ANALISIS *SECURITY ASSESSMENT* MENGGUNAKAN METODE *PENETRATION TESTING* DALAM MENJAGA KAPABILITAS KEAMANAN TEKNOLOGI INFORMASI PERTAHANAN NEGARA

SECURITY ASSESSMENT ANALYSIS USING PENETRATION TESTING METHODS IN MAINTAINING THE SECURITY CAPABILITY OF NATIONAL DEFENSE INFORMATION TECHNOLOGY

Bita Parga Zen[1], Rudy A.G Gultom[2], Agus H.S Reksoprodjo[3]

Prodi Teknologi Penginderaan, Fakultas Teknologi Pertahanan, Universitas Pertahanan
(bitapargazen@gmail.com, rudygultom@idu.ac.id, yono@sintesagroup.com)

Abstrak - Kemajuan teknologi informasi dan sistem pertahanan siber saat ini berkembang begitu pesat dengan kemajuan teknologi pada bidang siber khususnya pada webserver dan database dapat menjadi suatu ancaman dalam dalam pencurian data dan informasi sehingga perlu adanya penilaian keamanan untuk menanggulangi terjadinya pencurian data. Diperlukan langkah-langkah *Security Assessment* yang meliputi tahapan *Vulnerability Assessment* dan *Penetration Testing* fokus pada proses yang digunakan dalam merancang, meningkatkan, dan mengelola keamanan webserver dalam menekankan pada identifikasi area yang rentan terhadap serangan *hacker*. Dengan mengidentifikasi celah keamanan siber dalam Analisis Security Assessment bertujuan untuk memahami resiko keamanan sistem dari serangan siber melalui tahap *penetration testing,* selanjutnya mengkaji keamanan server dengan tujuan untuk meningkatkan keamanan sistem komputer dari pencurian data ilegal dengan pelanggaran keamanan pada jaringan komputer dan pengujian dalam peningkatan keamanan sistem pertahanan *firewall*, *router* dan *server*, selanjutnya untuk melakukan tahapan *Security Assessment* menggunakan beberapa metode seperti *Scanning Vulnerability* standar *Open Web Application Security Project*, *Common Vulnerability Scoring System* yang digunakan untuk mengidentifikasi keamanan untuk melakukan penilaian kelayakan pada suatu sistem, dan tahapan terakhir yaitu dengan melakukan *Lawful Penetration Testing* yang sudah memiliki izin pada penelitian untuk melihat data akses *login* dan akses *database* yang bisa masuk melalu celah-celah webserver sebagai akhir dari langkah uji coba untuk melihat celah dalam basis data.

Kata Kunci: *Security Assessment*, *Penetration Testing*, *CVSS*, OWASP, *Webserver*

Abstract - *The progress of various technological knowledge and cyber defense systems is currently developing so rapidly, and provides great support for the advancement, security, and resilience of the country, with technological advances in the field of cyberspace specifically in the web server and database can be by the needs in data and information security. there is a permit to cope with the transfer of data. Security Assessment measures that include the Vulnerability Assessment and Penetration Testing stages focus on the processes used to improve, enhance and manage web server security in discussing areas that are vulnerable to hacker attacks. By testing security vulnerabilities in security analysis Assessment examines system security challenges from cyberattacks through penetration testing, then examines server security to increase computer system security from illegal data theft by using security on computer networks and improving system security Firewall, router, and server security, then to carry out a Security Assessment using several methods such as Scanning*

[1] Program Studi Teknologi Penginderaan, Fakultas Teknologi Pertahanan, Universitas Pertahanan
[2] Program Studi Teknologi Penginderaan, Fakultas Teknologi Pertahanan, Universitas Pertahanan
[3] Program Studi Peperangan Asimetris, Fakultas Strategi Pertahanan, Universitas Pertahanan

Vulnerability Standards Open the Web Application Security Project, the General Vulnerability Assessment System used for security installations to conduct a feasibility study on a system, and subsequently carried out by conducting lawful Penetration Testing which must have permission on research to look at data access and database access that can enter through the webserver gaps as the end of the trial step to see the gap in the database.

Pendahuluan

Berbagai kemajuan ilmu pengetahuan teknologi informasi komunikasi dan sistem pertahanan saat ini berkembang begitu pesat dan luas hal ini memberi dukungan besar terhadap kemajuan, keamanan dan ketahanan bagi perlindungan suatu negara, Perkembangan teknologi dan informasi juga menciptakan berbagai peperangan yang berbasis pada jaringan dan dan memanfaatkan informasi serta mampu melaksanakan perang diranah digital maupun perang *cyber* hal ini tentu dapat berpengaruh terjadinya keretasan pada suatu sistem server. [4]

Apabila merujuk pada dasar konstitusi, dalam kekuatan pertahanan nir militer saat ini khususnya dalam ranah pertahanan pada bidang siber dibangun berdasarkan upaya dalam hal pembelaan negara Republik Indonesia, Kementerian Pertahanan Republik Indonesia merupakan salah satu unsur dukungan bersama kekuatan bangsa dalam menghadapi ancaman siber. Mengingat luas bidang pertahanan siber yaitu, untuk membangun *sense of defence* dalam bidang keamanan siber di sektor Pertahanan yang disusun Pedoman Pertahanan Siber. Melalui pemanfaatan teknologi informasi dan komunikasi saat ini mendorong terbentuknya ruang siber (*cyber space*).[5]

Melihat dari banyaknya pengguna internet di indonesia, tentu akan rentan terjadinya serangan siber, Serangan Siber adalah segala bentuk baik dalam perbuatan, perkataan, pemikiran baik yang dilakukan dengan sengaja maupun tidak sengaja oleh pihak mana pun, dengan motif dan tujuan yang dilakukan di lokasi mana pun, yang disasarkan pada sistem elektronik yang berupa muatan informasi maupun peralatan yang sangat bergantung pada teknologi dan jaringan. Bentuk ancaman siber yang terjadi saat ini

[4] Departemen Pertahanan Republik Indonesia. (2015). *Buku Putih Pertahanan Indonesia 2015*. Jakarta: Departemen Pertahanan Republik Indonesia

[5] Peraturan Menteri Pertahanan Republik Indonesia No 82 Tahun 2014 Tentang Pedoman Pertahanan Siber

diantaranya Serangan *Advanced Persistent Threats (APT), Denial of Service (DoS)* dan *Distributed Denial of Service (DDoS)*, Serangan *Defacement,* Serangan *Phising*, Serangan *Malware, Trojan Horse, Cracking Password*, dan *Spam.*

Ada beberapa acuan *framework* sistem keamanan, tata kelola, keamanan informasi untuk mengatasi serangan siber dalam perusahaan atau organisasi seperti : *Programming and Budgeting Cyber Security Framework* Dalam dunia maya, serangan hacker dapat terjadi dari berbagai macam celah, dan sebuah sistem harus siap untuk menangkal seluruh kemungkinan serangan yang dapat terjadi. Persiapan dan respon defensif ini mencakup berbagai kemungkinan dan aktivitas tersebut membutuhkan biaya untuk menjamin keamanan di dunia maya[6]

