Journal of Information Technology Ampera
Vol. 4, No. 3, 2023 e-ISSN: 2774-2121
https://journal-computing.org/index.php/journal-ita/index

Rancangan Infrastruktur Virtual Lab Untuk Mendukung Praktikum Keamanan Informasi Berdasarkan National Institute of Standards and Technology (NIST)

Doddy Ferdiansyah[1], Sali Alas Majapahit[2], Miftahul Fadli Muttaqin[3]

[1,2,3]Teknik Informatika, Universitas Pasundan, Bandung, Indonesia
Email: [1]doddy@unpas.ac.id, [2]sali@unpas.ac.id, [3]miftahulfadli@unpas.ac.id

Abstrak

Dalam era digital yang dinamis, kemajuan teknologi membawa peningkatan signifikan dalam kebutuhan sumber daya TI. Transformasi digital menjadi tren di banyak organisasi, yang berpindah dari layanan offline ke online. Namun, pertumbuhan ini juga menyertakan risiko keamanan yang lebih besar, terutama pada aset digital organisasi. Hal ini tercermin dari seringnya terjadi insiden Data Breach, Data Leak, dan Data Theft, yang mengancam reputasi dan integritas organisasi. Mengingat pentingnya keamanan siber, tujuan utama penelitian ini adalah mengembangkan sebuah sistem pengujian penetrasi (pentest) untuk aplikasi web sebelum dipublikasikan ke jaringan publik atau internet. Pengujian ini mencakup evaluasi keamanan secara internal dan eksternal, sehingga menjamin aplikasi lebih aman dari serangan siber. Penelitian ini menghasilkan rancangan komponen infrastruktur TI yang dapat mengimplementasikan konsep Penetration Testing. Desain ini dirancang berdasarkan standar Penetration Testing dari National Institute of Standards and Technology (NIST), memberikan kerangka kerja yang dapat diandalkan dan efektif untuk melindungi aplikasi-aplikasi web organisasi dari ancaman keamanan siber yang terus berkembang.

Kata Kunci: penetration testing, data breach, perancangan laboratorium, NIST

1. PENDAHULUAN

Meningkatnya insiden peretasan aplikasi dan pelanggaran data telah menimbulkan kekhawatiran serius di berbagai sektor, termasuk Pendidikan, Ekonomi, Perbankan, Industri, dan non-komersial. Tantangan ini tidak hanya berdampak pada organisasi yang menjadi target serangan, tetapi juga pada masyarakat pengguna layanan mereka, menciptakan lingkungan yang memerlukan perlindungan data dan keamanan aplikasi sebagai prioritas utama, bukan hanya bagi instansi yang bersangkutan tetapi juga bagi masyarakat luas.

Beberapa faktor dapat menyebabkan terjadinya insiden keamanan siber ini. Pertama, faktor manusia berperan penting, karena manusia secara alami rentan terhadap kesalahan, yang dapat menyebabkan celah keamanan [1]. Kedua, meskipun teknologi keamanan siber sangat canggih, keterbatasan sumber daya manusia yang mengelolanya tetap menjadi titik lemah [2]. Ketiga, keuntungan strategis yang dimiliki penjahat dunia maya memungkinkan mereka menemukan dan mengeksploitasi kelemahan dalam sistem [3]. Keempat, kejahatan dunia maya memberikan peluang yang menguntungkan bagi para pelakunya [3]. Kelima, kecenderungan manusia untuk lengah dalam pengelolaan keamanan siber menambah risiko serangan [4]. Terakhir, perkembangan teknologi yang sangat cepat sering kali sulit diikuti oleh upaya keamanan manusia, memunculkan pertanyaan apakah AI dapat mengambil alih tugas-tugas keamanan ini [5].

Kesimpulan dari enam alasan tersebut menunjukkan bahwa, seberapa canggih pun sistem yang dibangun, celah keamanan selalu ada dan dapat dieksploitasi oleh penjahat dunia maya. Risiko ini semakin meningkat ketika sebuah aplikasi dikembangkan tanpa melakukan pengujian yang memadai. Di samping itu, peraturan dalam UU Perlindungan Data Pribadi (PDP) menambah urgensi bagi organisasi untuk memastikan keamanan data pribadi dan pelanggan mereka [6].

