PENGEMBANGAN *CYBER RANGE* SEBAGAI MEDIA PELATIHAN KEAMANAN SIBER UNTUK *BLUE TEAM*

Disusun Oleh:

N a m a : Anugerah Ramadhan Arinal
NIM : 21523257

PROGRAM STUDI INFORMATIKA – PROGRAM SARJANA
FAKULTAS TEKNOLOGI INDUSTRI
UNIVERSITAS ISLAM INDONESIA
2025

HALAMAN PENGESAHAN DOSEN PEMBIMBING

PENGEMBANGAN *CYBER RANGE* SEBAGAI MEDIA PELATIHAN KEAMANAN SIBER UNTUK *BLUE TEAM*

TUGAS AKHIR

Disusun Oleh:

N a m a : Anugerah Ramadhan Arinal

NIM : 21523257

Yogyakarta, 8 Juli 2025

Pembimbing,

(Dr. Sri Kusumadewi, S.Si., M.T.)

HALAMAN PENGESAHAN DOSEN PENGUJI

PENGEMBANGAN *CYBER RANGE* SEBAGAI MEDIA PELATIHAN KEAMANAN SIBER UNTUK *BLUE TEAM*

TUGAS AKHIR

Telah dipertahankan di depan sidang penguji sebagai salah satu syarat untuk memperoleh gelar Sarjana Komputer dari Program Studi Informatika – Program Sarjana di Fakultas Teknologi Industri Universitas Islam Indonesia

Yogyakarta, 2025

Tim Penguji

Dr. Sri Kusumadewi, S.Si., M.T. _____

Anggota 1

Erika Ramadhani, S.T., M.Eng. _____

Anggota 2

Ari Sujarwo, S.Kom., MIT. (Hons) _____

Mengetahui,
Ketua Program Studi Informatika – Program Sarjana
Fakultas Teknologi Industri
Universitas Islam Indonesia

(Dhomas Hatta Fudholi, S.T., M.Eng., Ph.D.)

HALAMAN PERNYATAAN KEASLIAN TUGAS AKHIR

Yang bertanda tangan di bawah ini:

Nama : Anugerah Ramadhan Arinal

NIM : 21523257

Tugas akhir dengan judul:

PENGEMBANGAN *CYBER RANGE* SEBAGAI MEDIA PELATIHAN KEAMANAN SIBER UNTUK *BLUE TEAM*

Menyatakan bahwa seluruh komponen dan isi dalam tugas akhir ini adalah hasil karya saya sendiri. Apabila di kemudian hari terbukti ada beberapa bagian dari karya ini adalah bukan hasil karya sendiri, tugas akhir yang diajukan sebagai hasil karya sendiri ini siap ditarik kembali dan siap menanggung risiko dan konsekuensi apapun.

Demikian surat pernyataan ini dibuat, semoga dapat dipergunakan sebagaimana mestinya.

Yogyakarta, 8 Juli 2025

(Anugerah Ramadhan Arinal)

HALAMAN PERSEMBAHAN

Seluruh usaha dalam penyusunan tugas akhir ini saya dedikasikan kepada keluarga saya sebagai bentuk rasa syukur dan terima kasih atas seluruh dukungan yang telah diberikan.

HALAMAN MOTO

Jangan lupa minum air putih.

KATA PENGANTAR

Puji syukur penulis panjatkan ke hadirat Allah SWT atas kasih dan karunia-Nya, sehingga penulis dapat menyelesaikan penyusunan tugas akhir ini. Pada kesempatan ini, penulis ingin menyampaikan rasa terima kasih yang sebesar-besarnya kepada:

1. Keluarga penulis yang tiada hentinya selalu memberikan segala bentuk dukungan untuk penulis.
2. Bapak Prof. Fathul Wahid, S.T., M.Sc, Ph.D selaku Rektor Universitas Islam Indonesia.
3. Bapak Prof., Dr., Ir., Hari Purnomo, M.T., IPU, ASEAN.Eng. selaku Pimpinan Fakultas Teknologi Industri Universitas Islam Indonesia.
4. Bapak Dr. Raden Teduh Dirgahayu, S.T., M.Eng., Ph.D. Ketua Jurusan Informatika Universitas Islam Indonesia.
5. Bapak Dhomas Hatta Fudholi, S.T., M.Eng., Ph.D. Ketua Program Studi Informatika Universitas Islam Indonesia.
6. Ibu Dr. Sri Kusumadewi, S.Si., M.T. selaku dosen pembimbing tugas akhir yang senantiasa memberikan ilmu dan menuntun penulis sejak awal penjaluran tugas akhir hingga selesai.
7. Ibu Aridhanyati Arifin, S.T., M.Cs. selaku dosen akademik yang selalu membantu penulis terkait permasalahan akademik.
8. Seluruh dosen, staf, dan tenaga pendidik Program Studi Informatika Universitas Islam Indonesia.
9. Bapak Budi Hermawan, selaku Pimpinan PT. Adikarya Tata Informasi (Aditasi) yang telah memberikan kesempatan kepada penulis untuk menjalani penjaluran magang atas segala ilmu dan bimbingan yang telah diberikan.
10. Rekan-rekan kerja Aditasi yang selalu menemani dan membantu penulis dalam menjalani magang.
11. Sahabat seperjuangan penulis, Kuncoro, Ezra, Julio, dan Lala yang selalu peduli dan memberikan dukungan serta bantuan untuk penulis.
12. Sahabat penulis, Siraj, Juan, Nabil, Bintang, Satriya, Daud, Rafli, Ihwan, Hanuga, Naela, Asista, Kharisma, Zahwa, dan yang tidak bisa penulis sebutkan satu persatu, yang selalu memberikan dukungan dan menemani penulis dalam penyusunan tugas akhir.

13. Rekan-rekan perkuliahan penulis yang selalu memberikan dukungan dan bantuan dalam penyusunan tugas akhir.

Yogyakarta, 8 Juli 2025

(Anugerah Ramadhan Arinal)

SARI

Keamanan siber merupakan bidang yang terus berkembang seiring meningkatnya kompleksitas dan frekuensi serangan digital. Kebutuhan akan sumber daya manusia yang andal dalam menghadapi ancaman siber mendorong perlunya media pelatihan yang mampu menjembatani antara teori dan praktik. Penelitian ini bertujuan untuk mengembangkan *cyber range* sebagai media pelatihan keamanan siber yang berfokus pada penguatan kemampuan *blue team* dalam dua domain utama, yaitu analisis *malware* dan analisis lalu lintas jaringan. Metode yang digunakan dalam penelitian ini adalah *Research and Development* (R&D) dengan mengacu pada model pengembangan Borg & Gall. Pengembangan dilakukan melalui empat tahap, yaitu studi literatur dan pengumpulan data, perancangan skenario pelatihan, implementasi skenario dalam lingkungan virtual, serta penyusunan dokumentasi *walkthrough*. Skenario analisis *malware* menggunakan FireEye Redline untuk menyelidiki artefak pasca-infeksi *ransomware*, sementara skenario analisis jaringan memanfaatkan Wireshark dan NetworkMiner untuk menelusuri aktivitas serangan DDoS dalam *file* PCAP. Hasil akhir dari penelitian ini berupa dua modul *cyber range* yang dapat digunakan sebagai media pelatihan terstruktur. Pengembangan ini diharapkan dapat menjadi alternatif pelatihan praktis yang adaptif dan dapat direplikasi untuk memperkuat kompetensi teknis pertahanan siber, khususnya dalam konteks *blue team*.

Kata kunci: *cyber range*, *blue team*, keamanan siber, analisis *malware*, analisis jaringan.

GLOSARIUM

Artefak digital	bukti digital yang tersisa dari suatu aktivitas sistem atau serangan siber.
Blue team	tim keamanan siber yang bertugas mempertahankan sistem dan jaringan dari serangan.
CSIRT	singkatan dari *Computer Security Incident Response Team*, yang merupakan tim khusus dalam suatu organisasi yang bertanggung jawab dalam menangani, meresepons, dan memitigasi insiden keamanan siber.
Cyber range	lingkungan virtual yang digunakan untuk simulasi dan pelatihan keamanan siber.
DDoS	singkatan dari *Distributed Denial of Service*, yaitu serangan dengan teknik membanjiri trafik untuk membuat layanan tidak tersedia.
Decryptor	program atau alat yang dirancang untuk memulihkan *file* yang telah dienkripsi.
Defensive security	praktik keamanan siber yang berfokus pada perlindungan sistem dari serangan, termasuk deteksi serangan, respons insiden, dan pemulihan insiden.
DHCP	singkatan dari *Dynamic Host Configuration Protocol*, yaitu protokol jaringan yang digunakan untuk memberikan alamat IP secara otomatis kepada perangkat yang terhubung.
Endpoint	perangkat akhir yang terhubung ke jaringan, seperti komputer, laptop, atau *smartphone*.
FireEye Redline	perangkat lunak analisis forensik memori dan artefak sistem dari FireEye.
Host-Only	mode jaringan mesin virtual yang membatasi koneksi hanya antara mesin virtual dan host.
IOC	singkatan dari *Indicator of Compromise*, yaitu indikator teknis yang menandai kemungkinan adanya kompromi pada sistem. Contohnya seperti nilai *hash file* berbahaya, IP mencurigakan, lonjakan lalu-lintas jaringan yang meningkat, dsb.

Lingkungan virtual	perangkat lunak yang meniru fungsi komputer atau jaringan nyata, digunakan untuk pengujian dalam ruang lingkup keamanan siber tanpa risiko terhadap sistem produksi.
Log	catatan aktivitas sistem atau pengguna yang digunakan untuk audit dan analisis.
Login bypass	teknik eksploitasi yang memungkinkan penyerang mendapatkan akses ke sistem tanpa memasukkan kredensial yang valid dengan memanipulasi mekanisme otentikasi.
Malware	singkatan dari *malicious software*, yaitu perangkat lunak yang ditujukan untuk merusak atau mendapatkan akses tidak sah ke sistem.
Memory dump	catatan aktivitas sistem atau pengguna yang digunakan untuk audit dan analisis.
Metasploit	*framework* eksploitasi dan pasca eksploitasi yang digunakan untuk pengujian penetrasi.
Metasploitable	sebuah mesin virtual *open-source* yang dirancang untuk memiliki kerentanan yang dapat digunakan sebagai latihan pengujian penetrasi.
NAT	singkatan dari *Network Address Translation*, yaitu tipe pengaturan jaringan yang memungkinkan mesin virtual mengakses jaringan luar melalui alamat IP *host*.
NetworkMiner	alat forensik jaringan untuk mengekstraksi artefak dari file PCAP.
Offensive security	praktik keamanan siber yang menekankan strategi menyerang untuk mengidentifikasi kerentanan sistem.
Payload	kode atau data yang dikirimkan oleh penyerang sebagai bagian dari serangan.
PCAP	singkatan dari *Packet Capture*, yaitu format *file* hasil rekaman lalu lintas jaringan yang digunakan dalam analisis.
Pentest	singkatan dari *penetration test* atau pengujian penetrasi, yakni aktivitas simulasi serangan terhadap sistem atau jaringan untuk mengidentifikasi dan mengeksploitasi kerentanan yang mungkin ada, dengan tujuan mengevaluasi tingkat keamanan dan memberikan rekomendasi perbaikan.

Phishing	teknik rekayasa sosial untuk mengelabui korban agar memberikan informasi sensitif.
Ransom note	pesan ancaman dari pelaku *ransomware* yang berisi instruksi pembayaran tebusan.
Ransomware	jenis *malware* yang mengenkripsi file korban dan menuntuk pembayaran untuk pemulihan.
Red team	tim penyerang yang mensimulasikan serangan terhadap sistem dalam pengujian keamanan.
SOC	singkatan dari *security operation* center, yaitu pusat pemantauan dan respons insiden keamanan dalam suatu organisasi.
SQL *injection*	teknik serangan yang dilakukan dengan memasukkan perintah SQL berbahaya ke dalam input sistem, dengan tujuan mengakses atau memodifikasi suatu sistem.
Threat hunting	aktivitas proaktif untuk mencari ancaman atau aktivitas mencurigakan di sistem sebelum terdeteksi oleh alat otomatis.
Walkthrough	panduan langkah demi langkah untuk menyelesaikan skenario pelatihan.
Wireshark	perangkat lunak *open-source* yang berfungsi untuk menganalisis dan merekam lalu lintas jaringan.
XSS	singkatan dari *cross-site-scripting*, yaitu jenis serangan yang menyisipkan skrip berbahaya ke dalam halaman web.
Zero-day	kerentanan keamanan dalam perangkat lunak atau sistem yang belum diketahui oleh pengembang atau vendor, dan belum tersedia perbaikannya.
Zero Trust Architecture	pendekatan arsitektur keamanan yang mengasumsikan bahwa tidak ada entitas yang sepenuhnya dapat dipercaya dengan menggunakan prinsip "*never trust, always verify*".

DAFTAR ISI

HALAMAN JUDUL i
HALAMAN PENGESAHAN DOSEN PEMBIMBING ii
HALAMAN PENGESAHAN DOSEN PENGUJI iii
HALAMAN PERNYATAAN KEASLIAN TUGAS AKHIR iv
HALAMAN PERSEMBAHAN v
HALAMAN MOTO vi
KATA PENGANTAR vii
SARI ix
GLOSARIUM x
DAFTAR ISI xiii
DAFTAR TABEL xiv
DAFTAR GAMBAR xv
BAB I PENDAHULUAN 1
1.1 Latar Belakang 1
1.2 Ruang Lingkup 3
1.3 Tujuan 4
1.4 Manfaat 4
1.5 Batasan Masalah 5
BAB II KAJIAN PUSTAKA 6
2.1 Keamanan Siber 6
2.2 CIA *Triad* 8
2.3 Tantangan Keamanan Siber 9
2.4 *Blue Team* 10
2.5 Gamifikasi Pembelajaran Keamanan Siber 11
2.6 Cyber Range 17
BAB III PELAKSANAAN MAGANG 22
3.1 Pengembangan *Cyber Range* Analisis *Malware* 23
3.2 Pengembangan *Cyber Range* Analisis Jaringan 34
3.3 Evaluasi Luaran Proyek 44
3.4 Penyerahan Luaran Proyek 45
BAB IV REFLEKSI PELAKSANAAN MAGANG 46
4.1 Pemahaman sebelum Magang 46
4.2 Lingkungan Kerja 47
4.3 Perkembangan Kompetensi 48
4.4 Kontribusi terhadap Perusahaan 49
BAB V PENUTUP 51
5.1 Kesimpulan 51
5.2 Saran 52
DAFTAR PUSTAKA 53
LAMPIRAN 56

DAFTAR TABEL

Tabel 3.1 *Timeline* Pelaksanaan Magang 22
Tabel 3.2 Informasi mesin yang terlibat dalam skenario analisis *malware* 23
Tabel 3.3 Informasi mesin yang terlibat dalam skenario analisis jaringan 35

DAFTAR GAMBAR

Gambar 2.1 CIA *triad* beserta cakupannya 8
Gambar 2.2 Tampilan halaman web HackTheBox 13
Gambar 2.3 *Learning path* HackTheBox 13
Gambar 2.4 *Learning roadmap* TryHackMe 15
Gambar 2.5 Pilihan metode belajar LetsDefend 16
Gambar 2.6 Pilihan *Online Labs* dari CyberDefenders 16
Gambar 2.7 Taksonomi *cyber range* 17
Gambar 3.1 Proses menyiapkan aset berupa *file* gambar di mesin korban 24
Gambar 3.2 Informasi *ransomware* yang digunakan untuk infeksi mesin korban 25
Gambar 3.3 *File ransomware* diunggah ke situs file.io 26
Gambar 3.4 *Ransom Note* yang ditinggalkan setelah infeksi 27
Gambar 3.5 *File* gambar yang telah terenkripsi 27
Gambar 3.6 Tampilan mesin korban setelah terinfeksi *ransomware* 27
Gambar 3.7 Program *decryptor* yang dijalankan di mesin korban 28
Gambar 3.8 Tampilan aplikasi Redline 28
Gambar 3.9 Opsi tambahan konfigurasi *collector* 30
Gambar 3.10 Direktori *collector* Redline 31
Gambar 3.11 Tampilan *command prompt* dari proses *memory dump* 31
Gambar 3.12 *File* hasil disimpan dalam ekstensi Mandiat Analysis 31
Gambar 3.13 *File* Mandiant Analysis 32
Gambar 3.14 Contoh soal yang terdapat di *walkthrough* analisis *malware* 34
Gambar 3.15 Topologi jaringan skenario analisis jaringan 36
Gambar 3.16 Percakapan penyerang 1 dan penyerang 2 37
Gambar 3.17 Alat Pentmenu digunakan untuk serangan TCP SYN *flood* 37
Gambar 3.18 Alat LOIC dijalankan untuk serangan UDP *flood* 38
Gambar 3.20 Pesan yang terekam pada salah satu paket UDP serangan 39
Gambar 3.19 Penyerang 2 mengunggah salah satu *file* ke direktori dav target 39
Gambar 3.22 Penelusuran *file* yang diunggah penyerang menggunakan NetworkMiner 40
Gambar 3.21 Lalu lintas paket setiap *endpoint* yang terekam oleh Wireshark 40
Gambar 3.23 Percobaan dalam memicu eror dengan karakter ‘ 41
Gambar 3.24 Serangan SQL *injection* berhasil melakukan *login bypass* 41
Gambar 3.25 *Payload* yang digunakan untuk serangan XSS. 42

Gambar 3.26 Penelusuran serangan SQL *injection* menggunakan Wireshark 42
Gambar 3.27 Penelusuran serangan XSS menggunakan Wireshark 42
Gambar 3.28 Contoh soal yang terdapat di *walkthrough* analisis jaringan..... 43

BAB I
PENDAHULUAN

1.1 Latar Belakang

Meningkatnya digitalisasi dalam berbagai aspek kehidupan telah mendorong pertumbuhan eksponensial dalam penggunaan perangkat terhubung dan layanan berbasis internet. Namun, kemajuan ini juga diiringi dengan lonjakan ancaman siber yang semakin kompleks dan sulit diprediksi. Berbagai jenis serangan siber kini tidak hanya menargetkan sektor korporasi tetapi juga menargetkan layanan publik, infrastruktur publik, hingga ke ranah pemerintahan. Ancaman siber yang meningkat secara global tercermin di kawasan Asia Tenggara. Negara-negara anggota ASEAN menghadapi tantangan serupa dalam menjaga ketahanan sistem informasi mereka. Kerentanan ASEAN terhadap serangan berskala besar terlihat jelas dari beberapa insiden signifikan, seperti kebocoran data pemilu di Filipina dan peretasan sistem kesehatan SingHealth di Singapura (Lee et al., 2025). Insiden-insiden ini memperlihatkan dampak serius dari serangan siber terhadap stabilitas sosial, ekonomi, dan keamanan nasional. Di Indonesia sendiri juga telah mengalami berbagai serangan siber seperti kebocoran data sebagian besar layanan publik yang disimpan di Pusat Data Nasional (PDN), serangan *ransomware* WannaCry, dan beberapa serangan lainnya yang berskala nasional. Ancaman siber yang menyasar sektor perusahaan juga mengalami peningkatan tajam. Kebocoran data yang disebabkan oleh berbagai serangan telah menimbulkan kerugian, sehingga banyak perusahaan mulai menerapkan berbagai standar, *framework*, dan regulasi keamanan siber sebagai bagian dari strategi perlindungan aset digital mereka. Beberapa di antaranya seperti ISO/IEC 27001, General Data Protection Regulation (GDPR), dan *Zero Trust Architecture*.

Situasi ini mendorong para ahli memprediksi bahwa serangan siber di masa mendatang akan semakin canggih dan merusak. Ancaman ini diperkirakan akan meningkat tidak hanya secara teknis, tetapi juga dalam skala serangan dan dampaknya. Berdasarkan studi yang dilakukan oleh para pakar keamanan siber, *ransomware* diperkirakan tetap menjadi salah satu jenis serangan paling signifikan, tidak hanya dapat memblokir akses sistem, tetapi juga melibatkan pencurian dan pemerasan. Beberapa jenis serangan lainnya seperti serangan *phishing* juga diperkirakan akan meningkat dengan metode yang semakin canggih. Ancaman terhadap infrastruktur digital mulai menyasar sistem berbasis *cloud*. Kondisi ini semakin diperparah dengan meluasnya penggunaan *remote work environment* pasca pandemi COVID-

19. Celah keamanan yang muncul dari penggunaan perangkat pribadi yang tidak dilindungi oleh kebijakan keamanan organisasi menjadi salah satu titik lemah yang rawan dieksploitasi. Oleh karena itu, langkah proaktif dan adaptif menjadi krusial untuk menghadapi dinamika ancaman siber yang terus berubah (Al-Hawamleh, 2023).

Kompleksitas serangan siber yang terus meningkat menuntut kesiapan sumber daya manusia yang andal dalam menanganinya. Tidak cukup dengan mengandalkan alat dan perlengkapan keamanan seperti sistem pertahanan otomatis, kualitas dan kesiapan personel keamanan siber menjadi faktor kunci dalam mendeteksi, meresepons, serta memulihkan sistem dari insiden siber. Sayangnya, kesenjangan antara permintaan dan ketersediaan tenaga profesional keamanan siber masih menjadi tantangan besar. Permasalahan ini diperparah oleh kurangnya standar kompetensi yang seragam serta belum optimalnya integrasi kurikulum pendidikan dengan kebutuhan dunia kerja (Mallick & Nath, 2024). Akibatnya, proses rekrutmen di sektor industri maupun pemerintahan sering kali menghadapi kesulitan dalam menemukan kandidat yang berkualitas. Untuk menjembatani kesenjangan tersebut, diperlukan pengembangan model pelatihan yang berorientasi praktik, dengan pendekatan simulasi dan skenario yang merepresentasikan kondisi nyata, sehingga peserta pelatihan tidak hanya memahami konsep, tetapi juga terlatih dalam menerapkan solusi secara taktis dan strategis.

Untuk menjawab tantangan pengembangan keterampilan teknis di bidang keamanan siber, diperlukan materi pelatihan yang menekankan pada pendekatan berbasis praktik langsung. Pendekatan semacam ini memungkinkan peserta untuk memahamai konteks pembelajaran secara nyata dan aplikatif. Untuk meningkatkan minat dan keterlibatan peserta, elemen gamifikasi sering diintegrasikan ke dalam pelatihan sebagai pemicu motivasi belajar yang lebih kuat. Pendekatan pembelajaran berbasis gamifikasi, seperti *open-ended Capture The Flag* (CTF), terbukti mampu membangun lebih dari sekadar keahlian teknis. Studi yang dilakukan oleh (Williams et al., 2024) menunjukan bahwa metode ini turut mengembankan keterampilan kolaborasi, kemampuan riset, pemikiran kritis, serta pemecahan masalah yang merupakan kompetensi dasar penting lintas disiplin. Selain fleksibel dan dapat diadaptasikan ke berbagai modul pembelajaran, pendekatan ini juga memperkaya kurikulum akademik melalui pengalaman yang lebih kontekstual dan aplikatif. Tingginya antusiasme peserta dalam mengikuti pembelajaran dengan metode tersebut juga mengindikasikan efektivitas metode ini dalam menciptakan lingkungan belajar yang menarik. Beberapa layanan daring kini telah menyediakan platform pembelajaran keamanan siber berbasis gamifikasi dengan gaya CTF, seperti Hack The Box, TryHackMe, dan picoCTF. Opsi ini akan sangat menarik minat para

pelajar individual karena menawarkan pengalaman belajar yang interaktif dan dapat diakses dengan mudah. Namun, untuk pelatihan yang ditujukan dalam skala *enterprise*, platform daring semacam ini tidak selalu dapat memenuhi kebutuhan pembelajaran yang lebih spesifik. Perusahaan sering kali membutuhkan skenario pelatihan yang disesuaikan dengan konteks infrastruktur internal, peran spesifik dari tim keamanan, serta kebijakan organisasi yang berlaku. Di sisi lain, meskipun beberapa platform dari juga menawakan layanan pelatihan dengan skala *enterprise*, biaya yang diperlukan untuk lisensi dan implementasi dalam skala besar cenderung tinggi dan tidak selalu sebanding dengan fleksibiltas yang ditawarkan.

