PENGUJIAN KEAMANAN DENGAN METODE PENETRATION TESTING EXECUTION STANDARD (PTES) UNTUK MENEMUKAN KERENTANAN MISCONFIGURATIONS PADA PERANGKAT JARINGAN

SECURITY TESTING WITH PENETRATION TESTING EXECUTION STANDARD (PTES) METHODS TO FIND MISCONFIGURATIONS VULNERABILITIES IN NETWORK DEVICES

I Made Edy Listartha[1], Gede Arna Jude Saskara[2]

[1]Universitas Pendidikan Ganesha
[2]Universitas Pendidikan Ganesha
[1]listartha@undiksha.ac.id, [2]jude.saskara@undiksha.ac.id

Abstrak

Penelitian ini mengkaji keamanan jaringan WIFI di Universitas Pendidikan Ganesha menggunakan metode Penetration Testing Execution Standard (PTES). Tujuan dari penelitian ini adalah untuk mengidentifikasi dan menganalisis kerentanan yang disebabkan oleh misconfigurations dalam infrastruktur jaringan WiFi universitas. Metode PTES digunakan untuk melakukan pengujian dengan tahapan yang meliputi pre-engagement interactions, intelligence gathering, threat modeling, vulnerability analysis, exploitation, post-exploitation, dan reporting. Hasil pengujian menunjukkan beberapa kerentanan utama yang berkaitan dengan konfigurasi yang tidak tepat, seperti penggunaan protokol yang rentan dan pengaturan yang kurang aman. Analisis lebih lanjut mengungkapkan potensi risiko yang dapat dimanfaatkan oleh pihak yang tidak berwenang untuk mengakses data sensitif atau mengganggu layanan. Penelitian ini memberikan rekomendasi untuk perbaikan konfigurasi dan langkah-langkah mitigasi guna meningkatkan keamanan jaringan WIFI di universitas. Temuan ini diharapkan dapat menjadi dasar bagi pengembangan kebijakan keamanan yang lebih efektif dan perlindungan yang lebih baik terhadap infrastruktur jaringan di lingkungan akademik.

Kata kunci : Keamanan jaringan, WiFi, Penetration Testing Execution Standard (PTES), kerentanan, misconfigurations

Abstract

This study examines the security of the WiFi network at Universitas Pendidikan Ganesha using the Penetration Testing Execution Standard (PTES) method. The aim is to identify and analyze vulnerabilities caused by misconfigurations within the university's WiFi infrastructure. The PTES method is employed to conduct testing through phases including pre-engagement interactions, intelligence gathering, threat modeling, vulnerability analysis, exploitation, post-exploitation, and reporting. The testing results reveal several key vulnerabilities related to improper configurations, such as the use of vulnerable protocols and insecure settings. Further analysis exposes potential risks that could be exploited by unauthorized parties to access sensitive data or disrupt services. The study provides recommendations for configuration improvements and mitigation steps to enhance WiFi network security at the university. The findings are expected to serve as a foundation for developing more effective security policies and better protection for network infrastructure in academic environments.

Keywords: Network security, WiFi, Penetration Testing Execution Standard (PTES), vulnerabilities, misconfigurations

1. PENDAHULUAN

Pengujian keamanan jaringan adalah proses yang dilakukan untuk menguji keamanan sistem dan jaringan komputer dengan tujuan untuk menemukan celah keamanan dan mengatasi masalah keamanan yang muncul. Hal ini sama pentingnya dengan pengujian akan *availability* dari sistem yang di bangun[1]. Pengujian ini dilakukan dengan berbagai teknik dan metode untuk menemukan kelemahan dan celah pada sistem, sehingga dapat diambil tindakan pencegahan yang diperlukan untuk mengurangi risiko terjadinya serangan keamanan.

Pentingnya melakukan pengujian keamanan dan jaringan terletak pada fakta bahwa ancaman keamanan terus berkembang dan semakin canggih dari waktu ke waktu. Oleh karena itu, tidak hanya penting untuk melakukan pengujian keamanan secara berkala, tetapi juga memastikan bahwa sistem dan jaringan tetap aman dari serangan. Dengan melakukan pengujian keamanan dan jaringan secara teratur, organisasi dapat mengidentifikasi celah keamanan dan memperbaikinya sebelum terjadi serangan, sehingga dapat meningkatkan keamanan dan ketahanan sistem dan jaringan. Risiko dari adanya serangan ini terjadi di semua tempat di dunia [2].

