

LAPORAN AKHIR
MAGANG & STUDI INDEPENDEN BERSERTIFIKAT

Junior Cybersecurity Engineer
Magang/Studi Independen Batch 2
Di Vinix Seven Aurum

Ahdi Tri Julianto
42422058

Nama Dosen Pendamping Program (DPP) :
Khurotul Aeni, M.Kom



INFORMATIKA
UNIVERSITAS PERADABAN
2025

Kata Pengantar

Puji syukur saya panjatkan ke hadirat Allah SWT karena atas rahmat dan karunia-Nya, saya dapat menyelesaikan laporan akhir kegiatan Studi Independen Bersertifikat (MSIB) yang dilaksanakan bersama mitra Vinix Seven Aurum (VINIX7) dengan posisi Junior Cybersecurity Engineer, sebagai bagian dari program Kampus Merdeka yang diinisiasi oleh Kementerian Pendidikan, Kebudayaan, Riset, dan Teknologi Republik Indonesia.

Laporan ini disusun sebagai bentuk pertanggungjawaban akademik dan dokumentasi atas pelaksanaan program yang telah saya ikuti selama kurang lebih 4 bulan. Selama mengikuti kegiatan ini, saya memperoleh banyak pengalaman, ilmu baru, dan pengembangan keterampilan, khususnya dalam bidang keamanan siber dan manajemen kebijakan teknologi informasi.

Saya ingin menyampaikan terima kasih yang sebesar-besarnya kepada:

- Allah SWT atas segala limpahan nikmat dan kemudahan.
- Kementerian Pendidikan, Kebudayaan, Riset, dan Teknologi Republik Indonesia atas program MSIB.
- Mitra VINIX7, khususnya mentor divisi dan Kak Maunatul Mahida Sari selaku PIC Divisi Cybersecurity yang telah banyak membantu saya dalam memahami tugas serta memberikan bimbingan selama program berlangsung.
- Ibu Khurotul Aeni, M.Kom selaku Dosen Pendamping Program (DPP) dari Universitas Peradaban.
- Seluruh dosen di Program Studi Informatika Universitas Peradaban atas ilmu yang telah diberikan.
- Teman-teman seperjuangan MSIB yang selalu mendukung selama program berlangsung.

Saya menyadari bahwa laporan ini masih jauh dari sempurna. Oleh karena itu, saya terbuka terhadap segala bentuk kritik dan saran yang membangun demi perbaikan di masa yang akan datang. Semoga laporan ini dapat memberikan manfaat bagi semua pihak yang berkepentingan.

Brebes, 20 Mei 2025

Hormat saya,
Ahdi Tri Julianto

Daftar Isi

Kata Pengantar	i
Daftar Isi.....	ii
I. Gambaran Umum.....	1
A. Profil Perusahaan	1
B. Deskripsi Kegiatan	1
II. Aktivitas Bulanan	5
III. Penutup.....	8
A. Kesimpulan	8
B. Saran.....	9
Referensi	10
Lampiran	11

I. Gambaran Umum

A. Profil Perusahaan

VINIX7 adalah perusahaan yang berfokus pada sektor pendidikan dan pelatihan, dengan spesialisasi dalam pengembangan keahlian masa depan (future skills) dan keterampilan digital yang relevan dengan kebutuhan industri modern. Kami hadir dalam program Kampus Merdeka MBKM MSIB untuk program pemagangan dan studi independen. Dengan pendekatan yang inovatif dan adaptif, VINIX7 bertujuan untuk membekali generasi muda, profesional, dan pelaku usaha dengan kemampuan yang dibutuhkan untuk sukses dalam menghadapi tantangan dan peluang di era digital yang terus berkembang.

Struktur Perusahaan:

Komisaris: Umi Syarifah

Chairman: Budi Wasito

Kepala Program MSIB MBKM: Atina Cahyani

PIC MSIB MBKM: Zissiva

Program berjalan

- Magang
- Studi Independen

B. Deskripsi Kegiatan

Posisi : Junior Cybersecurity Enginner – Cyber Security Intern

Deskripsi : Selama mengikuti program Studi Independen Bersertifikat di VINIX7 sebagai Junior Cybersecurity Engineer, saya telah mengikuti 10 modul pembelajaran yang masing-masing disertai dengan praktik langsung dan tugas mendalam untuk memahami konsep serta penerapan cybersecurity di dunia nyata. Kegiatan diawali dengan pengenalan terhadap teknologi virtualisasi, di mana saya mempelajari berbagai tools seperti VirtualBox, VMware, Proxmox, dan OpenStack, sekaligus melakukan instalasi dan konfigurasi VM untuk sistem operasi Windows dan Kali Linux. Saya juga mempelajari teknik backup & restore

menggunakan UrBackup dan melakukan konfigurasi webserver dengan metode hardening serta kontrol akses berbasis ACL. Pada modul selanjutnya, saya mendalami teknik serangan siber seperti social engineering, password cracking, dan SQL injection dengan menggunakan tools Cain & Abel, Hydra, dan sqlmap. Saya juga mempelajari dan menggunakan tools vulnerability scanner seperti Arachni dan OpenVAS untuk melakukan analisa keamanan pada aplikasi web dan jaringan lokal. Selain itu, saya belajar mengidentifikasi kelemahan dalam sistem wireless dan mobile device melalui site survey menggunakan Kismet, serta memahami peran MDM tools seperti Miradore. Saya juga mengimplementasikan teknologi Public Key Infrastructure (PKI) menggunakan OpenSSL, dan memahami cara kerja serta proses pembuatan sertifikat SSL untuk dua domain berbeda. Kemudian, saya menggunakan Nessus untuk melakukan pemindaian terhadap sistem internal dan eksternal guna mengidentifikasi potensi celah keamanan. Pada bagian digital forensic dan SIEM, saya melakukan analisis terhadap image disk menggunakan tools seperti Autopsy dan FTK Imager, serta menginstal dan mengoperasikan SIEM Wazuh untuk memonitor agent yang terhubung dalam jaringan. Seluruh kegiatan ini ditutup dengan tugas penyusunan IT Policy Framework berdasarkan studi kasus di kampus saya sendiri (Universitas Peradaban) dan pembuatan makalah tentang pentingnya security awareness di lingkungan Pendidikan.

