Website Threat Monitoring Untuk Pemantauan dan Analisis Ancaman Pada *Web Server*

Mohammad Farid Susanto[1], Aldiyans Nurcahyo[2], Maya Rahayu[3]

[1]*Jurusan Teknik Elektro, Politeknik Negeri Bandung, Bandung 40012*
E-mail : mfarids@polban.ac.id
[2]*Jurusan Teknik* Elektro*, Politeknik Pos Indonesia, Bandung 40012*
E-mail : aldiyans.nurcahyo.tkom19@polban.ac.id
[3]*Jurusan Teknik* Elektro*, Politeknik Pos Indonesia, Bandung 40012*
E-mail : mayarahayu@polban.ac.id

ABSTRAK

Kemajuan teknologi jaringan semakin berkembang pesat serta kebutuhan pengguna semakin meningkat akan akses internet dan *website* yang memadai. Namun demikian, kebutuhan akan pengguna teknologi jaringan tentunya harus selaras dengan keamanan yang dimiliki oleh penyedia situs agar tidak terjadi serangan *cyber security* oleh pihak yang tidak bertanggungjawab. Ketahanan suatu situs dari ancaman tentunya menjadi pertimbangan bagi *developer* untuk memastikan keamanan data *user* dan perusahaan. Ada beberapa metode yang digunakan untuk menguji ketahanan suatu situs atau aplikasi salah satunya *penetration testing* (pentesting). Jenis pentesting yang digunakan dengan metode *Penetration Testing Methodologies and Standartds* (PTES) menggunakan *software* VMWare Workstation dengan OS Kali Linux untuk melakukan serangan terhadap *web server*. Pada percobaan didapatkan hasil pendeteksian berupa *tools* Nmap dan Metasploit yang digunakan untuk melakukan penyerangan terhadap web server. Ketika mendapatkan serangan ditampilkan pada server dengan mampu mendeteksi *time detection, attacking tools,* dan *list of agents.* Hasil pelaporan serangan terhadap *web server* akan ditampilkan pada *website monitoring* yang selanjutnya akan mempermudah untuk melakukan analisis terhadap hasil serangan pada *web server* yang nantinya dapat dikembangkan penelitian berikutnya.

Kata Kunci : *penetration testing, website threat monitoring,* serangan*, web server*

1. PENDAHULUAN

Keamanan jaringan komputer merupakan hal penting dari setiap sistem untuk menjaga validitas dan integritas data serta menjamin keamanan layanan kepada penggunanya. Pesatnya perkembangan teknologi telekomunikasi dan informasi tentunya membutuhkan peningkatan kualitas keamanan jaringan yang ada dan dibukanya pembelajaran *open source* membuka peluang bagi kelompok yang tidak bertanggung jawab untuk mempelajari tentang *hacking* dan *cracking*, didukung dengan banyaknya *tools* yang memudahkan setiap orang yang ada didalamnya untuk mempelajarinya lebih lanjut.

Kebutuhan akan internet yang tinggi tidak menjadikan masyarakat sadar dan paham akan privasi data mereka. Berdasarkan hasil riset yang dilakukan oleh Trend Micro, cyber risk index (CRI) Indonesia pada tahun 2020 berada di angka 0.26 dan tergolong dalam resiko sedang. Setahun setelahnya, pada tahun 2021 indeks tersebut turun menjadi -0.12 yang berarti risiko akan kejahatan siber meningkat meski belum masuk kategori *high risk* (risiko tinggi) [1].

