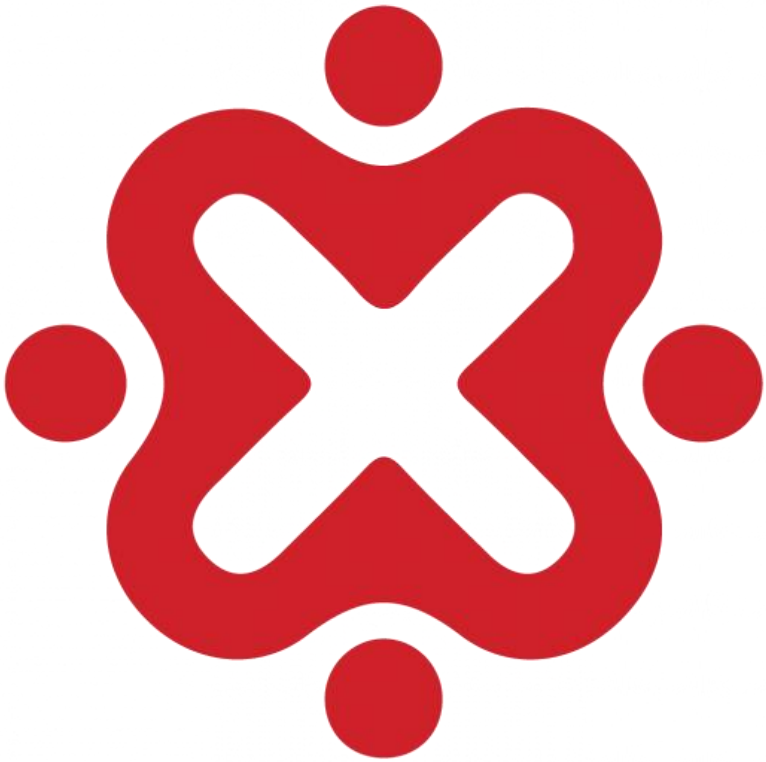
Raihan Putra Kurniawan

Any progress is better than none



ID-Networkers
Indonesian IT Expert Factory

Summary Findings Each Category

Category	Soal Selesai / Dari Soal yang ada	Point
Web Exploit	0/13	0
Other	1/2	10
Web 303	0/7	0
Cryptography	2/7	20
Log Analysis	9/9	90
USB Forensic	8/8	80
Browser Forensic	0/10	0
Windows Forensic	8/15	80

Point : 280
Pengurangan Nilai : 0 Point

Detail Challenge Solved

Others

User Guide

Deskripsi :

