
**SEKOLAH TINGGI TEKNOLOGI TERPADU NURUL FIKRI**

# ANALISA KERENTANAN APLIKASI WEB MENGGUNAKAN FRAMEWORK MITRE ATT&CK DENGAN METODE SIMULASI RED TEAM: STUDI KASUS DI PT. NURUL FIKRI CIPTA INOVASI

**TUGAS AKHIR**

**ALWI PUTRA SUPENDI**

**0110220084**

**PROGRAM STUDI TEKNIK INFORMATIKA**

**DEPOK**

**JANUARI 2023**

## HALAMAN PERNYANTAAN ORISINALITAS

**Tugas Akhir ini merupakan hasil upaya penulis,**

**dan segala referensi, baik yang disitir maupun dirujuk,**

**telah diakui dengan tepat.**

**Nama** **: Alwi Putra Supendi**

**NIM** **: 0110220084**

**Tanda Tangan** **:** 

**Tanggal** **: 5 Februari 2024**

## HALAMAN PENGESAHAN

Skripsi/Tugas Akhir ini diajukan oleh:

Nama : Alwi Putra Supendi

NIM : 0110220084

Program Studi : Teknik Informatika

Judul Skripsi : ANALISA KERENTANAN APLIKASI WEB MENGGUNAKAN FRAMEWORK MITRE ATT&CK DENGAN METODE SIMULASI RED TEAM: STUDI KASUS DI PT. NURUL FIKRI CIPTA INOVASI

**Telah berhasil dipertahankan di hadapan Dewan Penguji dan diterima sebagai persyaratan yang diperlukan untuk memperoleh gelar Sarjana Komputer pada Program Studi Teknik Informatika Sekolah Tinggi Teknologi Terpadu Nurul Fikri**

**DEWAN PENGUJI**

Pembimbing I

Henry Saptono, S.Si., M.Kom.

Penguji I

Nasrul, S.Pd.I, S.Kom, M.Kom

Ditetapkan di : Depok

Tanggal : 5 Februari 2024

## KATA PENGANTAR

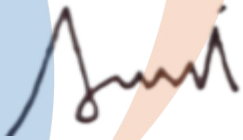
Dengan penuh syukur, penulis mengungkapkan rasa terima kasih kepada Allah SWT, karena atas berkat dan rahmat-Nya, penulis berhasil menyelesaikan skripsi/Tugas Akhir ini. Penulisan karya akhir ini merupakan bagian dari persyaratan untuk meraih gelar Sarjana dalam Program Studi Teknik Informatika di Sekolah Tinggi Teknologi Terpadu Nurul Fikri. Penulis menyadari bahwa tanpa bantuan dan bimbingan dari berbagai pihak, mulai dari masa perkuliahan hingga penyusunan skripsi ini, penulis akan menghadapi kesulitan yang besar. Oleh karena itu, penulis ingin menyampaikan rasa terima kasih kepada:

1. Allah SWT
2. Orang tua yang telah memberikan semangat sehingga penulis dapat menyelesaikan tugas ini.
3. Bapak Dr. Lukman Rosyidi, M.T, M.M., selaku Ketua Sekolah Tinggi Teknologi Terpadu Nurul Fikri.
4. Ibu Tifani Nabarian, S.Kom., M.T.I. selaku Ketua Program Studi Teknik Informatika Sekolah Tinggi Teknologi Terpadu Nurul Fikri.
5. Bapak Nasrul, S.Pd.I, S.Kom, M.Kom selaku Dosen Pembimbing Akademik yang telah membimbing penulis selama berkuliah di Sekolah Tinggi Teknologi Terpadu Nurul Fikri.
6. Bapak Henry Saptono, S.Si., M.Kom. selaku Dosen Pembimbing Tugas Akhir penulis dalam menyelesaikan penulisan ilmiah ini.
7. Para Dosen di lingkungan Sekolah Tinggi Teknologi Terpadu Nurul Fikri yang telah membimbing penulis dalam menuntut ilmu yang telah diberikan.
8. PT. Nurul Fikri Cipta Inovasi dan Manajer Bapak Drs. Rusmanto, M.M. beserta karyawan yang telah meluangkan waktunya untuk memberikan data yang diperlukan bagi penulisan ilmiah ini.
9. UPT Lab Sekolah Tinggi Teknologi Terpadu Nurul Fikri yang sudah meminjamkan laptop dalam pengerjaan tahap awal sampai pertengahan penulisan ilmiah ini.

Dalam penyusunan karya ilmiah ini, tentu masih terdapat kekurangan yang mungkin disebabkan oleh keterbatasan kemampuan dan pengetahuan penulis. Meskipun begitu, penulis telah berupaya menyelesaikan karya ilmiah ini dengan sebaik mungkin. Oleh karena itu, jika terdapat kekurangan dalam karya ilmiah ini, penulis dengan rendah hati menerima kritik dan saran dari pembaca.

Sebagai penutup, penulis berharap Allah SWT memberkahi semua pihak yang telah memberikan bantuan. Semoga karya ilmiah ini dapat memberikan manfaat bagi pengembangan ilmu.

Depok, 5 Februari 2024



Alwi Putra Supendi

## HALAMAN PERNYATAAN PERSETUJUAN PUBLIKASI TUGAS AKHIR UNTUK KEPENTINGAN AKADEMIS

Sebagai sivitas akademik Sekolah Tinggi Teknologi Terpadu Nurul Fikri, saya yang bertanda tangan di bawah ini:

Nama: Alwi Putra Supendi

NIM: 0110220084

Program Studi: Teknik Informatika

Jenis Karya: Tugas Akhir

Demi kemajuan ilmu pengetahuan, saya menyetujui untuk memberikan kepada Sekolah Tinggi Teknologi Terpadu Nurul Fikri **hak non-eksklusif tanpa royalti** atas karya ilmiah saya yang berjudul:

Analisis Kerentanan Aplikasi Web Menggunakan Framework MITRE ATT&CK Dengan Metode Simulasi Red Team: Studi Kasus di PT. Nurul Fikri Cipta Inovasi

Termasuk perangkat yang diperlukan (jika diperlukan). Dengan Hak Bebas Royalti Noneksklusif ini, STT-NF memiliki hak untuk menyimpan, mengubah media/format, mengelola dalam bentuk pangkalan data (database), merawat, dan mempublikasikan tugas akhir saya selama tetap mencantumkan nama saya sebagai penulis/pencipta serta sebagai pemilik Hak Cipta.

Demikian pernyataan ini saya buat dengan sebenarnya.

Dibuat di: Depok

Pada tanggal: 5 Februari 2024

Yang Menyatakan


Alwi Putra Supendi

## ABSTRAK

Penelitian ini mengevaluasi efektivitas penggunaan kerangka kerja MITRE ATT&CK dalam latihan red team untuk meningkatkan keamanan siber. Data diperoleh dari situasi dunia nyata dan studi kasus, menunjukkan bahwa tim red team mampu mensimulasikan serangan dengan akurat dan mengidentifikasi celah keamanan yang mungkin terlewat sebelumnya. MITRE ATT&CK membantu dalam kategorisasi dan evaluasi celah keamanan, serta berdampak positif terhadap perbaikan kebijakan dan prosedur keamanan organisasi. Temuan penelitian ini memberikan wawasan mendalam tentang penggunaan MITRE ATT&CK dalam meningkatkan postur keamanan, terutama dalam deteksi, pencegahan, dan respons terhadap ancaman siber. Integrasi MITRE ATT&CK dalam latihan red team terbukti menjadi pendekatan yang berharga dalam meningkatkan kesiapan keamanan organisasi di era ancaman siber yang terus berkembang. Kesimpulannya, MITRE ATT&CK memberikan kerangka kerja yang kuat dan efektif bagi organisasi untuk memperkuat pertahanan mereka terhadap serangan siber.



Kata kunci: Celah Keamanan, Deteksi, Evaluasi, Keamanan Siber, Kesiapan Keamanan, MITRE ATT&CK, Perbaikan Kebijakan, Pencegahan, Red team, Respons Terhadap Ancaman, Serangan Siber.

## ABSTRACT

*This research evaluates the effectiveness of employing the MITRE ATT&CK framework in red team exercises to enhance cybersecurity. Data were obtained from real-world scenarios and case studies, demonstrating that red teams accurately simulate attacks and identify previously overlooked security gaps. MITRE ATT&CK aids in categorizing and evaluating security vulnerabilities, positively impacting the improvement of organizational policies and security procedures. The research findings provide deep insights into the use of MITRE ATT&CK to enhance security posture, particularly in detection, prevention, and response to cyber threats. Integrating MITRE ATT&CK into red team exercises proves to be a valuable approach in enhancing organizational security readiness in an evolving cyber threat landscape. In conclusion, MITRE ATT&CK offers a robust and effective framework for organizations to strengthen their defenses against cyberattacks.*

*Keywords: Cyber Attack, Cybersecurity, Detection, Evaluation, MITRE ATT&CK, Policy Improvement, Prevention, Red team, Security Gap, Security Readliness, Threat Response.*

# DAFTAR ISI

## DAFTAR GAMBAR

# DAFTAR TABEL

# BAB I
# PENDAHULUAN

Dalam Bab 1, penelitian ini akan memperkenalkan latar belakang yang melatarbelakangi pemilihan topik, merumuskan permasalahan yang akan menjadi fokus utama, dan menyajikan tujuan serta manfaat dari penelitian ini. Selain itu, bab ini akan membahas batasan masalah untuk mengidentifikasi ruang lingkup penelitian dan menetapkan parameter-parameter tertentu yang dianggap relevan. Sistematika penulisan juga akan diuraikan, memberikan panduan terstruktur tentang bagaimana penulisan tugas akhir ini akan disusun, termasuk urutan dan pengaturan setiap bagian yang akan dijelaskan secara rinci.

## 1.1 Latar Belakang

Dalam era digital saat ini, keamanan cyber menjadi hal yang sangat krusial bagi organisasi, khususnya perusahaan seperti PT. Nurul Fikri Cipta Inovasi yang mengoperasikan sebagian besar aktivitas bisnisnya secara online. Ancaman cyber semakin berkembang dan kompleks dari waktu ke waktu, dengan serangan yang dilakukan oleh pihak-pihak jahat semakin canggih dan terorganisir. Oleh karena itu, penting bagi perusahaan untuk secara proaktif mengidentifikasi dan mengatasi kerentanan pada situs web mereka sebelum disusupi oleh serangan yang merugikan. Salah satu pendekatan yang telah dikenal dan digunakan secara luas adalah *MITRE ATT&CK*. Model ini memberikan panduan untuk memahami dan merencanakan strategi perlindungan terhadap ancaman siber yang mungkin terjadi[1].

Organisasi sektor publik dan swasta yang mengoperasikan Sistem Kontrol Industri *(Industrial Control System/ICS)* seperti jaringan kritis dan infrastruktur penting *(Critical Infrastructure)* harus memperhatikan risiko keamanan siber yang spesifik. Serangan terhadap Infrastruktur Kritis (ICS) dapat memiliki dampak yang sangat serius, termasuk gangguan produksi, kerusakan fisik, dan bahkan potensi ancaman terhadap keselamatan masyarakat. Untuk mengidentifikasi dan mengelola risiko ini, PT. Nurul Fikri Cipta Inovasi dapat menggunakan *MITRE ATT&CK*

*Framework*, yang memberikan *framework* berdasarkan taktik dan teknik yang sering digunakan oleh penyerang[2].

Namun, memiliki pemahaman yang baik tentang *MITRE ATT&CK Framework* tidaklah cukup. Budaya keamanan siber di dalam organisasi juga berperan penting dalam mengidentifikasi dan mengurangi risiko ancaman siber. Oleh karena itu, mengkombinasikan *MITRE ATT&CK Framework* dengan *Cultured Cyber Framework* dapat menjadi pendekatan yang efektif dalam mengelola risiko keamanan siber. Dengan memadukan dua aspek ini, PT. Nurul Fikri Cipta Inovasi dapat meningkatkan kesadaran akan keamanan siber di seluruh perusahaan dan mengurangi risiko serangan[3].

Kerentanan umum *(Common Vulnerabilities and Exposures/CVE)* adalah catatan tentang kerentanan perangkat lunak yang telah ditemukan. *Mapped* ke *MITRE ATT&CK Techniques, CVEs* dapat memberikan wawasan tentang teknik-teknik yang mungkin digunakan oleh penyerang untuk mengeksploitasi kerentanan tersebut. Penelitian telah dilakukan untuk mencocokkan *CVEs* dengan teknik-teknik yang ada dalam *MITRE ATT&CK Matrix*. Ini dapat membantu organisasi dalam mengidentifikasi risiko yang mungkin terkait dengan kerentanan perangkat lunak tertentu[4].

Analisis kerentanan menjadi langkah penting dalam meningkatkan keamanan situs web. Dengan melakukan analisis ini, perusahaan dapat mengidentifikasi celah atau kerentanan potensial dalam sistem mereka sebelum dimanfaatkan oleh pihak yang tidak bertanggung jawab. Hal ini memungkinkan perusahaan untuk mengambil langkah-langkah pencegahan yang diperlukan untuk mengurangi risiko serangan cyber.

Metode simulasi Red Team menjadi strategi yang efektif dalam menguji keamanan sistem dengan mensimulasikan serangan yang dilakukan oleh pihak jahat. Dalam konteks PT. Nurul Fikri Cipta Inovasi, simulasi Red Team dapat membantu dalam mengidentifikasi kerentanan yang mungkin tidak terdeteksi melalui metode pengujian konvensional. Perlunya fokus pada PT. Nurul Fikri Cipta

Inovasi menjadi sangat penting mengingat perusahaan ini beroperasi di sektor teknologi dan pendidikan, sehingga mungkin menjadi target menarik bagi para penyerang cyber. Oleh karena itu, penting bagi perusahaan ini untuk secara teratur melakukan analisis kerentanan dan simulasi Red Team guna memastikan keamanan situs web mereka, menjaga kepercayaan pelanggan, dan menjaga keberlanjutan bisnis mereka.

## 1.2 Rumusan Masalah

1. Bagaimana penggunaan *MITRE ATT&CK Framework* memengaruhi identifikasi celah dan kelemahan keamanan dalam suatu organisasi?
2. Apa dampak penggunaan *MITRE ATT&CK Framework* dalam *red team* terhadap perbaikan kebijakan dan prosedur keamanan organisasi?
3. Bagaimana hasil penelitian ini dapat memberikan wawasan yang lebih dalam tentang penggunaan *MITRE ATT&CK Framework* dalam konteks *red team* untuk menguji dan meningkatkan postur keamanan?

## 1.3 Tujuan dan Manfaat Penelitian

Tujuan dari penelitian ini adalah untuk menganalisis efektivitas penggunaan *MITRE ATT&CK Framework* dalam *red team* dan pengujian postur keamanan.

1. Mengukur sejauh mana penggunaan *MITRE ATT&CK Framework* dapat membantu tim *red team* dalam mengevaluasi keamanan siber suatu organisasi.
2. Menganalisis dampak penggunaan *MITRE ATT&CK Framework* terhadap identifikasi celah dan kelemahan keamanan dalam suatu organisasi.
3. Mengevaluasi efektivitas komunikasi antara tim *red team* dan tim keamanan dalam memproses temuan dan perbaikan yang dihasilkan dari *red team.*

Penelitian ini diharapkan akan memberikan manfaat sebagai berikut:

1. Kontribusi pada Peningkatan Keamanan Siber: Hasil penelitian ini akan memberikan wawasan yang berguna bagi organisasi dalam meningkatkan keamanan siber mereka. Dengan memahami efektivitas penggunaan *MITRE ATT&CK Framework* dalam *red team*, organisasi dapat mengidentifikasi area-area yang perlu diperkuat.

2. Peningkatan Identifikasi Celah Keamanan: Penelitian ini akan membantu organisasi dalam lebih efektif mengidentifikasi celah dan kelemahan keamanan mereka. Dengan demikian, mereka dapat mengambil langkah-langkah proaktif untuk mengatasi potensi risiko.
3. Perbaikan Kebijakan dan Prosedur Keamanan: Dengan pemahaman yang lebih dalam tentang dampak penggunaan *MITRE ATT&CK Framework*, organisasi dapat merancang kebijakan dan prosedur yang lebih efektif untuk melindungi sistem dan data mereka.

## 1.4 Batasan Masalah

1. Perbaikan Kebijakan dan Prosedur Keamanan: Dengan pemahaman yang lebih dalam tentang dampak penggunaan *MITRE ATT&CK Framework*, organisasi dapat merancang kebijakan dan prosedur yang lebih efektif untuk melindungi sistem dan data mereka.
2. Fokus pada Efektivitas dan Dampak: Penelitian ini akan lebih menekankan pada efektivitas penggunaan *MITRE ATT&CK Framework* dan dampaknya terhadap identifikasi celah keamanan, komunikasi *red team* dan tim keamanan, serta perbaikan kebijakan dan prosedur keamanan.
3. Tidak Mempertimbangkan Aspek Teknis Tertentu: Penelitian ini tidak akan terlalu mendalam membahas aspek teknis keamanan siber, seperti konfigurasi perangkat keras atau perangkat lunak tertentu.

## 1.5 Sistematika Penulisan

Laporan tugas akhir ini terdiri dari 5 bab, antara lain:

Bab I Pendahuluan

Menjelaskan mengenai latar belakang masalah, tujuan, manfaat, batasan masalah dan sistematika penulisan.

Bab II Tinjauan Pustaka

Menjelaskan tentang konsep *Red team*, *MITRE ATT&CK Framework*, pentingnya pengujian postur keamanan dan penelitian terkait.

Bab III Metodologi Penelitian

Menjelaskan mengenai metode pendekatan penelitian, desain penelitian, pengumpulan data dan analisis data.

Bab IV Implementasi dan Evaluasi

Menjelaskan Mengenai tahapan implementasi serta melakukan evaluasi terhadap hasil yang diperoleh.

Bab V Kesimpulan dan Saran

Kesimpulan dari pengujian mencakup hasil dan temuan, sementara saran berfokus pada langkah-langkah perbaikan. Kesimpulan memberikan gambaran umum, sedangkan saran menunjukkan tindakan konkret untuk meningkatkan kinerja atau efektivitas.

# BAB II
# KAJIAN LITERATUR

Pada bab 2 ini, akan diperkenalkan dasar-dasar konseptual yang mendukung pemahaman tentang penggunaan *MITRE ATT&CK Framework* dalam *red team* untuk pengujian postur keamanan. Konsep-konsep dasar yang mencakup *red team*, *MITRE ATT&CK Framework*, pengujian postur keamanan, serta definisi taktik, teknik, dan prosedur (TTP) akan menjadi landasan untuk pemahaman yang lebih mendalam tentang topik penelitian ini.

Pemahaman tentang *red team* sebagai metode pengujian keamanan yang aktif serta *MITRE ATT&CK Framework* sebagai panduan yang komprehensif untuk taktik dan teknik penyerangan akan membantu membentuk *framework* untuk penelitian ini. Pengertian tentang bagaimana *red team* digunakan untuk menguji postur keamanan dan bagaimana *MITRE ATT&CK Framework* mendukung langkah-langkah ini adalah kunci untuk memahami hasil penelitian nantinya.

Selain itu, akan dijelaskan konsep-konsep terkait lainnya, seperti komunikasi dalam *red team* dan tim keamanan, serta pentingnya kebijakan dan prosedur keamanan. Semua elemen ini akan membantu membentuk pemahaman yang komprehensif tentang cara penggunaan *MITRE ATT&CK Framework* dalam *red team* dapat berkontribusi pada peningkatan keamanan siber dalam konteks organisasi.

Dengan landasan yang kuat dalam konsep-konsep dasar ini, penelitian ini akan memperdalam wawasan tentang penggunaan *MITRE ATT&CK Framework* dalam *red team* dan dampaknya terhadap identifikasi celah keamanan, komunikasi, serta perbaikan kebijakan dan prosedur keamanan.

## 2.1 *Company Profile* PT. Nurul Fikri Cipta Inovasi

PT. Nurul Fikri Cipta Inovasi adalah sebuah perusahaan yang fokus pada pelatihan pendidikan dan pengembangan sumber daya manusia dalam bidang

teknologi informasi dan komunikasi. Mereka menawarkan berbagai jenis pelatihan, seperti kelas umum, kelas eksklusif, pelatihan di dalam perusahaan, serta kerjasama dengan lembaga pendidikan di Indonesia.

Berdiri sejak tahun 1994 dan beralamat di Jl. Situ Indah no.116 Kecamatan Cimanggis, Kota Depok, PT. Nurul Fikri Cipta Inovasi menyediakan layanan pelatihan untuk individu maupun perusahaan, termasuk juga layanan sertifikasi. Fokus perusahaan ini adalah meningkatkan kualitas sumber daya manusia di bidang pelatihan IT dan pengembangan perangkat lunak.

Selain itu, PT. Nurul Fikri Cipta Inovasi juga menyediakan layanan konsultasi yang tidak hanya memberikan pengetahuan tetapi juga membantu dalam pengembangan produk atau output bagi klien.

Visi PT. Nurul Fikri Cipta Inovasi adalah menjadi perusahaan pelatihan yang kompeten dan profesional dalam pendidikan teknologi informasi dan komunikasi di seluruh Indonesia. Misi perusahaan ini adalah membangun, memelihara, dan mengembangkan perusahaan pelatihan bisnis yang memiliki daya saing tinggi, berkarakter profesional, kompeten, serta mengutamakan integritas dan tanggung jawab sosial. Hal ini dilakukan dengan mengembangkan dan menyediakan produk pendidikan dan pelatihan teknologi informasi dan komunikasi yang unggul.

## 2.2 *Red Team*

*Red team* adalah praktik yang mempertanyakan rencana, kebijakan, sistem, dan asumsi secara ketat dengan mengambil pendekatan yang bersifat musuh. Sebuah *Red Team* bisa menjadi pihak eksternal yang dikontrak atau kelompok internal yang menggunakan strategi untuk mendorong sudut pandang dari pihak luar. Tujuan dari *red team* adalah untuk mengatasi kesalahan kognitif seperti *groupthink* dan bias konfirmasi, yang dapat mengganggu kemampuan pengambilan keputusan atau pemikiran kritis individu atau organisasi[5].

*Red Team* menggunakan metodologi simulasi serangan. Mereka mensimulasikan tindakan penyerang canggih (atau ancaman yang bertahan lama)

untuk menentukan seberapa baik orang, proses, dan teknologi organisasi Anda dapat menolak serangan yang bertujuan untuk mencapai tujuan tertentu.

Sebuah tim red seringkali terdiri dari sekelompok karyawan TI internal yang digunakan untuk mensimulasikan tindakan individu yang bersifat jahat atau musuh. Dari sudut pandang keamanan siber, tujuan *Red Team* adalah untuk mengeksploitasi atau mengkompromikan keamanan digital suatu perusahaan. Singkatnya, penilaian kerentanan dan pengujian penetrasi berguna untuk mengidentifikasi cacat teknis, sementara latihan *Red Team* memberikan wawasan yang dapat dijalankan tentang status keseluruhan postur keamanan TI.

### 2.2.1 Metodologi *Red Team*

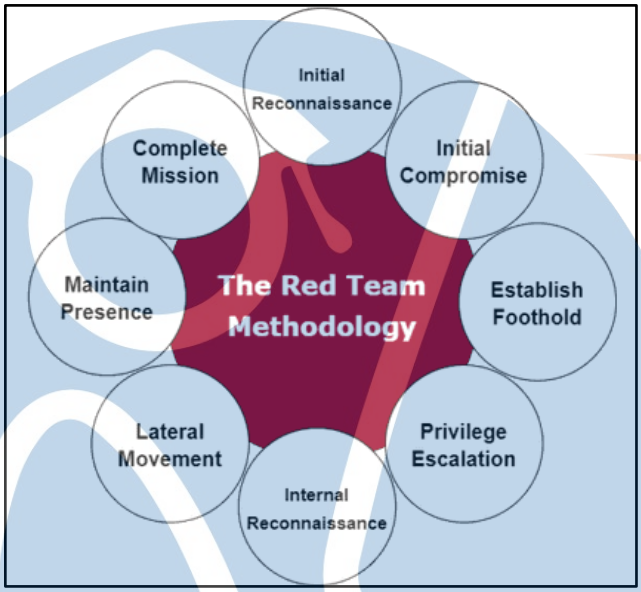
*Red team* melibatkan proses yang sangat taktis dan disengaja untuk menggali semua informasi yang diinginkan. Namun, untuk memastikan pengukuran dan pengendalian dari prosedur tersebut, sebuah penilaian harus diselesaikan sebelum simulasi. Penilaian ini harus bertujuan untuk menggunakan pola pikir dan tujuan penjahat siber sah untuk mengidentifikasi titik masuk dan kerentanan yang ingin dimanfaatkan[5].

Informasi yang dikumpulkan dari pemeriksaan ini sangat penting untuk merumuskan tujuan yang ingin dicapai oleh *Red Team*. Jika *Red Team* menemukan kelemahan yang terkait dengan aset digital, aset fisik, proses teknis, atau proses operasional, sesi *red team* akan berusaha memprioritaskan eksploitasi tersebut.

Setelah tujuan telah ditentukan, *Red Team* akan memulai serangan. Biasanya, tim biru akan dapat mengidentifikasi aktivitas *Red Team* sebagai yang bersifat jahat dan mulai membatasi atau membatasi kesuksesan upaya mereka. Setelah latihan selesai, setiap pihak akan memberikan daftar temuan yang memperlihatkan nilai dari perspektif mereka -- dan latihan secara keseluruhan.

Tim biru akan mengidentifikasi indikator kompromi *(IoC)* yang dapat mereka deteksi selama keterlibatan. *IoC* adalah tanda yang tim keamanan gunakan untuk mencatat aktivitas yang mencurigakan. Di sisi lain, *Red Team* akan menyiapkan pemecahan taktik, teknik, dan prosedur *(TTP)* mereka untuk tim biru.

Bersama-sama, kedua tim menggunakan hasil tersebut untuk membuat daftar tindakan yang dapat diambil -- seperti peningkatan *firewall* atau konfigurasi server -- yang dapat mereka lakukan untuk meningkatkan deteksi dan aktivitas respons dari sistem keamanan saat ini.




*Sumber: www.prplbx.com*

*Gambar 2.1 Red Team Methodology*

1. *Initial Reconnaissance*: Penyerang melakukan riset terhadap calon korban potensial. Penyerang memilih target (baik sistem maupun individu) dan strategi serangannya. Untuk mengeksploitasi, penyerang dapat mencari layanan yang terbuka di Internet atau individu yang dapat disasar.
2. *Initial Compromise*: Pada satu atau lebih sistem, penyerang berhasil menjalankan kode berbahaya. Hal ini biasanya dicapai dengan menggunakan Rekayasa Sosial (paling umumnya *spear phishing*), eksploitasi kerentanan pada sistem yang terbuka di Internet, atau melalui cara lain yang tersedia.
3. *Establish Foothold*: Penyerang memastikan bahwa sistem yang telah diretas tetap berada dalam kendalinya. Biasanya, penyerang mendapatkan akses pada mesin korban dengan menginstal pintu belakang yang persisten atau mengunduh program atau *malware* lainnya.

4. *Privilege Escalation*: Penyerang mendapatkan lebih banyak kendali atas sistem dan data. *Dumping hash* kata sandi (diikuti dengan peretasan kata sandi atau serangan *pass-the-hash*), pencatatan kegiatan tombol/*credential*, mendapatkan sertifikat PKI, memanfaatkan hak akses yang dimiliki oleh suatu aplikasi, atau menyerang perangkat lunak yang lemah adalah cara umum yang digunakan penyerang untuk meningkatkan hak akses mereka.
5. *Internal Reconnaissance*: Penyerang menyelidiki lingkungan korban untuk mendapatkan pemahaman lebih baik tentang lingkungan tersebut, peran dan tugas individu-individu penting, serta lokasi informasi sensitif yang disimpan oleh perusahaan.
6. *Lateral Movement*: Penyerang menggunakan aksesnya untuk berpindah dari satu sistem ke sistem lainnya dalam lingkungan yang telah diretas.
7. *Maintain Presence*: Penyerang memastikan akses terus berlanjut dalam lingkungan tersebut.
8. *Complete Mission*: Penyerang mencapai tujuannya. Ini sering melibatkan pencurian kekayaan intelektual, data keuangan, informasi tentang penggabungan dan akuisisi, atau Informasi yang Dapat Diidentifikasi Secara Pribadi *(PII)*[6].

### 2.2.2 Bagaimana Cara Kerja *Red Team*

Untuk mendapatkan akses ke jaringan dan bergerak tanpa terdeteksi di seluruh lingkungan, *Red Team* yang sukses harus cerdik, mengadopsi sikap lawan yang terampil. Anggota *Red Team* yang ideal memiliki keterampilan teknis dan kreatif, dengan kemampuan untuk mengeksploitasi kerentanan sistem dan sifat manusia.

*Red Team* juga harus familiar dengan taktik, metode, dan prosedur (TTPs) pelaku ancaman, serta alat dan *framework* serangan yang digunakan oleh lawan.

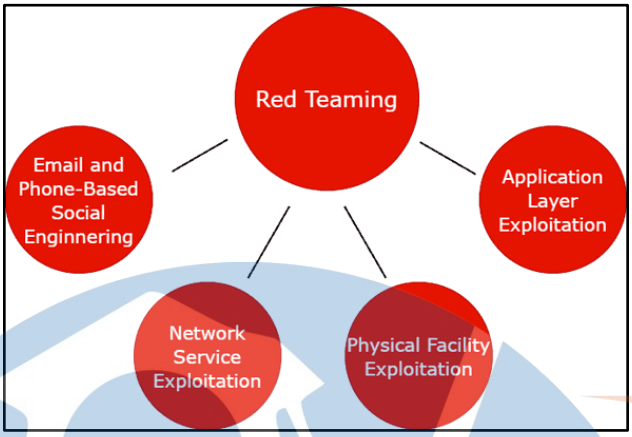
Seorang anggota *Red Team* seharusnya memiliki kualifikasi berikut:

1. Memiliki pemahaman mendalam tentang sistem komputer dan protokol, serta metodologi, alat, dan perlindungan keamanan.

2. Kemampuan pemrograman perangkat lunak yang kuat diperlukan untuk membuat alat khusus yang dapat melewati metode dan kontrol keamanan biasa.
3. Pengalaman dalam pengujian penetrasi, yang memungkinkan untuk mengeksploitasi kelemahan umum sambil menghindari aktivitas yang sering diamati atau mudah dikenali.
4. Keterampilan dalam rekayasa sosial yang memungkinkan anggota tim untuk meyakinkan orang lain untuk berbagi informasi atau kredensial.

Melihat bagaimana sebuah *Red Team* biasa berlangsung adalah cara terbaik untuk memahami detail tentang bagaimana *Red team* bekerja. Ada beberapa tahap dalam proses *Red Team* yang biasa:

1. Tujuan akan disepakati oleh *Red Team* organisasi (baik yang internal atau yang dikontrak eksternal). Tujuan ini bisa, misalnya, adalah pengambilan informasi sensitif dari server tertentu.
2. Setelah itu, *Red Team* akan melakukan pemetaan objektif. Sebagai hasil dari ini, akan dibuat peta sistem target, termasuk layanan jaringan, aplikasi web, dan layanan karyawan.
3. Upaya akan dilakukan untuk mendapatkan sesi pada sistem menggunakan teknik *phishing* atau kerentanan yang terdeteksi.
4. Setelah token akses yang sah diperoleh, *Red Team* akan menggunakan akses mereka untuk mencari kerentanan lain.
5. Jika ditemukan lebih banyak kerentanan, *Red Team* akan mencoba meningkatkan tingkat akses mereka ke tingkat yang diperlukan untuk mendapatkan akses ke target.
6. Data atau aset target tercapai begitu hal ini tercapai.

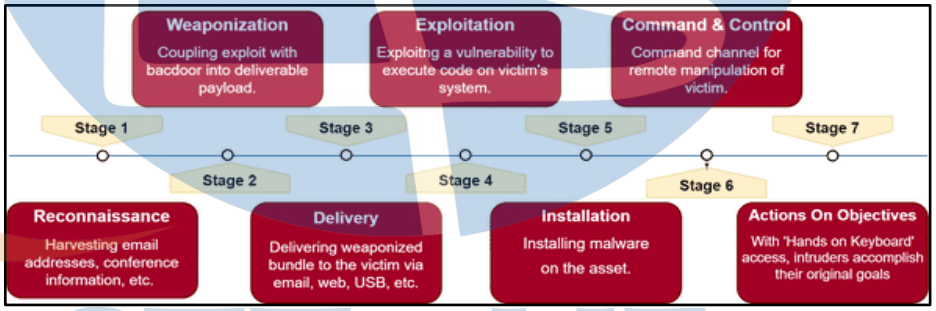



*Sumber: www.prplbx.com*

*Gambar 2.2 How Red Team Works*

### 2.2.3 Metode *Cyber Kill Chain*

*Cyber Kill Chain* pada dasarnya adalah model Keamanan Siber yang dibuat oleh Lockheed Martin yang menelusuri tahapan serangan siber, mengidentifikasi kerentanan, dan membantu tim keamanan menghentikan serangan di setiap tahap rantai.




*Sumber: www.prplbx.com*

*Gambar 2.3 Cyber Kill Chain*

1. *Reconnaissance*: Tahap pertama melibatkan penelitian awal terhadap target yang mencakup pengenalan sasaran potensial dan pencarian potensi kerentanan. Penyerang mencari informasi tentang target menggunakan metode seperti pencarian terbuka dan survei online.
2. *Weaponization*: Pada tahap ini, penyerang membuat atau mempersiapkan alat dan teknik yang akan digunakan dalam serangan. Ini bisa termasuk

menciptakan atau memilih perangkat lunak berbahaya atau alat yang akan digunakan.

