Pengembangan Laboratorium Virtual untuk Simulasi Uji Penetrasi Sistem Keamanan Jaringan

FahruRoszyMahtuf[1],Puspanda Hatta[2], EndarSuprih Wihidiyat[3]
[1]roszy_fahru@student.uns.ac.id, [2]hatta.puspanda@staff.uns.ac.id, [3]endars@staff.uns.ac.id

Pendidikan Teknik Informatika, Fakultas Keguruan dan Ilmu Pendidikan, Universitas Sebelas Maret

***Abstract*--This study aims to develop a virtualization-based laboratory for simulating penetration tests and comparing the level of performance between physical servers and virtual servers. Development of a virtual laboratory using the VmwareWokstation hypervisor. Penetration simulation testing uses the Information System Security Assessment Framework (ISSAF) guidelines while the Tools used for testing penetration simulations use tools provided in Kali Linux. This study shows that the stages of penetration testing can be done in a virtual environment. Based on the results of the performance level testing shows a comparison of the two server response time levels is quite significant while for physical server throughput 10 times faster than virtual servers. Comparison of CPU enhancements on both servers is also quite significant inversely proportional to the comparison of memory usage on virtual servers 2 times greater than physical servers**

Intisari—Penelitian ini bertujuan untuk mengembangkan sebuah laboratorium berbasis virtualisasi untuk simulasi uji penetrasi dan membandingkan tingkat performa antara server fisik dan server virtual. Tipe Pengembangan laboratorium virtual menggunakan hypervisor Vmware Wokstation. Pengujian simulasi Penetrasi menggunakan pedoman Information System Security Assessment Framework (ISSAF) sedangkan Tools yang digunakan untuk pengujian simulasi penetrasi menggunakan tools yang disediakan pada Kali Linux. Penelitian ini menunjukan jika tahapan-tahapan pengujian penetrasi dapat dilakukan pada lingkungan virtual. Berdasarkan hasil pengujian tingkat performa menunjukkan perbandingan tingkat respon time kedua server cukup signifikan sedangkan untuk throughput server fisik 10 kali lebih cepat dibandingkan server virtual. Perbandingan peningkatan CPU pada kedua server juga cukup signifikan berbanding terbalik dengan Perbandingan penggunaan memory pada server virtual 2 kali lebih besar dari server fisik.

Kata Kunci— Virtualisasi, Virtual Server, ISSAF, UjiPenetrasi, Vmware Workstation.

I. PENDAHULUAN

Kejahatan dunia maya (*Cybercrime*) adalah aktivitas kejahatan dengan komputer atau jaringan komputer yang digunakan sebagai alat dan sasaran terjadinya kejahatan. Data yang dipeloreh pada tahun 2011 kejahatan dunia maya berhasil mencapai angka 520 kasus dan tahun 2012 meningkat menjadi 600 kasus [1]. Untuk memahani pentingnya keamanan sistem perlunya pembelajaran berdasarkan pengalaman yang terkait dengan aksi atau pembelajaran praktis [2]. Pengalaman laboratorium merupakan faktor kunci dalam teknis dan pendidikan ilmiah. Keamanan jaringan dapat dipelajari pada kondisi riil maupun kondisi simulasi.

Kondisi simulasi yang dimaksud adalah kondisi non fisik atau pada kondisi lingkungan virtualisasi. Laboratorium virtual telah diusulkan untuk mengurangi biaya dan menyederhanankan pemeliharaan fasilitas dengan tetap memberikan siswa akses pada sistem yang nyata [3].Laboratotium virtual memberikan banyak manfaat, sumber daya sistem komputer dapat dimanfaatkan secara lebih efektif, beberapa lingkungan dapat dikonfigurasi dengan cepat dan mudah [4].Laboratorium virtual memastikan tidak ada aktivitas pengujian mencapai world wide web yang mencegah aktivitas pengujian secara tidak sengaja menjadi illegal[5].

Pengujian yang dilakukan pada server fisik meliputi pengujian *vulnerability* dan *penetration testing*. Tujuan pengujian adalahmenentukan dan mengetahui macam-macam serangan yangmungkin dilakukan pada sistem serta akibat yang bisa terjadikarena adanya kelemahan keamanan pada sistem komputeratau jaringan yang dimiliki[6]. Laboratorium virtual akan dikembangkan untuk melakukan simulasi pengujian *vulnerability* dan *penetration testing* pada lingkungan virtualisasi.