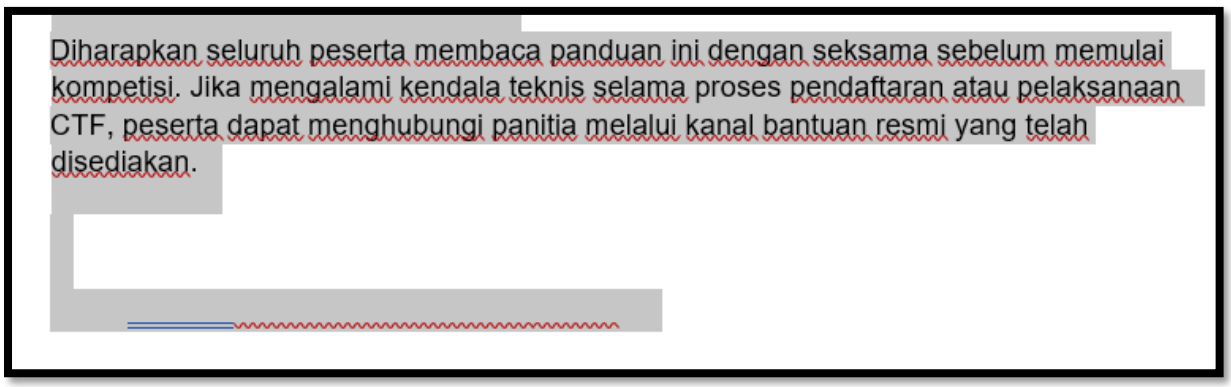
FLAG

Lampiran : none

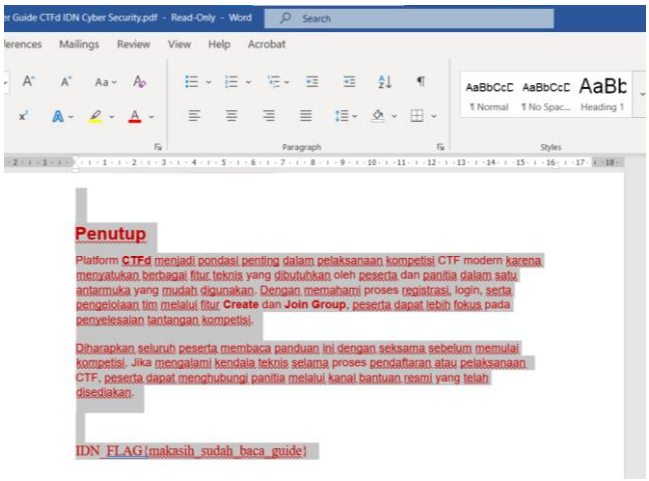
Solusi :

- Membaca seluruh **User Guide**.
- Menemukan format **flag**, lalu coba submit flag Namun **inccorect**.

- Mulai mencari text tersembunyi, dengan **CTRL + A** agar seluruh isi dalam document **ter-blok**. Menemukan baris yang ter-blok namun tidak ada textnya atau **tersembunyi**. Lalu coba **ubah warna** textnya.



- Setelah diubah warna textnya, menemukan **text yang tersembunyi**. Lalu coba submit sebagai **flag** dan **correct**.



Flag : IDN_FLAG{makasih_sudah_baca_guide}

Cryptography

Rot1Aoka

Deskripsi :

Clue nya udah jelas kan? VQA_SYNT{C3Z4A4F4A_QH1H_94F1u} Author : Mohamad Fattyr

Lampiran :

Solusi :

- Petunjuk : Rot1Aoka : Jenis Cipher ROT = ROT1 / ROT13
- Gunakan decoder online
- Coba ROT-1 = Incorrect

- Coba ROT13 untuk seluruh string = correct

Flag : IDN_FLAG{P3M4N4S4N_DU1U_94S1H}

Pramuka

Deskripsi :

terjemahan kan pesan tersebut. Format Flag

IDN_CTF{****}

Author : Mohamad Fattyr

morse.wav

Lampiran : morse.wav

Solusi :

- Terlihat dari judul " Pramuka " dan Nama file audio bahwa ini adalah pesan sandi Morse.
- Lalu mencoba decode dengan decoder online sandi morse.
- Hasil decode " M0RS3C0D3R19HT ".
- Lalu ditambahkan spasi.

Flag : IDN_CTF{ M0RS3_C0D3_R19HT}

USB Forensic

USB Forensic 1

Deskripsi :

ada hacker, physical acces ke laptop.. bantuin dong !

Merek usb apa yang dipakai oleh hacker untuk delivery file nya ?

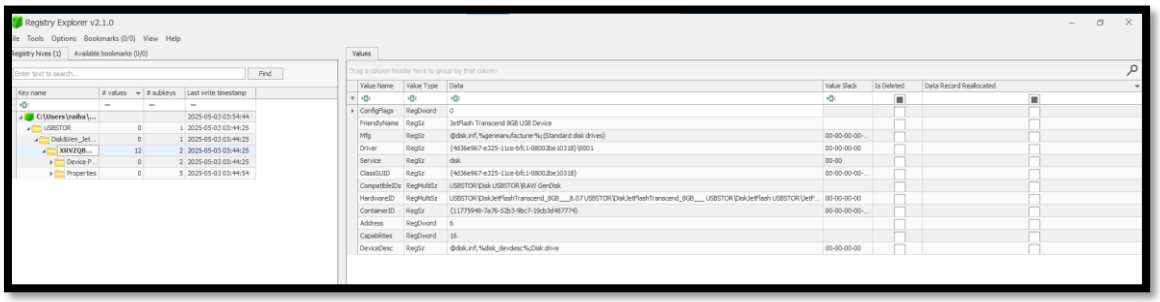
format flag : IDN_FLAG{Nama_Device_Ukuran_USB_Device}