Oleh karena itu, *cyber range* dapat menjadi solusi terhadap permasalahan tersebut. *Cyber range* merupakan lingkungan virtual yang diracang untuk menyimulasikan skenario ancaman dan insiden keamanan siber secara realistis, sehingga memungkinkan peserta untuk berlatih dalam situasi yang menyerupai kondisi nyata. Dengan kontrol penuh terhadap desain skenario, infrastruktur, serta tujuan pembelajaran, pengembang *cyber range* dapat menyesuaikan materi pelatihan agar sesuai dengan kebutuhan spesifik organisasi. Pelatihan keamanan siber yang tersedia saat ini juga cenderung lebih banyak berfokus pada aspek menyerang (*offensive*). Padahal, kebutuhan tenaga kerja yang berperan dalam segi *defensive* juga tidak kalah penting dan bahkan krusial dalam konteks ketahanan siber organisasi. Oleh karena itu, pengembangan *cyber range* yang mengakomodasi pelatihan untuk *blue team* menjadi langkah strategis dalam menjebatani kesenjangan tersebut.

Tujuan utama dari penyusunan laporan akhir ini adalah untuk mendeskripsikan proses perancangan dan pengembangan media pelatihan teknis yang disusun secara sistematis dan kontekstual sesuai dengan kebutuhan pembelajaran di bidang keamanan siber, khususnya untuk penguatan kapabilitas *blue team*. Selama pelaksanaan magang, telah dikembangkan dua skenario *cyber range* yang berfokus pada analisis lalu lintas jaringan dan investigasi artefak sistem. Bahan latihan dan soal berbasis CTF. Hasil yang dicapai diharapkan dapat memberikan wawasan mengenai pengembangan media pelatihan di bidang keamanan siber, serta mampu menghadirkan solusi alternatif yang relevan terhadap kebutuhan pelatihan yang nyata dan kontekstual.

1.2 Ruang Lingkup

Kegiatan magang telah dilaksanakan selama enam bulan di PT. Adikarya Tata Informasi, atau sering disebut Aditasi, dengan penempatan posisi sebagai IT Auditor. Selama menjalankan peran tersebut, berbagai aktivitas dilakukan yang berfokus pada bidang keamanan informasi,

khususnya materi pelatihan keamanan siber untuk Bank umum sesuai dengan regulasi OJK No 29/SEOJK.03/2022. Lingkup kegiatan yang dikerjakan meliputi:

a. Mengikuti sesi *onboarding* dari perusahaan dengan diskusi bersama *supervisor* dan perkenalan lingkungan kerja.
b. Melakukan penelusuran keperluan elemen *Tabletop Exercise* dan *Cyber Range* sesuai referensi dari perusahaan.
c. Menyusun materi teori dalam bentuk *Tabletop Exercise* beserta dokumen pelengkap seperti *After-Action Report*, *Exercise Brief Slide Deck*, *Logistic Checklist Template*, *Note Taking Template*, *Participant Guide*, dan *Participant Feedback Form*.
d. Mengembangkan *cyber range* sebagai materi praktik.
e. Menyusun *walkthrough* teknis.
f. Evaluasi dan revisi skenario pelatihan bersama *supervisor*.
g. Presentasi hasil kerja kepada rekan kerja perusahaan.

1.3 Tujuan

Tujuan yang diangkat adalah: 1) Mengkaji pengembangan materi pelatihan keamanan siber berbasis praktik melalui media *cyber range* yang dilengkapi dengan *walkthrough*, guna memfasilitasi pembelajaran teknis bagi personal keamanan siber, khususnya pada domain *defensive security* atau *blue team*. 2) Merancang materi yang mampu merepresentasikan situasi dan tantangan nyata di lingkungan kerja, sehingga dapat meningkatkan kesiapan peserta dalam menghadapi insiden keamanan serta memperkuat kemampuan analisis terhadap artefak digital.

1.4 Manfaat

Manfaat Akademis

a. Memberikan kontribusi sebagai sumber pengetahuan baru terkait media pelatihan di bidang keamanan siber
b. Menawarkan pendekatan alternatif dalam pembelajaran praktik yang menekankan kemampuan analisis dan pemecahan masalah.
c. Fokus pengembangan materi berada pada domain *defensive security*, yang masih relatif terbatas dibandingkan pelatihan *offensive*.
d. Dapat dimanfaatkan sebagai referensi maupun sarana belajar untuk memperdalam pemahaman teknis dalam keamanan siber.

Manfaat untuk Perusahaan

a. Membantu perusahaan dalam menyelesaikan proyek pembuatan materi latihan keamanan siber untuk sektor perbankan umum
b. Materi yang dirancang dapat digunakan kembali dan dapat disesuaikan dengan kebutuhan pelatihan internal perusahaan.
c. Pendekatan dan teknologi yang digunakan selama proses pengembangan memberikan wawasan baru yang relevan.
d. Memperkenalkan metode dan teknologi yang belum banyak diimplementasikan di perusahaan.

1.5 Batasan Masalah

1. Meskipun selama magang juga dikembangkan *cyber range* untuk *offensive* security, pembahasan berfokus pada pengembangan *cyber range* untuk domain *defensive security*, meliputin *network traffic analysis* dan *malware analysis*.
2. Pengujian dilakukan pada mesin virtual lokal dengan konfigurasi berikut:
    a. *Host* sistem operasi berbasis Windows.
    b. Mesin virtual berbasis Linux digunakan untuk menjalankan simulasi serangan
    c. Mesin virtual berbasis Windows digunakan sebagai target dan sekaligus sebagai *workstation* analisis.

BAB II
KAJIAN PUSTAKA

2.1 Keamanan Siber

Keamanan siber merupakan bidang yang berfokus pada perlindungan sistem informasi, jaringan, perangkat, dan data. Fokus utamanya adalah mencegah berbagai ancaman dan akses tidak sah. Menurut CISA (2021), keamanan siber bertujuan untuk menjaga tiga prinsip utama, yaitu kerahasiaan, integritas, dan ketersediaan informasi. Prinsip ini penting untuk memastikan bahwa data sensitif hanya diakses oleh pihak yang berwenang, tidak diubah tanpa izin, dan selalu tersedia saat dibutuhkan. Dalam era digital saat ini, peran keamanan siber menjadi semakin krusial karena hampir seluruh aktivitas ekonomi, sosial, dan pemerintahan bergantung pada infrastruktur digital yang rentan terhadap serangan siber.

Keamanan siber merupakan konsep multidisipliner yang tidak hanya mencakup perlindungan terhadap teknologi informasi, tetapi juga melibatkan faktor manusia, kebijakan organisasi, serta interaksi sosial-teknis dalam konteks yang dinamis. Dalam studi yang dilakukan oleh Cains (2021), ditemukan bahwa definisi keamanan siber yang komprehensif mencakup elemen-elemen seperti pemeliharaan kerahasiaan, integritas, dan ketersediaan (CIA *triad*), serta fungsi sistem yang tangguh (*resilient*), deteksi intrusi yang akurat, dan pemahaman terhadap konteks ancaman. Meskipun demikian, banyak definisi formal dari lembaga standar masih berfokus pada aspek teknis dan sering kali mengabaikan peran manusia sebagai aktor penting, baik sebagai pengguna, pembela, maupun penyerang. Perbedaan definisi antara kalangan akademik dan praktisi, sebagaimana terungkap dalam penelitian ini, juga menimbulkan tantangan dalam komunikasi risiko dan kolaborasi antar disiplin. Oleh karena itu, pemahaman yang menyeluruh terhadap keamanan siber menjadi krusial dalam merumuskan strategi pertahanan yang adaptif dan efektif di tengah kompleksitas ancaman digital yang terus berkembang.

Ruang lingkup keamanan siber mencakup berbagai domain teknis seperti keamanan jaringan, keamanan aplikasi, keamanan operasional, dan keamanan informasi. Keamanan siber dipetakan sebagai gabungan dari kebijakan keamanan, teknologi jaringan, dan sistem perlindungan data yang dirancang untuk mencegah gangguan terhadap integritas sistem komputasi (Narsimha et al., 2022). Dalam praktiknya, sistem keamanan harus mampu merespons secara cepat terhadap berbagai ancaman siber yang semakin dinamis dan kompleks, terutama di sektor-sektor vital seperti perbankan dan layanan keuangan yang menjadi sasaran

utama kejahatan digital. Selain tantangan teknis, aspek sumber daya manusia juga menjadi perhatian utama dalam penguatan keamanan siber. Krisis tenaga kerja keamanan siber yang berkualitas menjadi hambatan besar dalam menghadapi ancaman global, sehingga penting untuk mendorong profesionalisasi bidang ini melalui pendidikan, pelatihan, sertifikasi, dan pembentukan standar kompetensi yang sistematis (Burley et al., 2014). Keamanan siber tidak bisa diserahkan hanya kepada teknisi tanpa spesialisasi, tetapi membutuhkan ekosistem tenaga kerja yang memiliki keahlian khusus dan pemahaman terhadap peran serta tanggung jawab dalam melindungi infrastruktur digital. Di samping itu, dimensi etika juga menjadi pilar penting dalam praktik dan penelitian keamanan siber. Pengembangan teknologi keamanan harus memperhatikan prinsip seperti *informed consent*, keadilan, dan akuntabilitas sosial agar implementasinya tidak menimbulkan dampak negatif terhadap individu maupun masyarakat (Macnish & van der Ham, 2020).

2.2 CIA *Triad*

Konsep CIA merupakan kerangka dasar dalam keamanan siber yang diterima secara global. *Confidentiality* (kerahasiaan) berarti memastikan informasi hanya dapat diakses oleh pihak yang berwenang. *Integrity* (integritas) mengacu pada menjaga keakuratan dan keutuhan informasi, mencegah modifikasi dan perusakan data. *Availability* (ketersediaan) menekankan bahwa sistem dan informasi harus selalu dapat diakses dan digunakan oleh pihak yang berwenang saat dibutuhkan (EBSCO, 2024). Konsep CIA *triad* sering diilustrasikan dengan bentuk segitiga yang merepresentasikan tiga pilar utama keamanan informasi yang saling melengkapi. Gambar 2.1 menunjukkan representasi visual dari prinsip CIA.

Gambar 2.1 CIA *triad* beserta cakupannya

Sumber: cimcor.com (2023)

CIA *triad* dijadikan acuan utama dalam perumusan kebijakan dan praktik keamanan siber di berbagai organisasi. Sebagai contoh, standar seperti NIST SP 800-12 juga mengadopsi model CIA sebagai pilar perlindungan informasi (Cawthra et al., 2020). Dengan berpegang pada CIA *triad*, organisasi berupaya memastikan data rahasia tetap terlindungi, informasi terjaga keakuratannya, dan layanan yang dibutuhkan dapat beroperasi tanpa gangguan.

2.3 Tantangan Keamanan Siber

Dalam era transformasi digital yang kian pesat, tantangan keamanan siber terus mengalami eskalasi baik dari sisi volume maupun kompleksitas serangan, berbagai penelitian menunjukkan bahwa lanskap ancaman siber global tidak hanya berkembang dari sisi teknis, tetapi juga melibatkan dimensi manusia dan kebijakan (Cains, 2021; Stock et al., 2022). Jenis serangan seperti *ransomware* yang mengenkripsi data dan menuntut tebusan, masih menjadi salah satu ancaman paling merugikan dalam beberapa tahun terakhir. Selain itu, serangan berbasis *social engineering*, *phishing*, hingga serangan *insider* juga kian mengkhawatirkan, terutama karena sering kali luput dari deteksi alat otomatis (Cawthra et al., 2020).

Tantangan ini diperparah dengan munculnya teknik serangan berbasis *artificial intelligence* (AI), eksploitasi kerentanan *zero-day*, dan penggunaan infrastruktur *cloud* serta *Internet of Things* (IoT) yang memperluas vektor serangan. Oleh sebab itu, lembaga-lembaga seperti National Institute of Standards and Technology (NIST) dan International Organization for Standardization (ISO) telah mengembangkan berbagai kerangka kerja seperti NIST *Cybersecurity Framework* dan ISO/IEC 27001 untuk memperkuat postur keamanan organisasi. Namun, efektivitas penerapan standar-standar ini sangat bergantung pada kesiapan organisasi dalam mengintegrasikan strategi teknis dan peningkatan kapasitas sumber daya manusianya.

Salah satu tantangan utama dalam keamanan siber saat ini adalah dominasi faktor manusia sebagai titik lemah dalam sistem pertahanan digital. Laporan "Global Cybersecurity Outlook 2022" oleh World Economic Forum mengungkapkan bahwa penyebab insiden keamanan siber didominasi oleh kesalahan manusia, seperti kurangnya kesadaran, keteledoran, atau respons yang kurang tepat terhadap ancaman digital. Tantangan lainnya adalah minimnya tenaga profesional yang terampil di bidang keamanan siber. Kekurangan ini menghambat kemampuan organisasi untuk secara aktif melakukan deteksi dini, *incident response*, maupun upaya pemulihan. Dalam konteks global, tantangan-tantangan ini perlu dihadapi secara seksama, tidak hanya mengandalkan teknologi, tetapi juga membangun budaya keamanan yang kuat, peningkatan kesadaran, serta pengembangan kapasitas SDM secara strategis dan berkelanjutan (Stock et al., 2022).

Dari perspektif nasional, Indonesia menghadapi tantangan yang tidak kalah signifikan. Data dari Badan Siber dan Sandi Negara (BSSN) mencatat lebih dari 700 juta anomali trafik dan insiden siber sepanjang 2022, dengan *ransomware* dan *phishing*, menjadi dua jenis serangan paling dominan (CSIRT Banten, 2022). Laporan Interpol 2021 mengenai keamanan siber di Asia Tenggara bahkan menempatkan Indonesia sebagai negara dengan jumlah kasus

ransomware tertinggi di kawasan, mencapai lebih dari 1,3 juta insiden. Meskipun sejumlah kebijakan telah dicanangkan, termasuk Strategi Keamanan Siber Nasional melalui Peraturan Presiden No. 47 Tahun 2023 (paralegal, 2023), indeks kesiapan keamanan siber Indonesia masih tergolong rendah di tingkat global, menempati peringkat ke-83 dari 160 negara berdasarkan National Cyber Security Index (CSIRT Banten, 2022). Strategi nasional tersebut menargetkan penguatan regulasi, peningkatan kapabilitas teknik, pembentukan tim Computer Security Incident Response Team (CSIRT) di berbagai sektor, serta pengembangan literasi keamanan siber masyarakat. Namun demikian, tantangan fundamental tetap berada pada aspek kesenjangan kompetensi SDM. Banyak laporan yang menyarankan agar pendekatan yang bersifat *people-centric*, seperti pelatihan berbasis praktik dan pendidikan teknis yang kontekstual, perlu diperkuat untuk melengkapi kebijakan pemerintah (Aji, 2023; Cains, 2021). Dengan populasi digital yang besar dan ketergantungan tinggi terhadap teknologi, Indonesia membutuhkan pendekatan yang infklusif dan berkelanjutan guna membangun ekosistem pertahanan siber yang tangguh dan adaptif terhadap perubahan ancaman global.

2.4 *Blue Team*

Dalam domain keamanan siber, *blue team* merujuk pada kelompok profesional yang bertanggung jawab atas pertahanan sistem informasi dari berbagai ancaman dan serangan siber. Tugas utama mereka meliputi proses deteksi, respons, *containment* (isolasi), dan *recovery* (pemulihan) dari insiden siber yang terjadi di lingkungan organisasi. Di dalam sebuah *Security Operations Center* (SOC), *blue team* menggunakan berbagai alat dan metode untuk memantau jaringan, menganalisis *log*, melakukan *threat hunting*, serta menangani insiden secara sistematis dan *real-time* (Hofbauer, 2024). Mereka juga berperan dalam memperkuat kebijakan keamanan, mengelola konfigurasi sistem, serta menyiapkan rencana pemulihan untuk meminimalkan dampak serangan. Dari sudut pandang praktisi, *blue team* didefinisikan sebagai sekelompok profesional yang secara aktif mempertahankan jaringan dan sistem dari serangan, bukan hanya bereaksi terhadap insiden, tetapi juga mengambil peran proaktif dalam perencanaan keamanan, penguatan infrastruktur, dan validasi kontrol (Carey & Jin, 2020).

Untuk menjalankan peran *defensive security*, anggota *blue team* dituntut untuk memiliki beragam keterampilan teknis yang mendalam. Analisis forensik jaringan dan analisis *log* merupakan kompetensi penting untuk menyelidiki jejak serangan pada trafik jaringan maupun catatan sistem. Selain itu, *blue team* melakukan *threat hunting* guna mencari indikator serangan yang luput dari deteksi otomatis, serta menguasai prosedur *incident response* yang efektif dan

terstruktur. Survei profesional SOC tahun 2023 menunjukkan bahwa kemampuan *incident handling* merupakan keterampilan *defensive*, disusul oleh keahlian analisis trafik jaringan dan analisis *log server* sebagai tiga besar keterampilan yang paling dibutuhkan dalam *blue team* (Ophie, 2023). Temuan ini menegaskan pentingnya kompentensi dalam mengidentifikasi pola serangan melalui data lalu lintas jaringan maupun catatan *log* sistem, serta merespons insiden dengan cepat dan tepat. Lebih lanjut, peran spesialis seperti *incident responder* dan *threat hunter* di *blue team* menuntut kemampuan investigasi mendalam dan intelijen ancaman, termasuk analisis *malware* untuk dapat mengurangi dampak serangan yang lebih canggih (Kotwani, 2023). Penguatan keterampilan di bidang *Digital Forensics and Incident Response* (DFIR) pun diakui sangat vital bagi profesional *defensive security*, yang mendorong inisiatif pelatihan praktiks agar *blue team* siap menghadapi insiden nyata secara efektif.

Meningkatnya kompleksitas ancaman siber belakangan ini membuat organisasi kian bergantung pada personel *blue team* yang terampil, namun industri masih menghadapi kekurangan tenaga ahli di bidang ini. Badan keamanan siber Uni Eropa, ENISIA, menyoroti bahwa meskipun ancaman siber semakin canggih dan sulit ditanggulangi, sektor ini justru dihadapkan pada keterbatasan jumlah profesional terlatih dan melebarnya kesenjangan keterampilan di tenaga kerjanya (European Union Agency For Cybersecurity (ENISIA), 2025). Secara global, perkiraan kekurangan profesional keamanan siber sekitar 3,4 juta profesional keamanan siber yang menandakan permintaan tinggi untuk peran-peran *defensive security* belum terpenuhi oleh pasokan SDM yand ada. Khusus untuk posisi *security analyst*, tingkat pertumbuhannya diproyeksikan 150% lebih tinggi daripada rata-rata pertumbuhan pekerjan sektor siber secara umum (Ophie, 2023). Ini menunjukkan betapa tingginya kebutuhan industri akan ahli pertahanan siber. Sejalan dengan tren ini, para profesional *blue team* dituntut untuk terus memperbarui keahliannya sesuai perkembangan teknologi.

2.5 Gamifikasi Pembelajaran Keamanan Siber

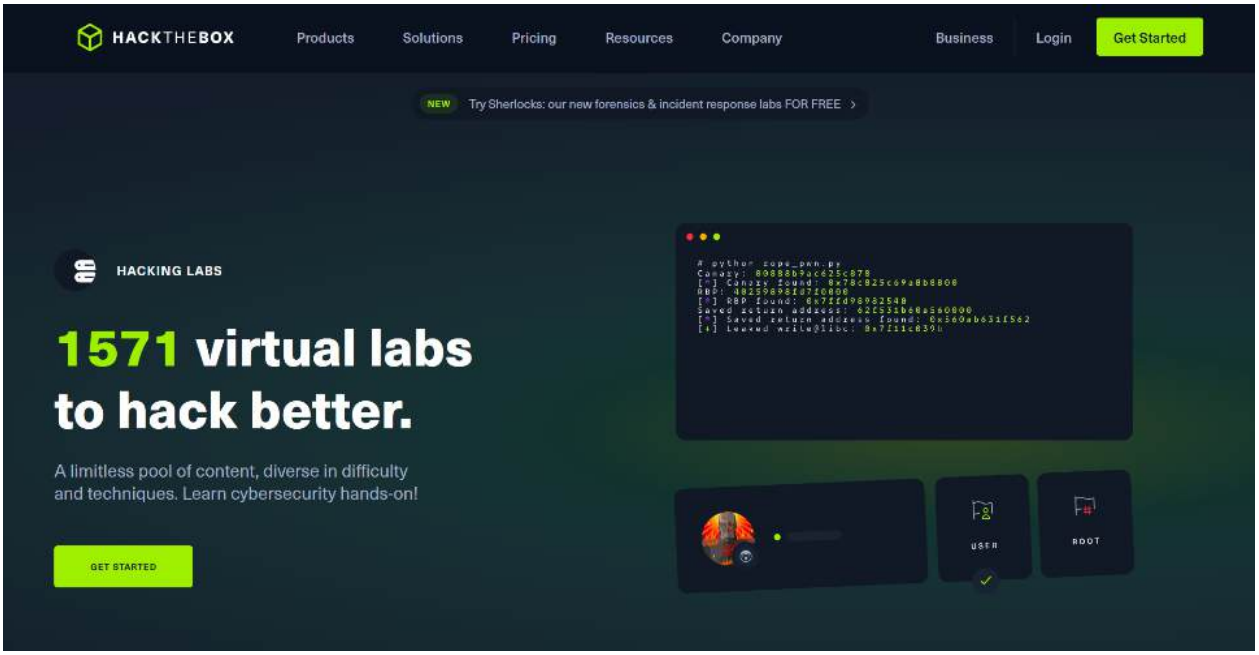
Pendekatan *puzzle-based learning* telah digunakan secara strategis dalam pendidikan keamanan siber sebagai metode untuk melatih pemikiran logis, deduktif, dan keterampilan teknis peserta. Metode ini menyajikan skenario dalam bentuk teka-teki atau tantangan yang perlu diselesaikan secara sistematis, sehingga peserta didorong untuk memahami konsep secara mendalam dan mengembangkan kemampuan *problem solving* yang aplikatif. Karakteristik interaktif dan berbasis tantangan membuat metode ini efektif dalam membangun keterampilan yang relevan dengan praktik pertahanan siber. Dalam konteks yang lebih luas, *puzzle-based*

learning juga menjadi dasar dari desain tantangan dalam *capture the flag* (CTF), di mana peserta harus menyelesaikan serangkaian tugas teknis yang merepresentasikan insiden atau kelemahan keamanan nyata. Dengan pendekatan ini, pembelajaran menjadi lebih kontekstual, menantang, dan berorientasi pada penguasaan keterampilan praktis (Dasgupta et al., 2013; Švábenský et al., 2021).

Capture The Flag (CTF) merupakan salah satu bentuk konkret dari pembelajaran berbasis gamifikasi yang mengadopsi pendekatan *puzzle-based* secara intensif. Dalam konteks pendidikan keamanan siber, CTF telah diakui sebagai sarana efektif untuk menyimulasikan skenario ancaman siber dalam format kompetitif dan terstruktur. CTF dirancang agar peserta dapat mengeksplorasi berbagai domain keamanan seperti eksploitasi jaringan, kriptografi, forensik digital, dan *reverse engineering* (Švábenský et al., 2021). Penelitian menunjukan bahwa partisipasi dalam CTF memperkuat keterampilan teknis, kreativitas, dan pemecahan masalah (Horcher, 2020).

Dari wawancara para profesional dalam buku "*Tribe of Hackers Blue Team*", terlihat bahwa pendekatan pembelajaran di bidang ini sangat menekankan eksplorasi teknis. Pembelajaran dari laporan hasil uji penetrasi dan pemahaman terhadap sistem seperti Windows Active Directory juga dianggap penting, terutama untuk menelaah logika serangan dari sudut pandang *defensive*. Berbagai metode pembelajaran seperti CTF dan pelatihan berbasis praktik turun direkomendasikan karena dinilai mampu mengembangkan kemampuan teknis dan pola pikir analitis yang dibutuhkan dalam peran pertahanan siber (Carey & Jin, 2020).

