

## ABSTRAK

*Supervisory Control and Data Acquisition (SCADA)* merupakan sistem kontrol unit yang telah digunakan hampir diberbagai industri di seluruh dunia dalam hal proses otomatisasi. Sistem ini menggambarkan infrastruktur secara nyata dan memberikan kemudahan dalam operasional dan monitoring, namun sistem ini memiliki kerentanan dalam aspek keamanan komunikasi data yang terhubung antara perangkat pendukung SCADA. Hal ini dapat berdampak besar terhadap industri dan ekonomi. Penelitian ini dilakukan dengan merancang dan membangun infrastruktur SCADA dan melakukan analisis terhadap kerentanan dan ancaman terhadap keamanan jaringan SCADA. Penelitian ini melakukan penetrasi testing terhadap jaringan SCADA menggunakan *Kali Linux* dan analisis lalu lintas data pada jaringan SCADA menggunakan *Wireshark*. Dari hasil analisis *Wireshark* didapatkan penyerang dengan User Anonymous. Analisis yang dilakukan dengan kondisi lalu lintas data normal dan tidak normal. Hasil dari penelitian ini merupakan penetrasi pada jaringan SCADA menggunakan *Kali Linux* yang digunakan untuk menyerang dan membuat lalu lintas data antara *Programable Logic Controler (PLC)* dengan *Human Machinery Interface (HMI)* menjadi padat dan hasil dari penetrasi *testing* sistem SCADA menjadi *down* akibat dari *traffic* data pada jaringan menjadi padat, dengan demikian menunjukkan bahwa jaringan SCADA rentan terhadap ancaman *malware* dan berbagai serangan. Hasil dari penelitian ini merupakan rekomendasi dan strategi keamanan jaringan SCADA *system*.

*Kata kunci: Keamanan SCADA, Kali Linux, Wireshark*

UNIVERSITAS  
MERCU BUANA

## ABSTRACT

Supervisory Control and Data Acquisition (SCADA) is a unit control system that has been used almost in various industries around the world in terms of process automation. This system delineates the real infrastructure and provides ease in operations and monitoring, but this system has a vulnerability in the security aspects of data communications connected between SCADA support devices. This can have a major impact on industry and the economy. This research was conducted by designing and building SCADA infrastructure and analyzing vulnerabilities against SCADA network security. This research penetrates SCADA network using *Kali Linux* and data traffic analysis on SCADA network using Wireshark. From the results of Wireshark analysis got the attacker with User Anonymous. Analysis performed with normal and abnormal data traffic conditions. The result of this research is penetration of SCADA network using *Kali Linux*, which is used to attack and make data traffic between Programable Logic Controler (PLC) with Human Machine Interface (HMI) becomes solid, and result from penetration testing, SCADA system become down due of data traffic on dense networks, thereby indicating that SCADA networks are vulnerable to malware threats and attacks, the results of which are recomendations and network security strategies of SCADA systems.

*Keywords: Security SCADA, Kali Linux, Wireshark.*

UNIVERSITAS  
MERCU BUANA