

OSINT AND SOCIAL ENGINEERING



Prepared by

Kayla Putri Maharani

5026231158

PAI B

```
// code block containing various JavaScript functions and logic related to OSINT and Social Engineering tasks.
```

OVER ---- VIEW

Praktikum 5 berfokus pada penerapan teknik **Open Source Intelligence (OSINT)** dan **Social Engineering** dalam konteks keamanan siber. Tujuannya adalah melatih kemampuan dalam mengumpulkan, menganalisis, dan memverifikasi informasi publik secara etis untuk mengidentifikasi potensi ancaman dan pola rekayasa sosial. Praktikum ini juga menekankan penggunaan berbagai alat OSINT, seperti Wayback Machine, Google Maps, dan MITRE ATT&CK, untuk mendukung proses investigasi dan penyusunan laporan intelijen yang sistematis.

PRAKTIKUM 5 ---- REPORT

Table of Content

Challenge 1.....	3
Planning & Direction.....	3
Collection.....	4
Processing & Exploitation.....	5
Analysis & Production.....	6
Dissemination & Integration.....	7
Challenge 2.....	8
Planning & Direction.....	8
Collection.....	9
Processing & Exploitation.....	10
Analysis & Production.....	11
Dissemination & Integration.....	12
Challenge 3.....	13
Planning & Direction.....	13
Collection.....	14
Processing & Exploitation.....	15
Analysis & Production.....	16
Dissemination & Integration.....	17
Challenge 4.....	18
Planning & Direction.....	18
Collection.....	19
Processing & Exploitation.....	20
Analysis & Production.....	21
Dissemination & Integration.....	22

Challenge 1

One morning, an analyst discovered something odd in the domain controller logs. The machine account password had been changed, but no one on the admin team had touched it. The logs indicated that the change originated from an anonymous session, and the IP address was that of a laptop contractor who wasn't even part of the domain. A few minutes later, the system showed privileged activity using the machine account instead of a regular user. The infrastructure team explained that they had recently relaxed Netlogon settings so that SAP BusinessObjects 4.2 running on Windows Server 2008 R2 could still authenticate to Active Directory.

Can you find which CVE this is?

Planning & Direction

Objective Statement

Tujuan dari analisis ini adalah untuk mencari tahu jenis kerentanan keamanan (CVE) yang paling sesuai dengan kasus pada soal, yaitu perubahan password akun mesin di Domain Controller yang terjadi dari sesi anonim. Analisis dilakukan untuk memahami penyebab kemungkinan dari kejadian tersebut.

Scope and Limitations

Analisis ini berfokus pada sistem Windows Server 2008 R2 dan layanan Netlogon yang digunakan untuk proses autentikasi ke Active Directory. Pencarian informasi dilakukan hanya melalui sumber terbuka seperti situs CVE dan Microsoft Security Response Center. Karena tidak memiliki akses langsung ke log sistem, hasil analisis ini hanya berdasarkan pada informasi yang tersedia secara publik.

Stakeholders

Hasil dari analisis ini ditujukan untuk dosen pengampu dan peserta praktikum keamanan informasi sebagai latihan dalam mengidentifikasi kerentanan sistem menggunakan sumber terbuka.

Priority and Timeline

Analisis ini bersifat prioritas karena kasus menggambarkan potensi serangan serius pada sistem domain. Pengeraaan dilakukan dalam satu sesi praktikum dengan waktu penyelesaian yang singkat.

Collection

Sources

Data dan informasi diambil dari:

1. National Vulnerability Database (NVD)
2. Microsoft Security Response Center (MSRC)
3. CVE Details

Collection Methods

Pencarian dilakukan secara manual dengan menggunakan beberapa kata kunci yang berasal dari isi soal, seperti "machine account password changed," "anonymous session," "Netlogon," dan "Windows Server 2008 R2."

Dari hasil pencarian tersebut ditemukan beberapa CVE yang mirip, kemudian dibandingkan satu per satu untuk melihat mana yang paling sesuai dengan kondisi yang ada di soal.

Ethical and Legal Compliance

Seluruh data diperoleh dari sumber publik dan tidak ada proses eksplorasi atau akses ke sistem manapun. Semua langkah dilakukan untuk tujuan pembelajaran.

Documentation

URL dari setiap situs beserta tanggal akses dicatat untuk dokumentasi hasil pencarian.