Penelitian ini bertujuan untuk menyediakan fasilitas pengujian penetrasi (pentest) aplikasi bagi organisasi yang ingin menguji aplikasinya. Pengujian ini akan menghasilkan laporan tentang bug, error, dan celah keamanan yang memungkinkan peretas menyerang, mengikuti standar dari NIST 800-115 yang berfokus pada panduan dalam menilai dan menguji keamanan informasi [7]. Tujuan lain penelitian ini adalah untuk menyediakan kesempatan bagi mahasiswa teknik informatika, khususnya yang berfokus pada keamanan, untuk mendapatkan pengalaman praktis sebagai pentester. Melalui lab berbasis mesin virtual yang mencakup Kali Linux dan sistem operasi yang rentan, mahasiswa akan berkesempatan untuk menggunakan alat seperti Wireshark, Nmap, dan Burp Suite dalam serangkaian pelajaran praktis [8].

2. METODOLOGI PENELITIAN

Penelitian yang difokuskan pada pengujian penetrasi ini merujuk pada pedoman dan kerangka kerja yang telah ditetapkan oleh National Institute of Standards and Technology (NIST) dalam dokumen NIST 800-115. Dokumen ini menjelaskan dengan rinci langkah-langkah, metode, dan praktik terbaik dalam pelaksanaan pengujian penetrasi yang efektif [7]. Dengan mengacu pada pedoman NIST 800-115, penelitian ini mendapatkan dasar yang kuat untuk mengidentifikasi potensi kerentanan keamanan dalam sistem dan infrastruktur teknologi informasi serta

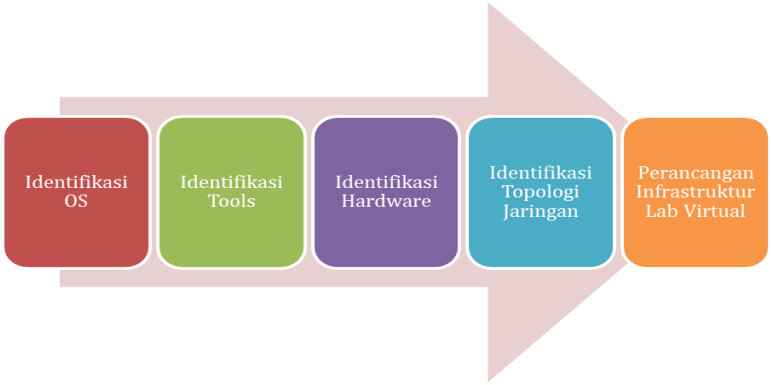
memberikan panduan dalam mengembangkan strategi pertahanan yang lebih tangguh.

Gambar 1. Metode Penelitian Berdasarkan NIST 800-115 [7]

Fokus utama dari penelitian ini adalah mengembangkan dengan cermat infrastruktur laboratorium virtual yang didedikasikan untuk kegiatan penetration testing, dengan landasan utama yang merujuk pada standar NIST 800-115 seperti digambarkan pada Gambar 1. Melalui pendekatan yang cermat dan komprehensif, tujuan penelitian ini adalah untuk menciptakan lingkungan laboratorium yang memberikan sarana untuk melakukan simulasi penetrasi yang efektif dan realistis. Dengan mematuhi pedoman yang dijelaskan dalam NIST 800-115, penelitian ini bertujuan untuk menghasilkan infrastruktur yang memungkinkan para profesional keamanan siber untuk menguji, menganalisis, dan meningkatkan tingkat keamanan sistem melalui skenario-skenario penetrasi yang mendalam dan terstruktur.

Dalam rangka menjalankan setiap fase pentest sesuai panduan NIST 800-115 [10], pendekatan yang akan diambil adalah memetakan setiap tahapan penting pada metodologi ini dengan sistem operasi (OS), alat-alat (tools), dan perangkat keras (hardware) yang paling sesuai dengan kebutuhan yang ada dalam lingkungan laboratorium virtual. Sehingga peran dari NIST disini adalah sebagai panduan dalam merancang laboratorium virtual untuk mendukung praktikum keamanan informasi. Hal ini bertujuan untuk menciptakan suatu lingkungan yang optimal dan representatif, memungkinkan uji coba serta eksplorasi yang mendalam terhadap setiap fase pentest, sehingga dapat dihasilkan pemahaman

yang komprehensif mengenai sistem keamanan dan potensi kerentanannya. Untuk tahapan pengerjaan penelitian ini dapat dilihar pada Gambar 2.



