NARATIF : Jurnal Ilmiah Nasional Riset Aplikasi dan Teknik Informatika
Vol. 05 No. 01 Juni 2023
P-ISSN: 2656-7377 || E-ISSN: 2714-8467

PENETRATION TESTING WEBSITE DENGAN METODE *BLACK BOX TESTING* UNTUK MENINGKATKAN KEAMANAN *WEBSITE* PADA INSTANSI (*REDACTED*)

Widi Linggih Jaelani[1], Yanto[2], Fitri Khoirunnisa[3]
Program Studi Teknik Informatika[1,2,3]
Sekolah Tinggi Teknologi Bandung[1,2], Universitas Adhirajasa Reswara Sanjaya[3]
jaelaniwidi@gmail.com [1], yan95452@gmail.com[2], fitrikhoirunnisa66@gmail.com[3]

Abstrak

Penetration testing website merupakan sebuah pengujian yang dilakukan untuk meningkatkan keamanan pada *website* agar tidak terkena serangan dari luar hak akses. *Penetration testing* memiliki 3 metode dalam melakukan pengujian diantaranya, *black box testing, white box testing* dan *gray box testing*. Dimana ketiga metode ini mempunyai *scope* pengujian yang berbeda dan memiliki kelebihan dan kekurangannya masing-masing. Metode *black box testing* hanya mendapatkan akses sebatas informasi tentang nama *website* atau alamat url saja. Pengetesan *white box testin*g akses yang penguji dapatkan itu sangat kompleks, karena dengan metode ini penguji dapat mengetahui *scope* yang banyak dimulai dari coding, alur dari aplikasi, dan hak akses yang cukup untuk melakukan pengetesan. Sedangkan metode *gray box testing* pada pengujian ini hak akses yang dimiliki penguji mengetahui alur dan memiliki akun yang bisa di akses ke dalam *website*. *Penetration testing website* dengan metode *black box testing* merupakan teknik pengujian *website* untuk meningkatkan keamanan *website*. Dengan mengimplementasikan metode *black box* testing ini cukup efektif apabila dilakukan untuk pengujian jangka pendek karena untuk melakukan metode testing ini cukup menggunakan *tools* yang *open source* maupun dengan *tools* manual lainnya. Oleh karena itu, pada penelitian ini penulis menggunakan *black box testing* karena akses yang diberikan hanyalah sebatas informasi alamat url saja.
Kata Kunci : *Keamanan Website, Penetration Testing, Black Box Testing*

Abstract

Website penetration testing is a test carried out to improve security on the website so that it is not exposed to attacks from outside access rights. Penetration testing has 3 methods of conducting tests including; black box testing, white box testing and gray box testing. Where these three methods have different scope of testing and have their respective advantages and disadvantages. The black box testing method only gets access to information about the website name or URL address, the white box testing access that the tester gets is very complex, because with this method the tester can find out a lot of scope starting from coding, the flow of the application, and access rights enough for testing. Whereas the gray box testing method in this test has access rights that the tester knows about the flow and has an account that can be accessed on the website. Website penetration testing using the black box testing method is a website testing technique to improve website security. By implementing the black box testing method it is quite effective if it is carried out for short-term testing because to carry out this testing method it is sufficient to use open source tools or other manual tools. Therefore, in this study the authors used black box testing because the access provided was only limited to url address information.
Keywords: Website Security, Penetration Testing, Black Box Testing

I. PENDAHULUAN

Penetration testing adalah sub kategori dari *etchical hacking* yaitu sebuah metode dan prosedur yang bertujuan untuk menguji dan melindungi keamanan informasi. *Penetration testing* merupakan aktifitas mengevaluasi sistem keamanan yang sudah dibuat dengan cara melakukan simulasi serangan menggunakan metode yang biasa digunakan oleh peretas. Kegiatan ini perlu mendapat persetujuan legal dari pemilik sistem tersebut. Seperti halnya sekarang sedang terjadi pembololan maupun *hacking* pada perusahaan maupun *website* tertentu yang mengakibatkan kerugian pada pihak yang bersangkutan. Data tersebut dijual dan disalahgunakan oleh pihak tidak berwajib dan diperjualbelikan untuk kepentingan tersendiri. *Penetration Testing* merupakan aktivitas dimana seseorang mencoba melakukan serangan kepada perusahaan dimana serangan tersebut di targetkan kepada jaringan pada perusahaan guna untuk mencari titik lemah maupun kelemahan pada sistem di jaringan perusahaan Hal ini dilakukan bertujuan untuk mengetahui serta menentukan serangan yang mungkin terjadi dan dilakukan terhadap kelemahan maupun celah pada sistem tersebut, dan mengetahui dampak bagi bidang bisnis yang diakibatkan oleh hasil eksploitasi data yang dilakukan oleh penyerang [1]. Oleh karena itu penelitian ini berfokus pada *penetration testing website* dengan metode *black box testing* untuk meningkatkan keamanan *website* pada instansi (*Redacted*).