No	Sumber	Jenis	URL atau rujukan	Tanggal Akses	Catatan
1	NVD - CVE-2020-1472	Database CVE	https://nvd.nist.gov/vuln/detail/CVE-2020-1472	31 Oktober 2025 21:10 WIB	Ringkasan CVE dan CVSS
2	Microsoft Security Response Center	Vendor advisory	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2020-1472	31 Oktober 2025 21:15 WIB	Panduan mitigasi dan rollout patch
3	CVE Details	Portal CVE	https://www.cvedetails.com/cve/CVE-2020-1472/	31 Oktober 2025 21:20 WIB	Daftar produk terdampak dan referensi tambahan

4	Query Google	Metode pencarian	Query: privilege Zerologon	Netlogon escalation	31 Oktober 2025 20:55 WIB	Kata kunci yang dipakai untuk menelusuri CVE terkait
---	--------------	------------------	----------------------------	---------------------	---------------------------	--

Processing & Exploitation

Data Cleaning

Hasil pencarian yang tidak berhubungan dengan Netlogon atau Windows Server 2008 R2 disaring agar hanya tersisa entri CVE yang relevan.

Normalization

Informasi dari setiap situs disusun dalam format yang sama, yaitu nama CVE, tahun, produk yang terdampak, dan penjelasan singkatnya.

Organization

Hasil pencarian disimpan dalam tabel sederhana supaya mudah dibandingkan antar CVE.

Tagging and Correlation

Kata kunci pada soal seperti “anonymous session” dan “Netlogon” dicocokkan dengan deskripsi yang ada pada setiap CVE untuk melihat apakah ada kesamaan konteks. Dari proses ini ditemukan satu CVE yang paling cocok dengan kasus di soal.

Analysis & Production

The screenshot displays the CVE-2020-1472 record from the NVD. Key details include:

- CNA:** Microsoft Corporation
- Published:** 2020-08-17 | **Updated:** 2024-05-29
- Title:** Netlogon Elevation Of Privilege Vulnerability
- Description:** An elevation of privilege vulnerability exists when an attacker establishes a vulnerable Netlogon secure channel connection to a domain controller, using the Netlogon Remote Protocol (MS-NRPC). An attacker who successfully exploited the vulnerability could run a specially crafted application on a device on the network. To exploit the vulnerability, an unauthenticated attacker would be required to use MS-NRPC to connect to a domain controller to obtain domain administrator access.
- CVSS:** 5.5 (Total)
- Product Status:** Affected (from 10.0.0 before publication)
- Vendor:** Microsoft
- Product:** Windows Server 2019 (Server Core installation)
- Platforms:** x64-based Systems
- References:** 17 Total (links to various security advisories and mailing lists).

Analytical Methods

Analisis dilakukan dengan membandingkan isi soal dengan hasil pencarian dari berbagai situs CVE. Fokus utama ada pada kesamaan konteks, mekanisme serangan, dan sistem yang terdampak.

Interpretation

Dari hasil pencarian dengan kata kunci yang diambil dari soal, ditemukan bahwa kerentanan yang paling sesuai adalah **CVE-2020-1472**, yang dikenal dengan nama *Zerologon*. CVE ini menjelaskan adanya celah keamanan pada layanan *Netlogon Remote Protocol* yang memungkinkan seseorang tanpa autentikasi bisa mengubah password akun mesin di Domain Controller. Hal ini sama seperti kondisi yang dijelaskan dalam soal.

Validation

Deskripsi resmi dari Microsoft Security Response Center dan NVD menunjukkan bahwa kerentanan ini memang berdampak pada Windows Server 2008 R2 dan bisa menyebabkan peningkatan hak akses hingga level administrator domain.

Findings and Implications

Temuan menunjukkan bahwa kasus pada soal menggambarkan skenario eksploitasi dari Zerologon ([CVE-2020-1472](#)). Jika hal ini terjadi di dunia nyata, dampaknya bisa sangat besar karena penyerang dapat mengambil alih seluruh sistem domain. Oleh karena itu, sistem harus segera diperbarui agar tidak rentan terhadap serangan ini.

Dissemination & Integration

Audience

Laporan ini dibuat untuk kegiatan praktikum keamanan informasi dan ditujukan untuk dosen serta asisten praktikum

Classification

Dokumen ini bersifat internal dan digunakan untuk keperluan akademik.

Recommendations

1. Melakukan update keamanan dari Microsoft untuk menutup celah CVE-2020-1472.
2. Mengatur ulang konfigurasi Netlogon agar hanya menerima koneksi yang aman.
3. Mengganti password akun mesin dan akun penting lainnya di domain setelah patch diterapkan.
4. Memantau aktivitas login atau perubahan akun yang mencurigakan di sistem.