Gambar 2. Alur Penyelesaian Penelitian

Harapan yang muncul dari penelitian ini terkait dengan pengembangan laboratorium penetrasi (pentest) memiliki dimensi yang luas dan mendalam. Pertama-tama, diharapkan bahwa laboratorium ini akan menjadi lingkungan yang ideal untuk mengembangkan dan menguji kemampuan para profesional keamanan siber dalam mensimulasikan serangan nyata di lingkungan yang terkendali. Selain itu, diharapkan laboratorium ini akan menjadi sarana pelatihan yang efektif untuk melatih para ahli keamanan siber masa depan, memberikan mereka wawasan mendalam tentang metode dan teknik serangan, serta strategi tanggapannya.

Selanjutnya, harapannya adalah bahwa laboratorium ini dapat berperan sebagai sumber penelitian yang berkelanjutan, memungkinkan eksplorasi mendalam terhadap tren terbaru dalam dunia serangan siber dan metode perlindungan yang inovatif. Dengan demikian, diharapkan laboratorium ini akan berkontribusi pada pengembangan pengetahuan keamanan siber secara umum. Tidak kalah penting, harapannya adalah bahwa laboratorium ini akan mendorong kolaborasi antara para profesional keamanan siber, akademisi, dan industri, menciptakan suatu ekosistem di mana penelitian, pengembangan, dan implementasi solusi keamanan dapat terjadi dengan sinergi.

Secara keseluruhan, tujuan utama dari penelitian ini adalah untuk memberikan kontribusi yang signifikan terhadap pemahaman tentang keamanan siber [9] dan menghasilkan laboratorium pentest yang tidak hanya efektif dalam melatih dan menguji, tetapi juga berdampak pada kemajuan keamanan siber secara keseluruhan.

3. HASIL DAN PEMBAHASAN

3.1 HASIL PENGUJIAN

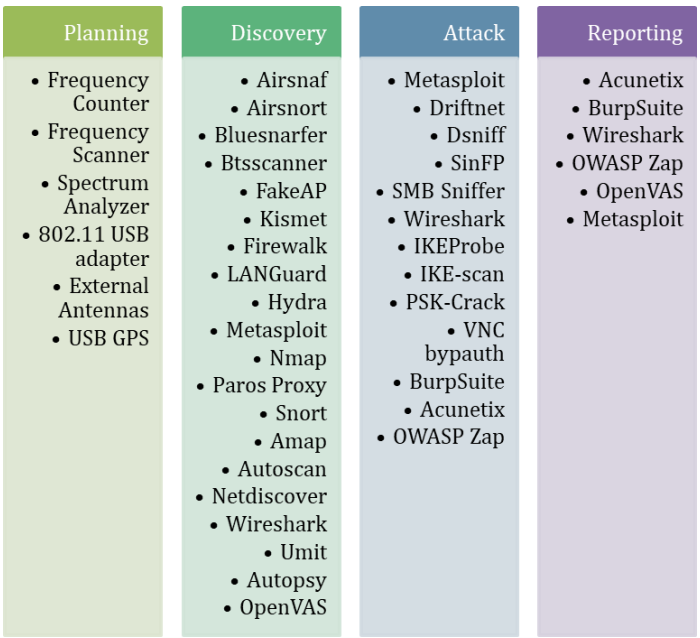
Proses awal yang krusial dalam merancang laboratorium uji penetrasi (pentest) adalah mengidentifikasi sistem operasi (OS) yang akan menjadi landasan bagi seluruh perancangan. Pemilihan OS ini menjadi langkah mendasar yang akan mempengaruhi keseluruhan kerangka kerja uji penetrasi. Dalam tahap ini, penting untuk mempertimbangkan faktor-faktor seperti kecocokan sistem dengan tujuan pengujian, keberlanjutan dukungan dan pemeliharaan OS, serta kebutuhan spesifik dari pengujian yang akan dilakukan. Dengan memahami secara mendalam karakteristik dan kemampuan masing-masing sistem operasi, proses identifikasi ini akan menjadi dasar kokoh untuk menciptakan lingkungan uji penetrasi yang efektif dan relevan. Dalam tahap ini, sistem operasi akan dikelompokkan berdasarkan kriteria tertentu, seperti tujuan penggunaan, kebutuhan perangkat keras, atau lingkungan pengembangan yang akan digunakan. Pengelompokkan ini akan membantu dalam mengatur pengaturan dan pengelolaan yang efisien untuk setiap jenis sistem operasi, serta memastikan bahwa sumber daya yang tersedia dimanfaatkan dengan optimal. Berikut daftar sistem operasi yang sudah diidentifikasi.