Laboratorium virtual yang dikembangkan untuk simulasi *penetration testing* memliki dua server virtual yaitu Metasploitable dan Windows Server 2008. Metasploitable digunakan untuk pengujian *penetration testing* sedangkan windows server 2008 digunakan sebagai web server. Perbandingan pengujian antara server fisik dan server virtual terdapat pada jumlah server yang digunakan. Pengujian *vulnerability* dan *penetration testing* pada server fisik memerlukan minimal dua buah server fisik yang digunakan, sedangkan pada server virtual hanya membutuhkan 1 server fisik dan didalam server fisik terdapat beberapa server virtual.

Pengujian penetrasi dan pengujian kerentanan adalah analisis sistematis dari status keamanan sistem informasi pada

server. Pengujian penetrasi merupakan praktik pengujian pada sistem komputer, jaringan dan aplikasi web untuk menentukan kerentanan yang dapat digunakan untuk dimanfaatkan oleh penyerang[7].

Mempelajari etika teknik peretasan menjadi komponen penting dari program keamanan informasi yang bertujuan untuk menghasilkan para professional keamanan informasi yang kompeten[7].

Pengembangan virtual server untuk uji penetrasi memiliki hasil yang cukup baik. Hal ini dibuktikan dengan pengujian penetrasi pada lingkungan virtual menggunakan Oracle VM Virtual Box. Pengujian dilakukan dengan membandingkan hasil exploit sistem server virtual dengan metaploit dan armitage. Hasil penelitian menunjukan metasploit dan armitage dapat melakukan uji penetrasi pada lingkungan virtual [8].

Penelitian lain yang dilakukan dengan mengembangkan kurikulum *penetration testing* baru sebagai modul pembelajaran. Media yang digunakan untuk melakukan latihan modul *penetration testing* menggunakan virtual laboratorium. Berdasarkan feedback dari siswa 67% setuju memahami konsep dari *penetration testing*.[9].

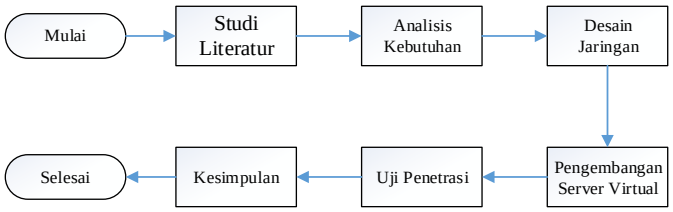
Penelitian lain dilakukan dengan mengembangkan laboratorium virtual sebagai media belajar kurikulum keamanan informasi. Pengembangan virtual server yang dilakukan menggunakan VMware wokstation , pengujian yang dilakukan hanya melakukan scanning kerentanan pada server [10].

Dari beberapa penelitian ditunjukkan bahwa uji penetrasi pada lingkungan virtual dapat dilakukan dengan baik [7][8][9]. Maka dari itu penelitin ini bertujuan untuk membangun laboratorium virtual (virtual server) untuk simulasi uji penetrasi dengan metode *penetration testing*. Penelitian juga menambahkan pengujian untuk mengukur perbandingan antara server fisik dan virtual. Perbandingan yang digunakan adalah perbandingan penggunaan resource CPU dan Memory. Penelitian juga membandingkan tingkat Respon Time dan Throuhput.

II. METODE PENELITIAN

Alur Penelitian

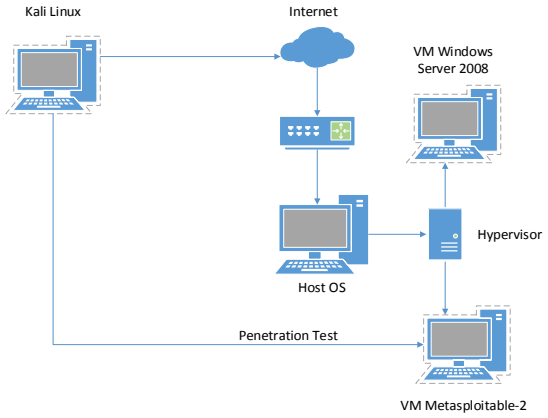
Dalampenelitianini,terdapat diagram alursebagaipedomandalam pengerjaan penelitian ini. Penelitian ini menggunakan ISSAF 0.2.1B tentang metodologi *penetration testing*. ISSAF memiliki beberapa kelebihan kontrol keamanan. ISSAF memiliki struktur yang jelas dan intuitif yang memandu penguji melalui langkah-langkah yang rumit [11]. Metodologi ini menjelaskan proses pengujian penetrasiyang optimal untuk membantu penguji melakukan pengujiansecara lengkap dan benar, menghindari kesalahan yangumumnya terkait dengan strategi serangan yang dipilih secaraacak Diagram penelitian ini dapat dilihat pada Gambar 1.



