INTISARI

PROYEK AKHIR

KLASIFIKASI DAN ANALISIS DATA SERANGAN PADA PROTOKOL *SAMBA* BERBASIS *HONEYPOT DIONAEA*

Abstrak — Protokol *Samba* atau protokol SMB (*Server Message Block*) merupakan sebuah protokol *file sharing* yang memungkinkan aplikasi pada komputer untuk dapat membaca, menulis, dan berbagi *file* dalam suatu jaringan. Beberapa versi protokol *Samba* dari 3.6.3 ke bawah memiliki masalah keamanan berupa eksploitasi kesalahan dalam prosedur *remote Samba*. Dari masalah keamanan inilah dilakukan klasifikasi dan analisis data lebih lanjut untuk menentukan jenis serangan yang terjadi pada protokol *Samba*. Klasifikasi data merupakan proses pengelompokan data sesuai yang dibutuhkan dan memenuhi syarat kebutuhan informasi berdasarkan data yang ada. Data yang akan diklasifikasi dalam penelitian proyek akhir ini didapatkan dari data serangan yang dikumpulkan oleh *Honeypot Dionaea* ke dalam *server* basis data *MongoDB* pada 10.33.109.102:27217 yang kemudian akan diklasifikasi dan dianalisis untuk setiap data yang relevan, yaitu data protokol *Samba* pada *port* 445. Metode klasifikasi yang digunakan yaitu *rule-based classifier* yang menghasilkan 2 klasifikasi berdasarkan data *offer_url* dan teknik dari *Phishing Style Attack* yaitu *Link Manipulation* dan *Session Hijacking*. Pada penelitian proyek akhir ini penulis menggunakan bahasa pemrograman *JavaScript* pada *framework Node.js* dan *library React* dalam pembangunan sistem informasi yang akan menampilkan hasil klasifikasi data serangan pada protokol *Samba*, *file* yang diinginkan oleh penyerang dari *server*, dan membuat statistika serangan. Serta untuk pengambilan data dari *server* basis data *MongoDB* ke *backend* sistem informasi memanfaatkan *API* dari *GraphQL*.

Kata Kunci : *Samba*, Klasifikasi Data, *Phishing Styel Attack*, *React*, *GraphQL*

ABSTRACT

Classification and Analysis of Attack Data on Samba Protocol Honeypot Dionaea based

Abstract — The Samba protocol or SMB protocol (Server Message Block) is a file sharing protocol that allows applications on computers to read, write, and share files on a network. Some versions of the Samba protocol from 3.6.3 and below have security issues in the form of exploiting errors in Samba remote procedures. From this security problem, further data classification and analysis were carried out to determine the types of attacks that occurred on the Samba protocol. Data classification is the process of grouping data as needed and meets the requirements for information needs based on existing data. The data that will be classified in this final project research is obtained from attack data collected by Honeypot Dionaea into the MongoDB database server at 10.33.109.102:27217 which will then be classified and analyzed for any relevant data, namely data on the Samba protocol on port 445. The classification method used is a rule-based classifier which produces 2 classifications based on offer_url data and techniques from Phishing Style Attack, namely Link Manipulation and Session Hijacking. In this final project the author uses the JavaScript programming language in the Node.js framework and the React library in the construction of an information system that will display the results of the classification of attack data on the Samba protocol, the files the attacker wants from the server, and create attack statistics. As well as for retrieving data from the MongoDB database server to the backend of the information system using the API from GraphQL.

Keywords : Samba, Data Classification, Phishing Style Attack, React, GraphQL