Pelatihan Dasar Keamanan Jaringan Menggunakan Nmap bagi Siswa SMA/SMK se-Kota Cirebon

Bambang Sugiarto[1], Arif Nursetya[2], Kusnadi[3]
[1]bambangsugiarto@cic.ac.id, [2]arifnursetya@cic.ac.id, [3]Kusnadi@cici.ac.id
[1,2,3]Program Studi Teknik Informatika, Fakultas Teknologin Informasi, Universitas Catur Insan Cendekia, Cirebon 45133

Artikel Info

Kata kunci:

Keamanan jaringan
NMAP
Pelatihan
Literasi digital
Analisis jaringan

ABSTRAK

Keamanan jaringan merupakan aspek penting dalam era digital, terutama bagi generasi muda yang semakin bergantung pada teknologi informasi. Kurangnya pemahaman dasar mengenai keamanan jaringan dapat menimbulkan risiko penyalahgunaan data dan serangan siber. Oleh karena itu, kegiatan pengabdian masyarakat ini dilaksanakan dengan tujuan memberikan pelatihan dasar penggunaan Nmap sebagai salah satu perangkat analisis jaringan kepada siswa SMA 1 Cirebon, SMK 1 Cirebon, dan SMK Wahidin Cirebon. Metode yang digunakan adalah pelatihan tatap muka dengan pendekatan praktik langsung, meliputi pengenalan konsep dasar keamanan jaringan, instalasi Nmap, serta simulasi pemindaian jaringan sederhana. Peserta diberikan modul pembelajaran dan didampingi dalam setiap tahap praktik untuk memastikan pemahaman yang komprehensif. Hasil kegiatan menunjukkan bahwa mayoritas siswa mampu memahami fungsi dasar Nmap dan dapat melakukan pemindaian jaringan secara mandiri. Selain itu, terjadi peningkatan kesadaran siswa terhadap pentingnya keamanan jaringan dalam aktivitas sehari-hari. Kesimpulannya, pelatihan ini berhasil meningkatkan literasi keamanan jaringan di kalangan siswa SMA 1 Cirebon, SMK 1 Cirebon, dan SMK Wahidin Cirebon serta memberikan bekal keterampilan praktis yang relevan dengan kebutuhan dunia digital saat ini.

Author Korespondensi :

Bambang Sugiarto,
Program Studi Teknik Informatika
Fakultas Teknologi Informasi
Universitas Catur Insan Cendekia, Cirebon 45133
Email: bambangsugiarto@cic.ac.id

1. PENDAHULUAN (10 PT)

Perkembangan teknologi informasi yang pesat telah membawa dampak signifikan terhadap aktivitas sehari-hari, termasuk di bidang pendidikan. Salah satu isu utama yang muncul adalah keamanan jaringan komputer, yang semakin rentan terhadap serangan siber seperti pencurian data, penyadapan, dan peretasan website [1], [2]. Serangan siber tidak hanya menargetkan institusi besar, tetapi juga sekolah dan lembaga pendidikan yang sering kali memiliki sistem keamanan terbatas. Kondisi ini menuntut adanya pemahaman dasar mengenai keamanan jaringan sejak dini, khususnya bagi siswa SMA/SMK yang akan menjadi generasi penerus di bidang teknologi informasi [3], [4]. Kurangnya literasi keamanan jaringan dapat menimbulkan risiko besar, baik bagi individu maupun institusi pendidikan, mulai dari kebocoran data pribadi hingga gangguan operasional sistem pembelajaran.

Isu literasi digital di kalangan pelajar menjadi semakin relevan dengan meningkatnya penggunaan internet untuk kegiatan akademik, seperti e-learning, ujian berbasis komputer, dan komunikasi daring [5], [6]. Tanpa pemahaman yang memadai mengenai keamanan jaringan, siswa berpotensi menjadi korban serangan siber atau bahkan secara tidak sadar melakukan praktik yang membahayakan system [7], [8], [9], [10]. Oleh karena itu, pelatihan berbasis praktik langsung mengenai keamanan jaringan menjadi salah satu solusi strategis untuk membekali siswa dengan keterampilan dasar yang dapat diaplikasikan dalam kehidupan sehari-hari maupun dalam dunia kerja di masa depan.