Indonesia sendiri telah menjadi target beberapa serangan siber yang signifikan dalam beberapa tahun terakhir. Salah satu serangan terbesar yang pernah terjadi adalah serangan terhadap sistem perbankan pada tahun 2017 [3], yang menyebabkan beberapa bank kehilangan jutaan dolar. Serangan ini dilakukan dengan menggunakan *malware* yang menyebar melalui email dan mencuri informasi *login* pengguna. Selain itu, Indonesia juga mengalami serangan terhadap Komisi Pemilihan Umum (KPU) pada tahun 2019 [4], di mana data pribadi hampir 2,3 juta pemilih dicuri oleh sekelompok peretas yang menggunakan teknik *phising* dan *malware*. Serangan-serangan ini menunjukkan bahwa Indonesia masih rentan terhadap serangan siber, dan perlu adanya upaya untuk meningkatkan keamanan siber dan kesadaran akan pentingnya keamanan siber bagi masyarakat luas.

Peningkatan keamanan dapat dilakukan dengan menghindari jenis-jenis kerentanan biasanya terjadi. Dalam keamanan komputer, kerentanan adalah kelemahan yang dapat dieksploitasi oleh aktor ancaman, biasanya untuk tujuan jahat. Kerentanan dapat ditemukan di berbagai bidang sistem, termasuk perangkat keras, perangkat lunak, jaringan, dan bahkan orang atau pengguna. Terdapat empat jenis utama kerentanan keamanan [5] yaitu *Misconfigurations*, *Unsecured API's*, *Outdated* atau *Unpatched Software*, dan *Zero-Day Vulnerabilities*.

Untuk menemukan kerentanan ini, biasanya dilakukan proses yang dikenal dengan istilah *penetration testing*. Proses ini dalam dilakukan dengan menggunakan metode PTES, dimana *Penetration Testing Execution Standard* (PTES) adalah sebuah standar industri yang digunakan untuk melakukan pengujian penetrasi atau *penetration testing* pada sistem komputer dan jaringan. PTES dirancang untuk memberikan kerangka kerja yang terstruktur dan menyeluruh bagi para profesional keamanan siber dalam melakukan pengujian penetrasi.

Dalam penelitian ini, metode PTES akan dilakukan pada jaringan Universitas Pendidikan Ganesha. Hal ini dilakukan karena Undiksha menyediakan akses jaringan kepada Mahasiswa, Dosen dan Pegawai melalui *WIFI* dengan SSID UNDIKSHA HARMONI dengan menggunakan SSO. Jaringan ini menjadi satu juga dengan beberapa perangkat jaringan seperti *Printer*, *Switch* Jaringan, *Router*, Komputer dan lain-lain. Hal ini dapat memberikan akses yang berbahaya ke dalam sistem jika perangkat jaringan ini memiliki salah satu atau keempat jenis utama kerentanan.

Penelitian ini khusus bertujuan untuk mencari kerentanan jenis *Misconfigurations* pada perangkat yang terhubung ke dalam jaringan UNDIKSHA HARMONI saja. Peneliti bertindak seperti pengguna biasa pada jaringan dan tidak mengetahui arsitektur *topologi* jaringan Undiksha, sehingga dapat memberikan gambaran akan risiko jika ada orang luar yang dapat masuk ke jaringan UNDIKSHA-HARMONI tanpa ijin.

2. DASAR TEORI

2.1 State of the Art

Missconfiguration (kesalahan konfigurasi) adalah kondisi ketika perangkat atau sistem tidak dikonfigurasi dengan benar atau tidak sesuai dengan kebijakan keamanan yang telah ditetapkan. Kesalahan konfigurasi dapat terjadi pada perangkat jaringan, server, aplikasi, atau perangkat lunak lainnya. Kesalahan konfigurasi dapat mempengaruhi keamanan, kinerja, dan fungsionalitas perangkat atau sistem tersebut. Contoh kesalahan konfigurasi yang umum meliputi pengaturan kata sandi yang lemah, izin akses yang tidak tepat, penggunaan protokol yang tidak aman, dan konfigurasi jaringan yang tidak tepat [6]. Kesalahan konfigurasi dapat menyebabkan kerentanan pada sistem dan memungkinkan penyerang untuk mencuri data, merusak atau menghancurkan sistem, atau memperoleh akses tidak sah ke sistem atau jaringan.