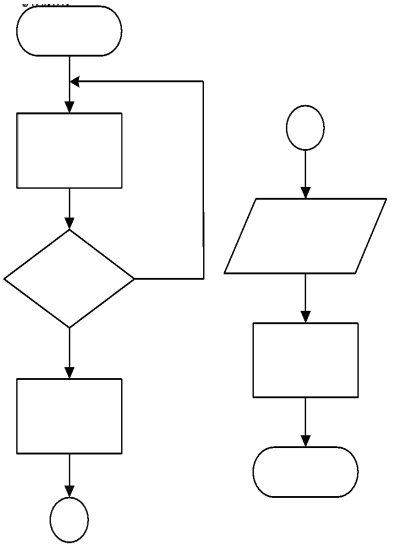
Ancaman dari serangan yang ada di jaringan internet akan terus terjadi selama internet ada sehingga dibutuhkan *tools* untuk memantau ancaman yang pada trafik di jaringan internet. Seperti fungsi CCTV yang digunakan untuk memantau dan merekan kejadian yang ada di perkantoran, rumah, bahkan fasilitas umum yang sering digunakan oleh masyarakat.

Artikel pertama yang dijadikan tinjauan yaitu pada Prosiding Seminar Nasional yang berjudul "Implementasi Teknik Hacking Web Server Dengan Port Scanning Dalam Scanning Dalam Sistem Operasi Kali Linux" dengan menggunakan *tools* Nmap, PHP, dan Netdiscover berhasil mendapatkan *vulnerable ftp open port* yang terdapat lubang keamanan

yang digunakan oleh penyerang untuk melakukan penetrasi terhadap *web server* [2].
Jurnal kedua yang berjudul "Intrusion Detection and Anomaly Menggunakan Wazuh Pada Universitas Muhammadiyah Palembang" mendeteksi serangan dengan menggunakan parameter *time response.* Hal tersebut diukur menggunakan *software* yang berbasis IDS yaitu Wazuh dengan menunjukkan bahwa OS Windows 7 memiliki lebih banyak *vulnerability* dan *integrity file* dibandingkan dengan OS lainnya [3].
Artikel ketiga mengenai "Analisis Keamanan Webserver Menggunakan *Penetration Test*. Dalam pengujian penulis menggunakan OS Parrot Linux dengan menggunakan metode Nmap untuk *Information Gathering"* dilakukan penelitian mengenai keamanan suatu *web server.* Terdapat tiga kategori kelemahan yaitu *high, medium,* dan *low.* Bagian yang diserang adalah adalah *port* 22 yaitu mengenai SSH [4].
Pada jurnal keempat yaitu mengenai "Evaluasi Kinerja *Software Web Penetration Testing*" pada injeksi SQL celah keamanan terbesar biasanya disebabkan oleh validasi input yang lemah. Ada beberapa celah keamanan antara lain *Cross Site Scripting* yang biasanya mengirim berupa *hyperlink* ke situs penyerang [5].
Pada jurnal kelima yang berjudul "*Penetration Testing* Untuk Deteksi *Vulnerability* Sistem Informasi Kampus" ditemukan beberapa celah keamanan dan kerentanan pada sistem informasi kampus dengan memanipulasi arsip lokal menggunakan Teknik DoS yang melakukan *clickjacking* [6]. Pada penelitian selanjutnya yang keenam yaitu "Sistem Informasi Manajemen dan Website Universitas Kristen Petra" membandingkan hasil pemindaian antara OpenVAS dan Acunextix Web Vulnerability Scanner perangkat lunak Acunetix dapat memindai lebih lengkap dari segi performa situs beserta keamannanya, namun dari sisi keamanan server kurang dalam pemindaiannya [7].
Pada penelitian yang berjudul "Pengujian Celah Keamanan Aplikasi Berbasis Web Menggunakan Teknik Penetration Testing dan DAST (Dynamic Application Security Testing)" evaluasi yang dilakukan adalah sebelum ke *database* berupa *script* diubah ke karakter biasa. Sehingga *source code* pada *website* tidak membaca inputan *script* [8].
Pada penelitian yang berjudul "Analisis Layanan Keamanan Sistem Kartu Transaksi Elektronik Menggunakan Metode *Penetration Testing*" menganalisisi layanan keamanan yang ada pada transaksi elektronik menggunakan metode itu. Layanan keamanan yang dianalisis antara lain adalah *integrity, availability,* dan *confidentiality* [9].
Pada penelitian ini akan dikembangkan *website threat monitoring* sebagai pendeteksi dan menampilkan hasil-hasil dari serangan yang dilakukan menggunakan *tools* pada kali linux ditujukan pada *web server* yang ada. Untuk *website threat monitoring* sendiri akan berfungsi untuk mendeteksi berbagai pola-pola ancaman yang menyerang ke komputer server. Sedangkan *software*-nya menggunakan VMware Workstation dengan medianya menggunakan OS Kali Linux dapat diisi oleh berbagai *tools* serangan yang akan ditujukan pada *web service* yaitu, *web server* Quaoar.