3. *Delivery*: Penyerang menyampaikan alat atau *malware* ke target melalui berbagai saluran seperti email berbahaya, situs web terkompromi, atau perangkat fisik yang dimodifikasi.
4. *Exploitation*: Penyerang mencoba untuk mengeksploitasi kerentanan atau celah keamanan dalam sistem atau aplikasi target untuk mendapatkan akses ke dalamnya.
5. *Installation*: Setelah berhasil dieksploitasi, penyerang menginstal *malware* atau alat berbahaya pada sistem target yang memungkinkan mereka mempertahankan akses.
6. *Command and Control*: Penyerang mendirikan jalur komunikasi rahasia antara sistem target dan infrastruktur yang mereka kendalikan untuk memungkinkan pengendalian sistem target dan pelaksanaan tindakan lebih lanjut.
7. *Actions on Objectives*: Tahap akhir adalah ketika penyerang mencapai tujuan mereka, yang bisa berupa pencurian data, kerusakan sistem, atau pengganggguan operasi target. Setelah mencapai tujuan, penyerang bisa memutuskan untuk melancarkan serangan lainnya atau mundur tanpa meninggalkan jejak[6].

**Contoh Skenario *Red Team***

Contoh skenario ditampilkan menggunakan metode *Cyber Kill Chain*

*Tabel 2.1 Red Team Example Scenario*

| **Stage** | **Scenario** |
|---|---|
| *Reconnaissance* | *IP address* pelanggan, port yang terbuka di alamat-alamat tersebut, layanan yang berjalan di port, akun media sosial, dan alamat email karyawan ditentukan. |
| *Weaponization* | Kode eksploitasi atau *malware* disiapkan dan diinstal dalam perangkat USB. |

| Stage | Scenario |
|---|---|
| *Delivery* | Tempat-tempat di mana orang aktif ditemukan dan perangkat USB yang telah disiapkan diletakkan ke tempat yang relevan. Dengan mengeksploitasi rasa ingin tahu orang, perangkat USB dipastikan diambil oleh seseorang. |
| *Exploitation* | Akses ke komputer target diberikan oleh orang yang menemukan perangkat USB dan mencolokkannya ke komputer milik pelanggan. |
| *Installation* | Kontrol otorisasi pengguna yang diperoleh pada komputer target dilakukan. Jika pengguna ini adalah pengguna berwenang rendah, kerentanannya dideteksi pada sistem di mana kami dapat meningkatkan otoritas. Jika hak akses pengguna kami tinggi, keberlanjutan dijamin dengan menambahkan kunci baru ke jalur "HKCU\Software\Microsoft\CurrentVersion\Run" untuk memastikan keberlanjutan. Selanjutnya, akses ke informasi kata sandi pengguna yang masuk ke komputer melalui memori disediakan. |
| *Command and Control* | Komunikasi dengan server perintah dimulai. Pergerakan horizontal dilakukan di jaringan dengan serangan *"Pass the Hash"* dengan menggunakan informasi pengguna yang diperoleh dari memori. Hingga pengguna *Domain Admin* diperoleh, informasi pengguna aktif diperoleh dari memori setiap komputer yang masuk. |
| *Actions on Objectives* | Dengan menggunakan metode seperti *DNS Tunneling*, *SSH Tunneling*, atau *ICMP tunneling*, data penting yang dikirimkan oleh pelanggan kepada kami bocor. *Red team* berhasil diselesaikan ketika data penting diekstraksi. |

## 2.3 *MITRE ATT&CK Framework*

*MITRE ATT&CK* adalah referensi pengetahuan yang disusun dengan cermat dan model perilaku penyerang siber, mencerminkan berbagai tahap siklus serangan penyerang dan platform yang biasanya menjadi sasaran mereka. *ATT&CK* berfokus pada cara penyerang eksternal mengkompromi dan beroperasi dalam jaringan informasi komputer. Ini bermula dari sebuah proyek untuk mendokumentasikan dan mengkategorikan taktik, teknik, dan prosedur penyerang setelah mereka berhasil melakukan kompromi terhadap sistem *Microsoft Windows*, dengan tujuan meningkatkan kemampuan mendeteksi perilaku berbahaya. Sejak itu, *ATT&CK* telah berkembang untuk mencakup *Linux* dan *macOS*, serta telah meluas untuk mencakup perilaku yang mengarah pada kompromi lingkungan, serta domain teknologi seperti perangkat seluler, sistem berbasis cloud, dan sistem kontrol industri. Secara garis besar, *ATT&CK* adalah model perilaku yang terdiri dari unsur inti berupa taktik, teknik, sub-teknik, dan penggunaan teknik oleh penyerang yang didokumentasikan beserta prosedur dan informasi lainnya[7].

### 2.3.1 *ATT&CK Use Cases*

1. ***Adversary Emulation*** – Proses penilaian keamanan dalam suatu domain teknologi dengan menerapkan intelijen ancaman siber mengenai penyerang tertentu dan cara operasi mereka untuk mengejarkan ancaman tersebut. Emulasi penyerang berfokus pada kemampuan sebuah organisasi untuk memverifikasi deteksi dan/atau mitigasi aktivitas penyerang dalam seluruh tahap siklusnya yang berlaku.

   *ATT&CK* dapat digunakan sebagai alat untuk membuat skenario emulasi[8] penyerang guna menguji dan memverifikasi pertahanan terhadap teknik penyerang umum. Profil untuk kelompok penyerang tertentu dapat dibangun dari informasi yang didokumentasikan dalam *ATT&CK* (lihat penggunaan intelijen ancaman siber). Profil ini juga dapat digunakan oleh tim pertahanan dan tim pencarian untuk menyelaraskan dan meningkatkan langkah-langkah pertahanan.

2. ***Red team*** – Menerapkan pola pikir penyerang tanpa menggunakan intelijen ancaman yang diketahui untuk melakukan . *Red team* berfokus pada pencapaian tujuan akhir dari suatu operasi tanpa terdeteksi untuk menunjukkan dampak misi atau operasional dari keberhasilan kompromi.

   *ATT&CK* dapat digunakan sebagai alat untuk membuat rencana *Red Team* dan mengorganisir operasi untuk menghindari tindakan pertahanan tertentu yang mungkin ada dalam jaringan. Ini juga dapat digunakan sebagai peta jalan penelitian untuk mengembangkan cara-cara baru untuk melakukan tindakan yang mungkin tidak terdeteksi oleh pertahanan umum.

3. ***Behavioral Analytics Development*** – Dengan melebihi indikator kompromi (IoC) atau tanda aktivitas berbahaya yang umum, analitik deteksi perilaku dapat digunakan untuk mengidentifikasi aktivitas berpotensi berbahaya dalam sistem atau jaringan yang tidak bergantung pada pengetahuan sebelumnya tentang alat dan indikator penyerang. Ini adalah cara memanfaatkan bagaimana penyerang berinteraksi dengan platform tertentu untuk mengidentifikasi dan menghubungkan aktivitas mencurigakan yang bersifat agnostik atau independen dari alat khusus yang mungkin digunakan.

   *ATT&CK* dapat digunakan sebagai alat untuk membuat dan menguji analitik perilaku untuk mendeteksi perilaku penyerang dalam suatu lingkungan. Repositori Analitik Siber1 *(CAR)* adalah salah satu contoh pengembangan analitik yang dapat digunakan sebagai titik awal bagi sebuah organisasi untuk mengembangkan analitik perilaku berdasarkan *ATT&CK*.

4. ***Defensive Gap Assessment*** – Penilaian celah pertahanan memungkinkan suatu organisasi untuk menentukan bagian dari lingkup perusahaannya yang kekurangan pertahanan dan/atau visibilitas. Celah-celah ini mewakili titik buta bagi vektor potensial yang memungkinkan penyerang mendapatkan akses ke jaringan mereka tanpa terdeteksi atau tidak teratasi.

   *ATT&CK* dapat digunakan sebagai model perilaku penyerang yang berfokus pada penilaian celah pertahanan guna menilai alat, pemantauan, dan mitigasi

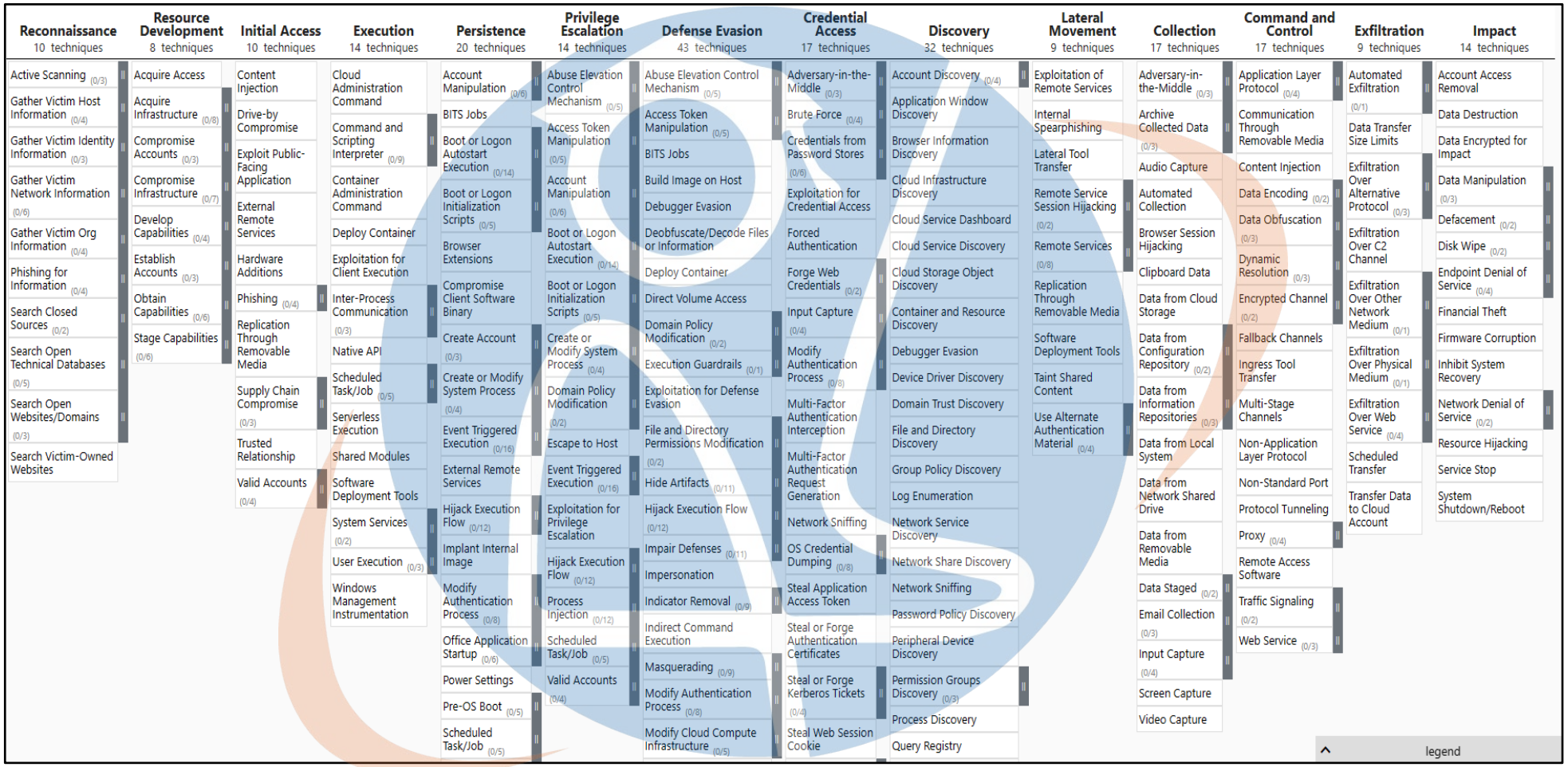
dari pertahanan yang ada dalam lingkungan perusahaan. Celah-celah yang diidentifikasi berguna sebagai cara untuk mengutamakan investasi untuk perbaikan program keamanan.

### 2.3.2 *The ATT&CK Model*

Landasan *ATT&CK* adalah serangkaian teknik dan sub-teknik yang menggambarkan tindakan yang dapat dilakukan oleh penyerang untuk mencapai tujuan. Tujuan-tujuan ini direpresentasikan oleh kategori taktik di bawah mana teknik dan sub-teknik berada. Representasi yang relatif sederhana ini menciptakan keseimbangan yang berguna antara rincian teknis yang memadai pada tingkat teknik dan konteks mengenai alasan mengapa tindakan-tindakan tersebut terjadi pada tingkat taktik.

***The ATT&CK Matrix***

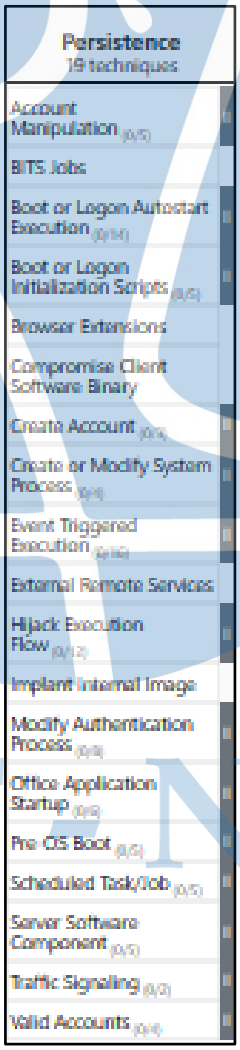
Keterkaitan antara taktik, teknik, dan sub-teknik dapat dilihat dalam *Matriks ATT&CK*. Sebagai contoh, dalam taktik Persistensi (ini adalah tujuan penyerang - bertahan dalam lingkungan target), terdapat sejumlah teknik termasuk *Hijack Execution Flow*, *Pre-OS Boot*, dan *Scheduled Task/Job*. Setiap teknik ini merupakan satu tindakan tunggal yang mungkin digunakan oleh penyerang untuk mencapai tujuan persistensi.




*Sumber: www.mitre-attack.github.io/attack-navigator/*

*Gambar 2.4 ATT&CK Navigator and Matrix*

Selain itu, beberapa teknik dapat dipecah menjadi sub-teknik yang memberikan penjelasan lebih rinci tentang bagaimana perilaku-perilaku tersebut dapat dilakukan. Sebagai contoh, *Pre-OS Boot* memiliki tiga sub-teknik yang mencakup *Bootkit*, Komponen *Firmware*, dan Sistem *Firmware* untuk menjelaskan bagaimana persistensi dicapai sebelum sistem operasi melakukan *boot*. Gambar 5 menggambarkan Taktik Persistensi dengan teknik dan empat teknik yang diperluas untuk menunjukkan sub-teknik: *Account Manipulation, Pre-OS Boot, Scheduled Tasks, and Server Software Components* [7].




*Sumber: www.mitre-attack.github.io/attack-navigator/*

*Gambar 2.5 Persistence Techniques*

## 2.4 *Kali Linux*

*Kali Linux*, yang dulunya dikenal sebagai BackTrack Linux, merupakan distribusi Linux berbasis Debian yang bersifat *open-source* dan ditujukan untuk *Penetration Testing* dan *Security Auditing* tingkat lanjut. Ini dicapai dengan menyediakan alat-alat, konfigurasi, dan otomatisasi yang umum, sehingga pengguna dapat fokus pada tugas yang perlu diselesaikan, bukan pada aktivitas di sekitarnya.

*Kali Linux* dilengkapi dengan modifikasi khusus untuk industri serta ratusan alat yang ditargetkan untuk berbagai tugas Keamanan Informasi, seperti *Penetration Testing*, Riset Keamanan, Forensik Komputer, *Reverse Engineering*, Manajemen Kerentanan, dan Pengujian *Red Team*.

### 2.4.1 *Wapiti*

*Wapiti*, sebuah alat *open-source*, bertujuan untuk mengaudit keamanan aplikasi web dengan mencari dan mengekspos celah-celah yang bisa dimanfaatkan oleh penyerang. Fitur utamanya meliputi pemindaian otomatis yang menggunakan serangkaian permintaan HTTP untuk menganalisis tanggapan dan mengidentifikasi kerentanan seperti *SQL injection*, *XSS*, dan injeksi perintah. Pengguna memiliki fleksibilitas dalam menyesuaikan parameter pemindaian, termasuk URL yang dituju dan *payload* yang digunakan untuk pengujian. Setelah pemindaian selesai, Wapiti menyusun laporan yang merinci kerentanan yang ditemukan serta memberikan rekomendasi perbaikan. Alat ini juga mendukung pemindaian pada aplikasi web yang diakses melalui protokol HTTP atau HTTPS dan dapat dijalankan pada berbagai sistem operasi termasuk Linux, Windows, dan macOS[9].

### 2.4.2 *Skipfish*

*Skipfish* merupakan sebuah perangkat pengujian keamanan aplikasi web yang didesain untuk melakukan pemindaian yang cepat dan menyeluruh terhadap situs-situs web. Dikembangkan oleh Google, alat ini menyediakan sejumlah fitur yang memungkinkan penggunaannya untuk menemukan serta memanfaatkan celah keamanan pada aplikasi web. Fitur utamanya meliputi kemampuan melakukan pemindaian dengan cepat, mendeteksi secara otomatis berbagai jenis kerentanan

keamanan seperti *SQL injection, XSS, dan CSRF*, serta memberikan kemungkinan kustomisasi parameter pemindaian agar sesuai dengan kebutuhan pengguna. Skipfish juga menghasilkan laporan pemindaian yang merinci kerentanan yang ditemukan berserta rekomendasi perbaikan, dan mendukung protokol HTTP dan HTTPS untuk memeriksa aplikasi web yang diakses melalui koneksi yang aman. Alat ini juga kompatibel dengan berbagai platform termasuk Linux, FreeBSD, dan MacOS[10].

### 2.4.3 *Nmap*

*Nmap*, yang singkatnya adalah *"Network Mapper,"* adalah alat perangkat lunak yang bersifat *open-source* dan berfungsi untuk menganalisis dan memetakan jaringan komputer. Tujuannya adalah untuk mengenali perangkat yang terhubung ke jaringan, menemukan layanan yang sedang berjalan di perangkat-perangkat tersebut, dan mengevaluasi keamanan jaringan. *Nmap* dapat digunakan untuk menyusun peta topologi jaringan, menentukan port yang terbuka, dan memberikan informasi dasar tentang perangkat dalam jaringan. Alat ini berguna bagi administrator jaringan dalam mengidentifikasi potensi kerentanan dan menjaga keamanan jaringan. Alat ini sangat berguna untuk memindai jaringan yang besar. Contoh perintah *Nmap*: nmap –T4 –A – v *Domain Name System (DNS)* digunakan untuk menghasilkan informasi seperti nama aplikasi, versi sistem operasi, dan sebagainya[11].

### 2.4.4 *Hydra*

*Hydra* adalah sebuah alat pengujian penetrasi yang kuat dan serbaguna yang digunakan untuk melakukan serangan *brute-force* atau serangan kamus untuk mendapatkan akses tidak sah ke sistem atau layanan. Alat ini dapat digunakan untuk mencoba kombinasi kata sandi secara otomatis dengan menggunakan serangan kekerasan atau kamus terhadap layanan seperti *SSH, FTP, Telnet, HTTP Basic* dan *Digest Authentication*, serta berbagai protokol lainnya[12].

### 2.4.5 *Wappalyzer*

*Wappalyzer* merupakan alat analisis *open-source* yang bertujuan untuk mengenali teknologi yang digunakan dalam pembangunan aplikasi web. Dengan

*Wappalyzer*, pengguna dapat memeriksa situs web untuk mengetahui teknologi yang dipakai, termasuk *CMS* seperti *WordPress*, *Drupal*, dan *Joomla*, *platform e-commerce* seperti *Shopify* dan *Magento*, serta *framework JavaScript* seperti *React.js* dan *AngularJS*. Beberapa fitur utama dan cara kerja *Wappalyze*r mencakup kemampuannya dalam mengidentifikasi teknologi, penyajian informasi dengan cara yang jelas dan sederhana, ketersediaan sebagai ekstensi pada *browser* populer seperti *Chrome*, *Firefox*, dan *Edge* untuk analisis langsung dari *browser*, analisis yang cepat dalam waktu singkat, serta kemampuan untuk disesuaikan sesuai kebutuhan pengguna melalui pengaturan dan filter yang dapat disesuaikan[13].

### 2.4.6 *Nikto*

*Nikto* adalah sebuah alat pemindaian otomatis yang dapat digunakan secara gratis dan berjalan melalui baris perintah. Alat ini melakukan pemindaian yang mencakup kerentanan umum, seperti masalah pada konfigurasi server, kesalahan dalam pengaturan file dan direktori, serta kerentanan terhadap serangan khusus seperti injeksi perintah dan *cross-site scripting (XSS)*. Nikto berguna bagi administrator sistem dan peneliti keamanan untuk mengenali titik masuk potensial yang memerlukan perbaikan pada aplikasi web mereka. Untuk mengidentifikasi kerentanan dalam aplikasi web[11].

### 2.4.7 *nslookup*

*Nslookup*, singkatan dari *"name server lookup,"* adalah perangkat baris perintah yang digunakan untuk melakukan kueri ke *DNS (Domain Name System)* dengan tujuan mengonversi nama domain menjadi alamat IP atau sebaliknya, serta mengakses data *DNS* lainnya.

*Nslookup* umumnya menjadi pilihan administrator jaringan sebagai alat bantu t*roubleshoot* dan pemecahan masalah *DNS*. Aplikasi ini dapat dijalankan di berbagai Sistem Operasi, termasuk *Windows*, *Mac*, dan *Linux* [14].

Fungsionalitas utama *nslookup*, seperti dijelaskan sebelumnya, adalah untuk melakukan kueri ke *DNS* guna mengonversi nama domain menjadi alamat IP atau sebaliknya, dan mengakses informasi *DNS* lainnya.

*Nslookup* berguna untuk memeriksa apakah koneksi jaringan sudah mengenali catatan *DNS* yang baru diubah. Selain itu, kita dapat menggunakan *nslookup* untuk memeriksa catatan *DNS* pada server *DNS* tertentu.

Dengan *nslookup*, kita dapat melakukan pemeriksaan terhadap integritas dan keakuratan informasi *DNS* dalam suatu sistem. Alat ini memberikan bantuan dalam memahami dan memperbaiki potensi masalah terkait dengan resolusi *DNS*, serta membantu memastikan ketersediaan dan keandalan layanan jaringan.

### 2.4.8 *theHarvester*

*TheHarvester* adalah sebuah alat open-source yang digunakan untuk mengumpulkan informasi tentang target tertentu dari berbagai sumber publik secara otomatis. Alat ini dirancang untuk membantu dalam pemetaan permukaan serangan (attack surface mapping) dan pengumpulan intelijen terbuka (OSINT) dalam konteks keamanan informasi. TheHarvester dapat digunakan untuk mendapatkan informasi seperti alamat email, nama domain, subdomain, dan alamat IP yang terkait dengan target dari sumber-sumber seperti mesin pencari, situs web publik, dan sumber lainnya yang terbuka untuk umum[15].

### 2.4.9 *whatweb*

*WhatWeb* merupakan pemindai web generasi berikutnya dengan tujuan utama mengidentifikasi situs web. Fungsinya adalah untuk menjawab pertanyaan, "Apa itu *Website* tersebut?". Alat ini memiliki kemampuan mengenali beragam teknologi web, termasuk sistem manajemen konten, *platform blogging*, paket statistik atau analitik, *JavaScript Library*, server web, dan perangkat tertanam.

Dengan lebih dari *1800 plugin*, masing-masing dirancang khusus untuk mengidentifikasi elemen yang berbeda, *WhatWeb* juga dapat mengenali nomor versi, alamat email, ID akun, modul kerangka kerja web, kesalahan SQL, dan informasi lainnya.

*WhatWeb* dapat beroperasi secara tersembunyi dan cepat, atau melakukan pemindaian menyeluruh namun dengan kecepatan yang lebih lambat. Alat ini mendukung tingkat agresi yang dapat disesuaikan, memberikan kontrol terhadap

keseimbangan antara kecepatan dan keandalan. Saat mengunjungi suatu situs web melalui *browser*, transaksi tersebut memberikan petunjuk tentang teknologi web apa yang digunakan oleh situs tersebut. Apabila informasi yang diinginkan tidak mencukupi dari satu kunjungan halaman web, *WhatWeb* dapat digunakan untuk menginterogasi situs web lebih lanjut.

Tingkat agresi default, yang disebut *'stealthy'*, adalah yang paling cepat dan hanya memerlukan satu permintaan *HTTP* dari situs *web*. Mode ini cocok untuk pemindaian situs web publik. Terdapat juga mode yang lebih agresif yang dikembangkan untuk digunakan dalam uji penetrasi, menawarkan pemindaian yang lebih menyeluruh namun dengan kecepatan yang lebih lambat. Dengan demikian, secara keseluruhan, *WhatWeb* memberikan pemahaman mendalam terhadap teknologi web yang digunakan oleh suatu situs dengan berbagai opsi pengaturan sesuai kebutuhan[16].

### 2.4.10 *Dirb*

*Dirb* adalah sebuah alat pengujian penetrasi yang digunakan untuk melakukan serangan kamus terhadap server web dengan tujuan menemukan direktori dan berkas tersembunyi yang mungkin rentan terhadap serangan. Alat ini secara otomatis mengirimkan permintaan *HTTP GET* untuk setiap direktori dan berkas yang diidentifikasi dalam daftar kata sandi atau kamus yang ditentukan oleh pengguna. Tujuan utama dari penggunaan *Dirb* adalah untuk mengidentifikasi area-area yang mungkin tidak terlindungi atau memiliki konfigurasi yang rentan, sehingga memungkinkan untuk dilakukan serangan lebih lanjut seperti penemuan akses tidak sah atau eksploitasi kerentanan[15].

## 2.5 *Vulnerability*

Kerentanan *(Vulnerability)* adalah kelemahan dalam suatu sistem atau perangkat lunak yang dapat dimanfaatkan oleh penjahat cyber untuk mendapatkan akses tanpa izin. Setelah berhasil dieksploitasi, kerentanan dapat digunakan untuk menjalankan kode berbahaya, menginstal malware, bahkan mencuri data sensitif. Metode eksploitasi termasuk *SQL injection, buffer overflow, cross-site scripting*

*(XSS)*, dan penggunaan perangkat eksploitasi *open-source* yang mencari celah keamanan dalam aplikasi web[17].

Berbagai faktor, seperti kesalahan perancangan, kekurangan dalam pengkodean perangkat lunak, atau kurangnya kebijakan keamanan yang tepat, dapat menjadi sumber kerentanan. Penjahat siber menggunakan metode dan teknik tertentu, seperti mencari celah keamanan yang belum teratasi atau menggunakan *malware*, untuk merusak integritas, kerahasiaan, atau ketersediaan data.

Identifikasi, pemahaman, dan mitigasi kerentanan merupakan bagian penting dari upaya keamanan informasi. Perusahaan dan pengembang perangkat lunak secara rutin melakukan pemindaian keamanan, pembaruan perangkat lunak, dan menerapkan praktik keamanan terbaik untuk mengurangi risiko kerentanan yang dapat dimanfaatkan oleh pihak jahat. Kerentanan semacam ini yang dieksploitasi tanpa pemberitahuan tercatat oleh *MITRE* sebagai *Common Vulnerability Exposure (CVE)*[17].

### 2.5.1 *Absence of Anti-CSRF Tokens*

*Absence of Anti-CSRF Tokens* mengacu pada keadaan di mana sebuah aplikasi web tidak mengimplementasikan token *Anti-CSRF (Cross-Site Request Forgery)* atau tidak menggunakan mekanisme perlindungan yang memadai terhadap serangan *CSRF*. *CSRF* adalah jenis serangan keamanan di mana penyerang dapat memaksa pengguna yang terautentikasi untuk melakukan tindakan tanpa izin melalui manipulasi permintaan *HTTP* yang dikirimkan dari situs web yang telah diatur sebelumnya.

Token Anti-CSRF adalah langkah keamanan yang umum digunakan untuk melindungi aplikasi web dari serangan *CSRF*. Token ini disematkan dalam formulir atau permintaan *HTTP* dan harus dikirimkan bersamaan dengan permintaan autentikasi untuk memastikan bahwa permintaan tersebut sah. Jika token tidak valid atau tidak ada, server dapat menganggap permintaan tersebut mencurigakan dan menolak untuk memprosesnya [18].

Ketidakhadiran token Anti-CSRF meningkatkan risiko serangan *CSRF*, karena serangan semacam itu dapat dilakukan dengan lebih mudah jika tidak ada mekanisme keamanan yang efektif. Oleh karena itu, pengembang web disarankan untuk selalu mengimplementasikan langkah-langkah keamanan, termasuk penggunaan token *Anti-CSRF*, guna melindungi aplikasi web dari potensi serangan.

### 2.5.2 *Content Security Policy (CSP)*

*Content Security Policy (CSP)* berfungsi sebagai mekanisme keamanan yang dirancang untuk melindungi situs web dari ancaman seperti injeksi skrip dan serangan *XSS (Cross-Site Scripting)*. Tujuan utamanya adalah memberikan kontrol yang lebih besar terhadap sumber daya yang dapat dimuat oleh halaman web, dengan membatasi jenis konten yang dapat dieksekusi. Dengan membatasi sumber daya ini, *CSP* efektif mengurangi risiko serangan *XSS*, di mana penyerang berusaha menyisipkan dan menjalankan skrip berbahaya di dalam halaman web.

Cara kerjanya melibatkan izin bagi situs web untuk menentukan sumber daya mana yang diizinkan untuk dimuat. Hal ini dicapai dengan menambahkan kebijakan keamanan *HTTP* header ke respon *HTTP* dari server. *Header* ini memberikan petunjuk kepada browser untuk membatasi jenis sumber daya yang dapat dimuat oleh halaman web, sehingga mengurangi potensi eksploitasi celah keamanan.

Pentingnya *CSP* terletak pada kemampuannya untuk memberikan panduan jelas kepada browser mengenai sumber daya yang boleh dimuat, membantu mencegah penyerangan yang dapat merugikan pengguna situs web. Dengan mengimplementasikan *CSP*, pengembang dapat lebih efektif menjaga integritas dan keamanan situs web mereka[19].

### 2.5.3 *Cookie without SameSite Attribute*

Ketika sebuah cookie tidak memiliki atribut *SameSite*, dapat menimbulkan risiko keamanan terhadap privasi pengguna. Atribut *SameSite* pada *cookie* mengatur cara dan kapan cookie dikirimkan dalam permintaan lintas situs (cross-site). Jika *cookie* tidak memuat atribut *SameSite*, secara *default browser* akan

memperlakukannya sebagai *SameSite=Lax*, yang membatasi pengiriman *cookie* hanya untuk navigasi *GET* yang dimulai dari halaman asal.

Sebelum versi Chrome 80, jika sebuah cookie tidak memiliki atribut SameSite, browser dapat menganggapnya sebagai *SameSite=None*. Hal ini memungkinkan pengiriman cookie dalam konteks lintas situs, membuka potensi celah keamanan, terutama terkait dengan serangan *CSRF (Cross-Site Request Forgery)* dan menjaga privasi pengguna [20].

Pada tahun 2020, sejumlah browser seperti *Chrome, Firefox, Edge*, dan *Safari* mulai menerapkan perubahan kebijakan terkait pengiriman *cookie* lintas situs. Kini, atribut *SameSite* menjadi persyaratan untuk mendefinisikan perilaku *cookie*, memastikan perlindungan yang lebih baik terhadap privasi dan keamanan pengguna.

### 2.5.4 *Cookie Without Secure Flag*

Penggunaan *cookie* tanpa menetapkan *flag Secure* dapat menimbulkan potensi risiko keamanan bagi situs web. *Flag Secure* pada cookie menunjukkan bahwa *cookie* hanya boleh ditransmisikan melalui koneksi *HTTPS (SSL/TLS)*, dan seharusnya tidak dikirim melalui koneksi *HTTP* yang tidak aman. Jika cookie dikirim tanpa *flag Secure* melalui koneksi *HTTP*, hal ini dapat mengekspos informasi sensitif pengguna kepada potensi ancaman keamanan, seperti pengawasan oleh pihak yang tidak berwenang.

Implementasi *flag Secure* pada *cookie* memiliki peran krusial dalam menjaga keamanan informasi yang dikirimkan antara pengguna dan server, terutama pada halaman web yang melibatkan akses atau penyimpanan data sensitif seperti informasi login[21].

### 2.5.5 *Cross Site Scripting (Reflected)*

*Cross-Site Scripting (XSS)* adalah jenis serangan keamanan pada aplikasi web di mana penyerang menyisipkan skrip berbahaya ke dalam halaman web yang nantinya akan dieksekusi oleh pengguna akhir. Salah satu bentuk *XSS* adalah *Reflected XSS*.

*Reflected XSS* terjadi saat skrip berbahaya disisipkan ke dalam parameter permintaan, seperti *URL*, dan kemudian nilai tersebut dipantulkan kembali oleh aplikasi web ke dalam halaman *HTML*. Ketika pengguna mengakses halaman tersebut, mereka tanpa sengaja dapat menjalankan skrip berbahaya tersebut.

Sebagai contoh, bayangkan ada formulir pencarian yang menampilkan hasil langsung di halaman web. Jika seorang pengguna memasukkan teks berbahaya dalam formulir pencarian, dan aplikasi web secara langsung menampilkan hasil pencarian tersebut di halaman *HTML* tanpa melakukan validasi atau penyaringan input, skrip berbahaya dapat dieksekusi oleh pengguna yang melihat hasil pencarian[22].

### 2.5.6 *Cross-Domain Misconfiguration*

*Cross-Domain Misconfiguration* merupakan kondisi di mana sebuah aplikasi web tidak berhasil mengelola atau mengonfigurasi dengan tepat kebijakan keamanan lintas domain *(Cross-Origin Resource Sharing/CORS)*. Kondisi ini dapat membuka peluang terjadinya kerentanan terhadap serangan dan akses yang tidak sah dari domain yang berbeda.

