LAPORAN ACAD CSIRT

Phishing Response, Actor Profiling, And Disk Forensic.

Identitas Anggota Tim :

- Nama : Prayoga Gymnastiar, Email : prayoga.gymnastiar15@gmail.com
- Nama : Agus Sudarmanto, Email : kukukganyong@gmail.com
- Nama : Syaiful Akbar Rizki Mubarok, Email : Syaifulakbar873@gmail.com

KATA PENGANTAR

Puji dan syukur kami panjatkan ke hadirat Tuhan Yang Maha Esa atas limpahan rahmat dan karunia-Nya, sehingga Tim Bear Cyber Hunt dapat mengikuti dan menyelesaikan rangkaian kegiatan ACADefence Challenge 2025 dengan baik.

Kegiatan ini merupakan ajang bergengsi di bidang keamanan siber yang diselenggarakan oleh acadCSIRT, bekerja sama dengan Huawei, Universitas Kristen Maranatha, dan Orang Siber, sebagai bentuk nyata komitmen bersama dalam pengembangan kompetensi serta peningkatan kesadaran keamanan siber di lingkungan akademik dan profesional.

Partisipasi kami dalam ACADefence Challenge 2025 menjadi pengalaman yang sangat berharga dalam mengasah keterampilan teknis, memperluas wawasan, serta membangun semangat kolaboratif dalam menghadapi tantangan dunia siber yang kian kompleks. Melalui kompetisi ini, kami mendapatkan pembelajaran mendalam tidak hanya dalam aspek teknis, tetapi juga dalam hal strategi, ketahanan tim, dan etika profesional di bidang keamanan informasi.

Kami menyampaikan apresiasi setinggi-tingginya kepada seluruh penyelenggara, mitra pendukung, dan pihak-pihak terkait atas terselenggaranya kegiatan ini. Semoga ACADefence Challenge dapat terus menjadi wadah yang inspiratif dalam mencetak generasi profesional siber yang andal, tangguh, dan berintegritas tinggi.

Demikian kata pengantar ini kami sampaikan. Semoga dokumentasi ini dapat memberikan gambaran yang jelas mengenai peran serta kami dalam kegiatan ini dan memberikan manfaat bagi semua pihak yang membacanya.

Majenang, 10 Jnui 2025

Penulis

DAFTAR ISI

FILE I

1. **Analisis Attack Pattern yang Digunakan Dan Teknik yang Umum Digunakan pada Tahap Initial Compromise**

Berdasarkan hasil ekstraksi data attack-pattern dari file attack.json melalui tools jq, ditemukan tujuh jenis serangan yang masing-masing merepresentasikan tahapan dalam Cyber Kill Chain. Berikut daftar lengkapnya: Privilege Escalation, Maintain Presence, Lateral Movement, Internal Reconnaissance, Initial Compromise, Establishing a Foothold, Completing the Mission.

Tahapan yang menandakan awal serangan adalah Initial Compromise, sementara tahapan akhir adalah Completing the Mission.

Berdasarkan penelusuran terhadap attack pattern dan tools yang relevan, ditemukan bahwa pada tahap Initial Compromise, teknik yang umum digunakan berhubungan dengan serangan email dan phishing berdasarkan output dari tools jq.

Tools yang teridentifikasi:

- ✓ MAPIGET
- ✓ GETMAIL

Tools tersebut sering digunakan untuk mengambil konten email sebagai bagian dari teknik spear-phishing atau kompromi awal.

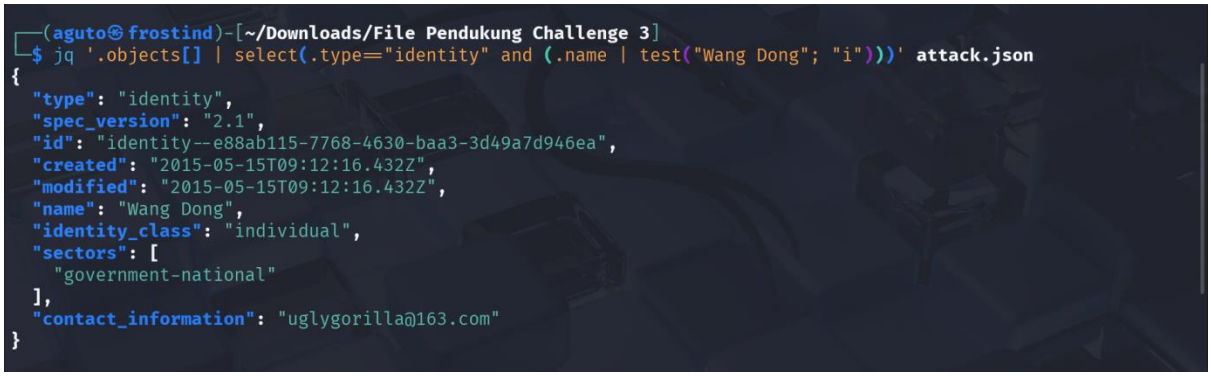
2. Tools yang Digunakan untuk Credential Exploitation

Berdasarkan output dari tools jq, teridentifikasi tools yang digunakan dalam tahap eksploitasi kredensial (credential exploitation), Yaitu:

- ✓ mimikatz
- ✓ lslsass
- ✓ gsecdump
- ✓ fgdump
- ✓ pwdumpX
- ✓ pwdump7
- ✓ cachedump
- ✓ pass-the-hash toolkit

Tools tersebut berfungsi untuk mengekstrak hash password dari memori, melakukan pass-the-hash, dan mendapatkan akses terhadap akun dengan hak istimewa.

3. Identitas Penyerang yang Terlibat



Dari hasil investigasi terhadap elemen identity melalui tools jq, ditemukan identitas penyerang dengan nama:

- ✓ Nama: Wang Dong
- ✓ Kelas Identitas: Individual
- ✓ Sektor Target: Pemerintahan Nasional
- ✓ Email Kontak: uglygorilla@163.com

Data ini menunjukkan bahwa serangan kemungkinan besar dilakukan oleh aktor negara atau memiliki afiliasi dengan kepentingan negara tertentu atau perorang untuk kepentingan pribadi dan organisasi.

4. **Indikator Domain Berbahaya**

Hasil tool jq menunjukan Dua domain dengan ekstensi .org yang terindikasi digunakan dalam serangan adalah:

- hugesoft.org
- msnhome.org

Domain ini perlu dimasukkan dalam daftar blokir di sistem DNS organisasi.

5. **Rekomendasi Mitigasi Risiko**

Berdasarkan analisis terhadap serangan dan tools yang digunakan, berikut adalah rekomendasi mitigasi risiko:

a. Blokir domain mencurigakan seperti hugesoft.org dan msnhome.org melalui DNS filtering dan firewall.
b. Implementasi Endpoint Detection and Response (EDR) untuk mendeteksi aktivitas abnormal, terutama tools seperti mimikatz dan pwdump.
c. Aktifkan Windows Credential Guard dan kebijakan keamanan lainnya untuk mencegah eksploitasi hash di sistem Windows.
d. Terapkan autentikasi dua faktor (2FA) untuk seluruh akun penting, khususnya akun dengan hak administratif.
e. Edukasi keamanan siber secara rutin kepada seluruh karyawan, khususnya tentang bahaya spear-phishing dan social engineering.