2. METODE PENELITIAN

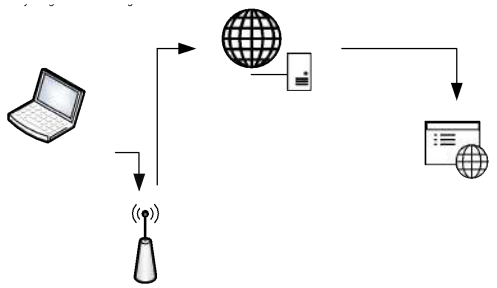
Dalam melakukan penelitian ini, berikut alur sistem yang disajikan dalam bentuk *flowchart* yang ada pada Gambar 1.



Gambar 1. Rancangan Sistem Penelitian

Pada Gambar 1. Merupakan rancangan dari sistem metode penelitian yang dikerjakan. Proses pertama yaitu pengumpulan informasi terkait *web server* terkait dan *tools* yang akan digunakan dalam melakukan penyerangan. Setelah itu akan dilakukan *vulnerability scanning* yaitu menemukan dan mencari celah-celah yang memungkinkan untuk dilakukan eksploitasi, apabila berhasil maka akan dilanjut dengan melakukan penyerangan, namun apabila tidak akan kembali ke pengumpulan infromasi. Setelah berhasil mengeksekusi maka akan mendapatkan hasil serangan yang kemudian

akan dilakukan analisis dari data hasil serangan tersebut.
Dalam penelitian ini ditunjukkan ilustrasi sistem yang akan dibuat ditunjukkan oleh Gambar 2.

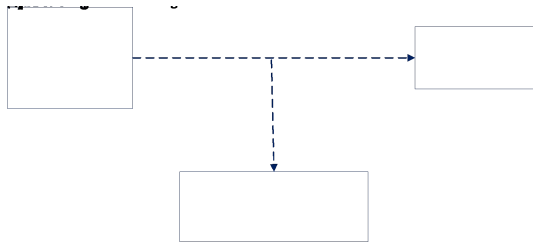


Gambar 2. Ilustrasi Jaringan

Komponen *Access Point* dapat berupa Wi-Fi untuk menghubungkan Laptop dengan internet. Pada bagian penyerang menggunakan Laptop yang sudah ter-install VMWare Workstation dengan OS Kali Linux untuk melakukan serangan terhadap *web server* Quaoar yang nantinya hasil dari serangan tersebut akan dikirimkan ke *website threat monitoring* untuk memberikan informasi terkait hasil serangan dan pendeteksian serangan.

17.1 Perancangan Sistem

Prinsip kerja dari *website threat monitoring* dengan menggunakan metode penetration testing yang akan dirancang secara umum adalah dengan menampilkan data-data berupa jenis serangan hasilnya akan dilampirkan untuk mengetahui ketahanan dari web server ketika diserang dan kemampuan website threat monitoring itu sendiri dalam mendeteksi serangan.