*CORS*, yang merupakan singkatan dari *Cross-Origin Resource Sharing*, adalah suatu mekanisme keamanan yang diterapkan oleh peramban web untuk melindungi pengguna dari potensi serangan lintas domain. Mekanisme ini memastikan bahwa permintaan sumber daya dari satu domain tidak dapat diambil oleh domain lain kecuali jika domain peminta memberikan izin dengan tegas.

*Cross-Domain Misconfiguration* terjadi ketika pengembang atau administrator web gagal mengatur konfigurasi *CORS* secara benar. Kesalahan konfigurasi ini dapat terjadi akibat pengaturan yang terlalu longgar, yang memungkinkan akses dari semua domain tanpa pembatasan, atau sebaliknya, pengaturan yang terlalu ketat sehingga menghambat akses yang seharusnya diizinkan [23].

Sebagai contoh, jika suatu situs web di domain A tidak berhasil mengonfigurasi kebijakan *CORS* dengan tepat, seorang penyerang dapat

memanfaatkan kondisi ini dengan membuat situs web palsu di domain B. Dengan mencoba melakukan permintaan lintas domain ke situs di domain A, penyerang dapat berhasil mengakses sumber daya dari situs di domain A secara tidak sah, asalkan kebijakan *CORS* tidak secara efektif melarang akses dari domain B.

Memahami konsep ini adalah krusial dalam mengelola keamanan aplikasi web, dan kehati-hatian dalam mengonfigurasi *CORS* dapat membantu mencegah potensi serangan lintas domain. Menjaga keselarasan antara keamanan dan fungsionalitas aplikasi web menjadi kunci untuk memitigasi risiko *Cross-Domain Misconfiguration.*

### 2.5.7 *Missing Anti-Clickjacking Header*

*Missing Anti-Clickjacking Header* merujuk pada kondisi di mana suatu aplikasi web tidak menyertakan header keamanan yang dikenal sebagai *X-Frame-Options* untuk melindungi dari serangan *clickjacking*. *Clickjacking* merupakan jenis serangan di mana seorang penyerang dapat menyembunyikan elemen-elemen yang menyesatkan di atas halaman web yang sebenarnya, mengarahkan pengguna untuk melakukan tindakan tanpa pengetahuan mereka.

*Header X-Frame-Options* merupakan bagian integral dari langkah-langkah keamanan yang dapat diimplementasikan pada aplikasi web untuk melindungi dari potensi *clickjacking*. Header ini memberikan panduan kepada peramban (*browser*) mengenai izin untuk memuat halaman dalam suatu frame atau iframe. Tiga nilai umum yang digunakan dalam konfigurasi header ini melibatkan "*DENY*" (penolakan pemuatan dalam *frame*), "*SAMEORIGIN*" (hanya memungkinkan pemuatan dalam frame dengan origin yang sama), dan "*ALLOW-FROM*" (mengizinkan pemuatan dalam frame dari domain tertentu) [24].

Ketika sebuah aplikasi web tidak mengonfigurasi *header X-Frame-Options* dengan benar atau sama sekali tidak menyertakannya, hal tersebut membuat aplikasi rentan terhadap serangan *clickjacking*. Dalam skenario ini, seorang penyerang dapat mencoba memanipulasi cara halaman tersebut dimuat dalam frame

untuk melancarkan serangan yang dapat merugikan pengguna tanpa pengetahuan mereka.

Memahami perlunya pengaturan header *X-Frame-Options* menjadi penting dalam melindungi aplikasi web dari ancaman *clickjacking*. Oleh karena itu, para pengembang web seharusnya memastikan bahwa aplikasi mereka telah dikonfigurasi dengan benar untuk mencegah risiko *clickjacking* dan melindungi pengalaman pengguna secara keseluruhan.

### 2.5.8 *SQL Injection*

*SQL Injection* adalah bentuk serangan keamanan yang terjadi pada aplikasi web ketika seorang penyerang memanfaatkan kelemahan keamanan dalam input yang diterima oleh aplikasi. Dalam serangan ini, penyerang memasukkan perintah *SQL* yang berbahaya, memanipulasi input agar dapat dieksekusi oleh basis data terkait. Proses penyisipan perintah *SQL* yang berhasil memungkinkan penyerang untuk melakukan berbagai tindakan, termasuk mengakses, memodifikasi, atau bahkan menghapus data di dalam basis data.

Mekanisme serangan *SQL Injection* terjadi saat aplikasi web tidak melakukan validasi atau penyaringan yang memadai terhadap input yang diterima dari pengguna sebelum mengintegrasikannya ke dalam perintah *SQL*. Penyerang dapat memanfaatkan celah ini dengan menyisipkan perintah *SQL* manipulatif melalui formulir input, parameter *URL*, atau elemen input lainnya. Jika aplikasi tidak memproses input dengan cermat, perintah *SQL* yang disisipkan dapat dieksekusi oleh sistem basis data.

Dampak dari serangan *SQL Injection* sangat serius, mencakup akses tidak sah ke data yang bersifat sensitif, perusakan data, atau bahkan pengambilalihan kontrol atas aplikasi. Penyerang dapat menggunakan teknik ini untuk melakukan tindakan ilegal pada basis data, seperti membaca informasi pengguna atau meretas data keuangan [25].

Mencegah *SQL Injection* melibatkan praktik keamanan yang cermat, seperti penggunaan prepared statements atau *parameterized queries*, validasi input dengan

tepat, dan penerapan mekanisme otentikasi yang kuat. Pemahaman mendalam mengenai risiko *SQL Injection* serta tindakan pencegahan yang diperlukan merupakan langkah penting dalam menjaga keamanan aplikasi web dari ancaman serangan ini.

### 2.5.9 *Vulnerable JS Library*

*Vulnerable JS Library* merujuk pada kondisi di mana suatu aplikasi web menggunakan versi *JavaScript Library (JS)* yang diketahui memiliki kerentanan keamanan atau belum diperbaiki. Dalam konteks ini, penyerang dapat memanfaatkan kerentanan tersebut untuk melancarkan serangan terhadap aplikasi web dan pengguna akhir.

Penggunaan Perpustakaan *JavaScript* umumnya terjadi ketika aplikasi web ingin memperluas fungsionalitas atau meningkatkan pengalaman pengguna. Beberapa contoh *Javascript Library* yang populer termasuk *jQuery, React, Angular*, dan lainnya.

Kerentanan keamanan dapat muncul pada perpustakaan *JavaScript* sebagaimana pada perangkat lunak lainnya, entah karena adanya *bug*, celah keamanan, atau masalah lainnya. Jika aplikasi web menggunakan versi perpustakaan yang rentan, hal ini memberikan peluang bagi penyerang untuk mengeksploitasi kelemahan tersebut.

Dampak dari penggunaan perpustakaan yang rentan dapat sangat serius. Penyerang dapat memanfaatkan kerentanan dalam perpustakaan JavaScript untuk melancarkan berbagai jenis serangan, seperti serangan *XSS (Cross-Site Scripting)* atau serangan *CSRF (Cross-Site Request Forgery)*. Melalui eksploitasi kerentanan di perpustakaan yang digunakan oleh banyak aplikasi, penyerang memiliki potensi untuk merugikan banyak pengguna secara bersamaan[26].

Dengan demikian, penting bagi pengembang dan administrator web untuk secara aktif memonitor keamanan perpustakaan yang digunakan dalam aplikasi mereka. Tindakan preventif, seperti memperbarui perpustakaan ke versi yang lebih

aman, dapat membantu melindungi aplikasi web dari risiko keamanan yang disebabkan oleh *Javascript Library* yang rentan.

### 2.5.10 *X-Content-Type-Options Header Missing*

*X-Content-Type-Options Header Missing* mengindikasikan situasi di mana respon *HTTP* dari suatu situs web tidak menyertakan atau mengonfigurasi dengan benar header keamanan *X-Content-Type-Options*. Header ini difungsikan sebagai langkah keamanan yang ditetapkan oleh server web untuk mengurangi risiko serangan terhadap potensi kelemahan di dalam pengurai (parser) tipe konten pada *browser*. Tujuan utamanya adalah memaksa browser agar menghormati tipe konten yang telah dinyatakan oleh server, dan nilai yang umum digunakan untuk header ini adalah "*nosniff*"[27].

*Header X-Content-Type-Options* merupakan suatu langkah keamanan yang server terapkan dalam respon *HTTP*. Penggunaan nilai "*nosniff*" memberitahu browser untuk tidak mencoba mengubah atau menafsir ulang tipe konten dari apa yang telah dinyatakan oleh server.

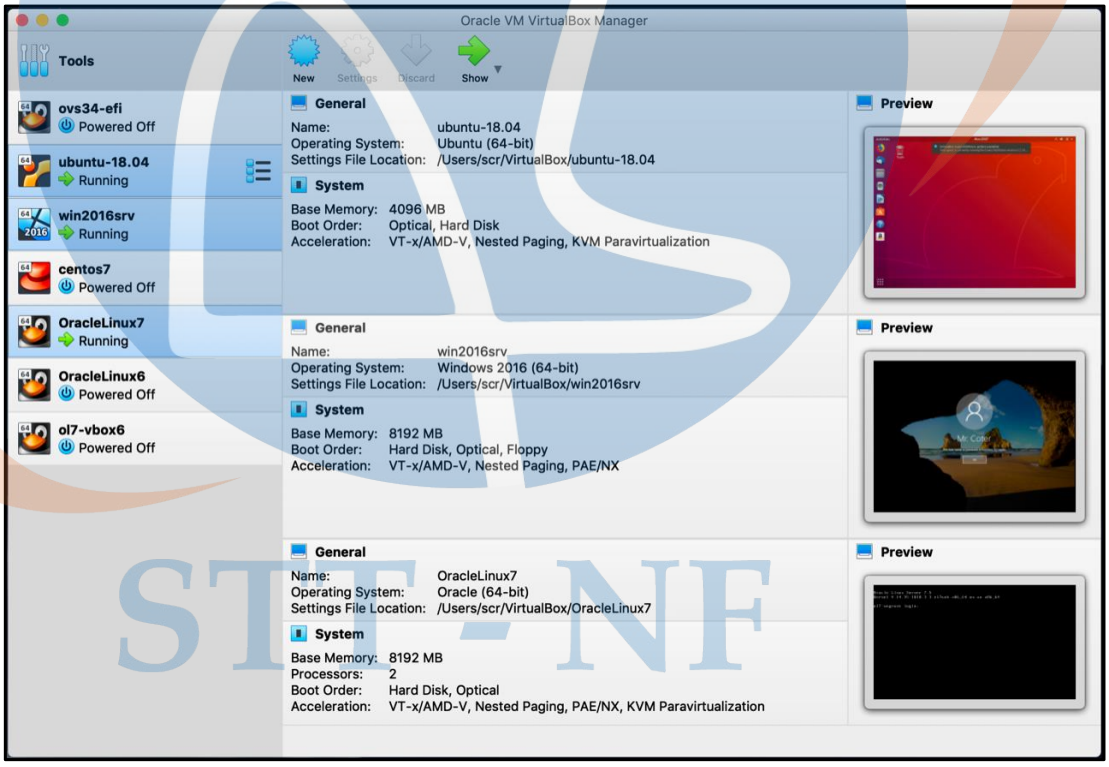
Ketika header *X-Content-Type-Options* tidak disertakan atau dikonfigurasi dengan benar pada respon *HTTP*, browser mungkin mencoba untuk menerjemahkan ulang tipe konten, yang membuka potensi risiko seperti serangan *MIME sniffing*. *MIME sniffing* terjadi ketika browser mencoba menentukan jenis file tanpa mematuhi tipe konten yang telah dinyatakan.

Dampak dari ketidaksetaraan ini dapat meningkatkan risiko keamanan, terutama jika situs web berisi konten yang dapat dianggap sebagai tipe konten yang berpotensi berbahaya, seperti skrip JavaScript yang seharusnya dieksekusi. Oleh karena itu, pentingnya penyertaan dan konfigurasi header X-Content-Type-Options yang tepat untuk memitigasi potensi risiko keamanan ini pada situs web. Para pengembang dan administrator web seharusnya memastikan bahwa langkah-langkah keamanan ini diimplementasikan dengan baik dalam konfigurasi server mereka.

## 2.6 *Oracle Virtual Box*

*VirtualBox*, dikembangkan oleh *Oracle Corporation*, adalah sebuah perangkat lunak virtualisasi yang memungkinkan pengguna untuk menciptakan dan menjalankan mesin virtual di dalam sistem operasi utama mereka. Dengan *VirtualBox*, pengguna dapat menjalankan beberapa sistem operasi secara bersamaan di satu komputer, yang dikenal sebagai "*host*".

Mesin virtual (*VM*) yang dihasilkan oleh *VirtualBox* dapat beroperasi secara independen dan terisolasi di dalam sistem operasi *host*. Ini memungkinkan pengguna untuk menjalankan sistem operasi yang berbeda-beda, seperti *Windows*, *Linux*, *macOS*, atau sistem operasi lainnya, tanpa mempengaruhi sistem operasi *host*[28].




*source:docs.oracle.com*

*Gambar 2.6 VirtualBox Manager*

*VirtualBox* mendukung berbagai sistem operasi *host*, termasuk *Windows*, *Linux*, *macOS*, dan *Oracle Solaris*. Fleksibilitas ini memungkinkan pengguna untuk

menjalankan aplikasi atau mengembangkan perangkat lunak di berbagai platform. Sistem operasi yang dijalankan di dalam mesin virtual disebut "*guest*," sementara sistem operasi utama di komputer disebut "*host*"[28].

Selain memberikan isolasi penuh antara host dan tamu untuk keamanan, *VirtualBox* juga memungkinkan pengguna untuk membuat snapshot atau salinan instan dari mesin virtual pada titik waktu tertentu. Ini memudahkan pengguna untuk kembali ke kondisi mesin virtual yang telah disimpan sebelumnya.

*VirtualBox* juga memiliki fitur ekstensi opsional, yaitu *Extension Pack*, yang menyediakan fungsionalitas tambahan. *Extension Pack* termasuk dukungan untuk perangkat *USB 2.0 dan 3.0*, enkripsi disk, remote desktop protocol (RDP), serta peningkatan performa grafis.

Dengan konsep ini, *VirtualBox* banyak digunakan oleh pengembang perangkat lunak, administrator sistem, dan pengguna umum untuk keperluan seperti uji coba perangkat lunak, pengembangan lintas-platform, dan isolasi lingkungan kerja[28]. *VirtualBox* tersedia sebagai sumber terbuka dan dapat diunduh secara gratis untuk penggunaan pribadi. Namun, pengguna bisnis perlu membeli lisensi komersial untuk beberapa fitur tambahan dan kebutuhan komersial.

## 2.7 Jenis Tes dalam *Pentesting*

1. Black Box Testing:
    a. Deskripsi: Tester tidak memiliki pengetahuan sebelumnya tentang sistem atau jaringan yang akan diuji.
    b. Tujuan: Mensimulasikan serangan dari pihak eksternal yang tidak memiliki pengetahuan internal sistem.
2. White Box Testing:
    a. Deskripsi: Tester memiliki pengetahuan penuh tentang sistem atau jaringan yang diuji, termasuk kode sumber, arsitektur, dan infrastruktur.
    b. Tujuan: Memberikan pemahaman mendalam tentang keamanan internal dan membantu mengidentifikasi potensi celah keamanan yang tidak dapat ditemukan dalam pengujian black box.

3. Gray Box Testing:
    a. Deskripsi: Kombinasi dari black box dan white box testing. Tester memiliki sebagian pengetahuan tentang sistem atau jaringan yang diuji.
    b. Tujuan: Memberikan keseimbangan antara serangan dari pihak eksternal dan internal.
4. Automated Testing:
    a. Deskripsi: Menggunakan alat otomatis untuk mengidentifikasi dan mengeksploitasi potensi celah keamanan.
    b. Tujuan: Menghemat waktu dan sumber daya dengan otomatisasi pengujian rutin.
5. Manual Testing:
    a. Deskripsi: Dilakukan oleh peneliti keamanan manusia untuk mengidentifikasi celah keamanan yang mungkin terlewat oleh alat otomatis.
    b. Tujuan: Menilai keamanan secara menyeluruh dan mendalam.
6. Network Penetration Testing:
    a. Deskripsi: Fokus pada pengujian keamanan jaringan, termasuk perangkat keras, perangkat lunak, dan konfigurasi jaringan.
    b. Tujuan: Mengidentifikasi dan mengeksploitasi potensi celah keamanan dalam infrastruktur jaringan.
7. Web Application Testing:
    a. Deskripsi: Memeriksa keamanan aplikasi web, termasuk pengujian SQL injection, cross-site scripting (XSS), dan kelemahan aplikasi web lainnya.
    b. Tujuan: Mengidentifikasi dan mengatasi celah keamanan pada aplikasi web.
8. Social Engineering:
    a. Deskripsi: Mencoba memanipulasi orang agar memberikan informasi rahasia atau mengambil tindakan tertentu.
    b. Tujuan: Menilai ketahanan organisasi terhadap serangan sosial dan mendidik pengguna agar lebih waspada.

9. Wireless Network Testing:
    a. Deskripsi: Fokus pada pengujian keamanan jaringan nirkabel.
    b. Tujuan: Mengevaluasi konfigurasi dan keamanan protokol nirkabel.
10. Physical Security Testing:
    a. Deskripsi: Menilai keamanan fisik suatu organisasi, termasuk akses fisik ke fasilitas dan perlindungan perangkat keras.

Penulis melakukan pengujian dengan menggunakan metode black box testing, automated testing, dan web application testing. Dikarenakan kurangnya pengetahuan sebelumnya terkait sistem atau jaringan yang akan diuji, penulis mengandalkan alat otomatis untuk mengidentifikasi dan mengeksploitasi potensi celah keamanan. Selain itu, penulis juga fokus pada pemeriksaan keamanan aplikasi web, termasuk uji SQL Injection, cross-site scripting (XSS), dan kelemahan lain yang mungkin ada pada aplikasi web.

*Tabel 2.2 Tabel Penelitian Terkait*

| No | Nama dan Tahun | Judul | Subjek | Hasil |
|---|---|---|---|---|
| 1 | Xiong, W., Legrand, E., Åberg, O., & Lagerström, R. (2022) | *Cyber security threat modeling based on the MITRE Enterprise ATT&CK Matrix* | *Software and Systems Modeling* | Mengembangkan metode pemodelan ancaman keamanan siber berdasarkan *MITRE ATT&CK Matrix* |
| 2 | Oruc, A., Amro, A., & Gkioulos, V. (2022) | *Assessing Cyber Risks of an INS Using the MITRE ATT&CK Framework* | *MITRE ATT&CK Framework* | Mengevaluasi risiko siber pada sistem kontrol industri (INS) dengan menggunakan *MITRE ATT&CK Framework* |

| No | Nama dan Tahun | Judul | Subjek | Hasil |
|---|---|---|---|---|
| 3 | Georgiadou, A., Mouzakitis, S., & Askounis, D. (2021) | *Assessing mitre att&ck risk using a cyber-security culture framework* | *MITRE ATT&CK Framework* | Menggunakan *cyber-security culture framework* untuk menilai risiko yang terkait dengan *MITRE ATT&CK* |
| 4 | Grigorescu, O., Nica, A., Dascalu, M., & Rughinis, R. (2022) | *CVE2ATT&CK: BERT-Based Mapping of CVEs to MITRE ATT&CK Techniques. Algorithms* | *MITRE ATT&CK Framework* | Menjelaskan desain dan filosofi di balik *MITRE ATT&CK Framework* |
| 5 | Strom, B. E., Applebaum, A., Miller, D. P., Nickels, K. C., Pennington, A. G., & Thomas, C. B. (n.d.) (2020) | *MITRE ATT&CK®: Design and Philosophy* | *MITRE ATT&CK Framework* | Menggunakan pemetaan berbasis BERT untuk menghubungkan *CVEs (Common Vulnerabilities and Exposures)* dengan teknik *MITRE ATT&CK* |
| 6 | Mahajan, A. (n.d.) (2014) | *Burp Suite essentials : discover the secrets of web* | Keamanan Aplikasi Web | Memperkenalkan *Burp Suite* sebagai alat untuk pengujian keamanan aplikasi web |

| No | Nama dan Tahun | Judul | Subjek | Hasil |
|---|---|---|---|---|
| | | *application pentesting using Burp Suite, the best tool for the job* | | |
| 7 | Ahmad Dahlan Yogyakarta Indonesia, U., & Ananda Raharja, P. (2019) | *Vulnerability Analysis of E-voting Application using Open Web Application Security Project (OWASP) Framework* | Keamanan Aplikasi E-voting | Menganalisis kerentanan dalam aplikasi *E-voting* dengan menggunakan kerangka kerja OWASP |
| 8 | Devi, R. S., & Kumar, M. M. (2020) | *Testing for Security Weakness of Web Applications using Ethical Hacking* | Keamanan Aplikasi Web | Mendeskripsikan pengujian kelemahan keamanan aplikasi web dengan menggunakan teknik ethical hacking |
| 9 | Baklizi, M., Atoum, I., Abdullah, N., Al-Wesabi, O. A., Ali Otoom, A., & Al | *A Technical Review of SQL Injection Tools and Methods: A Case Study of SQL Map* | *SQL Injection* | Menyajikan tinjauan teknis alat dan metode *SQL Injection* dengan studi kasus menggunakan *SQL Map* |

| No | Nama dan Tahun | Judul | Subjek | Hasil |
|---|---|---|---|---|
| | Sheikh Hasan, M. (n.d.) (2022) | | | |
| 10 | Rashid, S. M. Z. U., Kamrul, M. I., & Islam, A. (2019) | *Understanding the Security Threats of Esoteric Subdomain Takeover and Prevention Scheme* | Ancaman Keamanan Subdomain | Mempelajari ancaman keamanan yang terkait dengan pengambilalihan subdomain dan upaya pencegahannya |

Sejumlah penelitian terkait keamanan siber telah memberikan kontribusi yang signifikan dalam pemahaman dan penanganan risiko siber. Xiong, W., et al. (2022), menciptakan pendekatan pemodelan ancaman keamanan siber berbasis MITRE Enterprise ATT&CK Matrix sebagai landasan kerangka kerja, memperkaya pemahaman dan respons terhadap ancaman keamanan. Penelitian Oruc, A., et al. (2022), mengevaluasi risiko siber pada sistem kontrol industri (INS) dengan menggunakan MITRE ATT&CK Framework, menyoroti pentingnya penilaian risiko dalam melindungi infrastruktur kritis.

Lebih lanjut, Georgiadou, A., et al. (2021), mengenalkan pendekatan baru dengan menggunakan kerangka kerja budaya keamanan siber untuk menilai risiko terkait dengan MITRE ATT&CK. Ini menegaskan peran budaya keamanan dalam merumuskan strategi yang efektif. Sementara itu, Strom, B. E., et al. (n.d.), menjelaskan desain dan filosofi di balik MITRE ATT&CK Framework, memberikan wawasan mendalam tentang pendekatan yang digunakan dalam pengembangan kerangka kerja tersebut.

Grigorescu, O., et al. (2022), mengadopsi pendekatan berbasis teknologi dengan menggunakan pemetaan berbasis BERT untuk menghubungkan CVEs dengan teknik MITRE ATT&CK, memungkinkan identifikasi dan penanganan kerentanan yang lebih efisien. Di sisi lain, Mahajan, A. (n.d.), memperkenalkan Burp Suite sebagai alat esensial untuk pengujian keamanan aplikasi web, menunjukkan bahwa pemahaman praktis terhadap alat-alat tersebut juga memiliki dampak besar dalam memitigasi risiko.

Penelitian Ahmad Dahlan Yogyakarta Indonesia, U., & Ananda Raharja, P. (2019), menganalisis kerentanan dalam aplikasi E-voting dengan menggunakan kerangka kerja OWASP, sementara Devi, R. S., & Kumar, M. M. (2020), memberikan deskripsi mendalam tentang pengujian kelemahan keamanan aplikasi web dengan teknik ethical hacking. Baklizi, M., et al. (n.d.), menyajikan tinjauan teknis alat dan metode SQL Injection dengan studi kasus menggunakan SQL Map, memberikan pandangan yang kaya terkait dengan serangan khusus ini.

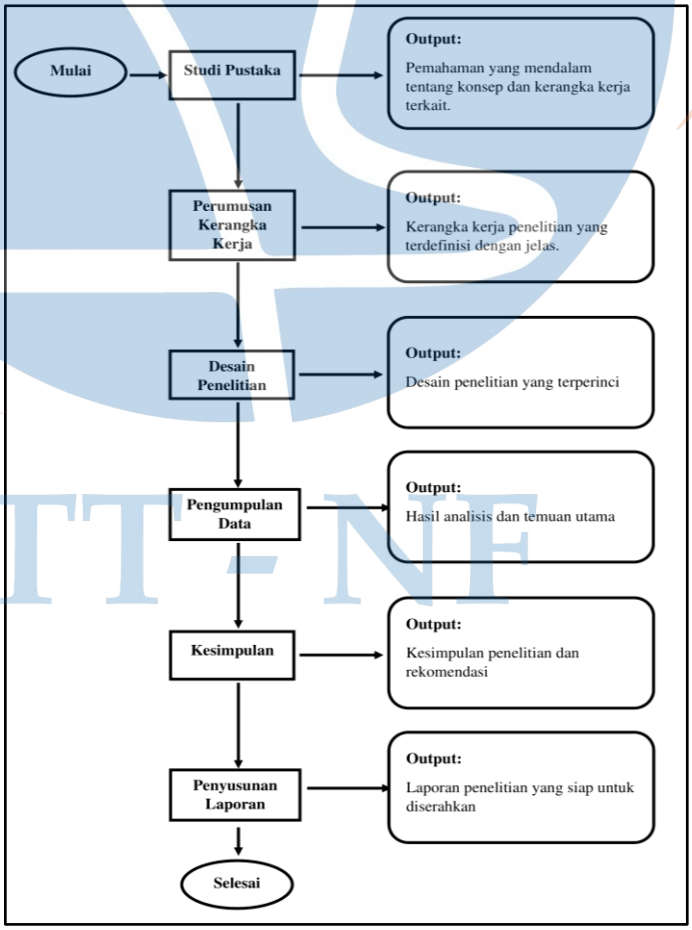
Terakhir, Rashid, S. M. Z. U., et al. (2019), memfokuskan perhatian pada ancaman keamanan yang terkait dengan pengambilalihan subdomain dan upaya pencegahannya, menyoroti kebutuhan untuk memahami dan melindungi lapisan keamanan yang mungkin terlupakan. Melalui penelitian ini, kontribusi berharga telah diberikan dalam menghadapi berbagai tantangan keamanan siber di era digital saat ini.

Dalam tugas akhir ini, penulis mengadopsi kerangka kerja MITRE ATT&CK Matrix untuk melakukan analisis kerentanan terhadap situs web PT. Nurul Fikri Cipta Inovasi. Penulis akan mengevaluasi risiko siber yang mungkin dihadapi oleh situs web tersebut dengan mengidentifikasi serangan potensial dan menerapkan langkah-langkah pencegahan yang sesuai. Penelitian sebelumnya seperti Xiong et al. (2022) dan Oruc et al. (2022) telah menginspirasi penulis dalam memperkuat metodologi red team dengan fokus pada kerentanan yang relevan dengan lingkungan perusahaan teknologi dan pendidikan seperti yang dihadapi oleh PT. Nurul Fikri Cipta Inovasi.

# BAB III
# METODOLOGI PENELITIAN

Dalam Bab 3, penelitian ini akan memaparkan secara mendalam tahapan penelitian dan rancangan metodologi yang digunakan. Pada bagian ini, setiap langkah penelitian akan dijabarkan secara sistematis, dimulai dari pemilihan metode penelitian yang paling sesuai hingga pelaksanaan eksperimen atau pengumpulan data lapangan. Rincian mengenai instrumen atau teknik pengumpulan data juga akan diuraikan secara terperinci untuk memastikan kejelasan dan reproduktibilitas proses penelitian. Selanjutnya, bab ini akan menjelaskan validitas dan reliabilitas dari metode yang diterapkan

## 3.1 Tahapan Penelitian




*Gambar 3.1* Tahapan Penelitian

## 3.2 Rancangan Penelitian

Penelitian ini dirancang dengan beberapa tahapan yang mencakup analisis lingkungan/studi kasus, pendefinisian, kebutuhan, pengolahan data, metode eksperimen, metode evaluasi, serta sebuah kerangka penelitian yang menggambarkan pemanfaatan konsep dan metode.

Tahap awal penelitian melibatkan analisis lingkungan keamanan siber organisasi yang menjadi subjek penelitian. Ini mencakup pemahaman tentang infrastruktur IT, kebijakan keamanan yang ada, dan sejarah serangan siber sebelumnya. Selain itu, studi kasus akan mengidentifikasi area-area yang rentan dan risiko potensial.

Setelah analisis lingkungan, penelitian akan mendefinisikan kebutuhan untuk pengujian postur keamanan. Ini mencakup tujuan eksperimen, parameter yang akan dievaluasi, serta lingkup serangan yang akan disimulasikan. Selama eksperimen, data akan dikumpulkan berdasarkan respons tim keamanan terhadap serangan simulasi. Data ini akan diproses untuk analisis lebih lanjut.

Eksperimen dilakukan dengan merancang dan meluncurkan serangan simulasi sesuai dengan skenario yang telah ditentukan. Ini mencakup penggunaan *MITRE ATT&CK Framework* sebagai panduan dalam merancang serangan. Evaluasi dilakukan berdasarkan parameter yang telah ditentukan pada tahap pendefinisian kebutuhan. Ini mencakup analisis data yang telah dikumpulkan selama eksperimen.

Kerangka penelitian mencakup konsep-konsep dan metode yang digunakan dalam penelitian. Ini mencakup pemahaman tentang *Red team, MITRE ATT&CK Framework*, dan teori keamanan informasi yang digunakan sebagai landasan penelitian.

Rancangan penelitian ini menjadi panduan dalam melaksanakan penelitian untuk memastikan bahwa langkah-langkah yang diambil sesuai dengan tujuan penelitian dan metode yang telah ditentukan.

Selanjutnya rancangan penelitian dapat didetailkan kembali sesuai sub-sub bab di bawah ini:

### 3.2.1 Jenis Penelitian

Penelitian ini termasuk dalam kategori penelitian eksperimen. Jenis penelitian eksperimen dipilih karena kami akan melaksanakan serangkaian serangan simulasi *(red team)* dan mengukur respons serta efektivitasnya.

Penelitian eksperimen adalah jenis penelitian yang dirancang untuk menguji hipotesis atau teori tertentu dengan mengendalikan faktor-faktor yang mempengaruhi fenomena yang diteliti. Dalam konteks penelitian ini, kami akan merancang dan melaksanakan serangan siber simulasi menggunakan *MITRE ATT&CK Framework* sebagai panduan.

Output dari penelitian ini adalah pemahaman yang lebih baik tentang efektivitas penggunaan *MITRE ATT&CK Framework* dalam *red team* dalam pengujian postur keamanan organisasi. Selain itu, penelitian ini juga akan menghasilkan identifikasi celah keamanan yang mungkin ada dalam pertahanan siber organisasi yang menjadi subjek penelitian. Output-output kunci penelitian ini termasuk:

1. Analisis mendalam tentang efektivitas penggunaan *MITRE ATT&CK Framework* dalam *red team*.
2. Identifikasi taktik dan teknik yang berhasil dieksploitasi oleh *red team*.
3. Evaluasi respons dan kemampuan tim keamanan dalam menghadapi serangan simulasi.
4. Dampak penggunaan *MITRE ATT&CK Framework* pada perbaikan kebijakan dan prosedur keamanan.
5. Kesimpulan mengenai sejauh mana penggunaan *MITRE ATT&CK Framework* dapat membantu dalam meningkatkan postur keamanan organisasi.

### 3.2.2 Metode Analisis

Metode analisis yang akan digunakan dalam penelitian ini, *red team* akan menggunakan dua metode analisis, yaitu analisis deskriptif dan analisis data kualitatif dan kuantitatif.

**Deskriptif:**

1. Identifikasi Taktik dan Teknik Penyerangan: Analisis akan dimulai dengan mengidentifikasi taktik dan teknik penyerangan yang digunakan oleh *red team* dalam serangan simulasi. Ini mencakup pengklasifikasian taktik dan teknik yang digunakan sesuai dengan *MITRE ATT&CK Framework*.
2. Evaluasi Respons Tim Keamanan: Pada penelitian ini akan menggambarkan dan menganalisis respons yang diberikan oleh tim keamanan siber dalam menghadapi serangan. Ini mencakup respons yang diambil, waktu respons, dan efektivitas respons.
3. Pengukuran Efektivitas: Pada penelitian ini akan menggunakan metrik yang sesuai untuk mengukur efektivitas respons dan dampak serangan. Metrik ini dapat mencakup lamanya waktu yang diperlukan untuk mendeteksi serangan, tingkat keberhasilan dalam mencegah serangan, dan sejauh mana kerusakan dihindari.
4. Analisis Dampak Penggunaan *MITRE ATT&CK Framework*: Pada penelitian ini akan menggambarkan dampak penggunaan *MITRE ATT&CK Framework* dalam proses *red team*. Ini mencakup apakah penggunaan *framework* ini membantu tim red team dalam merancang serangan yang realistis dan efektif, serta apakah itu membantu tim keamanan siber dalam memahami dan menghadapi serangan tersebut.
5. Penyusunan Kesimpulan: Berdasarkan hasil analisis deskriptif, Pada penelitian ini akan menyusun kesimpulan yang merangkum temuan utama penelitian ini. Kesimpulan ini akan memberikan gambaran tentang efektivitas penggunaan *MITRE ATT&CK Framework* dalam *red team* dan dampaknya terhadap keamanan siber organisasi.