Untuk menemukan kesalahan konfigurasi secara manual, administrator jaringan dapat melakukan beberapa cara berikut:

a. Review konfigurasi [7], Administrator jaringan dapat memeriksa konfigurasi perangkat jaringan secara manual untuk menemukan kesalahan konfigurasi. Ini dapat dilakukan dengan mengumpulkan konfigurasi dari perangkat jaringan dan memeriksanya satu per satu.
b. Analisis log [8], Administrator jaringan dapat menganalisis log dari perangkat jaringan untuk menemukan aktivitas yang mencurigakan atau indikasi kesalahan konfigurasi. Log ini dapat memberikan informasi yang berguna untuk mengidentifikasi masalah konfigurasi.
c. Network *scanning* [9], Administrator jaringan dapat menggunakan alat *scanning* jaringan untuk menemukan perangkat jaringan yang terhubung ke jaringan dan memeriksa konfigurasi perangkat jaringan. Dalam proses *scanning*, administrator jaringan dapat menemukan perangkat yang fungsinya tidak dikonfigurasi dengan benar atau memiliki kesalahan konfigurasi pada fungsinya.
d. *Penetration testing* [10], Administrator jaringan dapat melakukan *penetration testing* untuk menemukan kesalahan konfigurasi pada perangkat jaringan. Dalam proses ini, *pentester* akan melakukan simulasi serangan ke perangkat jaringan dan mencoba memanfaatkan kesalahan konfigurasi untuk mendapatkan akses ke jaringan.

Pada umumnya, cara manual review serta analisis log yang di gunakan untuk menemukan kesalahan konfigurasi memerlukan waktu dan sumber daya yang cukup banyak. Selain itu, proses manual mungkin tidak dapat menemukan semua kesalahan konfigurasi yang ada pada jaringan[11][12][13]. Beberapa contoh jenis-jenis *misconfiguration* pada perangkat meliputi:

a. Konfigurasi jaringan yang salah pada perangkat, seperti kesalahan dalam pengaturan IP *address, subnet mask, dan default gateway*.
b. Kesalahan dalam pengaturan VLAN dan *trunking* pada *switch*, yang dapat mengakibatkan masalah dalam akses jaringan dan konfigurasi yang tidak aman.

c. Konfigurasi *firewall* yang salah, seperti pengaturan aturan *firewall* yang tidak tepat atau kesalahan dalam konfigurasi VPN, yang dapat mengakibatkan kebocoran data dan kerentanan terhadap serangan.
d. Pengaturan keamanan yang buruk pada server, seperti menggunakan *password* yang lemah atau pengaturan hak akses yang salah, yang dapat memungkinkan akses yang tidak sah ke sistem dan informasi yang sensitif.
e. Kesalahan dalam konfigurasi perangkat IoT, seperti penggunaan kata sandi default atau tidak memperbarui perangkat lunak yang dapat membuat perangkat rentan terhadap serangan.

Kesalahan dalam konfigurasi pada keamanan perangkat tidak akan terdeteksi dalam *Network Scanning*, hal ini terjadi karena fungsi perangkat berjalan sesuai dengan fungsinya. Untuk melihat kesalahan konfigurasi dari keamanan perangkat ini, maka cara *Penetrations Testing* terlihat paling tepat untuk menemukannya karena menyimulasikan serangan pada keamanan perangkat jaringan.

2.2 Penetration Testing Execution Standard (PTES)

PTES terdiri dari 7 tahap yang harus dilakukan secara berurutan dalam melakukan pengujian penetrasi:

- **Pre-engagement Interactions**

Tahap ini merupakan tahap awal yang dilakukan sebelum memulai pengujian penetrasi. Pada tahap ini, perusahaan atau organisasi yang akan dilakukan pengujian penetrasi harus memberikan persetujuan tertulis dan pemahaman tentang tujuan dan lingkup pengujian penetrasi.