Tabel 1. Daftar Sistem Operasi

No	Sistem Operasi	Based	Peran
1	Windows XP	Windows	Target
	Windows 7	Windows	Target
	Windows 8.1	Windows	Target
	Windows 10	Windows	Target/host
	Windows server 2012 dan 2012 R2	Windows	Target
	Windows 11	Windows	Host
2	Kali Linux	Linux	Host
	Parrot Security OS	Linux	Host
	BlackArch Linux	Linux	Host
	Ubuntu	Linux	Target
3	MacOS X	MacOS	Host
4	VMware Workstation	Virtualisasi	Host

Kemudian, proses yang penting dalam menjalankan uji penetrasi (pentest) adalah mengidentifikasi alat-alat atau tools yang akan digunakan sesuai dengan tahapan yang dijelaskan dalam NIST 800-115. Tahapan ini menjadi panduan yang sangat

berharga dalam menyusun strategi dan pendekatan untuk menguji keamanan suatu sistem atau jaringan. Dengan memahami secara rinci setiap langkah yang diuraikan dalam NIST 800-115 [7], kita dapat dengan tepat menentukan tools pentest yang sesuai dengan kebutuhan dan tujuan uji penetrasi, sehingga dapat mendapatkan hasil yang akurat dan komprehensif dalam mengidentifikasi potensi kerentanan dan mengukur tingkat keamanan sistem.



Gambar 3. Daftar Tools di Setiap Fase NIST 800-115

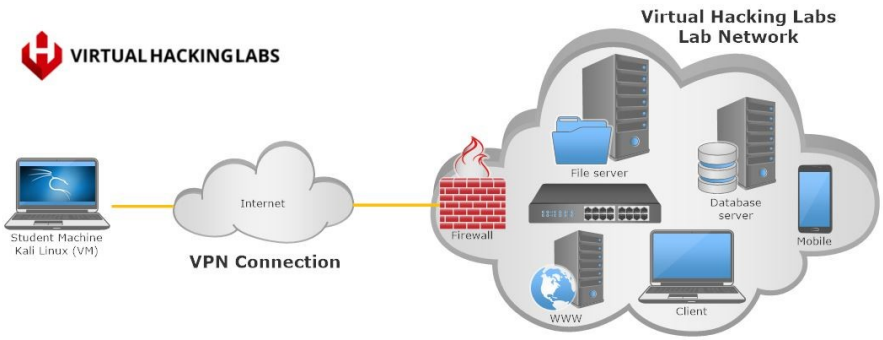
Dalam proses pengembangan perangkat pentest di dalam lingkungan laboratorium berbasis virtualisasi, langkah krusial yang harus diambil adalah mengidentifikasi kebutuhan hardware yang optimal. Kebutuhan hardware ini melibatkan pemilihan komponen yang sesuai untuk memastikan perangkat pentest beroperasi dengan efisiensi dan efektivitas. Pertimbangan utama meliputi CPU, RAM, penyimpanan, dan konektivitas jaringan. Kapasitas CPU yang cukup adalah penting, terutama mengingat aplikasi pengujian penetrasi yang memerlukan daya komputasi tinggi. CPU multi-core atau prosesor dengan kecepatan clock yang tinggi akan memungkinkan menjalankan alat-alat pentest yang memerlukan sumber daya yang signifikan. RAM juga harus mencukupi agar sistem dapat menjalankan beberapa mesin virtual (VM) bersamaan tanpa pengurangan kinerja yang signifikan. Ini akan memastikan kenyamanan dalam mengisolasi lingkungan pengujian.