NIST *Cyber Security Framework* sebuah proses untuk mengidentifikasi, menilai, dan merespons sebuah risiko yang sedang berlangsung. Dalam mengelola sebuah risiko, organisasi harus memahami kemungkinan tentang suatu peristiwa yang terjadi dan potensi dampak yang diakibatkan. Dengan informasi tersebut, organisasi dapat menentukan tingkat risiko yang mungkin akan dihadapi[7]

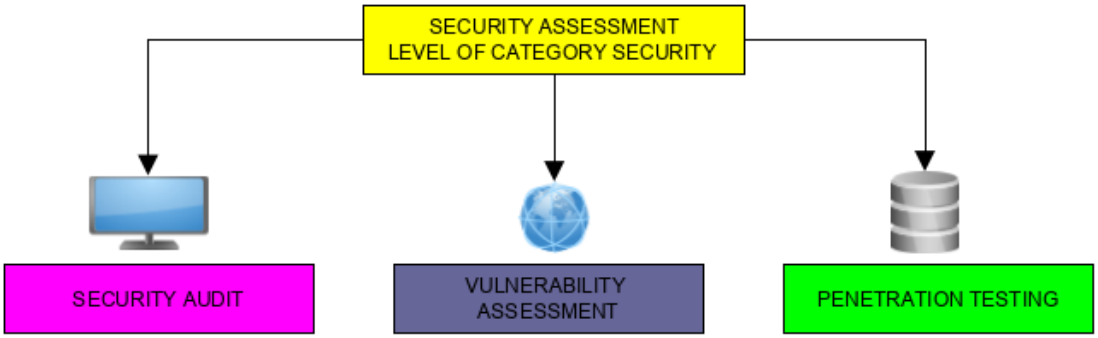
Information Secrity Management ISO 27001 : 2013 merupakan standar keamanan yang berfokus untuk menjaga informasi yang digunakan untuk mengamankan data, yang menguraikan persyaratan yang disarankan untuk membangun, memantau, memberikan panduan organisasi tentang cara membuat, menerapkan dan memelihara dan meningkatkan sistem manajemen keamanan informasi (SMKI). Pada ISO 27001 memiliki standar yang berfokus untuk menjaga kerahasiaan informasi pelanggan dan pemangku kepentingan dan menjaga integritas, bertujuan dalam penekanan pada identifikasi, evaluasi dan pengelolaan resiko yang dapat diterima oleh sistem informasi[8].

---

[6] Martin C Libicki. (2016). A Framework for Programming and Budgeting for CyberSecurity. Rand Corporation

[7] National Institute of Standards and Technology. (2018). Framework for Improving Critical Infrastructure Cyber Security. U.S Departement of Commerce

[8] Georg Disterer (2013). *ISO / IEC 27000, 27001, and 27002 for Information Security Management*, University of Applied Sciences, *Journal of Information Security*, 2013, 4, 92-100.



Gambar 1. *Security Assessment Category Level*
Sumber: Critical Ethical Hacking, 2012

Six Ware Network Security Framework merupakan konsep kerangka kerja keamanan awal, keamanan jaringan yang komprehensif sebagai solusi untuk meningkatkan ketahanan keamanan jaringan sebuah organisasi dari ancaman, serangan dan kerentanan, cara ini merupakan sebuah strategi keamanan tingkat operasional yang memungkinkan untuk mencari tahupaling banyak tindakan efesien dan efektif yang dapat memberikan solusi dalam keamanan jaringan[9], *Open Web Application Security Project (OWASP) Framework* (penjelasan detail terlampir di bab berikutnya) dalam hal ini peneliti berfokus pada penilaian keamanan webserver melalui metode *penetration testing*, *framework* yang tepat dan dalam melakukan penelitian ini yaitu dengan OWASP memiliki metode keamanan sistem data terbesar yang pernah dikumpulkan dalam persiapan standar keamanan aplikasi. *Framework* ini digunakan sebagai standar keamanan aplikasi dalam melakukan *vulnerability assessment* menggunakan *framework* standar *open web aplication security project* dalam melakukan dalam mengatasi risiko keamanan aplikasi paling berdampak yang saat ini dihadapi suatu instansi[10]

Pengujian penetrasi merupakan langkah penting dalam pengembangan sistem pertahanan berbasis komputer *server* yang aman yang terhubung dalam suatu jaringan dalam hal apapun karena tidak hanya menekankan operasi, tetapi implementasi dan desain sistem. ini adalah tindakan resmi dan dijadwalkan yang memisahkan tester penetrasi dari penyerang dan telah banyak diadopsi oleh organisasi dan lembaga[11]. Selain itu

[9] Gultom, Rudy AG. (2018). *Enhancing Computer Network Security Environment By Implementing The Six-Ware Network Security Framework (SWNSF)*, Indonesia Defense University, Conference Paper 2018. DOI: 10.5121/csit.2018.81714

[10] Nishant Shrestha (2012) *Security Assessment A Network and System Administrator's Approach*, Universitas Oslensis

[11] Critical Ethical Hacking, (2012), Penetration Testing

dalam pengujian penetrasi digunakan sebagai evaluasi keamanan pada sistem komputer atau *server* jaringan dengan mengidentifikasi kelemahan (*vulnerability*) sebagai identifikasi berupa celah keamanan, konfigurasi, *firewall* dan *wireless point*[12]

Langkah-langkah pada *vulnerability assasment* mencakup kerentanan yang dikumpulkan dari instansi beberapa kementerian dan lembaga *cyber* di indonesia. Dalam penilaian kerentanan tahapan yang akan dilalui yaitu melalui tahapan *Scanning* SQL *Injection* yaitu melihat kelemahan melalui database seperti SQL, XAMPP, *Broken Authentication* melihat kelemahan pada *password* dan *username, Sensitive Data Exposure* melihat kelemahan data sensitif seperti kelemahan pada enkripsi yang menyebabkan pencurian data dan identitas. *XML External Entities (XEE)* melihat sumber data yang tidak dipercaya

dalam dokumen XML, *Broken Access Control* memungkinkan penyerang untuk melewati proses autorisasi dan dapat melakukan hal-hal yang biasanya diakses oleh seorang admin[13]

saat ini Kementerian Pertahanan bahwa institusinya menerima 60 sampai 80 ribu serangan siber setiap harinya serangan berupa Ransomware, Trojan Policy, Policy dan lain lain, serangan ini meliputi data data strategis seperti informasi personil Tentara Nasional Indonesia seperti alamat, umur, golongan darah sebsite portal *database* dan penghargaan[14]

