

Analisis Keamanan Website dengan Metode *Penetration Testing* pada PT. PLN (Persero)

Muhammad Rifaldi Umasugi^a, Ramdan Satra^b, Andi Widya Mufila Gaffar^c

Universitas Muslim Indonesia, Makassar, Indonesia

^arifaldi0907@umi.ac.id; ^bramdan@umi.ac.id; ^cwidya.mufila@umi.ac.id

Received: xx xx xxxx | Revised: xx xx xxxx | Accepted: xx xx xxxx | Published: xx xx xxxx

Abstrak

PT. PLN (Persero) Pusmanpro - Unit Pelaksanaan Manajemen Konstruksi V Makassar beralamat di jl. Prof. Abdurahman Basalamah, Komplek Perumahan PLN, Kota Makassar, Sulawesi Selatan. Adapun permasalahan yang terjadi terhadap beberapa ancaman keamanan komputer seperti virus, worm, Trojan, spam serta tindakan merugikan dari para cracker ataupun heacker, dimana masing-masing memiliki cara untuk mencuri data dan merusak sistem. Proses *penetration testing* dalam hal ini melibatkan proses analisis kepada sebuah sistem untuk mencari potensi celah keamanan seperti kesalahan konfigurasi sistem. Berdasarkan hasil pengujian kerentanan sistem dengan menggunakan metode *penetration testing* penulis mendapatkan beberapa seperti security website yang terdapat pada situs <https://pln.co.id> telah menerapkan pengamanan yang cukup baik sehingga hanya ditemukan beberapa kerentanan yang tidak begitu berdampak buruk bagi sistem. Dari pengujian yang telah dilakukan maka dapat diambil kesimpulan bahwa seluruh tahapan penelitian telah dilakukan mulai dari tahapan menggali informasi, analisis hingga tahap pengujian untuk mencari kerentanan yang tersedia. penelitian hanya menggunakan beberapa teknik exploit yang dilakukan. Adapun hasil pengujian menggunakan metode *penetration testing* dapat mendeteksi celah keamanan pada website PT. PLN (Persero) Pusmanpro – Unit Pelaksanaan Manajemen Konstruksi V Makassar.

Kata kunci: *Penetration testing*, Website, PLN, Security

Pendahuluan

PT. PLN (Persero) Pusmanpro - Unit Pelaksanaan Manajemen Konstruksi V Makassar beralamat di jl. Prof. Abdurahman Basalamah, Komplek Perumahan PLN, Kota Makassar, Sulawesi Selatan. PT. PLN memiliki website yang bertujuan untuk menjadi wadah berupa media komunikasi, penyampaian berita, ataupun media penerima informasi bagi masyarakat untuk memahami hal-hal seputar perusahaan listrik negara (PLN) sebagai pengelola tenaga listrik milik negara. Adapun permasalahan yang terjadi terhadap beberapa ancaman keamanan komputer seperti virus, worm, Trojan, spam serta tindakan merugikan dari para cracker ataupun heacker, dimana masing-masing memiliki cara untuk mencuri data dan merusak sistem. Dengan adanya permasalahan tersebut maka tindakan yang diperlukan saat ini adalah membantu meminimalisir dan mengantisipasi server induk pada PLN dari kejahatan hacking. Salah satu hal yang dapat dilakukan adalah melakukan monitor pada server induk PLN yang berada didalam gedung server dan melakukan pengujian atau analisa percobaan pada sistem yang telah diterapkan.