Kompetensi yang dikembangkan :

1. Pemahaman konsep keamanan siber

- Mampu memahami prinsip dasar keamanan informasi (confidentiality, integrity, availability) serta ancaman umum seperti phishing, malware, social engineering, dan serangan berbasis jaringan.

2. Kemampuan praktis penggunaan tools keamanan

- Mampu menggunakan berbagai tools cybersecurity seperti.

1. Wireshark, Kismet dan Cisco Packet Tracer untuk analisis jaringan.

2. Cain & Abel, Hydra, sqlmap untuk simulasi serangan.
3. Arachni, OpenVAS, dan Nessus untuk vulnerability assessment.
4. Autopsy, FTK Imager, Wazuh untuk digital forensic & SIEM monitoring.
5. UrBackup untuk membackup dan merestore data.
6. Thunderbird untuk mengenkripsi data saat berkomunikasi.

3. *Perancangan dan Analisis Kebijakan Keamanan IT*

- Mampu menganalisis dan menyusun IT Policy Framework berdasarkan studi kasus nyata di lingkungan kampus maupun studi banding dengan kampus lain.

4. *Konfigurasi Jaringan dan Sistem Keamanan*

- Menguasai konfigurasi VLAN, Routing Inter-VLAN, pengamanan protokol (Telnet vs SSH, HTTP vs HTTPS), serta implementasi PKI dan sertifikat SSL pada server Apache.

5. *Kemampuan Menulis Laporan dan Dokumentasi Teknis*

- Terbiasa menyusun laporan teknis, dokumentasi konfigurasi, laporan penetration testing, dan makalah ilmiah seperti Security Awareness.

6. *Manajemen Resiko dan Insiden Respon*

- Memahami prinsip manajemen risiko dalam keamanan TI serta melakukan analisis hasil audit untuk menentukan langkah mitigasi dan rekomendasi perbaikan.

Selama mengikuti program MSIB di VINIX7, saya mempelajari berbagai materi terkait keamanan siber seperti cloud security, threat modeling, social engineering, digital forensic, hingga SIEM monitoring. Saya mengerjakan tugas praktik langsung seperti instalasi tools keamanan, analisis kelemahan jaringan dan sistem, penyusunan IT Policy Framework, serta membuat makalah security awareness. Program ini juga melibatkan simulasi serangan dan audit sistem menggunakan berbagai tools, serta pelaporan hasil dalam bentuk laporan teknis.

II. Aktivitas Bulanan

Bulan	Kegiatan
1	<p>Pada bulan pertama, fokus kegiatan saya adalah mempelajari dasar-dasar virtualisasi dan pengantar keamanan siber. Saya mempelajari berbagai platform virtualisasi seperti VMware, VirtualBox, XEN, Proxmox, dan OpenStack, lalu menginstal dua sistem operasi (Windows dan Kali Linux) pada VirtualBox. Selain itu, saya juga melakukan konfigurasi awal dan membuat OVA/OVF image dari virtual machine yang telah dibuat.</p> <p>Pada minggu kedua, saya mempelajari konsep social engineering dan melakukan praktik password cracking menggunakan tools Cain & Abel serta Hydra. Saya juga melakukan simulasi SQL Injection secara manual maupun dengan menggunakan tools otomatis seperti sqlmap pada situs target yang telah disediakan. Selain itu, saya mempelajari kisah nyata hacker ternama Kevin Mitnick sebagai studi kasus social engineering</p>
2	<p>Pada bulan kedua, kegiatan difokuskan pada praktik penggunaan berbagai tools vulnerability assessment dan network security. Saya mempelajari dan menginstal Arachni untuk melakukan pemindaian terhadap aplikasi web pada situs target, serta menyusun laporan penetration testing berdasarkan hasil scanning. Selain itu, saya juga menggunakan OpenVAS untuk melakukan pemindaian dan analisis terhadap jaringan lokal, termasuk identifikasi perangkat, sistem operasi, dan potensi kelemahannya.</p> <p>Di minggu berikutnya, saya mempelajari dan mengevaluasi sistem Single Sign-On (SSO) di kampus serta melakukan implementasi honeypot menggunakan ghost-usb-honeypot. Saya juga melakukan hardening webserver Apache2 serta mengonfigurasi beberapa folder aplikasi berdasarkan aturan akses berbasis IP dan otentikasi HTTP.</p> <p>Pada minggu ketiga bulan kedua, saya mendalami topik backup & restore menggunakan URBackup dan implementasi kriptografi dengan PGP melalui email client Thunderbird. Saya berhasil membuat dan mengelola pasangan kunci digital, mengirim email terenkripsi dan bertandatangan digital, serta memahami prinsip confidentiality, integrity, dan authenticity dalam komunikasi elektronik.</p> <p>Pada minggu terakhir, Saya juga mengerjakan konfigurasi jaringan VLAN dan Routing InterVLAN menggunakan Cisco</p>