Conclusion

Berdasarkan hasil analisis dari berbagai sumber terbuka, CVE yang paling sesuai dengan kasus pada soal adalah **CVE-2020-1472 (Zerologon)**. Kerentanan ini memungkinkan seseorang yang tidak terautentikasi untuk memanfaatkan layanan Netlogon dan mengubah password akun mesin pada Domain Controller. Hasil ini sesuai dengan deskripsi kasus, sehingga CVE-2020-1472 menjadi jawaban yang paling tepat untuk Challenge 1.

Challenge 2

An employee from the Finance team forwarded an email to the SOC team. The subject line read: “⚠ Action Required: Verify Your Microsoft 365 Account to Continue Access.” The sender was the “Microsoft Support Team” with the email address support-security@ms-verify-account[.]com. The message contained the company logo and a link labeled “Verify Now.” When hovered, the link redirected to [https://login-microsoft-secure\[.\]info/](https://login-microsoft-secure[.]info/). It turned out that the HR team received a similar email first, while the Marketing team received it a few days later.

Can you find this MITRE ATT&CK technique?

Planning & Direction

Objective Statement

Tentukan teknik MITRE ATT&CK yang paling sesuai dengan kasus email yang meminta verifikasi akun Microsoft 365 melalui tautan, dengan cara mencari dan membandingkan subteknik di situs MITRE ATT&CK menggunakan kata kunci phishing.

Scope and Limitations

Fokus analisis hanya pada klasifikasi teknik menggunakan katalog MITRE ATT&CK. Tidak ada pemeriksaan header email, WHOIS, atau scan URL. Hasil bersifat klasifikasi teknis berdasarkan deskripsi teknik di MITRE.

Stakeholders

Hasil ini ditujukan untuk dosen pengampu praktikum dan tim SOC sebagai klasifikasi teknik awal untuk insiden phishing.

Priority and Timeline

Prioritas tinggi karena berhubungan dengan potensi pencurian kredensial. Analisis dilakukan cepat menggunakan satu sumber referensi (MITRE) dan diselesaikan pada hari yang sama.

Collection

MITRE | ATT&CK®

Matrices ▾ Tactics ▾ Techniques ▾ Defenses ▾ CTI ▾ Resources ▾ Benefactors Blog 🔍 Search 🔎

ATT&CK v18 has been released! Check out the [blog post](#) or [changelog](#) for more information.

TECHNIQUES

Trusted Relationship

Valid Accounts

Wi-Fi Networks

Execution

Persistence

Privilege Escalation

Defense Evasion

Credential Access

Discovery

Lateral Movement

Collection

Command and Control

Exfiltration

Impact

Mobile

<https://attack.mitre.org>

Home > Techniques > Enterprise > Phishing > Spearphishing Link

Phishing: Spearphishing Link

Other sub-techniques of Phishing (4)

Adversaries may send spearphishing emails with a malicious link in an attempt to gain access to victim systems. Spearphishing with a link is a specific variant of spearphishing. It is different from other forms of spearphishing in that it employs the use of links to download malware contained in email, instead of attaching malicious files to the email itself, to avoid defenses that may inspect email attachments. Spearphishing may also involve social engineering techniques, such as posing as a trusted source.

All forms of spearphishing are electronically delivered social engineering targeted at a specific individual, company, or industry. In this case, the malicious emails contain links. Generally, the links will be accompanied by social engineering text and require the user to actively click or copy and paste a URL into a browser, leveraging User Execution. The visited website may compromise the web browser using an exploit, or the user will be prompted to download applications, documents, zip files, or even executables depending on the pretext for the email in the first place.

Adversaries may also include links that are intended to interact directly with an email reader, including embedded images intended to exploit the end system directly. Additionally,

ID: T1566.002

Sub-technique of: T1566

ⓘ Tactic: Initial Access

ⓘ Platforms: Identity Provider, Linux, Office Suite, SaaS, Windows, macOS

CONTRIBUTORS: Jeff Sakowicz, Microsoft Identity Developer Platform Services (IDPM Services); Kobi Haimovich, CardinalOps; Mark Wee; Menachem Goldstein; Philip Winther; Saisha Agrawal, Microsoft Threat Intelligent Center (MSTIC); Shailesh Tiwary (Indian Army)

Version: 2.8

Created: 02 March 2020

Last Modified: 24 October 2025

[Version Permalink](#)

Sources

Sumber yang digunakan hanya satu: MITRE ATT&CK website. Pencarian dilakukan dengan kata kunci phishing pada halaman <https://attack.mitre.org>.