Sejumlah penelitian terdahulu telah menyoroti efektivitas Nmap sebagai perangkat analisis jaringan. Chairil dan Jenih menekankan penggunaan Nmap dalam audit keamanan jaringan berbasis Linux, yang terbukti mampu mendeteksi port terbuka dan host aktif secara akurat [11]. Muhyidin dkk. membandingkan Nmap dengan Nikto dalam menguji keamanan website, dan hasilnya menunjukkan keunggulan Nmap dalam mendeteksi kerentanan system [12]. Walidin dkk. mengintegrasikan Nmap dengan Wireshark dan Metasploit dalam sistem operasi Kali Linux untuk analisis komprehensif, sementara penelitian lain menggunakan Nmap dalam monitoring jaringan hotel, yang membuktikan efektivitasnya dalam mendeteksi host dan kerentanan jaringan secara real-time [1].

Namun, penelitian-penelitian tersebut lebih banyak berfokus pada lingkungan profesional atau studi kasus institusi. Kontribusi utama penelitian ini adalah membawa konsep dan praktik dasar penggunaan Nmap ke ranah pendidikan menengah, melalui pelatihan bagi siswa SMA 1 Cirebon, SMK 1 Cirebon, dan SMK Wahidin Cirebon. Dengan pendekatan pengabdian masyarakat, penelitian ini menempati posisi unik sebagai upaya peningkatan literasi digital sekaligus penanaman kesadaran akan pentingnya keamanan jaringan sejak usia sekolah.

Selain itu, penelitian ini juga memberikan nilai tambah berupa transfer teknologi dari dunia akademik ke masyarakat, khususnya pelajar. Dengan melibatkan siswa secara langsung dalam praktik penggunaan Nmap, kegiatan ini tidak hanya memperkenalkan konsep keamanan jaringan, tetapi juga melatih keterampilan analisis yang dapat mendukung pembelajaran berbasis teknologi. Hal ini sejalan dengan kebutuhan dunia pendidikan yang semakin menekankan pada hands-on learning dan keterampilan abad 21, seperti pemecahan masalah, berpikir kritis, dan literasi digital [13], [14], [15].

Lebih jauh, kegiatan ini juga mendukung agenda nasional dalam meningkatkan literasi digital masyarakat Indonesia sebagaimana dicanangkan oleh Kementerian Komunikasi dan Informatika. Literasi digital tidak hanya mencakup kemampuan menggunakan perangkat teknologi, tetapi juga mencakup kesadaran akan keamanan dan etika dalam berinternet. Dengan memberikan pelatihan keamanan jaringan kepada siswa, penelitian ini berkontribusi pada pencapaian tujuan tersebut, sekaligus memperkuat kapasitas sekolah dalam menghadapi tantangan era digital.

Selain mendukung kebijakan nasional, penelitian ini juga relevan dengan tren global. Laporan dari berbagai lembaga internasional menunjukkan bahwa serangan siber terhadap sektor pendidikan meningkat signifikan dalam lima tahun terakhir. Hal ini menegaskan bahwa sekolah bukan lagi target yang diabaikan, melainkan menjadi sasaran empuk bagi pelaku kejahatan siber karena lemahnya sistem pertahanan. Oleh sebab itu, membekali siswa dengan keterampilan dasar keamanan jaringan melalui pelatihan Nmap menjadi langkah strategis untuk membangun budaya keamanan sejak dini.