Auhtor: Aditya Firman Nugroho

Lampiran : usb.zip

Solusi :

- Zip berisi file **Registry** :
  - MountPoints2.hiv = Volume & path USB yang dipasang
  - NTUSER.DAT = File dibuka, folder diakses, konfigurasi user
  - RecentDocs.hiv = Nama file terakhir yang dibuka
  - USBTOR.hiv = Vendor USB, Serial Number, kapasitas
  - USRCLASS.DAT = Folder terakhir yang diakses dari USB
- Gunakan tools forensic **Registry Explorer** (Eric Zimmerman's tools).
- Berdasarkan informasi di deskripsi, mulai lakukan forensik file **USBTOR.hiv** .
- Menemukan informasi Device USB di **" USBTOR.hiv: Disk&Ven_JetFlash&Prod_Transcend_8GB&Rev_8.07\XRVZQBFR&0 ".**
- Di value name **"friendlyName"** terdapat Value **"JetFlash Transcend 8GB USB Device".**



Flag : IDN_FLAG{JetFlash_Transcend_8GB_USB_Device}

USB Forensic 2

Deskripsi :

ada hacker, physical acces ke laptop.. bantuin dong !

(Filenya ada di pertanyaan pertama)

ClassGUID Pada USB Hacker ?

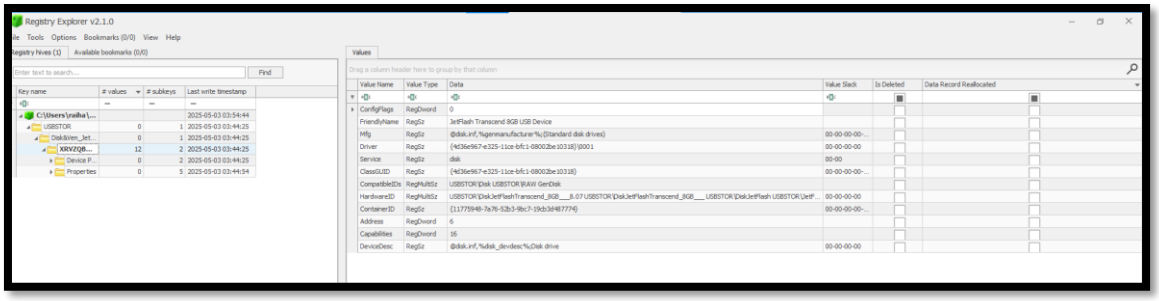
format flag : IDN_FLAG{Jawaban yang disoal}

Auhtor: Aditya Firman NugrohoAuthor: Rafly Permana

Lampiran : None

Solusi :

- Menemukan informasi Device USB di **" USBTOR.hiv: Disk&Ven_JetFlash&Prod_Transcend_8GB&Rev_8.07\XRVZQBFR&0 ".**
- Di value name **"ClassGUID"** terdapat Value **"{4d36e967-e325-11ce-bfc1-08002be10318}".**



Flag : IDN_FLAG{{4d36e967-e325-11ce-bfc1-08002be10318}}

USB Forensic 3

Deskripsi :

ada hacker, physical acces ke laptop.. bantuin dong !