Collection Methods

Pencarian manual di MITRE dengan kata kunci phishing. Dibuka daftar teknik terkait Phishing (T1566) kemudian diperiksa subteknik satu per satu untuk menemukan yang paling sesuai dengan deskripsi soal.

Ethical and Legal Compliance

Hanya mengakses materi publik yang tersedia di MITRE. Tidak ada tindakan scanning, eksploitasi, atau akses tidak sah ke sumber lain.

Documentation

Semua halaman MITRE yang dibuka dicatat URL dan tanggal akses. Hasil pencarian serta teknik yang dipilih dicatat untuk verifikasi.

Tabel dokumentasi sumber

N o	Sumber	Jenis	URL	Tanggal Akses	Catatan
1	MITRE ATT&CK	Katalog teknik	https://attack.mitre.org/	01 November 2025 00:10 WIB	Pencarian kata kunci "phishing"
2	MITRE ATT&CK T1566.002	Subteknik Spearphishing Link	https://attack.mitre.org/techniques/T1566/002/	01 November 2025 00:12 WIB	Deskripsi teknik yang dipilih sebagai paling cocok

Processing & Exploitation

Data Cleaning

Hanya teknik yang berkaitan langsung dengan phishing dipertahankan. Teknik lain yang tidak relevan disaring.

Normalization

Deskripsi teknik di MITRE diringkas ke format yang sama yaitu nama teknik, kode (mis. T1566.002), dan kalimat singkat fungsi teknik.

Organization

Hasil pencarian dan ringkasan disimpan di dokumen teks singkat yang memuat perbandingan antara deskripsi soal dan deskripsi teknik.

Tagging and Correlation

Setiap subteknik diberi tag sederhana: link, attachment, service. Teknik yang berhubungan dengan link diberi prioritas karena soal menyebut tautan "Verify Now".

Analysis & Production

Analytical Methods

Bandingkan elemen kunci soal dengan definisi setiap subteknik di MITRE:

- Apakah teknik menggunakan link untuk mengarahkan korban ke halaman palsu
- Apakah tujuan teknik adalah pencurian kredensial atau pengelabuan pengguna
- Teknik yang memenuhi kedua kriteria dianggap cocok.

Interpretation

Dari pemeriksaan subteknik di MITRE, subteknik yang paling sesuai adalah T1566.002 Spearphishing Link karena soal jelas menyebut email yang mengandung tautan yang mengarah ke halaman login palsu untuk meminta verifikasi akun.

Validation

Validasi dilakukan dengan membaca halaman resmi MITRE untuk T1566 dan T1566.002. Deskripsi T1566.002 menjelaskan penggunaan link untuk memancing korban memasukkan kredensial, sesuai dengan skenario soal.

Findings and Implications

Finding

Teknik MITRE ATT&CK yang paling tepat untuk kasus ini adalah T1566.002 Spearphishing Link.

Implications

Jika korban mengakses tautan dan memasukkan kredensial, pelaku dapat memperoleh akses ke akun Microsoft 365 korban. Dampaknya meliputi akses email, data bocor, penyalahgunaan akun untuk serangan lanjutan, dan potensi kompromi internal.

Conclusion

Setelah memeriksa daftar teknik di MITRE ATT&CK dengan kata kunci phishing, teknik yang paling sesuai dengan deskripsi email di soal adalah T1566.002 Spearphishing Link. Teknik ini menjelaskan penggunaan tautan untuk mengarahkan korban ke halaman palsu guna mencuri kredensial, yang sesuai dengan kasus yang diberikan.

Dissemination & Integration

Audience

Laporan singkat ini ditujukan untuk dosen pengampu, asisten praktikum, dan tim SOC sebagai klasifikasi teknik awal.

Classification

Dokumen bersifat internal akademik.

Recommendations

1. Laporkan teknik ini sebagai T1566.002 Spearphishing Link.
2. Segera beri tahu tim SOC untuk memblok domain atau URL yang tertera di email.
3. Minta helpdesk mengingatkan pengguna agar tidak mengklik tautan dan memeriksa setiap permintaan verifikasi.
4. Periksa aktivitas login yang tidak biasa pada akun yang menjadi target, dan pastikan MFA aktif pada akun Microsoft 365.

Challenge 3

A maze of light panels, polished floors, echoing footsteps, and distant chatter fades beneath curved ceilings. You've probably walked here without really seeing it. Guess where this is!