Lebih lanjut, penelitian ini juga menegaskan pentingnya peran sekolah sebagai pusat literasi digital. Sekolah tidak hanya berfungsi sebagai tempat transfer ilmu pengetahuan, tetapi juga sebagai ruang pembentukan karakter dan kesadaran teknologi. Dengan adanya pelatihan keamanan jaringan, siswa tidak hanya belajar mengenai aspek teknis, tetapi juga memahami nilai etika dalam penggunaan teknologi. Hal ini penting untuk membangun generasi yang tidak hanya cakap secara digital, tetapi juga bertanggung jawab dalam menjaga keamanan informasi.

Selain itu, kegiatan ini memberikan manfaat jangka panjang bagi institusi pendidikan. Dengan meningkatnya pemahaman siswa mengenai keamanan jaringan, sekolah dapat lebih siap menghadapi tantangan era digital, termasuk penerapan sistem pembelajaran daring yang aman dan terlindungi dari ancaman siber. Dengan demikian, pelatihan ini tidak hanya memberikan manfaat langsung bagi siswa, tetapi juga memperkuat ekosistem pendidikan secara keseluruhan. Dengan demikian, penelitian ini tidak hanya memperluas pemahaman siswa mengenai teknologi keamanan jaringan, tetapi juga memberikan bekal keterampilan praktis yang relevan dengan kebutuhan dunia digital. Hasil dari kegiatan ini diharapkan dapat menjadi model pengabdian masyarakat yang dapat direplikasi di sekolah lain, sehingga literasi keamanan

jaringan dapat berkembang secara lebih luas di kalangan pelajar dan mendukung terciptanya ekosistem pendidikan yang aman, adaptif, dan berdaya saing di era globalisasi.

2. METODE

Metode pelaksanaan kegiatan pengabdian masyarakat ini dirancang untuk menjawab permasalahan mitra secara sistematis melalui tahapan analisis, perancangan, implementasi, dan evaluasi. Fokus utama adalah peningkatan literasi keamanan jaringan bagi siswa SMA/SMK melalui pelatihan penggunaan Nmap.

2.1. Permasalahan Mitra dan Solusi

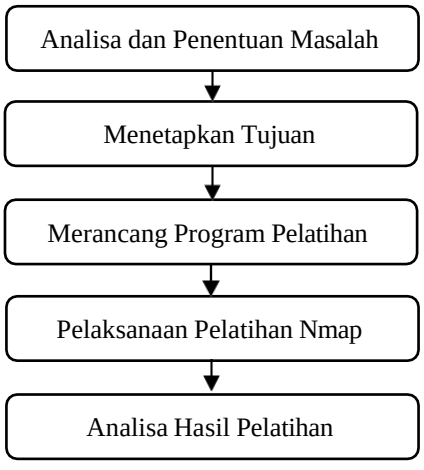
Permasalahan yang dihadapi mitra diidentifikasi melalui wawancara dengan guru, observasi kegiatan belajar, serta diskusi dengan siswa. Berikut tabel permasalahan dan solusi yang ditawarkan:

Tabel 1 Permasalahan dan Solusi

	Permasalahan		Solusi
1.	Rendahnya pemahaman siswa mengenai konsep dasar keamanan jaringan	1.	Memberikan materi pengantar tentang keamanan jaringan dan ancaman siber
2.	Siswa belum mengenal perangkat analisis jaringan seperti Nmap	2.	Pelatihan penggunaan Nmap mulai dari instalasi hingga praktik pemindaian port dan host
3.	Kurangnya keterampilan praktis dalam mengidentifikasi kerentanan jaringan	3.	Praktik langsung dengan simulasi jaringan sederhana menggunakan Nmap
4.	Minimnya kesadaran siswa terhadap pentingnya literasi digital dan etika berinternet	4.	Diskusi interaktif dan refleksi hasil pelatihan untuk menanamkan kesadaran keamanan

2.2. Alur Kegiatan

Alur kegiatan pelatihan dirancang dalam lima tahap utama yang saling berkesinambungan dan membentuk suatu proses sistematis, dimulai dari analisa serta penentuan masalah yang dihadapi mitra, dilanjutkan dengan penetapan tujuan yang jelas sebagai arah kegiatan, kemudian perancangan program pelatihan yang terstruktur, pelaksanaan pelatihan secara langsung kepada siswa sebagai inti kegiatan, hingga tahap akhir berupa analisa hasil pelatihan untuk menilai efektivitas dan memberikan rekomendasi tindak lanjut:



Gambar 1 Alur Kegiatan

(1) Analisa dan Penentuan Masalah Pada tahap ini dilakukan identifikasi kondisi mitra melalui observasi dan wawancara dengan guru serta siswa untuk mengetahui permasalahan utama yang dihadapi, yaitu rendahnya literasi keamanan jaringan dan minimnya keterampilan praktis dalam penggunaan perangkat analisis jaringan. (2) Menetapkan Tujuan Tujuan yang dirumuskan berfokus pada peningkatan pemahaman siswa

mengenai konsep dasar keamanan jaringan, pengenalan perangkat Nmap, serta keterampilan praktis dalam melakukan pemindaian port dan host. Penetapan tujuan ini menjadi dasar arah kegiatan agar sesuai dengan kebutuhan mitra. (3) Perancangan Program Pelatihan Pada fase ini disusun modul pelatihan berbasis praktik yang mencakup teori singkat mengenai keamanan jaringan, pengenalan Nmap, serta simulasi jaringan sederhana. Selain itu, dilakukan persiapan perangkat lunak, PC, dan jaringan lokal yang akan digunakan dalam kegiatan. (4) Pelaksanaan Pelatihan Pada Siswa Pelatihan dimulai dengan penyampaian teori dasar untuk memberikan landasan konseptual, dilanjutkan dengan demonstrasi penggunaan Nmap oleh instruktur. Setelah itu, siswa melakukan praktik mandiri dengan bimbingan sehingga mereka dapat secara langsung mengidentifikasi port terbuka dan host aktif pada jaringan simulasi. (5) Analisa Hasil Pelatihan Evaluasi dilakukan melalui pre-test dan post-test untuk mengukur peningkatan pengetahuan siswa, serta observasi keterampilan saat praktik. Hasil evaluasi kemudian dianalisis untuk mengetahui efektivitas pelatihan, dilanjutkan dengan refleksi bersama siswa dan guru guna menanamkan kesadaran akan pentingnya literasi digital dan keamanan jaringan.

3. PEMBAHASAN HASIL

Program kemitraan masyarakat ini dilaksanakan pada tanggal 06 Desember 2025 bertempat di ruang Laboratorium Komputer Universitas Catur Insan Cendekia, sebuah fasilitas yang secara rutin digunakan untuk kegiatan praktik mahasiswa maupun pelatihan berbasis teknologi. Pemilihan lokasi ini bukan tanpa alasan, melainkan didasarkan pada ketersediaan perangkat komputer yang memadai, jaringan internet yang stabil, serta suasana ruang yang mendukung pelaksanaan pelatihan berbasis praktik langsung. Laboratorium Komputer menjadi tempat yang strategis karena telah terbiasa digunakan untuk kegiatan eksplorasi teknologi, sehingga siswa peserta pelatihan dapat dengan mudah beradaptasi dengan lingkungan belajar yang kondusif. Dengan dukungan fasilitas tersebut, kegiatan pelatihan dapat berjalan lebih efektif, interaktif, dan sesuai dengan tujuan peningkatan literasi digital.

Pelaksanaan kegiatan ini melibatkan siswa dari beberapa sekolah mitra, yaitu SMA 1 Cirebon, SMK 1 Cirebon, dan SMK Wahidin Cirebon. Kehadiran siswa dari berbagai latar belakang sekolah memberikan dinamika tersendiri dalam proses pelatihan, karena mereka dapat saling bertukar pengalaman dan pengetahuan. Setiap tahapan pelatihan diikuti dengan antusias, mulai dari pengenalan konsep dasar keamanan jaringan, pemahaman mengenai ancaman siber yang sering terjadi, hingga praktik langsung penggunaan perangkat lunak Nmap. Dalam praktik tersebut, siswa diajak untuk melakukan pemindaian port dan host, mengidentifikasi kerentanan jaringan, serta memahami bagaimana hasil analisis dapat digunakan untuk meningkatkan keamanan sistem.