Gambar 3. Blok Diagram Sistem

Berdasarkan Gambar 3. Menunjukkan blok diagram dari sistem yang dirancang. Terdapat OS Kali Linux yang tertanam pada *software* VMWare Workstation yang didalam OS tersebut terdapat *tools* yang akan di uji cobakan terhadap *web server* untuk nantinya hasil dari pengujian tersebut akan ditampilkan pada *website threat monitoring* yang dibuat dan memuat data-data hasil serangan terhadap *web server.*

Tools yang akan digunakan dalam pengujian ini adalah Nmap yang berfungsi sebagai *network & port scanner* dan Metasploit berfungsi sebagai *exploitation framework.* Pada uji *pentesting* atau saat melakukan serangan terdapat tujuh fase yang digunakan, yaitu:

1. *Pre-Engagement Interaction*
2. *Intelligence Gatthering*
3. *Threat Modelling*
4. *Vulnerability Testing*
5. *Exploitation*
6. *Post Exploitation*
7. *Reporting*

Ketujuh fase tersebut menjadi standardisasi untuk melakukan pentesting dengan menggunakan *Penetration Testing Methodologies and Standards* (PTES) dimana menggunakan pendekatan kuantitaf yang mana nantinya parameter hasil pengujian akan dianalisis lebih lanjut untuk dijadikan acuan terkait lemah kuatnya suatu web server dan mengetahui kerentanannya.

Pembuatan *website threat monitoring* menggunakan kerangka sebagai berikut.

Bahasa Pemrograman : HTML, PHP, CSS, SQL
Text Editor : Sublime Text
Framework : Bootstrap
Database Tools : MySQL

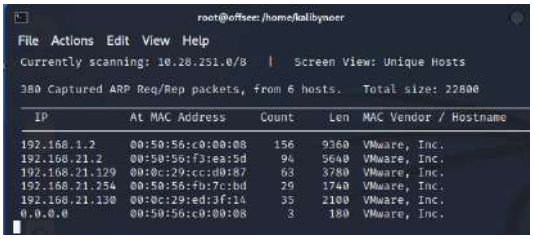
17.2 Parameter Uji

Beberapa parameter yang diuji terhadap hasil serangan yang nantinya akan dianalisis yaitu *list of agents, time response,* dan *detection anomaly.* Untuk mendapatkan nilai dari setiap parameter tersebut dengan *tools* yang digunakan untuk melakukan pengujian maka dilakukan penetration testing terhadap web server dan akan menampilkan data hasil serangan tersebut pada website threat monitoring yang akan dibuat.

17.3 Skenario Pengujian

Pengujian dilakukan dengan menggunakan lingkungan yang bersifat virtual. Lingkungan tersebut berjalan pada sebuah *software* yang bernama VMWare Workstation yang terdapat OS Kali Linux didalamnya berbasis Ubuntu. Untuk mendapatkan nilai dari setiap parameter tersebut dengan *tools* yang digunakan maka dilakukan penetration testing terhadap *web server* dan akan menampilkan data hasil serangan tersebut pada *website threat monitoring* yang dibuat.

Langkah pertama yang dilakukan adalah mencari IP Address yang berada dalam lingkungan tersebut dalam hal ini lingkungan virtualiasi dengan menggunakan tools yaitu netdiscover dengan command “netdiscover” maka akan didapatkan hasil seperti pada Gambar 4.



Gambar 4. Hasil *scan* menggunakan Netdiscover

IP *Address* dari web server Quaoar sendiri adalah 192.168.21.129 yang merupakan target penyerangan. Dengan menggunakan *tools* nmap maka memasukkan *command line* berikut untuk mengetahui jenis *port* yang terbuka:

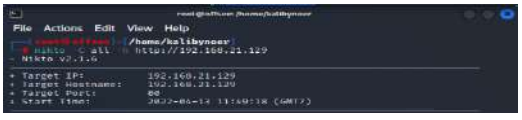
$ Nmap -sV -n 192.168.21.129.

Dari perintah tersebut terdapat tiga argument berbeda yang memiliki fungsi dijelaskan pada Tabel 1 berikut.