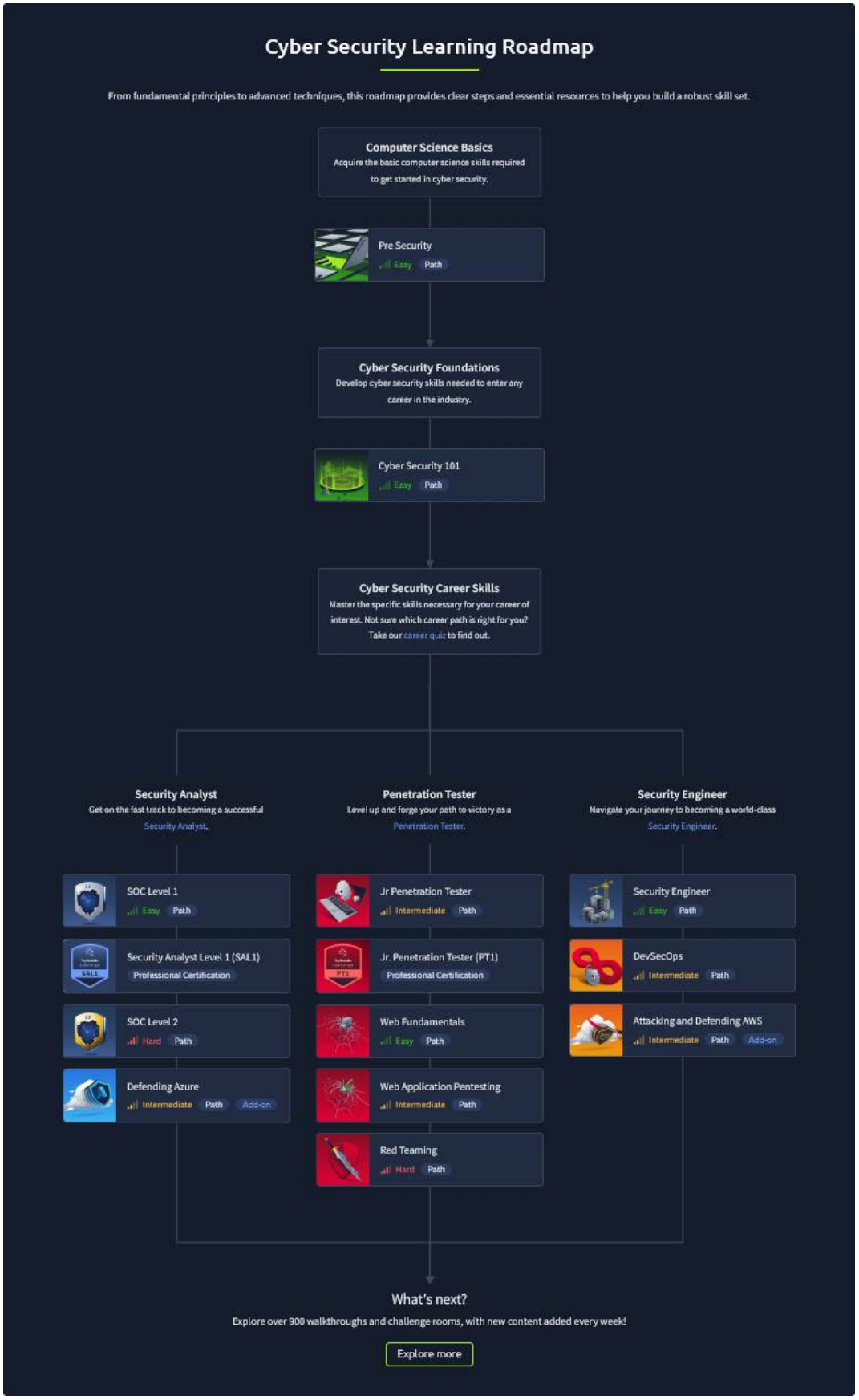
Berbagai platform CTF telah dikembangkan untuk mendukung pelatihan teknis secara mandiri maupun terstruktur. Platform-platform ini menyediakan skenario simulasi yang beragam, mulai dari pengenalan dasar hingga tantangan tngkat lanjut yang merefleksikan kondisi nyata di dunia kerja, Salah satu platform popupler adalah Hack The Box (HTB), yang menyediakan lingkungan virtual untuk melakukan eksploitasi sistem, *reverse engineering*, dan analisis forensik dengan pendekatan yang sangat praktis dan realistis. Tampilan halaman web HackTheBox dapat dilihat pada Gambar 2.2. HTB juga menawarkan *blue team labs* yang dirancang khusus untuk pelatihan pertahanan siber dan *incident response*¸seperti yang terlihat pada Gambar 2.3.



Gambar 2.2 Tampilan halaman web HackTheBox

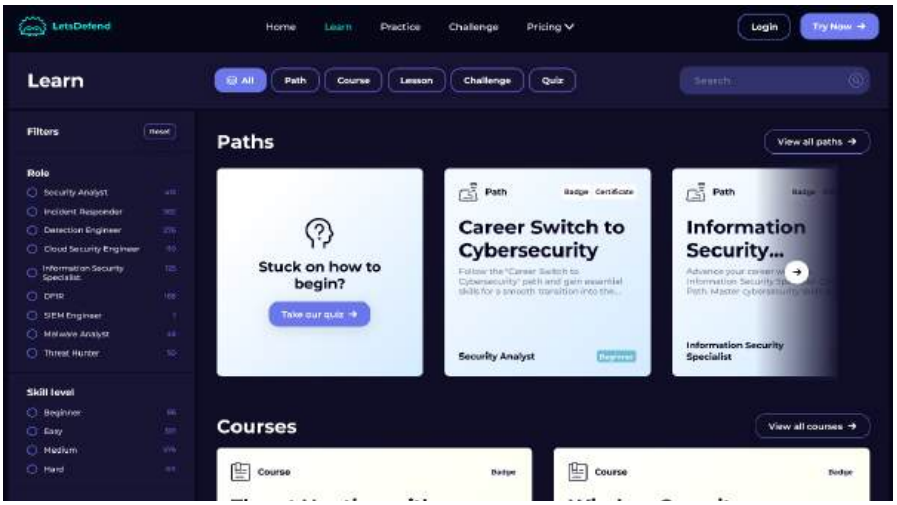
Gambar 2.3 *Learning path* HackTheBox

Selain HTB, terdapat TryHackMe, platform yang berfokus pada pembelajaran modular dan terpandu, menjadikannya cocok untuk pemula. TryHackMe menyediakan jalur pembelajaran bertahap dengan panduan dan penjelasan setiap langkahnya, serta simulasi jaringan yang interaktif. Platorm ini mencakup materi *offensive* dan *defensive*, termasuk pengenalan terhadap SOC, manajemen *log*, serta analisis serangan. Terdapat penjuruan spesialiasi dari keamanan siber yang ditawarkan oleh TryHackMe, seperti yang terlihat pada Gambar 2.4.

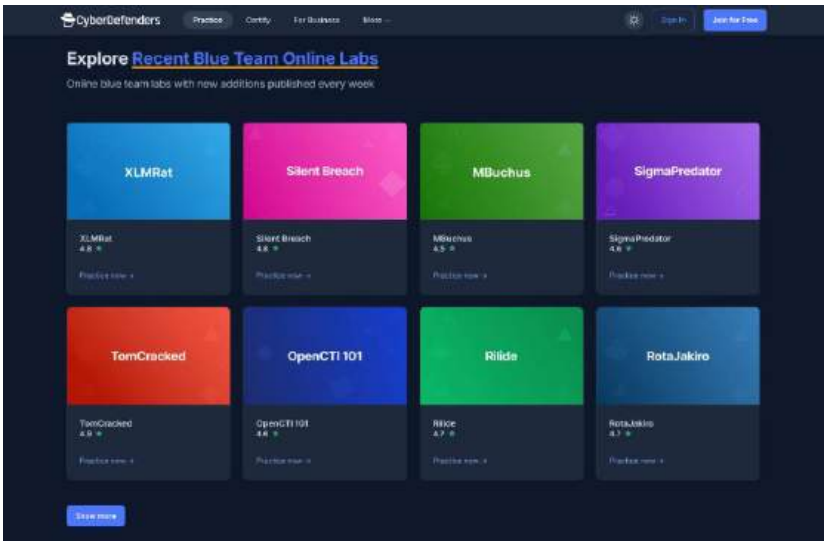


Gambar 2.4 *Learning roadmap* TryHackMe

Untuk kebutuhan pelatihan *blue team* yang lebih spesifik, terdapat platform seperti LetsDefend dan CyberDefenders. Tampilan halaman web dari kedua platform yang menawarkan berbagai metode belajar dapat dilihat pada Gambar 2.5 dan Gambar 2.6 LetsDefend menyediakan simulasi dunia nyata di lingkungan SOC, di mana pengguna dapat melakukan triase insiden dan penanganan kasus seperti serangan *phishing* atau *malware*. Platform ini menempatkan peserta langsung pada peran seorang analis keamanan. Sementara itu, CyberDefenders menawarkan berbagai tantangan forensik digital, analisis jaringan, dan investigasi *log* yang dikemas dalam bentuk CTF dengan skenario insiden siber yang nyata. Pilihan metode belajar LetsDefend



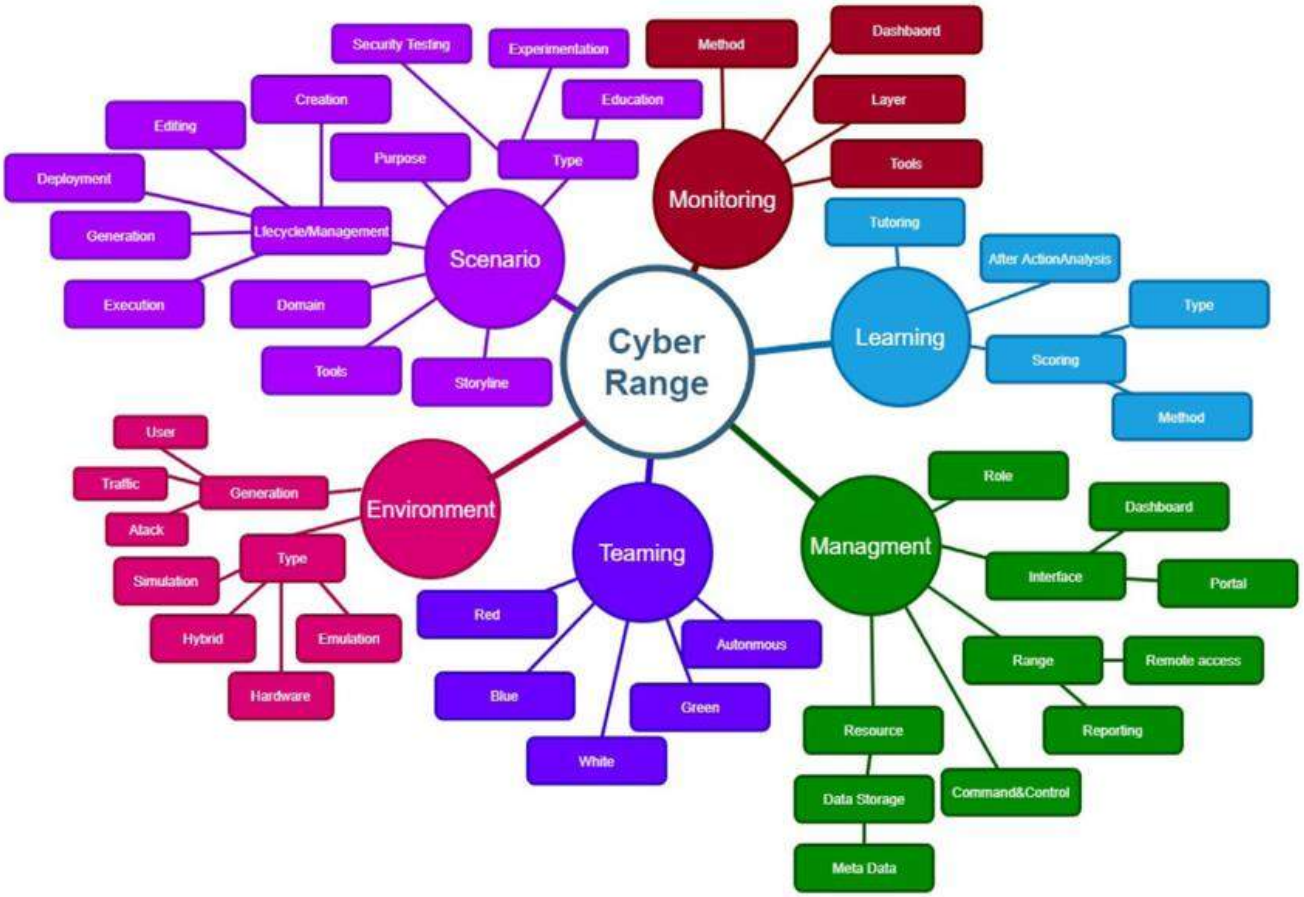
Gambar 2.5 Pilihan metode belajar LetsDefend



Gambar 2.6 Pilihan *Online Labs* dari CyberDefenders

2.6 Cyber Range

Cyber range secara umum didefinisikan sebagai sebuah lingkungan simulasi yang mereplikasi sistem, jaringan, dan perangkat lunak yang digunakan dalam skenario dunia nyata, dengan tujuan utama memberikan pengalaman langsung dalam menghadapi insiden siber (Beauchamp, 2022). Media ini memungkinkan peserta untuk mengasah keterampilan teknis secara praktis mulai dari pengujian penetrasi, analisis *malware*, deteksi serangan, hingga penggunaan alat-alat dalam keamanan siber tanpa menimbulkan risiko terhadap sistem produksi yang sesungguhnya. Terdapat taksonomi *cyber range* yang dikembangkan untuk memberikan kerangka klasifikasi atas berbagai bentuk dan fungsi dari *cyber range*, seperti yang terlihat pada Gambar 2.7.



Gambar 2.7 Taksonomi *cyber range*

Lebih lanjut, seiring meningkatnya kebutuhan pelatihan yang bersifat dinamis dan interaktif, pendekatan berbasis *cyber range* juga terus berkembang. Salah satu pendekatan yang mulai diterapkan adalah integrasi gamifikasi dalam desain *cyber range*. Penelitian menunjukan bahwa elemen-elemen permainan seperti tantangan, poin, papan peringkat, dan simulasi

kompetitif dapat meningkatkan motivasi, keterlibatan, serta efektivitas pembelajaran peserta (Jelo & Helebrandt, 2022). Hal ini membuat *cyber range* tidak hanya sekadar tempat latihan teknis, tetapi juga menjadi sarana pembelajaran yang menarik dan berorientasi pada pengembangan keterampilan. Maka dari itu, elemen gamifikasi dapat dimanfaatkan pada saat pengembangan *cyber range* untuk menambahkan unsur hiburan sehingga para peserta pelatihan menjadi lebih tertarik untuk menjalankan *cyber range*. Dengan demikian, *cyber range* merupakan sebuah pendekatan pedagogis yang terstruktur, fleksibel, dan dapat disesuaikan dengan kebutuhan pelatihan keamanan siber di berbagai tingkat keahlian.

Meskipun platform CTF daring seperti Hack The Box, TryHackMe, dan CyberDefenders terbukti efektif dalam mendukung pembelajaran mandiri dan pelatihan teknis individual, pendekatan ini tidak sepenuhnya dapat mengakomodasi kebutuhan pelatihan perusahaan eksternal yang bersifat adaptif. Berdasarkan pengalaman selama pelaksanaan magang, materi yang tersedia pada platform CTF umumnya bersifat generik dan kurang relevan terhadap konteks spesifik peserta pelatihan perusahaan, baik dari segi infrastruktur sistem, skenario operasional, maupun kebutuhan peran kerja yang dilatih. Selain itu, jika pun platform CTF menawarkan layanan pelatihan skala *enterprise*, biaya lisensi dan implementasinya tergolong tinggi dan tidak selalu sebanding dengan fleksibilitas yang ditawarkan.

Sebagai alternatif, pengembangan materi pelatihan secara mandiri memberikan sejumlah keuntungan strategis. Pertama, konten pelatihan dapat dirancang secara otentik dan disesuaikan dengan kebutuhan spesifik peserta. Kedua, tim pengembang dari pihak penyelenggara pelatihan dapat menguasai materi secara menyeluruh, sehingga pada saat pelatihan berlangsung, instruktur mampu memberikan penjelasan komprehensif dan responsif terhadap kendala teknis maupun non-teknis yang mungkin terjadi. Ketiga, aspek keamanan pelatihan lebih terjamin karena lingkungan pelatihan berada dalam kontrol penuh. Hal ini penting terutama untuk skenario yang melibatkan aktivitas yang dapat menimbulkan kerusakan sistem seperti analisis *malware*, di mana eksekusi tanpa *sandbox* atau virtualisasi dapat berisiko merusak sistem pengguna. Berbeda dengan platform CTF umum yang memberikan kebebasan kepada peserta untuk menggunakan berbagai alat, skrip, atau teknik eksploitasi tanpa batasan teknis, lingkungan pelatihan untuk perusahaan sebaiknya dikondisikan agar terstandar dan aman. Oleh karena itu, *cyber range* yang dikembangkan secara internal menjadi solusi yang lebih tepat dan efektif untuk mendukung pelatihan keamanan siber dalam skala organisasi.

Pengembangan *cyber range* dalam penelitian-penelitian sebelumnya telah menunjukkan variasi pendekatan, arsitektur, dan tujuan pelatihan yang saling melengkapi dalam mendukung

peningkatan keterampilan praktis tim keamanan siber. Salah satu contoh pengembangan *cyber range* ditunjukkan oleh jurnal "Developing a Cyber Incident Exercises Model to Educate Security Teams" oleh Alothman et al., (2022), yang mengembangkan sebuah model latihan insiden siber berbasis simulasi bernama Q8CR (Kuwait Cyber Range) yang bertujuan untuk meningkatkan keterampilan tim keamanan informasi dalam merespons serangan siber secara nyata. Model ini dirancang karena keterbatasan pendekatan pembelajaran konvensional yang cenderung teoritis dan tidak mencerminkan dinamika serangan di dunia nyata. Q8CR membagi peserta ke dalam tiga tim, yaitu *red team* (penyerang), *blue team* (pembela), dan *black team* (pengawas dan evaluator). Keunggulan utama dari model ini adalah adanya rotasi peran antar peserta agar semua anggota tim memperoleh pengalaman dari sisi ofensif dan defensif. Platform Q8CR dibangun dari awal menggunakan HTML, CSS, JavaScript, dan PHP, serta dilengkapi dengan lebih dari 60 skenario latihan yang dikategorikan ke dalam empat domain utama serangan: *fraud online*, *web defacement*, *malware*, dan serangan jaringan. Sistem ini juga menyediakan mekanisme login berbasis peran, fitur pengumpulan hasil, penilaian performa otomatis, dan laboratorium virtual yang dilengkapi dengan perangkat seperti Kali Linux untuk mendukung kegiatan *penetration testing* maupun deteksi insiden. Temuan penting dari penelitian ini menunjukkan bahwa pendekatan berbasis skenario praktis dalam Q8CR secara efektif meningkatkan kesiapsiagaan, ketangkasan respons, dan pemahaman teknis peserta terhadap serangan siber. Model ini memberikan kontribusi signifikan dalam pengembangan media pembelajaran keamanan siber yang adaptif dan aplikatif, serta dapat direplikasi oleh institusi pendidikan maupun pelatihan profesional untuk menyiapkan tim keamanan siber yang kompeten dalam menghadapi ancaman nyata.

Penelitian lainnya yang turut memberikan kontribusi penting dalam pengembangan *cyber range* adalah KYPO (Knowledge Yielding Cybersecurity Online Platform) yang dirancang sebagai sistem modular berbasis *cloud* untuk mendukung pelatihan dan penelitian keamanan siber secara realistis (Vykopal & Ošlejšek, 2017). Platform ini dirancang agar fleksibel, dapat diskalakan, hemat biaya, dan mudah diakses, dengan fokus pada penyediaan lingkungan virtual yang menyerupai infrastruktur nyata. KYPO mendukung virtualisasi penuh dari sistem operasi, perangkat jaringan, serta pemantauan lalu lintas jaringan dan aktivitas pengguna melalui sistem visualisasi interaktif. Salah satu hal yang dikembangkan secara unik adalah pendekatan *platform-as-a-service* dengan antarmuka web yang mendukung kolaborasi multi-peran (penyerang, pembela, pengawas) dalam skenario pelatihan. KYPO juga mendukung interaksi melalui mode individual, kolaboratif, dan berbasis peran, serta integrasi dengan perangkat fisik

seperti Raspberry Pi untuk koneksi ke lingkungan nyata. Temuan unik yang relevan mencakup integrasi *time manager portlet* untuk sinkronisasi waktu lintas tampilan, mekanisme manajemen identitas terfederasi untuk autentikasi pengguna, serta sistem visualisasi topologi jaringan real-time dan grafis analitik 2D/3D yang mendukung analisis anomali. KYPO juga membedakan antara monitoring internal untuk peserta dengan *monitoring* eksternal untuk pengawas, suatu pendekatan yang mempertimbangkan aspek intrusivitas dan kegunaan data. Hasil dari pengembangan ini menunjukkan bahwa KYPO mampu digunakan secara luas dalam tiga skenario utama: (1) *cybersecurity research* and development melalui pengujian metode mitigasi dan deteksi serangan; (2) *digital forensic analysis* dengan pemanfaatan lingkungan analitik siap pakai; dan (3) *cybersecurity education and training* melalui *game*, CTF, serta simulasi serangan-pertahanan yang dapat dijalankan secara mandiri maupun terstruktur. Validasi platform dilakukan dalam berbagai pelatihan dan kompetisi nasional, menunjukkan efektivitasnya sebagai sarana pelatihan keterampilan teknis dan non-teknis dalam konteks keamanan siber. Penelitian ini juga membuka arah pengembangan lebih lanjut ke integrasi sistem *cyber-physical* dan peningkatan otomatisasi dalam penyusunan skenario.

Terakhir, jurnal berjudul "CRaaS: Cloud-based Smart Grid Cyber Range for Scalable Cybersecurity Experiments and Training" mengusulkan dan mengembangkan sebuah kerangka kerja bernama CRaaS (*Cyber Range as a Service*), yaitu sebuah solusi *cyber range* berbasis *cloud* yang ditujukan untuk mendukung eksperimen dan pelatihan keamanan siber pada sistem *smart grid* (Chng et al., 2024). CRaaS memungkinkan pengguna untuk secara otomatis membangun dan menjalankan simulasi lingkungan *smart grid* yang realistis dengan berbagai komponen seperti IED (*Intelligent Electronic Devices*), PLC (*Programmable Logic Controller*), SCADA HMI, dan *controller node* yang dikemas dalam kontainer Docker. Keunikan utama dari CRaaS terletak pada kemampuannya untuk mengatasi hambatan besar dalam pengembangan *cyber range*, seperti keterbatasan skalabilitas, kesulitan replikasi, tingginya biaya perangkat keras, serta keterbatasan akses dan konfigurasi sistem. Selain itu, sistem ini dilengkapi dengan antarmuka pengguna berbasis web yang memudahkan pengguna dalam mengatur topologi, memulai dan menghentikan simulasi, serta menjalankan serangan siber seperti *false command injection* dan *man-in-the-middle* (MITM) terhadap logika pengendalian beban listrik. Evaluasi kinerja CRaaS menunjukkan bahwa satu *node* virtual mampu menjalankan hingga 80–85 IED secara stabil, yang mencerminkan kapasitas memadai untuk menyimulasikan sistem substasi transmisi skala kecil hingga menengah. Dalam studi kasus yang dilakukan, tim peneliti menunjukkan keberhasilan serangan injeksi perintah palsu

terhadap *circuit breaker*, serta serangan MITM dengan memanipulasi data pengukuran tegangan untuk memicu pelepasan beban yang tidak perlu oleh PLC. Seluruh proses ini dilakukan dengan bantuan jaringan v*irtual overlay* yang realistis, seperti *overlay-lans*, *overlay-wan*, *overlay-backend*, dan *overlay-attack*, yang menciptakan segmentasi komunikasi menyerupai sistem *smart-grid* nyata. Hasil akhir dari penelitian ini menunjukkan bahwa CRaaS mampu memberikan solusi *cyber range* yang skalabel, fleksibel, dan mudah diakses, sekaligus mendukung replikasi lingkungan untuk tujuan *benchmarking* dan pelatihan. Dengan demikian, CRaaS menjadi pendekatan efektif untuk memperluas akses terhadap sarana uji keamanan siber *smart grid* yang sebelumnya terbatas hanya pada *testbed* fisik berskala besar dan mahal.