Dokumentasi kegiatan yang ditampilkan pada Gambar 2 memperlihatkan suasana pelatihan secara nyata, mulai dari interaksi antara instruktur dengan siswa, diskusi kelompok kecil, hingga aktivitas praktik yang menjadi inti dari program ini. Dokumentasi tersebut tidak hanya berfungsi sebagai bukti pelaksanaan kegiatan, tetapi juga sebagai media refleksi yang menunjukkan keterlibatan aktif peserta. Kehadiran siswa yang fokus mengikuti arahan instruktur, serta keberhasilan mereka dalam menyelesaikan simulasi jaringan, menjadi indikator bahwa program ini berjalan sesuai dengan rencana.

Lebih jauh, dokumentasi kegiatan juga memperlihatkan bagaimana program kemitraan masyarakat ini mampu menciptakan suasana belajar yang kolaboratif. Siswa tidak hanya belajar secara individual, tetapi juga bekerja sama dalam kelompok untuk menyelesaikan tugas praktik. Hal ini sejalan dengan tujuan pelatihan yang tidak hanya menekankan aspek teknis, tetapi juga membangun keterampilan abad 21 seperti kerja sama tim, komunikasi, dan pemecahan masalah. Dengan demikian, kegiatan ini tidak hanya meningkatkan literasi digital dan keterampilan keamanan jaringan, tetapi juga memperkuat karakter siswa sebagai calon generasi yang siap menghadapi tantangan era digital.

Secara keseluruhan, pelaksanaan program kemitraan masyarakat di Laboratorium Komputer Universitas Catur Insan Cendekia pada tanggal 06 Desember 2025 dapat dikatakan berhasil. Dokumentasi kegiatan yang ditampilkan pada Gambar 2 menjadi bukti nyata keterlibatan peserta, efektivitas metode pelatihan berbasis praktik, serta keberhasilan program dalam mencapai tujuan utamanya, yaitu meningkatkan literasi digital dan keterampilan keamanan jaringan di kalangan pelajar. Keberhasilan ini diharapkan dapat menjadi model yang dapat direplikasi di sekolah lain, sehingga manfaat program dapat dirasakan lebih luas oleh masyarakat pendidikan.kemitraan masyarakat ini dilaksanakan pada tanggal 06 Desember 2025 bertempat di ruang Laboratorium Komputer Universitas Catur Insan Cendekia, sebuah fasilitas yang secara rutin digunakan untuk kegiatan praktik. Pemilihan lokasi ini didasarkan pada ketersediaan perangkat

komputer yang memadai serta suasana ruang yang mendukung pelaksanaan pelatihan berbasis praktik langsung. Laboratorium Komputer menjadi tempat yang strategis untuk kegiatan eksplorasi teknologi di ruangan tersebut, sehingga pelatihan dapat berjalan lebih efektif dan kondusif. Kegiatan berlangsung dengan melibatkan siswa dari beberapa sekolah mitra, yaitu SMA 1 Cirebon, SMK 1 Cirebon, dan SMK Wahidin Cirebon, yang secara aktif mengikuti setiap tahapan pelatihan mulai dari pengenalan konsep dasar keamanan jaringan hingga praktik penggunaan Nmap. Dokumentasi kegiatan yang ditampilkan pada Gambar 2 memperlihatkan suasana pelatihan, interaksi antara instruktur dan siswa, serta aktivitas praktik yang menjadi inti dari program ini. Dokumentasi tersebut sekaligus menjadi bukti keterlibatan peserta dan keberhasilan pelaksanaan program kemitraan masyarakat dalam meningkatkan literasi digital dan keterampilan keamanan jaringan di kalangan pelajar.