**Kualitatif dan Kuantitatif:**

1. Analisis Kualitatif: Data kualitatif akan dianalisis untuk mengidentifikasi pola, tren, dan temuan yang muncul selama pelaksanaan serangan dan respons tim keamanan. Ini akan melibatkan kategorisasi data, identifikasi tema, dan penafsiran makna dari respons tim keamanan.

2. Analisis Kuantitatif: Data kuantitatif akan dianalisis menggunakan metode statistik, seperti uji-t, analisis regresi, dan perhitungan rasio. Ini akan membantu dalam mengukur secara kuantitatif efektivitas penggunaan *MITRE ATT&CK Framework* dan dampaknya pada perbaikan kebijakan keamanan.

### 3.2.3 Metode Pengumpulan Data

Dalam penelitian ini, data akan dikumpulkan melalui berbagai metode, termasuk penggunaan log serangan dan keamanan, serta dokumentasi *MITRE ATT&CK Framework.*

1. Penggunaan Log Serangan dan Keamanan:
   a. Data *log* serangan akan dikumpulkan dari sistem keamanan organisasi yang menjadi subjek penelitian. Ini mencakup *log* kejadian terkait dengan serangan siber yang terdeteksi dan *log* aktivitas jaringan yang mencakup lalu lintas masuk dan keluar dari jaringan. Data *log* keamanan ini akan digunakan untuk merekam serangan simulasi yang dilakukan oleh *red team*.
   b. Data *log* keamanan juga akan digunakan untuk mengidentifikasi respons dan tindakan yang diambil oleh tim keamanan dalam merespons serangan simulasi.
2. Dokumentasi *MITRE ATT&CK Framework*:
   a. Dokumentasi resmi *MITRE ATT&CK Framework*, termasuk taktik, teknik, dan prosedur yang digunakan oleh penyerang dalam *framework* ini, akan dijadikan referensi utama dalam merancang serangan simulasi. Ini termasuk deskripsi lengkap tentang setiap taktik dan teknik yang terdapat dalam *framework* ini.
   b. Dokumentasi akan digunakan sebagai panduan untuk merancang serangan yang mencerminkan serangan yang mungkin terjadi di dunia nyata. Ini akan mencakup langkah-langkah, alat, dan teknik yang dapat digunakan oleh *red team*.

### 3.2.4 Lingkungan Pengembangan

1. *Framework MITRE ATT&CK: Framework MITRE ATT&CK* akan menjadi landasan utama dalam pengembangan dan pelaksanaan *red team*. Peneliti akan menggunakan *framework* ini untuk merancang taktik dan teknik serangan serta *red team* untuk mengevaluasi respons tim keamanan.
2. *Tools Red team*: Peneliti akan menggunakan sejumlah perangkat lunak dan perangkat keras yang umumnya digunakan dalam . Ini termasuk alat pemindaian jaringan, perangkat lunak simulasi serangan, dan alat manajemen keamanan.
3. Internet: Koneksi internet yang stabil diperlukan untuk mengakses sumber daya daring yang dibutuhkan selama penelitian.
4. Lokasi Penelitian: Penelitian akan dilaksanakan di lokasi yang ditentukan oleh organisasi yang menjadi subjek penelitian

### 3.2.5 Waktu Penelitian

1. Persiapan (1 bulan):
   a. Pemilihan subjek penelitian.
   b. Persiapan alat dan lingkungan pengembangan.
   c. Rancangan skenario dan serangan simulasi.
2. Pelaksanaan Penelitian (1 minggu):
   a. Pelaksanaan serangan simulasi.
   b. Pengumpulan data melalui observasi, wawancara, survei, dan dokumentasi.
3. Analisis Data (1 minggu):
   a. Analisis deskriptif
4. Penarikan Kesimpulan (1 minggu):
   a. Penyusunan kesimpulan berdasarkan analisis data.
5. Penyelesaian dan Publikasi (2 minggu):
   a. Penyelesaian final laporan penelitian.

### 3.2.6 Metode Pengujian

Pengujian dalam penelitian ini akan fokus pada evaluasi efektivitas penggunaan *MITRE ATT&CK Framework* dalam *red team*. Berikut adalah metode pengujian yang akan digunakan:

1. Pengujian *Red team*: *Red team* akan melaksanakan serangkaian serangan simulasi menggunakan *MITRE ATT&CK Framework* sebagai panduan. Serangan ini akan mencakup berbagai taktik dan teknik yang sering digunakan oleh penyerang siber. Pengujian ini akan menghasilkan data tentang bagaimana serangan simulasi dilaksanakan.
2. Pengukuran Hasil Serangan: Hasil serangan simulasi akan diukur berdasarkan taktik dan teknik yang berhasil dieksploitasi. Ini mencakup identifikasi celah keamanan yang berhasil dimanfaatkan dan sejauh mana *Framework MITRE ATT&CK* membantu dalam mengidentifikasi celah tersebut.
3. Pengumpulan Data: Data akan dikumpulkan melalui berbagai metode, termasuk wawancara dengan anggota *red team* dan tim keamanan siber, observasi langsung, dan dokumentasi hasil serangan simulasi.

### 3.2.7 Metode Implementasi dan Evaluasi

**Implementasi:**

Implementasi dalam penelitian ini berkaitan dengan langkah-langkah praktis yang akan diambil untuk melaksanakan serangan simulasi dan mengukur efektivitas penggunaan *MITRE ATT&CK Framework*. Berikut adalah metode implementasi yang akan digunakan:

1. Pemilihan Organisasi Subjek: Organisasi yang menjadi subjek penelitian akan dipilih berdasarkan kerja sama dan izin dari organisasi tersebut. Hal ini mencakup perundingan awal, persetujuan untuk melaksanakan *red team*, dan akses ke sumber daya yang diperlukan.
2. Pengembangan Skenario Serangan: *Red team* akan merancang serangkaian skenario serangan yang mencakup berbagai taktik dan teknik yang relevan.

Skenario ini akan mencerminkan ancaman nyata dan menjadi dasar pelaksanaan serangan simulasi.

3. Pelaksanaan Serangan Simulasi: *Red team* akan melaksanakan serangan simulasi sesuai dengan skenario yang telah direncanakan. Mereka akan mencoba untuk mengidentifikasi celah keamanan dan mengukur efektivitas tim keamanan siber dalam merespons serangan.

**Evaluasi:**

Evaluasi adalah langkah penting dalam penelitian ini, yang bertujuan untuk mengukur efektivitas penggunaan *MITRE ATT&CK Framework* dan dampaknya. Berikut adalah metode evaluasi yang akan digunakan:

1. Pengukuran Hasil Serangan: Hasil serangan simulasi akan diukur berdasarkan taktik dan teknik yang berhasil dieksploitasi. Dampak serangan, sejauh mana celah keamanan berhasil dimanfaatkan, dan efektivitas respons akan diukur.
2. Analisis Data Kualitatif dan Kuantitatif: Data yang diperoleh dari berbagai sumber, termasuk hasil serangan, survei, dan wawancara, akan dianalisis secara kualitatif dan kuantitatif untuk mengidentifikasi pola dan tren. Analisis ini akan membantu dalam menarik kesimpulan tentang efektivitas penggunaan *MITRE ATT&CK Framework*.
3. Penarikan Kesimpulan: Berdasarkan hasil evaluasi, penarikan kesimpulan akan disusun. Kesimpulan ini akan mencakup sejauh mana penggunaan *MITRE ATT&CK Framework* membantu dalam merancang serangan simulasi yang realistis dan memperbaiki postur keamanan organisasi.

# BAB IV
# IMPLEMENTASI DAN EVALUASI

Dalam Bab 4, penelitian ini akan mendetailkan tahapan implementasi serta melakukan evaluasi terhadap hasil yang diperoleh. Bagian ini akan menguraikan proses penerapan konsep atau metode yang telah dijelaskan dalam Bab 3 ke dalam konteks praktis. Langkah-langkah pelaksanaan, peran masing-masing variabel atau komponen, serta interaksi yang terjadi akan dipresentasikan dengan jelas.

Selanjutnya, bab ini akan membahas evaluasi terhadap implementasi tersebut, termasuk analisis keberhasilan, kendala yang dihadapi, dan solusi yang diterapkan selama proses implementasi. Data hasil evaluasi akan dianalisis secara kritis, mempertimbangkan relevansi dengan tujuan penelitian serta mencermati dampak positif yang diharapkan. Keseluruhan, Bab 4 bertujuan untuk memberikan gambaran komprehensif mengenai bagaimana konsep atau metode yang telah dijelaskan dalam Bab 3 diaplikasikan dalam konteks nyata, serta hasil dan evaluasi yang dihasilkan dari implementasi tersebut.

## 4.1 Analisisa dan Perancangan

### 4.1.1 Analisisa Topik Penelitian

Dalam tahap analisis ini, penelitian memfokuskan perhatian pada pemahaman mendalam terkait penggunaan *MITRE ATT&CK Framework* dalam *red team* dan pengujian postur keamanan. Evaluasi taktik dan teknik yang umumnya digunakan oleh penyerang dalam keamanan siber menjadi dasar untuk memahami sejauh mana *MITRE ATT&CK Framework* dapat merepresentasikan dan mengatasi risiko-risiko ini.

Analisis mencakup pemahaman mendalam tentang bagaimana serangan siber biasanya terjadi dan metode-metode apa yang paling sering digunakan oleh

penyerang. Pemahaman ini diperoleh melalui studi literatur terkait, laporan keamanan, dan tren terkini dalam serangan siber.

Evaluasi kemampuan *MITRE ATT&CK Framework* untuk mencakup tren terbaru dan mengakomodasi perubahan cepat dalam metode penyerangan menjadi fokus utama. Langkah-langkah ini membantu memastikan bahwa *red team* yang dijalankan mencerminkan ancaman-ancaman yang terkini dan relevan bagi organisasi yang sedang diuji.

### 4.1.2 Perancangan Pendekatan Penelitian

Perancangan pendekatan penelitian bertujuan untuk merinci strategi dan langkah-langkah yang akan diambil untuk menjawab pertanyaan-pertanyaan penelitian dan mencapai tujuan penelitian. Dalam konteks ini, perancangan pendekatan penelitian menitikberatkan pada penggunaan *MITRE ATT&CK Framework* dalam *red team* dan evaluasi postur keamanan.

Pertama, perancangan melibatkan pemilihan metode pengumpulan data yang sesuai. Ini mencakup observasi langsung terhadap *red team*, wawancara mendalam dengan anggota *red team*, dan analisis dokumen dan laporan yang terkait dengan penggunaan *MITRE ATT&CK Framework.*

Selanjutnya, perancangan mencakup pengembangan kerangka kerja atau panduan bagi tim red team. Hal ini bertujuan untuk memaksimalkan pemanfaatan *MITRE ATT&CK Framework*, termasuk cara mengidentifikasi celah keamanan, merancang serangan berdasarkan taktik dan teknik tertentu, dan berkomunikasi secara efektif dengan tim keamanan.

Langkah-langkah perancangan juga melibatkan pemilihan studi kasus atau skenario simulasi yang relevan untuk mengevaluasi efektivitas penggunaan *MITRE ATT&CK Framework.* Selain itu, perancangan mencakup definisi parameter dan metrik evaluasi yang sesuai untuk mengukur keberhasilan dan dampak dari *red team.*

### 4.1.3 Analisa Kebutuhan Sistem

**Kebutuhan *Hardware***

*Tabel 4.1* Tabel Kebutuhan *Hardware* 1

| Komponen | Spesifikasi Minimum | Spesifikasi yang digunakan |
|---|---|---|
| *Processor* | Pentium 4 atau processor AMD64 | Intel® Core™ i5-3210M Processor (2,5 GHz, Cache 3MB) |
| *RAM* | 512MB | 12GB |
| *Storage Memory* | 10GB | 300GB |
| *VGA* | 128MB | Intel HD Graphics 4000 |

Sistem yang terdapat dalam Tabel 1 menampilkan konfigurasi hardware yang jauh melampaui persyaratan minimum yang diperlukan. Dalam hal processor, di mana spesifikasi minimum mencakup Pentium 4 atau processor AMD64, sistem ini menggunakan Intel Core i5-3210M Processor dengan kecepatan 2,5 GHz dan cache 3MB. Selain itu, meskipun persyaratan RAM minimum hanya 512MB, sistem ini telah ditingkatkan dengan kapasitas sebesar 12GB. Hal serupa terjadi pada storage memory, di mana persyaratan minimumnya adalah 10GB, tetapi sistem ini dilengkapi dengan kapasitas penyimpanan sebesar 300GB. Begitu pula, untuk VGA atau Video Graphics Accelerator, di mana persyaratan minimumnya membutuhkan setidaknya 128MB, sistem ini menggunakan Intel HD Graphics 4000.



Tabel *4.2* Tabel Kebutuhan *Hardware* 2

| Komponen | Spesifikasi Minimum | Spesifikasi yang digunakan |
|---|---|---|
| *Processor* | Pentium 4 atau processor AMD64 | AMD Ryzen™ 5 7535HS 6-Core / 12-Thread Max Boost Clock 4.55 GHz |
| *RAM* | 512MB | 16GB |

| Komponen | Spesifikasi Minimum | Spesifikasi yang digunakan |
|---|---|---|
| *Storage Memory* | 10GB | 512GB |
| *VGA* | 128MB | AMD Radeon 660M dan RX 6550M |

Spesifikasi hardware pada Tabel 2 menunjukkan bahwa sistem ini memiliki konfigurasi yang jauh melebihi persyaratan minimum yang dibutuhkan. Dalam hal processor, di mana persyaratan minimum termasuk Pentium 4 atau processor AMD64, sistem ini mengadopsi AMD Ryzen™ 5 7535HS dengan 6-Core / 12-Thread dan Max Boost Clock hingga 4.55 GHz. Kapasitas RAM yang minimal diperlukan adalah 512MB, namun, sistem ini memiliki RAM sebesar 16GB. Demikian pula, untuk storage memory, di mana persyaratan minimum adalah 10GB, sistem ini dilengkapi dengan kapasitas penyimpanan sebesar 512GB. Untuk VGA atau *Video Graphics Accelerator*, di mana persyaratan minimum membutuhkan setidaknya 128MB, sistem ini menggunakan AMD Radeon 660M dan RX 6550M.

**Kebutuhan *Software***

Tabel *4.3* Tabel Kebutuhan *Software*

| Kategori | Kebutuhan | Penjelasan |
|---|---|---|
| *Operating System* | *Linux Distribution (Kali Linux, Ubuntu, Parrot OS,* dan sebagainya.) | Diperlukan untuk menjalankan sebagian besar *tools* dan *framework* keamanan. |
| *Penetration Testing Tools* | *Metasploit, Burp Suite, Wireshark, Nmap,* dan sebagainya. | *Tools* ini diperlukan untuk menjalankan serangan dan menganalisis keamanan jaringan dan aplikasi. |

| Kategori | Kebutuhan | Penjelasan |
|---|---|---|
| *Virtualization* | *VirtualBox*, *VMware*, atau hypervisor lainnya | Diperlukan untuk membuat lingkungan uji coba yang terisolasi dan dapat dipulihkan. |
| *MITRE ATT&CK Framework* | *ATT&CK* dan *Navigator*, *ATT&CK Matrix* | Diperlukan untuk merencanakan, melacak, dan menganalisis serangan berdasarkan matriks *MITRE ATT&CK*. |

Diperlukan sistem operasi yang mendukung untuk melaksanakan sejumlah alat dan kerangka keamanan yang umum digunakan. Oleh karena itu, esensial untuk memiliki Linux Distribution seperti Kali Linux, Ubuntu, atau Parrot OS, yang menyediakan berbagai alat dan dukungan yang diperlukan untuk pengujian keamanan.

Tidak kalah pentingnya adalah kebutuhan akan seperangkat alat pengujian penetrasi yang sesuai. Alat-alat seperti Metasploit, Burp Suite, Wireshark, dan Nmap menjadi krusial untuk menjalankan serangan dan menganalisis keamanan jaringan serta aplikasi. Misalnya, Metasploit digunakan untuk pengujian penetrasi dan eksploitasi, Burp Suite untuk menguji aplikasi web, Wireshark untuk menganalisis lalu lintas jaringan, dan Nmap untuk melakukan pemindaian jaringan.

Selain itu, untuk menciptakan lingkungan uji coba yang aman dan terisolasi, kebutuhan akan virtualisasi sangat penting. Pengguna memerlukan platform virtualisasi seperti VirtualBox, VMware, atau hypervisor lainnya. Dengan adanya virtualisasi, mereka dapat membuat mesin virtual independen untuk mengisolasi dan menguji skenario keamanan tanpa mempengaruhi sistem operasi utama.

Terakhir, untuk merencanakan, melacak, dan menganalisis serangan berdasarkan matriks MITRE ATT&CK, kebutuhan akan ATT&CK dan Navigator, serta ATT&CK Matrix, menjadi krusial. Framework ATT&CK memberikan wawasan tentang teknik dan taktik yang bisa digunakan oleh penyerang, sementara

ATT&CK Matrix memberikan gambaran visual tentang penggunaan teknik-teknik tersebut dalam serangan. Gabungan ini digunakan sebagai panduan untuk meningkatkan pertahanan dan deteksi serangan secara menyeluruh.

### 4.1.4 Perancangan Sistem

1. Tujuan Sistem

   Melakukan pengujian keamanan untuk mengidentifikasi dan memitigasi potensi risiko keamanan berdasarkan *MITRE ATT&CK Framework.*

2. Arsitektur Umum
   a. *Pentester Workbench*
   b. Menggunakan OS Linux (Kali Linux)
   c. Terinstal perangkat lunak seperti *Metasploit, Burp Suite, Wireshark,* dan *Nmap*.
   *d.* Terhubung ke jaringan virtual yang diatur menggunakan *virtualization software.*
   e. Server Uji Coba
   f. Menyediakan lingkungan terisolasi untuk uji coba.
   g. Terpasang *OS server* dan perangkat lunak pendukung.
   h. Terkoneksi ke jaringan virtual untuk simulasi serangan.
   *i. MITRE ATT&CK Navigator*
   j. Menggunakan *ATT&CK Navigator* untuk merencanakan dan melacak serangan.
   k. *Matrix ATT&CK* digunakan untuk memvisualisasikan teknik dan taktik yang digunakan.
3. Proses Uji Coba
   a. *Reconnaissance*:
   b. Penggunaan *OSINT* dan *tools* seperti Recon-ng.
   c. *Matrix ATT&CK* digunakan untuk menentukan teknik *reconnaissance* yang akan diuji.
   d. *Initial Access*:
   e. Penggunaan *Metasploit* untuk simulasi serangan awal.

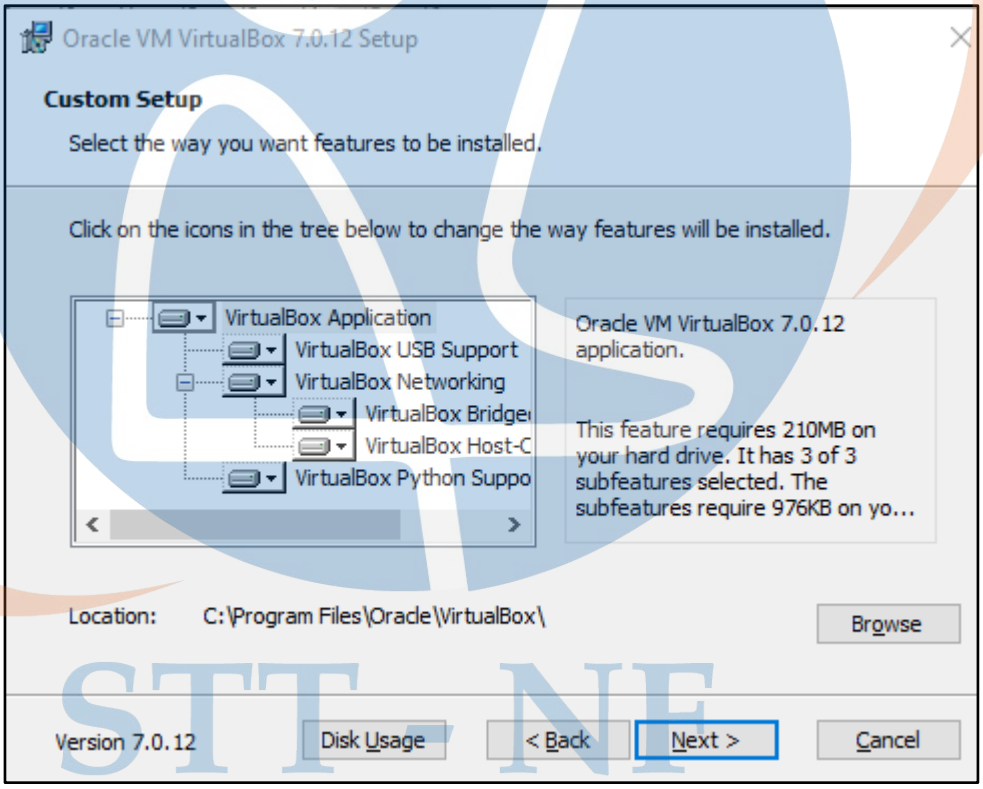
f. *Matrix ATT&CK* digunakan untuk mencocokkan teknik *initial access* yang berhasil.
g. *Execution, Persistence, Privilege Escalation*:
h. Penggunaan *tools* seperti *PowerShell Empire*.
i. Pemantauan *Matrix ATT&CK* untuk melihat dampak serangan pada tingkat eksekusi, persistensi, dan eskalasi hak akses.
j. *Defense Evasion, Credential Access*:
k. Penggunaan tools dan teknik untuk menghindari deteksi dan mendapatkan kredensial.
l. *Matrix ATT&CK* digunakan untuk mencocokkan teknik pertahanan yang dihindari dan kredensial yang diperoleh.
m. *Discovery, Lateral Movement*:
n. Menggunakan *tools* seperti *BloodHound* untuk pemindaian dan pergerakan lateral.
o. *Matrix ATT&CK* digunakan untuk mencocokkan teknik penemuan dan pergerakan lateral.
p. *Collection, Exfiltration*:
q. Simulasi pengumpulan data dan ekstraksi data.
r. *Matrix ATT&CK* digunakan untuk mencocokkan teknik pengumpulan dan ekstraksi.
s. *Impact:*
t. Simulasi dampak serangan terhadap sistem dan data.
u. *Matrix ATT&CK* digunakan untuk melihat dampak serangan secara keseluruhan.

4. Analisis dan Pelaporan
   a. Penggunaan *ATT&CK Navigator* untuk menyusun laporan hasil dan rekomendasi.
   b. Membuat laporan hasil, termasuk temuan dan rekomendasi.
5. Keamanan dan Kepatuhan
   a. Mematuhi kebijakan keamanan dan regulasi yang berlaku.
   b. Memastikan keamanan data dan informasi selama dan setelah uji coba.

## 4.2 Implementasi

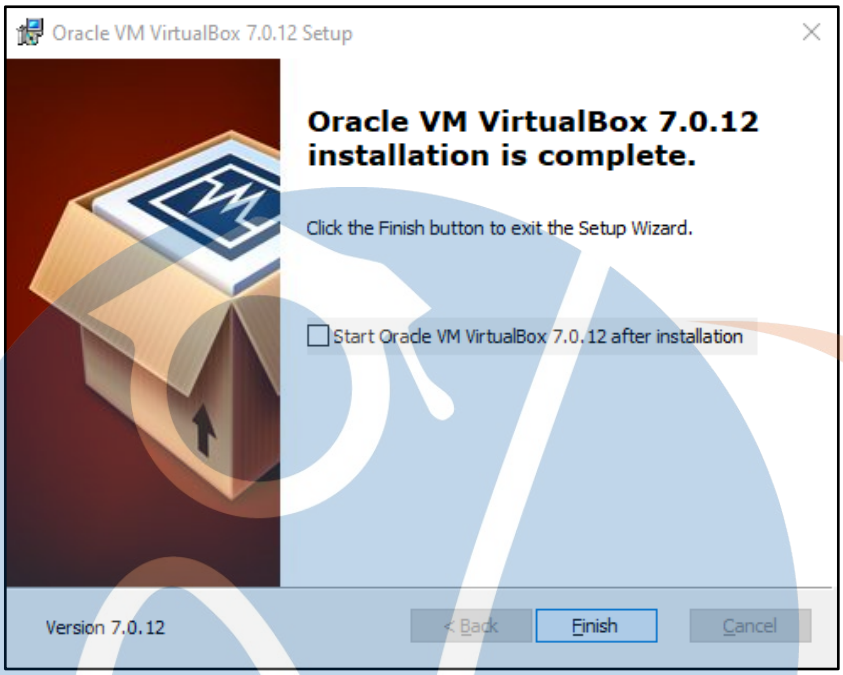
### 4.2.1 Memasang *Oracle VirtualBox*

1. Unduh *Oracle VirtualBox* dari situs resmi yang beralamat di: https://www.virtualbox.org/wiki/Downloads, kemudian pada bagian *platform packages* pilih *Windows hosts.*
2. Apabila sudah selesai buka hasil unduhan yang sudah selesai dan jalankan program untuk instalasi *Oracle VirtualBox.*
3. Pada bagian ini bisa pilih ingin dimana tempat untuk memasang *Oracle VirtualBox,* pada gambar dibawah ini peneliti memasang di *C:\ProgramFiles\Oracle\VirtualBox\.*




*Gambar 4.1* Tampilan disaat menentukan lokasi pemasangan

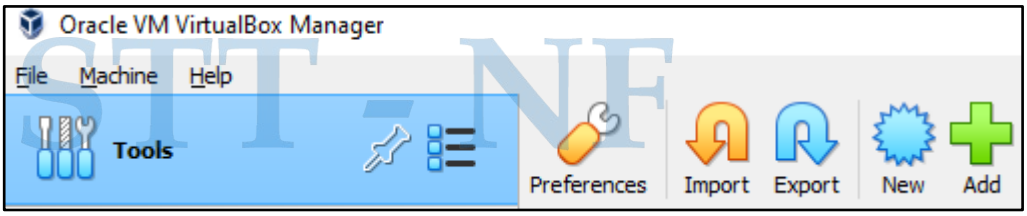
4. Setelah itu bisa pilih *next* dan tunggu proses pemasangan selesai.




*Gambar 4.2* Tampilan ketika proses pemasangan sudah selesai

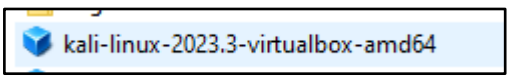
### 4.2.2 Memasang dan Konfigurasi *Kali Linux* di *Oracle VirtualBox*

1. Unduh terlebih dahulu *image Kali Linux* di situs resmi *Kali Linux* yang beralamat di: https://www.kali.org/get-kali/#kali-virtual-machines, kemudian pilih yang *VirtualBox.*
2. Setelah selesai mengunduh *image Kali Linux* ekstrak ke dalam sebuah *folder* dan buka *Oracle VirtualBox* dan pilih *Add.*



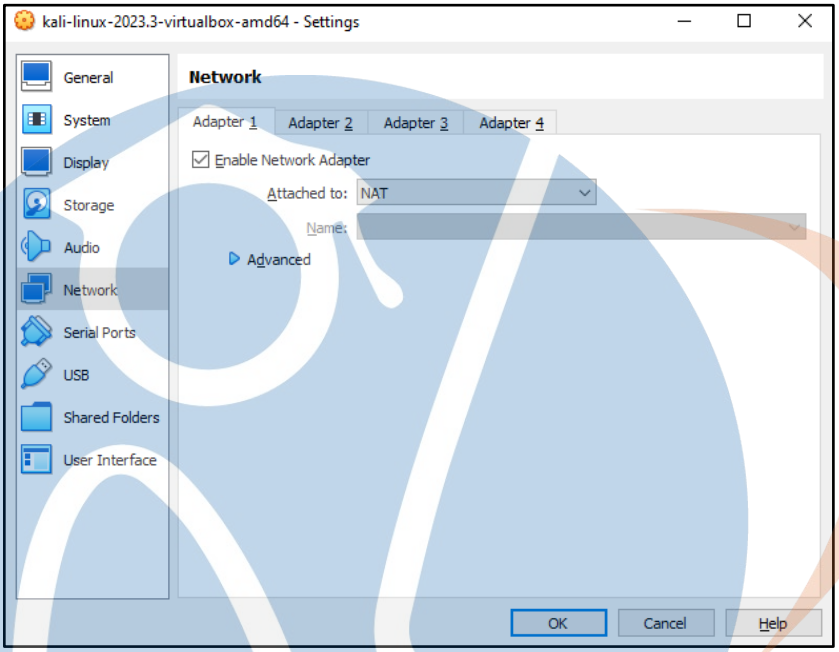

*Gambar 4.3* Tampilan pilihan yang ada di *Oracle VirtualBox*

3. Pilih *image* kali-linux-2023.3-virtualbox-amd64 lalu *open.*

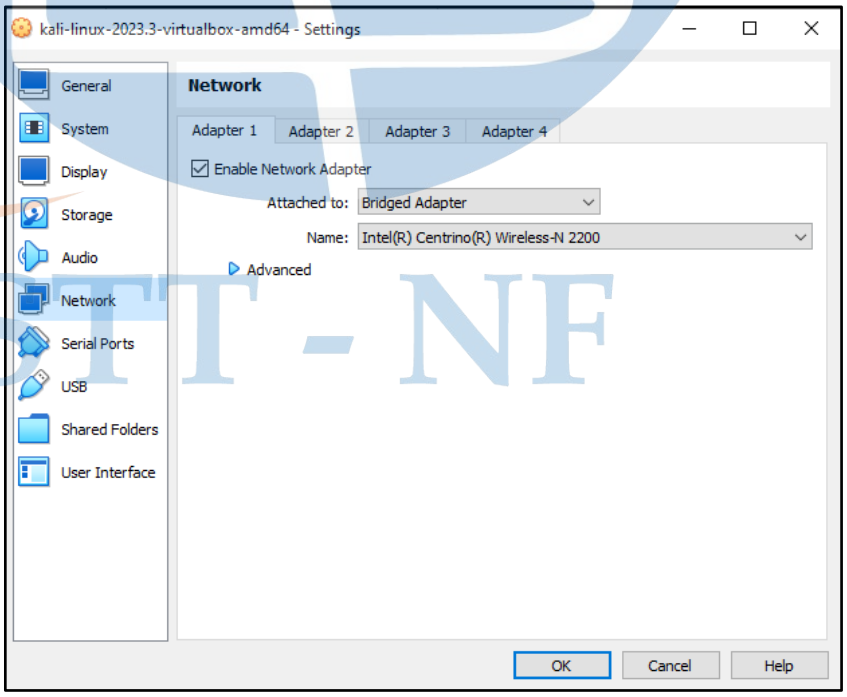



*Gambar 4.4 Image Kali Linux* yang akan digunakan

4. Sebelum menjalankan *Kali Linux* terdapat konfigurasi yang harus dilakukan, buka *settings* lalu ke menu *Network.* Dibagian *Attached to* yang awalnya *NAT* ubah ke *Bridged Adapter*.




Gambar 4.5 Sebelum di ubah ke *Bridged Adapter*




Gambar 4.6 Sesudah di ubah ke *Bridged Adapter*

Berikut penjelasan dari masing masing pengaturan *Network* di *Oracle VirtualBox*:

1. *NAT (Network Address Translation)*:
    a. Dengan menggunakan *NAT*, mesin virtual dapat terhubung ke jaringan luar melalui alamat *IP host* (komputer fisik).
    b. Ini menyembunyikan alamat IP mesin virtual di belakang alamat *IP host*, dan memungkinkan mesin virtual untuk berkomunikasi dengan internet.
    c. *NAT* sangat berguna jika Anda ingin mesin virtual dapat mengakses internet, tetapi tidak memerlukan akses langsung dari internet ke mesin virtual.
2. *Bridged Adapter*:
    a. Menggunakan *Bridged Adapter* memungkinkan mesin virtual untuk menjadi bagian dari jaringan fisik yang sama dengan *host*.
    b. Mesin virtual akan mendapatkan alamat IP unik di jaringan fisik, seperti halnya komputer fisik lainnya.
    c. Opsi ini berguna jika Anda ingin mesin virtual dapat diakses secara langsung dari komputer lain di jaringan, atau jika Anda ingin mesin virtual terlihat sebagai entitas terpisah di jaringan.
3. *Internal Network*:
    a. *Internal Network* memungkinkan komunikasi antara mesin virtual yang terhubung ke jaringan internal tersebut.
    b. Tidak ada koneksi langsung ke jaringan fisik atau internet, hanya komunikasi antara mesin virtual yang terhubung ke internal network yang sama.
    c. Opsi ini dapat digunakan untuk membuat jaringan pribadi antara beberapa mesin virtual.
4. *Host-Only Adapter*:
    a. *Host-Only Adapter* membatasi akses mesin virtual hanya pada host dan mesin virtual lainnya yang terhubung ke adapter yang sama.
    b. Mesin virtual dengan pengaturan ini tidak dapat berkomunikasi dengan mesin di luar *host* atau mesin virtual lainnya yang terhubung ke adapter jaringan yang berbeda.

5. *Generic Driver*:
    a. *Generic Driver* adalah opsi serba guna yang memungkinkan pengguna menentukan setelan jaringan secara manual.
    b. Ini memungkinkan pengguna untuk mengonfigurasi parameter jaringan sesuai kebutuhan spesifik.

### 4.3 Pengujian

*Penetration Testing* yang dilakukan dalam penelitian ini menggunakan *framework MITRE ATT&CK* dengan metode *Black Box* yang berjalan di sistem operasi *Kali Linux*.