BAB III
PELAKSANAAN MAGANG

Program magang dilaksanakan selama enam bulan, dengan masa pengerjaan proyek yang dimulai pada tanggal 17 September 2024 hingga awal Februari 2025. Selama periode tersebut, kegiatan magang difokuskan pada pengembangan materi pelatihan keamanan siber, baik dalam bentuk simulasi teoritis berupa *tabletop exercise* maupun simulasi praktik berbasis *cyber range*.

Tabel 3.1 *Timeline* Pelaksanaan Magang

No	Aktivitas Magang	Waktu Pelaksanaan
1.	*On-Boarding* magang	17 September 2024
2.	Penyusunan *tabletop exercise*	18 September – 21 November 2024
3.	Penyusunan *cyber range*	26 November 2024 – 23 Januari 2025
4.	Presentasi, evaluasi, dan penyerahan *output* proyek	• 31 Januari 2025 (Penyerahan pertama) • 1 Februari 2025 (Presentasi) • 3 Februari 2025 (Penyerahan kedua)

Kegiatan magang diawali dengan proses *on-boarding* yang dipandu langsung oleh *supervisor* dengan tujuan untuk memberikan orientasi awal mengenai perusahaan, ruang lingkup pekerjaan, serta ekspektasi selama periode magang berlangsung. Kegiatan kemudian dilanjutkan dengan persiapan penyusunan yang dilakukan dengan mempelajari berbagai referensi yang relevan dengan *tabletop exercise* dan *cyber range*. Adapun beberapa referensi yang dipelajari sebelum penyusunan *cyber range* adalah platform CTF dan beberapa *write-up* penyelesaian CTF. Selama pelaksanaan magang, penulis bertanggung jawab mengembangkan tiga jenis *cyber range* yang berbeda, yaitu:

1. **Metasploitable *pentest***

   Pelatihan untuk *red team* berupa simulasi pengujian penetrasi yang dilakukan menggunakan metasploitable dengan fokus teknik eksploitasi menggunakan alat Metasploit maupun tanpa menggunakan Metasploit.

2. ***Malware Analysis***

   Pelatihan untuk *blue team* berupa investigasi sistem yang terinfeksi *ransomware*

3. ***Network Traffic Analysis* (PCAP)**

   Pelatihan untuk *blue team* dalam menganalisis lalu lintas jaringan berdasarkan *file* PCAP yang memuat rekaman aktivitas serangan.

Secara khusus, dua dari tiga *cyber range* yang dikembangkan diarahkan untuk *blue team*, sesuai dengan arahan *supervisor* yang melihat adanya kekosongan materi praktik dalam domain defensif. Skenario analisis *malware* dan analisis lalu lintas jaringan dipilih karena keduanya merupakan kompetensi inti dalam fungsi *Security Operations Center* (SOC) maupun *Computer Security Incident Response Team* (CSIRT).

3.1 Pengembangan *Cyber Range* Analisis *Malware*

Cyber range ini dirancang untuk melatih peserta dalam melakukan analisis forensik terhadap sistem yang terinfeksi *malware*, khususnya *ransomware*. Pendekatan yang digunakan adalah forensik memori menggunakan alat FireEye Redline. Fokus utama dari skenario ini adalah menyimulasikan insiden nyata di mana sebuah sistem Windows terinfeksi oleh *ransomware*, dan peserta bertindak sebagai investigator yang harus mengidentifikasi artefak, aktivitas, serta bukti digital lainnya berdasarkan hasil *memory dump*. Simulasi ini melibatkan tiga buah mesin virtual berbasis Windows 10 yang berjalan di atas perangkat lunak VMware Workstation Pro:

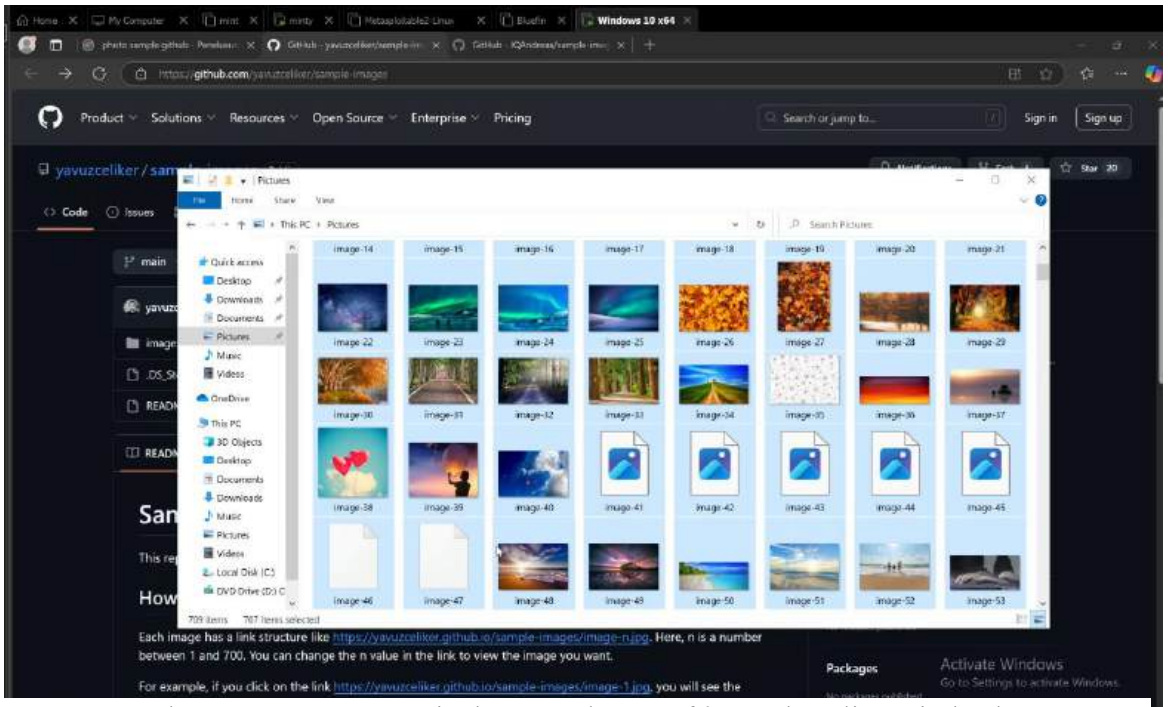
Tabel 3.2 Informasi mesin yang terlibat dalam skenario analisis *malware*

No	Mesin yang terlibat	Basis Sistem Operasi	Alamat IP	Adapter	Peruntukan
1.	Mesin yang terinfeksi	Windows 10	192.168.10.10/24	NAT	Digunakan untuk menjalankan *ransomware* dan melakukan *memory dump*
2.	Mesin investigator	Windows 10	192.168.10.8/24	NAT	Digunakan untuk menganalisis hasil *memory dump* dengan FireEye Redline
3.	Mesin Linux	Linux Mint	10.0.0.5/28	Host-Only	Digunakan untuk menyiapkan *file ransomware* yang akan dieksekusi di mesin yang terinfeksi

Langkah awal dalam pengembangan *cyber range* ini dimulai dengan pembuatan mesin virtual yang terinfeksi *ransomware*. Mesin ini bertindak sebagai sistem korban dalam simulasi dan bertujuan untuk meninggalkan artefak (jejak digital) yang relevan untuk keperluan forensik memori. Proses ini dilakukan secara terkontrol dalam lingkungan virtual menggunakan perangkat lunak VMware Workstation Pro.

A. Pembuatan mesin virtual yang terinfeksi

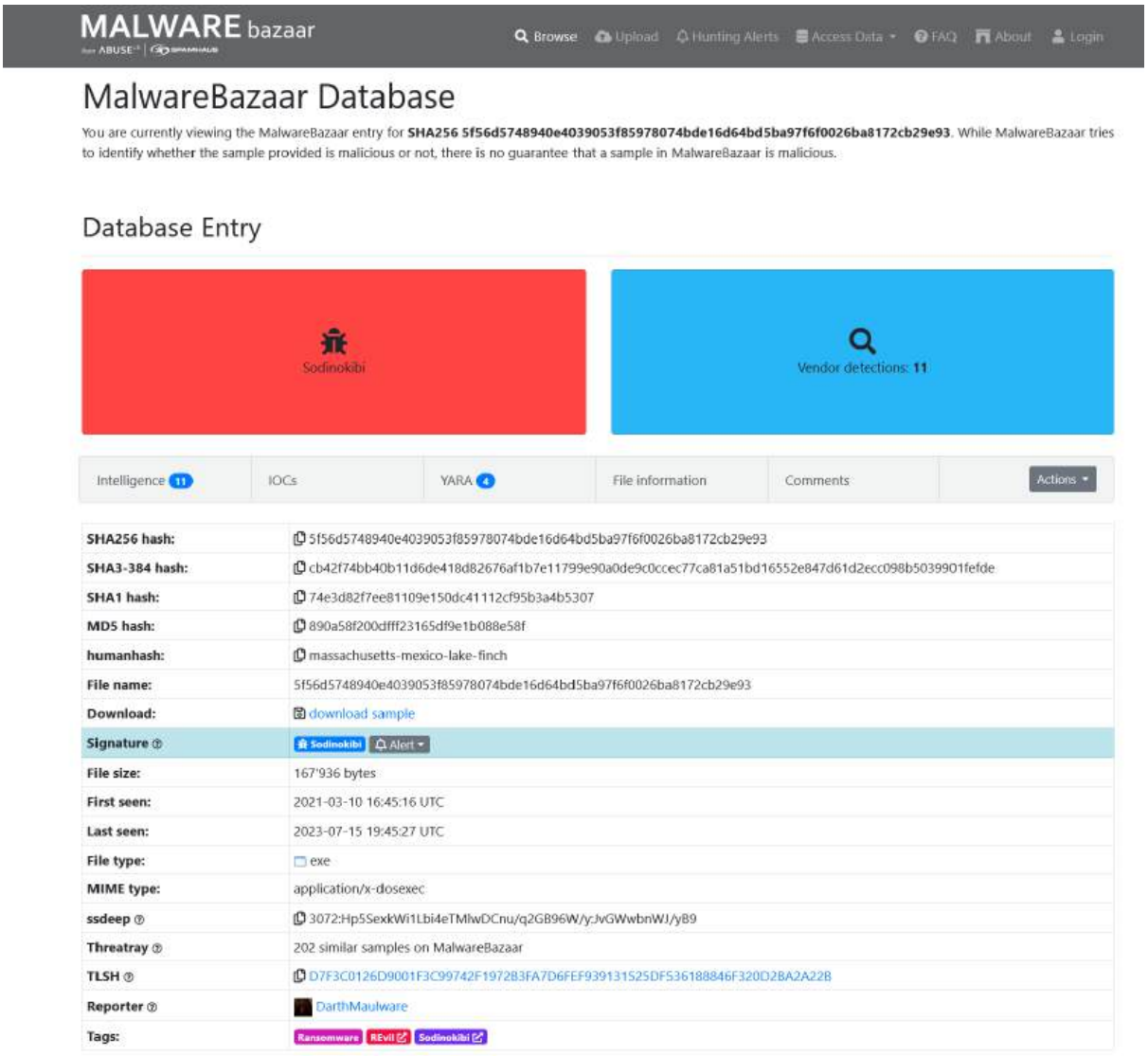
Tahap pertama adalah menyiapkan mesin virtual dengan sistem operasi Windows 10. Mesin ini menggunakan mode jaringan NAT dengan alamat IP yang diperoleh secara dinamis melalui DHCP dengan rentang 192.168.10.0. Konfigurasi ini diterapkan agar mesin korban dapat terkoneksi dengan internet untuk melakukan beberapa aktivitas dan diberikan beberapa aset berupa aplikasi serta *file* gambar yang ditambahkan secara manual, seperti yang ditunjukan pada Gambar 3.1.



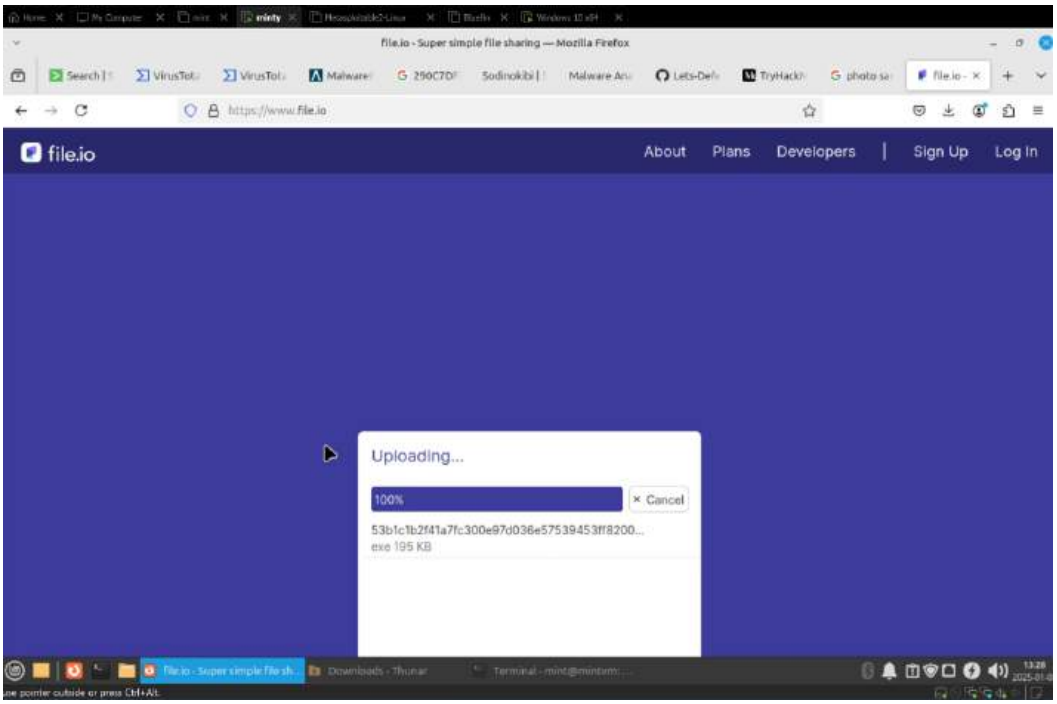
Gambar 3.1 Proses menyiapkan aset berupa *file* gambar di mesin korban

Penambahan aset ini bertujuan agar efek enkripsi dari *ransomware* dapat teridentifikasi secara visual oleh peserta pelatihan. Selain itu, sistem *antivirus* bawaan Windows secara sengaja dinonaktifkan untuk memastikan *ransomware* dapat berjalan secara *optimal* dan menimbulkan dampak maksimal pada sistem. Langkah berikutnya adalah melakukan proses infeksi *ransomware*. Skenario infeksi dirancang agar menyerupai kasus nyata, yaitu ketika pengguna secara tidak sengaja mengunduh dan mengeksekusi *file* berbahaya dari internet. Untuk mewujudkan hal ini, penulis terlebih dahulu memperoleh sampel *ransomware* Sodinokibi (REvil) dalam bentuk *file executab*le (.exe) dari platform MalwareBazaar menggunakan mesin Linux Mint. Sampel ini kemudian dinamai ulang menjadi vom.exe agar dapat diiedentifikasi saat proses investigasi. Setelah itu, file vom.exe diunggah ke layanan *file hosting* publik file.io untuk

membuat sebuah URL unduhan. Informasi *ransowmare* yang digunakan dan proses menggunggah *file ransomware* ke situs *file hosting* ini ditunjukan pada Gambar 3.2 dan Gambar 3.3.

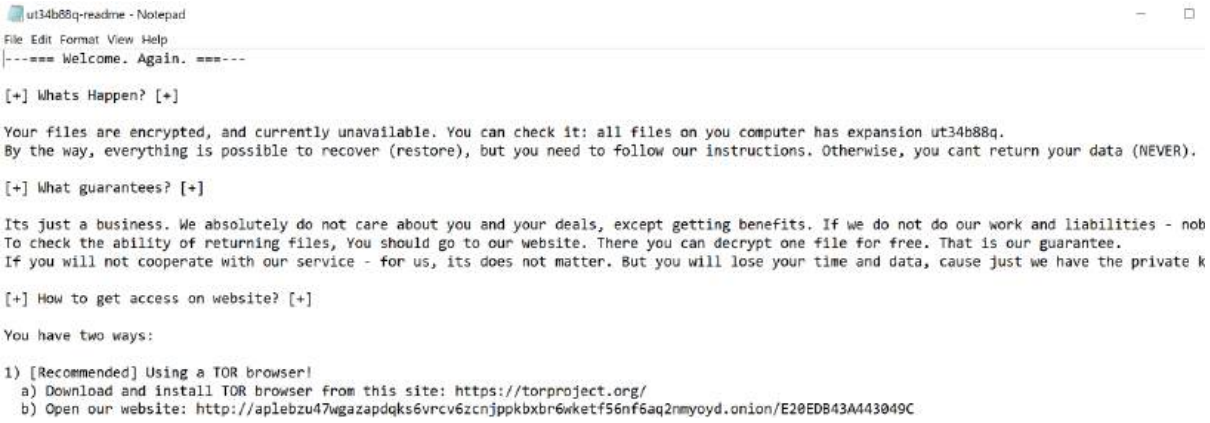


Gambar 3.2 Informasi *ransomware* yang digunakan untuk infeksi mesin korban

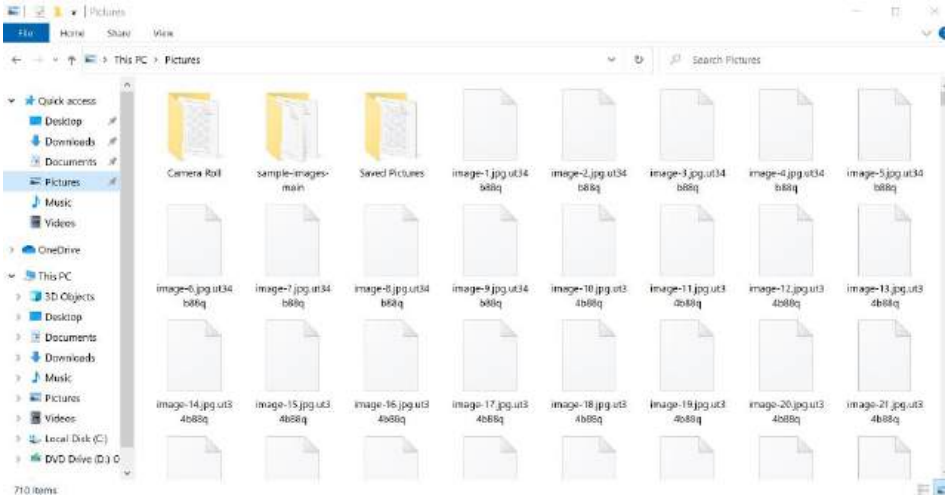


Gambar 3.3 *File ransomware* diunggah ke situs file.io

URL unduhan kemudian diakses melalui *browser* Microsoft Edge pada mesin Windows yang berperan sebagai korban. *File ransomware* diunduh dan dieksekusi secara langsung oleh pengguna. Setelah file dijalankan, sistem segera menunjukkan gejala infeksi. Gejala awal yang muncul adalah *file-file* pengguna mengalami perubahan nama dan ekstensi menjadi tidak dapat dibuka. Kondisi ini ditunjukkan secara jelas melalui tampilan *file* yang telah terenkripsi, sebagaimana diperlihatkan pada Gambar 3.4. Selanjutnya, *wallpaper desktop* secara otomatis diganti oleh sistem dengan gambar yang memuat pesan ancaman dari pelaku, seperti yang terlihat pada Gambar 3.5. Tidak hanya itu, sebuah *ransom note* turut muncul di direktori sistem untuk memberikan instruksi tebusan kepada korban, yang dapat dilihat pada Gambar 3.6. Untuk menambah kompleksitas skenario investigasi, korban dalam simulasi ini juga mengunduh serta menjalankan program *decryptor* palsu bernama decrypeeeez.exe dengan harapan dapat memulihkan *file* terenkripsi. Namun, program tersebut ternyata merupakan bagian dari keluarga *ransomware* yang sama dan tidak memberikan hasil apa pun. Tampilan dari program *decryptor* ini ditunjukkan pada Gambar 3.7, dan menjadi salah satu artefak tambahan yang dapat dianalisis oleh peserta pelatihan.

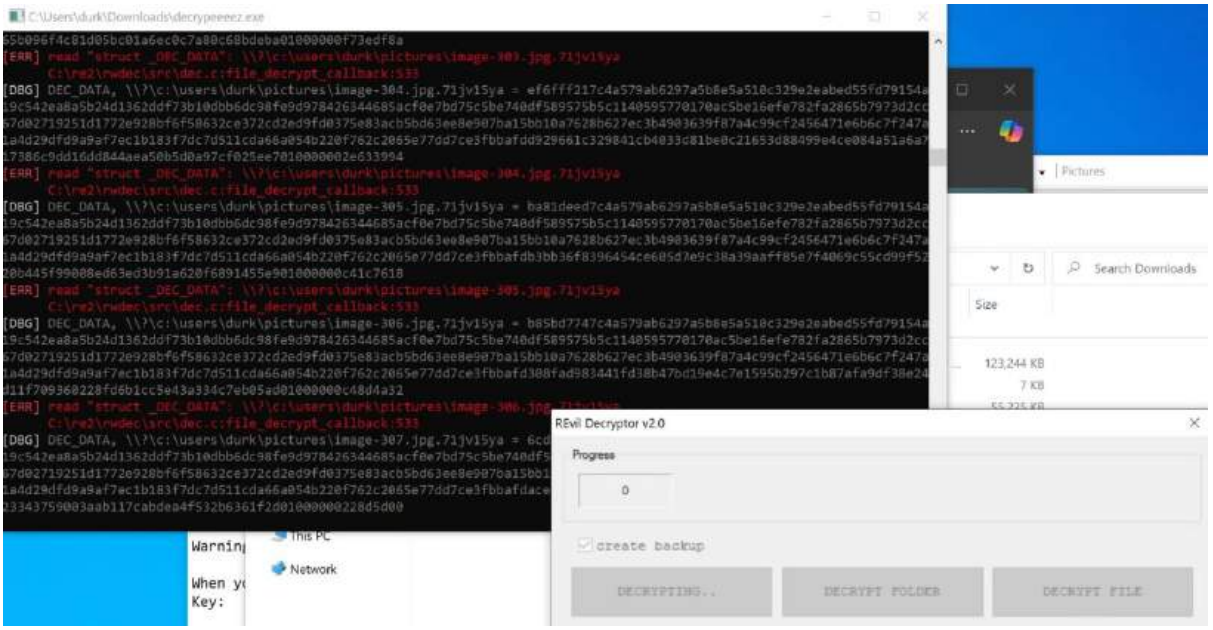


Gambar 3.4 *Ransom Note* yang ditinggalkan setelah infeksi



Gambar 3.5 *File* gambar yang telah terenkripsi

Gambar 3.6 Tampilan mesin korban setelah terinfeksi *ransomware*



Gambar 3.7 Program *decryptor* yang dijalankan di mesin korban

B. Proses *memory dump*

Setelah simulasi infeksi berhasil dilakukan, langkah selanjutnya adalah melakukan pengambilan citra memori (*memory dump*) dari mesin yang telah terinfeksi. Proses ini bertujuan untuk memperoleh seluruh data yang berada dalam memori sistem pada saat infeksi berlangsung, termasuk informasi proses, modul aktif, struktur *file* sementara, serta jejak perilaku *malware* yang tidak terekam secara permanen di *disk*. Pengambilan data memori dilakukan menggunakan perangkat lunak FireEye Redline, yaitu alat analisis forensik *endpoint* yang mampu mengoleksi dan menginterpretasi artefak sistem secara detail. Tampilan aplikasi Redline ketika dijalankan dapat dilihat pada Gambar 3.8.

