5,E*67
Parsed: $GPRMC,120030,A,3751.71,N,12218.51,W,000.0,360.0,280425,015.5,E*63
Parsed: $GPRMC,120035,A,3745.00,N,12210.00,W,000.0,360.0,280425,015.5,E*69
Parsed: $GPRMC,120040,A,3745.01,N,12210.01,W,000.0,360.0,280425,015.5,E*6B
Parsed: $GPRMC,120045,A,3745.02,N,12210.02,W,000.0,360.0,280425,015.5,E*6E

Potential spoofing detected at 1 point(s):
[2025-04-28 12:00:35+00:00] Distance jump: 17604.10 m | Time gap: 5.00s | Location: (37.75, -122.16666666666667)
```

Stellite Communication Security Scanner (SatCom)

The SatCom Security Scanner is a module of the STARSentinel toolkit designed to detect vulnerabilities in satellite communication systems. It simulates how attackers might scan and exploit SatCom devices and infrastructure. The module checks for insecure settings, such as open ports and default credentials, and verifies the integrity of satellite orbital data using TLE (Two-Line Element) records.

Purpose:

- Simulate network scans on satellite-linked IPs and services
- Identify weak authentication and misconfigurations
- Detect anomalies or tampering in TLE orbital data



SatCom Security Scanner
How It Works?

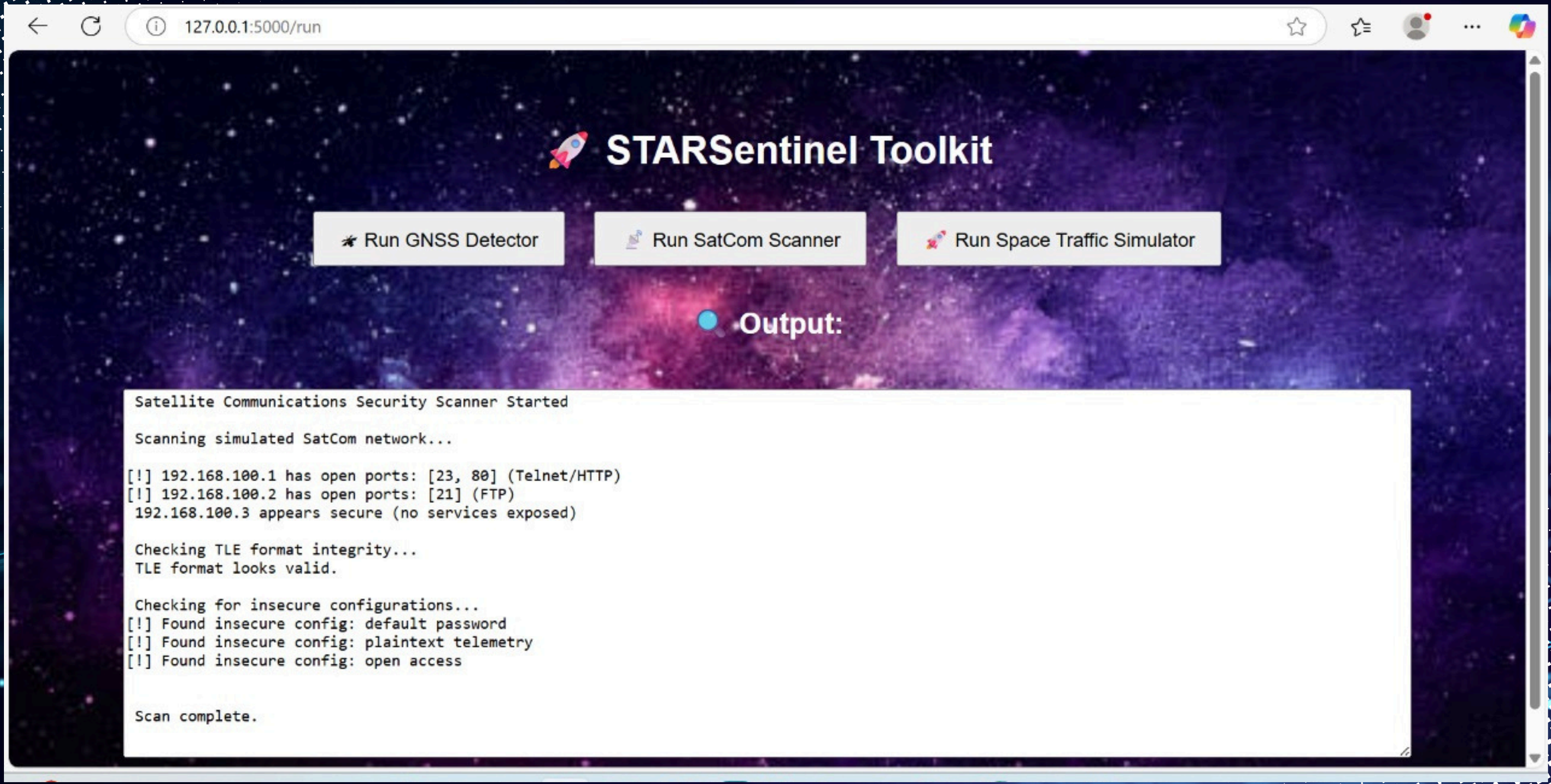
The SatCom Scanner works by simulating real-world cybersecurity techniques to identify satellite communication
vulnerabilities.