#### 4.3.1 *Reconnaissance* (TA0043)

Pengintaian terdiri dari teknik-teknik yang melibatkan musuh secara aktif atau pasif mengumpulkan informasi yang dapat digunakan untuk mendukung penargetan. Informasi tersebut mungkin mencakup rincian organisasi korban, infrastruktur, atau staf/personel. Informasi ini dapat dimanfaatkan oleh musuh untuk membantu dalam fase-fase lain dari siklus musuh, seperti menggunakan informasi yang dikumpulkan untuk merencanakan dan melaksanakan Akses Awal, untuk menetapkan dan memprioritaskan tujuan pasca-kompromi, atau untuk mendorong dan memimpin upaya pengintaian lebih lanjut.

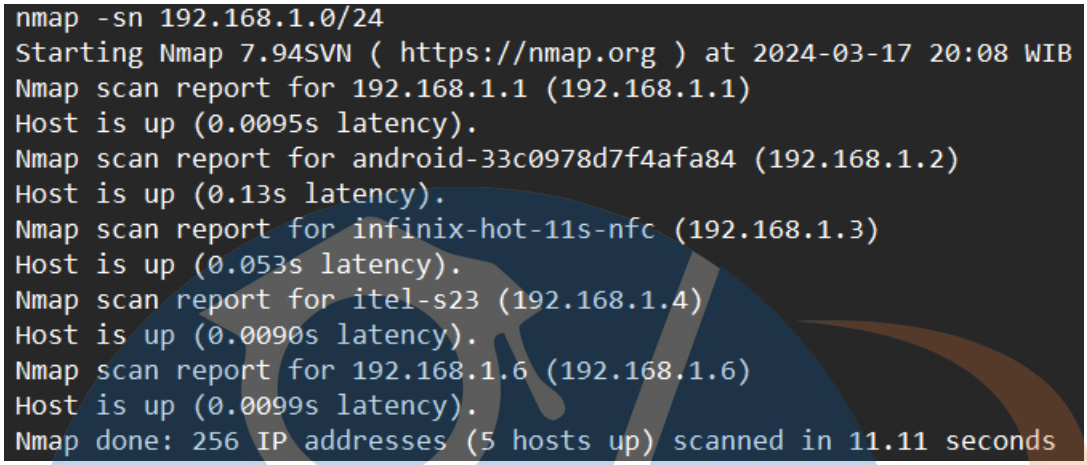
***Active Scanning* (T1595)**

Musuh bisa melakukan pengintaian yang aktif untuk kumpulkan informasi yang nantinya mereka pakai dalam menargetkan. Pada pengintaian aktif, musuh menyelidiki infrastruktur korban lewat lalu lintas jaringan, beda dengan jenis pengintaian lain yang tak melibatkan kontak langsung.

***Scanning IP Blocks* (T1595.001)**

Musuh bisa memindai blok IP korban untuk kumpulkan informasi yang berguna dalam menargetkan mereka. Alamat IP publik bisa diberikan kepada organisasi dalam bentuk blok, atau rentang alamat berurutan.

Hasil Scanning IP Blocks menggunakan NMAP dari Alamat IP yang rentan:



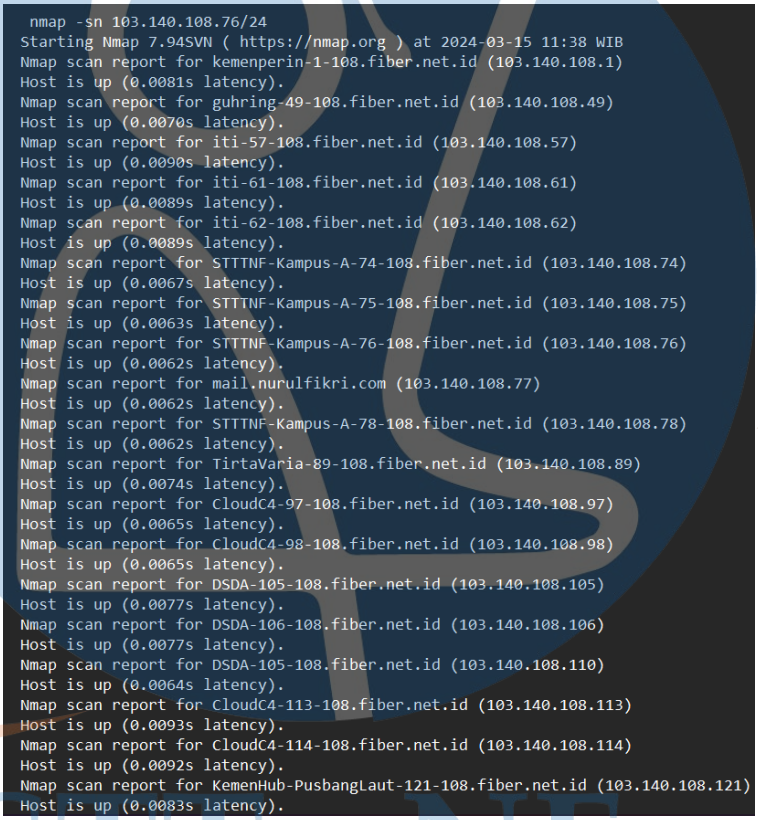

*Gambar 4.7* Hasil *ip blocks scanning nmap ip address* rentan

1. Nmap scan report for 192.168.1.1 (192.168.1.1):
   a. Ini menunjukkan bahwa ada perangkat dengan alamat IP 192.168.1.1 di dalam jaringan.
   b. Host tersebut aktif dengan latency (waktu respon) sekitar 0.0095 detik.
2. Nmap scan report for android-33c0978d7f4afa84 (192.168.1.2):
   a. Ini menunjukkan bahwa ada perangkat dengan alamat IP 192.168.1.2 di dalam jaringan.
   b. Host tersebut aktif dengan latency sekitar 0.13 detik.
3. Nmap scan report for infinix-hot-11s-nfc (192.168.1.3):
   a. Ini menunjukkan bahwa ada perangkat dengan alamat IP 192.168.1.3 di dalam jaringan.
   b. Host tersebut aktif dengan latency sekitar 0.053 detik.
4. Nmap scan report for itel-s23 (192.168.1.4):
   a. Ini menunjukkan bahwa ada perangkat dengan alamat IP 192.168.1.4 di dalam jaringan.
   b. Host tersebut aktif dengan latency sekitar 0.0090 detik.
5. Nmap scan report for 192.168.1.6 (192.168.1.6):
   a. Ini menunjukkan bahwa ada perangkat dengan alamat IP 192.168.1.6 di dalam jaringan.

b. Host tersebut aktif dengan latency sekitar 0.0099 detik.

6. Nmap done: 256 IP addresses (5 hosts up) scanned in 11.11 seconds:
   a. Nmap telah memindai total 256 alamat IP dalam jaringan.
   b. Dari 256 alamat IP tersebut, hanya 5 di antaranya yang aktif (up).
   c. Proses pemindaian selesai dalam waktu 11.11 detik.

Hasil Scanning IP Block menggunakan NMAP dari Alamat IP task.nurulfikri.com, esertifikat.nurulfikri.com dan learning.nurulfikri.com




*Gambar 4.8* Hasil *ip blocks scanning ip address* pengujian

1. Nmap scan report for kemenperin-1-108.fiber.net.id (103.140.108.1):
   a. Menunjukkan bahwa ada perangkat dengan nama "kemenperin-1-108.fiber.net.id" dan alamat IP 103.140.108.1 dalam jaringan.
   b. Host tersebut aktif dengan latency (waktu respon) sekitar 0.0081 detik.

2. Nmap scan report for guhring-49-108.fiber.net.id (103.140.108.49):
    a. Menunjukkan bahwa ada perangkat dengan nama "guhring-49-108.fiber.net.id" dan alamat IP 103.140.108.49 dalam jaringan.
    b. Host tersebut aktif dengan latency sekitar 0.0070 detik.
3. Nmap scan report for iti-57-108.fiber.net.id (103.140.108.57):
    a. Menunjukkan bahwa ada perangkat dengan nama "iti-57-108.fiber.net.id" dan alamat IP 103.140.108.57 dalam jaringan.
    b. Host tersebut aktif dengan latency sekitar 0.0090 detik.
4. Nmap scan report for iti-61-108.fiber.net.id (103.140.108.61):
    a. Menunjukkan bahwa ada perangkat dengan nama "iti-61-108.fiber.net.id" dan alamat IP 103.140.108.61 dalam jaringan.
    b. Host tersebut aktif dengan latency sekitar 0.0089 detik.
5. Nmap scan report for iti-62-108.fiber.net.id (103.140.108.62):
    a. Menunjukkan bahwa ada perangkat dengan nama "iti-62-108.fiber.net.id" dan alamat IP 103.140.108.62 dalam jaringan.
    b. Host tersebut aktif dengan latency sekitar 0.0089 detik.

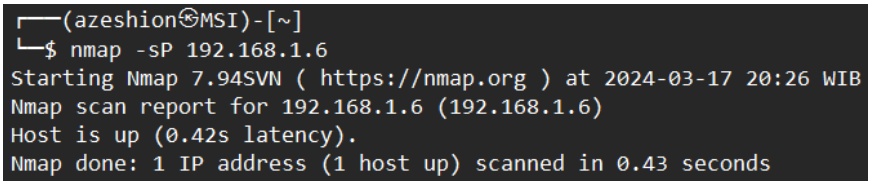
Dan seterusnya hingga ke perangkat terakhir yang ditemukan dalam jaringan.

6. Nmap done: 256 IP addresses (49 hosts up) scanned in 2.15 seconds:
    a. Merupakan ringkasan hasil pemindaian.
    b. Nmap telah memindai total 256 alamat IP dalam jaringan.
    c. Dari 256 alamat IP tersebut, 49 di antaranya aktif (up).
    d. Proses pemindaian selesai dalam waktu 2.15 detik.

***Vulnerability Scanning* (T1595.002)**

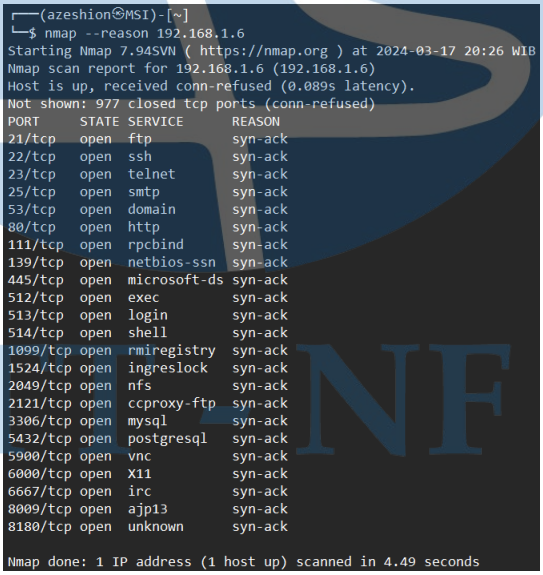
Penyerang bisa memindai korban untuk mencari kerentanan yang dapat digunakan selama menargetkan. Pemindaian kerentanan biasanya memeriksa apakah konfigurasi tuan rumah/aplikasi target (misalnya: perangkat lunak dan versi) secara potensial sesuai dengan sasaran eksploitasi spesifik yang mungkin ingin digunakan oleh penyerang.

Hasil Vulnerability Scanning menggunakan NMAP pada IP yang rentan:




*Gambar 4.9* Hasil *vulnerability scanning 1* pada *ip address rentan*

1. Nmap scan report for 192.168.1.6 (192.168.1.6):
   a. Menunjukkan bahwa host dengan alamat IP 192.168.1.6 dalam jaringan Anda aktif.
   b. Waktu respons (latency) dari host tersebut adalah sekitar 0.42 detik.
2. Nmap done: 1 IP address (1 host up) scanned in 0.43 seconds:
   a. Merupakan ringkasan hasil pemindaian.
   b. Nmap telah memindai satu alamat IP.
   c. Dari satu alamat IP tersebut, satu host terdeteksi aktif (up).
   d. Proses pemindaian selesai dalam waktu 0.43 detik.

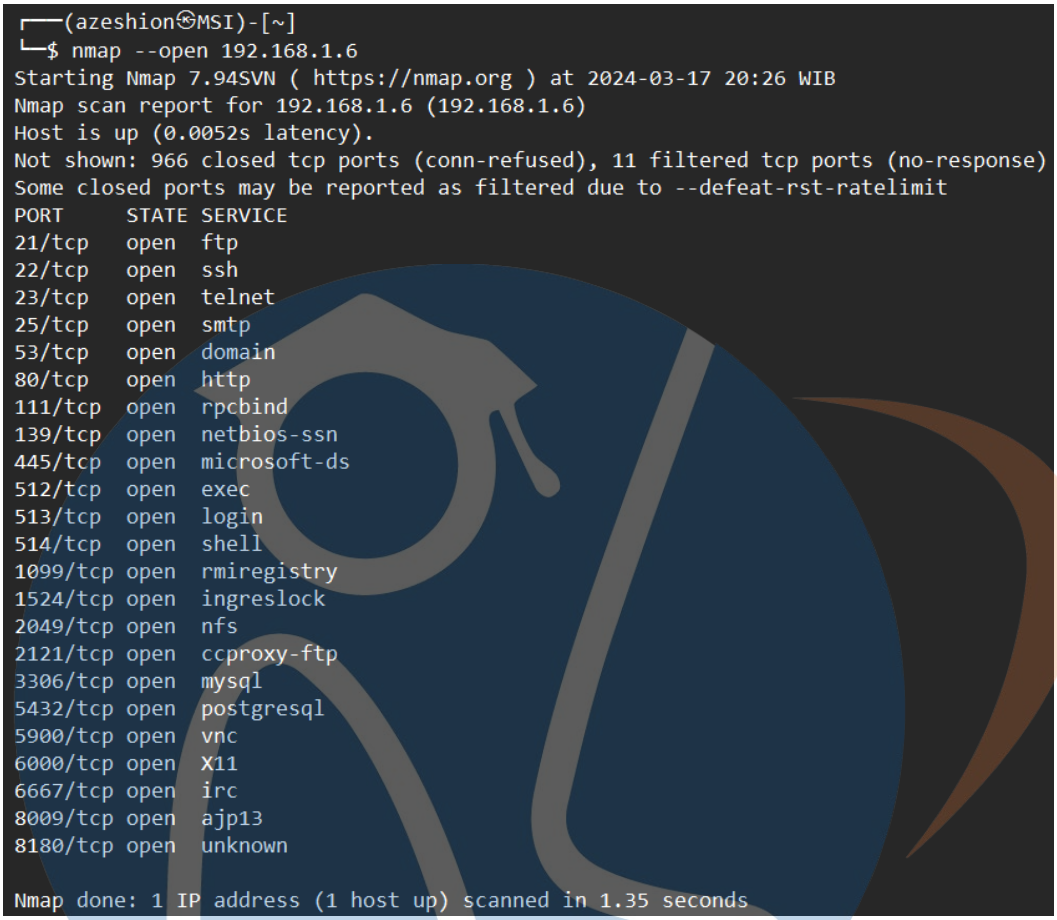



*Gambar 4.10* Hasil *vulnerability scanning 2* pada *ip address rentan*

1. Nmap scan report for 192.168.1.6 (192.168.1.6):
   a. Menunjukkan bahwa host dengan alamat IP 192.168.1.6 aktif dalam jaringan Anda.

b. Latensi (waktu respons) dari host tersebut adalah sekitar 0.089 detik.

2. Not shown: 977 closed tcp ports (conn-refused):
   a. Menunjukkan bahwa terdapat 977 port TCP yang ditutup dan Nmap menerima respon "connection refused" dari port-port tersebut.
3. PORT STATE SERVICE REASON:
   a. Menunjukkan daftar port-port yang terbuka beserta status dan alasan.
4. 21/tcp open ftp syn-ack:
   a. Port 21 (FTP) terbuka dan Nmap menerima respon "syn-ack" (synchronize-acknowledge) dari port tersebut.
5. 22/tcp open ssh syn-ack:
   a. Port 22 (SSH) terbuka dan Nmap menerima respon "syn-ack" dari port tersebut.
6. 23/tcp open telnet syn-ack:
   a. Port 23 (Telnet) terbuka dan Nmap menerima respon "syn-ack" dari port tersebut.
   b. Dan seterusnya untuk setiap port yang terbuka.
7. Nmap done: 1 IP address (1 host up) scanned in 4.49 seconds:
   a. Merupakan ringkasan hasil pemindaian.
   b. Nmap telah memindai satu alamat IP.
   c. Dari satu alamat IP tersebut, satu host terdeteksi aktif (up).
   d. Proses pemindaian selesai dalam waktu 4.49 detik.




*Gambar 4.11* Hasil *vulnerability scanning 3* pada *ip address rentan*

1. Nmap scan report for 192.168.1.6 (192.168.1.6):
   a. Menunjukkan bahwa host dengan alamat IP 192.168.1.6 dalam jaringan Anda aktif.
   b. Waktu respons (latency) dari host tersebut adalah sekitar 0.0052 detik.
2. Port-port yang Terbuka:

Dari hasil scanning, terdapat beberapa port TCP yang terbuka (open), yaitu:

a. 21/tcp : FTP
b. 22/tcp : SSH
c. 23/tcp : Telnet
d. 25/tcp : SMTP
e. 53/tcp : Domain
f. 80/tcp : HTTP

g. 111/tcp : RPCbind
h. 139/tcp : NetBIOS-SSN
i. 445/tcp : Microsoft-DS (SMB)
j. 512/tcp : Exec
k. 513/tcp : Login
l. 514/tcp : Shell
m. 1099/tcp : RMI Registry
n. 1524/tcp : Ingreslock
o. 2049/tcp : NFS
p. 2121/tcp : CCProxy-FTP
q. 3306/tcp : MySQL
r. 5432/tcp : PostgreSQL
s. 5900/tcp : VNC (Virtual Network Computing)
t. 6000/tcp : X11 (X Window System)
u. 6667/tcp : IRC (Internet Relay Chat)
v. 8009/tcp : AJP13 (Apache JServ Protocol)
w. 8180/tcp : Unknown

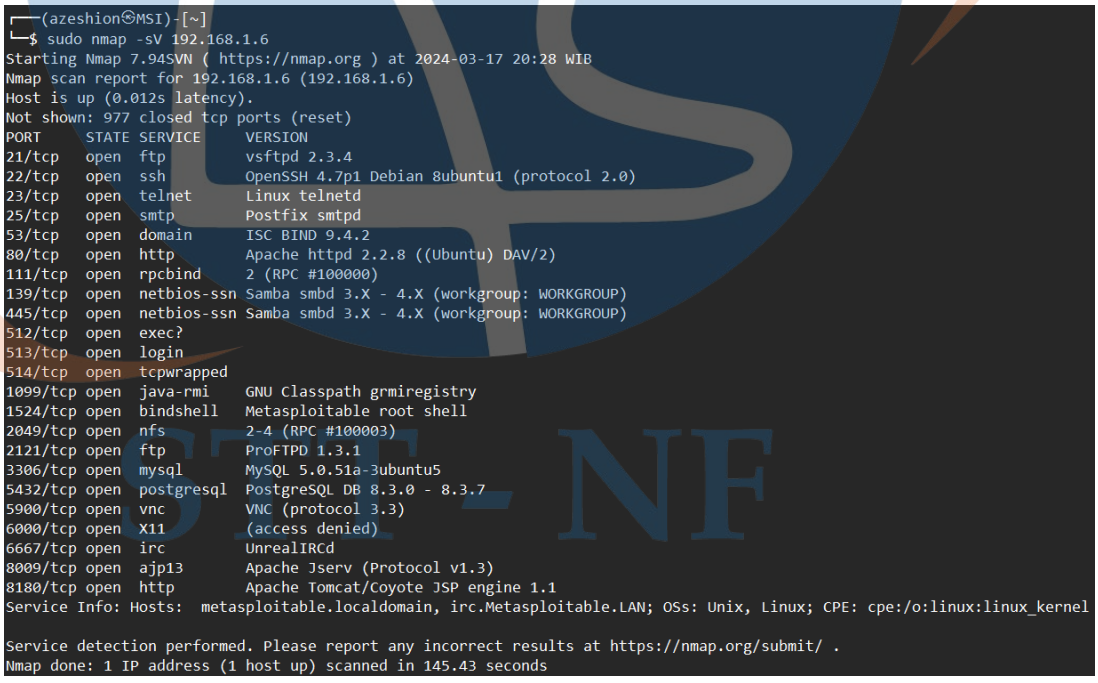
3. Tidak Ditampilkan:
   a. Ada juga beberapa port yang tidak ditampilkan karena statusnya adalah closed atau filtered, yaitu:
   b. 966 closed TCP ports (conn-refused)
   c. 11 filtered TCP ports (no-response)

```
┌──(azeshion㉿MSI)-[~]
└─$ sudo nmap -sA 192.168.1.6
[sudo] password for azeshion:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-17 20:27 WIB
Nmap scan report for 192.168.1.6 (192.168.1.6)
Host is up (0.0024s latency).
All 1000 scanned ports on 192.168.1.6 (192.168.1.6) are in ignored states.
Not shown: 1000 unfiltered tcp ports (reset)

Nmap done: 1 IP address (1 host up) scanned in 0.62 seconds
```

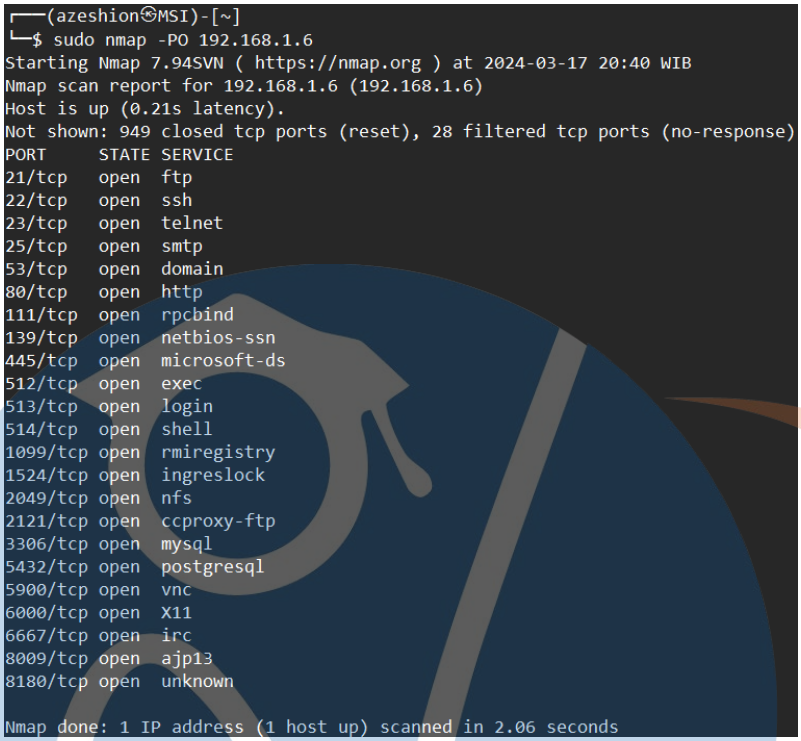
*Gambar 4.12* Hasil *vulnerability scanning 4* pada *ip address rentan*

1. Nmap scan report for 192.168.1.6 (192.168.1.6):
    a. Menunjukkan bahwa host dengan alamat IP 192.168.1.6 dalam jaringan Anda aktif.
    b. Waktu respons (latency) dari host tersebut adalah sekitar 0.0024 detik.
2. Status Port:
    a. Semua 1000 port yang dipindai berada dalam keadaan diabaikan (ignored states).
    b. Ini menandakan bahwa Nmap tidak dapat menentukan status port-port tersebut dengan akurat menggunakan metode ACK scan.
3. Not shown: 1000 unfiltered TCP ports (reset):
    a. Menunjukkan bahwa ada 1000 port TCP yang tidak ditampilkan dalam hasil scanning karena berada dalam keadaan tidak difilter (unfiltered), namun Nmap tidak bisa memastikan statusnya dengan pasti karena respon yang diterima adalah reset.




*Gambar 4.13* Hasil *vulnerability scanning 5* pada *ip address rentan*

1. Nmap scan report for 192.168.1.6 (192.168.1.6):
    a. Menunjukkan bahwa host dengan alamat IP 192.168.1.6 dalam jaringan Anda aktif.
    b. Waktu respons (latency) dari host tersebut adalah sekitar 0.012 detik.
2. Status Port:
    a. Terdapat beberapa port TCP yang terbuka (open), yaitu:
    b. 21/tcp : FTP (vsftpd 2.3.4)
    c. 22/tcp : SSH (OpenSSH 4.7p1 Debian 8ubuntu1)
    d. 23/tcp : Telnet (Linux telnetd)
    e. 25/tcp : SMTP (Postfix smtpd)
    f. 53/tcp : Domain (ISC BIND 9.4.2)
    g. 80/tcp : HTTP (Apache httpd 2.2.8)
    h. 111/tcp : RPCbind
    i. 139/tcp : NetBIOS-SSN (Samba smbd 3.X - 4.X)
    j. 445/tcp : NetBIOS-SSN (Samba smbd 3.X - 4.X)
    k. 512/tcp : Exec?
    l. 513/tcp : Login
    m. 514/tcp : TCP Wrapped
    n. 1099/tcp : Java RMI (GNU Classpath grmiregistry)
    o. 1524/tcp : Bindshell (Metasploitable root shell)
    p. 2049/tcp : NFS (RPC #100003)
    q. 2121/tcp : FTP (ProFTPD 1.3.1)
    r. 3306/tcp : MySQL (MySQL 5.0.51a-3ubuntu5)
    s. 5432/tcp : PostgreSQL (PostgreSQL DB 8.3.0 - 8.3.7)
    t. 5900/tcp : VNC (VNC protocol 3.3)
    u. 6000/tcp : X11 (access denied)
    v. 6667/tcp : IRC (UnrealIRCd)
    w. 8009/tcp : AJP13 (Apache Jserv Protocol v1.3)
    x. 8180/tcp : HTTP (Apache Tomcat/Coyote JSP engine 1.1)




*Gambar 4.14* Hasil *vulnerability scanning 6* pada *ip address rentan*

1. Nmap scan report for 192.168.1.6 (192.168.1.6):
   a. Menunjukkan bahwa host dengan alamat IP 192.168.1.6 dalam jaringan Anda aktif.
   b. Waktu respons (latency) dari host tersebut adalah sekitar 0.21 detik.
2. Status Port:

Terdapat beberapa port TCP yang terbuka (open), yang menunjukkan layanan-layanan yang berjalan di host tersebut.

a. 21/tcp : FTP
b. 22/tcp : SSH
c. 23/tcp : Telnet
d. 25/tcp : SMTP
e. 53/tcp : Domain
f. 80/tcp : HTTP
g. 111/tcp : RPCbind
h. 139/tcp : NetBIOS-SSN

i. 445/tcp : Microsoft-DS
j. 512/tcp : Exec
k. 513/tcp : Login
l. 514/tcp : Shell
m. 1099/tcp : RMI Registry
n. 1524/tcp : Ingreslock
o. 2049/tcp : NFS
p. 2121/tcp : CCProxy-FTP
q. 3306/tcp : MySQL
r. 5432/tcp : PostgreSQL
s. 5900/tcp : VNC
t. 6000/tcp : X11
u. 6667/tcp : IRC
v. 8009/tcp : AJP13
w. 8180/tcp : Unknown

3. Tidak Ditampilkan:
   a. Ada beberapa port yang tidak ditampilkan karena statusnya adalah closed atau filtered.
   b. 949 closed TCP ports (reset)
   c. 28 filtered TCP ports (no-response)

```
┌──(azeshion㉿MSI)-[~]
└─$ sudo nmap -sU 192.168.1.6
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-17 20:40 WIB
Stats: 0:09:26 elapsed; 0 hosts completed (1 up), 1 undergoing UDP Scan
UDP Scan Timing: About 64.73% done; ETC: 20:55 (0:05:09 remaining)
Nmap scan report for 192.168.1.6 (192.168.1.6)
Host is up (0.0049s latency).
Not shown: 955 closed udp ports (port-unreach), 41 open|filtered udp ports (no-response)
PORT     STATE SERVICE
53/udp   open  domain
111/udp  open  rpcbind
137/udp  open  netbios-ns
2049/udp open  nfs

Nmap done: 1 IP address (1 host up) scanned in 962.21 seconds
```

*Gambar 4.15* Hasil *vulnerability scanning 7* pada *ip address rentan*

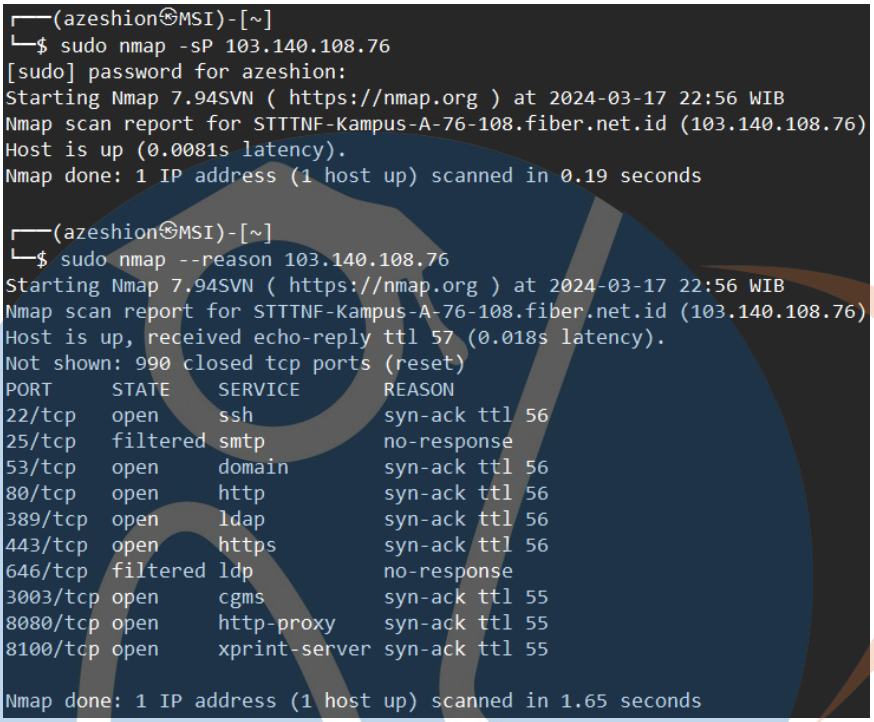
1. Nmap scan report for 192.168.1.6 (192.168.1.6):
    a. Menunjukkan bahwa host dengan alamat IP 192.168.1.6 dalam jaringan Anda aktif.
    b. Waktu respons (latency) dari host tersebut adalah sekitar 0.0049 detik.
2. Status Port UDP:

Terdapat beberapa port UDP yang terbuka (open), yaitu:

a. 53/udp : Domain
b. 111/udp : RPCbind
c. 137/udp : NetBIOS-NS
d. 2049/udp : NFS
e. Tidak Ditampilkan:
f. Ada beberapa port UDP yang tidak ditampilkan karena statusnya adalah closed atau filtered.
g. 955 closed UDP ports (port-unreach)
h. 41 open|filtered UDP ports (no-response)

3. UDP Scan Timing:
    a. Menunjukkan kemajuan proses pemindaian UDP, dengan sekitar 64.73% sudah selesai.
    b. ETC (Estimated Time Completion) menunjukkan perkiraan waktu penyelesaian pemindaian.

Hasil Vulnerability Scanning menggunakan NMAP dari Alamat IP task.nurulfikri.com, esertifikat.nurulfikri.com dan learning.nurulfikri.com




*Gambar 4.16* Hasil *vulnerability scanning 1* pada *ip address* pengujian

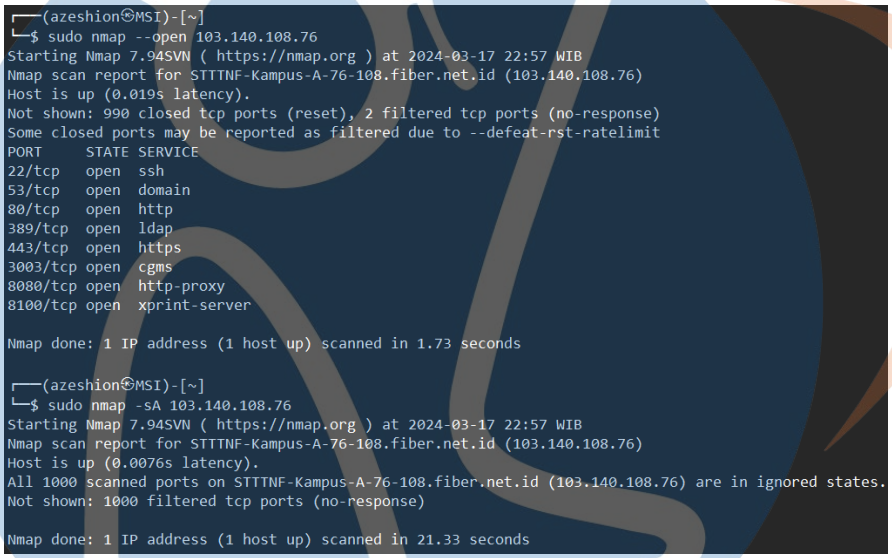
Pemindaian dengan -sP:

a. Menunjukkan bahwa host tersebut aktif dengan respon dalam waktu 0.0081 detik.
b. Pemindaian ini hanya menggunakan teknik ping scan untuk menentukan apakah host tersebut aktif atau tidak.