Tabel 2. Kebutuhan Perangkat Keras Komputer Uji

No	Hardware	Specs
1	Processor	Ryzen 9 3900X 12 Core, 24 Thread Unlocked Desktop Processor with Wraith Prism LED Cooler
2	RAM	64GB DDR4 Trident Z Royal Silver 4000Mhz PC4-32000 CL18 1.40V Dual Channel Kit (2x32GB)
3	Storage	2TB PCIe Gen3 x4 NVMe M.2-2280 Internal Solid-State Drive with V-NAND Technology & 1024MB Cache (2x1TB)
4	Graphic Card	RTX 4090 24GB GDRR6X 384-Bit HDMI/DP Nvlink Tri-Frozr 3 Ada Lovelace Architecture OC Graphics Card
5	LAN Card	PCIe x4 10Gb/s Network Adapter Card with Single RJ-45 Port
6	Wireless Card	USB-AC68 AC1900 Dual-band USB 3.0 WiFi Adapter
7	Cooler	CPU Cooler - Three AF120 RGB Elite Fans
8	Monitor	2x 38 Inch UltraGear Nano IPS 1ms Curved Monitor with 144HZ Refresh Rate

Penelitian ini secara khusus mengarahkan perhatiannya pada pengembangan laboratorium pentest sebagai fasilitas pembelajaran praktek bagi mahasiswa. Pengujian penetrasi memerlukan lingkungan yang sesuai dan realistis, dan laboratorium virtual ini diharapkan dapat menghadirkan situasi nyata yang mencerminkan skenario peretasan yang mungkin terjadi di dunia nyata. Oleh karena itu, langkah identifikasi jaringan ini penting untuk memastikan bahwa pengaturan laboratorium pentest mencakup berbagai aspek jaringan yang relevan dan memadai untuk memenuhi tujuan pengajaran dan pembelajaran.

Hasil penelitian ini nantinya akan memberikan kontribusi yang berarti dalam konteks pendidikan. Mahasiswa akan memiliki akses ke laboratorium pentest yang didasarkan pada dasar-dasar jaringan yang valid, memungkinkan mereka untuk secara aktif terlibat dalam pengujian penetrasi dan eksperimen keamanan siber. Dengan demikian, penelitian ini memiliki implikasi penting dalam meningkatkan kualitas pendidikan dan persiapan mahasiswa dalam menghadapi tantangan kompleks dalam bidang keamanan siber.