Penelitian terkait tentang implementasi Keamanan Jaringan VLAN dan VoIP menggunakan firewall dapat disimpulkan bahwa Panggilan suara pada VoIP berhasil mengirimkan suara antara user dalam VLAN berbeda terlihat pada hasil pengujian VLAN suara antar client berhasil terdengar, client dapat terhubung dan melakukan komunikasi sesama VLAN. Berdasarkan hasil pengujian firewall terlihat sistem mampu memblokir pengguna yang tidak terdaftar dalam router [1]. Adapun penelitian lain yang dilakukan mengenai salah satu pemeringkatan website yang populer dan terbesar di Indonesia adalah Webometrics, dimana penelitian ini dilakukan untuk menganalisa pemeringkatan Webometrics pada manajemen pengelolaan website pada UPT.PJP UMI yang masih terdapat permasalahan yang salah satunya pada aspek performa [2]. Selanjutnya yaitu pada tahun 2017 menghasilkan pengujian keamanan website dapat dilakukan dengan cara *Vulnerability Assessment* menggunakan aplikasi *acunetix*. Menentukan keamanan sebuah website dapat ditentukan dengan menggunakan *security metrics* yang dapat menampilkan hasil berlabel *High*, *Medium* atau *Low* yang ditentukan dengan menggunakan rumus *BaseScore* yang menghasilkan jumlah hasil 1-10 [3].

Selanjutnya yaitu pada tahun 2021 menghasilkan celah keamanan (*vulnerability testing*) dan pengujian

celah keamanan (*penetration testing*) ditemukan beberapa kelemahan yang terdapat pada website target. Kelemahan tersebut dapat *dieksploitasi* hingga database target dapat diakses oleh pihak yang tidak berwenang atau tidak memiliki hak akses [4]. Terakhir yaitu pada tahun 2021 menghasilkan keamanan website utama Institusi Universitas Internasional Batam www.uib.ac.id tergolong cukup aman dari serangan hacker. Dari 4 tahap pengujian menggunakan metode ISSAF didapati pada tahap *penetration DDOS Attack* website utama masih bisa ditembus dan mengakibatkan server down sementara [5].

Berdasarkan permasalahan dan penelitian sebelumnya, maka peneliti mengusulkan penelitian dengan menggunakan metode *Penetration Testing*, yang bertujuan melakukan analisis terhadap sistem keamanan website yang sudah diterapkan di PT. PLN (Persero) Pusmanpro UPMK V Makassar. Tujuan PT. PLN melakukan *penetration testing* karena masih memiliki banyak celah untuk dieksploitasi dimana hasil penelitian yang dilakukan bahwa dari empat jenis serangan yaitu *Analisa Lalulintas Jaringan (Traffic Network)* Menggunakan *Wireshark*, *Cracking The Encryption*, dan *Man In The Middle*, website belum memberi keamanan kepada user agar tidak mendapatkan gangguan pada saat menggunakan website.

Metode

Penetration And Vulnerability testing server sistem ini memang diperlukan. Hal ini dikarenakan server sistem informasi tersebut memegang peranan yang sangat penting pada perusahaan maupun instansi tertentu [6]. *Penetration And Vulnerability testing server* yang dilakukan yaitu dengan tujuan untuk mengetahui apakah terdapat celah-celah kerentanan pada sistem yang sudah diterapkan. Dari *range IP address* yang di-scanning, nantinya akan diketahui *IP address* yang mempunyai *NetBIOS* info dan yang tidak mempunyai *NetBIOS* info [7]. *Penetration testing* merupakan suatu aktivitas proses mensimulasikan serangan terhadap jaringan organisasi/perusahaan tertentu untuk menemukan kelemahan yang ada pada sistem jaringan tersebut [8]. Uji penetrasi dilakukan untuk mengukur dampak dan kemungkinan kerentanan sehingga memungkinkan organisasi untuk memprioritaskan langkah-langkah korektif untuk perbaikan sistem. Proses uji memerlukan banyak waktu, tenaga dan pengetahuan dalam menangani kompleksitas ruang pengujian [9]. *Penetration testing* metode yang dapat digunakan untuk menguji keamanan sistem sehingga kerentanan dalam aplikasi web dapat teridentifikasi yang selanjutnya digunakan untuk menutup celah keamanan tersebut [10].