	<p>Packet Tracer, mulai dari pengaturan IP Address, VLAN tagging, hingga router-on-stick untuk menghubungkan antar VLAN. Proyek ini mengajarkan saya cara menyusun arsitektur jaringan yang tersegmentasi secara aman dan efisien.</p> <p>Selain itu, saya mempelajari dan membuktikan perbedaan antara protokol aman (secure) dan tidak aman (unsecure) dengan menggunakan Wireshark untuk melakukan network interception. Saya melakukan pengujian terhadap protokol seperti Telnet vs SSH, HTTP vs HTTPS, FTP vs FTPS, dan lainnya, lalu mendokumentasikan hasilnya beserta port default dan jenis data yang bisa disadap dari masing-masing protokol</p>
3	<p>Pada bulan ketiga, saya mempelajari topik lanjutan terkait keamanan jaringan nirkabel (wireless security) dan manajemen perangkat mobile (Mobile Device Management/MDM). Saya melakukan site survey menggunakan tools Kismet di dua lokasi berbeda untuk menganalisis access point, channel, dan jenis keamanan yang digunakan, serta mengidentifikasi potensi perangkat mencurigakan. Selain itu, saya juga mengeksplorasi fitur-fitur dari beberapa tools MDM seperti Miradore untuk memahami bagaimana organisasi mengelola dan mengamankan perangkat mobile secara terpusat.</p> <p>Pada minggu berikutnya, saya mendalami materi Public Key Infrastructure (PKI) dengan membuat sertifikat self-signed menggunakan OpenSSL. Saya melakukan konfigurasi domain lokal menggunakan <code>/etc/hosts</code>, lalu mengintegrasikan sertifikat SSL ke dalam server Apache2. Selain itu, saya juga menggunakan Nessus untuk melakukan vulnerability scanning terhadap jaringan internal dan web target, serta menganalisis laporan hasil pemindaian untuk mengetahui celah keamanan dengan level severity tinggi.</p> <p>Di akhir bulan, saya mengerjakan proyek Digital Forensic menggunakan tools seperti Autopsy, FTK Imager, tsf_recovery, dan foremost untuk menganalisis image file <code>RAW-ImageDrive.dd</code>. Saya melakukan file recovery dan mengidentifikasi berbagai jenis file (video, gambar, dokumen) yang berhasil dikembalikan dari image tersebut. Selain itu, saya juga mempelajari implementasi SIEM (Security Information and Event Management) menggunakan Wazuh. Saya menginstal Wazuh Server dan Agent, lalu menghubungkan agent dari mesin lain untuk memantau aktivitas sistem secara real-time. Saya mengevaluasi berbagai fitur monitoring, log audit, serta insight keamanan yang diberikan oleh SIEM Wazuh</p>

4	<p>Pada bulan keempat, saya fokus pada penyelesaian modul terakhir (Modul 10) yang mencakup topik IT Policy Framework dan Security Awareness. Pada modul ini, saya melakukan analisis kebijakan teknologi informasi (TI) yang diterapkan di kampus Universitas Peradaban, serta membandingkannya dengan framework dari kampus lain yang lebih ideal, seperti Nanyang Technological University (NTU). Saya juga menyusun rekomendasi pengembangan kebijakan TI yang relevan dan dapat diimplementasikan untuk meningkatkan keamanan informasi di lingkungan akademik.</p> <p>Selain itu, saya menyusun sebuah makalah ilmiah yang membahas secara komprehensif tentang pentingnya security awareness di lingkungan kampus. Dalam makalah tersebut, saya mengulas ancaman siber umum, rendahnya kesadaran pengguna sebagai celah utama dalam keamanan sistem, serta strategi peningkatan kesadaran seperti pelatihan, simulasi serangan, dan integrasi edukasi keamanan dalam kurikulum.</p> <p>Pada tahap akhir program, saya menyusun dan menyelesaikan laporan akhir kegiatan Studi Independen sebagai bentuk pertanggungjawaban terhadap seluruh proses pembelajaran dan praktik yang telah saya lakukan. Laporan ini mencakup deskripsi kegiatan, kompetensi yang dikembangkan, dokumentasi tugas-tugas, serta refleksi pengalaman selama program.</p>
---	---

III. Penutup

A. Kesimpulan

Berdasarkan pengalaman dan kegiatan yang telah saya jalani selama mengikuti program Studi Independen Bersertifikat (MSIB) bersama mitra VINIX7 sebagai Junior Cybersecurity Engineer, saya dapat menarik beberapa kesimpulan sebagai berikut:

1. Proses Pelaksanaan Program MSIB

- Program MSIB memberikan pengalaman belajar yang sangat berharga karena menggabungkan antara materi teori, praktik langsung, dan penyusunan laporan tugas nyata. Meskipun dilakukan secara mandiri tanpa pendampingan mentor secara langsung.
- Pelaksanaan program berjalan sistematis dan fleksibel, memungkinkan peserta untuk mengeksplorasi berbagai tools dan metode di bidang cybersecurity secara mandiri maupun terstruktur.
- Materi dan tugas disusun secara bertahap dan terstruktur, sehingga tetap memungkinkan peserta untuk memahami dan mengerjakan setiap modul dengan baik.
- Interaksi dengan tim mitra terbatas, namun tantangan ini mendorong saya untuk lebih mandiri, proaktif dalam belajar, dan mengasah kemampuan problem solving secara nyata.
- Penggunaan modul mingguan membuat proses belajar lebih fokus dan progresif, dengan topik yang terus berkembang dari dasar hingga tingkat lanjut.
- Sebagai peserta dengan paket Basic, saya mengikuti seluruh materi melalui tayangan video di YouTube. Meskipun tidak mendapatkan akses langsung untuk berdiskusi melalui Zoom, saya tetap dapat memahami materi secara mandiri berkat penjelasan yang terstruktur dari mentor.