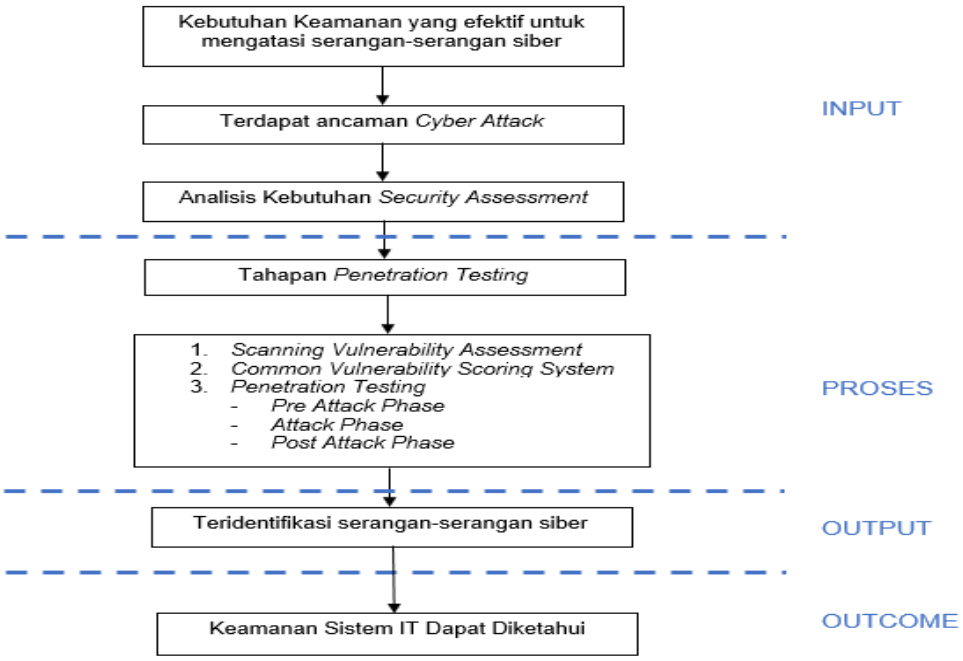
Metode Penelitian

Metode penelitian yang digunakan dalam melaksanakan penelitian ini adalah dengan menggunakan metode kuantitatif dengan uji penetrasi

[12] Yunanri W, et all. (2016). *Analisis Keamanan Web Server menggunakan metode Penetration testing*, UAD Yogyakarta, ISBN: 979-587-626-0

[13] OWASP Zed Attack Proxy Project (2019) https://www.owasp.org/index.php/OWASP_Zed_Attack_Proxy_Project diakses tanggal 31 Juli 2019

[14] CNN Indonesia (2018) https://www.cnnindonesia.com /teknologi/20181107155049-185-344721/kemenhan-terima-80-ribu-serangan-hacker-tiap-hari diakses tanggal 07 Juni 2018

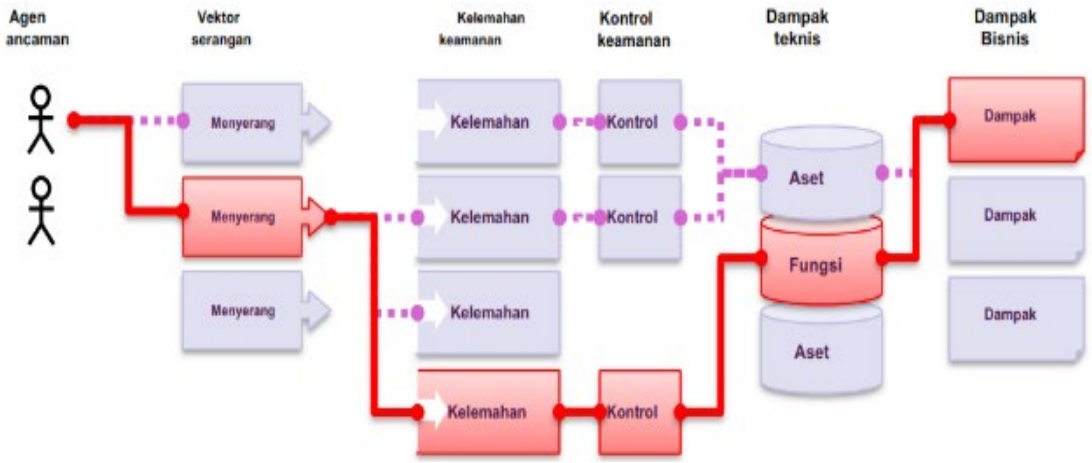


Gambar 2. Digram Alur *Security Assessment* oleh Peneliti
Sumber: Hasil olah peneliti, 2020

(*penetration testing*). Metode uji penetrasi berdasarkan jumlah informasi yang tersedia di Pusat Pertahanan Siber Kementerian Pertahanan (Pushansiber Kemhan) seperti yang sudah dijelaskan oleh peneliti pada latar belakang, selanjutnya peneliti melakukan untuk ujicoba dimana celah yang rentan untuk di *crack* atau diretas oleh sesorang yang tidak bertanggung jawab, selanjutnya kemudian peneliti memprediksi dan menentukan tingkat kerentanan yang belum terancang di Pusat Pertahanan Siber Kementerian Pertahanan, selanjutnya melakukan mengumpulkan informasi dan data untuk diolah

Penggunaan metode penelitian kuantitatif dengan *penetration testing* ini dijadikan acaun dan dasar sistem keamanan pada web*server* yang sebelumnya sudah peneliti teliti dengan menggunakan analisa *security assesment* dimana dalam hal ini menggunakan beberapa tahapan yaitu dengan penilaian kerentanan dengan standarisasi OWASP dan *Scoring System* dan melakukan uji penetrasi dengan standarisasi SQL *Injection.*

Dalam melakukan penelitian dapat menentukan langkah dari proses persiapan yaitu memasukan berdasarkan latar belakang masalah kebutuhan keamanan yang efektif untuk mengatasi serangan-serangan siber, ancaman *cyber attack* pada pusat pertahanan siber kementrian pertahanan, tahapan *Security Assessment* mulai dari *Scanning Vulnerability assessment* yang mengikuti standar OWASP , *Penetration testing* sehingga tujuan yang akan dicapai pada penelitian ini akan efektif. Selanjutnya adalah proses pelaksanaan penelitian



Gambar 3. Tahapan *Scanning Vulnerability*
Sumber: OWASP, 2017

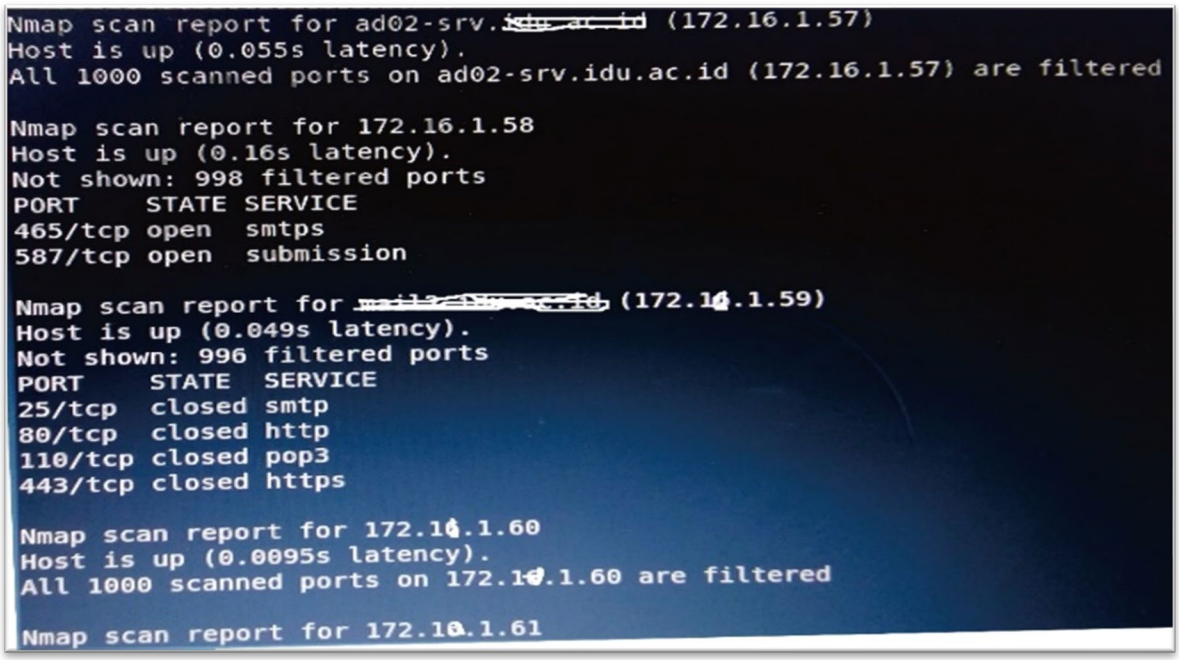
dengan tinjauan lokasi yang akan diuji, pengumpulan data, pengolahan data, dan berakhir pada hasil penelitian yang siap untuk dilakukan analisis berdasarkan metode yang akan dilakukan. Hasil analisis terdapat pada kesimpulan penelitian berupa identifikasi serangan-serangan siber sehingga menghasilkan *outcome* keamanan sistem IT dapat diketahui. Untuk Populasi pada penelitian ini adalah website dengan *internet protocol* 139.25*.2*5.2 yang akan dilakukan uji keamanannya. Sistem yang dirancang dalam penelitian ini ditujukan untuk mendeteksi kerentanan pada website melalui tahap uji penetrasi meliputi karakter secara menyeluruh hal yang akan diuji karena penelitian ini merupakan analisis *loboratory test* sistem keamanan terhadap kerentanan yang terjadi pada *webserver* dan bagaimana cara mengatasinya.