[whereisthis.jpg](#)

- Format: [Google Maps](#) Address
- Example: Jl. Manyar Kertoarjo No.110, Manyar Sabrangan, Kec. Mulyorejo, Surabaya, Jawa Timur 60116

Planning & Direction

Objective Statement

Tujuan dari analisis ini adalah untuk menentukan lokasi sebenarnya dari sebuah foto menggunakan sumber terbuka. Proses dilakukan dengan pengamatan visual dan pencarian manual melalui Google Maps untuk memastikan lokasi yang terlihat pada foto dapat diidentifikasi secara akurat.

Scope and Limitations

Analisis difokuskan pada pencarian lokasi menggunakan peta dan citra Google Maps, termasuk fitur Street View. Metode ini mengandalkan kecocokan elemen visual seperti logo toko, bentuk bangunan, dan posisi lantai. Tidak ada penggunaan metadata GPS atau alat otomatis lainnya. Hasil analisis didasarkan sepenuhnya pada observasi visual.

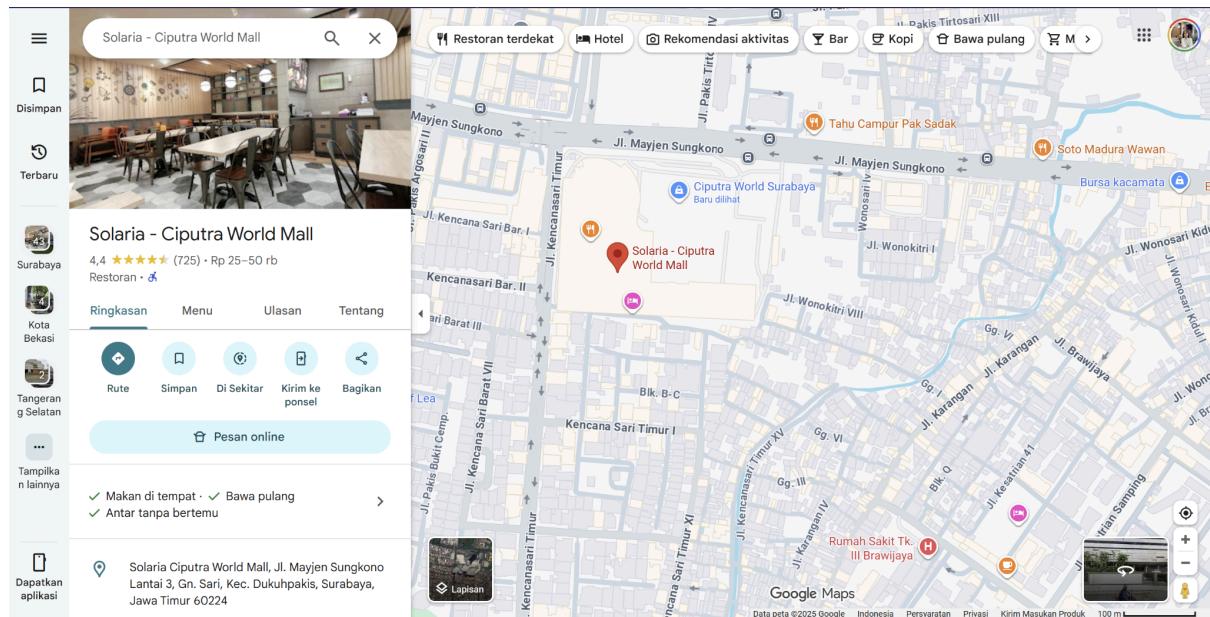
Stakeholders

Laporan ini disusun untuk dosen pengampu dan peserta praktikum keamanan informasi, sebagai latihan penerapan Open Source Intelligence (OSINT) untuk identifikasi lokasi.

Priority and Timeline

Analisis dilakukan dalam satu sesi karena kasus sederhana dan dapat diselesaikan dengan pencarian manual. Hasil verifikasi lokasi diperoleh dalam waktu kurang dari satu jam.

Collection



Note : Titik terdekat yang bisa di akses pada google maps namun tidak bisa terlihat di street view.

Sources

1. Google Maps (<https://maps.google.com>)
2. Google Street View di area Ciputra World Mall Surabaya
3. Foto yang diberikan sebagai bahan identifikasi

Collection Methods

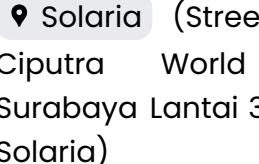
Pencarian dilakukan secara manual melalui Google Maps dengan membuka wilayah Surabaya dan mencari area Ciputra World Mall. Setelah lokasi utama ditemukan, dilakukan pengamatan visual pada lantai atas mall untuk mencocokkan tampilan dengan elemen pada foto, seperti logo restoran dan tata letak bangunan.