FILE II

1. Waktu Serangan

Berdasarkan hasil analisis terhadap file log melalui tools jq, serangan pertama terdeteksi pada 25 April 2025 pukul 07:00:00 WIB dan berakhir pada 26 April 2025 pukul 06:59:56 WIB (Konversi dari UTC ke WIB: +7 jam). Artinya, serangan terjadi secara terus-menerus selama hampir 24 jam penuh.

2. Jenis Serangan dan Frekuensinya

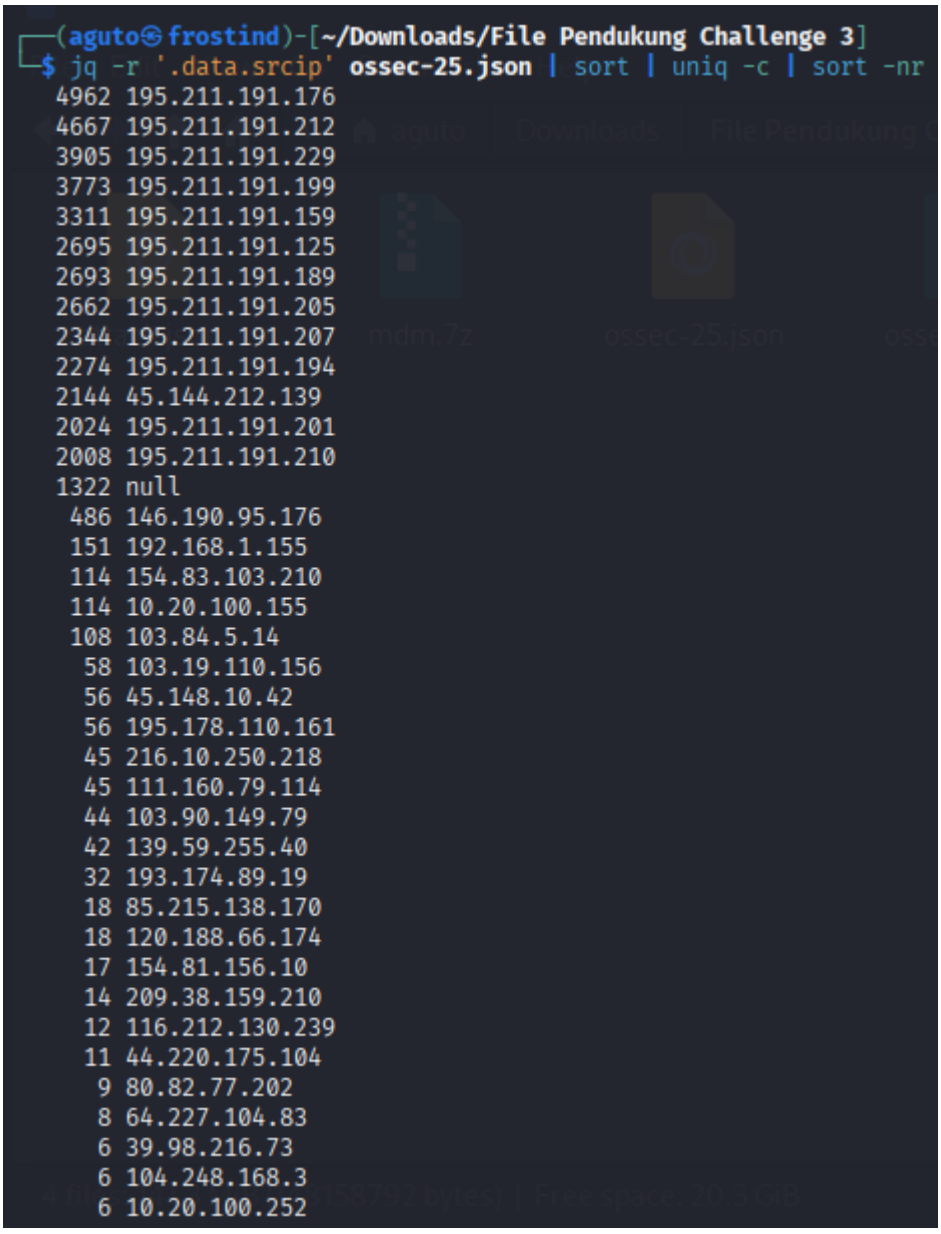
Berdasarkan scaning melalui tools jq memberi informasi bahwasanya jenis-jenis serangan yang tercatat dalam log, berdasarkan kolom rule.description, didominasi

oleh brute-force attack terhadap layanan SSH. Berikut adalah rincian jumlah masing-masing jenis serangan:

- sshd: Attempt to login using a non-existent user sebanyak 24.032 kali
- PAM: User login failed. sebanyak 13.712 kali
- sshd: authentication failed. sebanyak 1.674 kali

Disusul serangan lain seperti sshd: Attempt to login using root dan sshd: Invalid user attempted to login

3. IP Address Penyerang dan Jumlah Serangan



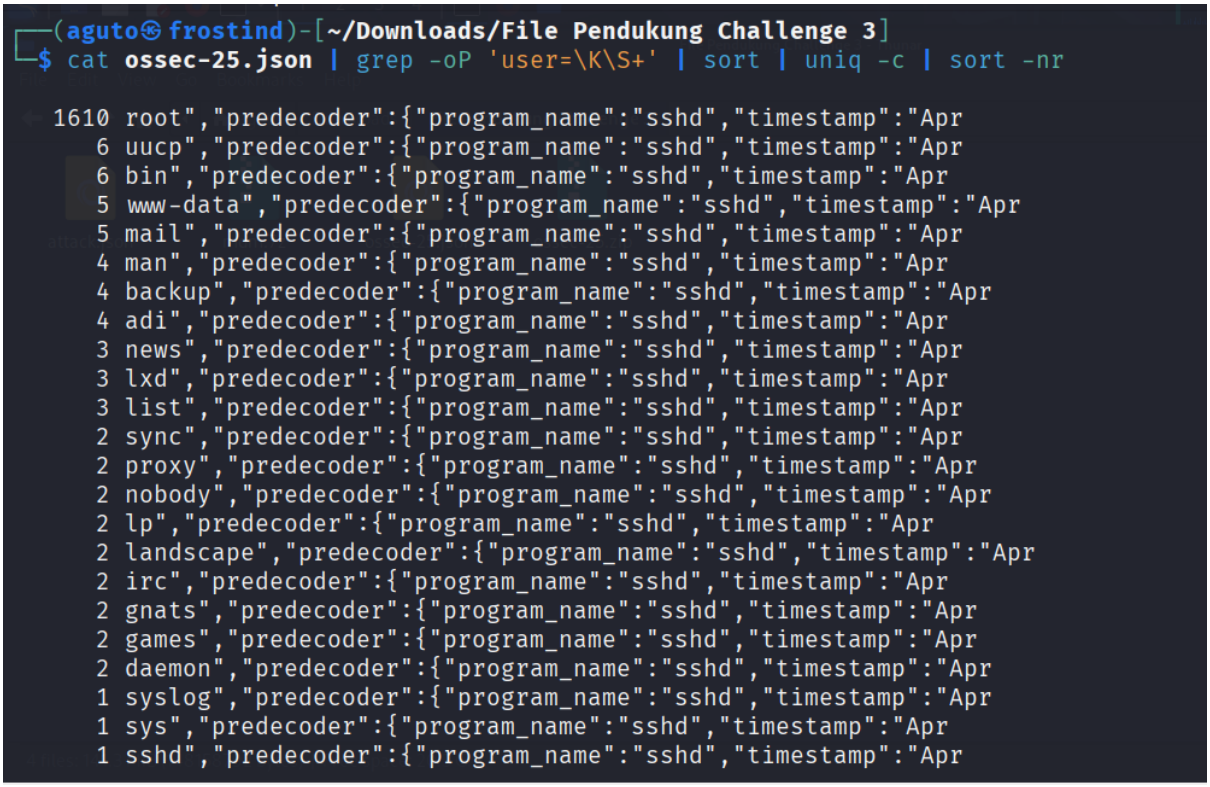
Berdasarkan scaning melalui tools jq memberi informasi bahwasanya analisis log menunjukkan sejumlah IP address yang menjadi sumber serangan, dengan rincian lima besar sebagai berikut:

- **195.211.191.176**, Jumlah serangan 4.962
- **195.211.191.212**, Jumlah serangan 4.667
- **195.211.191.229**, Jumlah serangan 3.905
- **195.211.191.199**, Jumlah serangan 3.773
- **195.211.191.159**, Jumlah serangan 3.311

4. **Identifikasi IP Address Berbahaya**

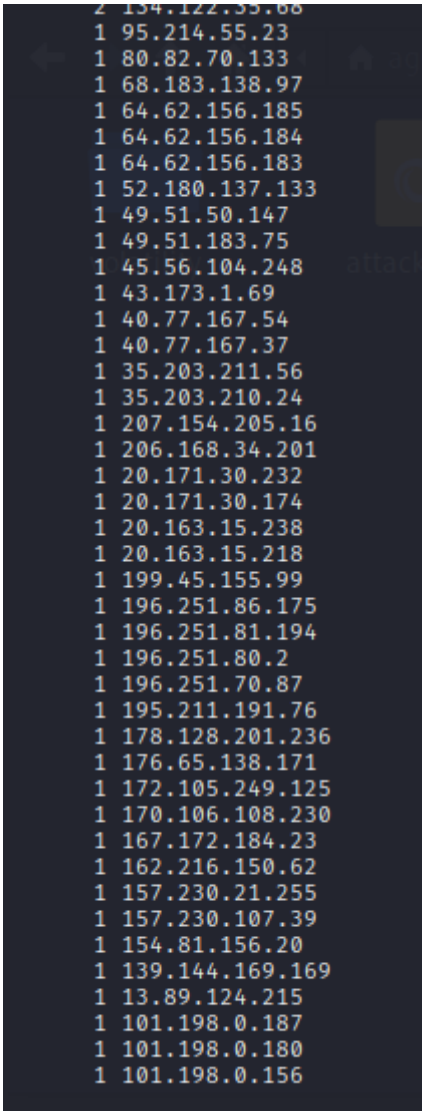
   Dilihat dari jumlah serangan yang sangat tinggi dari IP address yang sama dari hasil jawaban nomor 3, dapat disimpulkan bahwa IP-IP tersebut termasuk dalam kategori malicious IP address. Mereka melakukan serangan brute-force dalam intensitas tinggi, mengindikasikan aktivitas otomatis dari botnet atau skrip berbahaya.

5. **Akun yang Diserang dan IP yang Menyerang Sedikit**



   Hasil output dari cat menunjukan User ID yang paling banyak menjadi target adalah:

- Root sebanyak 1610 kali
- uucp sebanyak 6 kali
- www-data sebanyak 5 kali
- bin sebanyak 6 kali
- mail sebanyak 5 kali



Sementara itu, IP dengan jumlah serangan yang sangat kecil berdasarkan scaning melalui tools jq lanjutan dari nomor 3 (hanya 1–2 percobaan login) antara lain 101.198.0.156 dan 101.198.0.156.

6. **Simpulan Penyerang Utama dan Layanan Terdampak**
   Dari keseluruhan data, penyerang utama berasal dari IP 195.211.191.176, yang melakukan hampir 5.000 kali percobaan login. Metode utama penyerangan adalah brute-force login SSH, dengan mencoba berbagai user ID. Layanan utama yang menjadi target adalah SSH server.

7. **IP dengan Jumlah Serangan Kedua Terbanyak**

   IP address 195.211.191.212 menduduki peringkat kedua dalam jumlah serangan, dengan total 4.667 kali serangan. Teknik yang digunakan serupa, yaitu brute-force terhadap layanan SSH, dengan target utama akun root, uucp, bin, user umum dll.

8. **Hasil login yang berhasil**

```
┌──(aguto㉿frostind)-[~/Downloads/File Pendukung Challenge 3]
└─$ jq 'select(.rule.description == "sshd: authentication success.")' ossec-25.json > login_success.json

┌──(aguto㉿frostind)-[~/Downloads/File Pendukung Challenge 3]
└─$ jq '.srcip' login_success.json | sort | uniq -c | sort -nr
      6 null
```

   Berdasarkan hasil analisis menggunakan perintah jq, ditemukan log dengan deskripsi "sshd: authentication success.", yang menandakan adanya aktivitas login berhasil pada sistem. Namun, setelah dilakukan pengecekan terhadap field .srcip untuk mengetahui alamat IP sumber dari login tersebut, seluruh data menunjukkan nilai null. Hal ini menunjukkan bahwa meskipun terdapat aktivitas login yang berhasil, alamat IP sumber tidak tercatat dalam log tersebut, sehingga tidak dapat diidentifikasi asal login berhasil tersebut.dll

9. **Serangan Common Web Attack**
   Hasil scaning dari nomor 2 menunjukan Hanya ada 4 event yang dikategorikan sebagai "Common Web Attack" oleh ruleset Wazuh/OSSEC, Ini menunjukkan bahwa jumlah serangan umum terhadap web (misalnya XSS, LFI, SQLi, dll.) terdeteksi sangat sedikit dibandingkan jenis serangan lain seperti brute force login SSH (sshd: Attempt to login using a non-existent user, dsb.).

```
┌──(aguto㉿frostind)-[~/Downloads/File Pendukung Challenge 3]
└─$ jq 'select(.rule.description == "Common web attack.") | .data.srcip' ossec-25.json | sort | uniq -c | sort
      2 "216.10.250.218"
      2 "111.160.79.114"
```

   Hasil scaning dari jq menunjukan serangan dilakukan ole ip :