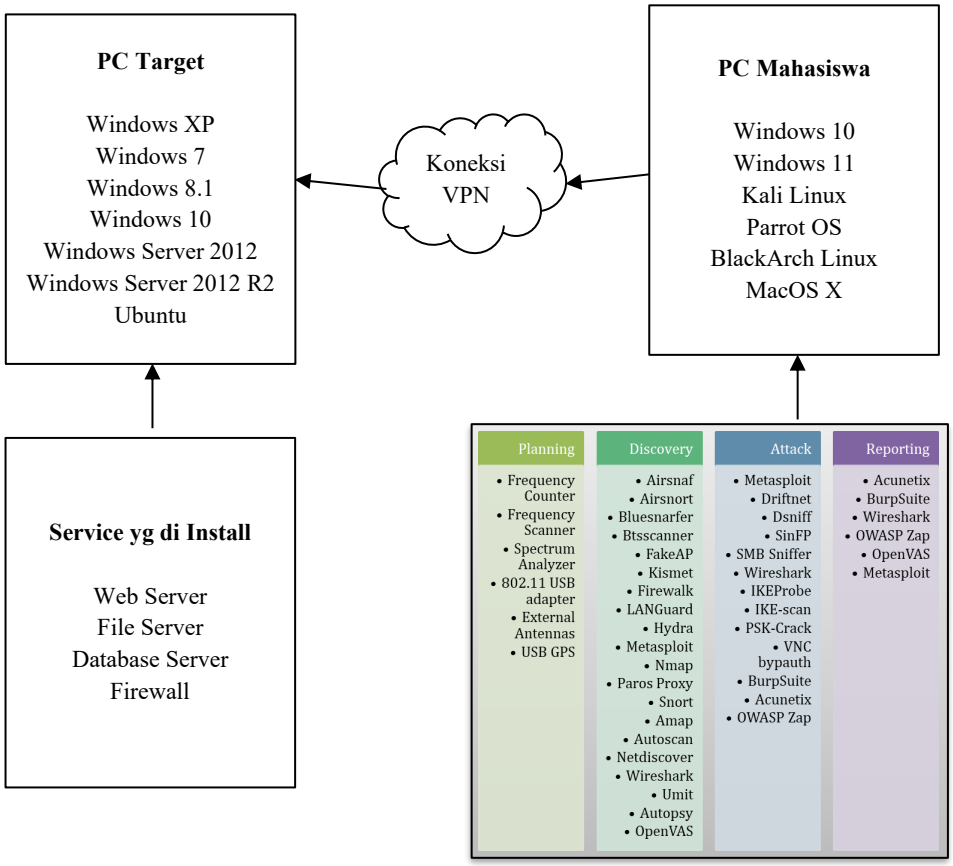


Gambar 4. Topologi Jaringan Lab Virtual Pentest

Dalam rangka merancang topologi laboratorium virtual yang memenuhi keperluan pengujian penetrasi, identifikasi dan pengaturan kebutuhan mendasar menjadi tahap yang penting. Kebutuhan ini melibatkan berbagai komponen yang saling berinteraksi, memberikan landasan bagi simulasi yang akurat dan mendalam terhadap kerentanan serta potensi ancaman keamanan dalam suatu sistem. Penting untuk mempertimbangkan adanya koneksi Virtual Private Network (VPN) sebagai fondasi keamanan yang mampu menghasilkan lingkungan terkendali, di mana akses diberikan hanya kepada pihak yang sah dan terotentikasi. Web server menjadi elemen integral dalam topologi ini, berfungsi sebagai titik fokus pengujian kerentanan pada aplikasi web, dan memungkinkan penilaian terhadap kerentanannya terhadap serangan seperti SQL injection atau Cross-Site Scripting (XSS).

Selanjutnya, hadirnya database server melibatkan aspek pengujian penetrasi terhadap lapisan penyimpanan data. Ini menjadi penting karena serangan terhadap basis data seringkali mengungkapkan celah yang signifikan dalam sistem. Komputer uji, sebagai entitas awal dalam rangkaian pengujian, memberikan titik awal dalam melakukan serangkaian eksperimen penting. File server dalam topologi ini menjadi bagian yang mengevaluasi bagaimana sistem mengelola akses terhadap berkas, juga bagaimana kerentanannya terhadap ancaman seperti serangan terhadap protokol SMB. Kehadiran switch dan firewall adalah langkah yang berfokus pada pengaturan lalu lintas jaringan yang aman dan pemisahan segmentasi, menjaga agar serangan tidak menyebar ke seluruh jaringan. Akhirnya, komputer target memainkan peran sentral sebagai sasaran uji penetrasi. Berdasarkan konfigurasi yang telah dibangun, komputer target akan menghadirkan tantangan berupa kerentanan-kerentanan yang beragam. Seluruh komponen ini saling berkolaborasi, membentuk ekosistem pengujian yang autentik dan konsekuensial. Melalui penggunaan topologi laboratorium virtual

yang cermat seperti ini, peneliti atau praktisi keamanan siber dapat mengembangkan pemahaman mendalam mengenai kerentanan dan potensi risiko dalam suatu system.



Gambar 5. Rancangan Infrastruktur Lab Virtual Pentest

Tahap perancangan infrastruktur dalam konteks pengembangan lingkungan pengujian penetrasi berbasis virtual memerlukan pendekatan yang teliti dan sistematis. Proses ini didasarkan pada hasil identifikasi yang telah dilakukan pada tahap sebelumnya, yang mencakup penentuan sistem operasi yang sesuai, alat-alat pengujian yang relevan, serta spesifikasi hardware yang diperlukan. Penggabungan elemen-elemen ini dalam perancangan infrastruktur bertujuan untuk menciptakan lingkungan yang mendukung pelaksanaan pengujian penetrasi dengan efisien dan akurat. Pengintegrasian sistem operasi yang telah diidentifikasi dengan perangkat keras yang memadai, serta alat-alat pengujian yang sesuai, akan membentuk dasar dari infrastruktur yang diharapkan dapat memberikan

wadah yang kuat untuk menguji keamanan suatu sistem atau jaringan. Dengan merinci komponen infrastruktur dan menggambarkannya secara sistematis, tahap perancangan ini memainkan peran penting dalam memastikan bahwa lingkungan pengujian dapat beroperasi sesuai dengan tujuan yang telah ditetapkan.