Ethical and Legal Compliance

Semua data yang digunakan bersumber dari platform publik dan resmi, tanpa mengakses informasi pribadi atau terbatas. Aktivitas hanya melibatkan pengamatan dan pencocokan visual.

Documentation

Berikut daftar sumber dan waktu akses selama proses pencarian:

No	Sumber	Jenis	URL atau Rujukan	Tanggal dan Waktu Akses (WIB)	Catatan
1	Foto Soal	Bukti input	 whereisthis.jpg	01 November 2025 01:23:00 AM WIB	Foto digunakan sebagai referensi visual utama
2	Google Maps	Peta digital	https://maps.google.com	01 November 2025 01:23:00 AM WIB	Digunakan untuk mencari lokasi bangunan dan arah pandang
3	Google Street View	Citra visual	 Solaria (Street View Ciputra World Mall Surabaya Lantai 3 Dekat Solaria)	01 November 2025 01:23:00 AM WIB	Membantu mencocokkan tampilan bangunan dan logo restoran

Processing & Exploitation

Data Cleaning

Karena hanya digunakan satu sumber utama, tidak ada proses penyaringan data tambahan. Foto diamati langsung dan dibandingkan dengan tampilan visual pada peta.

Normalization

Semua hasil observasi disusun dalam format catatan yang konsisten, termasuk koordinat lokasi, alamat lengkap, dan hasil kecocokan visual.

Organization

Data disimpan dalam bentuk catatan teks berisi observasi, tangkapan layar lokasi, serta hasil pencocokan elemen visual seperti nama restoran dan posisi lantai.

Tagging and Correlation

Elemen penting yang digunakan sebagai tag adalah "Ciputra World Mall", "Solaria", dan "Surabaya". Semua elemen menunjukkan kecocokan yang konsisten antara foto dan tampilan di Google Maps.

Analysis & Production

Analytical Methods

Metode analisis dilakukan dengan membandingkan elemen-elemen visual yang tampak di foto dengan tampilan pada Google Maps dan Street View. Ciri seperti papan nama “Solaria”, bentuk dinding, dan posisi lantai menjadi indikator utama untuk menentukan lokasi.

Interpretation

Hasil pengamatan menunjukkan bahwa foto diambil di area **Ciputra World Mall Surabaya**, tepatnya di **depan restoran Solaria lantai 3**. Elemen visual seperti logo restoran dan tata ruang mall sesuai dengan yang terlihat pada Google Maps.

Validation

Koordinat lokasi yang ditemukan adalah **-7.293261769654206, 112.71974808278759**, dengan alamat lengkap:

Solaria Ciputra World Mall, Jl. Mayjen Sungkono Lantai 3, Gn. Sari, Kec. Dukuhpakis, Surabaya, Jawa Timur 60224.

Findings and Implications

Lokasi foto berhasil diidentifikasi dengan tingkat keyakinan tinggi melalui pengamatan manual di Google Maps. Proses ini menunjukkan bahwa teknik pencarian visual sederhana dapat digunakan secara efektif dalam konteks OSINT untuk identifikasi lokasi gambar.

Dissemination & Integration

Audience

Laporan ini ditujukan untuk dosen dan peserta praktikum keamanan informasi sebagai bagian dari latihan analisis berbasis sumber terbuka.

Classification

Dokumen bersifat internal untuk keperluan akademik dan tidak mengandung informasi sensitif.

Recommendations

1. Gunakan **Google Maps dan Street View** sebagai langkah pertama untuk analisis lokasi ketika data GPS tidak tersedia.
2. Simpan **koordinat dan tangkapan layar** setiap kali lokasi berhasil diidentifikasi agar hasil dapat diverifikasi kembali.
3. Jika memungkinkan, padukan dengan **reverse image search** untuk memperkuat keyakinan hasil lokasi dari sumber lain.
4. Biasakan mencatat **waktu akses dan URL** dari semua sumber agar proses investigasi transparan dan dapat diulang.

Conclusion

Berdasarkan hasil pengamatan dan pencarian manual melalui Google Maps, lokasi foto berhasil diidentifikasi di **Ciputra World Mall Surabaya, lantai 3, tepat di depan restoran Solaria**. Koordinat lokasinya adalah **-7.293452587682312, 112.71928905109486**, dengan alamat lengkap **Jl. Mayjen Sungkono Lantai 3, Gn. Sari, Kec. Dukuhpakis, Surabaya, Jawa Timur 60224**. Hasil ini menunjukkan kecocokan visual yang tinggi antara foto dan citra Street View.