Gambar 2 Proses Pelaksanaan Kegiatan Pelatihan

Pada Gambar 3 merupakan dalam rangka memberikan pemahaman praktis kepada siswa mengenai teknik analisis keamanan jaringan, peserta pelatihan diminta untuk mengidentifikasi contoh situs web yang memiliki potensi kerentanan atau kelemahan sistem, dengan tetap memperhatikan aspek legalitas dan etika digital. Situs-situs tersebut dipilih bukan untuk diserang atau dieksploitasi, melainkan sebagai objek studi dalam simulasi pemindaian menggunakan perangkat lunak Nmap. Proses ini dilakukan dalam lingkungan yang terkontrol, dengan tujuan utama untuk melatih mahasiswa dalam mengenali struktur jaringan, memahami konsep port scanning, serta menginterpretasikan hasil pemindaian secara bertanggung jawab. Dalam pelaksanaannya, mahasiswa diarahkan untuk menggunakan situs uji coba atau simulasi yang telah disiapkan oleh instruktur, seperti DVWA (Damn Vulnerable Web Application), OWASP Juice Shop, atau Metasploitable, yang secara khusus dirancang untuk keperluan pembelajaran keamanan jaringan. Dengan pendekatan ini, mahasiswa dapat memperoleh pengalaman langsung dalam melakukan scanning web tanpa melanggar hukum atau etika profesi, sekaligus membangun kesadaran akan pentingnya praktik ethical hacking dalam dunia teknologi informasi.

Gambar 3 Proses Pelaksanaan Pelatihan Kegiatan

Gambar 4 merupakan dokumentasi kegiatan yang diambil setelah pelaksanaan pelatihan keamanan jaringan menggunakan Nmap. Foto ini diambil di ruang Laboratorium Komputer Universitas Catur Insan Cendekia, sesaat setelah seluruh rangkaian pelatihan selesai dilaksanakan. Suasana menunjukkan tingkat antusiasme siswa yang tinggi selama kegiatan pelatihan berlangsung.

Gambar 4 Dokumentasi Setelah Selesai Kegiatan Pelatihan

Hasil penelitian dan pengujian yang diperoleh disajikan dalam bentuk uraian teoritik, baik secara kualitatif maupun kuantitatif. Hasil percobaan sebaiknya ditampilkan dalam berupa grafik atau pun tabel. Untuk grafik dapat mengikuti format untuk diagram dan gambar. Grafik dan gambar harus ada penjelasannya dalam teks atau harus diacu dalam teks.

Tabel 2 Perbandingan Nilai Post-test dan Pre-test Siswa

No	Siswa	Nilai Pre-test	Nilai Post-test
1.	Siswa A	50	80
2.	Siswa B	55	85
3.	Siswa C	60	88
4.	Siswa D	52	78
5.	Siswa E	58	90

Dari data dalam Tabel 2 tersebut mencerminkan bahwa siswa mengalami peningkatan pemahaman yang signifikan setelah mengikuti pelatihan keamanan jaringan menggunakan Nmap. Nilai rata-rata post-test menunjukkan lonjakan yang cukup tinggi dibandingkan dengan nilai pre-test, yang menandakan bahwa materi pelatihan berhasil diserap dengan baik oleh peserta. Peningkatan ini tidak hanya menunjukkan keberhasilan metode pelatihan berbasis praktik langsung, tetapi juga mengindikasikan bahwa siswa mampu mengaplikasikan konsep-konsep dasar keamanan jaringan dalam simulasi nyata. Selain itu, hasil ini mencerminkan bahwa pendekatan hands-on learning yang diterapkan dalam kegiatan pelatihan mampu meningkatkan keterampilan analisis teknis siswa, khususnya dalam melakukan pemindaian port dan identifikasi host aktif. Dengan demikian, pelatihan ini tidak hanya berdampak pada aspek kognitif, tetapi juga pada penguatan literasi digital dan kesiapan siswa menghadapi tantangan dunia kerja di bidang teknologi informasi.