3.2 Pembahasan

Penelitian ini berfokus pada perancangan laboratorium pengujian penetrasi (pentest) yang mengadopsi pendekatan berbasis virtualisasi. Tujuan utama dari penelitian ini adalah mengembangkan suatu lingkungan yang memungkinkan pelaksanaan pengujian penetrasi dengan efisien dan efektif melalui penerapan teknologi virtualisasi. Dalam tahap identifikasi awal, penelitian ini secara teliti menganalisis dan mengidentifikasi sistem operasi yang sesuai, alat-alat pentest yang relevan, serta spesifikasi hardware yang dibutuhkan untuk mendukung lingkungan pengujian. Hasil identifikasi ini menjadi dasar bagi tahap perancangan infrastruktur, di mana elemen-elemen tersebut diintegrasikan secara holistik. Penerapan sistem operasi yang sesuai dan alat-alat pentest yang terkait dengan kebutuhan pengujian memberikan dasar yang kuat untuk lingkungan pengujian yang autentik dan realistis. Penelitian ini juga mengangkat peran teknologi virtualisasi dalam membentuk struktur dasar lingkungan pentest. Melalui pendekatan ini, penelitian ini menghasilkan desain infrastruktur yang dapat mengakomodasi berbagai scenario pengujian, mulai dari simulasi serangan hingga analisis keamanan lebih mendalam.

Selain itu, penelitian ini memberikan kontribusi penting dalam pembentukan lingkungan pentest yang dapat menghemat biaya dan waktu dalam perancangan dan pengaturan fisik. Dengan menggunakan teknologi virtualisasi, pengujian dapat dilakukan tanpa memerlukan berbagai perangkat keras fisik yang mahal. Lingkungan virtual ini memungkinkan fleksibilitas dalam menjalankan berbagai jenis pengujian dengan cepat, serta memudahkan pengelolaan dan replikasi lingkungan. Pada akhirnya, hasil penelitian ini memberikan landasan praktis bagi pembentukan laboratorium pentest berbasis virtual yang dapat dimanfaatkan oleh praktisi keamanan siber dan peneliti untuk menguji keamanan jaringan, sistem, dan aplikasi dalam lingkungan yang terkendali dan realistis. Dengan menggabungkan elemen-elemen seperti sistem operasi, alat-alat pentest, dan teknologi virtualisasi, penelitian ini menyediakan panduan berharga bagi perancangan laboratorium pentest yang sesuai dengan kebutuhan praktis dunia keamanan siber saat ini.

Tahapan berikutnya dalam perjalanan penelitian yang berjudul "Perancangan Lab Pentest Berbasis Virtual" melibatkan pemetaan kebutuhan alat-alat (tools) yang

akan digunakan dalam lingkungan pengujian penetrasi dengan standar yang ditetapkan oleh NIST 800-115. Proses ini adalah kelanjutan dari identifikasi dan perancangan infrastruktur, yang menyoroti pentingnya pemilihan alat-alat yang tepat dan sesuai dengan kebutuhan pengujian serta standar industri yang diakui. Pemetaan kebutuhan alat dengan standar NIST 800-115 melibatkan analisis menyeluruh terhadap daftar alat-alat yang diakui dan diakui oleh standar tersebut. Selain itu, alat-alat ini juga harus relevan dengan tujuan pengujian yang telah ditetapkan sebelumnya. Setiap alat akan dievaluasi berdasarkan karakteristik dan fitur-fitur yang mereka tawarkan, seperti pemindaian kerentanan, analisis keamanan, dan pengujian penetrasi pada berbagai lapisan sistem dan jaringan. Penting untuk memilih alat-alat yang memberikan cakupan yang tepat sesuai dengan lingkungan dan sistem yang akan diuji, sekaligus mempertimbangkan spesifikasi dan fitur yang relevan dengan standar NIST 800-115. Proses pemetaan ini juga mencakup peninjauan mendalam terhadap dokumentasi resmi masing-masing alat, serta ketersediaan sumber daya dan dukungan untuk penggunaannya. Hasil dari tahap ini akan berupa daftar final alat-alat yang akan digunakan dalam lingkungan pengujian berbasis virtual. Dengan mengikuti standar NIST 800-115, tahap pemetaan ini memberikan dasar yang kokoh bagi kelangsungan pengujian penetrasi, yang pada gilirannya akan menghasilkan hasil yang handal dan sesuai dengan praktik terbaik dalam industri keamanan siber.
Selain melakukan pemetaan, tahapan berikutnya dalam perjalanan penelitian ini adalah pembuatan prosedur pengujian penetrasi (pentest) berdasarkan standar NIST 800-115, yang dirancang khusus untuk memenuhi kebutuhan praktek mahasiswa. Proses ini berfokus pada konversi standar teoritis dari NIST 800-115 menjadi langkah-langkah operasional yang dapat diikuti dan diterapkan oleh mahasiswa sebagai bagian dari pengalaman praktik mereka.