Step-by-Step Functionality:

1. Uses python-nmap to scan a list of mock satellite IP addresses.
2. Detects open ports and exposed services that could be exploited.
3. Simulates checks for common issues such as:
    - Default login credentials
    - Unsecured or outdated protocols
    - Public-facing admin panels
4. Verifies TLE (Two-Line Element) data for authenticity and unexpected changes.
5. Flags each issue based on severity (e.g., critical, warning, low risk).

This module demonstrates how attackers could gain unauthorized access to SatCom devices or interfere with satellite operations.

OUTPUT


127.0.0.1:5000/run
STARSentinel Toolkit
Run GNSS Detector
Run SatCom Scanner
Run Space Traffic Simulator
Output:
Satellite Communications Security Scanner Started
Scanning simulated SatCom network...
[!] 192.168.100.1 has open ports: [23, 80] (Telnet/HTTP)
[!] 192.168.100.2 has open ports: [21] (FTP)
192.168.100.3 appears secure (no services exposed)
Checking TLE format integrity...
TLE format looks valid.
Checking for insecure configurations...
[!] Found insecure config: default password
[!] Found insecure config: plaintext telemetry
[!] Found insecure config: open access
Scan complete.

Space Traffic Control Threat Simulator

💡 What is it?

This tool is a small computer program that checks space for fake or spoofed satellites. These fake satellites can pretend to be real ones and might try to hide nearby to cause trouble or avoid being seen.

🎯 Goal:

To detect and warn when a suspicious or fake satellite is flying too close to a real one—especially satellites like the International Space Station (ISS).

🌍 Real-World Example Used:

- We use the real orbit path of the ISS from real satellite tracking data.
- Then we create a spoofed satellite that flies very close to it—almost the same path, just slightly shifted.

🚨 Why It Matters:

- If two satellites are too close, they could crash or interfere with each other.
- In the future, space agencies could use this kind of tool to catch fake or dangerous objects in orbit.

Space Traffic Threat Simulator

How it works?

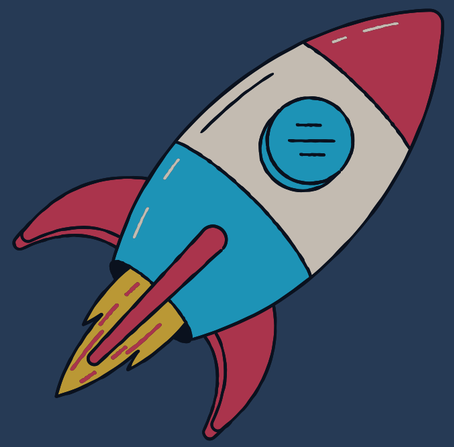
1 Get Satellite Data
- We use TLEs (Two-Line Element sets) to know where satellites are.
- One TLE is from the real ISS, and the other is a fake satellite we made to look similar.

2 Find Their Locations in Space
- We use a space math tool called Skyfield to calculate where each satellite is right now.
- It gives us their X, Y, and Z positions in space (in kilometers).