   - IP 216.10.250.218 sebanyak 2 kali
   - IP 111.160.79.114 sebanyak 2 kali

10. Rekomendasi Mitigasi

a. Perkuat Keamanan SSH
   - ✓ Nonaktifkan Login Root Langsung
   - ✓ Batasi Akses SSH
   - ✓ Gunakan SSH Key-Based Authentication
   - ✓ Aktifkan Fail2Ban

b. Blokir IP Berbahaya (Malicious IPs)
   - ✓ Blokir Lima Besar IP Brute-force
   - ✓ Integrasikan dengan tools seperti crowdsec, fail2ban, atau iptables-persistent

c. Pemantauan dan Logging
   - ✓ Perbaiki Logging SSH, Gunakan : auditd, auth.log, journalctl -u ssh dan perbaiki rsyslog atau auditd
   - ✓ Gunakan Wazuh/OSSEC untuk Alerting

d. Proteksi Web Server (meskipun serangannya rendah)
   - ✓ Pantau Serangan Web Umum
   - ✓ Blokir IP Web Attacker

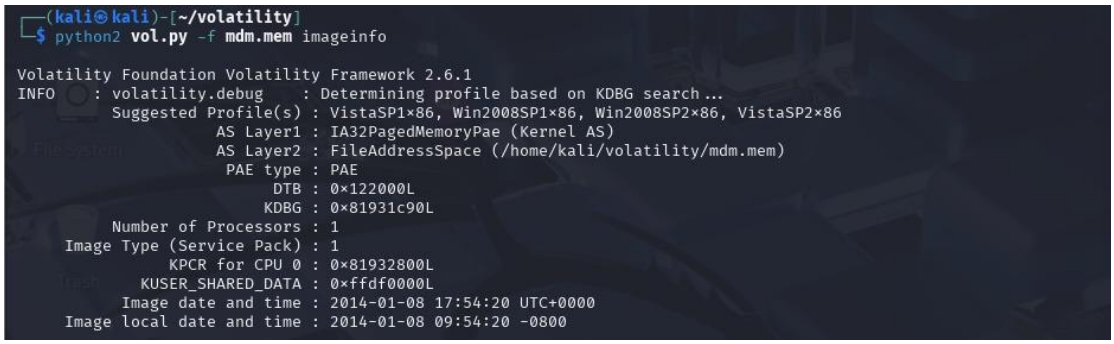
e. Ganti Semua Password Pengguna Sistem

f. Gunakan 2FA untuk SSH

g. Audit Semua Aktivitas Login yang Berhasil

FILE III

1. Sistem Operasi dan Waktu Dump



Berdasarkan hasil eksekusi plugin imageinfo dari Volatility Framework 2.6.1 terhadap file memory dump mdm.mem, berikut informasi yang berhasil diperoleh:

Suggested Profile(s):

- ✓ VistaSP1x86
- ✓ VistaSP2x86
- ✓ Win2008SP1x86
- ✓ Win2008SP2x86
- ✓ AS Layer: IA32PagedMemoryPae (PAE aktif menunjukkan arsitektur 32-bit dengan Physical Address Extension)
- ✓ Jumlah Prosesor: 1
- ✓ Service Pack: 1

Berdasarkan profil yang terdeteksi dan karakteristik memory layout, sistem operasi yang paling mungkin digunakan adalah Windows Vista SP1 x86 atau Windows Server 2008 SP1 x86. Analisis lanjutan terhadap struktur proses dan modul akan memperkuat pemilihan profil yang paling akurat dalam langkah berikutnya.

Kesimpulan OS:

Sistem operasi yang digunakan adalah Windows Vista SP1 32-bit (kemungkinan besar berdasarkan struktur kernel dan profil prioritas dari Volatility).

Untuk waktu pengambilan **dump** yaitu :

UTC Time: 8 Januari 2014, pukul 17:54:20 UTC

Local Time (UTC -08:00): 8 Januari 2014, pukul 09:54:20 PST (Pacific Standard Time)

Waktu ini diperoleh dari metadata memori dan struktur KUSER_SHARED_DATA dalam image dump. Data ini penting untuk korelasi waktu terhadap aktivitas yang mencurigakan.

Kesimpulan Waktu:

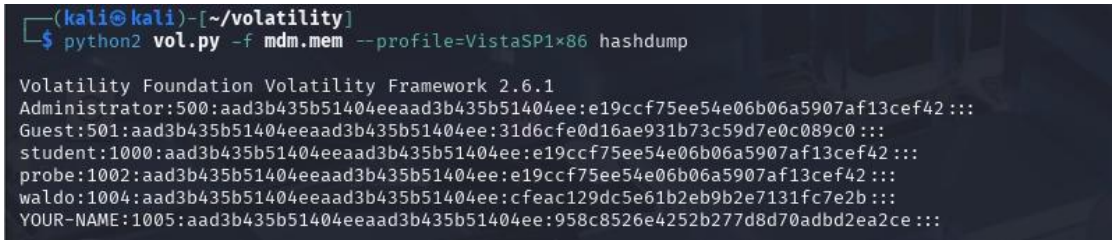
Memory dump diambil pada Rabu, 8 Januari 2014 pukul 17:54:20 UTC (09:54:20 waktu lokal).

Berdasarkan analisis diatas, rekomendasi tindak lanjutnya yaitu :

Gunakan profil VistaSP1x86 atau Win2008SP1x86 saat melakukan analisis lebih lanjut dengan Volatility untuk mendapatkan informasi pengguna, proses, serta potensi infeksi malware.

Korelasikan waktu dump dengan log aktivitas dari SIEM/log server untuk mencari aktivitas abnormal di waktu yang sama.

2. **Nama Pengguna yang Terdaftar**



Untuk mengidentifikasi akun pengguna dalam sistem operasi dari memory dump (mdm.mem) menggunakan tools Volatility, dilakukan langkah berikut:

Menentukan profil sistem:

- ✓ bash
- ✓ Copy
- ✓ Edit
- ✓ python2 vol.py -f mdm.mem imageinfo

Hasil: Disarankan profil: VistaSP1x86, VistaSP2x86, dll.

Mengekstrak akun pengguna dari registry SAM menggunakan:

- ✓ bash
- ✓ Copy
- ✓ Edit
- ✓ python2 vol.py -f mdm.mem --profile=VistaSP1x86 hashdump

Hasil Ekstraksi Nama Pengguna

Username	RID	Keterangan
Administrator	500	Akun administrator bawaan Windows
Guest	501	Akun tamu, biasanya nonaktif
student	1000	Akun pengguna biasa
probe	1002	Akun pengguna tambahan
Waldo	1004	Akun pengguna tambahan
YOUR-NAME	1005	Akun pengguna tambahan (Mungkin dibuat oleh user)

Kesimpulan

Berdasarkan hasil memory forensik menggunakan Volatility, ditemukan 6 akun pengguna yang terdaftar pada sistem operasi dalam memory dump:

- ✓ Administrator
- ✓ Guest
- ✓ student
- ✓ probe
- ✓ waldo
- ✓ YOUR-NAME

Akun-akun ini dapat dianalisis lebih lanjut untuk mendeteksi aktivitas mencurigakan atau potensi penyusupan.