Gambar 3.8 Tampilan aplikasi Redline

Dalam skenario ini, proses *memory dump* dilakukan langsung pada mesin korban, di mana aplikasi FireEye Redline diinstal dan dijalankan secara lokal. Setelah program terbuka, investigator diarahkan ke menu "Collect Data" untuk membuat *collector launcher*, yaitu skrip pengumpulan data yang dapat disesuaikan dengan kebutuhan analisis. Tampilan pilihan *collector* terlihat pada Gambar 3.8. Redline menyediakan tiga jenis *template collector*, yaitu:

1. *Standard Collector*

   Standard Collector merupakan *collector template* yang akan mengoleksi data yang diperlukan Redline, tanpa ada konfigurasi tambahan. Namun investigator bisa memodifikasi konfigurasi *collector* ini sesuai kebutuhan analisis di bagian "Edit your script".

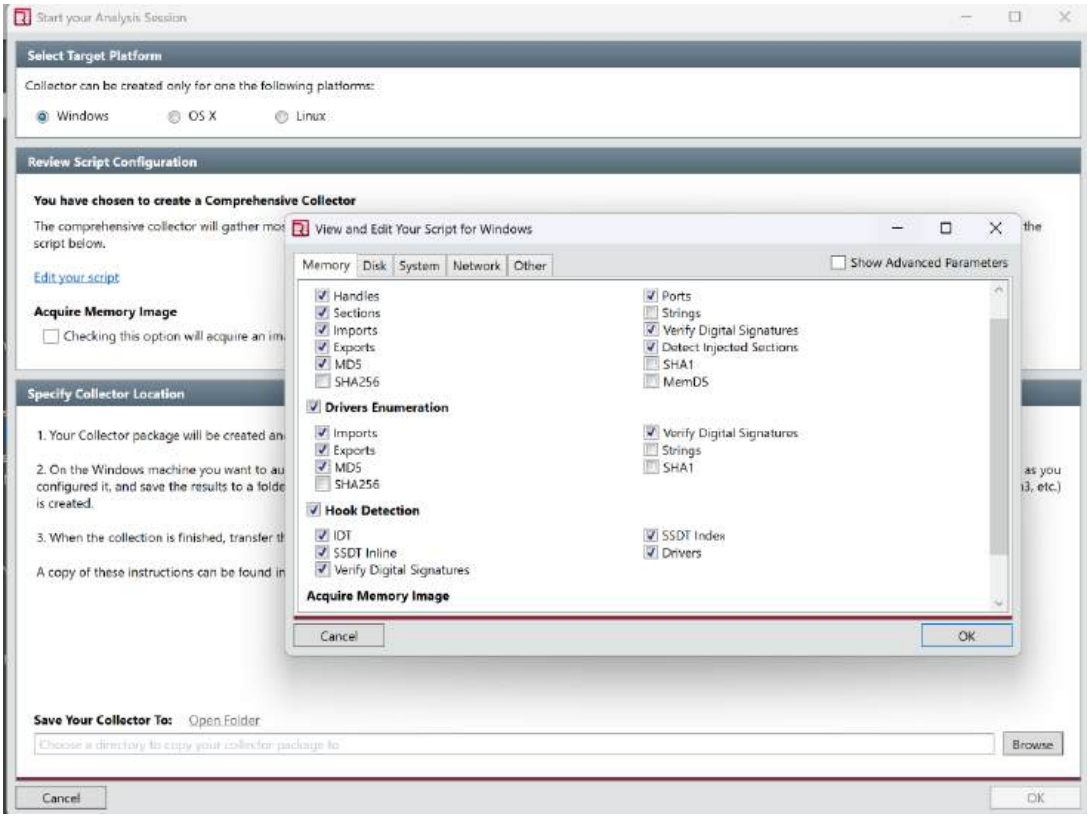
2. *Comprehensive Collector*

   Template ini sama seperti *Standard Collector*, namun menerapkan konfigurasi yang lebih banyak. Investigator tetap bisa memodifikasi konfigurasi *collector* ini sesuai kebutuhan di bagian "Edit your script".

3. *IOC Search Collector*

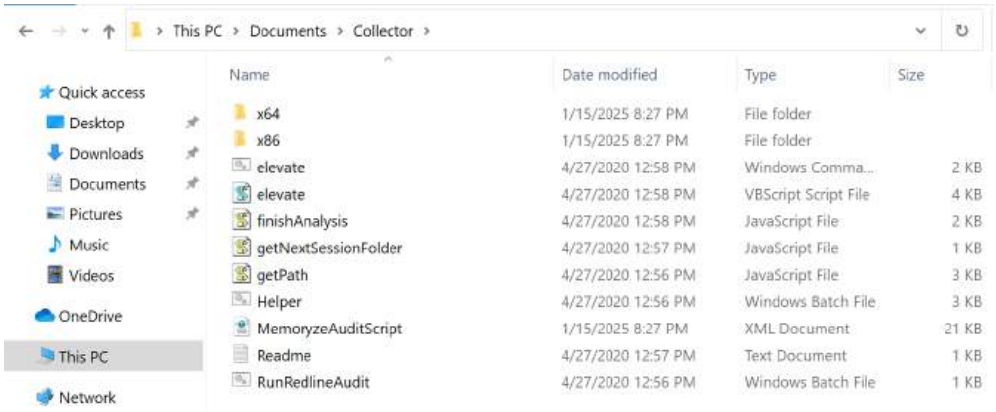
   Dirancang khusus untuk mengumpulkan data berdasarkan *Indicator of Compromise* (IOC) yang sudah diketahui sebelumnya, dan berguna dalam investigasi berbasis pola serangan tertentu.

Dalam skenario ini, investigator memilih Comprehensive Collector sebagai template dasar. Template ini tetap dapat disesuaikan melalui opsi “Edit your script” sesuai dengan kebutuhan forensik yang lebih spesifik. Seperti yang ditunjukkan pada Gambar 3.9, halaman konfigurasi juga memungkinkan investigator menentukan target platform, lokasi penyimpanan output, serta opsi tambahan lainnya.



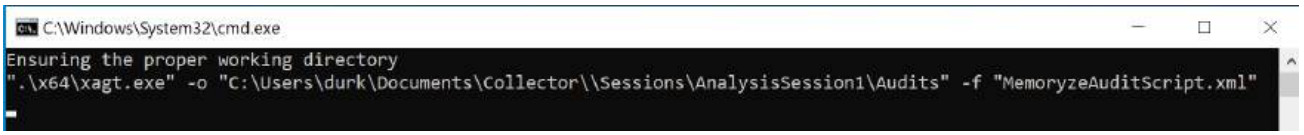
Gambar 3.9 Opsi tambahan konfigurasi *collector*

Salah satu pengaturan penting yang diaktifkan adalah “Acquire Memory Image”, yaitu fitur yang memerintahkan Redline untuk mengambil *snapshot* penuh dari memori sistem selama proses audit berlangsung. Setelah konfigurasi selesai, Redline membuat direktori *collector* di lokasi yang ditentukan seperti yang terlihat pada Gambar 3.10. *File* RunRedlineAudit.bat dieksekusi dengan mode administrator agar proses akuisisi memori berjalan maksimal dan memiliki akses penuh terhadap sistem.



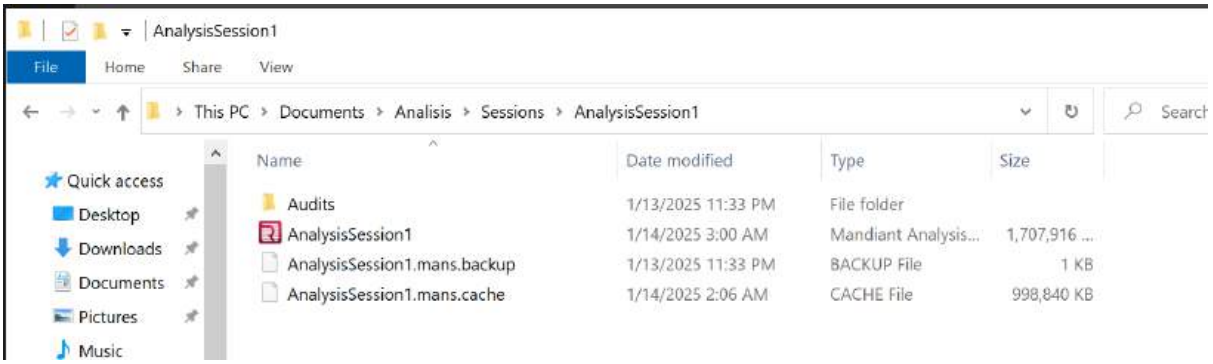
Gambar 3.10 Direktori *collector* Redline

Selama proses berlangsung, akan tampil jendela *command prompt* (cmd) sebagai indikator bahwa proses *memory dump* sedang berjalan. Proses berjalannya proses *memory dump* dapat dilihat pada Gambar 3.11.



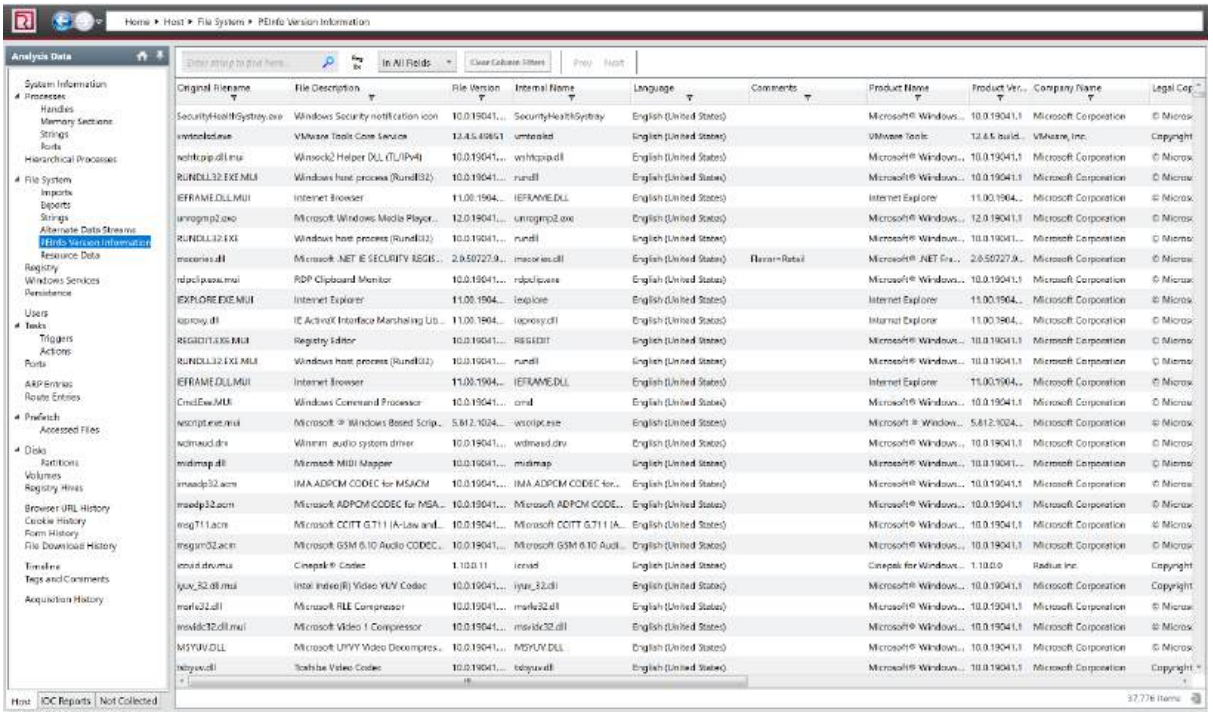
Gambar 3.11 Tampilan *command prompt* dari proses *memory dump*

Setelah proses selesai, jendela akan tertutup secara otomatis. Terilhat pada Gambar 3.12 bahwa *file* hasil *memory dump* disimpan di dalam subdirektori Session\AnalysisSession1 dengan ekstensi .mans, yaitu *file* audit utama yang digunakan dalam proses analisis selanjutnya.



Gambar 3.12 *File* hasil disimpan dalam ekstensi Mandiat Analysis

File .mans ini kemudian dipindahkan ke mesin investigator yang telah dikonfigurasi secara terpisah dan aman. Mesin ini digunakan secara eksklusif untuk menjalankan Redline dan menganalisis *memory dump* agar peserta dapat mempelajari jejak digital yang ditinggalkan oleh ransomware melalui proses forensik memori. Tampilan hasil *memory dump* dalam *file* Mandiant Analysis dapat dilihat pada Gambar 3.13.



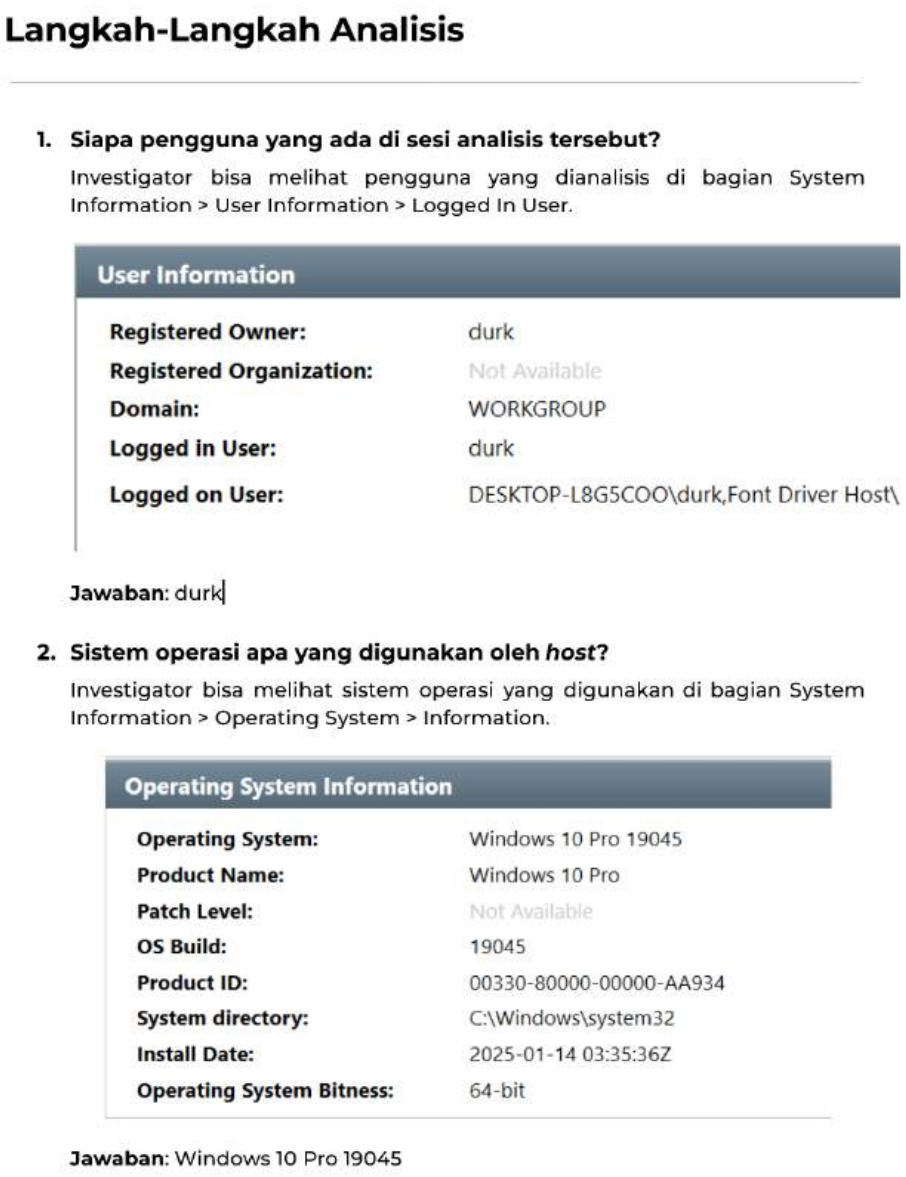
Gambar 3.13 *File* Mandiant Analysis

Pada skenario ini, *collector* langsung dijalankan dari direktori tersebut di sistem korban, tanpa menggunakan media eksternal. Metode ini tidak sepenuhnya sejalan dengan prinsip forensika digital mengenai non-kontaminasi bukti. Redline seharusnya diinstal pada sistem operasi terpisah, lalu *launcher* hasil konfigurasi dijalankan langsung dari *removable* media pada sistem target. Namun keputusan ini diambil berdasarkan pertimbangan keamanan teknis. Penulis khawatir jika mengikuti prosedur *best-practice* dari Fireye Redline yang menggunakan media eksternal seperti *flashdisk* dapat menyebabkan penyebaran *ransomware* ke *host operating system*. Namun, langkah-langkah dalam *walkthrough* tetap dituliskan berdasarkan *best-practice* dari FireEye, agar peserta memahami metode ideal yang seharusnya diterapkan dengan prinsip forensika digital. Meskipun metode ini tidak sepenuhnya sesuai dengan standar forensik digital, *supervisor* magang menyetujui keputusan tersebut untuk kepentingan simulasi. *Supervisor* juga memberikan catatan bahwa apabila materi ini akan diterapkan pada pelatihan yang sebenarnya, maka akan disediakan perangkat khusus yang memang diperuntukkan sebagai objek investigasi, guna menghindari potensi kerusakan sistem pribadi peserta pelatihan.

C. *Walkthrough*

Setelah proses *memory dump* dilakukan dan *file* hasil akuisisi dipindahkan ke mesin investigator, langkah selanjutnya adalah menyusun *walkthrough* sebagai bagian integral dari materi pelatihan. *Walkthrough* merupakan dokumen yang berfungsi sebagai panduan sistematis bagi peserta dalam menyelesaikan skenario pelatihan yang telah disiapkan. Dokumen ini dirancang agar peserta dapat memahami konteks permasalahan, menguji pemahaman teknis mereka, serta memverifikasi langkah-langkah investigasi yang dilakukan secara mandiri. *Walkthrough* ini memuat sekumpulan soal berbasis forensik memori yang disusun mengikuti alur cerita insiden. Soal-soal tersebut dirancang menggunakan pendekatan CTF, di mana peserta diminta menjawab pertanyaan berdasarkan artefak yang ditemukan dalam *memory dump*. Setiap soal diarahkan pada upaya menemukan informasi penting yang terkait dengan infeksi *ransomware*, seperti identifikasi *file* berbahaya, sumber unduhan, aktivitas sistem, perubahan ekstensi *file*, catatan tebusan, hingga perilaku jaringan dan entitas yang terasosiasi dengan *malware*.

Seperti yang terlihat pada Gambar 3.14 bahwa *walkthrough* ini tidak hanya menyajikan soal-soal, tetapi juga dilengkapi dengan jawaban dan pembahasan yang disusun secara runut. Hal ini bertujuan untuk memberikan umpan balik kepada peserta, serta memungkinkan mereka melakukan pembelajaran mandiri apabila menemui kesulitan dalam proses analisis. Selain itu, kehadiran *walkthrough* juga menjadi indikator keberhasilan dari proses pengembangan *cyber range*, karena menunjukkan bahwa skenario yang disusun dapat dijalankan dan diselesaikan secara teknis dari awal hingga akhir.



Langkah-Langkah Analisis

1. **Siapa pengguna yang ada di sesi analisis tersebut?**

   Investigator bisa melihat pengguna yang dianalisis di bagian System Information > User Information > Logged In User.

User Information	
Registered Owner:	durk
Registered Organization:	Not Available
Domain:	WORKGROUP
Logged in User:	durk
Logged on User:	DESKTOP-L8G5COO\durk,Font Driver Host\

   Jawaban: durk

2. **Sistem operasi apa yang digunakan oleh *host*?**

   Investigator bisa melihat sistem operasi yang digunakan di bagian System Information > Operating System > Information.

Operating System Information	
Operating System:	Windows 10 Pro 19045
Product Name:	Windows 10 Pro
Patch Level:	Not Available
OS Build:	19045
Product ID:	00330-80000-00000-AA934
System directory:	C:\Windows\system32
Install Date:	2025-01-14 03:35:36Z
Operating System Bitness:	64-bit

   Jawaban: Windows 10 Pro 19045

Gambar 3.14 Contoh soal yang terdapat di *walkthrough* analisis *malware*

3.2 Pengembangan *Cyber Range* Analisis Jaringan

Cyber range ini dirancang untuk memberikan pelatihan dalam melakukan analisis lalu lintas jaringan berbasis *file* PCAP. Fokus utama dari skenario ini adalah untuk melatih peserta dalam menelusuri, menginterpretasikan, dan mengidentifikasi aktivitas jaringan yang berkaitan dengan potensi serangan siber, seperti komunikasi berbahaya, transfer data mencurigakan, dan

eksploitasi terhadap layanan tertentu. Skenario ini merepresentasikan praktik yang umum dijalankan oleh *blue team* seperti SOC dan CSIRT dalam kegiatan *network forensic*.