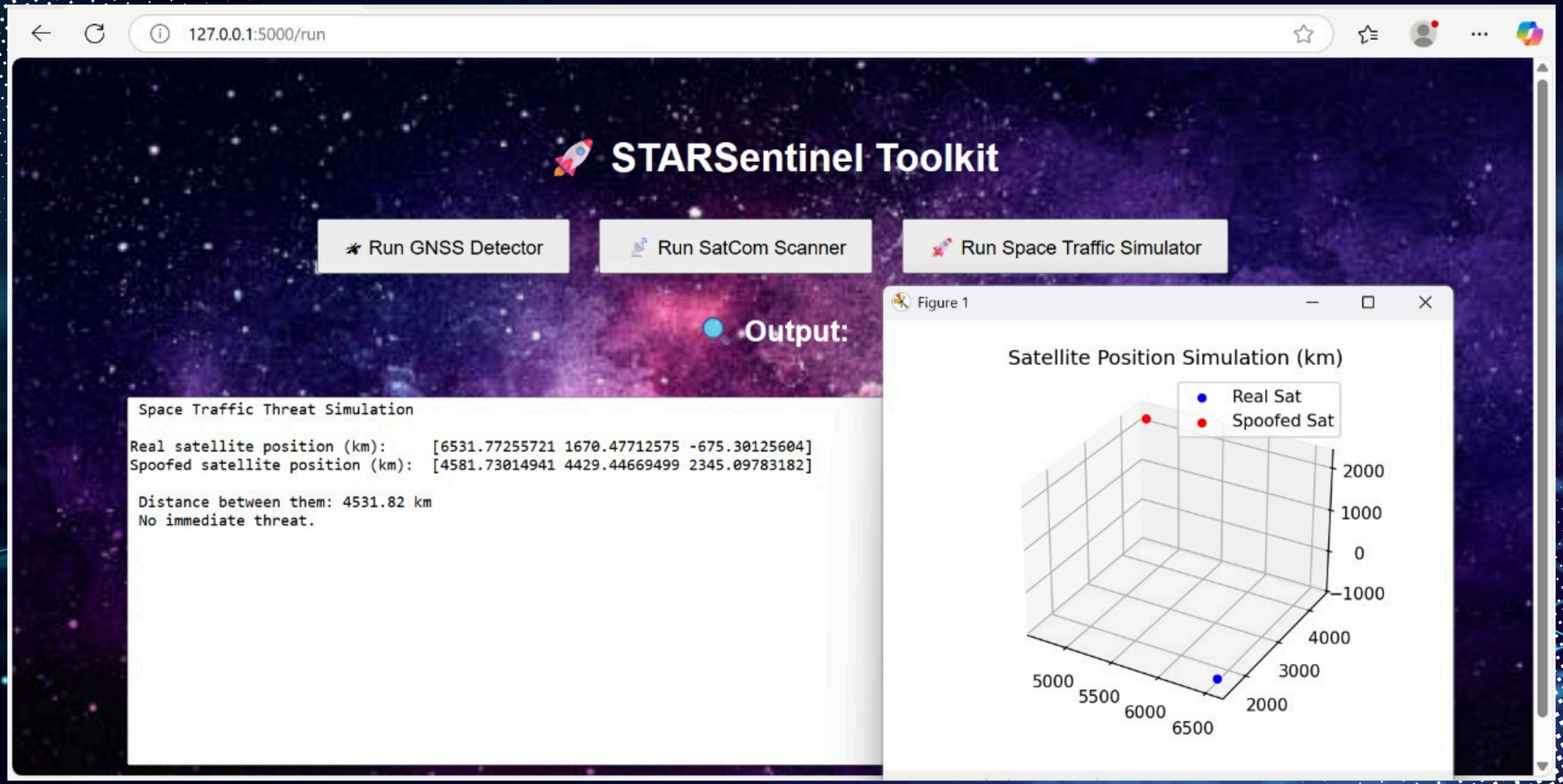
3 Check How Close They Are
- We calculate the distance between the real satellite and the spoofed one using simple 3D math.
- If they are closer than 50 km, that's risky!

4 Detect a Threat
- If the fake satellite is too close, the program shows a ⚠ warning:
- "Potential collision risk! Malicious spoof detected."

5 Show the Situation in 3D
- A 3D plot shows both satellites:
  - Blue Dot = Real ISS
  - Red Dot = Spoofed Satellite
- Helps you see how close they really are.



OUTPUT


127.0.0.1:5000/run
STARSentinel Toolkit
Run GNSS Detector
Run SatCom Scanner
Run Space Traffic Simulator
Output:
Space Traffic Threat Simulation
Real satellite position (km): [6531.77255721 1670.47712575 -675.30125604]
Spoofed satellite position (km): [4581.73014941 4429.44669499 2345.09783182]
Distance between them: 4531.82 km
No immediate threat.
Figure 1
Satellite Position Simulation (km)
Real Sat
Spoofed Sat
2000
1000
0
−1000
4000
3000
2000
5000
5500
6000
6500

Future Trends:

🔄 What Can Be Added Next

1. Live GPS Spoof Detection
2. → Use real-time radio signals (SDR) to catch spoofing as it happens.
3. Connect to Real Satellite Data
4. → Use public APIs to track real SatCom activity and spot problems.
5. Visual Dashboard (Web-based)
6. → Create a website that shows all data and warnings in charts and graphs.
7. AI and Machine Learning
8. → Train the system to detect spoofed or suspicious satellite movements using patterns and data.
9. Educational Game Mode
10. → Let students play as hackers or defenders to learn about space cybersecurity in a fun way.

🌟 Why This Matters

- Satellite threats are growing fast.
- This project can evolve into a powerful tool for training, research, and national security.
- Future upgrades can make it smarter, faster, and more interactive.

Thank You!