2. Substansi Materi dan Tugas yang Dikerjakan

- Saya mempelajari banyak aspek penting dalam cybersecurity, mulai dari virtualisasi, social engineering, password cracking, network security, sampai digital forensic dan SIEM monitoring.
- Tugas-tugas yang diberikan sangat sesuai dengan praktek nyata, seperti praktik SQL injection, konfigurasi VLAN, analisis protokol aman dan tidak aman, instalasi honeypot, hingga penyusunan IT Policy Framework.
- Seluruh materi dan tugas membantu saya dalam meningkatkan pemahaman mendalam terhadap konsep, tools, teknik, dan kebijakan keamanan informasi, yang sangat relevan dengan kebutuhan dunia kerja.

- Penyusunan laporan akhir dan makalah ilmiah juga membantu dan meningkatkan kemampuan saya dalam berpikir kritis, menyusun argumen berbasis data, serta menulis dokumentasi teknis secara sistematis.

B. Saran

Sebagai peserta MSIB dengan paket Basic, saya merasa program ini tetap memberikan manfaat yang besar dalam meningkatkan pemahaman saya di bidang keamanan siber. Namun, saya juga memiliki beberapa saran berdasarkan keterbatasan yang saya alami selama mengikuti program:

1. Saran untuk Proses Pelaksanaan di Mitra (VINIX7)

- Akan sangat membantu jika peserta paket Basic juga difasilitasi dengan akses mentoring terbatas atau sesi tanya jawab bulanan, agar peserta tetap bisa memperoleh bimbingan meski tidak seintensif peserta Full Package.
- Materi dan instruksi tugas sebaiknya diberikan dengan petunjuk teknis (panduan) yang lebih rinci, mengingat peserta Basic belajar sepenuhnya secara mandiri tanpa pendampingan.
- Perlu adanya sistem penilaian mandiri atau evaluasi sederhana, agar peserta dapat mengukur sendiri sejauh mana pemahamannya terhadap materi yang sudah dipelajari.

2. Saran terhadap Substansi/Topik yang Digeluti

- Materi yang diberikan sudah sangat luas dan mendalam, namun karena keterbatasan interaksi, beberapa bagian teknis terasa menantang untuk dipelajari sendiri, khususnya topik seperti SIEM, digital forensic, dan tool berbasis enterprise.
- Sebagai peserta Basic, akan sangat bermanfaat jika tersedia video tutorial atau rekaman sesi praktik yang bisa diakses secara on-demand sebagai pelengkap dari materi tertulis.
- Topik seperti analisis kebijakan IT (policy framework) dan security awareness sangat menarik, dan sebaiknya diberikan juga sebagai referensi agar peserta lebih mudah memahaminya secara kontekstual.
- Peserta paket Basic hanya dapat mengikuti melalui YouTube tanpa interaksi langsung, akan sangat membantu jika disediakan media tanya jawab alternatif seperti forum diskusi atau kolom Q&A untuk menjembatani kebutuhan peserta dalam memahami materi yang lebih kompleks secara lebih mendalam.