Hasil dan Pembahasan

Waktu Dalam Tahapan Penetration testing dilakukan setelah peneliti melakukan scanning vulnerability. Tahap yang dilakukan untuk pentetration testing yaitu dengan melakukan SQL Injection mulai dari tahap ini dihitung dari rentang waktu yang dibutuhkan pada saat penelitian dengan langkah-langkah Seorang User menentukan Web Aplikasi atau WebServer yang akan dilakukan Penetrasi, melakukan pencarian database, apakah ada celah kerentanan[15]

Penelitian dilakukan di Pusat Pertahanan Siber Kementerian Pertahanan dan Lab Siber Unhan, dimana Pusat Pertahanan Siber merupakan Unsur Pelaksana Tugas dan Fungsi Badan

[15] Veracode, "SQL Injection: Vulnerabilities & How to Prevent SQL Injection Attacks,"

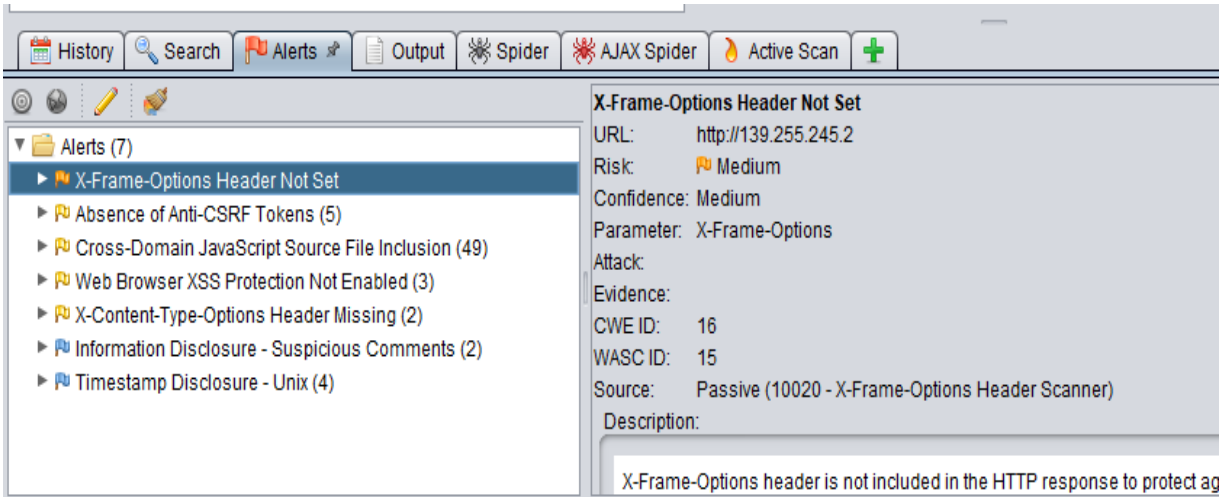


Gambar 4. *Scanning* Jaringan *IP* dengan *NMAP*
Sumber: NMAP modifikasi peneliti, 2019

Instalasi Strategis Pertahanan Kementerian Pertahanan dan Labsiber Universitas Pertahanan dan Lab Siber Universitas Pertahanan memiliki server yang dimiliki oleh Kementerian Pertahanan Republik Indonesia, setiap hari terjadi puluhan ribu serangan siber yang menyerang server di kementerian pertahanan, berikut data serangan siber yang terjadi di salah satu server Kementerian Pertahanan, antara lain Serangan Pada Website, Database dan Server

Lab Siber Unhan merupakan sebuah server yang dimiliki oleh Kementerian Pertahanan, yang terletak di Universitas Pertahanan yang berguna sebagai laboratoriun siber sebagai komponen yang dibangun untuk menangkal serangan-serangan siber yang saat ini berkembang pesat dan untuk mengetahui perkembangan di bidang teknologi informasi yang menjadi pilar revolusi industri 4.0, selanjutnya pada Lab Siber Unhan memiliki 1 IP Privat dengan nama IP 172.1*.1.0/24 dan 63 IP Publik mulai dari IP 172.1*.1.1/24 sampai dengan IP 172.1*.1.63/24 dari hasil Scan IP tersebut terdapat beberapa situs dan port seperti port 22 sebagai SSH, Port 80 alamat website (HTTP) dan Port 3306 sebagai port MYSQL, dari hasil scan terdapat celah untuk dilakukan tahapan uji kerentanan, selanjutnya dari IP Tersebut adakan dilakukan tahapan untuk pembuktian sistem keamanan dengan standar *Open Web Application Security Project* (OWASP) dan tahapan Common Vulnerability Scoring System (CVSS)

Melihatnya banyaknya perkembangan sistem pada sebuah software tentang sistem keamanan