4. KESIMPULAN

Hasil menunjukkan bahwa pelatihan keamanan jaringan menggunakan Nmap berhasil meningkatkan pemahaman siswa mengenai konsep dasar keamanan jaringan sekaligus keterampilan praktis dalam

melakukan pemindaian port dan host. Nilai rata-rata post-test mengalami peningkatan signifikan dibandingkan dengan nilai pre-test, sehingga dapat disimpulkan bahwa metode pelatihan berbasis praktik langsung lebih efektif dibandingkan hanya penyampaian teori. Kelebihan dari penelitian ini terletak pada keberhasilan dalam membangun keterampilan abad 21 seperti kerja sama tim, komunikasi, dan pemecahan masalah. Namun demikian, kegiatan ini juga memiliki beberapa kekurangan, antara lain pelatihan yang masih terbatas pada simulasi jaringan sederhana, waktu pelaksanaan yang relatif singkat sehingga belum memungkinkan eksplorasi mendalam terhadap fitur-fitur Nmap, serta evaluasi yang lebih berfokus pada aspek pengetahuan dan keterampilan teknis tanpa menyentuh aspek sikap atau perilaku digital secara komprehensif. Oleh karena itu, pengembangan selanjutnya dapat dilakukan dengan memperluas skenario jaringan yang lebih kompleks, mengintegrasikan aplikasi keamanan jaringan lain seperti Wireshark atau Snort, serta menyusun modul berbasis e-learning agar dapat diakses secara mandiri oleh siswa. Untuk menutup kekurangan penelitian, disarankan agar penelitian lanjutan memperpanjang durasi pelatihan, melakukan evaluasi longitudinal guna melihat dampak jangka panjang terhadap literasi digital siswa, melibatkan lebih banyak sekolah mitra agar hasil lebih representatif, serta menambahkan aspek pengukuran sikap dan etika digital sehingga hasil penelitian menjadi lebih komprehensif dan bermanfaat bagi pengembangan literasi keamanan jaringan di kalangan pelajar.

UCAPAN TERIMA KASIH

Ucapan terima kasih kami sampaikan kepada Universitas Catur Insan Cendekia yang telah memberikan dukungan penuh berupa fasilitas Laboratorium Komputer sehingga kegiatan pelatihan dapat terlaksana dengan baik. Kami juga menyampaikan apresiasi kepada para guru pendamping dari SMA 1 Cirebon, SMK 1 Cirebon, dan SMK Wahidin Cirebon yang telah memotivasi serta mendampingi siswa selama kegiatan berlangsung.

Tidak lupa, kami mengucapkan terima kasih kepada seluruh siswa peserta pelatihan yang telah berpartisipasi aktif dalam setiap tahapan kegiatan, mulai dari pengenalan konsep dasar keamanan jaringan hingga praktik penggunaan Nmap. Antusiasme dan semangat belajar yang ditunjukkan menjadi faktor penting keberhasilan program ini.

REFERENCES

[1] A. Prana Walidin *et al.*, “KALI LINUX SEBAGAI ALAT ANALISIS KEAMANAN JARINGAN MELALUI PENGGUNAAN NMAP, WIRESHARK, DAN METASPLOIT,” 2025.

[2] R. Taupaani and R. Harwahyu, “ZTSCAN: ENHANCING ZERO TRUST RESOURCE DISCOVERY WITH MASSCAN AND NMAP INTEGRATION,” *JITK (Jurnal Ilmu Pengetahuan dan Teknologi Komputer)*, vol. 10, no. 4, pp. 868–877, May 2025, doi: 10.33480/jitk.v10i4.6628.

[3] S. Parulian, D. A. Pratiwi, and M. Cahya Yustina, “Ancaman dan Solusi Serangan Siber di Indonesia.” [Online]. Available: http://ejournal.upi.edu/index.php/TELNECT/

[4] R. Ripai, R. A. Pari, F. Sidik, S. V. Shandy, and F. Mahardika, “Implementasi Layanan Cloudflare sebagai Mitigasi terhadap Ancaman Pemindaian dan Eksploitasi Siber Menggunakan Nmap dan Metasploit,” *sudo Jurnal Teknik Informatika*, vol. 4, no. 1, pp. 40–49, Jun. 2025, doi: 10.56211/sudo.v4i1.902.