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 [11]. Strategi keamanan informasi melalui indentifikasi kerentanan yang cepat dan akurat, penghapusan proaktif dari risiko yang teridentifikasi, pelaksanaan tindakan korektif, dan peningkatan pengetahuan TI [12]. Proses *penetration testing* dengan melibatkan proses analisis kepada sebuah sistem untuk mencari potensi celah keamanan seperti kesalahan konfigurasi sistem, cacat dalam pengembangan *software* maupun *hardware* dan kelemahan dalam logika dari sebuah proses [13]. Istilah *Penetration testing* atau yang lebih dikenal dengan *penetrasi* adalah serangkaian kegiatan yang dilakukan untuk mengidentifikasi dan mengeksploitasi kerentanan yang ada [14].

Perancangan

Dalam penelitian ini, program aplikasi (*tool*) yang digunakan adalah program yang sesuai dengan langkah *penetration testing*. *Tool* yang digunakan ada yang didapatkan melalui cara download dari internet maupun dari buku CEH (Certified Ethical Hacker) sendiri. Pada Tabel 1 dapat dilihat sistem (*tool*) yang digunakan untuk *penetration testing* dalam pengerjaan penelitian.

Tabel 1. Tahapan Penelitian

NO	STEP (METODE)	TOOLS
1.	Footprinting	Angry IP Scanner atau Nmap
2.	Scanning Fingerprinting And Enumeration	Acunetix Web VulnerabilityScanner 9.5, OpenVAS atauNessus
3.	Exploit	Sqlmap

4.	Reporting	Acunetix & Manual
----	-----------	-------------------

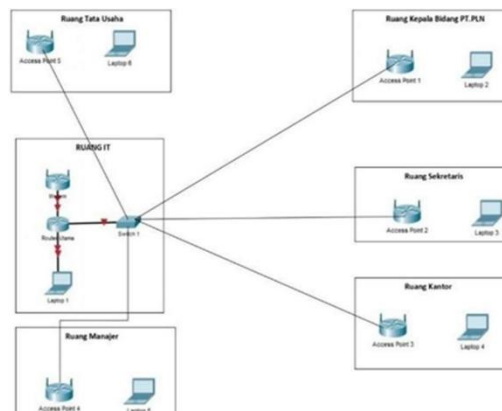
Alur Pengujian



Gambar 1. Alur Pengujian *Penetration Testing*

Gambar 1. Merupakan penjelasan singkat terhadap langkah – langkah penulis dalam melakukan *penetration testing*. Tahap awal dalam melakukan *penetration testing* yaitu *start* atau memulai, selanjutnya yaitu *Footprinting* yang dimana pada tahap ini penulis harus menggali informasi mengenai target, setelah mendapatkan informasi penulis akan melakukan langkah *Scanning fingerprint And Enumeration* untuk mencari dan menampilkan *rage IP Address*, menemukan *Vulnerability*, dan mengevaluasi *port* yang terbuka untuk di cocokan dengan *IP Address*. Berikutnya yaitu tahap *Exploit* yang menjadi langkah kunci untuk pengujian dengan melakukan penyerangan terhadap website yang di targetkan dalam melakukan *penetration testing*, setelah itu penulis akan melakukan pelaporan atau *Reporting* kepada pemilik website (*Developer*) agar melakukan tindakan pengamanan *extra* pada websitenya agar lebih aman jikalau terdapat kelemahan pada website tersebut.

A. Topologi



Gambar 2. Topologi Jaringan Fisik PLN

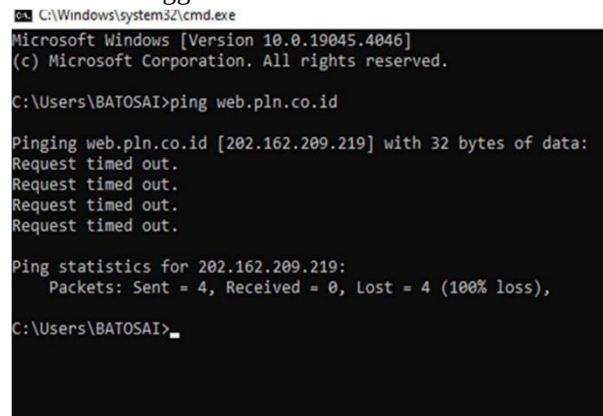
Dalam perancangan topologi, kantor PT. PLN (Persero) UPMK V Makassar menggunakan jaringan kabel pada setiap ruangan, yang dimana setiap ruangan memiliki *Access Point* yang bersumber dari server yang berada di ruangan IT PLN. Topologi yang digunakan adalah topologi star, yaitu topologi yang menggambarkan sistem jaringan dari beberapa komputer yang memiliki koneksi dengan *node* (komputer pribadi) yang berada di tengah dan menjadi pusat segala aktivitas sistem jaringan, Prosesnya dapat dilihat pada Gambar 2.