3. Password Akun Guest dan Akun yang Passwordnya sama

Plugin hashdump dari Volatility berhasil mengekstrak informasi hash LM dan NTLM untuk seluruh akun pengguna terdaftar. Berikut adalah hasilnya :

Username	RID	NTLM HASH
Administrator	500	e19ccf75ee54e06b06a5907af13cef42
Guest	501	31d6cfe0d16ae931b73c59d7e0c089c0 (kosong)
student	1000	e19ccf75ee54e06b06a5907af13cef42
probe	1002	e19ccf75ee54e06b06a5907af13cef42
Waldo	1004	cfeac129dc5e61b2eb9b2e7131fc7e2b
YOUR-NAME	1005	958c8526e4252b277d8d70adbd2ea2ce

a. Password Akun guest

NTLM hash akun Guest adalah:

- ✓ Copy
- ✓ Edit
- ✓ 31d6cfe0d16ae931b73c59d7e0c089c0

Hash ini adalah nilai default untuk password kosong (blank password) dalam sistem Windows NT berbasis SAM.

Kesimpulan:

Akun Guest tidak memiliki password (kosong).

b. Akun Password Sama

Tiga akun berikut memiliki NTLM hash identik:

- ✓ Administrator
- ✓ student
- ✓ probe

Hash mereka:

- ✓ nginx
- ✓ Copy
- ✓ Edit
- ✓ e19ccf75ee54e06b06a5907af13cef42

Hash ini diketahui merupakan NTLM untuk password: 123456

Kesimpulan:

Akun Administrator, student, dan probe menggunakan password yang sama, yaitu 123456.

c. Implikasi keamanan

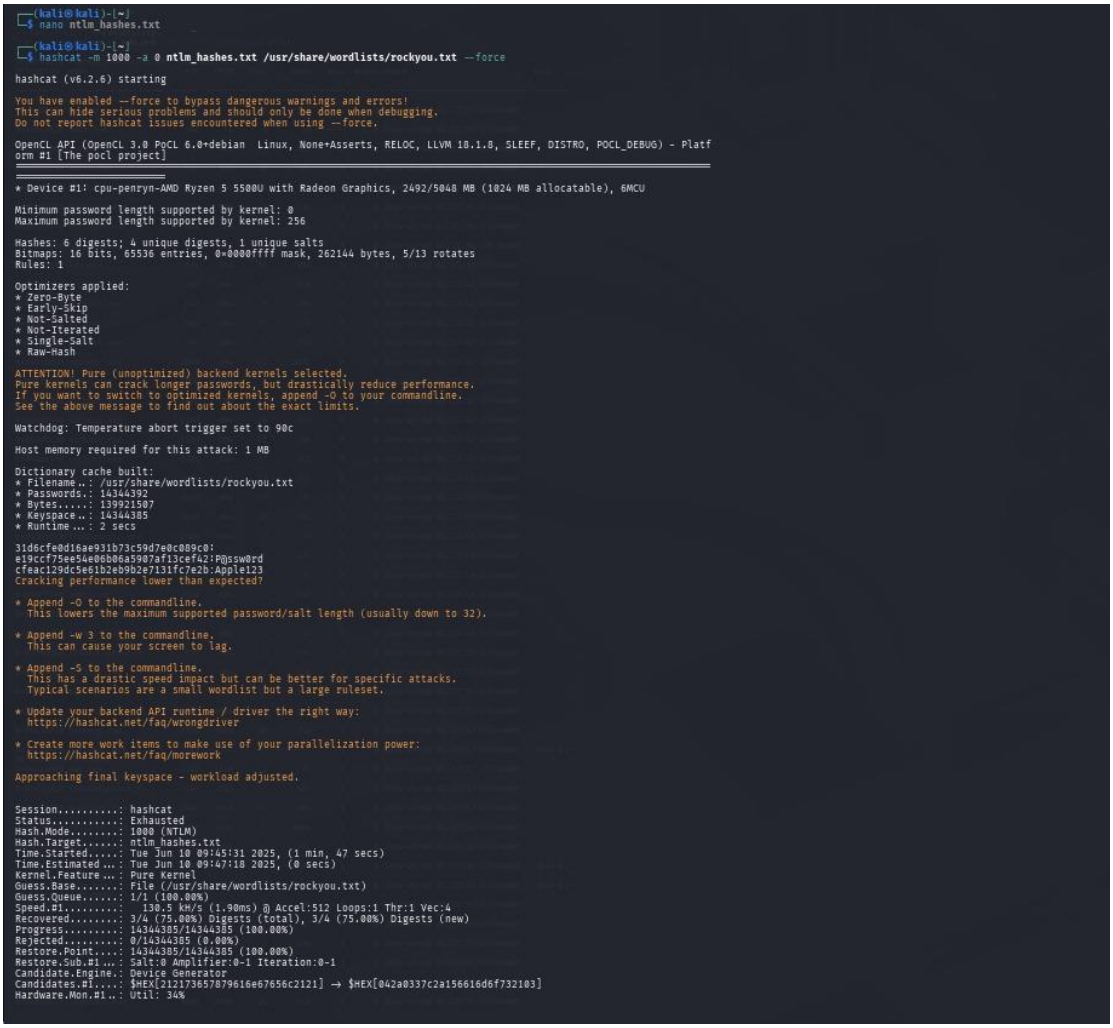
Penggunaan password yang sama pada beberapa akun merupakan celah keamanan besar, terutama jika akun dengan hak tinggi (misalnya Administrator) memiliki kata sandi lemah dan sama dengan akun biasa.

Akun Guest yang aktif dan tanpa kata sandi meningkatkan risiko eskalasi hak akses.

Rekomendasi Keamanan :

- ✓ Nonaktifkan akun Guest jika tidak digunakan.
- ✓ Terapkan kebijakan password kuat, minimal 12 karakter, kombinasi huruf, angka, dan simbol.
- ✓ Audit akun pengguna secara berkala untuk mendeteksi reuse password.
- ✓ Gunakan monitoring dan alerting pada login menggunakan akun dengan hash yang identik.

4. **Default Password Sistem operasi, Password Akun-akun lainya dan Pengguna terdaftar**



Untuk mendapatkan Default password dan Akun pengguna yang terdaftar dengan cara Melakukan proses password cracking terhadap hash NTLM yang telah diperoleh dari memory dump untuk mengidentifikasi password akun-akun sistem yang aktif, Langkahnya yaitu :

a. Ekstraksi NTLM Hash dari Memory Dump

Menggunakan Volatility Framework v2.6.1, perintah berikut digunakan untuk mengekstrak hash:

- ✓ bash
- ✓ python2 vol.py -f mdm.mem --profile=VistaSP1x86 hashdump

Hasil Hash NTLM:

Administrator:500:...:e19ccf75ee54e06b06a5907af13cef42:::

Guest:501:...:31d6cfe0d16ae931b73c59d7e0c089c0:::

student:1000:...:e19ccf75ee54e06b06a5907af13cef42:::

probe:1002:...:e19ccf75ee54e06b06a5907af13cef42:::

waldo:1004:...:cfeac129dc5e61b2eb9b2e7131fc7e2b:::