(Filenya ada di pertanyaan pertama)

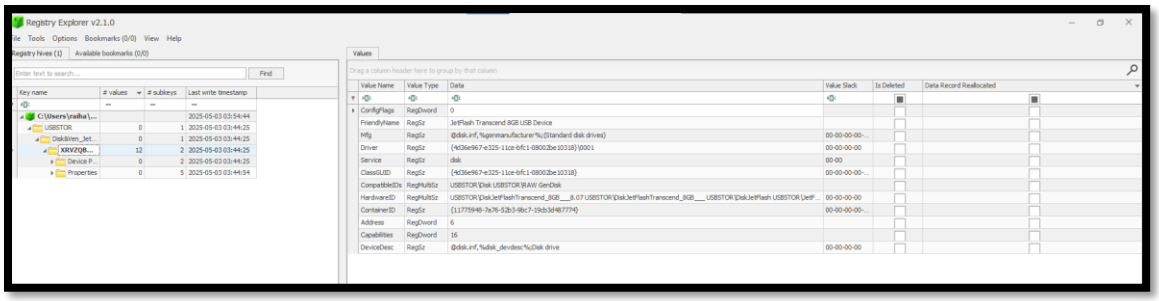
Apa Containder ID USB Yang dipakai Hacker ?

format flag : IDN_FLAG{Jawaban yang disoal}

Lampiran : None

Solusi :

- Menemukan informasi Device USB di **" USBTOR.hiv: Disk&Ven_JetFlash&Prod_Transcend_8GB&Rev_8.07\XRVZQBFR&0 ".**
- Di value name **"ContainerID"** terdapat Value **{11775948-7a76-52b3-9bc7-19cb3d487774}".**



Flag : IDN_FLAG{{11775948-7a76-52b3-9bc7-19cb3d487774}}

USB Forensic 4

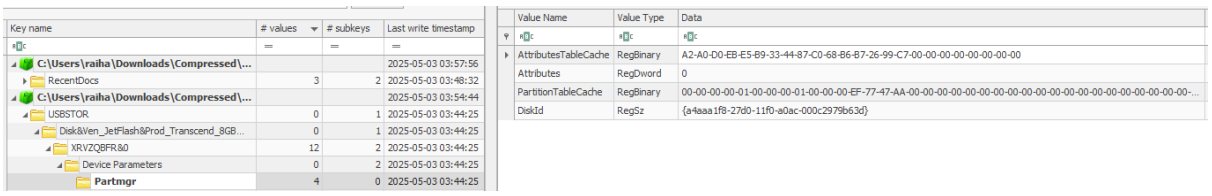
Deskripsi :

ada hacker, physical acces ke laptop.. bantuin dong !
(Filenya ada di pertanyaan pertama)
Apa Disk ID yang dipakai hacker ?
format flag : IDN_FLAG{Jawaban yang disoal}
Auhtor: Aditya Firman Nugroho

Lampiran : None

Solusi :

- Menemukan informasi Device USB di **"USBTOR.hiv: Disk&Ven_JetFlash&Prod_Transcend_8GB&Rev_8.07\XRVZQBFR&0\Device Parameters\Partmgr ".**
- Di value name **"DiskId"** terdapat Value "**{a4aaa1f8-27d0-11f0-a0ac-000c2979b63d}}".**



Key name	# values	# subkeys	Last write timestamp
C:\Users\raiha\Downloads\Compressed\...			2025-05-03 03:57:56
RecentDocs	3	2	2025-05-03 03:48:32
C:\Users\raiha\Downloads\Compressed\...			2025-05-03 03:54:44
USBSTOR	0	1	2025-05-03 03:44:25
Disk&Ven_JetFlash&Prod_Transcend_8GB...	0	1	2025-05-03 03:44:25
XRVZQBFR&0	12	2	2025-05-03 03:44:25
Device Parameters	0	2	2025-05-03 03:44:25
Partmgr	4	0	2025-05-03 03:44:25

Value Name	Value Type	Data
AttributesTableCache	RegBinary	A2-A0-D0-EB-E5-B9-33-44-87-C0-68-B6-B7-26-99-C7-00-00-00-00-00-00-00-00
Attributes	RegDword	0
PartitionTableCache	RegBinary	00-00-00-00-01-00-00-00-01-00-00-00-EF-77-47-AA-00-00-00-00-00-00-00-00-...
DiskId	RegSz	{a4aaa1f8-27d0-11f0-a0ac-000c2979b63d}