Pemindaian dengan --reason:

a. Menunjukkan informasi lebih detail tentang host tersebut.
b. Host merespon dengan pesan "echo-reply" dengan TTL (Time to Live) 57, yang menunjukkan bahwa host tersebut dapat dijangkau dalam 57 lompatan router.
c. Pemindaian port menunjukkan beberapa port yang terbuka (open) dan beberapa port yang difilter (filtered) atau tertutup (closed).

d. Port yang terbuka meliputi SSH (22/tcp), Domain (53/tcp), HTTP (80/tcp), LDAP (389/tcp), HTTPS (443/tcp), CGMS (3003/tcp), HTTP Proxy (8080/tcp), dan XPrint Server (8100/tcp).
e. Port yang difilter atau tertutup meliputi SMTP (25/tcp) dan LDP (646/tcp), di mana Nmap tidak menerima respons apapun (no-response).
f. Status port ditunjukkan bersama dengan alasan (reason) dan TTL yang diterima dari respon.



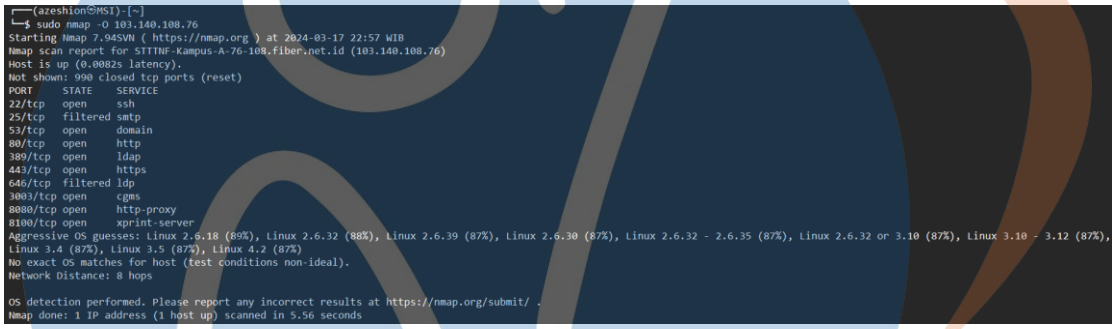

*Gambar 4.17* Hasil *vulnerability scanning 2* pada *ip address* pengujian

Pemindaian dengan --open:

a. Host dengan alamat IP 103.140.108.76 dalam jaringan Anda aktif, dengan latency sekitar 0.019 detik.
b. Beberapa port TCP terbuka, termasuk SSH (22/tcp), Domain (53/tcp), HTTP (80/tcp), LDAP (389/tcp), HTTPS (443/tcp), CGMS (3003/tcp), HTTP Proxy (8080/tcp), dan XPrint Server (8100/tcp).
c. Beberapa port TCP tertutup (closed) atau difilter (filtered), yang mungkin disebabkan oleh pembatasan akses atau firewall.

Pemindaian dengan -sA:

a. Host dengan alamat IP 103.140.108.76 dalam jaringan Anda aktif, dengan latency sekitar 0.0076 detik.
b. Namun, semua 1000 port TCP yang dipindai berada dalam keadaan yang diabaikan (ignored states), yang berarti Nmap tidak dapat menentukan status pasti dari port-port tersebut.
c. Semua port yang dipindai ditampilkan sebagai difilter (filtered), yang berarti Nmap tidak menerima respons apapun dari port-port tersebut.



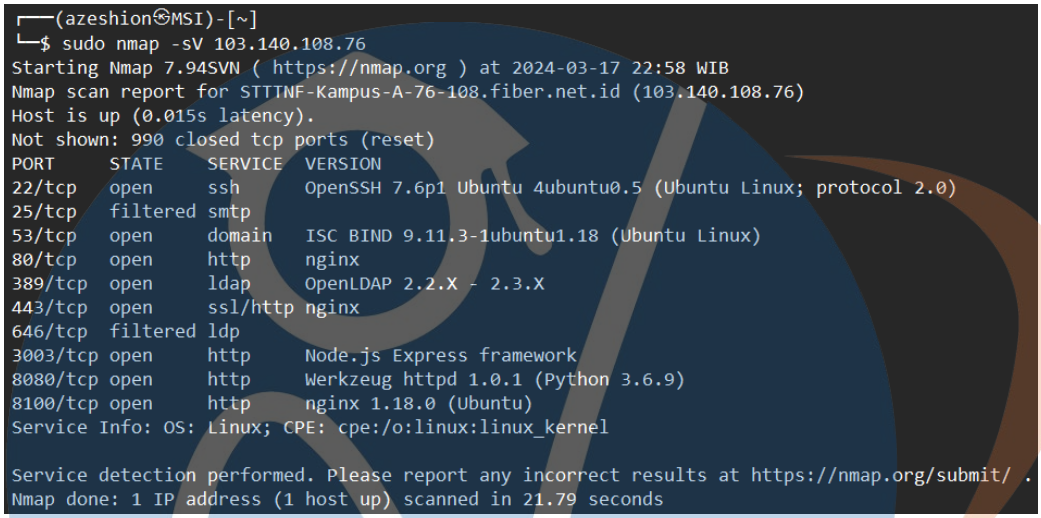

*Gambar 4.18* Hasil *vulnerability scanning 3* pada *ip address* pengujian

Pemindaian dengan -O (Fingerprinting OS):

a. Host dengan alamat IP 103.140.108.76 dalam jaringan Anda aktif, dengan latency sekitar 0.0082 detik.
b. Beberapa port TCP terbuka, termasuk SSH (22/tcp), Domain (53/tcp), HTTP (80/tcp), LDAP (389/tcp), HTTPS (443/tcp), CGMS (3003/tcp), HTTP Proxy (8080/tcp), dan XPrint Server (8100/tcp).
c. Beberapa port TCP tertutup (closed) atau difilter (filtered), yang mungkin disebabkan oleh pembatasan akses atau firewall.
d. Nmap tidak dapat menentukan status pasti dari port-port tertentu, seperti SMTP (25/tcp) dan LDP (646/tcp).
e. Berdasarkan informasi yang dikumpulkan, Nmap mencoba untuk menebak sistem operasi yang dijalankan oleh host tersebut. Hasilnya menunjukkan beberapa tebakan OS yang agresif, dengan probabilitas tinggi bahwa host tersebut menjalankan sistem operasi Linux versi 2.6.x,

3.x, atau 4.x. Namun, tidak ada kesesuaian OS yang tepat karena kondisi pengujian tidak ideal.

f. Jarak jaringan (network distance) dari host tersebut adalah 8 lompatan (hops).

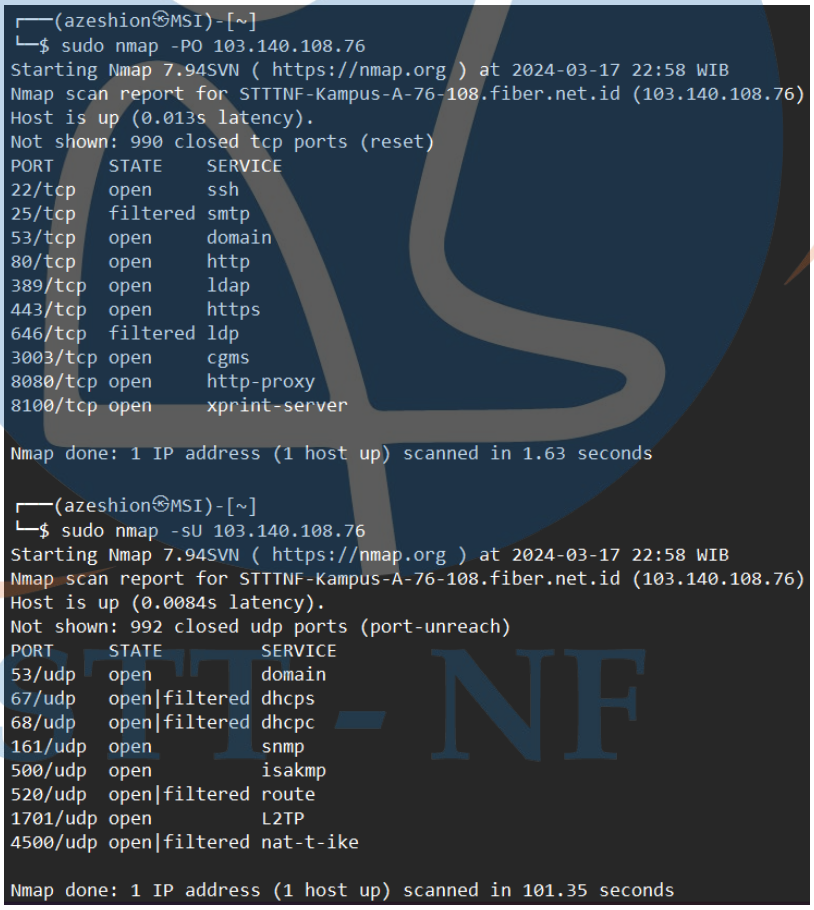



*Gambar 4.19* Hasil *vulnerability scanning 4* pada *ip address* pengujian

Pemindaian dengan -sV (Fingerprinting Service):

a. Host dengan alamat IP 103.140.108.76 dalam jaringan Anda aktif, dengan latency sekitar 0.015 detik.
b. Beberapa port TCP terbuka, beserta informasi tentang layanan yang berjalan di setiap port tersebut.
c. Port SSH (22/tcp) terbuka dan menjalankan OpenSSH versi 7.6p1 pada sistem operasi Ubuntu Linux.
d. Port Domain (53/tcp) terbuka dan menjalankan layanan ISC BIND versi 9.11.3-1ubuntu1.18 pada sistem operasi Ubuntu Linux.
e. Port HTTP (80/tcp) terbuka dan menjalankan layanan nginx.
f. Port LDAP (389/tcp) terbuka dan menjalankan layanan OpenLDAP versi 2.2.X - 2.3.X.
g. Port HTTPS (443/tcp) terbuka dan menjalankan layanan nginx dengan SSL.

h. Port HTTP (3003/tcp) terbuka dan menjalankan layanan Node.js Express framework.
i. Port HTTP (8080/tcp) terbuka dan menjalankan layanan Werkzeug httpd versi 1.0.1 dengan Python 3.6.9.
j. Port HTTP (8100/tcp) terbuka dan menjalankan layanan nginx versi 1.18.0 pada sistem operasi Ubuntu Linux.
k. Beberapa port tertutup (closed) atau difilter (filtered), seperti SMTP (25/tcp) dan LDP (646/tcp).
l. Informasi layanan juga menyertakan informasi tentang sistem operasi yang digunakan (Linux).




*Gambar 4.20* Hasil *vulnerability scanning 5* pada *ip address* pengujian

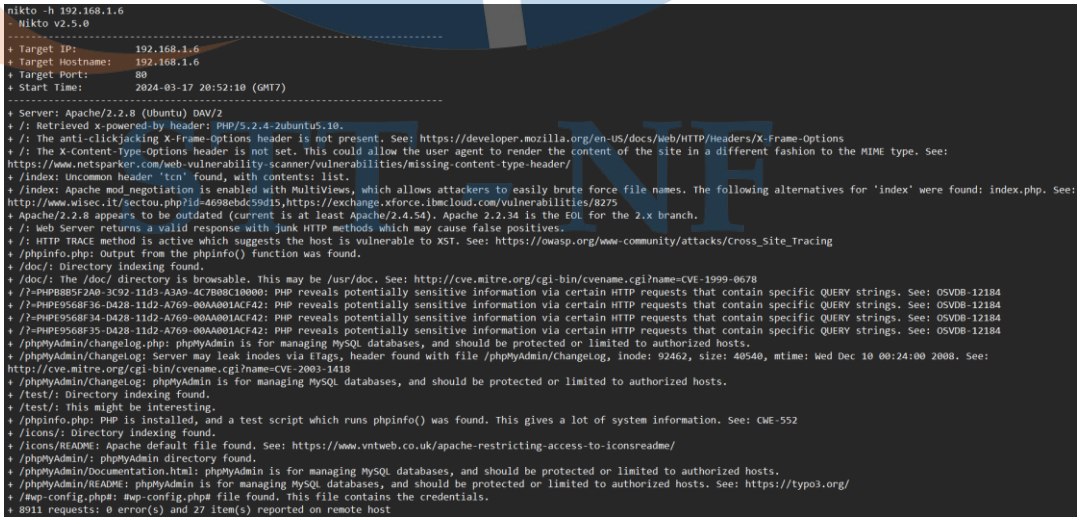
Pemindaian dengan -PO (Ping Only):

a. Host dengan alamat IP 103.140.108.76 dalam jaringan Anda aktif, dengan latency sekitar 0.013 detik.
b. Beberapa port TCP terbuka, termasuk SSH (22/tcp), Domain (53/tcp), HTTP (80/tcp), LDAP (389/tcp), HTTPS (443/tcp), CGMS (3003/tcp), HTTP Proxy (8080/tcp), dan XPrint Server (8100/tcp).
c. Beberapa port TCP tertutup (closed) atau difilter (filtered), seperti SMTP (25/tcp) dan LDP (646/tcp).

Pemindaian dengan -sU (UDP Scan):

d. Host dengan alamat IP 103.140.108.76 dalam jaringan Anda aktif, dengan latency sekitar 0.0084 detik.
e. Beberapa port UDP terbuka, termasuk Domain (53/udp), SNMP (161/udp), ISAKMP (500/udp), L2TP (1701/udp), serta port-port lainnya yang berstatus "open" atau "open|filtered".
f. Beberapa port UDP tertutup (closed) atau difilter (filtered), seperti DHCP Server (67/udp, 68/udp), serta port-port lainnya yang berstatus "open|filtered".

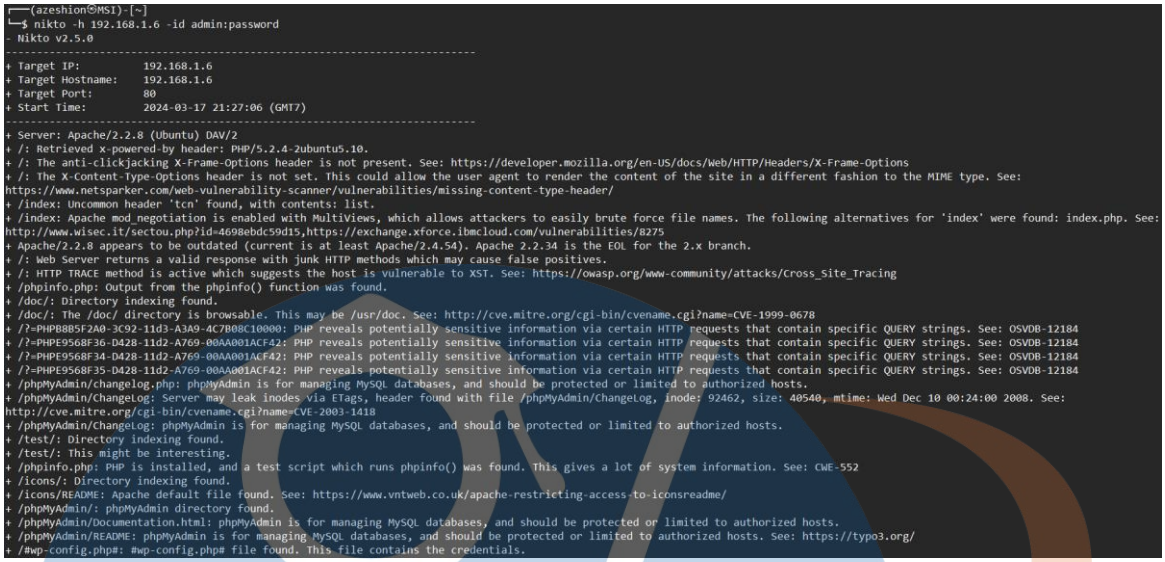
Hasil Vulnerability Scanning menggunakan Nikto pada IP yang rentan:




*Gambar 4.21* Hasil *vulnerability scanning nikto 1* pada *ip address* rentan

Nikto Scan pada Alamat IP 192.168.1.6:

1. Target IP: 192.168.1.6
2. Target Hostname: 192.168.1.6
3. Port yang dipindai: 80 (HTTP)
4. Server Web: Apache/2.2.8 (Ubuntu) DAV/2
5. Beberapa temuan penting:
    a. Header X-Powered-By: PHP/5.2.4-2ubuntu5.10
    b. Header X-Frame-Options tidak ada, yang dapat meningkatkan risiko clickjacking.
    c. Header X-Content-Type-Options tidak diatur.
    d. Temuan header "tcn" yang tidak umum dengan isi "list".
    e. Apache mod_negotiation diaktifkan dengan MultiViews, yang dapat memungkinkan serangan brute force pada nama file.
    f. Apache/2.2.8 terlihat usang, saran untuk memperbarui ke versi lebih baru.
    g. Metode HTTP junk yang tidak lazim.
    h. Metode HTTP TRACE aktif, menunjukkan rentan terhadap Cross Site Tracing (XST).
    i. Adanya file phpinfo.php yang dapat memberikan informasi sensitif.
    j. Direktori /doc/ dan /test/ bersifat browseable.
    k. phpMyAdmin ditemukan, yang sebaiknya dibatasi aksesnya.
    l. Potensi kebocoran inode melalui ETags pada file /phpMyAdmin/ChangeLog.
    m. Direktori /icons/ dan beberapa file terkait Apache ditemukan.
    n. Temuan file #wp-config.php# yang berpotensi mengandung kredensial sensitif.

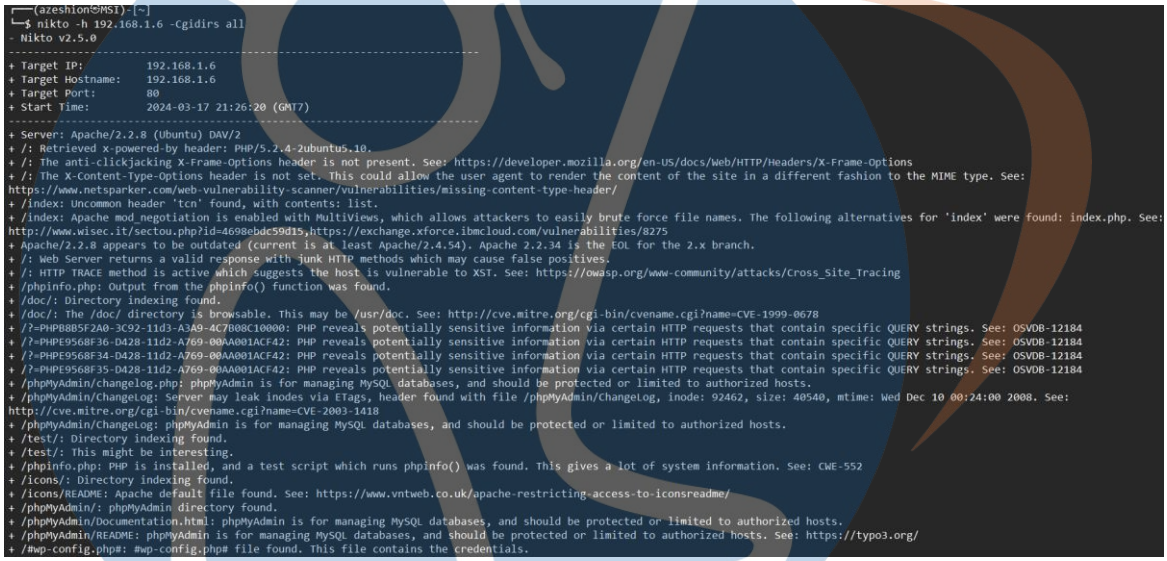



*Gambar 4.22* Hasil *vulnerability scanning nikto 2* pada *ip address* rentan

Pemindaian Nikto pada Alamat IP 192.168.1.6 (dengan Kredensial Admin:Password):

1. Target IP: 192.168.1.6
2. Target Hostname: 192.168.1.6
3. Port yang dipindai: 80 (HTTP)
4. Server Web: Apache/2.2.8 (Ubuntu) DAV/2
5. Beberapa temuan penting:
    a. Header X-Powered-By: PHP/5.2.4-2ubuntu5.10
    b. Header X-Frame-Options tidak ada, yang dapat meningkatkan risiko clickjacking.
    c. Header X-Content-Type-Options tidak diatur.
    d. Temuan header "tcn" yang tidak umum dengan isi "list".
    e. Apache mod_negotiation diaktifkan dengan MultiViews, yang dapat memungkinkan serangan brute force pada nama file.
    f. Apache/2.2.8 terlihat usang, saran untuk memperbarui ke versi lebih baru.
    g. Metode HTTP junk yang tidak lazim.
    h. Metode HTTP TRACE aktif, menunjukkan rentan terhadap Cross Site Tracing (XST).
    i. Adanya file phpinfo.php yang dapat memberikan informasi sensitif.

j. Direktori /doc/ dan /test/ bersifat browseable.
k. phpMyAdmin ditemukan, yang sebaiknya dibatasi aksesnya.
l. Potensi kebocoran inode melalui ETags pada file /phpMyAdmin/ChangeLog.
m. Direktori /icons/ dan beberapa file terkait Apache ditemukan.
n. Temuan file #wp-config.php# yang berpotensi mengandung kredensial sensitif.




*Gambar 4.23* Hasil *vulnerability scanning nikto 3* pada *ip address* rentan

Pemindaian Nikto pada Alamat IP 192.168.1.6 (dengan CgiDirs All):

1. Target IP: 192.168.1.6
2. Target Hostname: 192.168.1.6
3. Port yang dipindai: 80 (HTTP)
4. Server Web: Apache/2.2.8 (Ubuntu) DAV/2
5. Beberapa temuan penting:
   a. Header X-Powered-By: PHP/5.2.4-2ubuntu5.10
   b. Header X-Frame-Options tidak ada, yang dapat meningkatkan risiko clickjacking.
   c. Header X-Content-Type-Options tidak diatur.
   d. Temuan header "tcn" yang tidak umum dengan isi "list".

e. Apache mod_negotiation diaktifkan dengan MultiViews, yang dapat memungkinkan serangan brute force pada nama file.
f. Apache/2.2.8 terlihat usang, saran untuk memperbarui ke versi lebih baru.
g. Metode HTTP junk yang tidak lazim.
h. Metode HTTP TRACE aktif, menunjukkan rentan terhadap Cross Site Tracing (XST).
i. Adanya file phpinfo.php yang dapat memberikan informasi sensitif.
j. Direktori /doc/ dan /test/ bersifat browseable.
k. phpMyAdmin ditemukan, yang sebaiknya dibatasi aksesnya.
l. Potensi kebocoran inode melalui ETags pada file /phpMyAdmin/ChangeLog.
m. Direktori /icons/ dan beberapa file terkait Apache ditemukan.
n. Temuan file #wp-config.php# yang berpotensi mengandung kredensial sensitif.

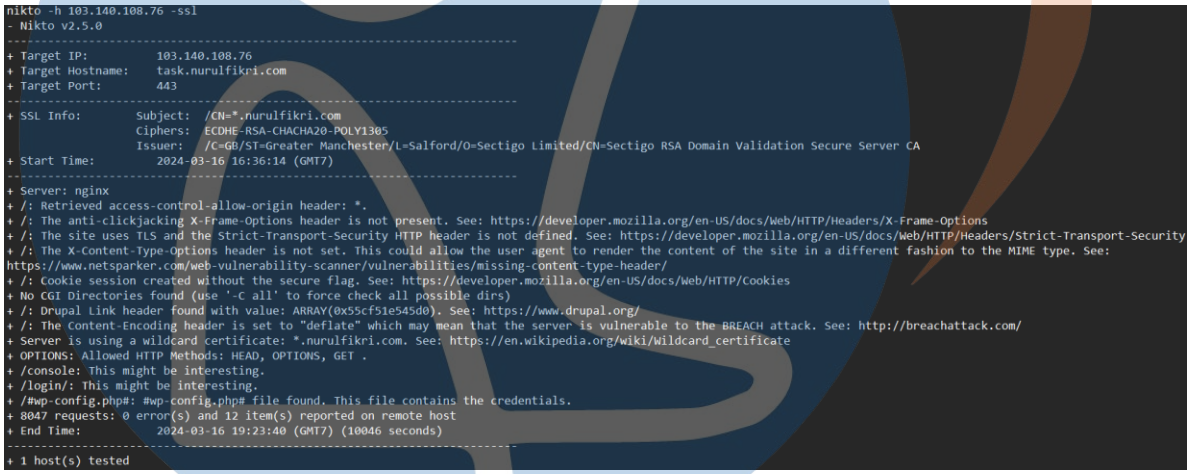
Hasil Vulnerability Scanning menggunakan Nikto dari Alamat IP task.nurulfikri.com, esertifikat.nurulfikri.com dan learning.nurulfikri.com


*Gambar 4.24* Hasil *vulnerability scanning nikto 1* pada *ip address* pengujian

Pemindaian Nikto pada Alamat IP 103.140.108.76:

1. Target IP: 103.140.108.76
2. Target Hostname: task.nurulfikri.com
3. Port yang dipindai: 80 (HTTP)
4. Server Web: nginx
5. Beberapa temuan penting:

a. Header X-Frame-Options tidak ada, yang dapat meningkatkan risiko clickjacking.
b. Header X-Content-Type-Options tidak diatur.
c. Halaman root / diarahkan ke: https://task.nurulfikri.com/
d. Tidak ditemukan direktori CGI (gunakan '-C all' untuk memeriksa semua direktori yang mungkin).
e. Temuan header Drupal Link dengan nilai ARRAY(0x5652645370f8).
f. Temuan header tidak lazim 'server-timing' dengan isi: wp-before-template;dur=144.11.
g. Temuan header tidak lazim 'x-litespeed-tag' dengan isi: fc6_HTTP.200.




*Gambar 4.25* Hasil *vulnerability scanning nikto 2* pada *ip address* pengujian

Pemindaian Nikto pada Alamat IP 103.140.108.76 (SSL):

1. Target IP: 103.140.108.76
2. Target Hostname: task.nurulfikri.com
3. Port yang dipindai: 443 (HTTPS)
4. Informasi SSL:
   a. Subject: /CN=*.nurulfikri.com
   b. Cipher: ECDHE-RSA-CHACHA20-POLY1305
   c. Issuer: /C=GB/ST=Greater Manchester/L=Salford/O=Sectigo Limited/CN=Sectigo RSA Domain Validation Secure Server CA
5. Server Web: nginx

6. Beberapa temuan penting:
    a. Header access-control-allow-origin diambil dengan nilai: *.
    b. Header X-Frame-Options tidak ada, yang dapat meningkatkan risiko clickjacking.
    c. Situs menggunakan TLS tetapi header HTTP Strict-Transport-Security tidak didefinisikan.
    d. Header X-Content-Type-Options tidak diatur.
    e. Sesuai cookie dibuat tanpa flag secure.
    f. Tidak ditemukan direktori CGI (gunakan '-C all' untuk memeriksa semua direktori yang mungkin).
    g. Temuan header Drupal Link dengan nilai ARRAY(0x55cf51e545d0).
    h. Header Content-Encoding diatur ke "deflate" yang dapat membuat server rentan terhadap serangan BREACH.
    i. Server menggunakan wildcard certificate: *.nurulfikri.com.
    j. Metode HTTP yang diizinkan: HEAD, OPTIONS, GET.
    k. Beberapa halaman yang mungkin menarik ditemukan, seperti /console dan /login/.
    l. Ditemukan file #wp-config.php# yang berpotensi berisi kredensial.


*Gambar 4.26* Hasil *vulnerability scanning nikto 3* pada *ip address* pengujian

Pemindaian Nikto pada Alamat IP 103.140.108.76 (Autentikasi dengan Kredensial Admin:Password):

1. Target IP: 103.140.108.76
2. Target Hostname: task.nurulfikri.com

3. Port yang dipindai: 80 (HTTP)
4. Server Web: nginx
5. Beberapa temuan penting:
    a. Header anti-clickjacking X-Frame-Options tidak ada, yang dapat meningkatkan risiko clickjacking.
    b. Header X-Content-Type-Options tidak diatur.
    c. Halaman root / diarahkan ke https://task.nurulfikri.com/.
    d. Header Drupal Link dengan nilai ARRAY(0x55d1f13f7ca8).
    e. Ditemukan header yang tidak lazim, yaitu x-litespeed-tag dengan konten fc6_HTTP.200.
    f. Ditemukan header yang tidak lazim, yaitu server-timing dengan konten wp-before-template;dur=150.41.
6. Jumlah permintaan: 8046
7. Tidak ada kesalahan yang dilaporkan pada host remote.


*Gambar 4.27* Hasil *vulnerability scanning nikto 4* pada *ip address* pengujian

Pemindaian Nikto pada Alamat IP 103.140.108.76 (CGI Directories All):

1. Target IP: 103.140.108.76
2. Target Hostname: task.nurulfikri.com
3. Port yang dipindai: 80 (HTTP)
4. Server Web: nginx
5. Beberapa temuan penting:
    a. Header anti-clickjacking X-Frame-Options tidak ada, yang dapat meningkatkan risiko clickjacking.

b. Header X-Content-Type-Options tidak diatur.
c. Halaman root / diarahkan ke https://task.nurulfikri.com/.
d. Header Drupal Link dengan nilai ARRAY(0x55b8ccb209c8).
e. Ditemukan header yang tidak lazim, yaitu x-litespeed-tag dengan konten fc6_HTTP.200.
f. Ditemukan header yang tidak lazim, yaitu server-timing dengan konten wp-before-template;dur=166.5.

6. Jumlah permintaan: 26584
7. Tidak ada kesalahan yang dilaporkan pada host remote.

Hasil Vulnerability Scanning menggunakan Skipfish pada IP yang rentan:


*Gambar 4.28* Hasil *vulnerability scanning skipfish* pada *ip address* rentan

**Medium Risk - Data Compromise**

1. PHP Inclusion Error:

   URL: http://192.168.1.6/mutillidae/documentation/vulnerabilities.php

Memo: Terdeteksi kesalahan inklusi PHP selama pengujian traversal.

2. Directory Traversal / File Inclusion Possible:

   URL: http://192.168.1.6/dav/?C=N;O=.\D

   Memo: Kemungkinan traversal direktori / inklusi file.

3. Interesting Server Messages:

   URL: http://192.168.1.6/dvwa/dvwa/includes/dvwaPage.inc.php

   Memo: PHP (HTML) warning detected.

   Medium Risk - Data Compromise (Higher Risk Level)

4. External Content Embedded on Pages:

   URL: http://192.168.1.6/mutillidae/documentation/Mutillidae-Test-Scripts.txt

   Memo: Konten eksternal dari TWiki.org ditempatkan pada halaman.

   XSS - Cross-Site Scripting

5. XSS Vector in Document Body:

   URL: http://192.168.1.6/phpMyAdmin/phpmyadmin.css.php

   Memo: Injeksi sintaks dalam kode JS/CSS.

6. Low Risk or Low Specificity

   Terdapat beberapa temuan dengan risiko rendah atau spesifikitas rendah yang meliputi deteksi tanda tangan, direktif penyimpanan cache yang tidak benar, dan form HTML tanpa perlindungan XSRF yang jelas.

7. Internal Warning

   Terdapat beberapa peringatan internal terkait deteksi kesalahan, respons yang bervariasi secara acak, dan kegagalan pengambilan sumber daya.

Hasil Vulnerability Scanning menggunakan Skipfish dari Alamat IP task.nurulfikri.com, esertifikat.nurulfikri.com dan learning.nurulfikri.com


*Gambar 4.29* Hasil *vulnerability scanning skipfish* pada *ip address* pengujian

**task.nurulfikri.com**

Medium Risk - Data Compromise

1. Findings: Interesting files

   URL: https://task.nurulfikri.com/static/appbuilder/js/jquery-latest.js/

   Memo: Terdapat dump basis data yang dibatasi.

Low Risk or Low Specificity

1. SSL certificate host name mismatch

2. SSL certificate expired or not yet valid


*Gambar 4.30* Hasil *vulnerability scanning skipfish* pada *ip address* pengujian

**esertifikat.nurulfikri.com**

Medium Risk - Data Compromise

1. Findings: Interesting files

   URL: https://esertifikat.nurulfikri.com/static/appbuilder/js/jquery-latest.js/

   Memo: Terdapat dump basis data yang dibatasi.

Medium Risk - Data Compromise (Higher Risk Level)

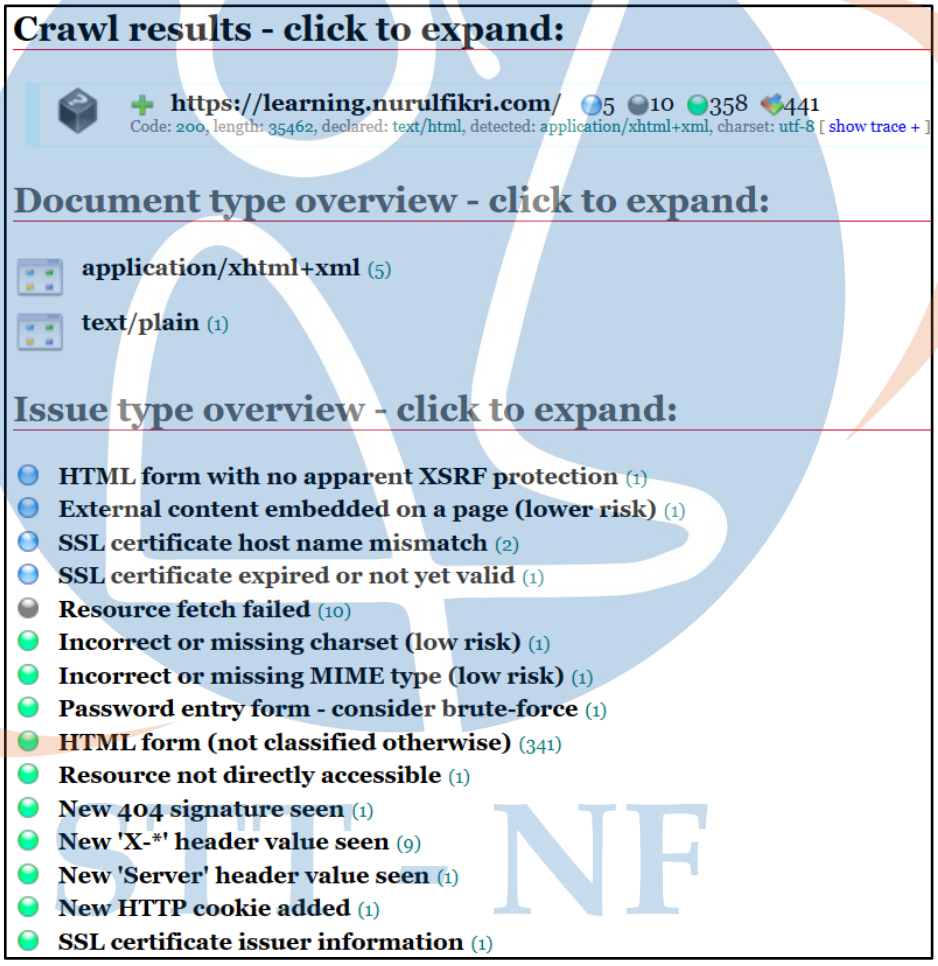
2. Temuan: Konten eksternal tertanam pada halaman

URL: https://esertifikat.nurulfikri.com/sertifikatformview/form

Memo: Skrip reCAPTCHA dari Google tertanam di halaman.