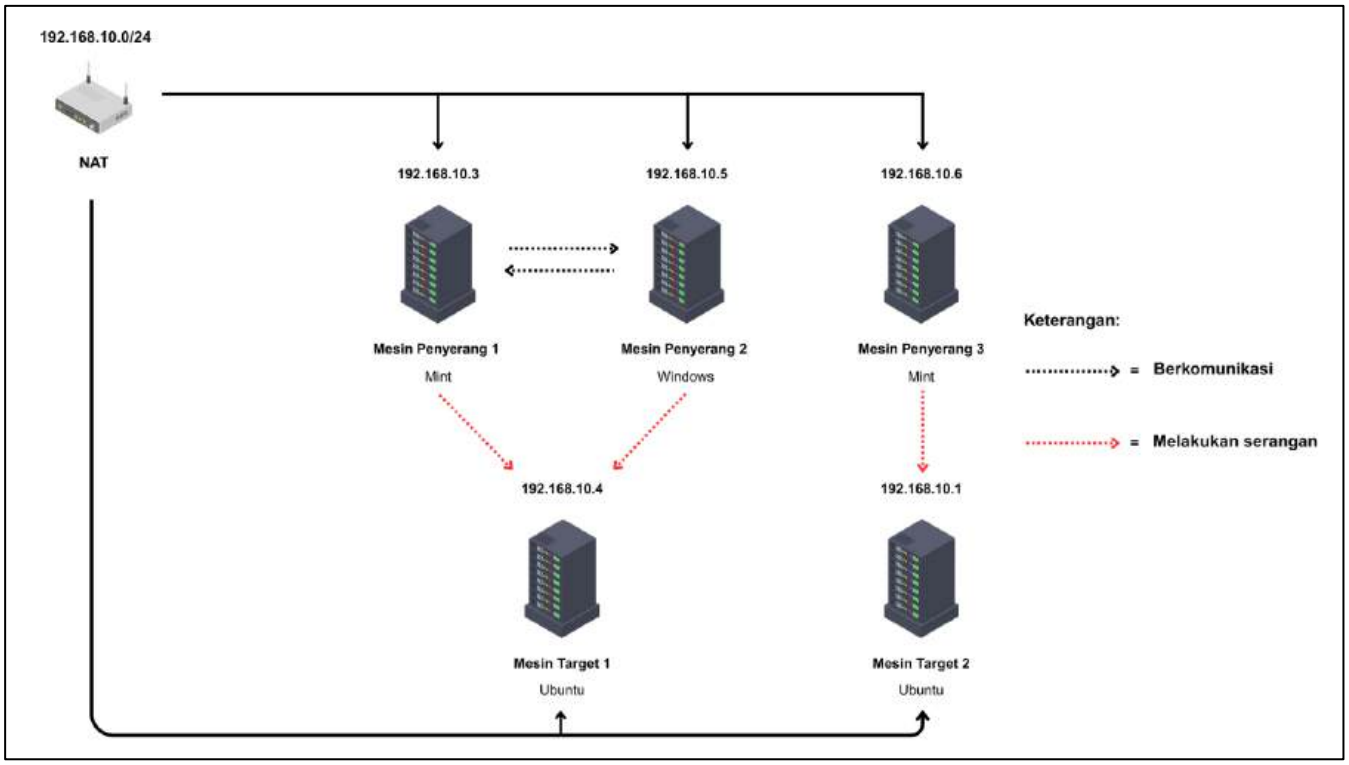
A. Perancangan Skenario

Lingkungan virtual yang digunakan dalam skenario ini terdiri atas lima mesin virtual, seperti yang disajikan pada Tabel:

Tabel 3.3 Informasi mesin yang terlibat dalam skenario analisis jaringan

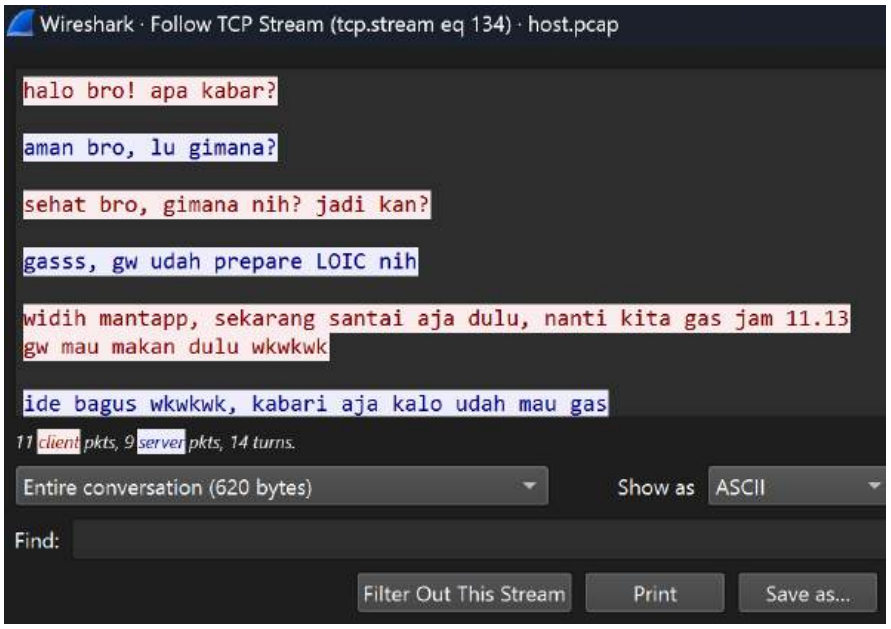
No	Mesin yang terlibat	Basis Sistem Operasi	Alamat IP	Adapter	Peruntukan
1.	Mesin Penyerang 1	Linux Mint	192.168.10.3/24	NAT	Digunakan untuk melakukan komunikasi dengan Penyerang 2 dan melakukan serangan pada mesin Target 1
2.	Mesin Penyerang 2	Windows 10	192.168.10.5/24		Digunakan untuk melakukan komunikasi dengan Penyerang 1 dan melakukan serangan pada mesin Target 2
3.	Mesin Penyerang 3	Linux Mint	192.168.10.6/24		Digunakan untuk melakukan serangan pada Target 3
4.	Mesin Target 1	Linux Ubuntu	192.168.10.4/24		Digunakan untuk target serangan Penyerang 1 dan Penyerang 2
5.	Mesin Target 2	Linux Ubuntu	192.168.10.1/24		Digunakan sebagai *server* yang menjalankan Docker Vulnlab untuk target serangan Penyerang 3

Seluruh mesin dikonfigurasi menggunakan adapter jaringan NAT dengan alokasi IP dinamis melalui DHCP dalam satu *subnet* jaringan 192.168.10.0/24. Topologi jaringan ini divisualisasikan dalam struktur yang ditunjukkan pada Gambar 3.15.

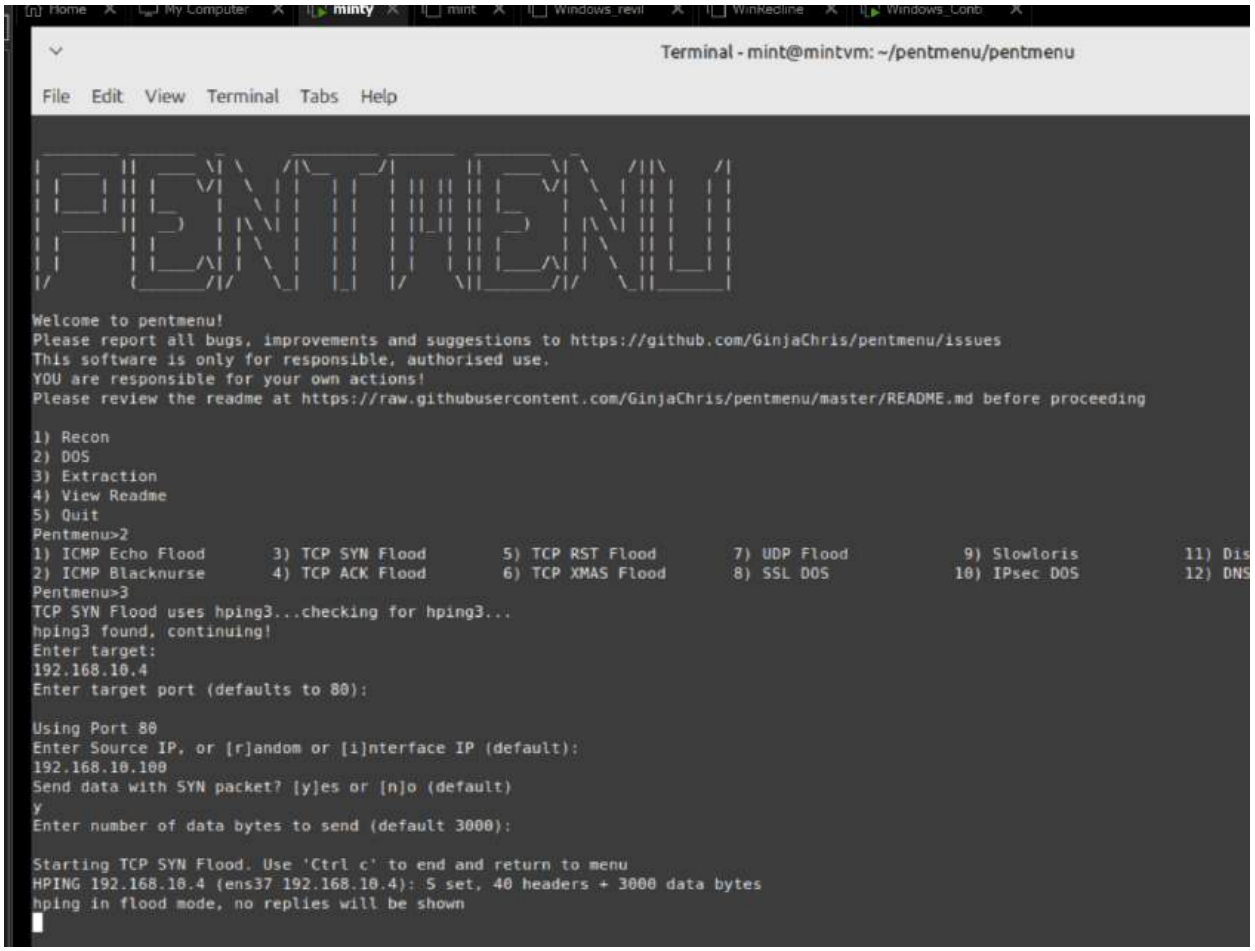


Gambar 3.15 Topologi jaringan skenario analisis jaringan

Sejak awal aktivitas, Wireshark dijalankan untuk merekam seluruh lalu lintas jaringan. Wireshark merupakan perangkat lunak *open source* yang digunakan untuk merekam dan menganalisis lalu lintas jaringan secara *real-time* maupun *offline*. Skenario dimulai dengan komunikasi teks berbasis netcat antara Penyerang 1 dan Penyerang 2 melalui *port* 12345. Tujuan dari percakapan ini adalah menciptakan trafik teks sebagai artefak jaringan awal, yang dapat diidentifikasi dan ditelusuri melalui Wireshark, seperti yang terlihat pada Gambar 3.16. Langkah berikutnya adalah menjalankan simulasi serangan *Distributed Denial of Service* (DDoS), di mana Penyerang 1 melakukan TCP SYN *flood* menggunakan alat Pentmenu dan Penyerang 2 melakukan serangan UDP *flood* dengan menggunakan alat Low Orbit Ion Cannon (LOIC). Penggunaan dari alat Pentmenu untuk melakukan serangan dapat dilihat pada Gambar 3.17.

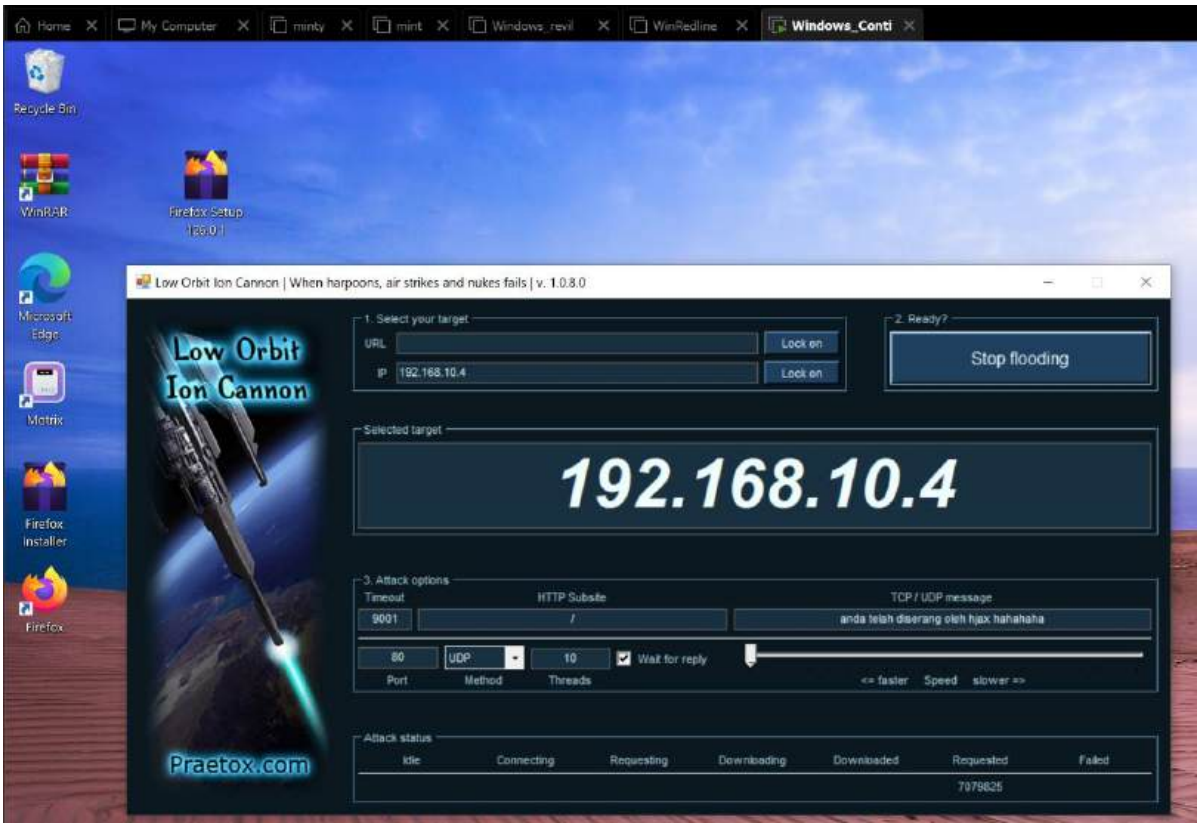


Gambar 3.16 Percakapan penyerang 1 dan penyerang 2

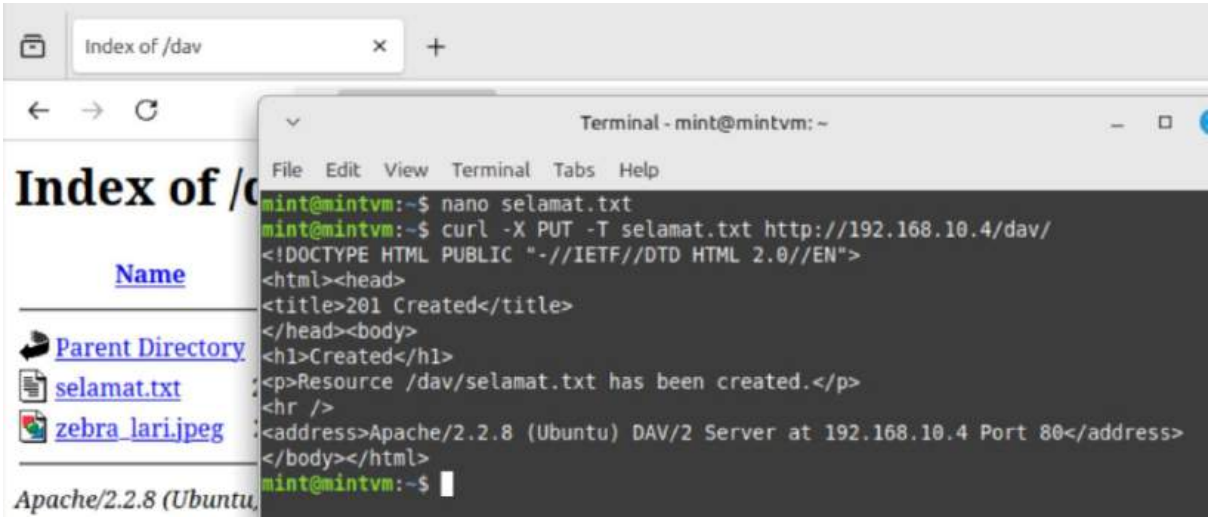


Gambar 3.17 Alat Pentmenu digunakan untuk serangan TCP SYN *flood*

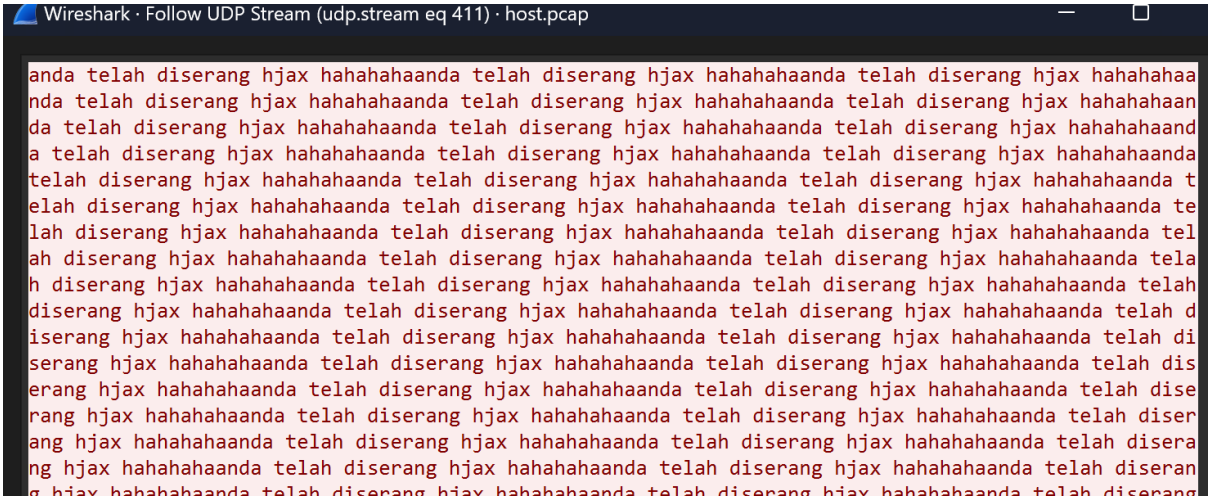
Sebelum penggunaan LOIC, *antivirus* di mesin penyerang 2 dinonaktifkan agar serangan tidak diblokir. Terlihat pada Gambar 3.18, *Payload* LOIC dikustomisasi untuk meninggalkan pesan khusus dalam lalu lintas. Setelah DDoS dilakukan, mesin Penyerang 2 mengunggah dua *file* gambar dan *file* teks ke *server* web Target 1 dengan memanfaatkan kerentanan HTTP *dangerous methods* melalui direktori /dav, seperti yang terlihat pada Gambar 3.19. Seperti yang terlihat pada Gambar 3.20, Gambar 3.21, dan Gambar 3.22, lalu lintas jaringan yang dijalankan bisa ditelusuri menggunakan Wireshark maupun NetworkMiner.



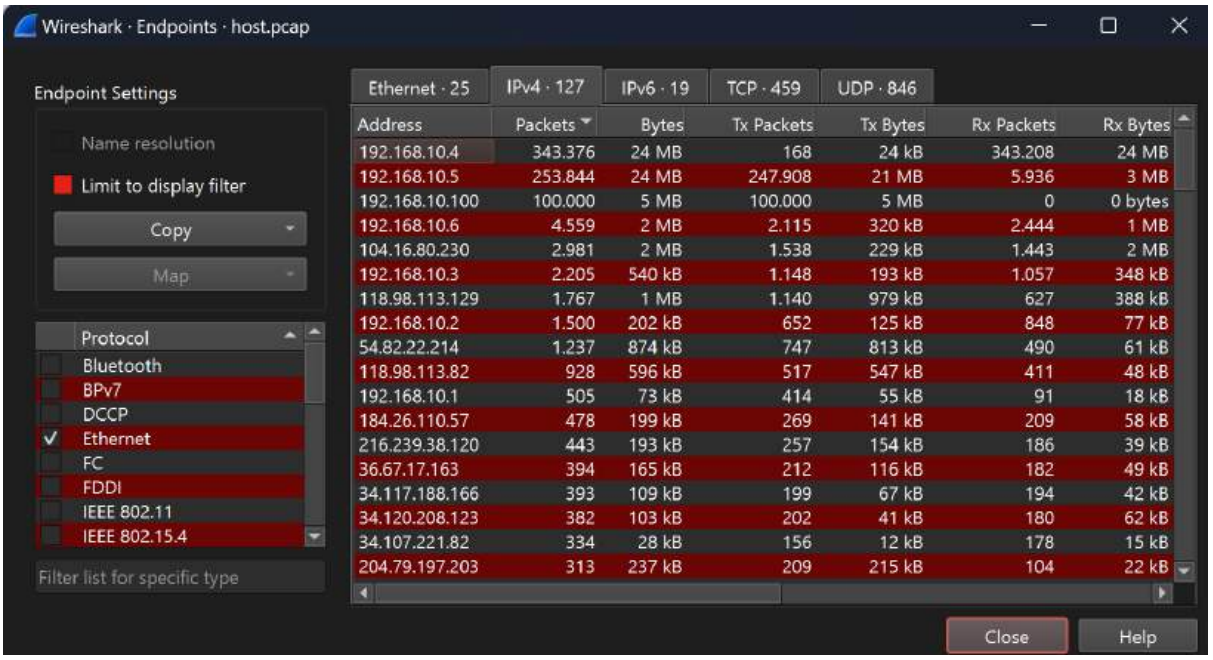
Gambar 3.18 Alat LOIC dijalankan untuk serangan UDP *flood*



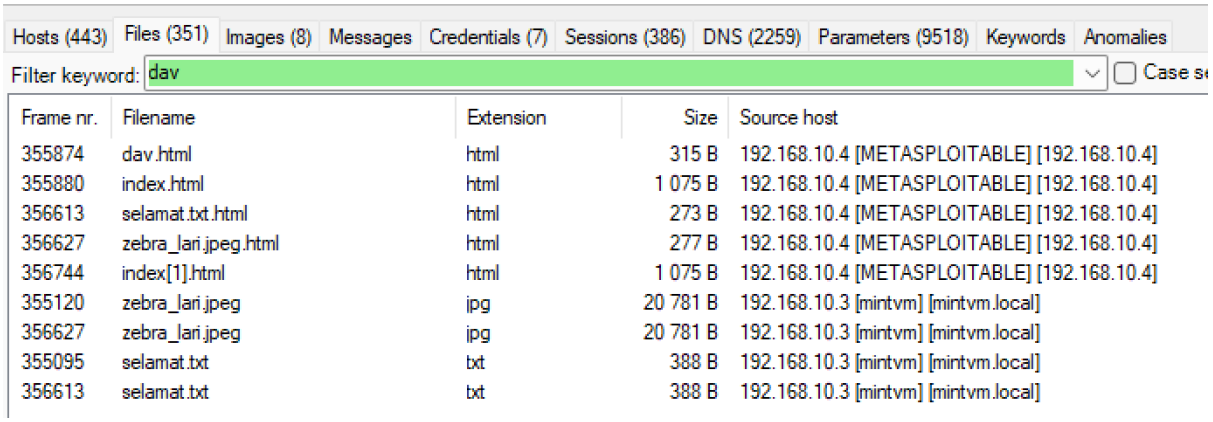
Gambar 3.20 Penyerang 2 mengunggah salah satu *file* ke direktori dav target



Gambar 3.19 Pesan yang terekam pada salah satu paket UDP serangan

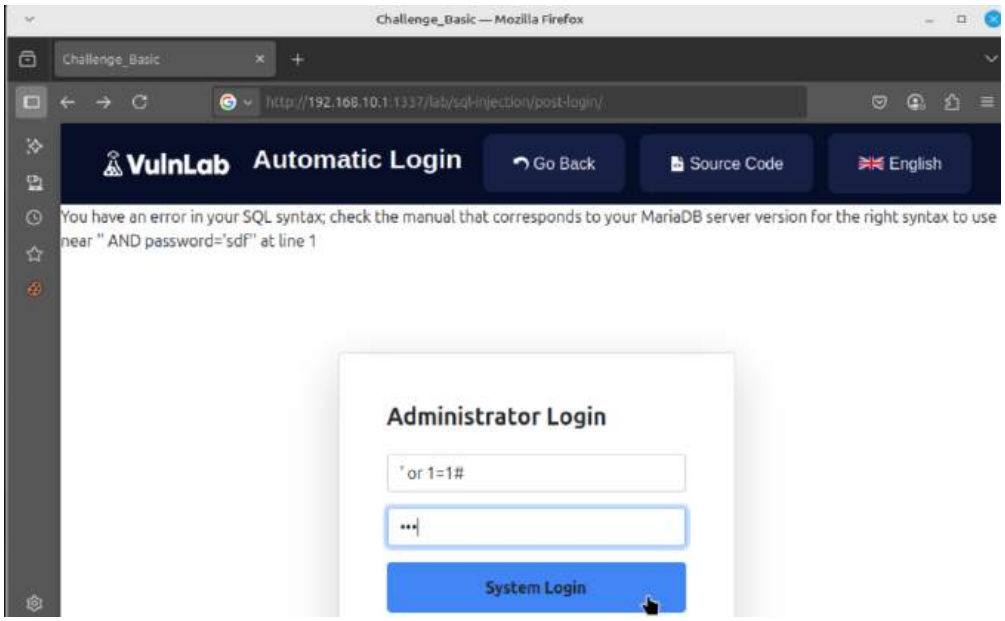


Gambar 3.22 Lalu lintas paket setiap *endpoint* yang terekam oleh Wireshark

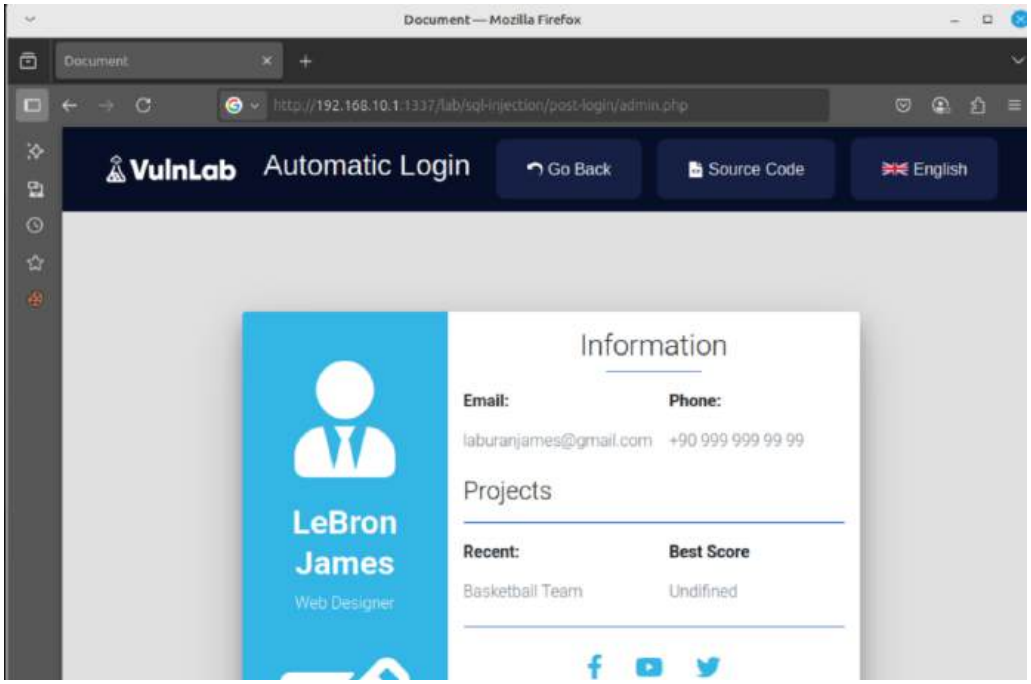


Gambar 3.21 Penelusuran *file* yang diunggah penyerang menggunakan NetworkMiner

Skenario dilanjutkan dengan Penyerang 3 yang mengakses layanan vulnlab melalui *port* 1337 dan melakukan serangan SQL *injection*, dimulai dari input karakter ' untuk memicu eror, lalu *payload* ' or 1=1# untuk memperoleh akses ilegal. Proses produksi serangan SQL *injection* tersaji dalam Gambar 3.23 dan 3.24.