II. TINJAUAN PUSTAKA

1. *Penetration Test Execution Standard*

Penetration testing execution standard (PTES) ini merupakan acuan yang dibuat dan dikembangkan pada tahun 2010 dan dapat digunakan untuk melakukan penganalisaan dan audit sebuah sistem keamanan *website*, ini umumnya terjadi pada prosedur keamanan, *software*, kontrol sistem internal, atau saat melakukan pemasangan infrastruktur yang dapat meningkatkan integritas, kerahasiaan [2].

2. OWASP Top 10

OWASP Top 10 atau OWASP 10 merupakan sebuah daftar kerentanan yang dirilis oleh komunitas OWASP yang berisi 10 celah keamanan teratas yang dapat mengancam keamanan dari sebuah *website*/aplikasi web. Daftar ini terus berkembang dan berubah-ubah seiring perkembangan teknologi *website*/aplikasi web yang terus berkembang. OWASP Top 10 pertama kali dirilis tahun 2003, lalu dilakukan pembaruan minor pada tahun 2007, 2010, dan 2017. OWASP 10 sendiri sebenarnya sudah memiliki versi terbaru yaitu OWASP 10 2021, namun masih dalam proses pengerjaan yang menyebabkan belum sampai hasil akhir/versi rilis, sehingga dalam pengerjaan proyek ini masih menggunakan OWASP 10 2017. OWASP Top 10 dibuat dengan tujuan untuk meningkatkan kesadaran masyarakat mengenai keamanan aplikasi dengan cara mengidentifikasi beberapa risiko celah keamanan yang sering dihadapi atau ditemui dalam banyak kasus. Berikut contoh risiko kerentanan yang masuk ke dalam OWASP 10 [3].

III. METODE

1. Pendekatan penelitian

Pada penelitian ini dilakukan pendekatan untuk melihat tingkat dari *security* yang ada pada *website* Instansi (*Redacted*), serta bagaimana pengetesan yang dilakukan untuk meningkatan keamanan pada *website* yang nantinya akan disrahkan sepenuhnya ke pihak Instansi (*Redacted*).

Penelitian ini menggunakan penelitian kualitatif. Tujuan seorang peneliti menggunakan metode kualitatif ketika akan melakukan penelitian adalah untuk memahami bagaimana suatu komunitas atau individu-individu dalam menerima isu tertentu. Peneliti juga harus faham dan mengerti serta memiliki pengetahuan memadai terkait permasalahan yang akan ditelitinya. Jika peneliti tidak faham dengan apa yang ingin diteliti maka sebuah penelitian tersebut tidak memenuhi syarat sebagai penelitian kualitatif. Selain itu, peneliti juga mampu mendapatkan *information* yang tepat, membatasi asumsi, dan menulis secara persuasif agar pembaca dapat merasakan pengalaman yang sama.

2. Teknik *Penetration Testing*

Pada penelitian ini peneliti menggunakan metode *penetration testing* dengan standar eksekusinya mengacu pada *Penetration Testing Excecution Standard* (PTES) dimana pada satandar ini terdapat tujuh tahapan yaitu sebagai berikut [4][5]:

a. Tahapan *Pre-engagement*

Pada tahapan ini penulis menjelaskan kepada pihak manajemen metode dan alat yang akan terlibat dalam tes penetrasi, penulis meminta penjelasan kepada pihak manajemen web yang akan di tes penetrasi lalu cakupan dalam melakukan pentest. Setelah mendengar penjelasan pihak manajemen penulis menentukan metode yang akan digunakan dalam tes penetrasi ini dan melakukan perjanjian menjaga kerahasian salah satu standar pentest. setelah hal tersebut manajemen menentukan batasan waktu dalam melakukan tes penetrasi.