- **Intelligence Gathering**

Pada tahap ini, pengujian penetrasi akan dilakukan untuk mengumpulkan informasi yang diperlukan mengenai target. Informasi yang dapat dikumpulkan antara lain seperti sistem yang digunakan, aplikasi yang digunakan, jaringan yang digunakan, dan sebagainya.

- **Threat Modeling**

Tahap ini dilakukan untuk mengidentifikasi ancaman dan risiko yang mungkin terjadi pada target yang akan diuji. Pada tahap ini, dilakukan analisis mengenai ancaman yang mungkin terjadi dan kerentanan yang dapat dimanfaatkan oleh penyerang.

- **Vulnerability Analysis**

Tahap ini dilakukan untuk mengidentifikasi celah keamanan atau kerentanan yang dapat dimanfaatkan oleh penyerang. Pada tahap ini, dilakukan analisis mengenai kerentanan yang telah diidentifikasi pada tahap sebelumnya.

- **Exploitation**

Tahap ini dilakukan untuk mengeksploitasi celah keamanan atau kerentanan yang telah ditemukan pada tahap sebelumnya. Pada tahap ini, dilakukan upaya untuk mengambil alih sistem atau aplikasi yang diuji.

- **Post Exploitation**

Tahap ini dilakukan setelah berhasil mengambil alih sistem atau aplikasi yang diuji pada tahap sebelumnya. Pada tahap ini, dilakukan upaya untuk mempertahankan akses pada sistem atau aplikasi yang telah diambil alih.

- **Reporting**

Tahap ini merupakan tahap terakhir yang dilakukan setelah selesai melakukan pengujian penetrasi. Pada tahap ini, dilakukan pelaporan hasil pengujian penetrasi kepada pihak yang berwenang. Pelaporan harus dilakukan secara jelas, terperinci dan lengkap mengenai celah

keamanan yang ditemukan serta rekomendasi untuk memperbaiki keamanan sistem, aplikasi atau jaringan yang diuji.

Kerangka kerja PTES membantu dalam memastikan bahwa pengujian penetrasi dilakukan dengan cara yang terstruktur dan efektif sehingga dapat membantu dalam mengidentifikasi dan meminimalkan celah keamanan dalam sistem, aplikasi, atau jaringan.

2.3 SSID UNDIKSHA HARMONI Undiksha

Jaringan internal ini memiliki konfigurasi akses dengan memanfaatkan *authentication* akun SSO. Konfigurasi jaringan yang digunakan adalah Network ID: 10.10.0.0/18, Broadcast ID: 10.10.63.255, Host IP mulai dari: 10.10.0.1, Host IP Akhir: 10.10.63.254, dengan total Host yang didukung: 16382 host. Setiap user Mahasiswa, Dosen, Pegawai maupun perangkat yang login akan memiliki subnet IP ini. Hal ini memungkinkan proses *penetration testing* dapat dilakukan dengan hanya dengan *login* terlebih dahulu ke dalam jaringan dan mencari perangkat yang memiliki kerentanan.

3. HASIL DAN PEMBAHASAN

3.1 Hasil Intelligence Gathering

Jaringan UNDIKSHA HARMONI terhubung dengan perangkat milik mahasiswa, pegawai dan dosen dimana perangkat ini tidak akan melalui proses pengujian dikarenakan bukan bagian dari arsitektur jaringan Undiksha. Sehingga perangkat yang bukan bagian dari arsitektur jaringan akan di hilangkan. Pada framework PTES, untuk mencari informasi perangkat ini nantinya akan menggunakan teknik Internal Footprinting. Fase Internal Footprinting dari Intelligence Gathering melibatkan pengumpulan hasil respons dari target berdasarkan interaksi langsung dari perspektif internal. Informasi perangkat yang akan dicari adalah:

- Layanan Port terbuka pada Router.
- IP & Layanan Port Terbuka pada Switch.
- IP & Layanan Port Terbuka pada AP
- Perangkat pendukung kerja yang bersifat permanen (Printer, CCTV, Scanner, Dll)

Perangkat yang bersifat *mobile* maupun BYOD (Smartphone, Laptop, Tablet, Smartwatch, dll) akan dipisahkan dengan melakukan *Network Scanning* beberapa kali pada jaringan dalam kurun waktu di luar jam kerja (tengah malam). Hasil dari proses ini terlihat pada tabel 1.