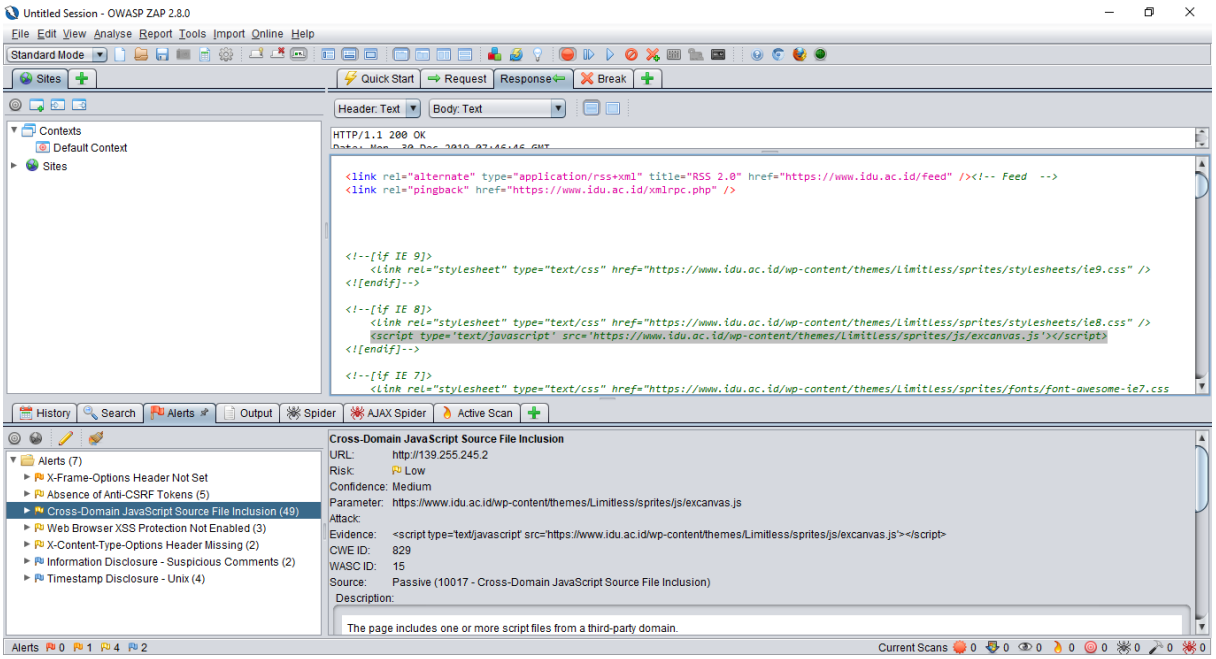
Gambar 5. *X-Frame Options Scanner*
Sumber: OWASP ZAP TOP 10, 2019

informasi dan keamanan pada web server membuat peneliti melakukan uji sampel IP 139.25*.2*5.2 yang akan menjadi target untuk melakukan uji *security assessment* dimana pada uji *security assessment* terdapat 3 tahapan , yang pertama melakukan tahapan ujian vulnerability assessment (Peniliain Kerentanan) dimana tahapan ini yaitu tahapan mencari kelemahan pda webserver melalui uji scanning, pada uji scanning ini tahapan yang dilakukan mengikuti standar framework OWASP TOP 10, dari hasil uji *scanning* terdapat pemberitahuan tingkat kerentanan, diantaranya :

X-Frame Options Header Scanner

Pada Tahapan Scanning melalui aplikasi OWASP ZAP terdapat kerentanan yang terdeteksi bisa masuk pada alamat situs 139.25*.2*5.2 tersebut dengan tingkat resiko rendah, terdapat pada "*X-Frame Options Header Not Set*" yang dapat menyerang web melalui *ClickJacking*, *ClickJacking* adalah sebuah serangan yang dapat memanipulasikan sebuah tampilan website dan seolah olah ketika seseorang melakukan klik tersebut dapat beresiko dan dapat menyebabkan kerugian seperti dapat mengakses *webcam* yang terdeteksi, pencurian akses email atau data pribadi lainnya dengan cara menyembunyikan *user interface* sensitif dengan membuatnya transparan sehingga berpotensi mengungkapkan informasi rahasia atau mengendalikan komputer pada halaman web yang tampaknya tidak berbahaya, karena itu pada webserver dibutuhkan sebuah *X-Frame-Options* untuk menghindari terjadinya *clickjacking* dengan menambahkan script seperti berikut <*frame*> <*iframe*> <*embed*> <*object*> yang digunakan untuk mencegah situs dari serangan *ClickJacking*.

Absence of Anti-CSRF Tokens (Cross Site Scripting)



Gambar 6. *Cross Domain Script Inclusion*
Sumber: OWASP ZAP TOP 10, 2019

Dampak dari *Cross Site Scripting* (XSS) adalah dapat dengan mengeksekusi jarak jauh kode pada browser webserver, seperti mencuri kredensial, sesi, atau memberikan malware kepada pengguna, bukti kelemahan pada Cross Site Scripting

Pada Kelemahan Absence of Anti CSRF Tokens Fase yang dapat terjadi kelemahan yaitu pada Arsitektur Desain yang memungkinkan seseorang memasukan script sisi klien ke halaman web pengguna lain webserver seharusnya memiliki paket anti CSRF seperti OWASP Guard sebagai penangkal jika terjadi serangan berupa *Cross Site Scripting*

Absence of Anti-CSRF Tokens (*Cross Site Scripting*)

URL : 13*.25*.2*5.2

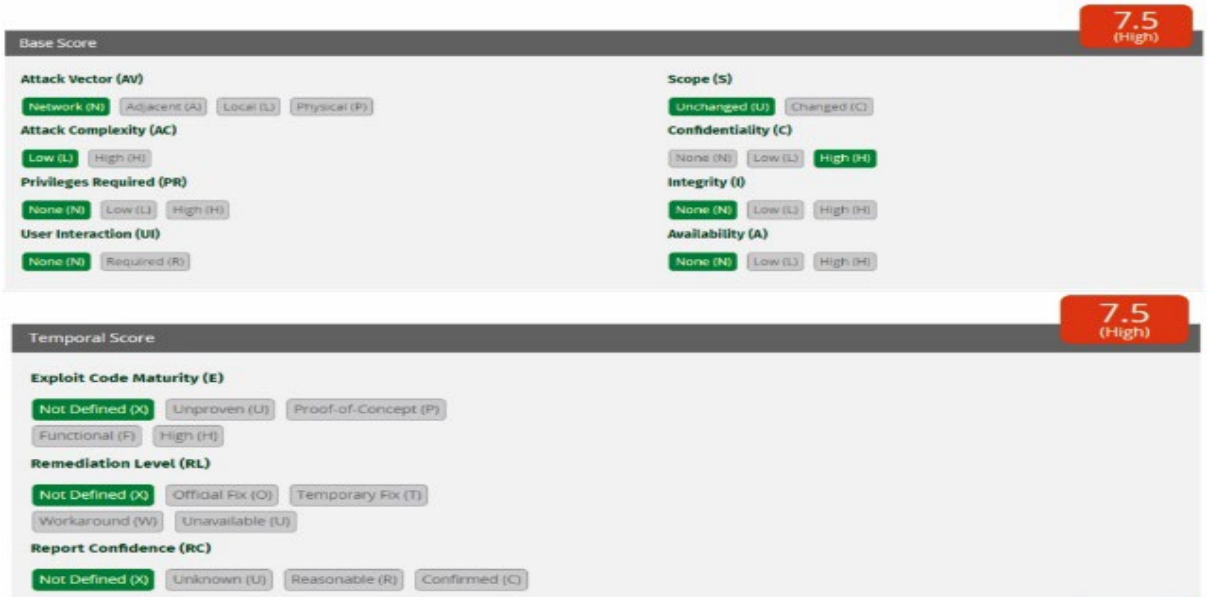
Risk : Low

Confidence : Medium

Server: Apache/2.4.18 (Ubuntu)

Cross Domain Script Inclusion

Dari hasil *scanning* dengan alamat URL : 13*.25*.2*5.2 menggunakan OWASP terdapat pemberitahuan *Cross-Domain JavaScript Source File Inclusion* yang berarti adalah terdapat kerentanan pada *javascript* seperti padah HTML pada web dan CSS pada layout keselarasan website bahwa kelemahan yang akan dihadapi ini merupakan sebagai sistem keamanan yang perlu ditingkatkan karena harus memperbarui referensi Javascript secara manual setiap kali versi baru dirilis seperti pada website ini menggunakan template *wordpress* untu tingkat resiko rendah.