Challenge 4

Cloudflare shields much of the internet, keeping countless websites fast and secure while staying almost unseen. Back in late 2017, its name marked a certain office in Washington. I dare you to find the exact address!

- Format: Address you found somewhere
- Example: 357 Terry St SE, Atlanta, GA 30312, United States

Planning & Direction

Objective Statement

Tujuan dari analisis ini adalah untuk menemukan alamat kantor Cloudflare yang berlokasi di Washington, D.C. pada akhir tahun 2017, sesuai petunjuk soal yang menyebut "Back in late 2017."

Scope and Limitations

Analisis difokuskan pada penelusuran situs resmi Cloudflare melalui arsip web *Wayback Machine* (web.archive.org) untuk melihat perubahan alamat kantor yang tercantum selama tahun 2017. Fokus utama adalah bagian *About* / *Overview* situs Cloudflare. Analisis dilakukan hanya berdasarkan arsip publik yang tersedia secara online.

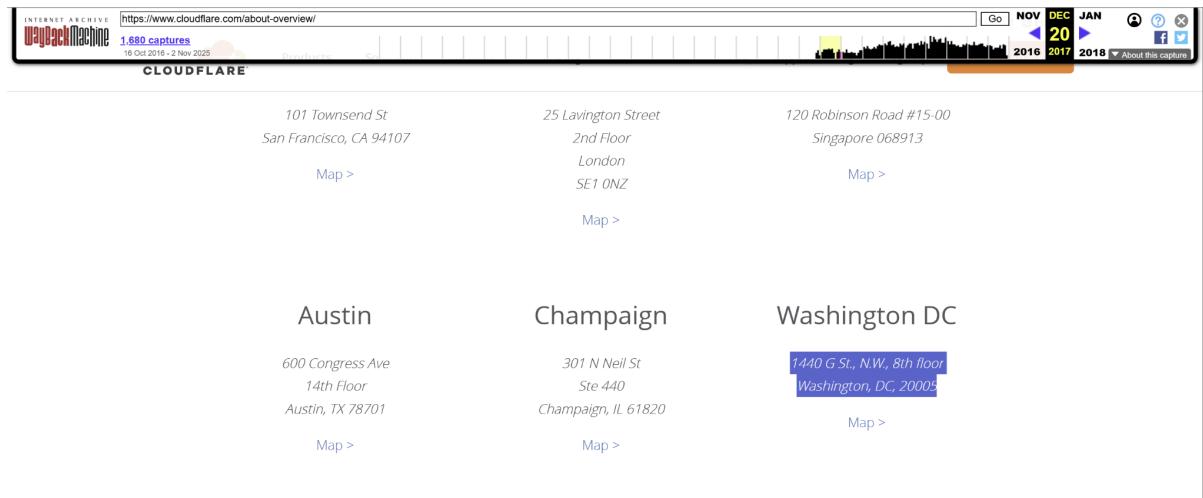
Stakeholders

Hasil ini ditujukan untuk dosen pengampu dan peserta praktikum keamanan informasi sebagai latihan penerapan metode OSINT dalam pelacakan informasi historis melalui arsip web.

Priority and Timeline

Analisis dilakukan dalam satu sesi karena data arsip dapat diakses langsung melalui Wayback Machine. Pencarian dilakukan secara berurutan dari bulan Januari hingga Desember 2017.

Collection



Sources

1. Wayback Machine (<https://web.archive.org/>)
2. Situs resmi Cloudflare versi arsip tahun 2017 (<https://www.cloudflare.com/about-overview/>)

Collection Methods

Langkah-langkah pengumpulan data dilakukan secara manual:

1. Membuka situs Wayback Machine dan memasukkan alamat situs resmi Cloudflare.
2. Menelusuri tangkapan situs (*snapshot*) dari Januari hingga Juli 2017 untuk menemukan alamat kantor yang tercantum.
3. Membuka tangkapan situs bulan Desember 2017 untuk melihat apakah alamatnya berubah pada akhir tahun.
4. Mencatat perbedaan alamat yang ditemukan di masing-masing snapshot.

Ethical and Legal Compliance

Seluruh informasi diperoleh dari sumber publik dan arsip web yang terbuka untuk umum. Tidak ada pelanggaran privasi atau akses tidak sah yang dilakukan.