Gambar 3.23 Percobaan dalam memicu eror dengan karakter ‘



Gambar 3.24 Serangan SQL *injection* berhasil melakukan *login bypass*

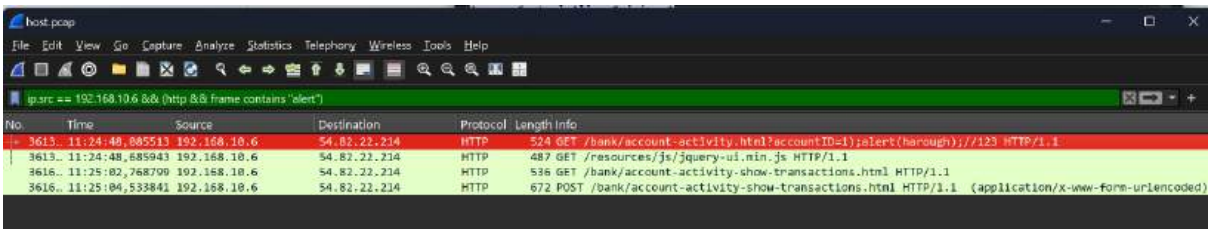
Sebagai tahap akhir, dibuat skenario dimana penyerang 3 mengakses situs web yang dikhususkan untuk latihan eksploitasi, yakni http://zero.webappsecurity[.]com dan melakukan serangan *Cross-Site Scripting* (XSS) dengan menyisipkan payload ke dalam parameter URL:

```
http://zero.webappsecurity[.]com/bank/accountactivity.html?accountID=1);alert(harough);//123.
```

Gambar 3.25 *Payload* yang digunakan untuk serangan XSS.

Terlihat pada Gambar 3.26 dan Gambar 3.27 bahwa setiap serangan yang dijalankan dapat ditelusuri menggunakan Wireshark. Seluruh lalu lintas dari simulasi di atas direkam ke dalam *file* PCAP dan PCAPNG yang kemudian disertakan sebagai bagian dari materi pelatihan.

Gambar 3.26 Penelusuran serangan SQL *injection* menggunakan Wireshark

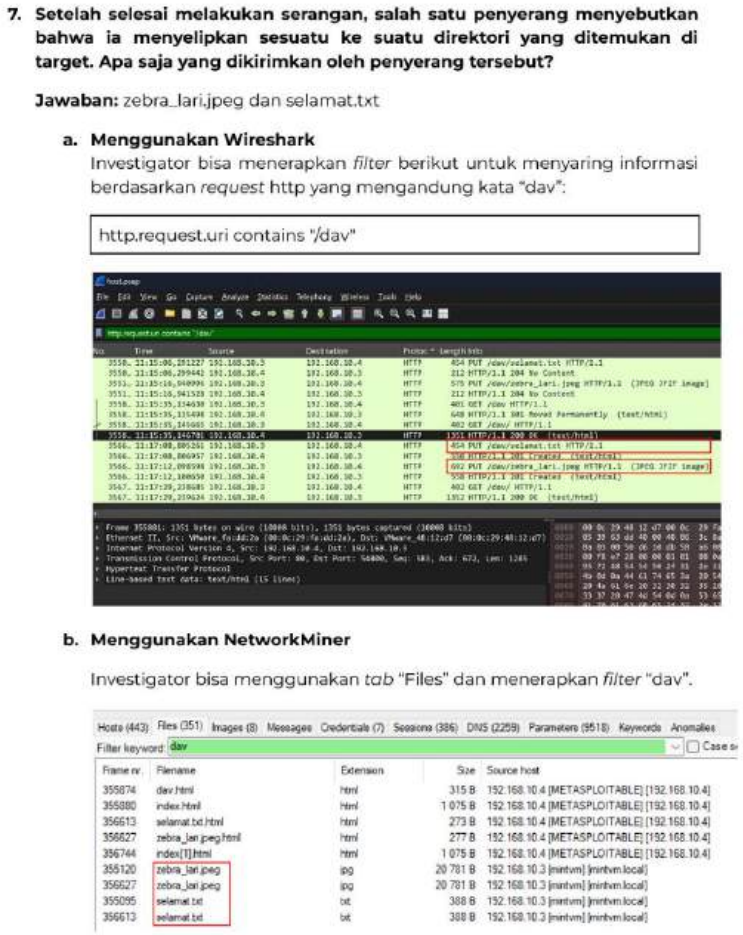


Gambar 3.27 Penelusuran serangan XSS menggunakan Wireshark

B. *Walkthrough*

Walkthrough disusun berdasarkan hasil rekaman lalu lintas jaringan dari skenario serangan yang telah dikembangkan sebelumnya. Struktur dokumen mencakup pengantar simulasi, informasi teknis mesin, alat yang digunakan, serta serangkaian soal investigasi yang disusun secara bertahap mengikuti kronologi serangan. Di bagian pembuka dokumen, terdapat penjelasan singkat mengenai apa itu *file* PCAP serta bagaimana peranannya dalam kegiatan keamanan siber, khususnya dalam proses investigasi lalu lintas jaringan. Selain itu, dijelaskan mengenai spesifikasi teknis dari mesin virtual yang digunakan dalam pelatihan, termasuk konfigurasi jaringan yang diterapkan selama simulasi. Peserta juga diperkenalkan dengan alat bantu utama seperti Wireshark dan NetworkMiner, lengkap dengan tautan rujukan untuk mempelajari cara penggunaannya secara mandiri.

Bagian inti dari *walkthrough* memuat serangkaian soal yang disusun menggunakan pendekatan CTF. Soal-soal ini dirancang untuk menguji dan mengembangkan kemampuan peserta dalam mengidentifikasi berbagai elemen penting dalam *file* PCAP, seperti alamat IP dari pelaku dan korban, jenis serangan yang terjadi, serta *payload* dari komunikasi jaringan yang terekam. Selain itu, peserta juga ditantang untuk menemukan artefak digital berupa *file* yang disisipkan atau ditransfer oleh penyerang, serta menganalisis pola komunikasi mencurigakan berdasarkan protokol atau *port* tertentu yang digunakan dalam skenario serangan. Gambar 3.28 menyajikan salah satu halaman dari *walkthrough* yang memuat soal skenario analisis jaringan.



Gambar 3.28 Contoh soal yang terdapat di *walkthrough* analisis jaringan

3.3 Evaluasi Luaran Proyek

Sebelum hasil pengembangan diserahkan, proses evaluasi dilakukan terhadap luaran proyek untuk memastikan kesesuaian antara produk yang dikembangkan dengan tujuan awal yang ditetapkan. Evaluasi ini juga bertujuan untuk menyinkronkan pemahaman terhadap alur dari setiap materi pelatihan, sehingga pihak perusahaan dapat menguasai terlebih dahulu materi yang telah disiapkan sebelum diterapkan dalam sesi pelatihan sesungguhnya. Evaluasi menackup aspek kelengkapan dan kejelasan dari keseluruhan media pelatihan yang dikembangkan, yakni *tabletop exercise* dan *cyber range*.

Evaluasi dilaksanakan dalam dua sesi, yaitu sesi pertama dilakukan secara langsung bersama *supervisor*, dan sesi keduai berpua presentasi akhir proyek yang dihadiri oleh dua penguji dari rekan kerja magang. Sesi pertama difokuskan pada validasi substansi dan kelayakan teknis materi pelatihan, sedangkan sesi kedua lebih menekankan pada aspek dokumentasi dan kelengkapan akhir. Dalam sesi evaluasi bersama *supervisor*, ditemukan beberapa bagian dari materi yang masih memerlukan penyempurnaan. Salah satu contohnya adalah pada *walkthrough* versi pertama, belum terdapat penjelasan rinci mengenai langkah-langkah pengunaan mesin investigator dan proses pengunaan FireEye Redline untuk melakukan *memory dump*. Kekurangan ini berpotensi menimbulkan kebingungan peserta saat pelatihan berlangsung, karena tahapan teknis tidak dijelaskan secara sistematis. Berdasarkan masukan tersebut, *walkthrough* kemudian direvisi dengan menambahkan bagian instruksi mengenai konfigurasi dan penggunaan FireEye Redline.

Setelah proses evaluasi bersama *supervisor* selesai dilaksanakan, presentasi akhir dilakukan untuk menguji kelengkapan dan koherensi materi, Mesikpun secara umum materi telah dinyatakan layak, terdapat beberapa catatan tambahan yang perlu diperhatikan dan disempurnakan, antara lain:

1. Pada komunikasi antara Penyerang 1 dan Penyerang 2 dalam skenario analisis jaringan, tim evaluator menanyakan alasan penggunaan *port* 12345. Penulis mengklarifikasi bahwa *port* 12345 dipilih agar memudahkan peserta dalam melakukan penelusuran selama investigasi.
2. Pada skenario analisis *malware*, belum terdapat ringkasan awal yang menjelaskan konteks insiden. Hal ini dapat menyebabkan peserta meraba-raba peristiwa yang sedang terjadi. Revisi dilakukan dengan menambahkan narasi pembuka bahwa peserta akan melakukan investigasi terhadap sebuah mesin yang diduga terdampak oleh *malware*.

3. Catatan terakhir berkaitan dengan adanya URL pada *ransom note*. Tim evaluator mempertanyakan apakah URL tersebut telah diuji untuk diakses selama pengembangan. Penulis mengklarifikasi bahwa URL tersebut telah diperiksa dan dinyatakan tidak dapat diakses.

3.4 Penyerahan Luaran Proyek

Setelah seluruh proses revisi selesai dilaksanakan dan divalidasi oleh para evaluator, seluruh luaran proyek secara resmi diserahkan kepada *supervisor*. Penyerahan ini mencaup semua komponen dari skenario pelatihan yang dikembangkan, baik *cyber range* untuk *red teami* maupun maupun *cyber range* untuk *blue team*.

Dalam skenario analisis *malware*, dua mesin virtual utama yakni mesin yang telah terinfeksi *ransomware* serta mesin investigator dikonversi terlebih dahulu ke dalam format Open Virtual Appliance (.ova). Format ini dipilih agar mesin virtual dapat diimpor dan dijalankan pada berbagai platform virtualisasi. Untuk skenario analisis jaringan, seluruh file rekaman lalu lintas yang telah disimulasikan diserahkan dalam dua format, yaitu PCAP dan PCAPNG. Selain itu, dokumen *walkthrough* dari seluruh *cyber range* juga disertakan dalam bentuk final yang telah direvisi berdasarkan masukan evaluasi. Penyerahan ini juga sekaligus menandakan bahwa pengembangan proyek telah selesai dilaksanakan.

BAB IV
REFLEKSI PELAKSANAAN MAGANG

4.1 Pemahaman sebelum Magang

Sebelum kegiatan magang dimulai, penulis memiliki ekspektasi besar untuk dapat belajar langsung dari para profesional yang telah berpengalaman di industri keamanan siber. Penulis berharap kegiatan magang dapat menjadi media pembelajaran nyata yang tidak hanya memperluas wawasan teknis, tetapi juga memberikan pemahaman tentang praktik kerja profesional di dunia industri. Harapan tersebut terbukti terpenuhi, bahkan melebihi ekspektasi awal, karena selama pelaksanaan magang penulis mendapatkan bimbingan dan arahan langsung dari *supervisor* dan rekan kerja yang memiliki keahlian tinggi dalam bidangnya. Pada awalnya, penulis mengekspektasikan bahwa pengalaman magang akan lebih berfokus pada sisi *red team*. Namun, seiring berjalannya waktu, penulis justru terlibat langsung dalam proyek-proyek yang juga mencakup sisi *blue team*, khususnya dalam pengembangan media pelatihan seperti *tabletop exercise* dan *cyber range*. Hal ini menjadi nilai tambah yang sangat berarti karena memungkinkan penulis untuk mempelajari dua perspektif utama dalam dunia keamanan siber secara terpadu. Proses pengerjaan proyek yang dijalankan secara terstruktur, dimulai dari pendekatan *red team* hingga dilanjutkan ke sisi *blue team*, membantu penulis beradaptasi dan memperoleh pemahaman menyeluruh tentang dari kedua perspektif.

Dari segi pengetahuan awal, penulis telah memiliki latar belakang akademik yang relevan sebelum memasuki dunia magang. Mata kuliah Sistem dan Jaringan Komputer yang diikuti pada semester tiga menjadi fondasi awal dalam memahami aspek teknis jaringan dan sistem informasi. Pengalaman tersebut kemudian dilanjutkan dengan pembelajaran melalui mata kuliah Forensika Digital serta Keamanan Siber dan Informasi pada semester lima, yang memberikan pemahaman dasar mengenai keamanan informasi dan proses investigasi digital. Di semester enam, penulis juga mengikuti program Studi Independen Bersertifikat Kampus Merdeka (SIBKM) dengan fokus pada keamanan siber untuk *blue team*. Seluruh pengalaman belajar ini memudahkan penulis dalam memahami materi serta beradaptasi selama pelaksanaan proyek, meskipun tetap diperlukan penyesuaian terhadap penggunaan alat baru dan eksplorasi teknik yang belum pernah dipelajari sebelumnya.

Meskipun demikian, penulis juga memiliki sejumlah kekhawatiran sebelum magang dimulai, terutama terkait budaya kerja dan kemampuan beradaptasi di lingkungan profesional. Ketidaktahuan mengenai ritme kerja, tata cara komunikasi profesional, serta ekspektasi yang

harus dipenuhi sebagai peserta magang menjadi kekhawatiran tersendiri. Namun, seiring berjalannya waktu, penulis dapat menyesuaikan diri berkat dukungan dari rekan kerja, arahan dari supervisor, serta bimbingan dari dosen pembimbing.

Pengalaman magang ini juga menjadi momen pertama bagi penulis dalam mengenal istilah seperti *cyber range* dan *tabletop exercise*, yang sebelumnya belum pernah diperoleh dari perkuliahan maupun kegiatan pelatihan. Konsep yang lebih dikenal sebelumnya adalah CTF, baik dalam bentuk kompetisi maupun platform daring yang ditujukan untuk pelatihan individu. *Cyber range* dan *tabletop exercise* cenderung jarang dibahas karena lebih umum digunakan dalam skala pelatihan *enterprise*. Oleh karena itu, keterlibatan dalam proyek pengembangan media pelatihan berbasis *cyber range* menjadi pengalaman baru yang sangat berharga, serta membuka wawasan baru tentang kebutuhan pelatihan yang lebih luas dan terstruktur di dunia profesional.

4.2 Lingkungan Kerja

Selama pelaksanaan magang, penulis menjalani sistem kerja *onsite*. Meskipun demikian, proses pengerjaan proyek juga memiliki fleksibilitas, karena beberapa tugas masih dapat diselesaikan di luar jam kerja. Dalam situasi seperti ini, komunikasi dengan *supervisor* tetap terjalin secara aktif, baik untuk menyampaikan progres maupun untuk meminta arahan teknis.

Lingkungan kerja yang ada di perusahaan sangat mendukung proses pembelajaran. Pola komunikasi yang terbentuk cenderung bersifat bimbingan langsung bersama dengan *supervisor* yang menjadi pembimbing utama selama pengerjaan proyek. Pengembangan proyek yang penulis kerjakan dibawahi langsung oleh *supervisor*, sehingga komunikasi intensif berlangsung melalui pertemuan tatap muka dan pesan melalui WhatsApp. Sementara itu, komunikasi dengan rekan kerja lainnya berlangsung dalam intensitas yang lebih terbatas. Hal ini dapat dimaklumi karena sebagian besar rekan kerja memiliki beban kerja yang kompleks dan menuntut konsentrasi tinggi. Meski begitu, rekan-rekan kerja selalu bersedia membantu ketika penulis membutuhkan bantuan, terutama dalam memahami alat atau materi baru. Percakapan di luar jam kerja, seperti saat istirahat atau makan siang, turut menciptakan suasana kerja yang akrab dan tidak kaku, menjadikan penulis merasa diterima dan didukung oleh lingkungan sekitar. *Supervisor* memiliki peran yang sangat penting dalam proses adaptasi. Selain memberikan panduan teknis, *supervisor* juga berperan dalam membentuk pola pikir dan etika kerja yang baik. Arahan yang diberikan tidak hanya terbatas pada penyelesaian tugas, tetapi juga menyentuh aspek manajemen waktu, skala prioritas, dan dokumentasi hasil kerja. Proses

evaluasi dilakukan secara rutin dan mendalam, yang pada akhirnya membantu penulis meningkatkan ketelitian dan kedisiplinan dalam setiap tahapan pengembangan proyek. Interaksi dengan rekan kerja juga mendorong penulis untuk tidak ragu bertanya maupun berdiskusi, terutama karena rekan-rekan kerja menunjukkan sikap terbuka dan sabar dalam memberikan penjelasan. Pada beberapa kesempatan, penulis juga diberi ruang untuk menyampaikan ide atau masukan dalam diskusi, yang menjadi pengalaman berharga dalam membangun kemampuan komunikasi profesional.

Salah satu nilai penting yang diperoleh penulis selama proses adaptasi adalah pentingnya ketelitian dan perhatian terhadap detail, terutama dalam pengembangan materi pelatihan seperti *tabletop exercise*. Dalam proyek tersebut, penulis belajar bahwa setiap skenario harus disusun dengan akurat sesuai dengan peran dan tanggung jawab masing-masing unit, seperti perbedaan fungsi antara CSIRT dan SOC yang sempat tertukar. Pengalaman ini memperkuat pemahaman bahwa produk yang baik tidak hanya diukur dari kelengkapan teknis, tetapi juga dari presisi dan relevansi pembahasan. Meskipun penulis merasa belum sepenuhnya mampu menyamai tingkat keterampilan dan pengalaman dari rekan kerja maupun *supervisor*, proses adaptasi yang dilalui telah menjadi fondasi penting dalam membentuk pola kerja yang lebih matang. Melalui bimbingan dan pengalaman yang diperoleh selama magang, penulis mulai menerapkan nilai-nilai positif yang berlaku di lingkungan profesional, yang kelak akan menjadi bekal penting dalam menghadapi dunia kerja yang sesungguhnya.

4.3 Perkembangan Kompetensi

Selama menjalani program magang, penulis belajar untuk mengembangkan keterampilan teknis dan keterampilan non-teknis. Dari sisi teknis, magang ini menjadi momentum pertama bagi penulis untuk mendalami proses dokumentasi teknis secara profesional, khususnya dalam menyusun *walkthrough*, soal pelatihan berbasis skenario CTF, serta panduan penggunaan alat bantu forensik. Sebelum magang, penulis belum pernah menyusun dokumen semacam ini. Tantangan awal yang dihadapi adalah ketiadaan struktur maupun acuan untuk menyusun *walkthrough*, sehingga penulis mencari referensi dari penyelesaian CTF. Dukungan dan masukan dari *supervisor* sangat membantu dalam merumuskan format dokumentasi yang lebih sistematis dan mudah dipahami. Salah satu pencapaian yang paling memuaskan bagi penulis adalah keberhasilan dalam menyelesaikan proyek pengembangan *cyber range*, baik untuk *red team* maupun *blue team*. Dalam proyek ini, penulis memperoleh pengalaman langsung dalam mengonfigurasi mesin virtual, menjalankan pengujian penetrasi, menjalankan proses infeksi

ransomware, serta melakukan proses *memory dump* menggunakan FireEye Redline. Penulis juga mempelajari berbagai alat baru seperti NetworkMiner, Pentmenu, dan tentu saja Wireshark, yang digunakan dalam proses analisis jaringan terhadap data PCAP.

Di sisi lain, kompetensi non-teknis juga berkembang dalam aspek kemampuan komunikasi profesional, baik secara lisan maupun tertulis, menjadi salah satu aspek yang diperoleh dari lingkungan kerja yang sangat mendukung. Berbeda dengan lingkungan akademik, komunikasi di dunia kerja mengedepankan kejelasan, efisiensi, dan struktur dalam penyampaian informasi. Penulis belajar untuk berinteraksi secara efektif dengan *supervisor* maupun rekan kerja, serta mampu menerima dan menindaklanjuti masukan secara konstruktif. Keterampilan *problem solving* juga menjadi bagian penting yang diasah selama magang. Dalam proyek pengembangan, sebagian besar proses perancangan alur dan struktur materi pelatihan berada di tangan penulis. Ini menuntut kemampuan berpikir sistematis serta inisiatif tinggi untuk memecahkan tantangan teknis maupun non-teknis yang muncul selama pengerjaan. Selain itu, proses evaluasi dari *supervisor* turut membentuk mentalitas kerja yang lebih tangguh, berperan dalam memberikan pengaruh besar terhadap pola kerja penulis. Setiap tantangan teknis yang sebelumnya tidak dikuasai justru menjadi kesempatan belajar yang bermakna. Penulis menyadari bahwa proses belajar dari ketidaktahuan adalah bagian penting dalam mengembangkan pribadi yang profesional.

4.4 Kontribusi terhadap Perusahaan

Kontribusi utama yang diberikan selama program magang adalah dalam bentuk pengembangan dua jenis materi pelatihan keamanan siber, yaitu *tabletop exercise* dan *cyber range*. Kedua materi ini menjadi bagian penting dalam proyek pengembangan pelatihan keamanan siber berbasis skenario yang dilaksanakan oleh perusahaan. Seluruh proses pengembangan dilakukan secara terstruktur dan berorientasi pada hasil, dengan melibatkan berbagai tahapan mulai dari riset, desain, pengujian, dokumentasi teknis, hingga evaluasi.