Gambar.1 Diagram Alur Penelitian

Desain Topologi

Topologi jaringan terdiri dari satu perangkat komputer atau laptop yang terhubung langsung dengan internet. Komputer berfungsi sebagai Host Os yang digunakan untuk menginstall Hypervisor. Hypervisor yang digunakan untuk pengembangan laboratorium virtual adalah VMware Workstation yang berfungsi sebagai tempat untuk membangun virtual server pada server fisik. Topologi jaringan pengembangan virtual server digambarkan pada Gambar 2.



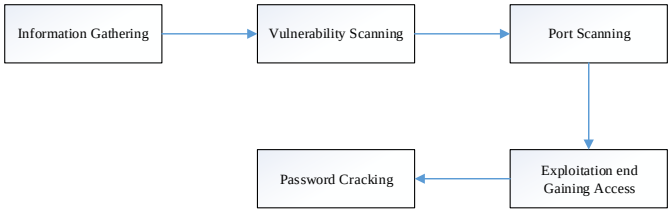
Gambar.2 TopologiJaringan

Pada Gambar 2 Topologi Jaringan, pengembangan laboratorium virtual menggunakan teknik virtualisasi tipe II yaitu hypervisor VMware Workstation berjalan diatas sistem operasi. Laboratorium virtual yang dikembangkan memiliki 2 buah virtual machine yang akan dikembangkan yaitu Metasploitable-2 dan Windows Server 2008. Kali Linux digunakan sebagai komputer penyerang karena memiliki tools-tools peretasan yang lumayan lengkap.

Tahap Uji Penetrasi

Pada tahap ini dilakukan uji penetrasi pada server virtual yang sudah dikembangkan. Server yang digunakan untuk target uji penetrasi adalah metasploitable-2 karena dikhususkan untuk latihan uji penetrasi dan komputer penyerang menggunakan kali linux. Tahap pengujian penetrasi dibagi menjadi 5 yaitu tahap awal adalah mengumpulkan informasi, pemetaan jaringan, indentifikasi kerentanan,

eksploitasi, mendapatkan akses dan password cracking. Tahapan uji penetrasi dapat dilihat pada Gambar.3.



Gambar.3. Tahap Uji Penetrasi

Uji Kinerja Server

Selain pengujian uji penetrasi, kinerja dari server virtual yang dikembangkan perlu diuji untuk memperoleh data yang dapat digunakan untuk melakukan perbadingan dengan server non virtual. Pengujian kinerja server dilakukan untuk mengukur nilai Respon Time, Throughput, penggunaan Memory dan penggunaan CPU. Data yang diperoleh digunakan untuk melakukan perbandingan antara server virtual dan server non virtual. Pengujian dilakukan dengan mengirimkan 10 paket pada server dengan beban yang berbeda pada setiap paket yang dikirim.

III. HASIL DAN PEMBAHASAN

Penetration testing menunjukan hal-hal yang dilakukan sebelum dan proses pengujian keamanan pada server. Pada penelitian ini pengujian penetrasi berfokus pada technical control assessment. Berikut merupakan tahapan pada pengujian *penetration testing* yang dilakukan.