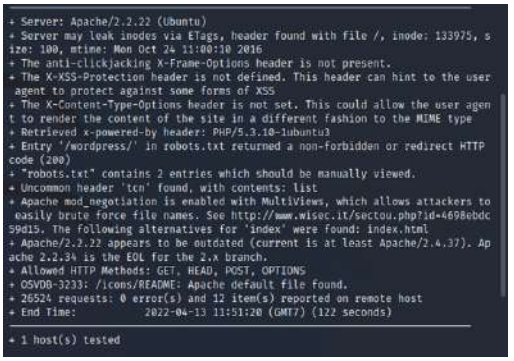
Tabel 1. Argumen *scanning port* pada *web server*

Argumen	Penjelasan
-sV	Mendeteksi versi layanan dari nmap
-n	Menonaktifkan resolusi *reverse* DNS
IP Address tujuan	Dalam kasus ini adalah IP Address dari *web server*

Setelah mendapatkan informasi mengenai *port* yang terbuka selanjutnya adalah melakukan pencarian lebih lanjut mengenai *port* tujuan penyerangan yaitu *port* 80 dengan *service* http yang terdapat informasi mengenai *wordpress* yang berada dalam *web server* tersebut. Dengan menggunakan *tools* nikto seperti pada Gambar 5 dapat melihat hal-hal yang berpotensi di eksploitasi seperti

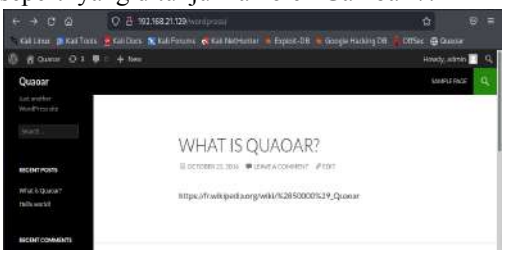


yang ditunjukkan pada Gambar 6.



Gambar 6. Hasil *scan* menggunakan Nikto

Dalam hasil *scanning* tersebut terdapat robots.txt yang memberi informasi bahwa ada dua *entry* yang dapat dilihat secara manual. Dengan menggunakan hal tersebut maka dapat melakukan akses kepada *wordpress* seperti yang ditunjukkan oleh Gambar 7.



Gambar 7. Tampilan wordpress dari *web server* Quaoar

Selanjutnya melakukan eksploitasi melalui *templates* 404.php dengan memasukkan *script* yang diambil dari *reverse-shell*. Setelah menyimpan *script* yang dibutuhkan lalu dikompresi untuk dijadikan *plugin* yang nantinya akan di unggah pada wordpress tersebut untuk mendapatkan akses akses guna melakukan eksploitasi dengan menggunakan *tools* Metasploit.

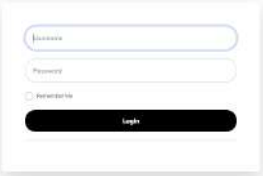
Eksploitasi menggunakan *tools* Metasploit terlebih dahulu mengakses dengan membuka terminal pada Kali Linux dengan memasukkan perintah $msfconsole lalu akan terlihat versi dari Metasploit tersebut. Setelah mengetahui *username* dan *password* yang digunakan untuk mengakses *web server* Quaoar selanjutnya adalah menggunakan perintah *exploit* untuk mengetahui informasi mengenai *module option, payload options,* dan *exploit target* seperti pada Gambar 8.

Gambar 8. Hasil eksploit menggunakan metasploit

Berdasarkan hasil eksploit menggunakan Metasploit didapatkan akses baru yaitu meterpreter. Setelah mendapatkan akses meterpreter langkah selanjutnya yaitu memasukkan perintah *getuid* yang menghasilkan *username* dari server tersebut yaitu: www-data seperti yang dijelaskan pada Gambar 9.

