INTISARI

Pada tanggal 23 Maret hingga 30 April 2021, tim *Capstone Project* melakukan uji penetrasi pada sistem jaringan nirkabel berupa *hotspot* atau *access point* UGM-Secure di Laboratorium Sistem Digital yang berlokasi di Departemen Teknik Elektro dan Teknologi Informasi Fakultas Teknik Universitas Gadjah Mada (DTETI FT UGM) dengan tujuan untuk menemukan kelemahan pada sistem tersebut. Tahapan-tahapan yang dilakukan selama proses uji penetrasi yaitu eksplorasi sistem dan arsitektur jaringan UGM-Secure, analisis kelemahan sistem untuk dilakukan eksploitasi, eksploitasi sistem, serta pelaporan, di mana penguji mendokumentasikan seluruh proses uji penetrasi sekaligus mitigasi yang perlu dilakukan dalam laporan asesmen. Metode uji penetrasi yang akan diujicobakan menggunakan metode *evil twin* sekaligus beberapa metode lainnya yang dapat mendukung serangan metode *evil twin*, yaitu *packet sniffing* dan *pairwise master key identifier* (PMKID). Hasil laporan tersebut disampaikan dalam laporan asesmen dengan kaidah dan tata cara yang ditetapkan oleh *National Institute of Standards and Technology* (NIST). Hasil dari penelitian tersebut menunjukkan bahwa *access point* UGM-Secure memiliki celah keamanan berupa kredensial yang tidak dienkripsi sehingga kredensial tersebut dapat diketahui oleh penyerang sewaktu-waktu terjadi peretasan. Oleh karena itu, pihak pengelola UGM-Secure perlu melakukan pembaharuan pada sistem yang mendukung enkripsi pada autentikasi untuk mengurangi kemungkinan penyerang mendapatkan informasi terbuka untuk menyerang *access point* dengan metode yang serupa.

ABSTRACT

From March 23 to April 30, 2021, the Capstone Project team conducted a penetration test on a wireless network system in the form of a hotspot or UGM-Secure access point at the Digital Systems Laboratory located at the Department of Electrical Engineering and Information Technology, Faculty of Engineering, Universitas Gadjah Mada (DTETI FT UGM). with the aim of finding weaknesses in the system. The stages carried out during the penetration test process are exploration of the UGM-Secure system and network architecture, analysis of system weaknesses for exploitation, system exploitation, and reporting, in which the examiner documents the entire penetration test process as well as the mitigations that need to be carried out in the assessment report. The penetration test method that will be tested uses the evil twin method as well as several other methods that can support the evil twin method attacks, namely packet sniffing and pairwise master key identifier (PMKID). The results of the report are presented in an assessment report with the rules and procedures established by the National Institute of Standards and Technology (NIST). The results of this study indicate that the UGM-Secure access point has a security vulnerability in the form of unencrypted credentials so that these credentials can be known by attackers at any time when hacking occurs. Therefore, the UGM-Secure management needs to update the system that supports encryption for authentication to reduce the possibility of attackers getting open information to attack access points with a similar method.