b. Tahapan *Intelligence Gathering*

Tahapan ini penulis melakukan pengintaian terhadap target yang telah ditentukan untuk mendapatkan informasi untuk digunakan dalam tes kerentanan dan *exploit.* Target yang diintai lebih sering yaitu domain yang diberikan oleh pihak manajemen. Ditemukan dalam pengintaian domain seperti port yang terbuka, bahasa pemrograman yang digunakan, dan versi *server* yang digunakan. Adapun *tools* yang digunakan dalam melakukan pengintaian.

a. *Scanning* menggunakan NMAP

NMAP merupakan sebuah *tools* digunakan untuk memindai *port* yang terbuka dari IP publik ataupun domain dan dapat digunakan untuk melihat versi dari *port* terbuka. Perintah umum yang digunakan pada NMAP yaitu :

NMAP "IP atau domain target" hasil *scanning* menggunakan perintahnya sebagai berikut.

Gambar 1. Scanning menggunakan NMAP

Menggunakan *tools* NMAP ini penulis menemukan 3 *port* yang terbuka ini menjadi sebuah temuan yang nantinya akan dilakukan eksploitasi untuk mendapatkan hasil yang pasti. NMAP juga dapat melakukan *scanning* terhadap *port* yang sudah terbuka untuk mendapatkan informasi seperti versi dari OS yang digunakan. Versi *database* yang digunankan dan bahasa apa yang digunakan dalam pengembangan sebuah *website*.

c. Tahapan *Threat Modeling*

Penulis pada tahapan *threat modeling* melakukan pemodelan hasil dari pengumpulan informasi sebelumnya telah dikumpulkan. Pemodelan ini diperlukan untuk pelaksanaan pengujian tes penetrasi agar mempermudah penguji dan memberikan pandangan yang akurat untuk manajemen terhadap ancaman mungkin terdapat pada web yang sedang dites.

a. Pemodelan terhadapan ancaman tingkat tinggi.
b. Kumpulkan dokumentasi
c. Mengidentifikasi aset primer dan sekunder
d. Mengkategorikan aset primer dan sekunder
e. Mengidentifikasi ancaman dan komunitas ancaman
f. Mengkategorikan ancaman dan komunitas ancaman
g. Memetakan komunitas ancaman terhadap aset primer dan sekunder

d. Tahapan *Vulnerability Analysis*

Pada tahap *vulnerability analysis* penulis melakukan pengujian kerentanan untuk menemukan kerentanan pada web yang dapat dimanfaatkan oleh penyerang. Kelemahan ini dapat berkisar kesalahan konfigurasi host dan layanan atau desain aplikasi yang tidak aman. Selain itu penulis pun menguji kerentanan terhadap otentikasi web, phising pada web dan mencoba pengunduhan berkas yang tidak sesuai. Apabila pengujian tersebut ada pada web yang di tes penetrasi maka mengindikasikan rentan terhadap hal tersebut.

Alat yang digunakan dalam pengujian kerentanan.

a. Dirb

Sebuah alat yang disediakan oleh OS Linux yang dapat digunakan untuk mengecek direktori. Dirb bekerja dengan teknik *brute forcing* pada web yang diuji dan menganalisa respon web terhadap serangan *brute forcing* yang dilakukan oleh dirb.

Perintah umum pada dirb.

dirb "ip atau host target"

b. Nikto

Suatu *tools* yang digunakan untuk memeriksa *web server open source* yang melakukan pengujian menyeluruh terhadap server web untuk beberapa item termasuk file yang berpotensi berbahaya. Selain itu nikto dapat memeriksa item konfigurasi *server* seperti adanya beberapa file indeks, pilihan *server* HTTP dan mengidentifikasi *server web* dan perangkat lunak yang diinstal. Nikto akan

menguji *web server* dengan waktu cepat dan mendukung anti IDS. Perintah umum yang digunakan pada nikto.

nikto -h "ip atau host target".

e. Tahapan *Exploitation*

Pada tahapan *exploitation* tes penetrasi hanya berfokus dan mendalami hasil pengujian keamanan sebelumnya dengan menggunakan kode yang telah ditentukan untuk memunculkan kerentanan berbahaya yang memungkinkan terjadinya pencurian data sensitif dan memastikan server dapat diakses atau tidak oleh pihak luar. Pada tahapan ini dapat menggunakan alat ataupun secara manual dalam melakukan *eksploit*.

f. Tahapan pelaporan (*Reporting*)