[5] A. Bhardwaj, V. Sapra, and L. Sapra, “Evading Firewalls & Enumerate SNMP Using Advanced NMAP Techniques,” in *2023 3rd Asian Conference on Innovation in Technology (ASIANCON)*, IEEE, Aug. 2023, pp. 1–6. doi: 10.1109/ASIANCON58793.2023.10270155.

[6] A. Roup, “Risk Analysis Of Accounting Information System Security Based On Vulnerability Data From OPENVAS, OWASP ZAP, And NMAP Tools: A Cybersecurity Perspective,” *Jurnal Ilmiah Akuntansi Kesatuan*, vol. 13, no. 3, pp. 433–438, Jun. 2025, doi: 10.37641/jiakes.v13i3.3590.

[7] J. Wołoszyn and M. Wołoszyn, “Using Nmap and Python for an automated network security audit,” *Dydaktyka Informatyki*, vol. 19, pp. 227–238, Dec. 2024, doi: 10.15584/di.2024.19.19.

[8] Z. Al-Khazaali, A. Al-Ghabban, H. Al-Musawi, A. Sabah, and N. Al Mahdi, “Characteristics of Port Scan Traffic: A Case Study Using Nmap,” *Journal of Engineering and Sustainable Development*, vol. 29, no. 1, pp. 26–35, Jan. 2025, doi: 10.31272/jeasd.2638.

[9] G. C. Arnanto, “PEMINDAI KERENTANAN SEDERHANA BERBASIS NMAP OTOMATIS,” *Jurnal Jarkom*, vol. 13, no. 02, pp. 61–68, Dec. 2025, doi: 10.34151/jarkom.v13i02.5379.

[10] W. A. A. W. Mohamed, N. M. A. Mohamad, and A. Nasir, “Development of Raspberry-Pi Kali Linux Kit as Vulnerability Scanner,” 2024. [Online]. Available: https://tatiuc.edu.my/ijset/index.php/ijset/

[11] T. Rizky Chairil and J. Jenih, "Merancang Keamanan Jaringan Internet Menggunakan Program Network Mapper Di Linux Ubuntu," *Jurnal Teknologi Informasi*, vol. 9, no. 1, pp. 45–55, Jun. 2023, doi: 10.52643/jti.v9i1.3174.
[12] Y. Muhyidin, M. Hafid Totohendarto, E. Undamayanti, and S. Tinggi Teknologi Wastukancana, "Perbandingan Tingkat Keamanan Website Menggunakan Nmap Dan Nikto Dengan Metode Ethical Hacking Comparison of Website Security Levels Using Nmap and Nikto With Ethical Hacking Methods."
[13] "Journal of Natural and Applied Sciences Ural A Quarterly Multidisciplinary Scientific Journal Issued by European Academy for Development and Research / Brussels and Center of Research and Human Resources Development Ramah-Jordan," *Journal of natural and applied sciences URAL*.
[14] K. Kaushik, I. Punhani, S. Sharma, and M. Martolia, "An Advanced Approach for performing Cyber Fraud using Banner Grabbing," in *2022 5th International Conference on Contemporary Computing and Informatics (IC3I)*, IEEE, Dec. 2022, pp. 298–302. doi: 10.1109/IC3I56241.2022.10072445.
[15] H. Kanojia, R. Agarwal, D. Dube, T. S. Kumar, and D. Rajput, "A Python-Based Network Vulnerability Scanner Tool for Enhanced Cybersecurity," in *2025 12th International Conference on Computing for Sustainable Global Development (INDIACom)*, IEEE, Apr. 2025, pp. 1–4. doi: 10.23919/INDIACom66777.2025.11115758.