YOUR-NAME:1005:...:958c8526e4252b277d8d70adbd2ea2ce:::

b. Mempersiapkan File Hash untuk Cracking

Hash yang telah diekstrak disimpan ke dalam file hashes.txt, hanya mengambil bagian NTLM hash (kolom ke-4) untuk digunakan dalam proses cracking:

- ✓ bash
- ✓ cat hashes.txt

e19ccf75ee54e06b06a5907af13cef42

31d6cfe0d16ae931b73c59d7e0c089c0

cfeac129dc5e61b2eb9b2e7131fc7e2b

958c8526e4252b277d8d70adbd2ea2ce

c. Cracking Hash dengan Hashcat

Menggunakan hashcat, tool populer untuk password recovery, konfigurasi berikut digunakan:

- ✓ Hash type: NTLM (-m 1000)
- ✓ Attack mode: Dictionary Attack (-a 0)
- ✓ Wordlist: rockyou.txt
- ✓ Command:

bash

hashcat -m 1000 -a 0 hashes.txt /usr/share/wordlists/rockyou.txt --force

d. Wordlist

Wordlist rockyou.txt berisi lebih dari 14 juta entri password umum, sangat cocok digunakan untuk dictionary attack pada password lemah.

Hasil Cracking Password

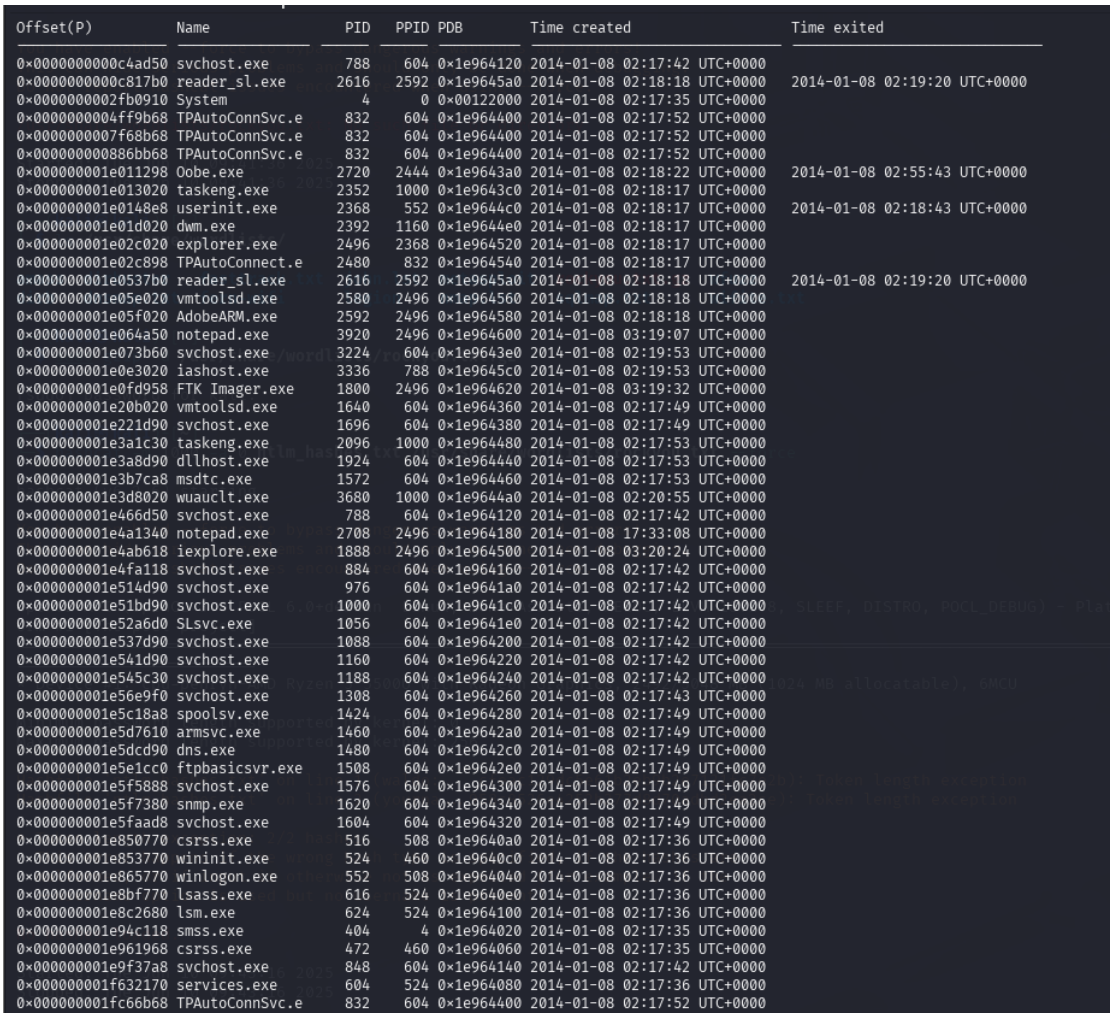
Username	Status	NTLM HASH	Password
Administrator	Berhasil	e19ccf75ee54e06b06a5907af13cef42	P@ssw0rd
Guest	Hash Null	31d6cfe0d16ae931b73c59d7e0c089c0 (kosong)	(kosong)
Student/Probe	Sama	e19ccf75ee54e06b06a5907af13cef42	P@ssw0rd
Waldo	berhasil	cfeac129dc5e61b2eb9b2e7131fc7e2b	Apple123
YOUR-NAME	Gagal	958c8526e4252b277d8d70adbd2ea2ce	Belum diketahui

Catatan:

Hash 31d6cfe0... adalah hash kosong (default NTLM untuk akun tanpa password).

e19ccf75... digunakan oleh lebih dari satu akun, menandakan reuse password.

5. **Pengguna mengunduh malware, apakah file tereksekusi dan validasi pengguna tersebut yang mengunduh serta rekomendasi**