Information gathering

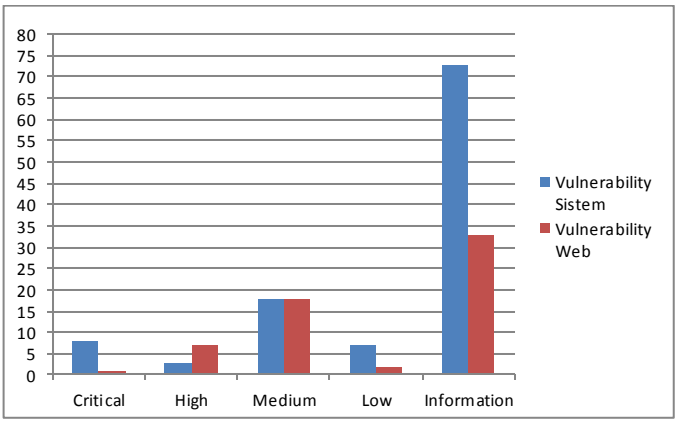
Tahap *information gathering* ini digunakan untuk mencari informasi awal yang dibutuhkan untuk melakukan tahap selanjutnya. Informasi yang dibutuhkan berupa ip address dari server metasploitable-2. Ip address yang didapatkan digunakan untuk melakukan *vulnerability scanning* dan *port scanning*,*information gathering* yang dilakukan menggunakan tools netdiscover. Hasil dari *information gathering* dapat dilihat pada Tabel.2.

Tabel 2. Hasil *Information gathering*

IP	At *Mac address*
192.168.76.1	00:50:56:c0:00:08
192.168.76.2	00:50:56:e7:c0:b2
192.168.76.128	00:0c:29:10:a0:75
192.168.76.130	00:0c:30:20:b0;85
192.168.76.254	00:50:56:e8:bd:47

Vulnerability scanning

Tahap *vulnerability scanning* digunakan untuk mencari celah keamanan pada server metasploitable-2 dengan menggunakan ip address server 192.168.76.128 yang berhasil didapatkan pada tahap *information gathering*. Hasil pengujian berupa jumlah kerentanan sistem dan kerentanan web yang dapat ditemukan menggunakan tools Nessus. Hasil pengujian *vulnerability* dapat dilihat pada Gambar 4.



Gambar 4. Hasil *Vulnerability scanning*

Berdasarkan hasil pengujian pada Gambar.4, hasil analisis dari server metasploitable-2 memiliki kerentanan sistem 8 kerentanan tingkat kritikal, 3 kerentanan tingkat tinggi, 18 kerentanan tingkat medium, 7 kerentanan tingkat rendah, 73 kerentanan tingkat informasi. Kerentanan pada web yang ditemukan memiliki 1 kerentanan tingkat kritikal, 7 kerentanan tingkat tinggi, 18 kerentanan tingkat medium, 2 kerentanan tingkat rendah dan 33 kerentanan tingkat informasi.

Port scanning

Tahap *port scanning* bertujuan untuk menemukan celah keamanan yang berada pada server dengan mencari port yang berstatus terbuka pada server. Celah keamanan yang dicari pada tahap *port scanning* ada 4 jenis yaitu port, status, service yang berjalan dan versi dari sistem operasi yang digunakan. Celah keamanan yang ditemukan digunakan untuk melakukan peretasan pada sistem server. Celah keamanan juga digunakan untuk melakukan planning untuk menentukan jenis serangan dan tools yang akan digunakan untuk melakukan serangan pada sistem server. Proses tahap *port scanning* dapat dilihat pada Gambar 5.

```
root@Attacker:~# nmap -F -sV -O 192.168.76.128

Starting Nmap 7.60 ( https://nmap.org ) at 2018-03-02 04:34 PST
Nmap scan report for 192.168.76.128
Host is up (0.017s latency).
Not shown: 64 filtered ports
PORT     STATE  SERVICE        VERSION
7/tcp    closed echo
13/tcp   closed daytime
21/tcp   open   ftp            vsftpd 2.3.4
22/tcp   open   ssh            OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp   open   telnet         Linux telnetd
25/tcp   open   smtp           Postfix smtpd
53/tcp   open   domain         ISC BIND 9.4.2
79/tcp   closed finger
80/tcp   open   http           Apache httpd 2.2.8 ((Ubuntu) DAV/2)
```

Gambar 5. Proses *Port scanning*

p-ISSN: 2541-3619
e-ISSN: 2541-6448

Exploitation* dan *Gaining access

Tahap *exploitation* dan *gaining access* merupakan tahap yang bertujuan untuk masuk pada sistem server dan mencari informasi yang berada pada server. Tahap *exploitation* dan gaining acces dilakukan melalui celah keamanan atau kerentanan yang ditemukan pada tahap *port scanning*. Metode peretasan dan tools yang digunakan disesuaikan dengan celah atau kerentanan yang berhasil ditemukan. Salah satu proses tahap *exploitation* dan *gaining access* pada celah yang ditemukan pada phpmysql dapat dilihat pada Gambar 6.

```
root@Attacker:~# mysql -u root -p -h 192.168.76.128
Enter password:
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MySQL connection id is 9
Server version: 5.0.51a-3ubuntu5 (Ubuntu)

Copyright (c) 2000, 2017, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MySQL [(none)]> show databases;
+--------------------+
| Database           |
+--------------------+
```