Tabel 1 Perangkat yang terdeteksi pada jaringan di luar jam kerja.

IP	MAC	PORT
10.10.0.5	FC:5B:26:41:09:BA	80.443
10.10.0.248	F0:9F:C2:79:DD:4A	22
10.10.1.157	80:05:88:44:80:F6	22,23,80,443
10.10.1.242	44:5C:E9:88:CA:C0	8080
10.10.1.244	B4:8C:9D:66:A0:75	80.443
10.10.1.253	FC:5B:26:41:09:BA	80.443
10.10.3.81	00:74:9C:C5:F3:52	23,80,443
10.10.3.155	00:74:9C:C5:F3:DC	23,80,443
10.10.4.60	00:74:9C:C5:7A:F9	23,80,443
10.10.4.198	4C:EB:BD:AC:C2:79	80.443.8080
10.10.4.229	00:74:9C:C5:7A:39	23,80,443
10.10.5.33	00:74:9C:C5:7B:4B	23,80,443

10.10.5.92	E0:BB:9E:57:45:6E	80.443
10.10.5.167	E0:BB:9E:ED:F6:A1	80.443
10.10.5.230	00:74:9C:C5:7B:C7	23,80,443
10.10.6.7	00:74:9C:C5:7A:37	23,80,443
10.10.6.35	00:74:9C:C7:C0:0A	23,80,443
10.10.6.60	00:74:9C:C5:F3:3E	23,80,443
10.10.6.226	68:14:01:28:6A:61	21,23,80,443,8080
10.10.7.3	00:74:9C:C5:F3:70	23,80,443
10.10.9.217	B4:B5:B6:35:58:AC	80.443.8080
10.10.11.32	30:0D:9E:43:56:92	23,80,443
10.10.18.93	70:77:81:6D:DE:4A	80

Tabel 1 memperlihatkan beberapa perangkat yang menjalankan *service* melalui *port* tertentu, informasi port ini selanjutnya digunakan untuk mengidentifikasi jenis layanan dan *tool* yang cocok untuk pengujian. Sesuai dengan topik penelitian, kerentanan berfokus pada *misconfiguration* pada perangkat-perangkat arsitektur jaringan yang bersifat permanen di Undiksha. *Misconfiguration* yang akan di analisis adalah pada proses *login service*:

- Webservice pada perangkat (80,8080,443).
- SSH (22).
- TELNET (23).
- FTP Server (21).

3.2 Hasil Vulnerability dan Eksploitasi

Hasil ini didapatkan dengan melakukan proses *login* ke layanan sesuai dengan *port* yang di targetkan. Pengujian awalnya di lakukan dengan memanfaatkan informasi default *login*, jika tidak berhasil maka dilakukan proses *bruteforce*. Tabel 2 memperlihatkan hasil dari pengujian yang di lakukan.

Tabel 2 Hasil percobaan login dengan informasi *default login* dan brute force.

IP	DEFAULT LOGIN	BRUTE FORCE TOOLS	USERNAME	PASSWORD
10.10.0.5	Gagal	Gagal		
10.10.0.248	Gagal	Gagal		
10.10.1.157	Gagal	Gagal		
10.10.1.242	Gagal	Gagal		
10.10.1.244	Gagal	Gagal		
10.10.1.253	Gagal	Gagal		
10.10.3.81	Gagal	Gagal		
10.10.3.155	YA		admin	admin
10.10.4.60	Gagal	Gagal		
10.10.4.198	Gagal	Gagal		
10.10.4.229	Gagal	Gagal		
10.10.5.33	YA		admin	admin
10.10.5.92	Gagal	Gagal		

10.10.5.167	Gagal	Gagal		
10.10.5.230	YA		admin	admin
10.10.6.7	Gagal	Gagal		
10.10.6.35	YA		admin	admin
10.10.6.60	Gagal	Gagal		
10.10.6.226	Gagal	Gagal		
10.10.7.3	Gagal	Gagal		
10.10.9.217	Gagal	Gagal		
10.10.11.32	Gagal	Gagal		
10.10.18.93	Gagal	Gagal		

Berdasarkan data tabel 2, terlihat masih ada perangkat yang menggunakan *username* dan *password* bawaan dari pabriknya. Hal ini memperlihatkan bahwa secara fungsi, perangkat tersebut dapat berjalan sebagai mana seharusnya namun konfigurasinya tidak memenuhi unsur keamanan.