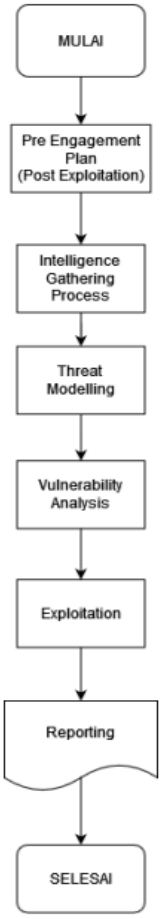
Pada tahapan ini penulis melakukan dokumentasi hasil dari pengujian keamanan dan eksploitasi yang digunakan untuk membuat laporan sebagai cara penyampaian kepada manajemen agar mudah untuk dimengerti. Isi laporan terdiri dari penjelasan mengenai pengertian dari pentest, metode yang digunakan, skala resiko keamanan, penjelasan kerentanan yang ditemukan, dampak dari kerentan tersebut, POC atau langkah-langkah mendapatkan kerentanan tersebut. Penulis menggunakan Kalkulator CVSS sebagai acuan dalam menghitung dampak dari kerentan yang telah ditemukan dan cara mengatasi kerentanan tersebut.

Skala resiko keamanan.

a. *High*
   Komponen indikator *high* harus segera diperbaiki karena sangat rentan atau berpeluang menerima serangan dan juga akan mengganggu performa aplikasi.
b. *Medium*
   Komponen indikator *medium* berarti permasalahan pada internal web seperti ada kerusakan pada sektor data.
c. *Low*
   Komponen indikator *low* terindikasi melakukan sebuah tindakan seperti memperbarui penyimpanan dan sektor-sektor yang diperbaiki.
d. *Information*
   Komponen indikator terindikasi memberi informasi pada web sektor-sektor mana yang tidak memerlukan perbaikan.

3. Diagram Alur Tahapan PTES

Tahapan yang digunakan oleh peneliti dalam melakukan penelitian ini dapat dilihat pada Gambar 2 di bawah ini.



Gambar 2. Diagram Alur PTES

IV. HASIL PENELITIAN DAN PEMBAHASAN

1. Kegiatan penelitian

Penelitian yang dilakukan secara garis besar menjadi beberapa bagian, yaitu dengan cara wawancara dengan pihak terkait untuk melakukan *penetration testing* pada *website* Instansi (*Redacted*) dan menggunakan beberapa pendekatan dengan metode *Penetration Testing Excecution Standard* PTES. Kegiatan ini dimaksudkan untuk mengetahui celah keamanan yang ada pada *website* Instansi (*Redacted*).

Hasil wawancara yang didapat akan dijadikan sebagai bahan rujukan untuk pengujian sistem yang berjalan yang akan dipakai untuk pengeksekusian keamanan diamana ketika telah mengetahui alur yang ada maka akan mempermudah dalam pemerosesan *penetration testing.*

2. Hasil Penelitian

Dari hasil penelitian wawancara dengan pihak Instansi (*Redacted*) penulis mempertimbangkan beberapa pedapat yang dapat di simpulakan bahwasannya *website* yang saat ini digunakan oleh Instansi (*Redacted*) belum aman terutama dalam hal *penetration testing.* Ketidak amanan tersebut bisa dipicu oleh beberapa insiden diantaranya:

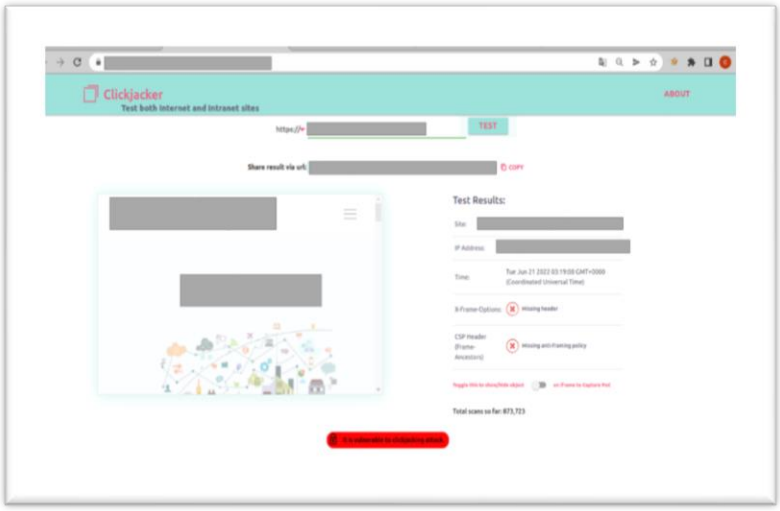
a. Sistem belum melakukan pengetesan seperti (*Penetration Testing).*
b. Sistem merupakan sistem baru.
c. Sistem belum menerapkan keamanan yang baik.
d. Sistem masih harus terus *update* agar tidak terjadi serangan.