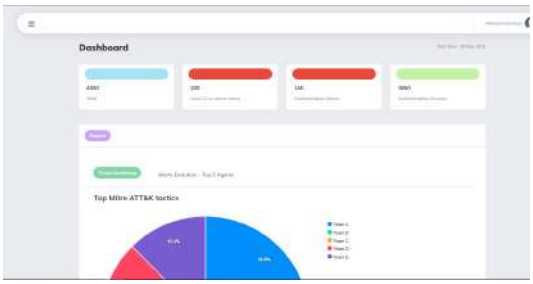
Gambar 9. Hasil dari perintah getuid

Berikut adalah tampilan *website threat monitoring* yang dirancang untuk memberikan informasi terkait hasil serangan yang ditujukan kepada web server Quaoar ditunjukkan pada Gambar 10.



Gambar 10. Tampilan halaman login.php

Ketika ingin mengakases *website* tersebut diperlukan *login* menggunakan *username* dan *password* yang sudah terdaftar supaya pihak lain tidak memiilki akses terhadap data sekaligus demi keamanan. Jika berhasil melakukan *login* maka akan terlihat tampilan *dashboard* seperti yang ditunjukkan oleh Gambar 11.



Gambar 11. Tampilan *dashboard website threat monitoring*

3. HASIL DAN PEMBAHASAN

Dalam melakukan *scanning* dan eksploitasi menggunakan *tools* nmap dan Metasploit yang hasilnya akan ditampilkan pada *website threat monitoring* berdasarkan parameter pengujian didapatkan hasil berikut:

Hasil *port scanning* menggunakan *tools* Nmap ditunjukkan pada Tabel 2 yang menunjukkan bahwa terdapat 9 port dalam keadaan terbuka dan tujuan serangan berada di *port* 80 yang menyerang http atau wordpress dari *web server* tersebut.

Tabel 2. Hasil *Scanning Port*

No	Port	State	Service
1	23	open	ssh
2	53	open	domain
3	80	open	http
4	110	open	pop3
5	139	open	netbios-ssn
6	143	open	imap
7	445	open	netbios-ssn
8	993	open	ssl/imap
9	995	open	ssl/pop3

Selanjutnya pada *website threat monitoring* terdapat tiga parameter hasil serangan yang disajikan pada Tabel 3, Tabel 4, dan Tabel 5. Hasil *detection anomaly* yang ditunjukkan oleh Tabel 3. yang memberikan informasi mengenai *attacking tools* yang digunakan, *attacking methodes,* dan *attack name* yang ada. Pada *tools* Nmap menggunakan metode penyerangan *commonly used port* sedangkan *tools* Metasploit menggunakan metode penyerangan *credentials access.*

Tabel 3. *Detection Anomaly*

No	*Attacking Tools*	*Attacking Methodes*	*Attack Name*
1.	Port Scanning (Nmap)	*Commonly Used Port*	Scan
2.	Metasploit	*Credential Access*	Exploit Public

Hasil pendeteksian berdasarkan *time detection* didapatkan bahwa terdapat dua *tools* yang digunakan untuk melakukan penyerangan terhadap web *server* yaitu Nmap dan Metasploit. Dalam pendeteksian terdapat waktu penyerangan dengan menggunakan *tools* Nmap dimana melakukan penyerangan pada pukul 14:10:15 dan terdeteksi pada pukul 14:10:25 dimana selisih dari waktu serangan dan deteksi adalah 10 sekon. Sedangkan pada *tools* Metasploit melakukan

penyerangan pada pukul 14:45:23 dan terdeteksi pada pukul 14:46:55 dengan selisih 32 sekon.

Tabel 4. *Time Detection*

No	*Attacking Tools*	*Attacking* (Waktu)	*Detection* (Waktu)	Δt (*Detection – Attacking*)
1.	Port Scanning (Nmap)	14:10:15	14:10:25	10 sekon
2.	Metasploit	14:45:23	14:46:55	32 sekon

Tabel 5. menunjukkan *list of agents* yang terhubung dengan server. Terdapat 3 *agents* yang terhubung yang masing-masing terdapat informasi mengenai IP *Address*, sistem operasi, dan status untuk mengetahui apakah *agents* tersebut masih terhubung dengan server atau tidak.

