UNIVERSITAS
GADJAH MADA
IMPLEMENTASI HONEYPOT PADA SISTEM SCADA DENGAN MENGUMPULKAN DATA KARAKTERISTIK SERANGAN SIBER DDOS
Angga Rustico Hadiyanto, Drs. Bambang Nurcahyo Prastowo, M.Sc.
Universitas Gadjah Mada, 2025 | Diunduh dari http://etd.repository.ugm.ac.id/

INTISARI

IMPLEMENTASI *HONEYPOT* PADA SISTEM SCADA DENGAN MENGUMPULKAN DATA KARAKTERISTIK SERANGAN SIBER DDOS

Oleh
Angga Rustico Hadiyanto
21/477976/PA/20721

Dalam era digitalisasi industri yang berkembang pesat, sistem *Supervisory Control and Data Acquisition* (SCADA) semakin rentan terhadap ancaman serangan siber. Penelitian ini mengimplementasikan *honeypot* guna mengamankan sistem (SCADA) dengan cara mempelajari karakteristik serangan siber *Distributed Denial of Server* (DDoS) dan ancaman lainnya terhadap keamanan jaringan SCADA agar dapat mempersiapkan strategi pengamanan yang sesuai. Penelitian ini difokuskan pada simulasi layanan-layanan yang dijalankan oleh sistem SCADA pada umumnya. *Honeypot* yang digunakan adalah Dionaea, yang dikonfigurasi untuk mendeteksi dan mengumpulkan data aktivitas serangan yang ditargetkan pada sistem SCADA. Dalam penelitian ini, perangkat SCADA penelitian terdiri dari Raspberry Pi sebagai *web server Human Machine Interface* (HMI), ESP32 sebagai *Remote Terminal Unit* (RTU), dan sensor DHT22. Penelitian mencakup konfigurasi *honeypot* agar dapat menyimulasikan layanan SCADA dan memungkinkan penyerang untuk mengaksesnya, sehingga karakteristik serangan dapat dikumpulkan. Sistem penelitian diuji dengan uji coba pemetaan jaringan dengan Nmap serta simulasi serangan DDoS dengan Slowloris untuk mengevaluasi efektivitas *honeypot* dalam mengumpulkan karakteristik serangan siber. Hasil penelitian menunjukkan bahwa implementasi *honeypot* dalam sistem SCADA berhasil mengumpulkan data karakteristik serangan siber sebanyak 156 koneksi tidak sah dari 7 perangkat yang berbeda selama 24 jam saat dijalankan pada jaringan Fakultas Matematika dan Ilmu Pengetahuan Alam, Universitas Gadjah Mada. Implementasi *honeypot* juga berhasil mendeteksi adanya pemetaan jaringan *aggressive* dengan Nmap dengan mengumpulkan 140 koneksi tidak sah dari 1 perangkat. Selain itu, implementasi *honeypot* juga berhasil mendeteksi serangan siber DDoS dengan Slowloris dengan mengumpulkan sebanyak 1500 koneksi HTTP tidak sah dari 1 perangkat dalam waktu 5 menit.

Kata Kunci: *honeypot*, SCADA, Dionaea, Keamanan Siber, HTTP, Karakteristik Serangan Siber, *Distributed Denial of Service*

UNIVERSITAS
GADJAH MADA
IMPLEMENTASI HONEYPOT PADA SISTEM SCADA DENGAN MENGUMPULKAN DATA KARAKTERISTIK SERANGAN SIBER DDOS
Angga Rustico Hadiyanto, Drs. Bambang Nurcahyo Prastowo, M.Sc.
Universitas Gadjah Mada, 2025 | Diunduh dari http://etd.repository.ugm.ac.id/

ABSTRACT

IMPLEMENTATION OF HONEYPOT ON SCADA SYSTEMS FOR COLLECTING CYBERATTACK CHARACTERISTICS OF DDOS

By
Angga Rustico Hadiyanto
21/477976/PA/20721

In today's era of rapid industrial digitalization, Supervisory Control and Data Acquisition (SCADA) systems face an increasing risk of cyberattacks. This research focuses on implementing a honeypot to enhance SCADA system security by analyzing the characteristics of Distributed Denial of Service (DDoS) attacks and other potential threats. The goal is to develop effective strategies for safeguarding SCADA networks. The study involves simulating typical SCADA system services using Dionaea, a honeypot configured to detect and gather data on cyberattack activities targeting SCADA systems. The experimental setup includes a Raspberry Pi serving as a web server for the Human-Machine Interface (HMI), an ESP32 as the Remote Terminal Unit (RTU), and a DHT22 sensor. By configuring the honeypot to mimic SCADA services, it creates an environment for attackers to interact with, allowing the capture of attack data. The system was tested using network mapping tools like Nmap and a DDoS attack simulation with Slowloris to evaluate the honeypot's effectiveness in gathering attack characteristics. The results demonstrated the honeypot's success in capturing data on cyberattacks, logging 156 unauthorized connections from seven different devices within 24 hours when deployed in the Faculty of Mathematics and Natural Sciences network at Universitas Gadjah Mada. It effectively detected aggressive network mapping with Nmap, identifying 140 unauthorized connections from a single device. Additionally, during a simulated Slowloris DDoS attack, the honeypot captured 1,500 unauthorized HTTP connections from one device in just five minutes.

Keywords: honeypot, SCADA, Dionaea, cybersecurity, HTTP, cyber-attack characteristics, Distributed Denial of Service