3.3 Hasil Post Exploitation

Proses ini dilakukan secara manual setelah berhasil masuk ke dalam sistem pada IP 10.10.3.155, 10.10.5.33, 10.10.5.230 dan 10.10.6.35. Tabel 3 memperlihatkan eksploitasi apa saja yang berhasil dilakukan di perangkat jaringan tersebut.

Tabel 3 Hasil eksploitasi.

IP	**Pencurian Data**	**Manipulasi Data**	**Gangguan Layanan**	**Penggunaan Sumber Daya**	**Penyebaran Malware**
10.10.3.155	Bisa	Bisa	Tidak	Bisa, Ping	Tidak
10.10.5.33	Bisa	Bisa	Tidak	Bisa, Ping	Tidak
10.10.5.230	Bisa	Bisa	Tidak	Bisa, Ping	Tidak
10.10.6.35	Bisa	Bisa	Tidak	Bisa, Ping	Tidak

4. KESIMPULAN

Dalam pemeriksaan keamanan yang dilakukan pada alamat IP 10.10.3.155, 10.10.5.33, 10.10.5.230, dan 10.10.6.35, ditemukan serangkaian kerentanan yang mengindikasikan potensi ancaman serius terhadap integritas, kerahasiaan, dan ketersediaan data. Temuan tersebut merinci tiga jenis kerentanan utama, yakni Pencurian Data, Manipulasi Data, dan Penggunaan Sumber Daya yang tidak sah.

1. Pencurian Data:

Pada semua empat alamat IP yang disurvei, terdeteksi potensi pencurian data. Kelemahan ini membuka pintu bagi pihak yang tidak berwenang untuk mengakses dan mengambil informasi rahasia yang disimpan di dalam sistem. Adanya celah keamanan semacam ini dapat mengakibatkan kerugian serius, termasuk kebocoran data pribadi atau bisnis yang dapat disalahgunakan oleh pihak yang tidak bertanggung jawab.

2. Manipulasi Data:

Selain pencurian data, ditemukan kerentanan terhadap manipulasi data pada IP yang disebutkan. Hal ini menciptakan potensi risiko modifikasi, penyisipan, atau penghapusan data yang dapat mengacaukan integritas informasi yang disimpan. Ancaman manipulasi data dapat merusak

reputasi organisasi, mempengaruhi keputusan bisnis, dan bahkan menyebabkan dampak negatif pada operasional sehari-hari.

3. Penggunaan Sumber Daya:

Kerentanan pada penggunaan sumber daya menunjukkan bahwa entitas yang tidak sah dapat memanfaatkan daya komputasi dan infrastruktur pada alamat IP tersebut tanpa izin. Dengan demikian, dapat timbul konsekuensi serius seperti kinerja sistem yang menurun, beban sumber daya yang tidak perlu, dan potensi kegagalan operasional. Penggunaan sumber daya yang tidak sah juga dapat berdampak pada biaya operasional yang tidak terduga.

Tindakan Rekomendasi:

Untuk mengatasi kerentanan yang telah diidentifikasi, perlu segera diimplementasikan langkah-langkah keamanan yang tepat. Ini melibatkan penggantian *password default* atau standar, pembaruan sistem keamanan, penerapan enkripsi data yang kuat, monitoring aktif terhadap aktivitas mencurigakan, serta penguatan kebijakan akses. Selain itu, dilakukan juga audit keamanan secara berkala untuk memastikan bahwa sistem tetap terlindungi dari ancaman yang terus berkembang.

Kesimpulannya, kerentanan pada alamat IP 10.10.3.155, 10.10.5.33, 10.10.5.230, dan 10.10.6.35 harus dianggap sebagai priotitas tinggi dalam rangka menjaga keamanan sistem dan data yang tersimpan di dalamnya. Dengan mengambil langkah-langkah yang tepat, dapat meminimalkan risiko serta memastikan kelangsungan operasional dan kepercayaan stakeholders terhadap keamanan sistem informasi.