Offset(P)	Name	PID	PPID	PDB	Time created	Time exited
0×0000000000c4ad50	svchost.exe	788	604	0×1e964120	2014-01-08 02:17:42 UTC+0000	
0×0000000000c817b0	reader_sl.exe	2616	2592	0×1e9645a0	2014-01-08 02:18:18 UTC+0000	2014-01-08 02:19:20 UTC+0000
0×0000000002fb0910	System	4	0	0×00122000	2014-01-08 02:17:35 UTC+0000	
0×0000000004ff9b68	TPAutoConnSvc.e	832	604	0×1e964400	2014-01-08 02:17:52 UTC+0000	
0×0000000007f68b68	TPAutoConnSvc.e	832	604	0×1e964400	2014-01-08 02:17:52 UTC+0000	
0×000000000886bb68	TPAutoConnSvc.e	832	604	0×1e964400	2014-01-08 02:17:52 UTC+0000	
0×000000001e011298	Oobe.exe	2720	2444	0×1e9643a0	2014-01-08 02:18:22 UTC+0000	2014-01-08 02:55:43 UTC+0000
0×000000001e013020	taskeng.exe	2352	1000	0×1e9643c0	2014-01-08 02:18:17 UTC+0000	
0×000000001e0148e8	userinit.exe	2368	552	0×1e9644c0	2014-01-08 02:18:17 UTC+0000	2014-01-08 02:18:43 UTC+0000
0×000000001e01d020	dwm.exe	2392	1160	0×1e9644e0	2014-01-08 02:18:17 UTC+0000	
0×000000001e02c020	explorer.exe	2496	2368	0×1e964520	2014-01-08 02:18:17 UTC+0000	
0×000000001e02c898	TPAutoConnect.e	2480	832	0×1e964540	2014-01-08 02:18:17 UTC+0000	
0×000000001e0537b0	reader_sl.exe	2616	2592	0×1e9645a0	2014-01-08 02:18:18 UTC+0000	2014-01-08 02:19:20 UTC+0000
0×000000001e05e020	vmtoolsd.exe	2580	2496	0×1e964560	2014-01-08 02:18:18 UTC+0000	
0×000000001e05f020	AdobeARM.exe	2592	2496	0×1e964580	2014-01-08 02:18:18 UTC+0000	
0×000000001e064a50	notepad.exe	3920	2496	0×1e964600	2014-01-08 03:19:07 UTC+0000	
0×000000001e073b60	svchost.exe	3224	604	0×1e9643e0	2014-01-08 02:19:53 UTC+0000	
0×000000001e0e3020	iashost.exe	3336	788	0×1e9645c0	2014-01-08 02:19:53 UTC+0000	
0×000000001e0fd958	FTK Imager.exe	1800	2496	0×1e964620	2014-01-08 03:19:32 UTC+0000	
0×000000001e20b020	vmtoolsd.exe	1640	604	0×1e964360	2014-01-08 02:17:49 UTC+0000	
0×000000001e221d90	svchost.exe	1696	604	0×1e964380	2014-01-08 02:17:49 UTC+0000	
0×000000001e3a1c30	taskeng.exe	2096	1000	0×1e964480	2014-01-08 02:17:53 UTC+0000	
0×000000001e3a8d90	dllhost.exe	1924	604	0×1e964440	2014-01-08 02:17:53 UTC+0000	
0×000000001e3b7ca8	msdtc.exe	1572	604	0×1e964460	2014-01-08 02:17:53 UTC+0000	
0×000000001e3d8020	wuauclt.exe	3680	1000	0×1e9644a0	2014-01-08 02:20:55 UTC+0000	
0×000000001e466d50	svchost.exe	788	604	0×1e964120	2014-01-08 02:17:42 UTC+0000	
0×000000001e4a1340	notepad.exe	2708	2496	0×1e964180	2014-01-08 17:33:08 UTC+0000	
0×000000001e4ab618	iexplore.exe	1888	2496	0×1e964500	2014-01-08 03:20:24 UTC+0000	
0×000000001e4fa118	svchost.exe	884	604	0×1e964160	2014-01-08 02:17:42 UTC+0000	
0×000000001e514d90	svchost.exe	976	604	0×1e9641a0	2014-01-08 02:17:42 UTC+0000	
0×000000001e51bd90	svchost.exe	1000	604	0×1e9641c0	2014-01-08 02:17:42 UTC+0000	
0×000000001e52a6d0	SLsvc.exe	1056	604	0×1e9641e0	2014-01-08 02:17:42 UTC+0000	
0×000000001e537d90	svchost.exe	1088	604	0×1e964200	2014-01-08 02:17:42 UTC+0000	
0×000000001e541d90	svchost.exe	1160	604	0×1e964220	2014-01-08 02:17:42 UTC+0000	
0×000000001e545c30	svchost.exe	1188	604	0×1e964240	2014-01-08 02:17:42 UTC+0000	
0×000000001e56e9f0	svchost.exe	1308	604	0×1e964260	2014-01-08 02:17:43 UTC+0000	
0×000000001e5c18a8	spoolsv.exe	1424	604	0×1e964280	2014-01-08 02:17:49 UTC+0000	
0×000000001e5d7610	armsvc.exe	1460	604	0×1e9642a0	2014-01-08 02:17:49 UTC+0000	
0×000000001e5dcd90	dns.exe	1480	604	0×1e9642c0	2014-01-08 02:17:49 UTC+0000	
0×000000001e5e1cc0	ftpbasicsvr.exe	1508	604	0×1e9642e0	2014-01-08 02:17:49 UTC+0000	
0×000000001e5f5888	svchost.exe	1576	604	0×1e964300	2014-01-08 02:17:49 UTC+0000	
0×000000001e5f7380	snmp.exe	1620	604	0×1e964340	2014-01-08 02:17:49 UTC+0000	
0×000000001e5faad8	svchost.exe	1604	604	0×1e964320	2014-01-08 02:17:49 UTC+0000	
0×000000001e850770	csrss.exe	516	508	0×1e9640a0	2014-01-08 02:17:36 UTC+0000	
0×000000001e853770	wininit.exe	524	460	0×1e9640c0	2014-01-08 02:17:36 UTC+0000	
0×000000001e865770	winlogon.exe	552	508	0×1e964040	2014-01-08 02:17:36 UTC+0000	
0×000000001e8bf770	lsass.exe	616	524	0×1e9640e0	2014-01-08 02:17:36 UTC+0000	
0×000000001e8c2680	lsm.exe	624	524	0×1e964100	2014-01-08 02:17:36 UTC+0000	
0×000000001e94c118	smss.exe	404	4	0×1e964020	2014-01-08 02:17:35 UTC+0000	
0×000000001e961968	csrss.exe	472	460	0×1e964060	2014-01-08 02:17:35 UTC+0000	
0×000000001e9f37a8	svchost.exe	848	604	0×1e964140	2014-01-08 02:17:42 UTC+0000	
0×000000001f632170	services.exe	604	524	0×1e964080	2014-01-08 02:17:36 UTC+0000	
0×000000001fc66b68	TPAutoConnSvc.e	832	604	0×1e964400	2014-01-08 02:17:52 UTC+0000	

Analisis ini menggunakan Plugin malfind pada Volatility digunakan untuk mengidentifikasi kemungkinan injeksi kode berbahaya dalam proses yang berjalan di sistem. Ia mendeteksi Virtual Address Descriptor (VAD) yang memiliki hak akses PAGE_EXECUTE_READWRITE, yang sangat tidak umum untuk memori normal, dan mengindikasikan adanya potensi eksekusi kode berbahaya.

Hasil Analisis malfind terhadap File mdm.mem (profil: VistaSP2x86)

- Proses: explorer.exe (PID: 2496)

Offset: 0x1790000

- ✓ Proteksi: PAGE_EXECUTE_READWRITE

Disassembly menunjukkan pola shellcode berupa jump table:

python-repl	
Copy	
Edit	
b000	MOV AL, 0x0
eb70	JMP ...
b001	MOV AL, 0x1

Analisis: Ini adalah pola khas dari shellcode berbasis jump table, yang sering digunakan dalam injeksi kode. Lokasi dan hak akses memori tidak lazim bagi proses explorer.exe.