Pemodelan

A. *Footprinting*

Footprinting sebagai tahapan awal yang akan dilakukan oleh penulis dalam melakukan *Penetration and Vulnerability Testing* guna menggali informasi sebanyak mungkin mengenai target yang telah ditentukan seperti *Whois*, *NSLookup*, *Mapping Network* dan informasi lainnya yang dibutuhkan. Dalam tahapan ini, peneliti akan menggunakan beberapa *tool software* maupun *tool online scanner* untuk dapat melakukannya seperti *tools NMAP*.

Pada tahap ini, Penulis menggunakan *Command Prompt (CMD)* sebagai langkah awal untuk melihat *IP Public* dari web.pln.co.id, yang dimana *IP* website yang telah diketahui akan digunakan dalam tahap analisa lebih mendalam menggunakan *tool NMAP*.



```
C:\Windows\system32\cmd.exe
Microsoft Windows [Version 10.0.19045.4046]
(c) Microsoft Corporation. All rights reserved.

C:\Users\BATOSAI>ping web.pln.co.id

Pinging web.pln.co.id [202.162.209.219] with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 202.162.209.219:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\Users\BATOSAI>
```

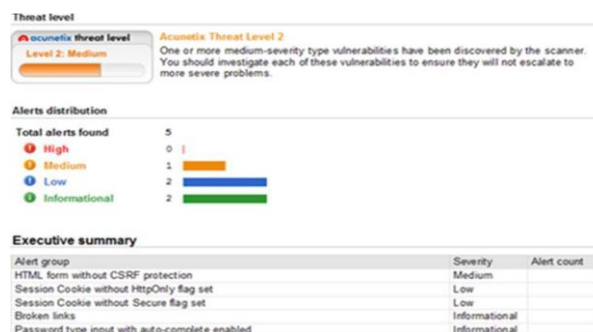
Gambar 3. Menulis perintah dan Mendapatkan *IP Public*

Setelah memasukan perintah pada *Command Prompt* yang dapat dilihat pada Gambar 3, penulis mendapatkan *IP Public* website yaitu 202.162.209.219.

B. *Scanning Fingerprinting and Enumeration*

a. *Scanning fingerprint*

Langkah *scanning fingerprinting* ini akan menggunakan *tool Acunetix Web Vulnerability*, dimana *tool* ini dapat digunakan pada sistem operasi linux maupun windows, *tool* ini dapat menampilkan dari suatu *range IP Address*, sebagai administrator *tool* ini akan membantu dalam menemukan *vulnerability* dalam jaringan (*IP Address* atau *hostname*). Selain menampilkan kelemahan dari suatu *source*, *tool* ini akan menampilkan level tingkat kelemahan dari *alerts (vulnerability)* yang ditemukan.