Tahapan melakukan pentest ini, penulis mendapatkan beberapa temuan kerentanan pada *website redacted* , yang memungkinkan dapat dimanfaatkan oleh orang yang tidak bertanggung jawab.

3. *Clickjacking*

Penulis menemukan *clickjacking* adalah Jenis serangan pada aplikasi web yang membuat korbannya secara tidak sengaja mengklik elemen halaman web yang sebenarnya tidak ingin di klik. Kerentanan ini memungkinkan web dapat digunakan untuk melakukan *phising*.

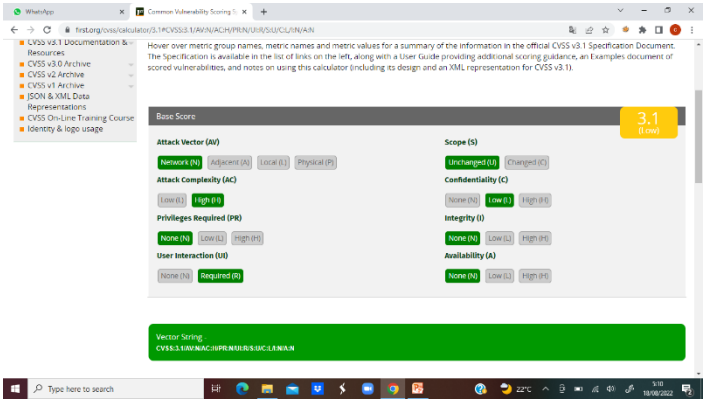
Menemukan kerentanan ini penulis menggunakan sebuah *tools* berbasis web bernama *clickjacker*, pada *tools* ini domain yang telah penulis masukan akan dicek terdapat atau tidak kerentanan *clickjacking*. Hasil pengujian menggunakan *tools* clickjacker.io adalah sebagai berikut.



Gambar 3. Pengetesan Kerentanan *Clickjacking*

a. *Reporting clickjacking*

Tahapan melakukan *reporting* ini, penulis menggunakan sebuah kalkulator CVSS 3.1.



Gambar 4. Hasil Perhitungan Menggunakan CVSS

Pada serangan *clickjacking* didapatkan hasil penilai senilai 3.1 (*Low*) yang digambar pada Gambar 4.3, penulis mendapatkan nilai *low* ini dari hasil kalkulasi berdasarkan *variable Base Score* yang sesuai dengan skenario ketika kerentanan *clickjacking*

Vector String: **CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:N/A:N**

Solusi agar web tidak dapat dibajak dengan menambahkan *header X-Frame Options* untuk menghindari serangan *clickjacking.*