Gambar 6. Proses Exploitaion database MySQL

Peretasan Password

Tahap peretasan password merupakan tahapan tahapan mencari password yang berada pada server. Beberapa teknik dapat digunakan untuk melakukan tahap peretasan password antara lain : Dictionary attack, brute force, phising dan masih banyak teknik yang bisa digunakan. Tahap peretasan password dapat dilihat pada Gambar 7.

```
root@Attacker:~# unshadow
Usage: unshadow PASSWORD-FILE SHADOW-FILE
root@Attacker:~# unshadow /root/Password/passwd /root/Password/shadow > mypassword
root@Attacker:~# john -show mypassword
0 password hashes cracked, 7 left
root@Attacker:~# john mypassword
Warning: detected hash type "md5crypt", but the string is also recognized as "aix-smd5"
Use the "--format=aix-smd5" option to force loading these as that type instead
Using default input encoding: UTF-8
Loaded 7 password hashes with 7 different salts (md5crypt, crypt(3) $1$ [MD5 128/128 AVX 4x3])
Press 'q' or Ctrl-C to abort, almost any other key for status
postgres         (postgres)
```

Gambar 7. Proses Peretasan Password

Perbandingan Server Fisik dan Virtual

Perbandingan antara server fisik dan server laboratorium virtual (virtual server) dilakukan dengan membandingkan respon time dan throughput antara web server yang berada pada server fisik dan server virtual. Pengujian dilakukan dengan mengirimkan paket request pada web server sebanyak 10 kali dengan jumlah request yang berbeda. Hasil pengujian respon time webserver dapat dilihat pada Tabel 3.

Tabel 3. Hasil Respone Time Webserver

Httpef	Respon Time (duration test/second)	
	Server Virtual	Server Fisik
100	9.932	9.901
200	19.933	19.900
300	29.928	29.901
400	39.948	39.901
500	49.915	49.981
600	60.517	59.901
700	69.928	69.901
800	79.928	79.981
900	91.351	89.902
1000	102.109	99.901

Berdasarkan Tabel 3, dapat diketahui respon time rata dari kedua webserver. Webserver pada server fisik memiliki rata-rata respon time sebesar 54.912 dan webserver pada virtual server sebesar 55.349. Perbandingan rata-rata respon time antara server fisik dan server virtual cukup signifikan.

Tabel 4. Perbandingan Throughput Web Server

Httperf	Throughput (Kbps/s)	
	Server Virtual	Server Fisik
100	11.1	100.7
200	11.1	100.1
300	11.1	100
400	11.1	107.9
500	11.1	107.8
600	11	107.8
700	11.1	107.8
800	11.1	107.7
900	10.9	107.7
1000	10.9	107.7

Berdasarkan Tabel 4. hasil pengujian throughput pada Tabel 4 dapat diketahui perbedaan throughput antara server virtual dan server fisik. Perbandingan rata-rata throughput antara server virtual dan server fisik adalah 11.05 Kbps/s dan 105.52 Kbps/s. Perbandingan rata-rata throughput server fisik 10 kali lebih cepat dibandingkan dengan server virtual.

Tabel 5. Perbandingan Memory Server Virtual dan Fisik

Httperf	Penggunaan Memory (Mb)			
	Virtual Server	%	Server Fisik	%
100	399.644	77.53	584.84	34.17
200	404.476	78.47	585.468	34.21
300	409.240	79.40	586.568	34.27
400	407.936	79.14	587.176	34.31
500	408.812	79.31	589.26	24.43
600	410.432	79.63	590.62	34.51
700	408.82	79.31	592.832	34.64
800	408.944	79.34	594.112	34.72
900	409.06	79.36	597.056	34.89
1000	409.704	79.49	598.938	35

p-ISSN: 2541-3619
e-ISSN: 2541-6448

Berdasarkan Tabel 5 perbandingan penggunaan memory pada saat pengujian menggunakan hhtperf dengan 10 kali pengujian dan beban request yang berbeda dapat dilihat penggunaan rata-rata memory server virtual 79.10 % dan rata-rata penggunaan memory pada server fisik 34.52 %. Perbandingan rata-rata penggunaan memory server virtual 2 kali lebih besar jika dibandingkan dengan penggunaan memory pada server fisik.