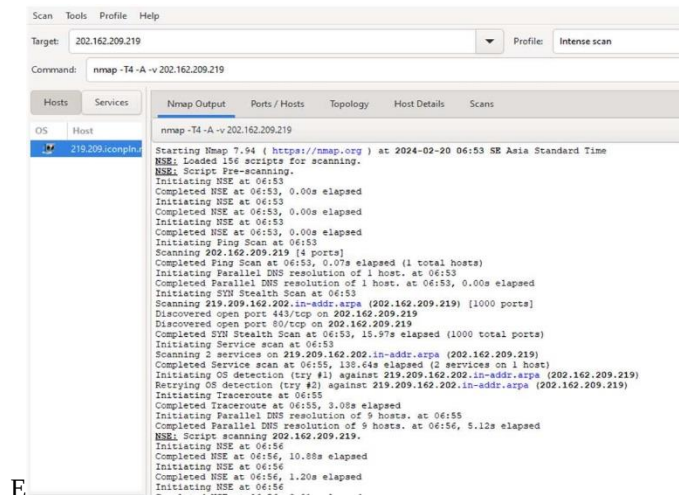
Gambar 4. Hasil Scanning tool Acunetix

Pada tahapan melakukan langkah *scanning web vulnerability* menggunakan *tool acunetix*, peneliti mendapatkan berbagai informasi kerentanan atau celah yang terdapat pada situs <https://pln.co.id>. Dengan demikian hasil tersebut kemungkinan dapat di eksploitasi dengan berbagai cara serta teknik yang sesuai dengan berbagai level kerentanan (*vulnerability*) yang ada. Hasil dapat dilihat pada Gambar 4.

b. *Enumeration*

Langkah *enumeration* ini akan menggunakan *NMAP Scanner* di mana *tool* ini dapat menampilkan detail dari suatu *range IP Address*, seperti *port* apa saja yang terbuka, terfilter atau tertutup dari suatu *IP Address*. Jadi sebagai seorang tester, akan mendapatkan dan mengevaluasi *port* yang

terbuka apakah *port* tersebut cocok dengan *IP Address* yang terkait. Dengan hasil *enumeration* juga langsung dilanjutkan ke arah *scanning web vulnerability* untuk mendapatkan seluruh informasi mengenai celah atau kerentanan apa saja yang didapat dari hasil *scanning* tersebut.



Gambar 5. Hasil Scanning NMAP

c. *Exploit*

Langkah *exploit*, pada tahapan ini penulis akan melakukan penyerangan pada sebuah *website* sederhana yang telah dibuat dengan tujuan membuat simulasi bagaimana cara melakukan serangan pada sebuah *website*, dengan menggunakan *Operating System Kali Linux* dan beberapa *tools* yaitu *NMAP* untuk melihat kerentanannya serta melakukan penyerangan pada *database* dengan menggunakan *SQL Injection*.

1. Langkah pertama yaitu dengan menjalankan *Operating System Kali Linux* yang telah terinstall menggunakan *VirtualBox*.



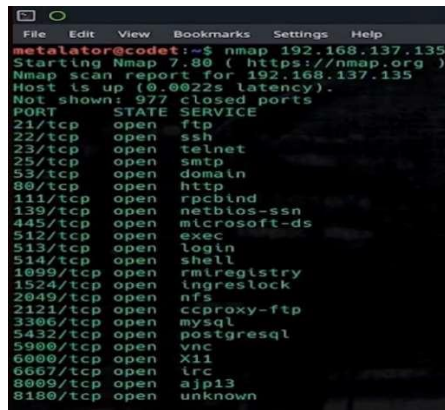
Gambar 6. Tampilan Awal Dari Kali Linux

2. Buka *Browser* yang ada pada *Operating System Kali Linux* untuk mencari *website* yang akan di jadikan target dalam melakukan penyerangan.



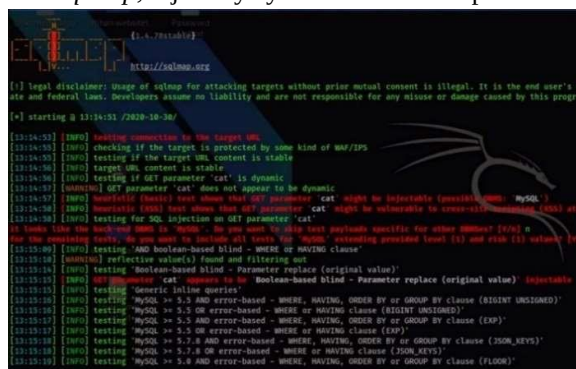
Gambar 7. Tampilan Website Target

3. Selanjutnya penulis akan membuka terminal pada *Kali Linux* dan masukan perintah untuk menjalankan *tool NMAP* agar dapat melihat *port* apa saja yang terbuka dari *ip website* tersebut.