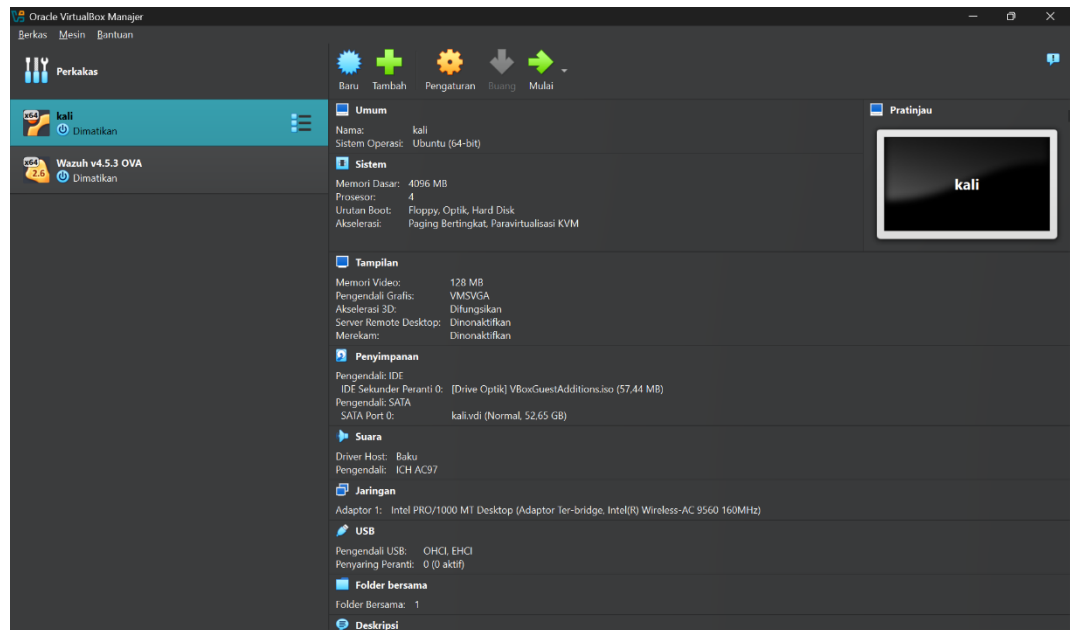
Referensi

1. Arachni Web Application Security Scanner. <https://github.com/Arachni/arachni>.
2. OpenVAS Vulnerability Scanner. <https://www.ceos3c.com/security/install-openvas-kali-linux/>
3. Universitas Peradaban – Official Website. <https://peradaban.ac.id>.
4. Nanyang Technological University (NTU) IT Policy. <https://www.ntu.edu.sg/it>.
5. YouTube VINIX7 MSIB Official Channel – Materi Modul 1–10.
6. Rootbrain Cybersecurity Labs – Tugas Praktik. <https://target.rootbrain.com>.
7. Kevin Mitnick – The Art of Deception. (2002). Wiley Publishing.
8. Nessus Vulnerability Scanner. <https://www.tenable.com/products/nessus>
9. URBackup – Open Source Backup Software. <https://www.urbackup.org/>
10. Autopsy Digital Forensics. <https://www.sleuthkit.org/autopsy/>
11. Cisco Packet Tracer – VLAN & InterVLAN Routing. Cisco Networking Academy
12. Wazuh SIEM Platform. <https://documentation.wazuh.com>
13. SQLMap – Automatic SQL Injection Tool. <https://sqlmap.org>
14. VINIX7. (2025). *Modul 1–10: Materi Pembelajaran Cybersecurity Engineer – MSIB Batch 6*. Dokumen pembelajaran internal.
15. LC Learning Center. (2025). *Video Pembelajaran Cybersecurity – MSIB Batch 6 VINIX7*. YouTube Channel <https://www.youtube.com/@ilclearningcenter>
16. Cryptography with PGP. <https://www.openpgp.org/>
17. OpenSSL Project. (n.d.). *OpenSSL Documentation*. <https://www.openssl.org/docs/>
18. Cybersecurity & Infrastructure Security Agency (CISA). (2021). *Security Awareness Training for Employees*. <https://www.cisa.gov>
19. Miradore. *Mobile Device Management (MDM) Platform Overview*. <https://www.miradore.com>
20. Apache Software Foundation. *Apache HTTP Server Documentation*. <https://httpd.apache.org/docs/>

Lampiran

1. Instalasi VirtualBox dan Kali Linux (Modul 1)

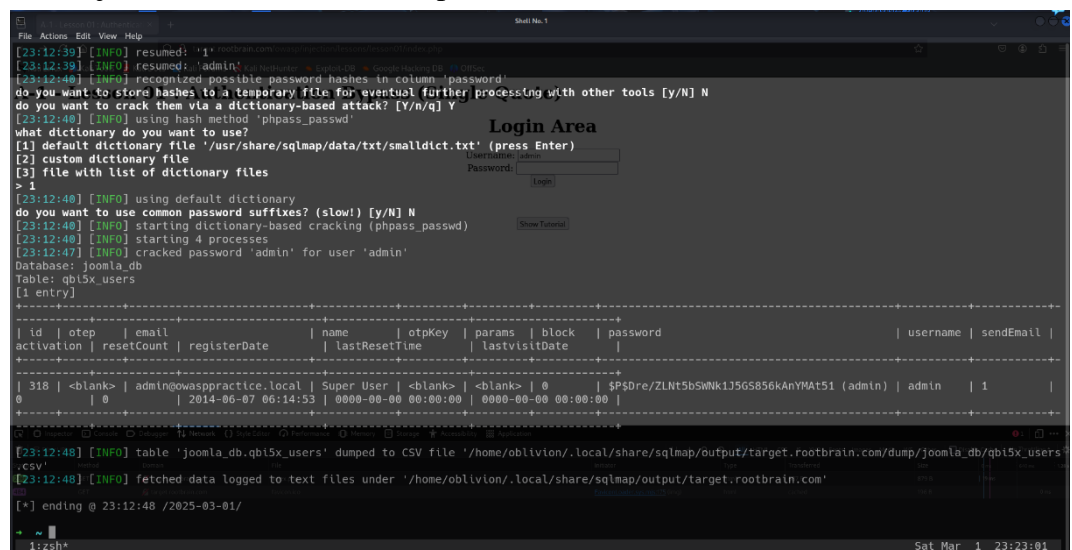
Gambar berikut menunjukkan hasil instalasi VirtualBox dan sistem operasi Kali Linux yang digunakan untuk simulasi praktik keamanan jaringan.



Gambar 1

2. Praktik SQL Injection Menggunakan SQLMap (Modul 2)

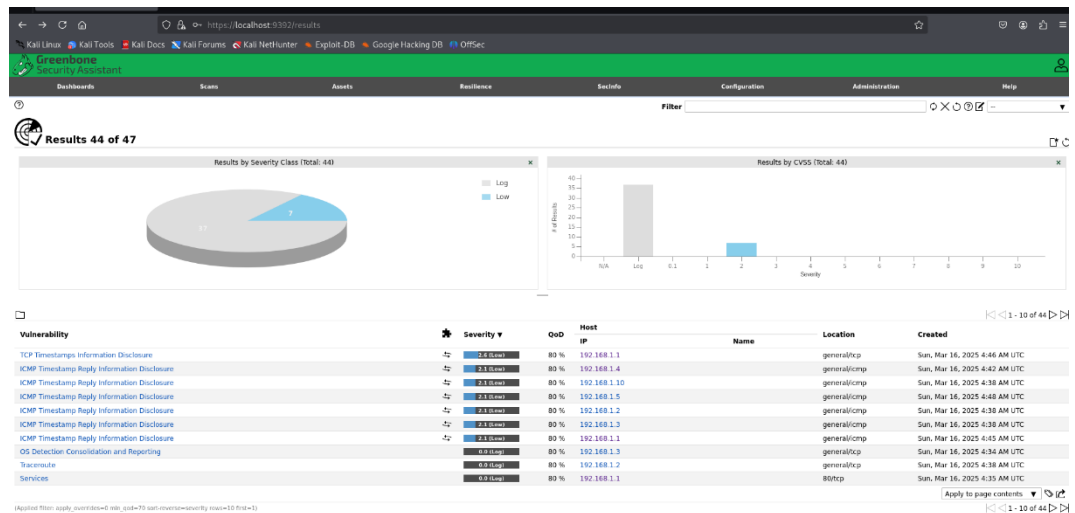
Tampilan command line saat menjalankan SQLMap pada situs uji coba, menunjukkan data username dan password berhasil diekstrak dari database.



Gambar 2

3. Laporan Scan OpenVAS (Modul 3)

Berikut hasil pemindaian keamanan jaringan menggunakan OpenVAS yang menampilkan beberapa temuan dengan tingkat risiko tinggi dan sedang.