- ✓ Offset: 0x3190000

  Disassembly didominasi oleh padding (ADD [EAX], AL, TEST [EAX], AL)

  Analisis: Meskipun ini bisa jadi memori yang dialokasikan tapi belum digunakan, tetap mencurigakan karena proteksi eksekusi diaktifkan. Bisa juga merupakan bagian dari persiapan injeksi.

- ✓ Offset: 0x5d70000

  Berisi instruksi kompleks dan tidak lazim (PUSHA, SHR, XLAT, MOVZX, dll.)

  Analisis: Ini mengindikasikan kode yang disusun secara manual (bukan hasil kompilasi standar), kemungkinan merupakan payload malware atau loader.

  - Proses: notepad.exe (PID: 3920)

- ✓ Offset: 0x840000

  Disassembly berisi banyak padding dan NOP-like behavior (ADD [EAX], AL)

  Proteksi: PAGE_EXECUTE_READWRITE

  Analisis: Tidak lazim untuk notepad.exe memiliki region memori seperti ini. Bisa jadi bagian dari proses injeksi atau pemanfaatan hollowing, namun belum cukup bukti untuk menyatakan berbahaya tanpa analisis lebih lanjut.

  - Proses: iexplore.exe (PID: 1888)

- ✓ Offset: 0x0d60000

  Identik dengan shellcode yang ditemukan pada explorer.exe di 0x1790000

Analisis: Ini sangat menguatkan dugaan bahwa proses telah disusupi dan shellcode telah diinjeksikan ke beberapa proses secara bersamaan (kemungkinan code reuse atau loader terpadu).

- ✓ Offset: 0x39a0000

Sama seperti offset 0x3190000, berisi padding

Analisis: Memori ini bisa digunakan sebagai cadangan untuk injeksi atau penampungan kode sebelum dieksekusi.

- **Kesimpulan Analisis**

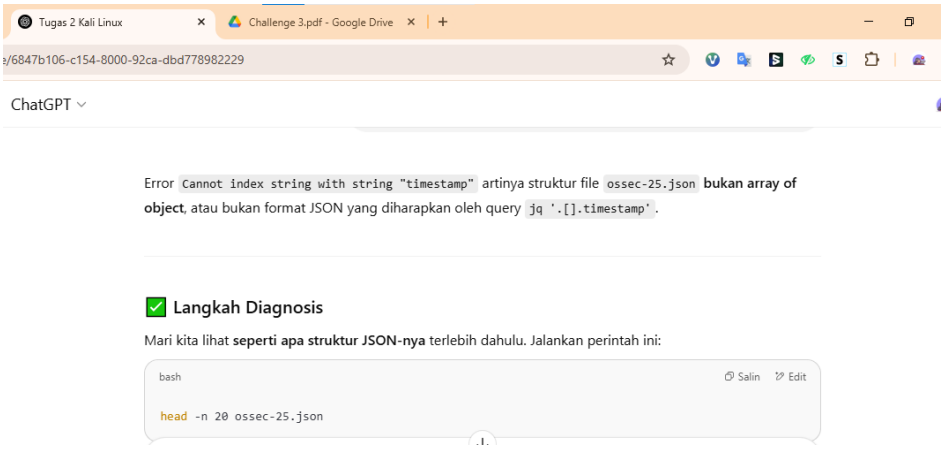
Berdasarkan temuan dari malfind, terdapat indikasi kuat bahwa sistem telah mengalami injeksi kode berbahaya. Shellcode ditemukan di proses-proses umum (explorer.exe dan iexplore.exe), yang menunjukkan bahwa malware menyisipkan kode ke dalam proses sah untuk menyamarkan aktivitasnya (process injection).

Teknik seperti jump table shellcode digunakan untuk menyembunyikan eksekusi.

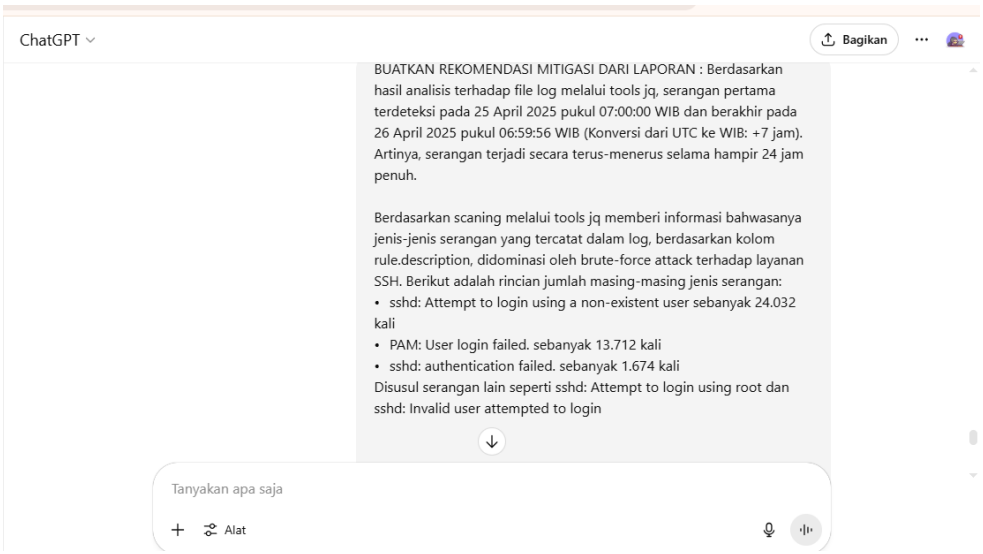
Region memori dengan proteksi EXECUTE_READWRITE digunakan, yang umum dalam teknik injeksi seperti:

- ✓ Reflective DLL injection
- ✓ Shellcode injection
- ✓ Process hollowing

PENGGUNAAN AI



Tim Bear Cyber Hunt menggunakan kecerdasan buatan (AI) untuk menganalisis struktur file ossec-25.json dan mengidentifikasi penyebab kegagalan query pada file 1. Berdasarkan hasil analisis, ditemukan bahwa file JSON tersebut tidak memiliki struktur array of object seperti yang diharapkan, sehingga query jq '.[].timestamp' gagal dijalankan. Langkah diagnosis lanjutan dilakukan dengan memeriksa isi awal file guna memahami format data secara menyeluruh dan menyesuaikan pendekatan parsing yang tepat.



Tim Bear Cyber Hunt menggunakan pendekatan berbasis AI untuk mempercepat proses identifikasi pola serangan dan penyusunan rekomendasi mitigasi pada file 2. Berdasarkan hasil parsing file log menggunakan tool jq, sistem mendeteksi adanya serangan brute-force yang masif terhadap layanan SSH, berlangsung hampir 24 jam penuh. Teknologi AI membantu mengelompokkan jenis serangan, menghitung frekuensi, dan memetakan intensitas waktu serangan untuk mendukung pengambilan keputusan cepat dan tepat dalam mitigasi. Temuan ini memperkuat kebutuhan akan pembatasan login, aktivasi fail2ban, serta implementasi autentikasi multi-faktor (MFA) untuk mengurangi risiko di masa mendatang.