ANALISIS SERANGAN EVIL TWIN MENGGUNAKAN WI-FI PUMPKIN PADA GEDUNG UNIVERSITAS JENDERAL ACHMAD YANI YOGYAKARTA UNIT 1

Bambang Sadewo, Dedy Hariyadi, Adkhan Sholeh

INTISARI

Dalam berbagi data melalui jaringan nirkabel masih terdapat kerentanan dalam mengakses jaringan yang diakses secara ilegal oleh peretas. Dalam hal ini masih kurangnya tingkat kesadaran Mahasiswa Universitas Jenderal Achmad Yani Yogyakarta tentang ancaman/serangan pada jaringan nirkabel, sehingga mereka tanpa sadar terhubung ke jaringan nirkabel yang berbahaya, seperti *Access Point palsu*. Contoh serangan jaringan nirkabel adalah serangan *Evil Twin*. Serangan ini bersifat *active attack* seperti *Denial of Service, Hijacking* atau *passive attack* melalui *Rogue Access Point*. Serangan yang menggunakan teknik MITM (*Man In The Middle*) berpotensi mencuri atau memodifikasi informasi pengguna.

Penelitian ini bertujuan untuk mengetahui perangkat yang terdampak serangan *Evil Twin* yang dilancarkan pada area gedung Universitas Jenderal Achmad Yani Yogyakarta unit 1, dengan menggunakan metode *ETSniffer*. Metode *ETSniffer* yaitu tahapan yang terdiri dari ITA (ITA adalah interval waktu antara dua paket data TCP yang berurutan yang tiba disisi pengguna), kemudian melakukan koneksi ke perangkat komputer untuk menyambungkan *Access Point ITA* dan server ITA. Dalam penelitian ini akan melakukan modifikasi dari metode penelitian sebelumnya dengan melakukan analisis serangan *Evil Twin*.

Hasil penelitian menunjukkan bahwa penelitian yang dilakukan selama 8 hari yaitu pada tanggal 15 Juni sampai dengan 22 Juni 2023 menunjukan hasil jumlah perangkat yang terhubung ke *Access Point* palsu dan *Captive Portal Login*, berjumlah 101 perangkat yang terhubung ke *Access Point* palsu dan 1721 perangkat yang masuk dan keluar dari *Access Point* palsu, 63 perangkat yang *login* ke *Captive Portal Login* dan 706 yang masuk dan keluar *Captive Portal Login*. Jadi serangan Evil Twin pada Gedung Universitas Jenderal Achmad Yani Yogakarta Unit 1 dapat di simpulkan masih banyak pengguna yang masih belum sadar bahwa perangkatnya terhubung ke access point palsu dan wifi pumpkin 3 dapat melakukan serangan *MITM*.

Kata-kunci*: Evil Twin, Access Point, MITM, ETSniffer, Captive Portal Login.*

ANALISIS SERANGAN EVIL TWIN MENGGUNAKAN WI-FI PUMPKIN PADA GEDUNG UNIVERSITAS JENDERAL ACHMAD YANI YOGYAKARTA UNIT 1

Bambang Sadewo, Dedy Hariyadi, Adkhan Sholeh

ABSTRACT

Sharing data over wireless networks still has vulnerabilities that can be accessed illegally by hackers. In this regard, there is a lack of awareness among students at Universitas Jenderal Achmad Yani Yogyakarta about threats/attacks on wireless networks, leading them to unknowingly connect to dangerous wireless networks, such as fake Access Points. An example of a wireless network attack is the Evil Twin attack. This attack can be an active attack, such as Denial of Service or Hijacking, or a passive attack through a Rogue Access Point. Attacks that use the Man In The Middle (MITM) technique have the potential to steal or modify user information.

This research aims to determine the devices affected by Evil Twin attacks launched in the area of Unit 1 building, Universitas Jenderal Achmad Yani Yogyakarta, using the ETSniffer method. The ETSniffer method consists of several stages, including ITA (Inter-packet Time Analysis, which refers to the time interval between two consecutive TCP data packets arriving at the user's side). Additionally, the method involves establishing connections to the computer devices to link the ITA Access Point and ITA server. This study will modify the previous research method to conduct an analysis of Evil Twin attacks. The focus will be on understanding the impact of these attacks on various devices in the specified area of the university.

The research results show that during the 8-day study period from June 15 to June 22, 2023, there were 101 devices connected to the Evil Twin Access Point and Captive Portal Login. Out of these, 1721 devices entered and left the Evil Twin Access Point, and 63 devices logged into the Captive Portal Login, with 706 devices entering and leaving the Captive Portal Login. Therefore, it can be concluded that the Evil Twin attack on Unit 1 building, Universitas Jenderal Achmad Yani Yogyakarta, indicates that many users are still unaware that their devices are connected to a fake access point and that Wi-Fi Pumpkin 3 is capable of conducting Man-In-The-Middle (MITM) attacks.

***Keywords**: Evil Twin, Access Point, MITM, ETSniffer, Captive Portal Login.*