Gambar 7. Hasil Analisis *Directory Listening* Melalui *CVSS*
Sumber: CVSS, 2019

Penilaian Hasil Kerentanan Menggunakan *Common Vulnerability Scoring System*

Dari hasil kerentanan menggunakan *Common Vulnerability Scoring System* (CVSS) terdapat 3 sistem yang terdeteksi bisa mengakibatkan data atau sistem diserang karena terdapat kelemahan pada server tersebut, dari 3 sistem tersebut diantaranya kerentanan diantarnya:

1. *Directory Listening* artinya Folder yang terbuka yang bisa dengan mudah dapat diakses oleh oranglain yang dengan mudah untuk mencuri gambar, laporan dan file file lainnya
2. *Insecure transition from http to https* artinya pada HTTPS berisi halaman aman yang dapat memposting ke halaman tidak aman seperti http, namun pada webserver ini hanya menggunakan http sebagai aksesnya dan ini dapat menjadikan target serangan dan dapat mengganti target form.
3. *HTML form without CSRF protection* artinya pada HTML tidak terdapat terdapat sebuah sistem dengan kerentanan di mana penyerang menipu korban untuk mengajukan permintaan yang tidak ingin dilakukan oleh korban. Oleh karena itu, dengan CSRF, penyerang menyalahgunakan kepercayaan aplikasi web dengan browser yang telah dimanipulasi karena itu dibutuhkan Token Anti CSRF yang aman dari sebuah kriptografi yang dihasilkan oleh algoritma yang kuat

Pada hasil Analisis *Insecure transition from HTTP to HTTPS* melalui *Common Vulnerability Scoring System* dijelaskan tingkat kerentanan tinggi dengan skor 7.5 dikarenakan pada *Attack*

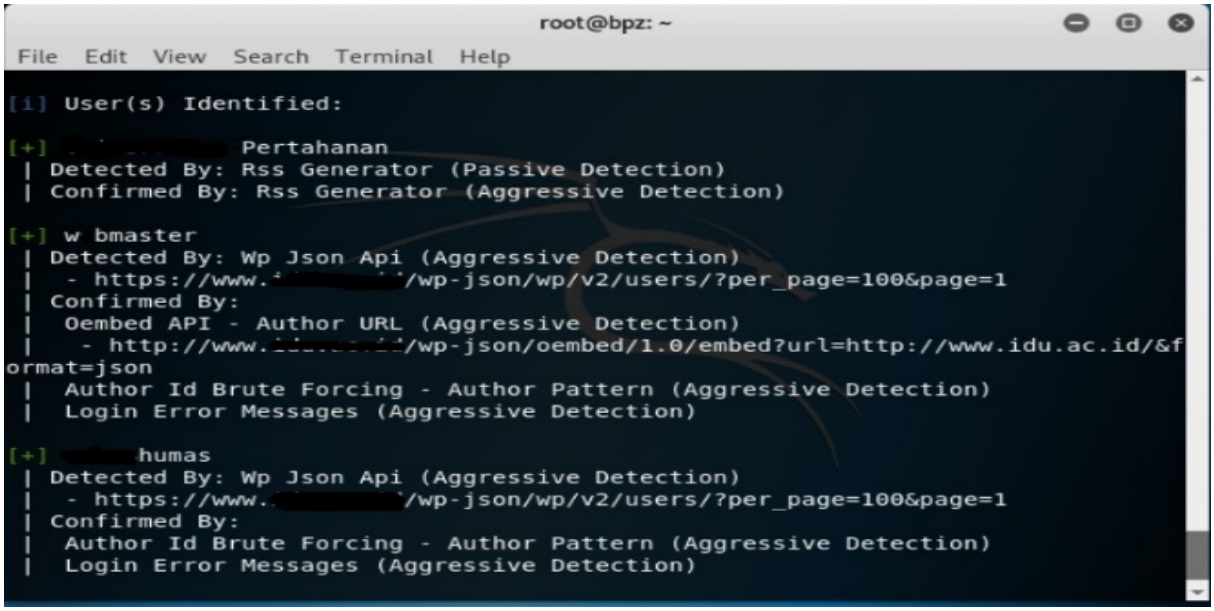
Vector menunjukkan bagaimana cara untuk mengeksploitasi kerentanan, pad penilaian kerentanan dilihat dari seberapa jauh penyerang dapat masuk ke sistem menandakan *network* (n) yang artinya penyerang dapat menyerang sistem melalui jaringan dengan mudah, berbeda jika skor menandakan *adjacent* skor 6.5 tingkat kerentanan medium, jika menandakan *local* (L) skor 6.2 tingkat kerentanan medium dan *physical* (p) menandakan skor 4.6 yang berarti tingkat kerentanan medium

Selanjutnya pada *Attack Complexity* (AC) berpengaruh pada tingkat kerentanan dikarenakan menandakan *low* (L) yang berarti kompleksitas serangan ketika penyerang mendapatkan akses pada sistem dengan mudah. Karena semakin rendah kompleksitas yang diperlukan, maka semakin tinggi nilai kerentanannya, begitupun pada *Privileges Required* (PR) yang berfungsi sebagai menentukan nilai tingkat hak akses yang dimiliki oleh penyerang sebelum berhasil mengeksploitasi kerentanan pada sistem ini menandakan *none* (n) yang berarti penyerang dapat mengeksploitasi sistem sehingga tingkat kerentanan mencapai 7.5 yang berarti kerentanan tinggi

Pada *User Interaction* (UI) berpengaruh pada penilaian persyaratan pengguna jika *none* (n) menandakan ada nya celah kerentanan, namun jika menandakan *required* ® tingkat keamanan lebih kuat krena penyerang atau pihak lain yang berkaitan dengan komponen kerentanan sulit untuk menembus server

Hasil Uji Penetration Testing

Saat melakukan uji penetrasi yaitu dengan melakukan SQL Injection dengan melakukan Bruite Password untuk melakukan pencarian database, apakah ada celah kerentanan. Yang dapat dilakukan oleh seorang hacker melalui tahapan *Bruite Force Password*, tahapan ini dilakukan dimana penyerang melakukan berbagai percobaan untuk



Gambar 8. Hasil Akses *ID Pentest* Melalui *WPScan*
Sumber: Hasil olah peneliti, 2019

masuk ke dalam sebuah sistem dan mempelajari respon sistem tersebut ketika diberikan masukan alamat situs, Saat melakukan tahapan penetration test dengan kata kunci: wpscan –url http://13*.2*5.2*5.2 –enumerate u