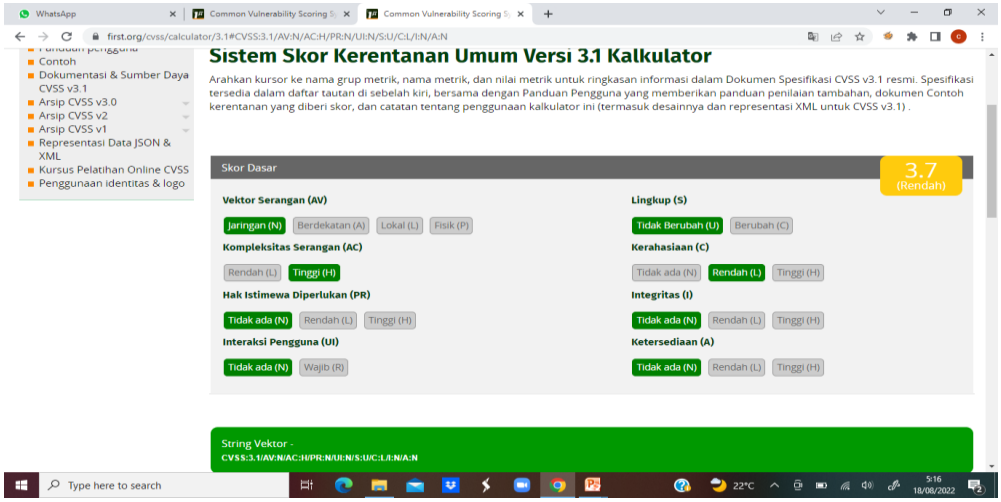
4. *Brute Force Directory*

Penulis menemukan *brute force directory* adalah teknik serangan terhadap sebuah sistem keamanan komputer yang menggunakan percobaan terdiri dari penyerang yang mengonfigurasi nilai yang telah ditentukan, membuat permintaan ke *server* menggunakan nilai tersebut dan kemudian menganalisis responnya. Untuk melakukan serangan ini penulis menggunakan sebuah *tools* bernama dirb, pada *tools* ini akan melakukan sebuah serangan *brute force directory* tanpa harus penulis menambahkan file yang digunakan untuk melakukan serangan tersebut. Penulis melihat respon apabila ada respon yang hasilnya 200 *OK* dapat dipastikan itu celah direktori yang ditemukan. Pada gambar dibawah ini merupakan bukti terdapat celah kerentanan menggunakan dirb.

Gambar 5. Pengetesan Menggunakan *Tools* Dirb

a. Reporting brute force direktori

Tahapan melakukan *reporting* ini, penulis menggunakan sebuah kalkulator CVSS 3.1.



Gambar 6. Hasil Perhitungan Kerentanan Menggunakan CVSS

Pada serangan *brute force directory* didapatkan hasil penilai senilai 3.7(Low) yang digambar pada Gambar 4.5, penulis mendapatkan nilai low ini dari hasil kalkulasi berdasarkan *variable Base Score* yang sesuai dengan skenario ketika kerentanan *brute force directory.*

Vector String: **CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:N**

Solusi agar web tidak dapat diserang menggunakan serangan *brute force directory* gunakan php *brute force attack detector* untuk membantu dengan cepat mengidentifikasi.

V. KESIMPULAN

Berdasarkan pada permasalahan yang ada pada penelitian dan pengujian *website redacted* dapat di simpulkam sebagai berikut:

1. Metode *Penetration Testing Execution Standard* (PTES) layak untuk dijadikan sebuah referensi dalam melakukan kegiatan evaluasi keamanan pada *website* dikarenakan terdapat beberapa kerentanan.
2. *Tools* nikto dan dirb yang digunakan oleh penulis dalam melakukan evaluasi keamanan sangat membantu dalam menemukan beberapa kerentanan yang terdapat pada subdomain *website* perusahaan atau Instansi.
3. Penggunaan CVSS (*Common Vulnerability Scoring System*) oleh penulis sangat membantu untuk menentukan sebuah *severity* dari temuan bug menggunakan CVSS, terlebih karena CVSS adalah standar industri untuk menilai tingkat severity kerentanan keamanan sistem.
4. Terdapat 2 kerentanan yang penulis temukan berdasarkan daftar kategori dari OWASP Top 10 2017, yakni, *Brute Forc*e *Directory* dan *Security Misconfiguration* (*Clickjacking*).

REFERENSI

[1] Hidayat, Saputra, 2018, Anasila dan Problem Solving Keamanan Router Mikrotik RB750RA dan RB750GR3 Deangan Metode *Penetration Testing* (study Kasus: Warnet Aulia.Net, Tanjung Harapan Lampung Timur

[2] Stefanus Eko Prasetyo, Ricky Chandra Lee. (2021) Analisis Keamanan Jaringan Pada Pay2home Menggunakan MetodePenetration Testing, 1(1)

[3] Hidayat, A., & Saputra, I. P. (2018). IMPLEMENTATION VOICE OVER INTERNET PROTOCOL (VOIP) AS A COMMUNICATION MEDIA BETWEEN UNIT AT UNIVERSITY MUHAMMADIYAH METRO. IJISCS (International Journal Of Information System and Computer Science), 2(2), 59- 66.

[4] Denis, M., Zena, C., & Hayajneh, T. (2016). Penetration testing: Concepts, Attack Methods, and Defense Strategies. 2016 IEEE Long Island Systems, Applications and Technology Conference, LISAT 2016. https://doi.org/10.1109/LISAT.2016.7494156.

[5] Sari, D. M., Yamin, M., & Aksara, L. B. (2017). Analisis Sistem Keamanan Jaringan Wireless (WEP, WPAPSK/WPA2PSK) Mac Address, Menggunakan Metode Penetration testing. SemanTIK, 3(2), 203–208. https://doi.org/10.1016/j.neuropharm.2007.08.010.