Gambar 8. Hasil *scanner* NMAP

4. Pada tahap ini penulis akan mencoba melakukan serangan menggunakan *SQL Injection* dengan nama *tool sqlmap*, tujuannya yaitu untuk mendapatkan *database* dari *website* target.



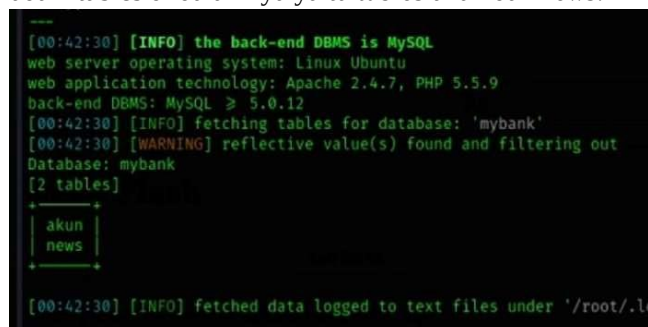
Gambar 9. Menjalankan *tool sqlmap*

- Setelah meleakukan Injeksi maka langkah berikut adalah pengecekan *database* yang telah dilakukan berhasil di dapatkan. Hasil dari *SQL Injection* menunjukan terdapat 3 *database* yang tampil yaitu (*information_schema*, *mybank*, dan *test*).



Gambar 10. Mendapatkan *database*

6. Pada tahap ini penulis hanya akan coba untuk membuka 1 *database* yaitu (mybank), dan mendapati ada 2 tables di dalamnya yaitu *tables* akun dan *news*.



Gambar 11. Terdapat 2 Tables pada *database* (mybank)

7. Tahap berikutnya yaitu penulis akan masuk lagi pada tables (akun) untuk melihat data apa lagi yang ada di dalamnya, dan ditemukan 4 entries dimana itu merupakan *Password* dan *Username* yang akan digunakan untuk *Login* pada website yang telah di targetkan.

```
[00:43:41] [INFO] writing hashes to a temporary file '/tmp/sqlmap0857pm02730/sqlmaphashes-64mhknf.txt'
do you want to crack them via a dictionary-based attack? [Y/n/q] y
[00:43:48] [INFO] using hash method 'md5_generic_passwd'
[00:43:48] [INFO] resuming password 'budi' for hash '00dfc53ee86af02e742515cdcfc075ed3' for user '012345'
[00:43:48] [INFO] resuming password 'bola' for hash 'aec07f935649a5b028c070251f617de7' for user '012346'
Database: mybank
Table: akun
[4 entries]

+----+-----+-----+-----+-----+-----+
| id | nama      | status | balance | password | username |
+----+-----+-----+-----+-----+-----+
| 1  | Budi Raharjo | 1      | 1        | 00dfc53ee86af02e742515cdcfc075ed3 (budi) | 012345 |
| 2  | Tuti Maruti Kelopo | 1      | 1        | aec07f935649a5b028c070251f617de7 (bola) | 012346 |
| 3  | Amir Mahmud | 1      | 1        | 00dfc53ee86af02e742515cdcfc075ed3 (budi) | 012347 |
| 4  | Ani Maarfuah | 1      | 1        | 00dfc53ee86af02e742515cdcfc075ed3 (budi) | 012348 |
+----+-----+-----+-----+-----+-----+

[00:43:48] [INFO] table 'mybank.akun' dumped to CSV file '/root/.local/share/sqlmap/output/cloud.producode.1
[00:43:48] [INFO] fetched data logged to text files under /root/.local/share/sqlmap/output/cloud.producode.
```

Gambar 12. Terdapat 4 entries berupa *Password* dan *Username*

8. Tahap terakhir dari simulasi penyerangan ini yaitu, penulis akan mencoba untuk melakukan *Login* pada website target, dan hasil dari *Login* menggunakan *Password* dan *Username* yang telah di dapatkan, penulis telah berhasil *Login* ke dalam website tersebut. Hasil dapat dilihat pada gambar 13 dan 14.