Gambar 3

4. Konfigurasi Webserver Apache dan Hardening Akses Folder (Modul4)

Screenshot ini menunjukkan konfigurasi VirtualHost pada Apache2 untuk membatasi akses folder menggunakan aturan berbasis IP dan autentikasi .htpasswd

```

GNU nano 8.2
<VirtualHost *:80>
    # ServerName bisa ditambahkan jika perlu
    ServerName localhost

    ServerAdmin webmaster@localhost
    DocumentRoot /var/www/html

    # Log Files
    ErrorLog ${APACHE_LOG_DIR}/error.log
    CustomLog ${APACHE_LOG_DIR}/access.log combined

    # Konfigurasi folder-folder sesuai soal
    <Directory /var/www/html/publicapp>
        Require all granted
    </Directory>

    <Directory /var/www/html/privateapp>
        Require ip 192.168.1.0/24
    </Directory>

    <Directory /var/www/html/specialapp>
        <RequireAll>
            Require all granted
            Require not ip 192.168.1.100
        </RequireAll>
    </Directory>

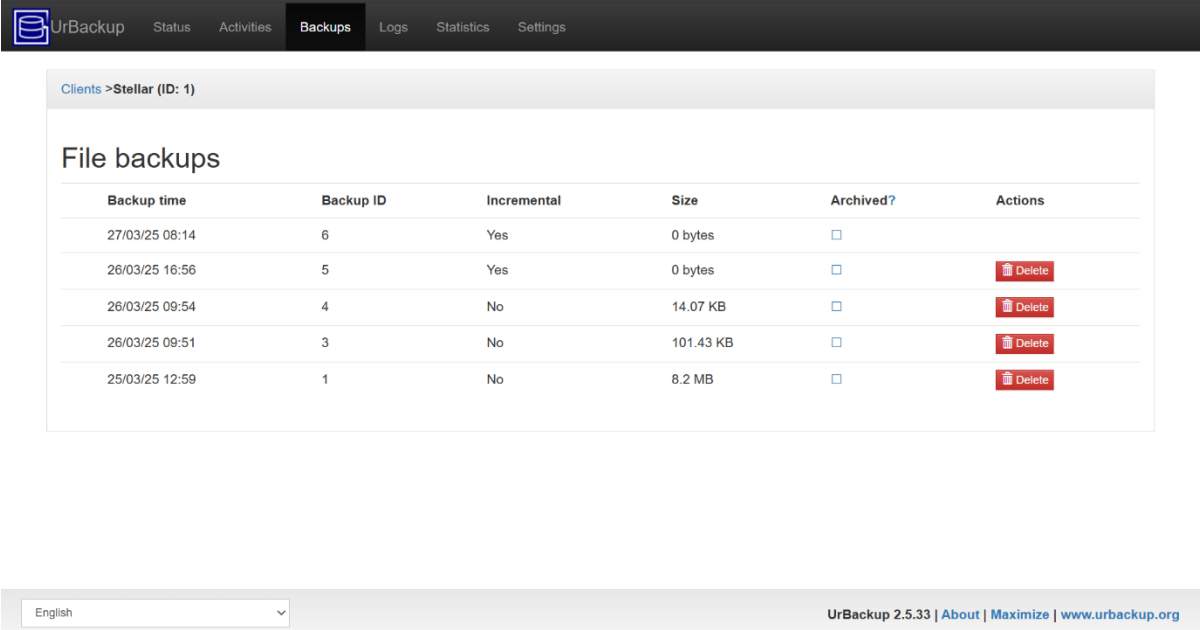
    <Directory /var/www/html/protectapp>
        AuthType Basic
        AuthName "Restricted Access"
        AuthUserFile /etc/apache2/.htpasswd
        Require valid-user
    </Directory>
</VirtualHost>

```

Gambar 4

5. Backup dan Email PGP Encryption (Modul 5)

Gambar ini menunjukkan praktik backup menggunakan UrBackup serta pengiriman email terenkripsi dengan PGP melalui Thunderbird, termasuk penggunaan digital signature.



UrBackup Status Activities **Backups** Logs Statistics Settings

Clients > Stellar (ID: 1)