Flag : IDN_FLAG{{a4aaa1f8-27d0-11f0-a0ac-000c2979b63d}}

USB Forensic 5

Deskripsi :

> ada hacker, physical acces ke laptop.. bantuin dong !
>
> (Filenya ada di pertanyaan pertama)
>
> Apa Serial ID USB Yang dipakai Hacker ?
>
> format flag : IDN_FLAG{Jawaban yang disoal}
>
> Auhtor: Aditya Firman Nugroho

Lampiran : None

Solusi :
Serial ID USB biasanya terletak sebagai nama folder / subkey dari " USBTOR.hiv ". Dan menemukan serial IDnya di path "USBTOR.hiv: Disk&Ven_JetFlash&Prod_Transcend_8GB&Rev_8.07\XRVZQBFR&0" yaitu "XRVZQBFR&0".

Flag : IDN_FLAG{XRVZQBFR&0}

USB Forensic 6

Deskripsi :

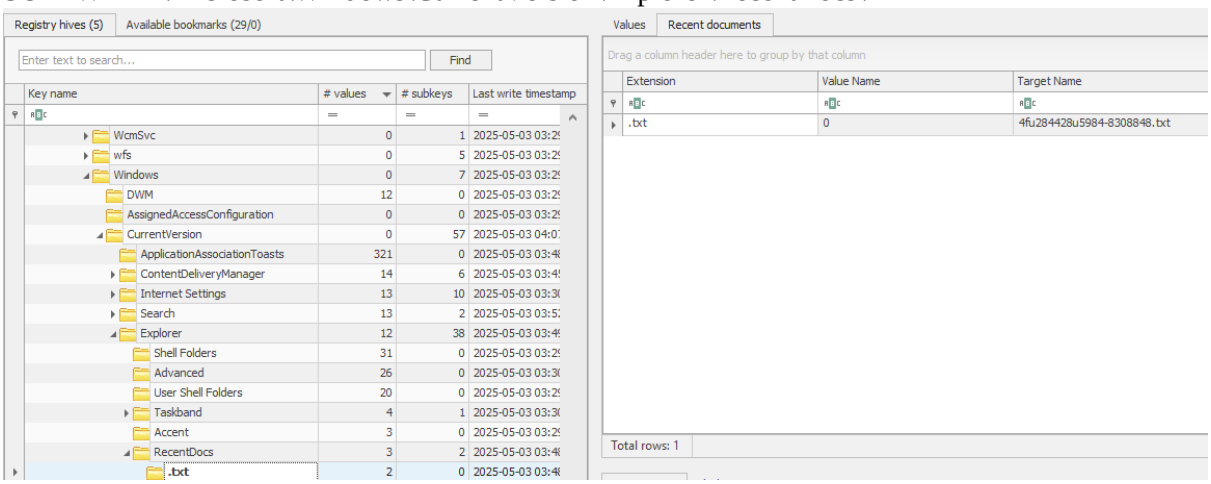
> ada hacker, physical acces ke laptop.. bantuin dong !
>
> (Filenya ada di pertanyaan pertama)
>
> Nama File Yang ada di USB ?
>
> format flag : IDN_FLAG{Jawaban yang disoal}
>
> Auhtor: Aditya Firman Nugroho

Lampiran : None

Solusi :

- RecentDocs registry menyimpan file-file terakhir yang dibuka di komputer, termasuk file dari USB.
- Mencoba cari recentdocs registry Explorer di Ntuser.dat .