Gambar 13. Proses *Login*

Gambar 14. Berhasil dalam melakukan *Login*

C. Reporting

Pada tahapan *reporting*, penulis akan membahas serta mengevaluasi dari seluruh kegiatan pengujian pada PT. PLN (Persero) Pusmanpro UMPK V Makassar yang dimana pada tahapan *scanning fingerprinting and enumeration*, penulis menemukan beberapa kerentanan atau celah yang terdapat pada sistem. Hasil *reporting* ini akan membahas deskripsi kerentanan atau celah yang ditemukan serta mengevaluasi bagaimana cara menanggulanginya atau memperbaikinya dan akan mendapatkan suatu hasil rekomendasi mengenai sistem keamanan yang telah diterapkan.

Pada tahapan *exploit* juga kembali penulis tekankan bahwasannya tahapan tersebut hanya sebagai simulasi bagaimana cara *pentester* dapat menembus web server untuk memperoleh informasi apa saja yang mereka anggap berharga dan kemudian berhasil mengeksekusinya dari sistem.

Hasil Pengujian

Berdasarkan hasil analisa pengujian kerentanan system dengan menggunakan metode *penetration testing* maka penulis mendapatkan beberapa hal berikut ini :

1. Security website yang terdapat pada situs <https://pln.co.id> telah menerapkan pengamanan yang baik sehingga hanya ditemukan beberapa kerentanan yang tidak begitu berdampak buruk bagi sistem.

2. Tidak ditemukannya kelemahan SQL injection menandakan bahwa database server PT. PLN (Persero) Pusmanpro UPMK V Makassar aman terhadap serangan SQL injection yang berdampak pada akibat pencurian data atau perubahan data terutama pada data Kariawan.
3. Kurangnya kedisiplinan administrator dalam update serta patch software maupun seperti Apache maupun webserver lainnya.
4. Sudah diterapkannya pengamanan firewall dan IPS/IDS pada seluruh jaringan internal sehingga dapat memblokir paket-paket yang dianggap sistem berbahaya.
5. Dalam pengujian ini penulis tidak dapat mengexploit secara keseluruhan, hanya sekedar menganalisa dengan menggunakan *tools* dan memberikan sedikit simulasi dikarenakan akan mengakibatkan gangguan terhadap sistem yang berjalan.

Kesimpulan

Dari pengujian diatas maka dapat diambil kesimpulan bahwa seluruh tahapan penelitian telah dilakukan mulai dari tahapan menggali informasi, analisis, hingga tahap pengujian untuk mencari dan mengetahui tingkat level kerentanan yang tersedia. Maka dengan ini dapat dinyatakan bahwa keamanan sistem yang telah diterapkan pada PT. PLN (Persero) Pusmanpro UPMK V Makassar dalam keadaan level keamanan yang baik (*secure*).