Wpscan digunakan sebagai tools untuk melakukan uji penetrasi untuk mengetahui dalam mendeteksi nama pengguna pada saat login ke akses webserver terdapat beberapa port yang terbuka dengan tingkat kerentanan tertera pada saat sistem sedang berjalan, seperti terdapat celah plugin, plugin yaitu suatu fitur tambahan pada wordpress seperti captcha, statitstik pengunjung seperti berikut:

wp-content/plugins/wp-statistics/

wp-content/plugins/wp-statistics/readme.txt

wp-content/plugins/captcha/css/front_end_style.css?ver=4.4.5

Selanjutnya setelah melakukan deteksi akses login melalui username, peneliti melakukan percobaan pembobolan password dengan melakukan beberapa script sebagai percobaan, dan melakukan coding sebagai berikut ini:

wpscan--url-P /usr/share/wordlists/ dirb/ common.txt -U webmaster

wpscan --url **********/ -P ~/Downloads/rockyou.txt -U webmaster

Selanjutnya untuk tahapan yang lebih sensitif lagi, peneliti melakukan investigasi dengan cara masuk ke daerah identitas diri, pada gambar dibawah ini sebagaian data di sensor untuk menjaga kerahasiaan instansi terkait, terdapat 3 celah untuk dapat dimasukan oleh

peneliti agar bisa masuk dalam sistem, ternyata terdapat 3 celah yaitu

1. Akses ID ******* Pertahanan
2. Akses ID W*master
3. Akses ID *****humas

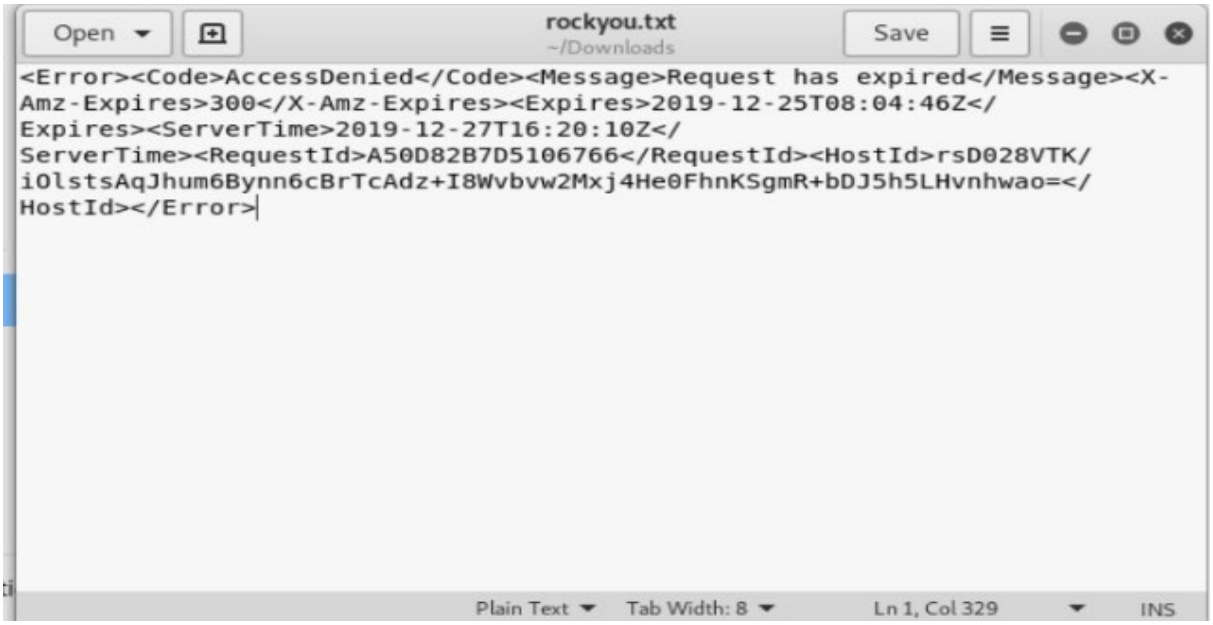
Dengan cara seperti ini dapat ditemukan celah kerentanan yang dapat mengakibatkan data-data pada server bisa dimasukan oleh *hacker* untuk melakukan hal yang dapat merugikan sistem karena memungkinkan hacker mengambil data yang bersifat rahasia.

Kesimpulan berdasarkan analisis dari data yang diperoleh dan pembahasan tentang penilaian keamanan menggunakan metode penetration testing pada webserver dapat ditarik kesimpulan sebagai berikut:

Dengan analisis *security assessment* terdapat tahapan untuk melakukan tingkat kerentanan dengan standar OWASP TOP 10 yaitu dapat mengidentifikasi celah-celah yang bisa menjadi target serangan *hacker* untuk masuk ke sebuah website[16] secara ilegal selanjutnya dengan menggunakan metode *Common Vulnerability Scoring System* cara ini bisa digunakan untuk dapat menentukan tingkat kerentanan dan menghasilkan skor yang mencerminkan tingkat kerentanan pada webserver dan CVSS terdapat kualifikasi ke dalam representasi rendah, sedang, tinggi, dan kritis untuk membantu sebuah organisasi menilai dengan benar dan memprioritaskan proses manajemen kerentanan website[17]. *Security Assessment* pada penelitian ini membantu dalam pengambilan keputusan untuk menghindari serangan-serangan siber dengan efektif berdasarkan data-data tersebut di atas, maka penelitian sistem keamanan webserver menggunakan menggunakan metode penetration testing terbukti optimal karena terdapat celah-celah untuk masuk ke sebuah akses user ID dan akses *database* dalam menentukan rancangan webserver yang lebih aman untuk kedepan, selanjutnya Setelah melakukan uji *penetration testing* pada IP 139.2*5.2*5.2 sistem firewall pada webserver ini cukup baik sehingga cukup

[16] Ankita Gupta et all. (2013). *Vulnerability assessment and Penetration testing*, University of Technology India. International Journal of Engineering Trends and Technology- Volume4Issue3- 2013

[17] Klima, Tomas. (2016). *Methodology of Information Systems Security Penetration testing*, Acta Informatica Pragensia



Gambar 9. Tampilan *Script Hacking Bruite Force Attack*
Sumber: Modifikasi peneliti, 2019

menyulitkan dalam mengeksploitasi sistem, namun pada sistem operasi pada webserver menggunakan Apache/2.4.18 Ubuntu dapat diketahui dengan ditemukan 3 akses login yang bisa menjadikan penyerang masuk ke sistem webserver dengan masuk melalui celah user ID dan akses *database.*

Script ini merupakan teknik yang dilakukan oleh peneliti untuk melakukan *hacking* dengan tahap *SQL Injection* cara melakukan bilangan-bilangan acak yang dijadikan percobaan seperti dibawah ini sebagai percobaan untuk melakukan teknik hacking dalam melakukan akses ID

nrz+525ZgiJuqiTaAqrqvrH7gogaJUvkbm
UuUdFPNdC0P4kQkXIDQ4OCvL6nKbRKI
wwmL8s7Vd4=
XKRCRnCqgkaXIoY3asZQSUcE53dRKcLW
Po88bEX/kL1osVfoZk49Bk4spRaKJWvED
DUzN8MDC4o=
BtJ/nZFMLHFWtoPslJjFhi56loPQIBKyeo
m6vsJcIZM/zS/jWNHo/C4vwC2DQ2kiWK
CWvYwqPsk=

Dengan cara seperti ini dapat ditemukan celah kerentanan yang dapat mengakibatkan data-data pada server bisa dimasukan oleh *hacker* untuk melakukan hal yang dapat merugikan sistem karena memungkinkan hacker mengambil data yang bersifat rahasia.