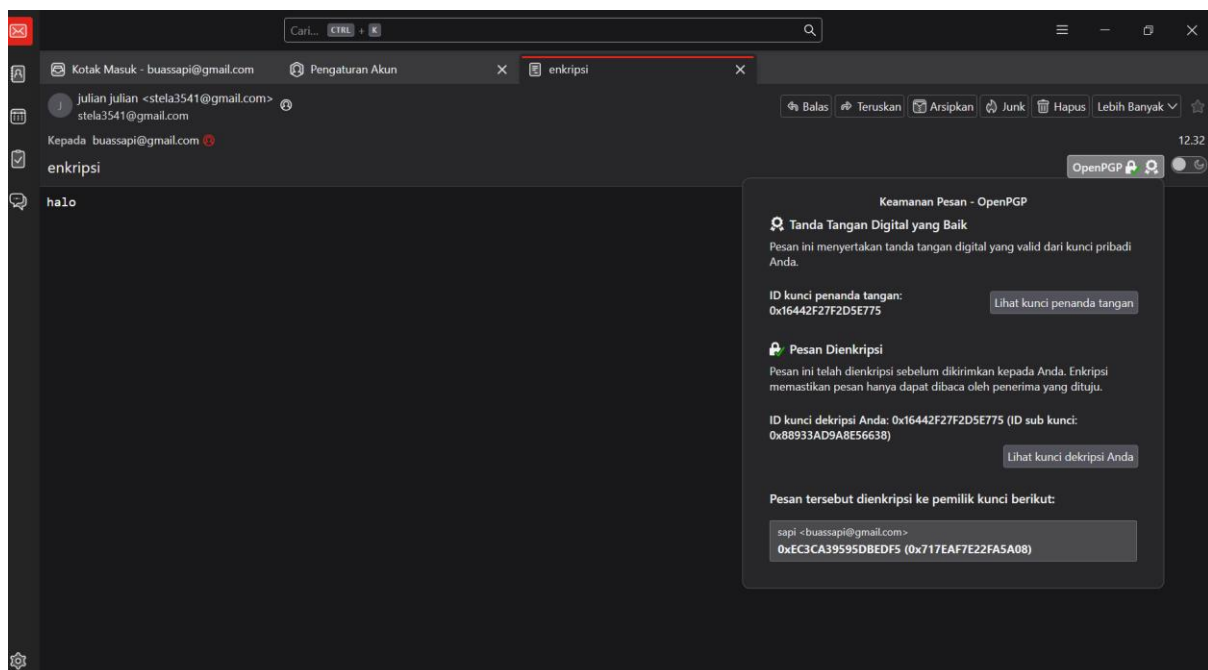
File backups

Backup time	Backup ID	Incremental	Size	Archived?	Actions
27/03/25 08:14	6	Yes	0 bytes	<input type="checkbox"/>	
26/03/25 16:56	5	Yes	0 bytes	<input type="checkbox"/>	Delete
26/03/25 09:54	4	No	14.07 KB	<input type="checkbox"/>	Delete
26/03/25 09:51	3	No	101.43 KB	<input type="checkbox"/>	Delete
25/03/25 12:59	1	No	8.2 MB	<input type="checkbox"/>	Delete

English

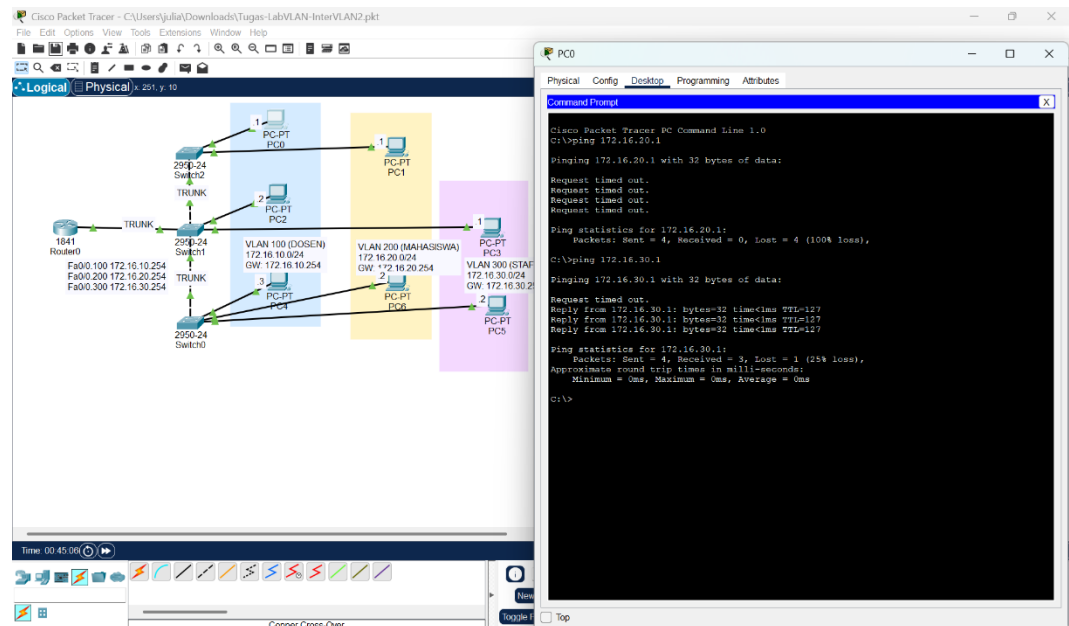
UrBackup 2.5.33 | [About](#) | [Maximize](#) | www.urbackup.org

Gambar 5



Gambar 6

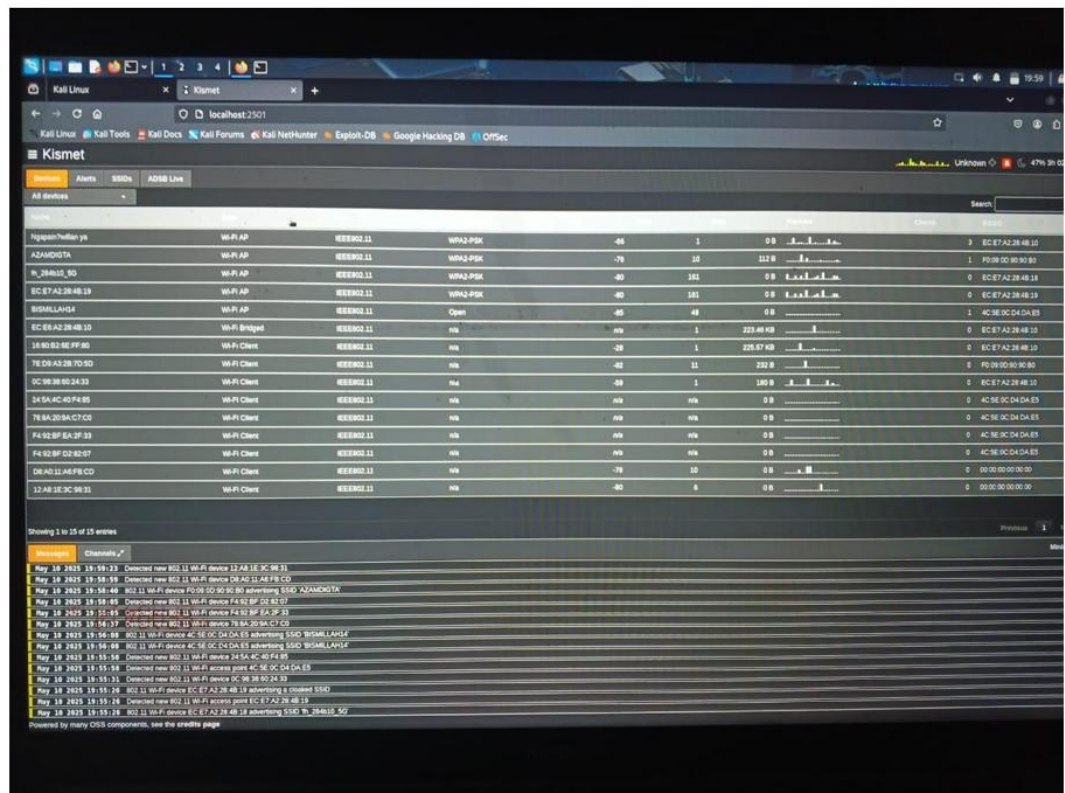
- Konfigurasi VLAN dan Routing InterVLAN (Modul 6)
Tangkapan layar dari Cisco Packet Tracer yang menunjukkan konfigurasi VLAN dan pengujian konektivitas antar segmen jaringan.