Daftar Pustaka

- [1] R. Satra and F. Fattah, "Buletin Sistem Informasi dan Teknologi Islam Keamanan Jaringan VLAN dan VoIP Menggunakan Firewall INFORMASI ARTIKEL ABSTRAK," vol. 2, no. 1, pp. 27–35, 2021.
- [2] Anraeni, S., Alwi, E. I., Belluano, P. L. L., Gaffar, A. W. M., Satra, R., & Syafie, L. (2024). Pendampingan Pengelolaan Website UPT. PJP UMI (Pusat Jurnal dan Publikasi) untuk Peningkatan Peningkatan Webometrics. Jurnal Abdidas, 5(1), 1-7. M. Z. Maharani *et al.*, "Analisis Keamanan Website Menggunakan Metode *Scanning* dan Perhitungan *Security Metriks*," vol. 3, no. 3, 2017.
- [3] A. Rochman *et al.*, "Analisis Keamanan Website dengan *Information System Security Assessment Framework* (ISSAF) dan *Open Web Application Security Project* (OWASP) di Rumah Sakit XYZ," vol. 2, no. 4, 2021.
- [4] S. E. Prasetyo dan N. Hassanah, "Analisis Keamanan Website Universitas International Batam Menggunakan Metode ISSAF," vol. 9, no. 2, 2021.
- [5] Chu, G., & Lisitsa, A. (2018). *Penetration Testing* for Internet of Things and Its Automation. In 2018 IEEE 20th International Conference on High Performance Computing and Communications; IEEE 16th International Conference on Smart City; IEEE 4th International Conference on Data Science and Systems (HPCC/SmartCity/DSS), 1479- 1484.
- [6] A. Kukuh *et al.*, "Analisis Serangan *Penetration Testing*: Sebuah Review Sistematis," *Jurnal Ilmiah Informatika dan Komputer*, vol. 1, no. 2, 2022.
- [7] D. K. Abdul Kholiq, "Analisis Keamanan Wireless Local Area Network (WLAN) Dengan Metode *Penetration Testing* Execution Standard (PTES) (Studi Kasus : PT. Win Prima Logistik)," 46 *J. Ilm. Fak. Tek. LIMIT'S Vol.15*, vol. 15, no. 1, pp. 46–55, 2019, [Online]. Available: https://teknik.usni.ac.id/jurnal/ABDUL_KHOLIQ.pdf
- [8] B. V. Tarigan, A. Kusyanti, and W. Yahya, "Analisis Perbandingan *Penetration Testing* Tool Untuk Aplikasi Web," *J. Pengemb. Teknol. Inf. dan Ilmu Komput.*, vol. 1, no. 3, pp. 206– 214, 2017, [Online]. Available: <http://j-ptiik.ub.ac.id/index.php/j-ptiik/article/download/73/37>
- [9] N. F. Saragih *et al.*, "Analisis dan Implementasi *Secure Code* Pada Pengembangan Sistem Keamanan Website Fikom-Methodist.com Menggunakan *Penetration Testing* dan OWASP ZAP," *Technology Informatics and Computer System*, vol. 12, no. 1, 2023.
- [10] S. E. Prasetyo dan R. C. Lee, "Analisis Keamanan Jaringan Pada Pay2home Menggunakan Metode *Penetration Testing*," *Conference on Management, Business, Innovation, Education and Social*

- Science*, vol. 1, no. 1, 2021.
- [11] B. V. Tarigan *et al.*, "Analisis Perbandingan *Penetration Testing Tool* untuk Aplikasi Web," *Jurnal Pengembangan Teknologi Informasi dan Ilmu Komputer*, vol. 1, no. 3, 2017.
 - [12] A. Dharmawan *et al.*, "Penetration Testing Menggunakan OWASP Top 10 Pada Domain XYZ.AC.ID," *Jurnal Elektro Luceat*, vol. 8, no. 1, 2022.
 - [13] Tarigan, B. V., Kusyanti, A., & Yahya, W, "Analisis Perbandingan *Penetration Testing Tool* Untuk Aplikasi Web" *Jurnal Pengembangan Teknologi Informasi Dan Ilmu Komputer (J- PTIIK) Universitas Brawijaya.*, 1(3), 206–214, 2017.
 - [14] M. C. Ghanem and T. M. Chen, "Reinforcement Learning for Efficient Network Penetration Testing," *Information*, vol. 11, no. 1, p. 6, Dec. 2019, doi: 10.3390/info11010006.
 - [15] R. N. Dasmen, R. Rasmila, T. L. Widodo, K. Kundari, and M. T. Farizky, "Pengujian Penetrasi Pada Website Elearning2.Binadarma.Ac.Id Dengan Metode Ptes (Penetration Testing Execution Standard)," *J. Komput. dan Inform.*, vol. 11, no. 1, pp. 91–95, Mar. 2023, doi: 10.35508/jicon.v11i1.9809.