Tabel 6. Perbandingan CPU

Httperf	Penggunaan CPU (%)	
	Server Virtual	Server Fisik
100	12	2.77
200	12.3	5.77
300	12.7	10.1
400	13.3	14.29
500	13.9	14.94
600	14	14
700	14.3	20.88
800	14.9	22.48
900	15.3	24.96
1000	15.7	28.89

Berdasarkan Tabel 6 Perbandingan peningkatan CPU dapat diketahui penggunaan rata-rata cpu pada server virtual 13.84 % dan penggunaan rata-rata cpu pada server fisik 15.905 %. Perbandingan rata-rata penggunaan resource cpu pada server fisik dan virtual cukup signifikan jika dilihat pada Tabel 6.

IV. KESIMPULAN DAN SARAN

Penelitian ini menunjukan bahwa simulasi uji penetrasi pada lingkungan virtual dapat dilakukan sesuai dengan tahapan uji penetrasi pada kondisi non virtual. Ini dibuktikan dengan tahapan – tahapan uji penetrasi berhasil dilakukan pada server virtual. Pada pengujian respon time dan penggunaan CPU pada server fisik dan virtual mempunyai perbedaan tingkat respon time dan CPU yang cukup signifikan, sedangkan pada pengujian throughput server fisik 10 kali lebih cepat dibandingkan throughput pada server virtual. Hal ini berbanding terbalik pada penggunaan memory, server virtual 2 kali lebih besar pemakaian memory dibandingkan pada server fisik. Berdasarkan hasil pengujian dapat ditunjukkan bahwa Teknik virtualisasi dapat dimanfaatkan untuk mengoptimalkan penggunaan cpu dan memory.

DAFTAR PUSTAKA

[1] Pirmansyah, "Analisis Persepsi Auditor Sistem Informasi mengenai Pencegahan atas Tindakan Cybercrime.

[2] Moon,J. A Handbook of Reflective and Experiential Learning:Theory andpractice.London:Routledge Falmer.pp.126.2004

[3] Wolf. Tilman, "Assessing Sudent Learning in Virtual Laboratory Environment. IEEE Transcalation on Education", Vol. 53, No.2, pp. 216-221, 2010.

[4] Bulbrook. Harry, "Using Virtual Machine to provide a secure Teaching Lab environmnet,". 2009.

[5] Arjun, CV 2017, '*Penetration testing*: *Vulnerability* analysis in a virtual environment' *Journal of Engineering and Applied Sciences*, vol. 12, no. Specialissue9, pp. 8723-8729. DOI: 10.3923/jeasci.2017.8723.8729

[6] Trabelsi Z. and McCoey M., "Ethical hacking in information security curricula," International Journal of Information and Communication Technology Education (IJICTE), Vol. 12, Issue 1, pp. 1-10, 2016.

[7] Ankita Gupta, Kavita, kirandeep Kaur.*"VulnerabilityAssessment and Penetration testing". Computer ScienceDepartment, PEC University of Technology, India*∗*Electronics and Electrical Communication Depertement,PEC University of Technology, India IJETT Vol 4Issue3 - 2013*

[8] S. Christoper, Z. Janusz, *Penetration testing in a Virtual Environment*. CNT 4104 Fall Networks, 2011

[9] Li, C. (2015). *Penetration testing* curriculum development in practice. *Journal of Information Technology Education: Innovations in Practice, 14*, 85-99. Retrieved from http://www.jite.org/documents/Vol14/JITEv14IIPp085-099Li1014.pdf

[10] Bulbrook.H, "Using Virtual Machine to provides a secure Teaching Lab Environment."

[11] Hutagalung. R. H, Nugroho. L. E and Hidayat. R, "Analisis Uji Penetrasi Menggunakan ISSAF", ISSN : 2338 - 0276, 2017.

[12] T. Edition, *Top-Down Network Design*. .

p-ISSN: 2541-3619
e-ISSN: 2541-6448