Gambar 7

7. Wireless Survey dengan Kismet (Modul 7)

Screenshot ini menunjukkan hasil site survey jaringan nirkabel menggunakan Kismet untuk mendeteksi access point, channel, dan jenis enkripsi jaringan Wi-Fi.



Gambar 8

8. Pembuatan Sertifikat SSL dengan OpenSSL (Modul 8)

Berikut tampilan saat pembuatan sertifikat self-signed SSL menggunakan OpenSSL untuk dua domain lokal yang diintegrasikan dengan Apache.



Gambar 9

```

(obliv@kali)-[~/pki/CA]
$ openssl req -x509 -new -nodes -key ca.key -sha256 -days 3650 -out ca.crt \
-subj "/C=ID/ST=Jawa Tengah/L=Brebes/O=MyCA/CN=MyCA"

(obliv@kali)-[~/pki/CA]
$ openssl req -new -key anto-lab2025.com.key -out anto-lab2025.com.csr \
-subj "/C=ID/ST=Jawa Tengah/L=Brebes/O=AntoLab/CN=anto-lab2025.com"

Could not open file or uri for loading private key from anto-lab2025.com.key: No such file or directory

(obliv@kali)-[~/pki/CA]
$ openssl genrsa -out anto-lab2025.com.key 2048

(obliv@kali)-[~/pki/CA]
$ openssl req -new -key anto-lab2025.com.key -out anto-lab2025.com.csr \
-subj "/C=ID/ST=Jawa Tengah/L=Brebes/O=AntoLab/CN=anto-lab2025.com"

(obliv@kali)-[~/pki/CA]
$ openssl x509 -req -in anto-lab2025.com.csr -CA ca.crt -CAkey ca.key \
-CAcreateserial -out anto-lab2025.com.crt -days 825 -sha256

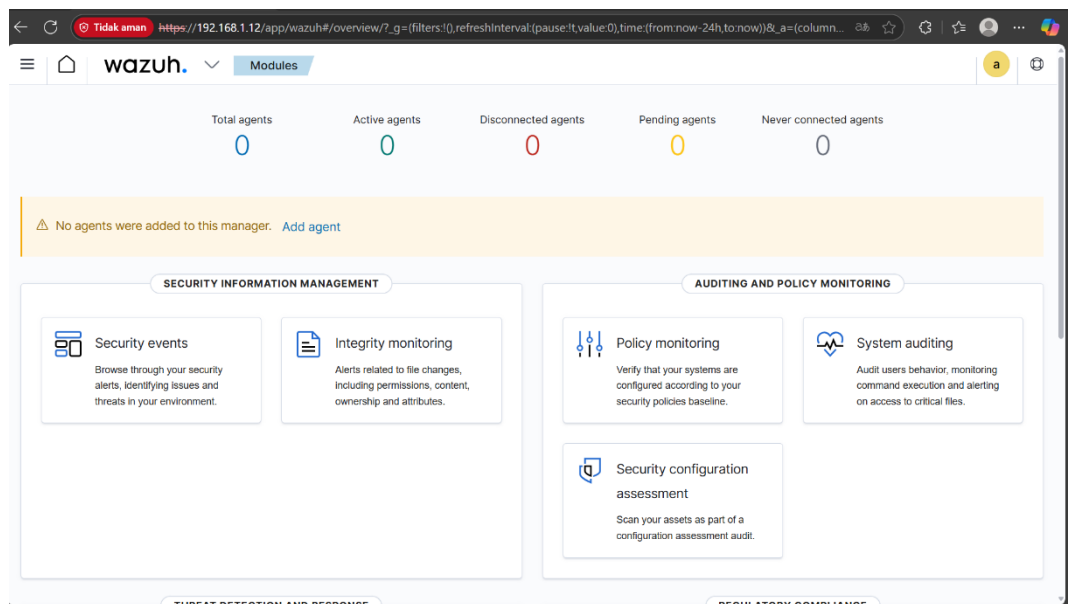
Certificate request self-signature ok
subject=C=ID, ST=Jawa Tengah, L=Brebes, O=AntoLab, CN=anto-lab2025.com

```

Gambar 10

9. Dashboard Wazuh SIEM (Modul 9)

Gambar dashboard SIEM Wazuh yang menunjukkan monitoring log dan alert dari agent yang terpasang pada sistem endpoint.



Gambar 11

10. Dokumen IT Policy Framework dan Makalah Security Awareness (Modul 10)

Lampiran ini berisi dokumen tugas akhir berupa IT Policy Framework untuk kampus Universitas Peradaban dan makalah ilmiah tentang pentingnya security awareness di lingkungan kampus.