Low Risk or Low Specificity

1. HTML form with no apparent XSRF protection
2. SSL certificate host name mismatch
3. SSL certificate expired atau tidak valid




*Gambar 4.31* Hasil *vulnerability scanning skipfish* pada *ip address* pengujian

**learning.nurulfikri.com**

Low Risk or Low Specificity

1. HTML form with no apparent XSRF protection

2. External content embedded on a page
3. SSL certificate host name mismatch
4. SSL certificate expired or not yet valid

Hasil Vulnerability Scanning menggunakan Wapiti dari Alamat IP task.nurulfikri.com, esertifikat.nurulfikri.com dan learning.nurulfikri.com

**Summary**

| Category | Number of vulnerabilities found |
|---|---|
| Backup file | 0 |
| Blind SQL Injection | 0 |
| Weak credentials | 0 |
| CRLF Injection | 0 |
| Content Security Policy Configuration | 1 |
| Cross Site Request Forgery | 0 |
| Potentially dangerous file | 0 |
| Command execution | 0 |
| Path Traversal | 0 |
| Htaccess Bypass | 0 |
| HTTP Secure Headers | 3 |
| HttpOnly Flag cookie | 0 |
| Open Redirect | 0 |
| Secure Flag cookie | 1 |
| SQL Injection | 0 |

*Gambar 4.32* Hasil *vulnerability scanning wapiti* pada *ip address* task.nurulfikri.com

**Summary**

Content Security Policy Configuration: 1 vulnerability found

1. HTTP Secure Headers:
    a. X-Frame-Options is not set
    b. X-Content-Type-Options is not set
    c. Strict-Transport-Security is not set

Secure Flag cookie: 1 vulnerability found

Vulnerability Details

1. Content Security Policy Configuration
    a. Description: CSP (Content Security Policy) is not set.
    b. Solutions: Configure CSP by adding the Content-Security-Policy HTTP header to the web page.
2. HTTP Secure Headers
    a. X-Frame-Options

        Description: X-Frame-Options is not set.

    b. X-Content-Type-Options

        Description: X-Content-Type-Options is not set.

    c. Strict-Transport-Security

        Description: Strict-Transport-Security is not set.

        Solutions: Harden HTTP Security Headers according to recommendations.
3. Secure Flag cookie
    a. Description: The Secure flag is not set in the cookie named "session".
    b. Solutions: Set the Secure Flag to True when generating the cookie.

**Summary**

| Category | Number of vulnerabilities found |
|---|---|
| Backup file | 0 |
| Blind SQL Injection | 0 |
| Weak credentials | 0 |
| CRLF Injection | 0 |
| Content Security Policy Configuration | 1 |
| Cross Site Request Forgery | 0 |
| Potentially dangerous file | 0 |
| Command execution | 0 |
| Path Traversal | 0 |
| Htaccess Bypass | 0 |
| HTTP Secure Headers | 3 |
| HttpOnly Flag cookie | 0 |
| Open Redirect | 0 |
| Secure Flag cookie | 1 |

*Gambar 4.33* Hasil *vulnerability scanning wapiti* pada *ip address* esertifikat.nurulfikri.com

**Summary**

Content Security Policy Configuration: 1 vulnerability found

1. HTTP Secure Headers:
    a. X-Frame-Options is not set
    b. X-Content-Type-Options is not set
    c. Strict-Transport-Security is not set

Secure Flag cookie: 1 vulnerability found

Internal Server Error: 3 anomalies found

Vulnerability Details:

2. Content Security Policy Configuration
    a. Description: CSP (Content Security Policy) is not set.
    b. Solutions: Configure CSP by adding the Content-Security-Policy HTTP header to the web page

3. HTTP Secure Headers
    a. X-Frame-Options

       Description: X-Frame-Options is not set.

    b. X-Content-Type-Options

       Description: X-Content-Type-Options is not set.

    c. Strict-Transport-Security

       Description: Strict-Transport-Security is not set.

       Solutions: Harden HTTP Security Headers according to recommendations.

4. Secure Flag cookie
    a. Description: The Secure flag is not set in the cookie named "session".
    b. Solutions: Set the Secure Flag to True when generating the cookie.

Internal Server Error

a. Description: Terjadi kesalahan di sisi server, mengakibatkan kode kesalahan HTTP 500 saat mencoba memasukkan muatan ke dalam parameter "f".
b. Solutions: Informasi tentang kesalahan ini dapat ditemukan di log server.

**Summary**

| Category | Number of vulnerabilities found |
|---|---|
| Backup file | 0 |
| Blind SQL Injection | 0 |
| Weak credentials | 0 |
| CRLF Injection | 0 |
| Content Security Policy Configuration | 1 |
| Cross Site Request Forgery | 0 |
| Potentially dangerous file | 0 |
| Command execution | 0 |
| Path Traversal | 0 |
| Htaccess Bypass | 0 |
| HTTP Secure Headers | 2 |
| HttpOnly Flag cookie | 1 |
| Open Redirect | 0 |
| Secure Flag cookie | 1 |



*Gambar 4.34* Hasil *vulnerability scanning wapiti* pada *ip address* learning.nurulfikri.com

**Summary**

Content Security Policy Configuration: 1 vulnerability found

1. HTTP Secure Headers:
    a. X-Content-Type-Options is not set
    b. Strict-Transport-Security is not set

HttpOnly Flag cookie: 1 vulnerability found

Secure Flag cookie: 1 vulnerability found

Vulnerability Details

2. Content Security Policy Configuration
    a. Description: CSP (Content Security Policy) is not set.
    b. Solutions: Configure CSP by adding the Content-Security-Policy HTTP header to the web page.
3. HTTP Secure HeadersX-Content-Type-Options:
    a. X-Content-Type-Options

        Description: X-Content-Type-Options is not set.

    b. Strict-Transport-Security

        Description: Strict-Transport-Security is not set.

        Solutions: Harden HTTP Security Headers according to recommendations.

    c. HttpOnly Flag cookie

        Description: Flag HttpOnly tidak disetel pada cookie bernama "MoodleSession".

        Solutions: Set the HttpOnly Flag to True when generating the cookie.

4. Secure Flag cookie
    a. Description: Secure flag is not set in the cookie named "MoodleSession".
    b. Solutions: When generating the cookie, make sure to set the Secure Flag to True.

***Gather Victim Informatin* (T1590)**

Penyerang mengumpulkan informasi tentang jaringan korban yang dapat digunakan saat menargetkan. Informasi tentang jaringan dapat mencakup berbagai detail, termasuk data administratif (misalnya: rentang IP, nama domain, dan lain lain.) serta detail-detail mengenai topologi dan operasinya.

***Domain Properties* (T1590. 001)**

Penyerang mengumpulkan informasi tentang domain jaringan korban yang bisa digunakan saat menargetkan. Informasi tentang domain dan propertinya mungkin mencakup berbagai detail, termasuk domain apa yang dimiliki korban serta data administratif (misalnya: nama, registrar, dan lain lain.) dan informasi yang lebih langsung bisa digunakan seperti kontak (alamat email dan nomor telepon), alamat bisnis, dan name server.

***Domain Properties* dari *Domain* yang Diuji**

Alamat IP: 103.140.108.76. Untuk Alamat IP yang digunakan diketiga domain tersebut sama, karena menggunakan sistem shared hosting.

Registrar: Key-Systems GmbH

Terdaftar di: 199-12-31

Berakhir pada: 2026-12-31

Diperbarui pada: 2023-10-23

Status: OK

Name Servers: alice.ns.cloudflare.com dan rory.ns.cloudflare.com

Server Type: nginx

SSL/TLS: Kadaluarsa 117 hari yang lalu

Country: Indonesia

Region: Jakarta

City: Jakarta

ISP: PT. Fiber Networks Indonesia

Organization: PT. Fiber Networks Indonesia

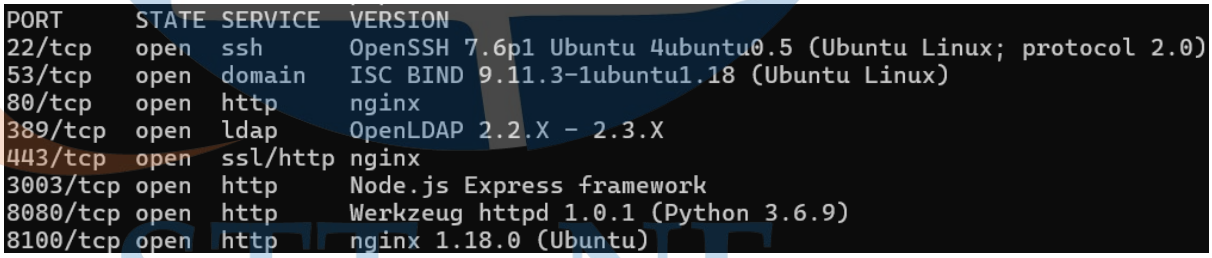
Latitude: -6.2087

Longtitude: 106.8455

***Network Security Appliances* (T1590. 006)**

Musuh bisa mengumpulkan informasi tentang perangkat keamanan jaringan korban yang bisa digunakan saat menargetkan. Informasi tentang perangkat keamanan jaringan bisa mencakup berbagai detail, seperti keberadaan dan detail dari firewall, filter konten, dan proxy/hostname bastion yang telah diterapkan. Musuh juga bisa menargetkan informasi tentang sistem deteksi intrusi berbasis jaringan (NIDS) korban atau perangkat lain yang terkait dengan operasi keamanan siber defensif.

Dengan menggunakan perintah nmap -sV 103.140.108.76 dapat diketahui Network Security Appliances sebagai berikut:




*Gambar 4.35* Hasil *network security appliances dengan nmap* pada *ip address* pengujian

1. SSH (Port 22): Layanan ini mungkin digunakan untuk mengakses host secara remote. Meskipun SSH tidak secara khusus merupakan perangkat keamanan jaringan, namun seringkali digunakan untuk mengakses dan mengelola perangkat keamanan jaringan.

   Informasi "OpenSSH 7.6p1 Ubuntu 4ubuntu0.5 (Ubuntu Linux; protocol 2.0)" yang diberikan dalam hasil scan Nmap adalah deskripsi tentang versi dan

implementasi OpenSSH yang berjalan pada port 22 (SSH) pada host yang dipindai. Apabila dijabarkan sebagai berikut:

a. OpenSSH 7.6p1: Ini adalah versi OpenSSH yang digunakan. OpenSSH adalah perangkat lunak yang digunakan untuk mengamankan koneksi jaringan, terutama untuk mengakses shell jarak jauh atau transfer file secara aman melalui protokol SSH (Secure Shell). Versi 7.6p1 menunjukkan versi spesifik dari OpenSSH yang berjalan.
b. Ubuntu 4ubuntu0.5: Ini menunjukkan bahwa OpenSSH ini dikompilasi dan dikemas untuk distribusi Ubuntu Linux. Bagian "4ubuntu0.5" mengacu pada nomor versi paket Ubuntu spesifik. Nomor versi ini dapat berubah tergantung pada versi Ubuntu dan pembaruan paket yang diinstal.
c. Ubuntu Linux: Ini menunjukkan bahwa sistem operasi yang digunakan adalah Ubuntu Linux. Ubuntu adalah salah satu distribusi Linux yang populer dan sering digunakan di berbagai lingkungan, termasuk server dan desktop.
d. protocol 2.0: Ini mengindikasikan bahwa versi protokol SSH yang digunakan adalah versi 2.0. SSH protocol versi 2.0 adalah versi protokol yang lebih baru dan lebih aman dibandingkan dengan versi 1.0

2. DNS (Port 53): ISC BIND adalah server DNS yang dijalankan di host. Server DNS ini mungkin digunakan untuk menangani permintaan DNS dalam jaringan, yang penting untuk pengelolaan jaringan yang aman.
3. LDAP (Port 389): Layanan LDAP (Lightweight Directory Access Protocol) yang dijalankan mungkin digunakan untuk otentikasi dan otorisasi pengguna dalam jaringan, yang dapat menjadi bagian dari infrastruktur keamanan jaringan.

### 4.3.2 Credential Access (TA0006)

Penyerang mencoba mencuri nama akun dan sandi. Akses Kredensial terdiri dari teknik-teknik untuk mencuri kredensial seperti nama akun dan sandi. Teknik yang digunakan untuk mendapatkan kredensial meliputi keylogging atau credential dumping. Menggunakan kredensial yang sah dapat memberikan musuh akses ke

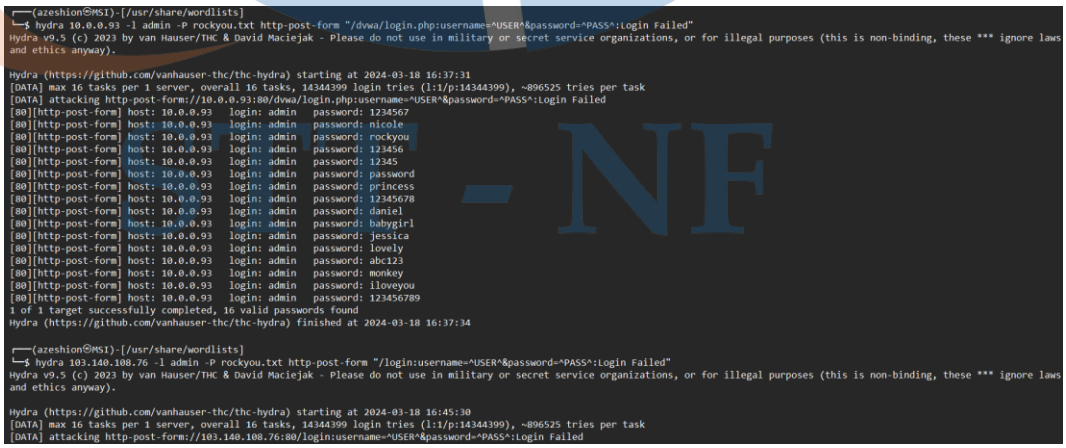
sistem, membuat mereka lebih sulit terdeteksi, dan memberikan kesempatan untuk membuat lebih banyak akun untuk membantu mencapai tujuan mereka.

### *Brute Force* (T1110)

Penyerang dapat menggunakan teknik brute force untuk mendapatkan akses ke akun ketika sandi tidak diketahui atau ketika hash sandi diperoleh. Tanpa pengetahuan tentang sandi untuk suatu akun atau sekumpulan akun, seorang musuh dapat secara sistematis menebak sandi menggunakan mekanisme yang repetitif atau iteratif. Proses brute forcing sandi dapat terjadi melalui interaksi dengan layanan yang akan memeriksa validitas kredensial tersebut atau secara offline terhadap data kredensial yang sebelumnya diperoleh, seperti hash sandi.

### *Password Spraying* (T1110. 003)

Penyerang dapat menggunakan satu atau beberapa kata sandi yang umum digunakan untuk mencoba mendapatkan kredensial akun yang valid. Password spraying menggunakan satu kata sandi (misalnya 'Password01'), atau daftar kecil kata sandi yang umum digunakan, yang mungkin sesuai dengan kebijakan kompleksitas domain. Login dicoba dengan kata sandi itu terhadap banyak akun yang berbeda di jaringan untuk menghindari pemblokiran akun yang biasanya terjadi saat melakukan brute force pada satu akun dengan banyak kata sandi.




*Gambar 4.36* Hasil *password spraying* dengan *hydra* pada *ip address* pengujian

Pertama, Anda mencoba masuk ke alamat IP 10.0.0.93, yang mungkin merupakan alamat dari suatu situs atau layanan web. Hydra akan mengirimkan permintaan login ke halaman /dvwa/login.php pada alamat tersebut. Setiap kata sandi dari daftar kata sandi rockyou.txt akan dicoba, dan Hydra akan memeriksa respon dari halaman tersebut. Jika Hydra menemukan pesan "Login Gagal" di halaman tersebut, itu berarti percobaan login tidak berhasil. Namun, jika tidak, Hydra akan menganggap bahwa itu adalah kata sandi yang benar.

Kemudian, Anda menggunakan Hydra lagi untuk mencoba masuk ke alamat IP 103.140.108.76, mungkin sebuah situs atau layanan web lainnya. Prosesnya mirip dengan yang pertama, namun kali ini Hydra akan mengirimkan permintaan login ke halaman /login. Hal yang sama dilakukan, yaitu mencoba berbagai kata sandi dari daftar kata sandi yang sama.

Pada akhirnya, Hydra berhasil menemukan beberapa kata sandi yang benar untuk akun dengan nama pengguna "***admin***" dan passwordnya adalah **"*password*"** pada IP 10.0.0.93 yang merupakan alamat dari IP yang memiliki kerentanan. Alasan mengapa pada percobaan di alamat IP 103.140.108.76 tidak berhasil karena:

1. Perbedaan Pengaturan: Mungkin konfigurasi aplikasi web atau firewall pada alamat IP kedua lebih ketat daripada pada alamat IP pertama. Beberapa situs web menerapkan langkah-langkah keamanan tambahan, seperti membatasi jumlah upaya login, menunda percobaan login yang gagal, atau meminta verifikasi CAPTCHA setelah sejumlah percobaan gagal.
2. Perbedaan Struktur Halaman Login: Halaman login pada alamat IP kedua mungkin memiliki struktur yang berbeda, sehingga pola yang digunakan oleh Hydra untuk menentukan apakah login berhasil atau tidak tidak sesuai. Ini bisa disebabkan oleh perbedaan atribut HTML, tata letak halaman yang berbeda, atau penggunaan JavaScript untuk mengelola proses login.
3. Firewall atau Sistem Keamanan Jaringan: Firewall atau Sistem Pencegahan Intrusi (IPS) mungkin telah mendeteksi aktivitas yang mencurigakan dari alamat IP Anda dan secara otomatis memblokir atau membatasi akses dari alamat IP Anda ke alamat IP tersebut.

4. Perbedaan Izin atau Autentikasi: Ada kemungkinan bahwa akun "admin" pada alamat IP kedua memiliki keamanan yang lebih baik, seperti kebijakan kata sandi yang lebih kuat atau mekanisme autentikasi tambahan, sehingga membuat serangan bruteforce lebih sulit untuk berhasil.
5. Proteksi CSRF Token: Kemungkinan besar halaman login pada alamat IP kedua dilindungi oleh token CSRF (Cross-Site Request Forgery) yang menghalangi serangan bruteforce. Token ini dapat mempersulit atau bahkan menghentikan serangan bruteforce karena setiap permintaan login harus menyertakan token yang valid yang hanya diperoleh dari halaman login itu sendiri.

### 4.3.3 Discovery (TA0007)

Discovery terdiri dari teknik-teknik yang mungkin digunakan oleh musuh untuk mendapatkan pengetahuan tentang sistem dan jaringan internal. Teknik-teknik ini membantu penyerang mengamati lingkungan dan mengorientasikan diri sebelum memutuskan cara bertindak. Mereka juga memungkinkan penyerang untuk mengeksplorasi apa yang dapat mereka kendalikan dan apa yang ada di sekitar titik masuk mereka untuk menemukan bagaimana hal itu dapat mendukung tujuan mereka saat ini. Alat bawaan sistem operasi sering digunakan untuk mencapai tujuan pengumpulan informasi pasca-kompromi ini.

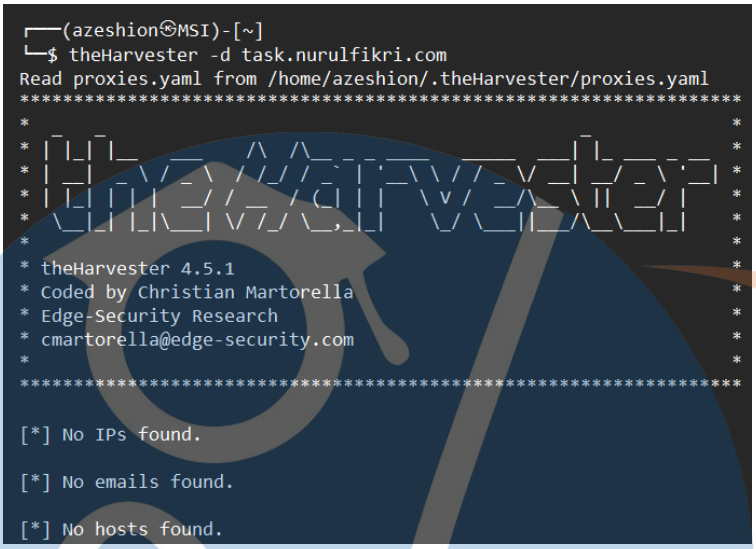
#### *Account Discovery* (T1087)

Musuh mungkin mencoba mendapatkan daftar akun yang valid, nama pengguna, atau alamat email di sebuah sistem atau dalam lingkungan yang terpengaruh. Informasi ini dapat membantu musuh menentukan akun mana yang ada, yang dapat membantu dalam perilaku lanjutan seperti *brute-forcing*, serangan *spear-phishing*, atau pengambilalihan akun (misalnya, akun yang valid).

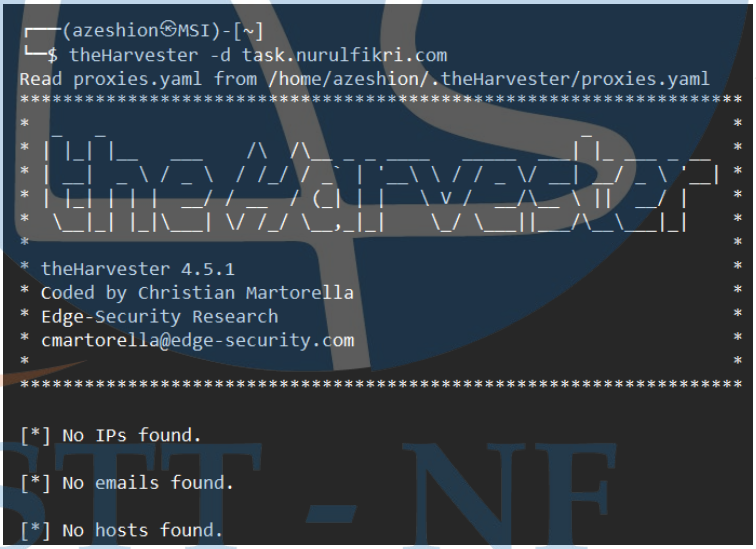
#### *Email Account* (T1087. 003)

Musuh mungkin mencoba mendapatkan daftar alamat email dan akun. Musuh dapat mencoba untuk mengambil daftar alamat email Exchange seperti daftar alamat global.

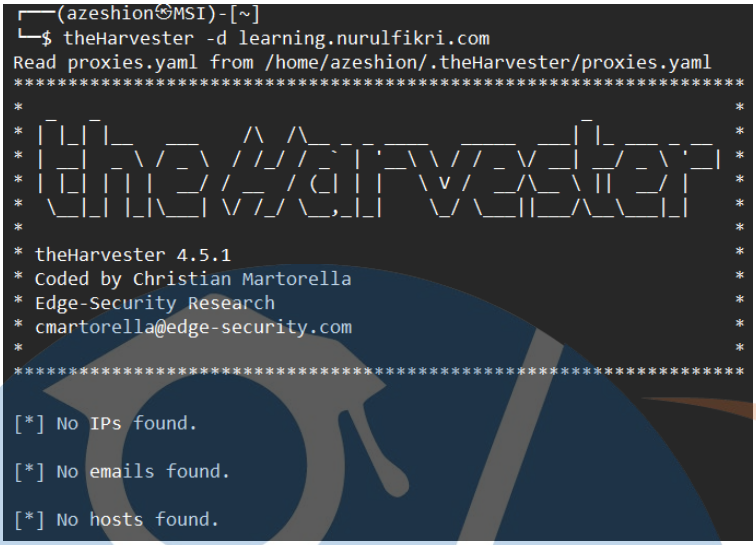
Hasil Discovery Email Account dari tools theHarvester pada domain task.nurulfikri.com, esertifikat.nurulfikri.com dan learning.nurulfikri.com.




*Gambar 4.37* Hasil *discovery* dengan *theHarvester* pada *ip address* task.nurulfikri.com



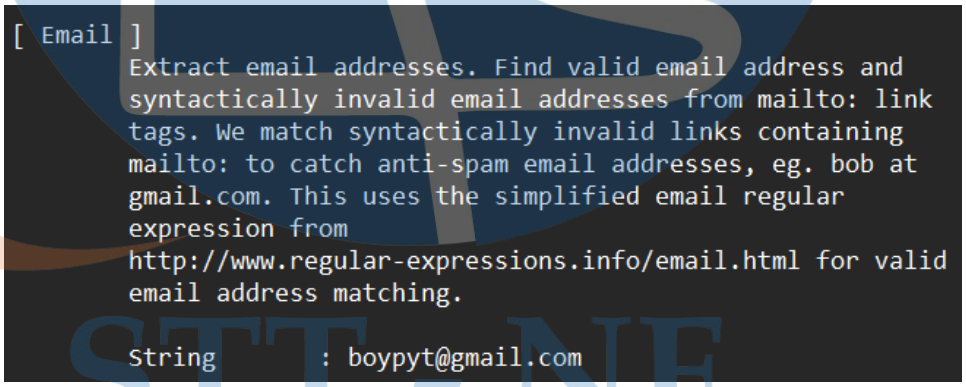

*Gambar 4.38* Hasil *discovery* dengan *theHarvester* pada *ip address* esertifikat.nurulfikri.com




*Gambar 4.39* Hasil *discovery* dengan *theHarvester* pada *ip address* learning.nurulfikri.com

Di hasil pengujian theHarvester di atas, tidak ada alamat email yang terkait ditemukan dengan situs web yang sedang diperiksa.

Hasil Discovery Email Account dari tools WhatWeb pada domain task.nurulfikri.com, esertifikat.nurulfikri.com dan learning.nurulfikri.com.




*Gambar 4.40* Hasil *discovery* dengan *whatweb* pada *ip address* pengujian

Hasil dari perangkat lunak WhatWeb menunjukkan bahwa alamat email "boypyt@gmail.com" ditemukan dalam kode sumber halaman web yang diperiksa. WhatWeb secara otomatis mengekstrak alamat email dari tag 'mailto:' dalam kode HTML. Ini mencakup pencarian alamat email yang valid serta alamat email yang mungkin tidak valid secara sintaksis, seperti contoh "bob at gmail.com", yang sering digunakan untuk menghindari pengambilan alamat email oleh program

spam. Metode ini didasarkan pada ekspresi reguler sederhana yang diambil dari sumber yang disebutkan. Dalam konteks ini, WhatWeb telah berhasil menemukan alamat email "boypyt@gmail.com" dalam halaman web yang dianalisis.

***File and Directory Discovery* (T1083)**

Musuh melakukan enumerasi file dan direktori atau mencari di lokasi tertentu dari sebuah host atau berbagi jaringan untuk mencari informasi tertentu dalam sistem file. Musuh dapat menggunakan informasi dari Penemuan Berkas dan Direktori selama penemuan otomatis untuk membentuk perilaku lanjutan, termasuk apakah musuh sepenuhnya menginfeksi target dan/atau mencoba tindakan-tindakan tertentu.

Hasil File and Directory Discovery dari tools Dirb pada alamat IP yang rentan:

```
---- Entering directory: http://10.0.0.93/twiki/bin/ ----
+ http://10.0.0.93/twiki/bin/attach (CODE:200|SIZE:4350)
+ http://10.0.0.93/twiki/bin/changes (CODE:200|SIZE:21773)
+ http://10.0.0.93/twiki/bin/edit (CODE:200|SIZE:5339)
+ http://10.0.0.93/twiki/bin/manage (CODE:302|SIZE:0)
+ http://10.0.0.93/twiki/bin/passwd (CODE:302|SIZE:0)
+ http://10.0.0.93/twiki/bin/preview (CODE:302|SIZE:0)
+ http://10.0.0.93/twiki/bin/register (CODE:302|SIZE:0)
+ http://10.0.0.93/twiki/bin/save (CODE:302|SIZE:0)
+ http://10.0.0.93/twiki/bin/search (CODE:200|SIZE:3530)
+ http://10.0.0.93/twiki/bin/statistics (CODE:200|SIZE:1194)
+ http://10.0.0.93/twiki/bin/upload (CODE:302|SIZE:0)
+ http://10.0.0.93/twiki/bin/view (CODE:200|SIZE:10024)
+ http://10.0.0.93/twiki/bin/viewfile (CODE:302|SIZE:0)

---- Entering directory: http://10.0.0.93/twiki/lib/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)

---- Entering directory: http://10.0.0.93/twiki/pub/ ----
+ http://10.0.0.93/twiki/pub/favicon.ico (CODE:200|SIZE:1078)
==> DIRECTORY: http://10.0.0.93/twiki/pub/Main/

---- Entering directory: http://10.0.0.93/phpMyAdmin/setup/frames/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)

---- Entering directory: http://10.0.0.93/phpMyAdmin/setup/lib/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)

---- Entering directory: http://10.0.0.93/twiki/pub/Main/ ----

-----------------
END_TIME: Mon Mar 18 10:45:33 2024
DOWNLOADED: 32284 - FOUND: 56
```

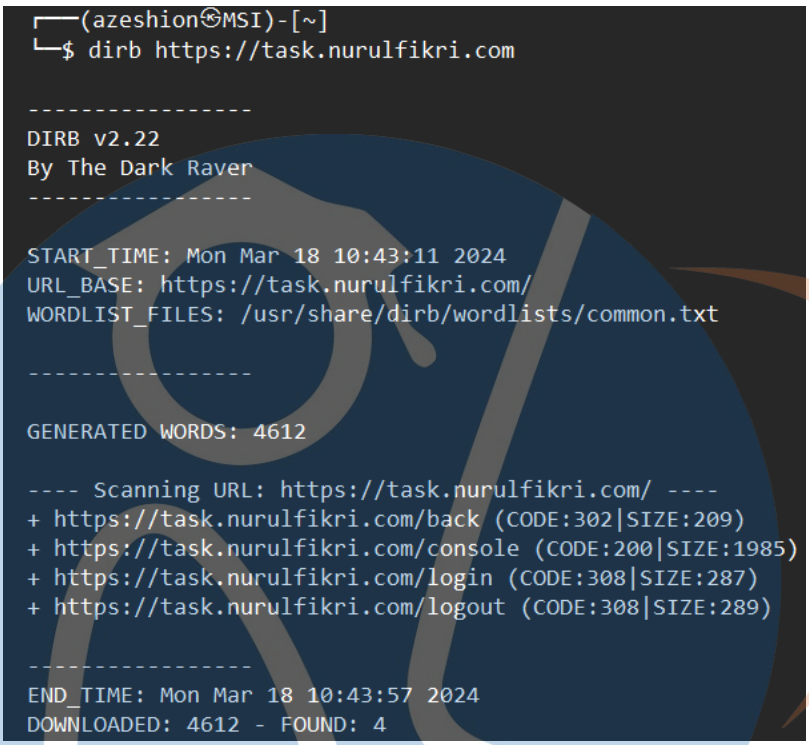
*Gambar 4.41* Hasil *file and directory discovery* dengan *dirb* pada *ip address* rentan

Hasil pemindaian dengan Dirb pada URL http://10.0.0.93 menunjukkan beberapa halaman dan direktori yang ditemukan:

1. /cgi-bin/ - Halaman tidak diizinkan (kode respons 403) dengan ukuran respons 290.
2. /dav/ - Direktori dengan akses yang diizinkan.
3. /index dan /index.php - Halaman yang terbuka dengan kode respons 200 dan ukuran respons 891.
4. /phpinfo dan /phpinfo.php - Halaman phpinfo yang terbuka dengan kode respons 200 dan ukuran respons yang berbeda-beda.
5. /phpMyAdmin/ - Direktori dengan beberapa sub-direktori dan halaman yang terbuka dengan kode respons 200.
6. /server-status - Halaman tidak diizinkan (kode respons 403) dengan ukuran respons 295.
7. /test/ dan /twiki/ - Direktori dengan akses yang diizinkan.

Selain itu, terdapat juga direktori dan halaman-halaman di dalam direktori /phpMyAdmin/, /test/, dan /twiki/ yang terbuka untuk diakses. Beberapa direktori juga memiliki akses yang diizinkan dan memberikan daftar file di dalamnya dan terdapat beberapa halaman dan direktori yang tidak dapat diakses atau tidak ditemukan, seperti /phpMyAdmin/phpinfo dan /phpMyAdmin/phpinfo.php, yang memberikan respons dengan ukuran 0.