Documentation

N	Sumber	Jeni	URL atau Rujukan	Tanggal Akses	Catatan
1	Wayback Machine	Arsip web	https://web.archive.org/	01 November 2025 01:45 AM WIB	Situs yang digunakan untuk melihat versi lama website Cloudflare
2	Cloudflare (Januari-Juli 2017)	Snap shot arsip	https://web.archive.org/web/202507110734/https://www.cloudflare.com/about-overview/	01 November 2025 01:45 AM WIB	Menampilkan alamat 900 19th Street, N.W., Suite 375, Washington, DC 20006
3	Cloudflare (Desember 2017)	Snap shot arsip	https://web.archive.org/web/20171220231727/https://www.cloudflare.com/about-overview/	01 November 2025 01:45 AM WIB	Menampilkan alamat 1440 G St., N.W., 8th Floor, Washington, DC 20005

Processing & Exploitation

Data Cleaning

Dari hasil penelusuran arsip, hanya dua snapshot utama yang digunakan: satu dari pertengahan tahun (Juli 2017) dan satu dari akhir tahun (Desember 2017). Snapshot lain diabaikan karena menampilkan isi halaman yang sama.

Normalization

Alamat yang ditemukan ditulis ulang dengan format alamat resmi Amerika Serikat agar seragam dan mudah dibaca.

Organization

Data hasil penelusuran disusun berdasarkan urutan waktu, dari awal tahun hingga akhir tahun, untuk melihat perubahan lokasi kantor Cloudflare.

Tagging and Correlation

Kedua alamat diberi tag waktu “early 2017” dan “late 2017”. Perubahan alamat dikonfirmasi sebagai perpindahan kantor dari 900 19th Street ke 1440 G Street, N.W.

Analysis & Production

Analytical Methods

Analisis dilakukan dengan membandingkan dua tangkapan arsip situs Cloudflare pada tahun 2017. Setiap versi halaman *About Overview* diperiksa untuk menemukan teks alamat kantor di Washington, D.C.

Interpretation

Pada snapshot awal tahun 2017 (sekitar Januari–Juli), alamat yang tercantum adalah:

900 19th Street, N.W., Suite 375, Washington, DC 20006.

Namun, pada snapshot tanggal **20 Desember 2017**, alamat tersebut berubah menjadi:

1440 G St., N.W., 8th Floor, Washington, DC 20005.

Perubahan ini menunjukkan bahwa menjelang akhir tahun 2017, Cloudflare memindahkan atau memperbarui alamat kantornya di Washington, D.C.

Validation

Kedua alamat dikonfirmasi langsung dari halaman arsip resmi web.archive.org. Teks alamat terlihat jelas di bagian bawah halaman *About Overview* milik Cloudflare pada masing-masing snapshot.

Findings and Implications

Temuan menunjukkan bahwa alamat kantor Cloudflare di Washington, D.C. **berubah pada penghujung tahun 2017**, sesuai petunjuk soal.

Alamat akhir (pada Desember 2017) yang valid adalah:

1440 G St., N.W., 8th Floor, Washington, DC 20005, United States.

Dissemination & Integration

Audience

Hasil ini ditujukan untuk dosen dan peserta praktikum OSINT sebagai latihan analisis arsip web untuk menemukan informasi historis.

Classification

Dokumen bersifat publik-akademik, menggunakan sumber yang terbuka dan dapat diakses umum.

Recommendations

1. Gunakan Wayback Machine sebagai alat utama untuk melacak perubahan historis situs web perusahaan atau organisasi.
2. Catat tanggal snapshot dan URL arsip lengkap untuk menjaga transparansi dan integritas bukti.
3. Untuk analisis lanjutan, padukan dengan sumber lain seperti LinkedIn atau artikel berita guna memastikan alasan perpindahan kantor.
4. Simpan tangkapan layar (screenshot) dari halaman arsip yang memuat alamat sebagai bukti visual dalam laporan.
5. Biasakan mencatat perbandingan antara awal dan akhir tahun ketika soal mencantumkan kata kunci waktu seperti "*late 2017*".

Conclusion

Melalui pencarian menggunakan *Wayback Machine*, ditemukan bahwa pada awal tahun 2017 Cloudflare beralamat di **900 19th Street, N.W., Suite 375, Washington, DC 20006**, sedangkan pada akhir tahun (snapshot 20 Desember 2017) alamatnya telah berubah menjadi **1440 G St., N.W., 8th Floor, Washington, DC 20005**. Berdasarkan petunjuk soal yang menyebut *late 2017*, maka alamat akhir tersebut merupakan jawaban yang benar.