Tabel 5. *List of Agents*

No	List Agent	IP *Address*	Sistem Operasi	Status
1.	DESKTOP-2922T99 (Lenovo)	192.168.255.212	Windows	Active
2.	DESKTOP-9NHDHGE (Asus)	192.168.255.105	Windows	Active
3.	Kali	192.168.255.169	Kali GNU/Linux 2022.1	Active

4. KESIMPULAN

Dari hasil penelitian ini berhasil dilakukan sebuah simulasi penyerangan terhadap web server Quaoar dengan menggunakan *tools* Nmap dan Metasploit. Nmap berhasil mendapatkan menemukan port yang terbuka pada web *server* sedangkan Metasploit berhasil melakukan eksploitasi pada web server tersebut. Pada server menampilkan data-data hasil penyerangan namun belum dapat terhubung dengan *website threat monitoring* yang dikembangkan belum berhasil untuk melakukan pendeteksian terkait serangan terhadap *web server* yang dapat memberikan informasi terkait *list of agents, time response,* dan *detection anomaly* sesuai dengan yang direncanakan.

UCAPAN TERIMA KASIH

Ucapan terima kasih penulis atas dedikasi dan bantuan kepada pihak yang membantu dalam penelitian ini.

DAFTAR PUSTAKA

[1]Shella, “Serangan Siber Meresahkan Netizen,” *IDS Digital College STMIK INDO DAYA SUVANA*, Jakarta, 2021.

[2]M. R. Rusydianto, E. Budiman, and H. J. Setyadi, “Implementasi Teknik Hacking Web Server Dengan Port Scanning Dalam Sistem Operasi Kali Linux,” *Pros. Semin. Nas. Ilmu Komput. dan Teknol. Inf. e-ISSN*, vol. Vol.2 No, no. 2, 2017.

[3]A. G. S. Harahap and H. Hutrianto, “Intrusion Detection and Anomaly Menggunakan Wazuh Pada Universitas Muhammadiyah Palembang,” *Bina Darma ...*, pp. 324–328, 2021, [Online]. Available: https://conference.binadarma.ac.id/index.php/BDCCS/article/view/2150.

[4]F. Fachri, A. Fadlil, and I. Riadi, “Analisis Keamanan Webserver menggunakan Penetration Test,” *J. Inform.*, vol. 8, no. 2, pp. 183–190, 2021, doi: 10.31294/ji.v8i2.10854.

[5]M. Ula, “Evaluasi Kinerja Software Web Penetration Testing,” *TECHSI - J. Tek. Inform.*, vol. 11, no. 3, p. 336, 2019, doi: 10.29103/techsi.v11i3.1996.

[6]Sahren, R. Ashari Dalimuthe, and M. Amin, “Prosiding Seminar Nasional Riset Information Science (SENARIS) Penetration Testing Untuk Deteksi Vulnerability Sistem Informasi Kampus,” no. September, pp. 994–1001, 2019.

[7]R. Pangalila, “Penetration Testing Server Sistem Informasi Manajemen Dan Website Universitas Kristen Petra,” *J. Teknol. Inf.*, vol. 3, no. 2, p. pp.271-p.276, 2015, [Online]. Available: http://publication.petra.ac.id/index.php/teknik-informatika/article/view/3145.

[8]B. Wicaksono, “TESTING OF SECURITY GAP APPLICATION BASED ON WEB USING PENETRATION TESTING AND DAST (DYNAMIC APPLICATION SECURITY TESTING) TECHNIQUES,” 2020.

[9]H. Azis and F. Fattah, “Analisis Layanan Keamanan Sistem Kartu Transaksi Elektronik Menggunakan Metode Penetration Testing,” *Ilk. J. Ilm.*, vol. 11, no. 2, pp. 167–174, 2019, doi: 10.33096/ilkom.v11i2.447.167-174.