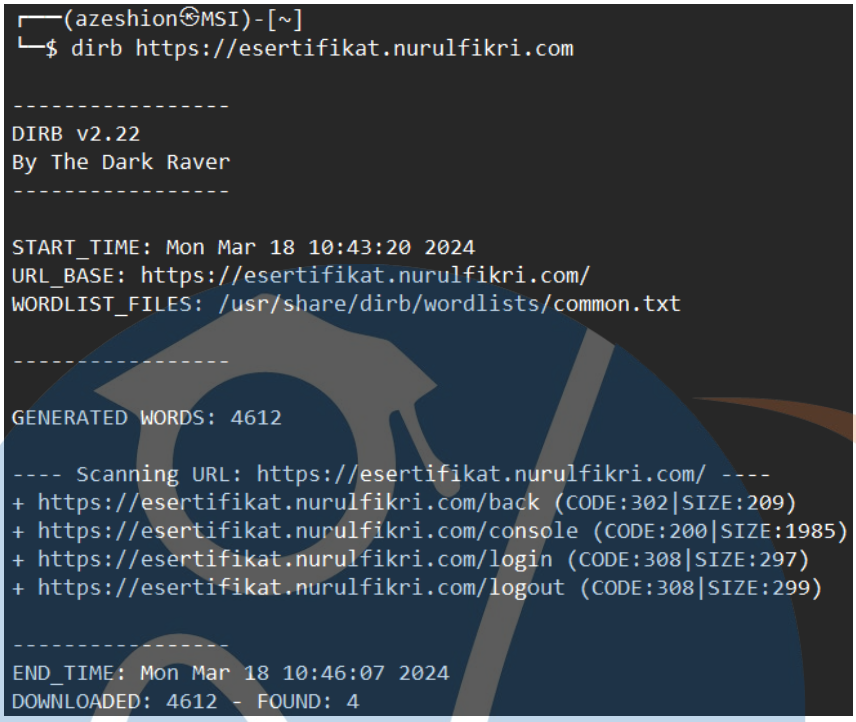
Hasil File and Directory Discovery dari tools Dirb pada domain task.nurulfikri.com, esertifikat.nurulfikri.com dan learning.nurulfikri.com.




*Gambar 4.42* Hasil *file and directory discovery* dengan *dirb* pada *ip address* task.nurulfikri.com

Dirb melakukan pemindaian pada URL https://task.nurulfikri.com dan menemukan beberapa direktori atau halaman:

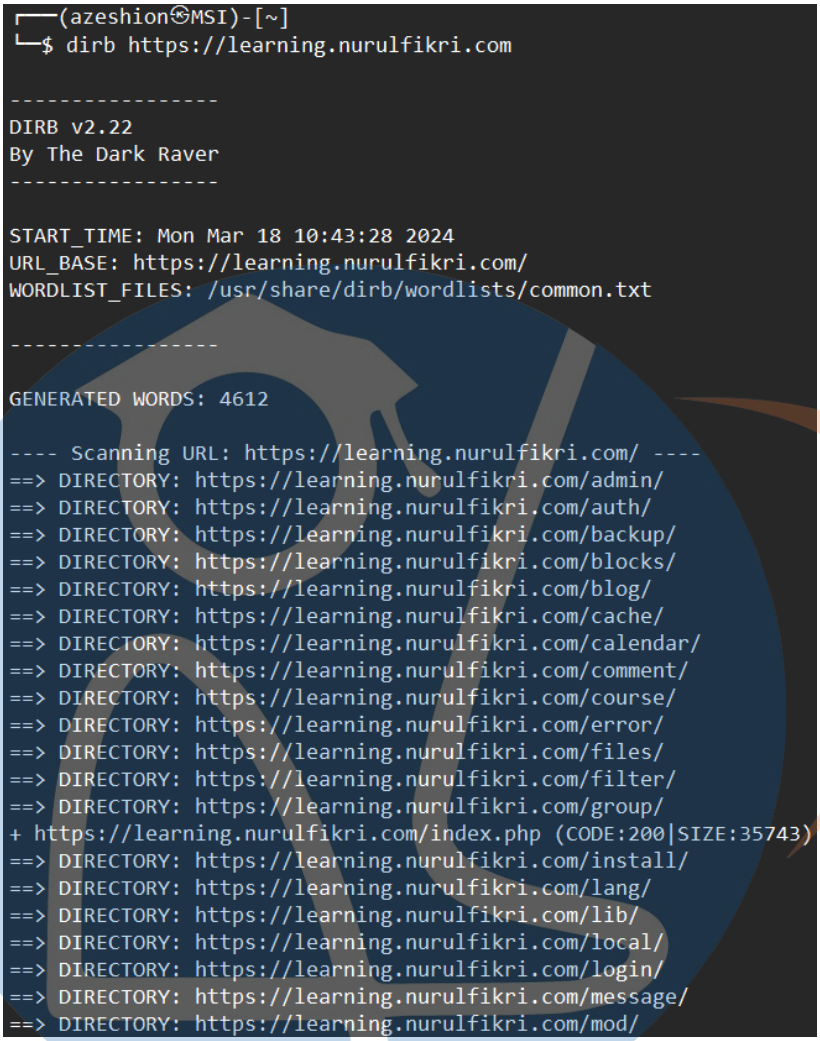
1. /back - Mengarahkan pengguna dengan kode respons 302 (Redirect) dan memiliki ukuran respons 209.
2. /console - Halaman terbuka dengan kode respons 200 (OK) dan memiliki ukuran respons 1985.
3. /login - Mengarahkan pengguna dengan kode respons 308 (Permanent Redirect) dan memiliki ukuran respons 287.
4. /logout - Mengarahkan pengguna dengan kode respons 308 (Permanent Redirect) dan memiliki ukuran respons 289.




*Gambar 4.43* Hasil *file and directory discovery* dengan *dirb* pada *ip address* esertifikat.nurulfikri.com

Dirb melakukan pemindaian pada URL https://esertifikat.nurulfikri.com dan menemukan beberapa direktori atau halaman:

1. /back - Mengarahkan pengguna dengan kode respons 302 (Redirect) dan memiliki ukuran respons 209.
2. /console - Halaman terbuka dengan kode respons 200 (OK) dan memiliki ukuran respons 1985.
3. /login - Mengarahkan pengguna dengan kode respons 308 (Permanent Redirect) dan memiliki ukuran respons 297.
4. /logout - Mengarahkan pengguna dengan kode respons 308 (Permanent Redirect) dan memiliki ukuran respons 299.




*Gambar 4.44* Hasil *file and directory discovery* dengan *dirb* pada *ip address* learning.nurulfikri.com

Dirb melakukan pemindaian pada URL https://learning.nurulfikri.com dan menemukan beberapa direktori atau halaman:

1. /admin/ - Direktori dengan beberapa sub-direktori seperti registration/, roles/, settings/, tests/, tool/, user/, webservice/. Juga terdapat dua file, yaitu index.php dan phpinfo.php, yang semuanya diarahkan dengan kode respons 303 (See Other) dan memiliki beberapa ukuran respons.
2. /auth/, /backup/, /blocks/, /blog/, /cache/, /calendar/, /comment/, /course/, /error/, /files/, /filter/, /group/, /install/, /lang/, /lib/, /local/, /login/, /message/, /mod/, /my/, /notes/, /pix/, /portfolio/, /question/, /rating/, /report/, /repository/,

/rss/, /tag/, /theme/, /user/, /webservice/ - Semua ini adalah direktori tanpa file yang terdeteksi.

Terdapat pula halaman lain seperti:

1. /index.php - Halaman terbuka dengan kode respons 200 (OK) dan memiliki ukuran respons 35743.
2. /server-status - Halaman terbuka dengan kode respons 403 (Forbidden) dan memiliki ukuran respons 312.

Alamat IP yang rentan, yang memiliki banyak kerentanan, mengalami serangan Directory Brute Force menggunakan dirb. Dalam serangan tersebut, banyak file dan folder yang dapat dilihat dan diakses karena menggunakan nama folder yang umum. Hal ini berbeda dengan alamat IP yang terhubung ke domain task.nurulfikri.com, esertifikat.nurulfikri.com, dan learning.nurulfikri.com yang menerapkan langkah-langkah pencegahan terhadap serangan Directory Brute Force seperti:

1. Penggunaan nama folder yang tidak umum: Hindari penggunaan nama folder yang umum atau mainstream. Menggunakan nama folder yang tidak mudah ditebak atau mengandung kombinasi karakter yang rumit dapat membuat serangan directory brute force lebih sulit dilakukan. Misalnya, mengganti nama folder default seperti "admin", "uploads", atau "images" dengan nama yang unik dan tidak mudah ditebak dapat memberikan lapisan perlindungan tambahan.
2. Pembatasan percobaan akses: Mengimplementasikan pembatasan percobaan akses pada server web dapat membantu mencegah serangan brute force. Ini membatasi jumlah percobaan yang dapat dilakukan dalam jangka waktu tertentu, sehingga serangan brute force menjadi tidak efektif.
3. Monitoring dan deteksi aktivitas mencurigakan: Memantau aktivitas pada server web dan mendeteksi pola akses yang mencurigakan dapat membantu dalam mengidentifikasi serangan directory brute force secara cepat. Dengan memperhatikan pola lalu lintas yang tidak biasa atau percobaan akses yang

berulang, tindakan pencegahan dapat diambil dengan cepat untuk melindungi folder dan file.

4. Pembaruan dan patching teratur: Melakukan pembaruan dan patching teratur pada sistem operasi, perangkat lunak server, dan aplikasi web dapat membantu dalam memperbaiki kerentanan keamanan yang mungkin dapat dieksploitasi oleh serangan directory brute force dan serangan lainnya.

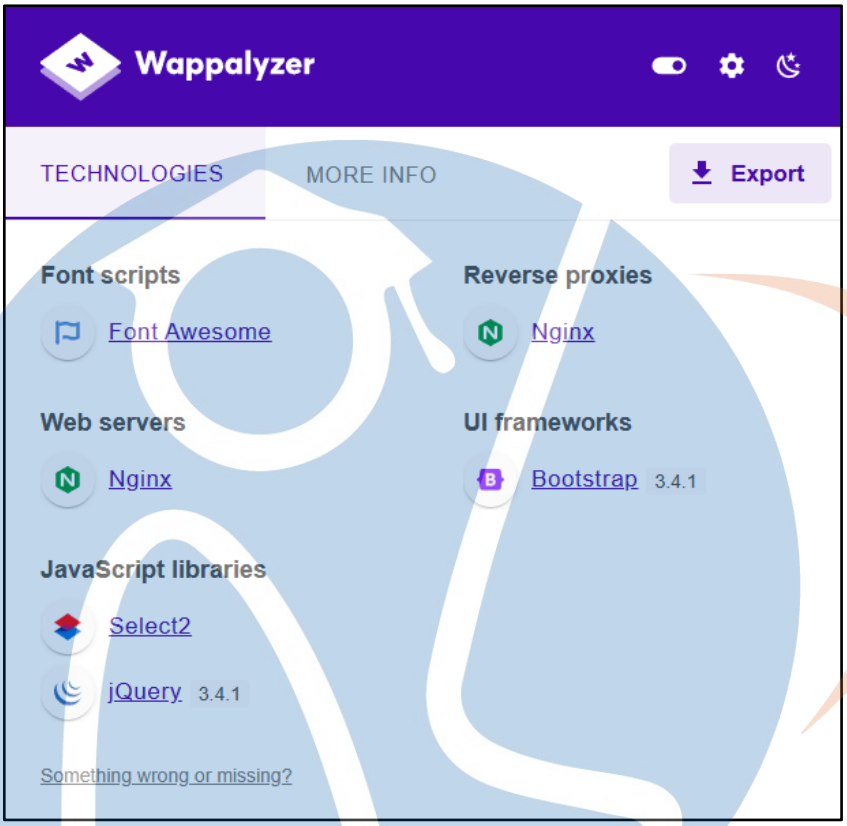
***Software Discovery* (T1518)**

Penyerang mencoba mendapatkan daftar perangkat lunak dan versi perangkat lunak yang terpasang di sistem atau dalam lingkungan cloud. Musuh dapat menggunakan informasi dari Penemuan Perangkat Lunak selama penemuan otomatis untuk membentuk perilaku lanjutan, termasuk apakah musuh sepenuhnya menginfeksi target dan/atau mencoba tindakan-tindakan tertentu.

***Security Software Discovery* (T1518. 001)**

Penyerang mencoba mendapatkan daftar perangkat lunak keamanan, konfigurasi, alat pertahanan, dan sensor yang terpasang di sistem atau dalam lingkungan cloud. Hal ini dapat mencakup hal-hal seperti aturan firewall dan antivirus. Musuh dapat menggunakan informasi dari Penemuan Perangkat Lunak Keamanan selama penemuan otomatis untuk membentuk perilaku lanjutan, termasuk apakah musuh sepenuhnya menginfeksi target dan/atau mencoba tindakan-tindakan tertentu.

Hasil dari Security Software Discovery menggunakan tools Wappalyzer pada domain task.nurulfikri.com



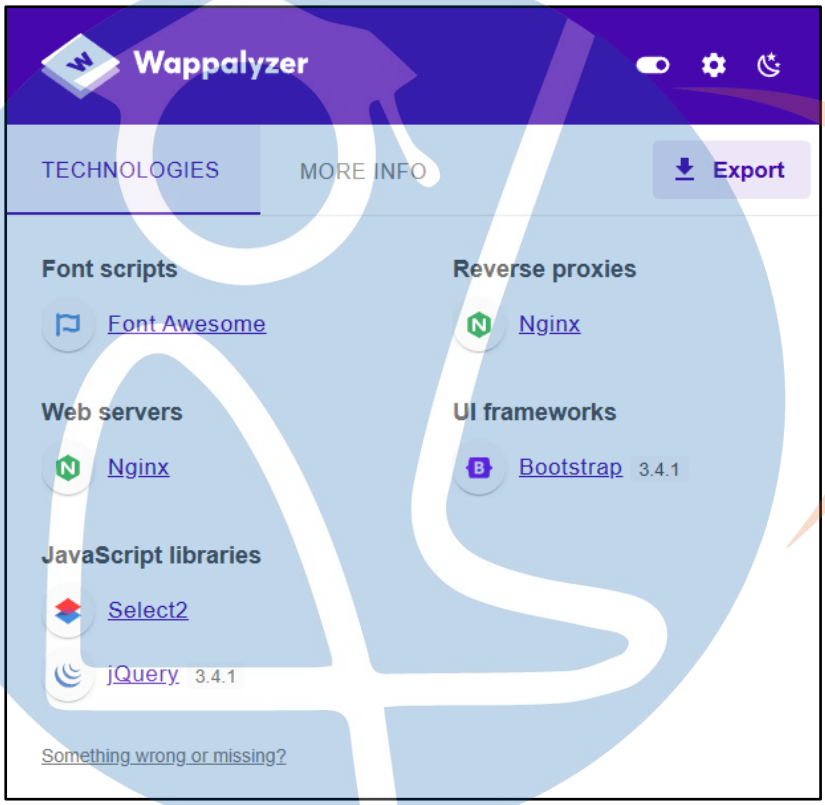

*Gambar 4.45* Hasil *security software discovery* dengan *wappalyzer* pada task.nurulfikri.com

Berdasarkan hasil dari Wappalyzer pada situs task.nurulfikri.com, ditemukan beberapa informasi mengenai teknologi yang digunakan:

1. Font Scripts: Situs menggunakan Font Awesome untuk manajemen font pada halaman webnya.
2. Reverse Proxies: Nginx digunakan sebagai reverse proxy server untuk melayani permintaan dari klien dan mengarahkannya ke server backend.
3. Web Servers: Server web yang digunakan adalah Nginx, yang bertindak sebagai server utama untuk mengirimkan konten halaman web kepada pengguna.
4. UI Frameworks: Situs menggunakan Bootstrap versi 3.4.1 sebagai framework UI untuk memperindah tampilan halaman web dan mempercepat pengembangan.

5. Javascript Libraries: Ditemukan penggunaan Select2 dan jQuery versi 3.4.1 untuk mengelola elemen formulir dan menambahkan fungsi interaktif pada halaman web.

Hasil dari Security Software Discovery menggunakan tools Wappalyzer pada domain esertifikat.nurulfikri.com



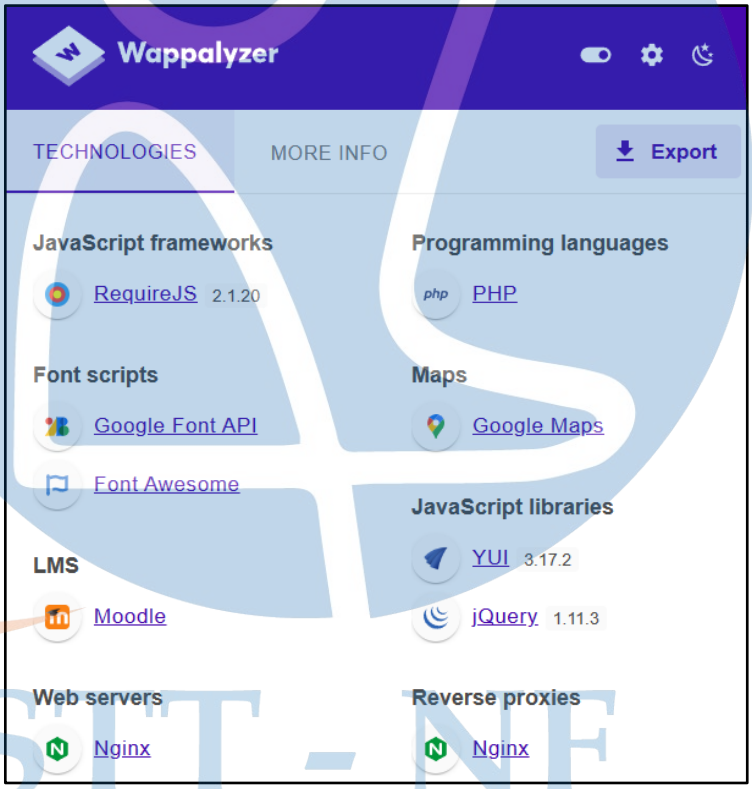

*Gambar 4.46* Hasil *security software discovery* dengan *wappalyzer* pada esertifikat.nurulfikri.com

Berdasarkan hasil dari Wappalyzer pada situs task.nurulfikri.com, ditemukan beberapa informasi teknologi yang digunakan:

1. Keamanan: Situs menggunakan reCAPTCHA untuk meningkatkan keamanan dan mencegah akses yang tidak diinginkan.
2. Pustaka JavaScript: Ditemukan penggunaan Select2 dan jQuery versi 3.4.1 untuk menyediakan fitur interaktif pada halaman web.
3. Font Scripts: Font Awesome digunakan untuk manajemen font pada halaman webnya.

4. Reverse Proxies: Nginx berfungsi sebagai reverse proxy server untuk mengelola permintaan dari klien dan mengarahkannya ke server backend.
5. Server Web: Server web yang digunakan adalah Nginx, yang bertindak sebagai server utama untuk mengirimkan konten halaman web kepada pengguna.
6. Framework UI: Situs menggunakan Bootstrap untuk mengatur tata letak dan desain halaman web, memperindah tampilan serta mempercepat pengembangan.

Hasil dari Security Software Discovery menggunakan tools Wappalyzer pada domain learning.nurulfikri.com




*Gambar 4.47* Hasil *security software discovery* dengan *wappalyzer* pada learning.nurulfikri.com

Berdasarkan hasil analisis dari Wappalyzer pada situs task.nurulfikri.com, ditemukan beberapa informasi teknologi yang digunakan:

1. Pustaka JavaScript: Situs menggunakan Yui versi 3.17.2 dan jQuery versi 1.11.3 untuk mengimplementasikan berbagai fungsi JavaScript di dalam halaman webnya.

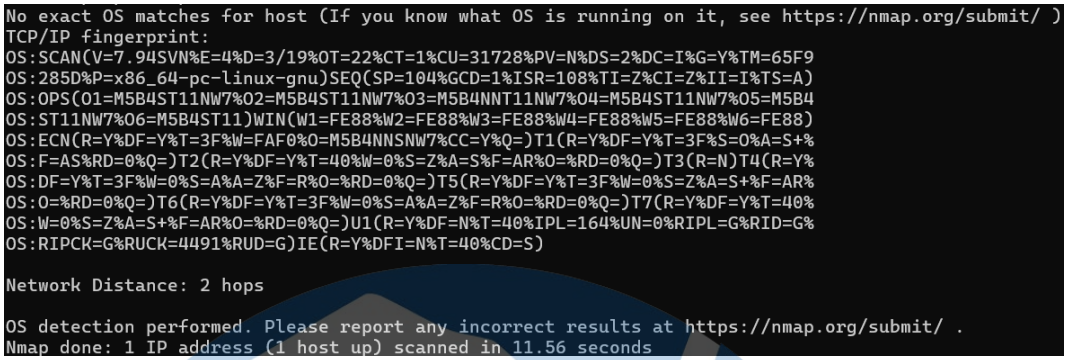
2. Font Scripts: Font Awesome dan Google Font API digunakan untuk manajemen dan pengaturan tampilan font pada halaman web.
3. Reverse Proxies: Nginx berfungsi sebagai reverse proxy server yang mengelola lalu lintas HTTP antara klien dan server backend.
4. Server Web: Situs menggunakan Nginx sebagai server web utama untuk melayani konten halaman web kepada pengguna.
5. Frameworks JavaScript: RequireJS versi 2.1.20 digunakan untuk manajemen dependensi JavaScript pada halaman web, memungkinkan pengaturan modul dan pemuatan sumber daya secara dinamis.
6. LMS (Learning Management System): Moodle digunakan sebagai platform LMS untuk menyediakan berbagai konten pembelajaran dan manajemen kursus.
7. Bahasa Pemrograman: PHP digunakan sebagai bahasa pemrograman utama untuk mengembangkan fungsi dan fitur pada situs.

***System Information Discovery* (T1082)**

Seorang penyerang mungkin mencoba untuk mendapatkan informasi terperinci tentang sistem operasi dan perangkat keras, termasuk versi, patch, hotfixes, service pack, dan arsitektur. Penyerang dapat menggunakan informasi dari Penemuan Informasi Sistem selama penemuan otomatis untuk membentuk perilaku lanjutan, termasuk apakah penyerang sepenuhnya menginfeksi target dan/atau mencoba tindakan tertentu.

```
Aggressive OS guesses: Linux 2.6.18 (89%),
Linux 2.6.32 (88%), Linux 2.6.39 (87%), Linux 2.6.30 (87%),
Linux 2.6.32 - 2.6.35 (87%), Linux 2.6.32 or 3.10 (87%),
Linux 3.10 - 3.12 (87%), Linux 3.4 (87%), Linux 3.5 (87%),
Linux 4.2 (87%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 8 hops
```

*Gambar 4.48* Hasil *system information discovery 1* dengan *nmap -O* pada *ip address* pengujian




*Gambar 4.49* Hasil *system information discovery 2* dengan *nmap -O* pada *ip address* pengujian

Hasil pada gambar 4.48 dilakukan lima hari sebelum hasil pada gambar 4.49 dilakukan. Pada hasil pertama, terlihat kemungkinan sistem operasi yang digunakan, sementara pada hasil kedua, sistem operasi yang kemungkinan digunakan tidak terlihat, dan hasilnya tetap sama setelah beberapa kali pemindaian, hal ini dapat terjadi karena:

1. Firewall atau Filtering: Host target mungkin berada di belakang firewall atau perangkat penyaringan jaringan yang mengubah atau memblokir paket tertentu, sehingga sulit bagi alat identifikasi sistem operasi untuk menentukan sistem operasi dengan akurat.
2. Limited Information: Alat mungkin tidak menerima cukup respons dari host target untuk dengan percaya diri menentukan sistem operasinya. Hal ini bisa disebabkan oleh kemacetan jaringan, kehilangan paket, atau masalah jaringan lainnya.
3. Unusual Configuration: Host target mungkin menjalankan konfigurasi sistem operasi yang tidak lazim atau disesuaikan yang tidak cocok dengan tanda tangan OS yang dikenal dalam database identifikasi sistem operasi yang digunakan oleh alat.
4. Anti-Fingerprinting Techniques: Host target mungkin disengaja dikonfigurasi untuk menghambat upaya identifikasi sistem operasi, menggunakan teknik seperti penyaringan paket, merandomkan respons, atau meniru beberapa sistem operasi.

5. Outdated Fingerprint Database: Alat identifikasi sistem operasi mungkin menggunakan database tanda tangan sistem operasi yang usang atau tidak lengkap, menyebabkan ketidakakuratan dalam proses identifikasi.

# BAB V
# KESIMPULAN DAN SARAN

Pada Bab V ini, akan diuraikan kesimpulan dari analisis dan pembahasan pada bab-bab sebelumnya. Kesimpulan ini mencerminkan pemahaman mendalam terhadap topik yang dibahas dan menyoroti temuan kunci yang diidentifikasi. Bab ini juga memberikan saran-saran konstruktif sebagai landasan untuk pengembangan lebih lanjut dalam konteks penelitian ini. Sebagai puncak penelitian, Bab V memberikan gambaran komprehensif dan arah untuk pengembangan pengetahuan di masa mendatang.

## Kesimpulan

1. Penggunaan MITRE ATT&CK Framework memengaruhi identifikasi celah dan kelemahan keamanan dalam suatu organisasi dengan memberikan kerangka kerja yang komprehensif untuk memahami serangan siber yang potensial. Dengan menggunakan MITRE ATT&CK, organisasi dapat mengidentifikasi teknik-teknik yang mungkin digunakan oleh penyerang dan menyesuaikan strategi pertahanan mereka di sepanjang siklus hidup serangan.
2. Dampak penggunaan MITRE ATT&CK Framework dalam red team terhadap perbaikan kebijakan dan prosedur keamanan organisasi adalah signifikan. Red team dapat menggunakan framework ini untuk merancang serangan simulasi yang realistis dan mencari celah keamanan yang mungkin tidak terdeteksi sebelumnya. Hasil dari serangan red team dapat memberikan wawasan yang berharga kepada organisasi tentang kelemahan dalam sistem keamanan mereka dan mendorong perbaikan kebijakan serta prosedur keamanan.
3. Hasil penelitian ini memberikan wawasan yang lebih dalam tentang penggunaan MITRE ATT&CK Framework dalam konteks red team untuk menguji dan meningkatkan postur keamanan. Dengan menggabungkan teknik-teknik serangan yang terdokumentasi dengan pemahaman mendalam tentang infrastruktur dan kebijakan keamanan organisasi, red team dapat melakukan evaluasi yang lebih efektif terhadap keamanan organisasi. Hasil dari evaluasi tersebut dapat digunakan untuk memperbaiki sistem keamanan, meningkatkan

kesiapan dalam menghadapi serangan siber, dan mengurangi risiko yang dihadapi oleh organisasi.

**Saran**

Organisasi disarankan untuk mengonfigurasi kebijakan keamanan web seperti Content Security Policy (CSP) dan memastikan pengaturan HTTP security headers seperti X-Content-Type-Options dan Strict-Transport-Security telah diaktifkan. Selain itu, pemindaian berkala menggunakan alat seperti Nmap dapat membantu mengidentifikasi perangkat dan layanan yang berjalan di jaringan, sementara alat Skipfish dapat digunakan untuk mengevaluasi dan menangani kerentanan keamanan web yang mungkin ada.

Dalam konteks strategi pertahanan, penggunaan MITRE ATT&CK Framework dapat memberikan pemahaman yang lebih baik tentang teknik-teknik serangan yang mungkin digunakan oleh penyerang, memungkinkan organisasi untuk memperbaiki kebijakan dan prosedur keamanan mereka. Evaluasi dan perbaikan proses keamanan, termasuk memberikan pelatihan keamanan kepada personel yang terlibat, juga menjadi kunci dalam mengurangi risiko serangan dan melindungi aset organisasi dari ancaman siber.

# DAFTAR PUSTAKA


[1] Xiong, W., Legrand, E., Åberg, O., & Lagerström, R. (2022). Cyber security threat modeling based on the MITRE Enterprise ATT&CK Matrix. *Software and Systems Modeling*, *21*(1), 157–177. https://doi.org/10.1007/s10270-021-00898-7

[2] Oruc, A., Amro, A., & Gkioulos, V. (2022). Assessing Cyber Risks of an INS Using the MITRE ATT&CK Framework. *Sensors*, *22*(22). https://doi.org/10.3390/s22228745

[3] Georgiadou, A., Mouzakitis, S., & Askounis, D. (2021). Assessing mitre att&ck risk using a cyber-security culture framework. *Sensors*, *21*(9). https://doi.org/10.3390/s21093267

[4] Grigorescu, O., Nica, A., Dascalu, M., & Rughinis, R. (2022). CVE2ATT&CK: BERT-Based Mapping of CVEs to MITRE ATT&CK Techniques. *Algorithms*, *15*(9). https://doi.org/10.3390/a15090314

[5] Strom, B. E., Applebaum, A., Miller, D. P., Nickels, K. C., Pennington, A. G., & Thomas, C. B. (n.d.). *MITRE ATT&CK®: Design and Philosophy*.

[6] g0tmi1k. (2023, March 13). *About Kali Linux*. https://www.kali.org/docs/introduction/what-is-kali-linux/ *(accessed on October 2023)*

[7] Bryce G. Hoffman. (2017). *Red Teaming: How Your Business Can Conquer the Competition by Challenging Everything*.

[8] Ahmad Dahlan Yogyakarta Indonesia, U., & Ananda Raharja, P. (2019). Vulnerability Analysis of E-voting Application using Open Web Application Security Project (OWASP) Framework. In *IJACSA) International Journal of Advanced Computer Science and Applications* (Vol. 10, Issue 11). www.ijacsa.thesai.org

[9] Devi, R. S., & Kumar, M. M. (2020). Testing for Security Weakness of Web Applications using Ethical Hacking. *Proceedings of the 4th International*

*Conference on Trends in Electronics and Informatics, ICOEI 2020*, 354–361. https://doi.org/10.1109/ICOEI48184.2020.9143018

[10] Baklizi, M., Atoum, I., Abdullah, N., Al-Wesabi, O. A., Ali Otoom, A., & Al-Sheikh Hasan, M. (n.d.). International Journal of INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING A Technical Review of SQL Injection Tools and Methods: A Case Study of SQL Map. In *Original Research Paper International Journal of Intelligent Systems and Applications in Engineering IJISAE* (Vol. 2022, Issue 3). www.ijisae.org

[11] Rashid, S. M. Z. U., Kamrul, M. I., & Islam, A. (2019, April 1). Understanding the Security Threats of Esoteric Subdomain Takeover and Prevention Scheme. *2nd International Conference on Electrical, Computer and Communication Engineering, ECCE 2019*. https://doi.org/10.1109/ECACE.2019.8679122

[12] Hossein Ashtari. (2022, August). *What Is VirtualBox? Meaning, Working, Installation, and Uses*. https://Www.Spiceworks.Com/Tech/Cloud/Articles/What-Is-Virtualbox/.

[13 ]Rudiharto. (2021, May). *Apa itu nslookup? Pengertian, Fungsi dan Cara Menggunakan*. https://Www.Rumahweb.Com/Journal/Apa-Itu-Nslookup-Adalah/.

[14] Micah Zenko. (2015). *Red Team: How to Succeed By Thinking Like the Enemy*.

[15 ]Containerize. (2023). *Ruby Based Next Generation Website Vulnerability Scanner*. Https://Products.Containerize.Com/Security-Testing-Tools/Whatweb/.

[16] Abi Tyas Tunggal. (2023, July). *What is a Vulnerability? Definition + Examples*. https://Www.Upguard.Com/Blog/Vulnerability.

[17] Dafydd Stuttard, & Marcus Pinto. (2011). *The Web Application Hacker's Handbook: Finding and Exploiting Security Flaws* (2nd ed.). John Wiley & Sons.

[18] MDN contributors. (2023, July 7). *Content Security Policy (CSP)*. https://Developer.Mozilla.Org/En-US/Docs/Web/HTTP/CSP.

[19] MDN contributors. (2024, January 10). *Set-Cookie*. https://Developer.Mozilla.Org/En-US/Docs/Web/HTTP/Headers/Set-Cookie#samesitesamesite-Value.

[20] Adam Barth. (2011, April). *HTTP State Management Mechanism*. https://Datatracker.Ietf.Org/Doc/Html/Rfc6265.

[21] KirstenS. (n.d.). *Cross Site Scripting (XSS)*. https://Owasp.Org/Www-Community/Attacks/Xss/.

[22] MDN contributors. (2023, December 19). *Cross-Origin Resource Sharing (CORS)*. https://Developer.Mozilla.Org/En-US/Docs/Web/HTTP/CORS.

[23] MDN contributors. (2023, December 12). *X-Frame-Options*. https://Developer.Mozilla.Org/En-US/Docs/Web/HTTP/Headers/X-Frame-Options.

[24] kingthorin. (n.d.). *SQL Injection*. https://Owasp.Org/Www-Community/Attacks/SQL_Injection.

[25] OWASP. (2017). *A9:2017-Using Components with Known Vulnerabilities*. https://Owasp.Org/Www-Project-Top-Ten/2017/A9_2017-Using_Components_with_Known_Vulnerabilities.Html.

[26] MDN contributors. (2023, May 10). *X-Content-Type-Options*. https://Developer.Mozilla.Org/En-US/Docs/Web/HTTP/Headers/X-Content-Type-Options.

[27] thc hydra. (n.d.). *Hydra Official Documentation*. Retrieved March 19, 2024, from https://github.com/vanhauser-thc/thc-hydra

[28] Wappalyzer. (n.d.). *Wappalyzer Official Documentation*. Retrieved March 19, 2024, from https://www.wappalyzer.com/

[29] Peter Kim. (2018). *The Hacker Playbook 3: Practical Guide to Penetration Testing*. Secure Planet LLC.

[30] Nicolas Surribas. (n.d.). *Wapiti*. Retrieved March 19, 2024, from https://wapiti-scanner.github.io/