Kesimpulan

Kesimpulan berdasarkan analisis dari data yang diperoleh dan pembahasan tentang penilaian keamanan menggunakan metode penetration testing pada webserver dapat ditarik kesimpulan sebagai berikut:

Dengan analisis security assessment terdapat tahapan untuk melakukan tingkat kerentanan dengan standar

OWASP TOP 10 yaitu dapat mengidentifikasi celah-celah yang bisa menjadi target serangan hacker untuk masuk ke sebuah website secara ilegal selanjutnya dengan menggunakan metode Common Vulnerability Scoring System cara ini bisa digunakan untuk dapat menentukan tingkat kerentanan dan menghasilkan skor yang mencerminkan tingkat kerentanan pada webserver dan CVSS terdapat kualifikasi ke dalam representasi rendah, sedang, tinggi, dan kritis untuk membantu sebuah organisasi menilai dengan benar dan memprioritaskan proses manajemen kerentanan website. Security Assessment pada penelitian ini membantu dalam pengambilan keputusan untuk menghindari serangan-serangan siber dengan efektif berdasarkan data-data tersebut di atas, maka penelitian sistem keamanan webserver menggunakan menggunakan metode penetration testing terbukti optimal karena terdapat celah-celah untuk masuk ke sebuah akses user ID dan akses database dalam menentukan rancangan webserver yang lebih aman untuk kedepan.

Setelah melakukan uji penetration testing pada IP 139.2*5.2*5.2 sistem firewall pada webserver ini cukup baik sehingga cukup menyulitkan dalam mengeksploitasi sistem, namun pada sistem operasi pada webserver menggunakan Apache/2.4.18 Ubuntu dapat diketahui dengan ditemukan 3 akses login yang bisa menjadikan penyerang masuk ke sistem webserver dengan masuk melalui celah user ID dan akses database.

Berdasarkan hasil penelitian, peneliti memberikan saran yang diajukan sesuai dengan masalah pada latar belakang penelitian. Harapan dari peneliti, asumsi dari hasil penelitian ini dapat dijadikan sebagai bahan pertimbangan oleh pihak pada pushansiber kementerian pertahanan, lab siber universitas pertahanan untuk dilanjutkan dalam penelitian terkait keamanan siber karena pada kementerian pertahanan terjadi puluhan ribu serangan siber setiap harinya

Pada webserver sebaiknya digunakan *plugin wordfence* karena terdapat firewall dan malware scan untuk keamanan sebuah website dan menghindari serangan DdoS dan sebaiknya Pada webserverver jangan terlalu banyak instal plugin, karena jika terlalu banyak instal plugin seperti adobe flash sangat rentan terjadi pembajakan seperti "*ClickJacking*" dan selalu Gunakan *Hypertext Transfer Protocol Secure*

(HTTPS) karena HTTPS terdapat *Secure Socket Layer* yang terenkripsi dengan baik dan sulit untuk diretas

Daftar Pustaka

Buku

Departemen Pertahanan Republik Indonesia. (2015). *Buku Putih Pertahanan Indonesia 2015*. Jakarta: Departemen Pertahanan Republik Indonesia

Critical Ethical Hacking, (2012), Penetration Testing

Fatahna, An'im M (2011) CentOS Indonesia Community, Surabaya

Jurnal

Nishant Shrestha (2012) *Security Assessment A Network and System Administrator's Approach*, Universitas Oslensis

Yunanri W, et all. (2016). *Analisis Keamanan Web Server menggunakan metode Penetration testing*, UAD Yogyakarta, ISBN: 979-587-626-0

Libicki, C Martin et all. (2016). A Framework for Programming and Budgeting for CyberSecurity. Rand Corporation

National Institute of Standards and Technology. (2018). Framework for Improving Critical Infrastructure Cyber Security. U.S Departement of Commerce

Disterer, Georg. (2013). *ISO / IEC 27000, 27001, and 27002 for Information Security Management*, University of Applied Sciences, *Journal of Information Security*, 2013, 4, 92-100.

Gultom, Rudy AG. (2018). *Enhancing Computer Network Security Environment by Implementing The Six-Ware Network Security Framework (SWNSF)*, Indonesia Defense University, Conference Paper 2018. DOI: 10.5121/csit.2018.81714

Ankita Gupta et all. (2013). *Vulnerability assessment and Penetration testing*, University of Technology India. International Journal of Engineering Trends and Technology-Volume4Issue3- 2013

Klima, Tomas. (2016). *Methodology of Information Systems Security Penetration testing*, Acta Informatica Pragensia

Peraturan

Peraturan Menteri Pertahanan Republik Indonesia No 82 Tahun 2014 Tentang Pedoman Pertahanan Siber

Website

OWASP Zed Attack Proxy Project (2019) https://wwwowasp.org/ index.php/ OWASP_Zed_Attack_Proxy_Project diakses tanggal 31 Juli 2019

CNN Indonesia (2018) https:// www.cnnindonesia.com/teknologi/ 2018 1107155049-185-344721/kemenhan-terima-80-ribu-serangan-hacker-tiap-hari diakses tanggal 07 Juni 2018

Veracode, "SQL Injection: Vulnerabilities & How to Prevent SQL Injection Attacks," https:// www. veracode. com/security/sqlinjection

Lampiran

Tabel 1. Jenis Serangan Siber pada Webserver di Wilayah Kemhan, 30 Oktober 2019

2019-10-28T04:17:53.674Z	ET-POLICY Outgoing Basic Auth Base64 HTTP Password detected unencrypted
2019-10-28T04:21:36.871Z	ET-POLICY curl User-Agent Outbound
2019-10-28T04:03:53.609Z	ET POLICY External IP Lookup ip-api.com
2019-10-28T04:22:55.703Z	SURICATA TLS invalid handshake message
2019-10-28T05:54:18.136Z	ET CNC Ransomware Tracker Reported CnC Server group 72
2019-10-30T11:43:42.803Z	ET CINS Active Threat Intelligence Poor Reputation IP group 75

Data serangan komentar spam hasil analisis *security assessment*

"LiveBroadcast","mejs.afrikaans":"Afrikaans","mejs.albanian":"Albanian","mejs.arabic":"Arabic","mejs.belarusian":"Belarusian","mejs.bulgarian":"Bulgarian","mejs.catalan":"Catalan","mejs.chinese":"Chinese","mejs.chinese-simplified":"Chinese (Simplified)","mejs.chinese-traditional":"Chinese (Traditional)","mejs.croatian":"Croatian","mejs.czech":"Czech","mejs.danish":"Danish","mejs.dutch":"Dutch","mejs.english":"English","mejs.estonian":"Estonian","mejs.filipino":"Filipino","mejs.finnish":"Finnish","mejs.french":"French","mejs.galician":"Galician","mejs.german":"German","mejs.greek":"Greek","mejs.haitian-creole":"Haitian Creole","mejs.hebrew":"Hebrew","mejs.hindi":"Hindi","mejs.hungarian":"Hungarian","mejs.icelandic":"Icelandic","mejs.indonesian":"Indonesian","mejs.irish":"Irish","mejs.italian":"Italian","mejs.japanese":"Japanese","mejs.korean":"Korean","mejs.