Dalam proyek *tabletop exercise*, kontribusi yang diberikan mencakup penyusunan skenario insiden siber berbasis referensi dari CISA Tabletop Exercise Package dan NIST 800-84, penyusunan dokumen-dokumen pendukung seperti *After-Action Report*, *Participant Guide, Logistic Checklist*, hingga *Brief Slide Deck*. Materi ini dirancang agar sesuai dengan kebutuhan pelatihan lintas divisi, dengan melibatkan berbagai peran seperti SOC, CSIRT, legal, dan tim manajemen.

Adapun kontribusi pada pengembangan *cyber range* melibatkan proses yang lebih kompleks secara teknis, karena memerlukan konfigurasi mesin virtual, desain alur serangan, perekaman lalu lintas jaringan, dan pembuatan soal berbasis CTF. Terdapat tiga *cyber range* yang dikembangkan Metasploitable *pentest*, Analisis *malware* menggunakan FireEye Redline, dan Analisis File PCAP. Secara khusus, pengembangan *cyber range* untuk *blue team* menjadi kontribusi yang paling signifikan. Kedua skenario *blue team* tersebut (analisis *malware* dan analisis jaringan) dikerjakan sebagai upaya untuk mengisi kekosongan materi praktik *blue team* yang selama ini belum banyak tersedia. Dalam pelaksanaannya, *cyber range* ini dirancang sebagai aset *reusable* yang dapat dimanfaatkan untuk pelatihan keamanan siber di sektor perbankan umum sesuai dengan segmen klien perusahaan.

Kontribusi lain yang diberikan penulis adalah dalam bentuk penyusunan pedoman materi pelatihan, yang dapat digunakan kembali oleh perusahaan dalam sesi pelatihan berikutnya. Penulis juga terlibat dalam proses evaluasi dan perbaikan materi berdasarkan masukan dari supervisor dan penguji. Revisi yang dilakukan mencakup penambahan deskripsi latar belakang serangan, pelengkapan langkah-langkah investigasi, dan penyempurnaan validitas soal pelatihan. Seluruh aset proyek, termasuk *file* mesin virtual dalam format OVA, *file* PCAP, serta dokumentasi pelatihan, telah diserahkan kepada perusahaan dan telah divalidasi sebagai materi yang layak digunakan.

BAB V
PENUTUP

5.1 Kesimpulan

Pengembangan *cyber range* dalam kegiatan magang ini difokuskan pada dua skenario utama, yaitu analisis malware menggunakan FireEye Redline dan analisis lalu lintas jaringan menggunakan *file* PCAP. Kedua skenario tersebut dirancang sebagai media pelatihan berbasis simulasi untuk meningkatkan keterampilan teknis dalam bidang keamanan siber, khususnya pada domain *blue team*. Seluruh proses pengembangan dilakukan secara bertahap, mulai dari perancangan skenario, pengumpulan data simulasi, konfigurasi mesin virtual, hingga penyusunan soal dan *walkthrough*.

Pada skenario analisis *malware*, *cyber range* dibangun dengan pendekatan simulasi sistem Windows yang telah terinfeksi *ransomware*. Peserta diarahkan untuk melakukan investigasi artefak melalui proses *memory dump* yang kemudian dianalisis menggunakan FireEye Redline. Proses ini mencakup identifikasi temuan artefak. *Walkthrough* yang disusun mendukung peserta dalam memahami tahapan forensik digital. Sementara itu, pada skenario analisis jaringan, pengembangan dilakukan dengan merancang alur serangan berbasis komunikasi jaringan, seperti DDoS, SQL *injection*, dan XSS. Lalu lintas jaringan yang dihasilkan direkam menggunakan Wireshark dan disimpan dalam format PCAP serta PCAPNG. Materi pelatihan ini memungkinkan peserta untuk menelusuri jejak serangan melalui protokol jaringan, *payload*, dan komunikasi antar *host*, menggunakan alat bantu seperti Wireshark dan NetworkMiner. Soal investigasi disusun dengan pendekatan CTF dan dilengkapi dengan pembahasan untuk mendukung proses belajar mandiri.

Kedua *cyber range* tersebut telah melalui proses evaluasi internal, direvisi berdasarkan masukan *supervisor* dan penguji, serta diserahkan sebagai aset pelatihan yang dapat digunakan ulang oleh perusahaan. Dengan selesainya kegiatan magang ini, penulis merasa lebih siap secara teknis maupun mental untuk menghadapi tantangan dunia kerja profesional di bidang keamanan siber. Magang ini tidak hanya memperkuat fondasi pengetahuan, tetapi juga memberikan perspektif yang lebih luas mengenai pentingnya sinergi antara *red team* dan *blue team* dalam membangun sistem pertahanan siber yang kuat.

5.2 Saran

Berdasarkan pengalaman yang diperoleh selama pelaksanaan magang, penulis menyampaikan beberapa saran yang diharapkan dapat bermanfaat bagi pihak-pihak terkait. Bagi mahasiswa yang akan mengikuti program magang, disarankan untuk mempersiapkan diri tidak hanya dari aspek teknis, tetapi juga dari sisi non-teknis seperti kemampuan komunikasi, adaptasi terhadap lingkungan kerja, serta keterampilan menyusun dokumentasi yang baik. Pemahaman dasar terkait proyek dan kemauan untuk belajar secara mandiri akan sangat membantu dalam menghadapi tantangan proyek yang kompleks dan dinamis. Bagi pihak program studi Informatika Universitas Islam Indonesia, diharapkan program magang dapat terus dikembangkan dan diperkuat melalui kerja sama strategis dengan industri. Penambahan materi pembekalan sebelum magang, seperti komunikasi profesional, etika kerja, serta praktik penulisan teknis, dapat menjadi bekal yang penting bagi mahasiswa sebelum terjun ke dunia kerja. Hal ini akan meningkatkan kesiapan dan kepercayaan diri mahasiswa dalam melaksanakan tugas magangnya.

Sementara itu, bagi pihak Aditasi penulis sangat mengapresiasi kesempatan dan kepercayaan yang telah diberikan selama kegiatan berlangsung. Bimbingan dan arahan dari supervisor serta lingkungan kerja yang suportif sangat membantu dalam proses pengembangan kompetensi penulis. Penulis berharap hasil proyek yang telah diserahkan dapat memberikan manfaat nyata dalam pelatihan keamanan siber perusahaan. Penulis juga berharap program magang ini dapat terus dipertahankan dan ditingkatkan, agar semakin banyak mahasiswa yang dapat memperoleh pengalaman belajar langsung dari para profesional di industri keamanan siber.

DAFTAR PUSTAKA

Aji, M. P. (2023). Sistem Keamanan Siber dan Kedaulatan Data di Indonesia dalam Perspektif Ekonomi Politik (Studi Kasus Perlindungan Data Pribadi) [Cyber Security System and Data Sovereignty in Indonesia in Political Economic Perspective]. *Jurnal Politica Dinamika Masalah Politik Dalam Negeri dan Hubungan Internasional*, *13*(2), Article 2. https://doi.org/10.22212/jp.v13i2.3299

Al-Hawamleh, A. (2023). Predictions of Cybersecurity Experts on Future Cyber-Attacks and Related Cybersecurity Measures. *International Journal of Advanced Computer Science and Applications*, *14*, 2023. https://doi.org/10.14569/IJACSA.2023.0140292

Alothman, B., Alhajraf, A., Alajmi, R., Al Farraj, R., Alshareef, N., & Khan, M. (2022). Developing a Cyber Incident Exercises Model to Educate Security Teams. *Multidisciplinary Digital Publishing Institute (MDPI)*, *11*. https://doi.org/10.3390/electronics11101575

Beauchamp, C. L. (2022). *Exploring Cyber Ranges in Cybersecurity Education*. http://hdl.handle.net/10919/109524

Burley, D. L., Eisenberg, J., & Goodman, S. E. (2014). Would cybersecurity professionalization help address the cybersecurity crisis? *Commun. ACM*, *57*(2), 24–27. https://doi.org/10.1145/2556936

Cains, M. G. (2021). Defining Cyber Security and Cyber Security Risk within a Multidisciplinary Context using Expert Elicitation. *ResearchGate*. https://doi.org/10.1111/risa.13687

Carey, M. J., & Jin, J. (2020a). Tribe of Hackers Blue Team Tribal Knowledge from the Best in Defensive Cybersecurity || Chris Sistrunk. In *Tribe of Hackers Blue Team* (pp. 274–279). John Wiley & Sons, Ltd. https://doi.org/10.1002/9781119643432.ch45

Carey, M. J., & Jin, J. (2020b). Tribe of Hackers Blue Team: Tribal Knowledge from the Best in Defensive Cybersecurity || Tanya Janca. In *Tribe of Hackers Blue Team* (pp. 113–118). John Wiley & Sons, Ltd. https://doi.org/10.1002/9781119643432.ch18

Cawthra, J., Ekstrom, M., Sexton, J., Sweetnam, J., & Townsend, A. (2020). *NIST SP 1800-26*. https://www.nccoe.nist.gov/publication/1800-26/VolA/index.html

Chng, B., Ng, B., Roomi, M. M., Mashima, D., & Lou, X. (2024). CRaaS: Cloud-based Smart Grid Cyber Range for Scalable Cybersecurity Experiments and Training. *2024 IEEE International Conference on Communications, Control, and Computing Technologies for*

Smart Grids (SmartGridComm), 333–339. https://doi.org/10.1109/SmartGridComm60555.2024.10738051

CISA. (2021, February 1). *What is Cybersecurity?* https://www.cisa.gov/news-events/news/what-cybersecurity

CSIRT Banten. (2022). *RI Dihantam 700 Juta Serangan Siber di 2022, Modus Pemerasan Dominan*. https://csirt.bantenprov.go.id/portal/articles/read/ri-dihantam-700-juta-serangan-siber-di-2022-modus-pemerasan-dominan

Dasgupta, D., Ferebee, D. M., & Michalewicz, Z. (2013). Applying Puzzle-Based Learning to Cyber-Security Education. *Proceedings of the 2013 on InfoSecCD '13: Information Security Curriculum Development Conference*, 20–26. https://doi.org/10.1145/2528908.2528910

EBSCO. (2024). *Confidentiality, integrity and availability (CIA triad)*. https://www.ebsco.com/research-starters/information-technology/confidentiality-integrity-and-availability-cia-triad

European Union Agency For Cybersecurity (ENISIA). (2025). *Skills and competences*. https://www.enisa.europa.eu/topics/skills-and-competences

Hofbauer, J. (2024). (PDF) Blue Team Fundamentals: Roles and Tools in a Security Operations Center. *ResearchGate*. https://www.researchgate.net/publication/385514927_Blue_Team_Fundamentals_Roles_and_Tools_in_a_Security_Operations_Center

Horcher, A.-M. (2020). Shall We Play a Game? : Building Capture the Flag Games for Non-Traditional Players. *2020 Research on Equity and Sustained Participation in Engineering, Computing, and Technology (RESPECT)*, *1*, 1–2. https://doi.org/10.1109/RESPECT49803.2020.9272410

Jelo, M., & Helebrandt, P. (2022). Gamification of cyber ranges in cybersecurity education. *2022 20th International Conference on Emerging eLearning Technologies and Applications (ICETA)*, 280–285. https://doi.org/10.1109/ICETA57911.2022.9974714

Kotwani, B. (2023). Red Teaming vs. Blue Teaming: A Comparative Analysis of CyberSecurity Strategies in the Digital Battlefield. *International Journal of Scientific Research in Engineering and Management (IJSREM)*. http://dx.doi.org/10.55041/IJSREM27675

Lee, B. T. F., Kornphetcharat, K., Sims, J., Đinh, L., & Ali, S. (2025). ASEAN Cybersecurity Cooperation Strategy: Combating Cyber Terrorism and Hackers Through CERT Coordination. *International Journal of Law and Public Policy (IJLAPP)*, *7*, 20–30. https://doi.org/10.36079/lamintang.ijlapp-0701.788

Macnish, K., & van der Ham, J. (2020). Ethics in cybersecurity research and practice. *Technology in Society*, *63*, 101382. https://doi.org/10.1016/j.techsoc.2020.101382

Mallick, M. A. I., & Nath, R. (2024). Navigating the Cyber security Landscape: A Comprehensive Review of Cyber-Attacks, Emerging Trends, and Recent Developments. *World Scientific News*. https://www.researchgate.net/publication/378343830_Navigating_the_Cyber_security_Landscape_A_Comprehensive_Review_of_Cyber-Attacks_Emerging_Trends_and_Recent_Developments

Narsimha, B., Raghavendran, C. V., Rajyalakshmi, P., Reddy, G. K., Bhargavi, M., & Naresh, P. (2022). Cyber Defense in the Age of Artificial Intelligence and Machine Learning for Financial Fraud Detection Application. *International Journal of Electrical and Electronics Research*, *10*(2), 87–92. https://doi.org/10.37391/ijeer.100206

Ophie. (2023). *Hack The Box report reveals the most in-demand defensive cybersecurity skills*. Hack The Box. https://www.hackthebox.com/blog/htb-report-on-360-upskilling

paralegal. (2023). *Pengertian Strategi Keamanan Siber Nasional menurut Undang-Undang*. https://paralegal.id/pengertian/strategi-keamanan-siber-nasional/

Stock, J., Teo, J., Gurnani, C. P., & Lee, R. M. (2022). *Global Cybersecurity Outlook 2022* [Podcast]. https://www.weforum.org/podcasts/agenda-dialogues/episodes/global-cybersecurity-outlook-2022/

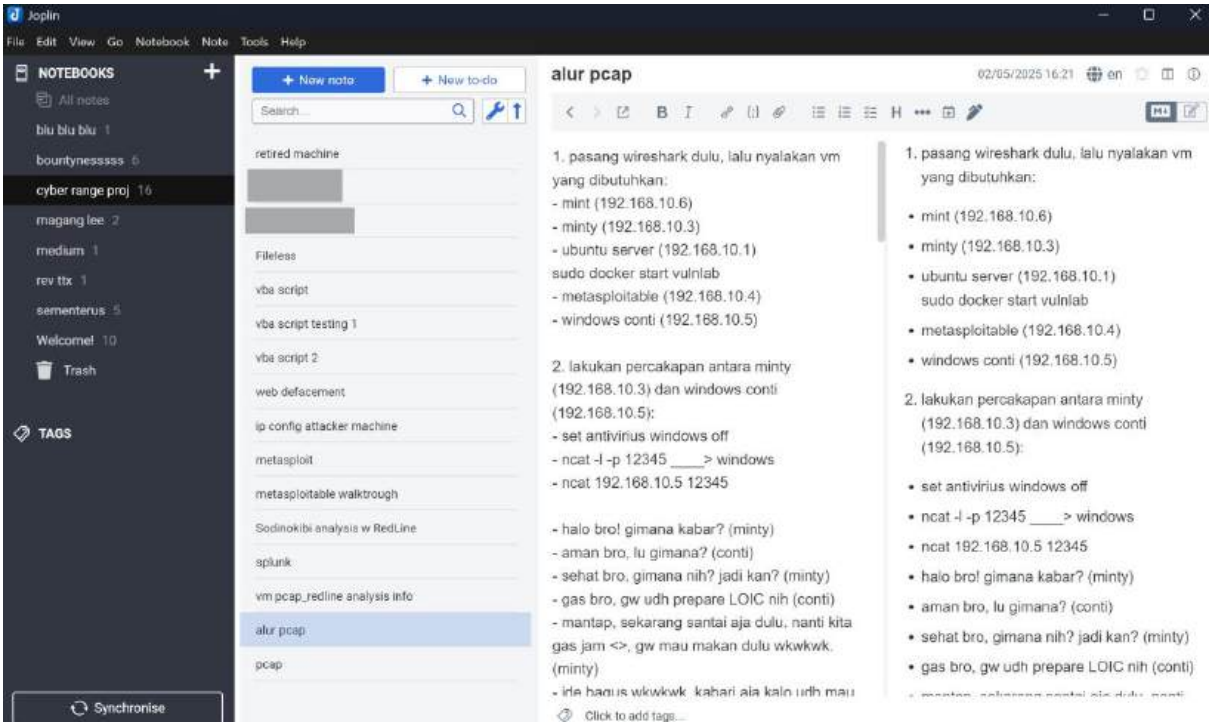
Švábenský, V., Čeleda, P., Vykopal, J., & Brišáková, S. (2021). Cybersecurity knowledge and skills taught in capture the flag challenges. *Computers & Security*, *102*, 102154. https://doi.org/10.1016/j.cose.2020.102154

Vykopal, J., & Ošlejšek, R. (2017). KYPO Cyber Range: Design and Use Cases. *International Conference - Software Technologies ICSOFT*. https://doi.org/10.5220/0006428203100321

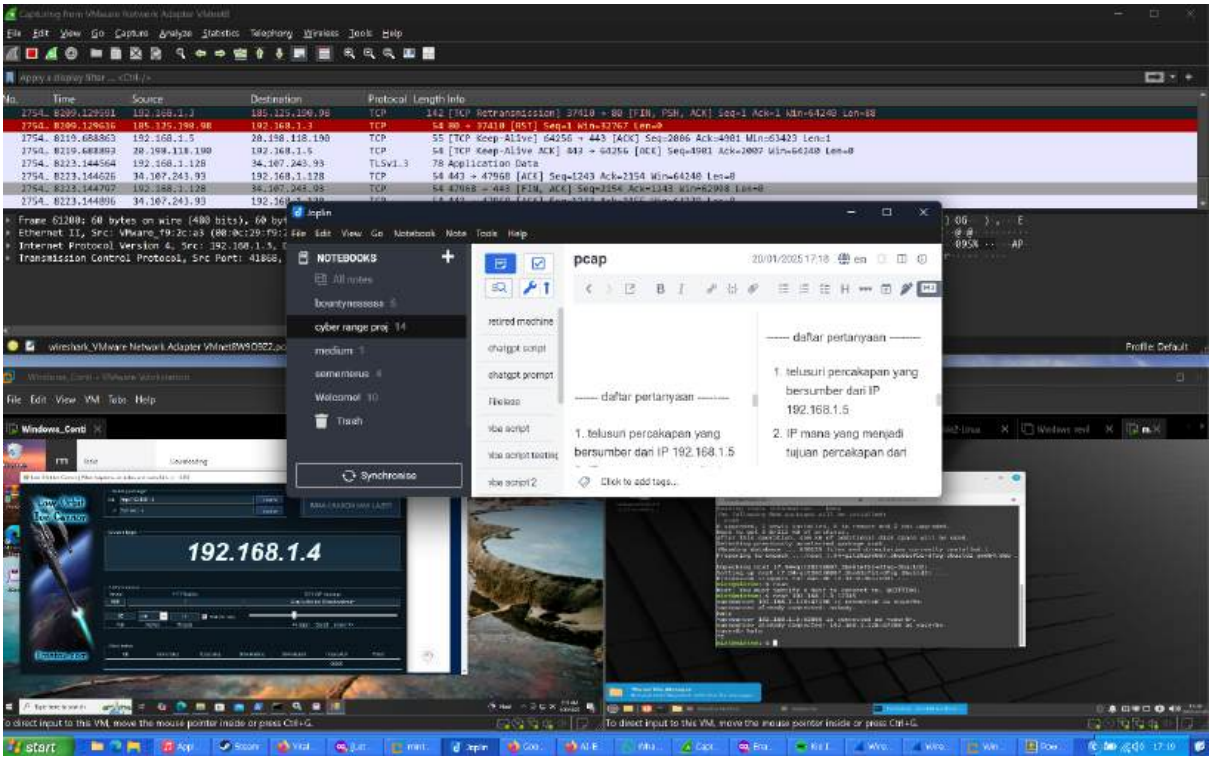
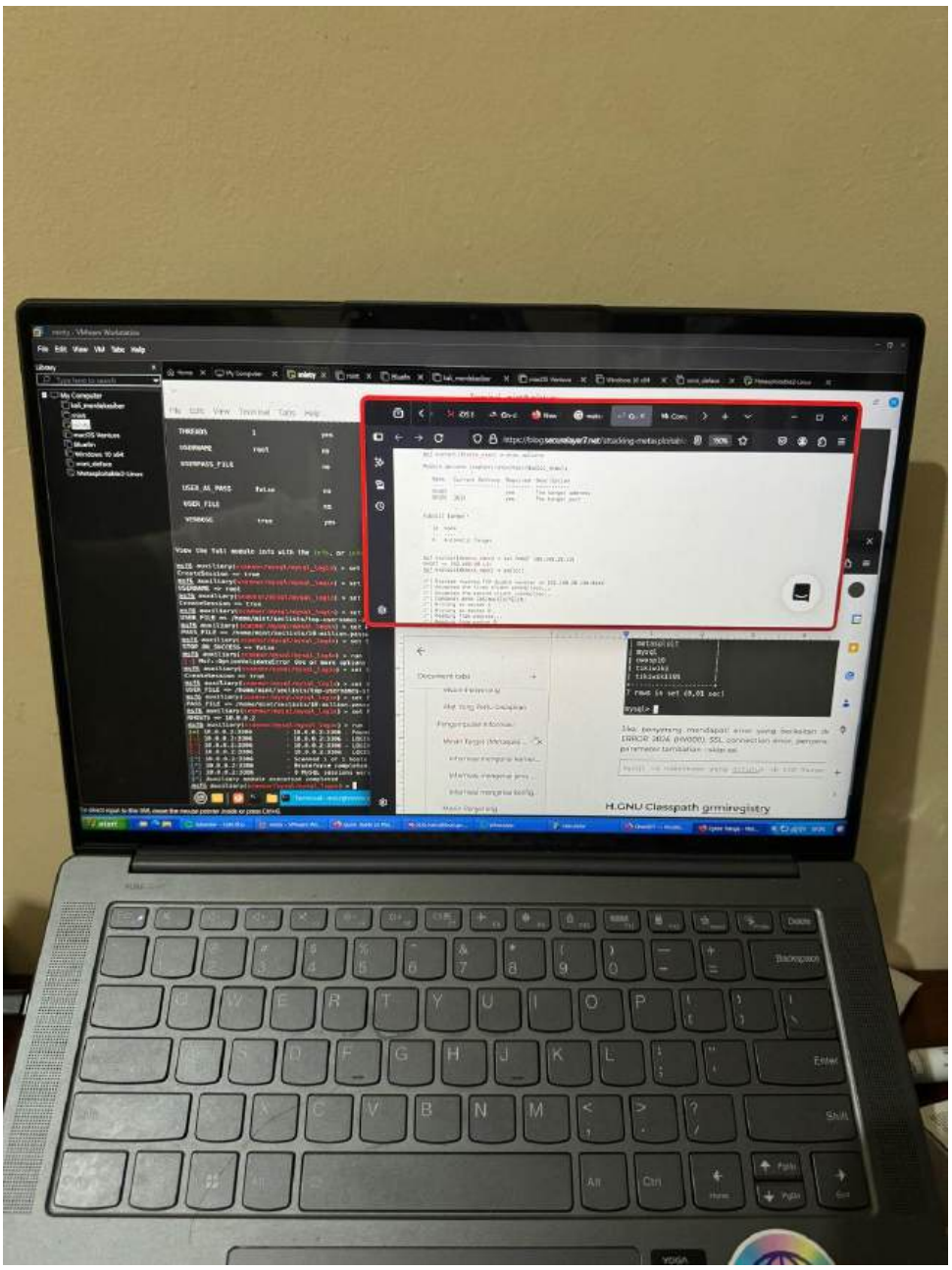
Williams, L., Anthi, E., Cherdantseva, Y., & Javed, A. (2024). Leveraging Gamification and Game-based Learning in Cybersecurity Education: Engaging and Inspiring Non-Cyber Students. *Journal of The Colloquium for Information Systems Security Education*, *11*(1), Article 1. https://doi.org/10.53735/cisse.v11i1.186

LAMPIRAN

1. Alur skenario yang disusun untuk *cyber range* analisis jaringan.



2. Aktivitas penyusunan *cyber range* analisis jaringan.



3. Aktivitas penyusunan *cyber range* metasploitable *pentest*.