

Subnet Deception Tool: A Testbed for Understanding Adversarial Decision-Making in Realistic Cyber Deception Scenarios

Application Number: 202211005795

Inventors: Dr. Varun Dutt, Ms. Maghna Sharma

ABSTRACT

SUBNET DECEPTION TOOL: A TESTBED FOR UNDERSTANDING ADVERSARIAL DECISION-MAKING IN REALISTIC CYBER DECEPTION SCENARIOS discloses a cyber security system for understanding adversarial decision making in the presence of subnetworks on a computer in realistic cyber deception scenarios wherein said tool (100) comprises of: network nodes, to depict the characteristics of real web servers; strategies 10 configured (110) to induce deception (120); and commands configured to interact with the network and a method of subnet deception wherein said process (200) has a probe phase (130) followed by an attack phase (140) wherein the probe phase involves scanning of web servers in the network for loopholes, and the attack phase involves attaining access to systems and obtaining information present in those systems.

KEY APPLICATION AREAS

1. Cybersecurity & Cyber Defense.
2. Cyber Deception & Honeypot Systems.
3. Network Security Testing.
4. Cybersecurity Training & Simulation.
5. Threat Intelligence & Adversarial Behavior Analysis.
6. Security Research & Cyber Range Platforms.

POTENTIAL USE

1. Simulating realistic cyberattack scenarios to study attacker decision-making.
2. Testing deception strategies using honeypots, fake files, and subnet configurations.
3. Cybersecurity training for ethical hackers, analysts, and students in controlled environments.
4. Evaluating network security against modern cyber vulnerabilities and attack techniques.
5. Analyzing attacker behavior and cognitive biases to improve cyber defense strategies.
6. Developing adaptive and resilient security solutions for enterprise and critical infrastructure networks.
7. Cyber range and research platform for testing security tools, policies, and defense mechanisms.