4. KESIMPULAN

Dari penelitian yang sudah dilakukan, maka telah dibuatnya sebuah rancangan infrastruktur teknologi informasi (TI) terhadap laboratorium praktikum keamanan informasi berbasis virtualisasi. Salah satu pendekatan dalam menentukan kebutuhaan tools dan sistem operasi adalah dengan mengacu pada NIST 800-115. Dimana setiap fase pengujian penetrasi berdasarkan NIST 800-115 yang memiliki empat langkah yaitu planning, discovery, attack, dan reporting sudah berhasil mengidentifikasi seluruh kebutuhan tools dan sistem operasi yang akan digunakan pada penelitian berikutnya. Selain kebutuhan tools dan sistem operasi, penilitian ini juga menghasilkan rancangan jaringan yang akan menghubungkan antara PC target yang akan di serang dengan PC mahasiswa sebagai penguji (tester). Dimana koneksi yang digunakan adalah Virtual Private Network (VPN)

agar dapat di akses dari luar jaringan kampus dan mengamankan koneksi agar terhindar dari interferensi dan intersepsi pada jalur komunikasi atau jaringan.

REFERENSI

[1] K. R. Kont, "Libraries and cyber security: the importance of the human factor in preventing cyber attacks," Library Hi Tech News, 2023.

[2] Bandoi, C. Sitnikov, D. Danciulescu, L. Mandache, and I. Riza, "The Importance of Human Resources Competencies in Organisational Cyber Risk Management," in Managing Risk and Decision Making in Times of Economic Distress, Part B, vol. 108, pp. 75-90, Emerald Publishing Limited, 2022.

[3] F. Lemieux, "Cyber Threats, Intelligence Operations, and Mass Surveillance," in Intelligence and State Surveillance in Modern Societies, pp. 139-163, Emerald Publishing Limited, 2018.

[4] Oxford Analytica, "State cyber threats will multiply globally," Emerald Expert Briefings, oxan-db, 2016.

[5] Y. R. Masakowski, "Artificial intelligence and the future global security environment," in Artificial Intelligence and Global Security: Future Trends, Threats and Considerations, pp. 1-34, Emerald Publishing Limited, 2020.

[6] "Undang-undang (UU) Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi," Indonesia, 17 Oktober 2022. [Online]. Available: https://peraturan.bpk.go.id

[7] K. Scarfone, M. Souppaya, A. Cody, and A. Orebaugh, "Technical guide to information security testing and assessment," NIST Special Publication, 800(115), pp. 2-25, 2008.

[8] G. D. Singh, Learn Kali Linux 2019: Perform Powerful Penetration Testing Using Kali Linux, Metasploit, Nessus, Nmap, and Wireshark, Packt Publishing Ltd, 2019.

[9] Q. S. Qassim, N. Jamil, M. Daud, A. Patel, and N. Ja'affar, "A review of security assessment methodologies in industrial control systems," Information & Computer Security, vol. 27, no. 1, pp. 47-61, 2019.

[10] W. Wardana, A. Almaarif, and A. Widjajarto, "Vulnerability assessment and penetration testing on the xyz website using NIST 800-115 standard," J. Ilm. Indones, vol. 7, no. 1, pp. 520-529, 2022.