DAFTAR PUSTAKA

[1] I. M. E. Listartha, “Pengujian Performa dan Tingkat Stress pada Website Legalisir Ijasah Online Universitas Pendidikan Ganesha,” *Electro Luceat*, vol. 6, no. 1, hlm. 66–73, Jul 2020, doi: 10.32531/JELEKN.V6I1.182.

[2] Mark Lukehart, “2023 Cyber Attack Statistics, Data, and Trends | Parachute,” Paracute. Diakses: 12 Maret 2023. [Daring]. Tersedia pada: https://parachute.cloud/cyber-attack-statistics-data-and-trends/

[3] H. Shemi, “Serangan Siber Meningkat, Sektor Keuangan Paling Terancam,” IDN Times. Diakses: 12 Maret 2023. [Daring]. Tersedia pada: https://www.idntimes.com/business/economy/helmi/hati-hati-sektor-keuangan-paling-terancam-nomor-2-kejahatan-siber

[4] F. C. Farisa, “Kaleidoskop 2019: Serangan Hoaks Hantam KPU,” Kompas.com. Diakses: 12 Maret 2023. [Daring]. Tersedia pada: https://nasional.kompas.com/read/2019/12/30/05472211/kaleidoskop-2019-serangan-hoaks-hantam-kpu

[5] R. Clancy, “Network Security Threats and Vulnerabilities | Types of Attacks in Network Security,” EC-Coucil. Diakses: 12 Maret 2023. [Daring]. Tersedia pada: https://www.eccouncil.org/cybersecurity-exchange/network-security/network-security-threats-vulnerabilities/

[6] A. Dizdar, "Security Misconfiguration: Impact, Examples, and Prevention," Brightsec. Diakses: 12 Maret 2023. [Daring]. Tersedia pada: https://brightsec.com/blog/security-misconfiguration/

[7] S. Thorgren, J. Wincent, dan D. Örtqvist, "Designing interorganizational networks for innovation: An empirical examination of network configuration, formation and governance," *Journal of Engineering and Technology Management*, vol. 26, no. 3, hlm. 148–166, Sep 2009, doi: 10.1016/J.JENGTECMAN.2009.06.006.

[8] A. Ambre dan N. Shekokar, "Insider Threat Detection Using Log Analysis and Event Correlation," *Procedia Comput Sci*, vol. 45, no. C, hlm. 436–445, Jan 2015, doi: 10.1016/J.PROCS.2015.03.175.

[9] A. Tundis, W. Mazurczyk, dan M. Mühlhäuser, "A review of network vulnerabilities scanning tools: Types, capabilities and functioning," *ACM International Conference Proceeding Series*, Agu 2018, doi: 10.1145/3230833.3233287.

[10] S. Shah dan B. M. Mehtre, "An overview of vulnerability assessment and penetration testing techniques," *Journal of Computer Virology and Hacking Techniques*, vol. 11, no. 1, hlm. 27–49, Feb 2015, doi: 10.1007/S11416-014-0231-X/METRICS.

[11] Y. Stefinko, A. Piskozub, dan R. Banakh, "Manual and automated penetration testing. Benefits and drawbacks. Modern tendency," *Modern Problems of Radio Engineering, Telecommunications and Computer Science, Proceedings of the 13th International Conference on TCSET 2016*, hlm. 488–491, Apr 2016, doi: 10.1109/TCSET.2016.7452095.

[12] Hidayah, Rifki Rahmatun. *"Simulasi Penetration Testing Pada Sistem Pembelajaran Daring (SPaDa) Fakultas Teknik Universitas Islam Riau Dengan Metode Owasp dan Ptes."* PhD diss., Universitas Islam Riau, 2024

[13] Latif, Nuraida, Hartanto Tantriawan, Sabrina Aulia Rahmah, Agus Halid, Annisa Nurul Puteri, Wa Ode Rahma AUM, Ery Murniyasih et al. *Komunikasi Data*. Yayasan Kita Menulis, 2022.