- Menemukan target name registry “4f624842b5984-8308848.txt “ di path “NTUSER.dat: SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs\.txt “



Flag : IDN_FLAG{4f624842b5984-8308848.txt}

USB Forensic 7

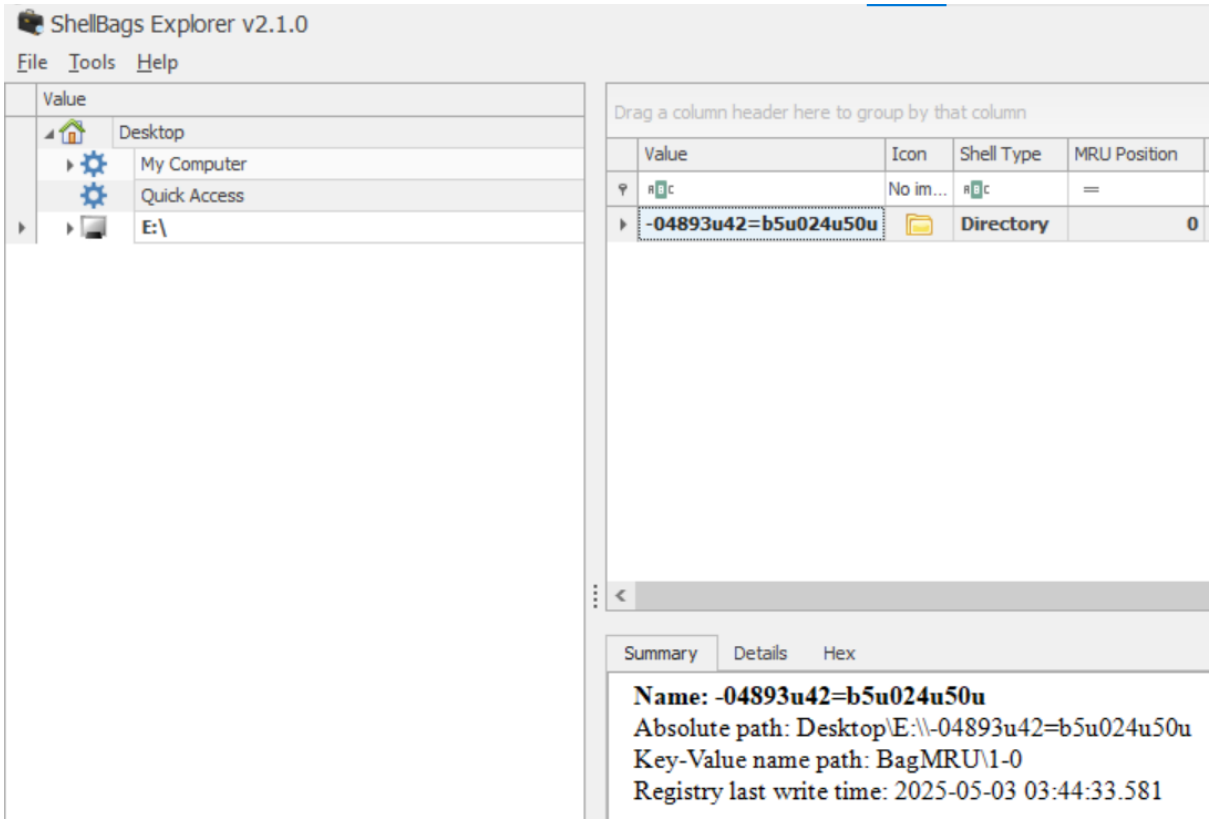
Deskripsi :

> ada hacker, physical acces ke laptop.. bantuin dong !
>
> (Filenya ada di pertanyaan pertama)
>
> Direktory Yang ada di usb ?
>
> format flag : IDN_FLAG{Jawaban yang disoal} example : *:\directory
>
> Auhtor: Aditya Firman Nugroho

Lampiran : None

Solusi :

- Gunakan **ShellBags Explorer** untuk mengekstrak informasi dari ShellBags file “ **USRCLASS.dat** “(karena Registry Explorer tidak menampilkan path direktori USB secara utuh).
- Mendapatkan informasi directory path USB yaitu “ **Absolute path: Desktop\E:\\-04893u42=b5u024u50u** “ .



Flag : IDN_FLAG{E:\-04893u42=b5u024u50u}

USB Forensic 8

Deskripsi :

ada hacker, physical acces ke laptop.. bantuin dong !

(Filenya ada di pertanyaan pertama)

File dibuka pada jam ?

format flag : IDN_FLAG{Jawaban yang disoal} example : xxxx-xx-xx xx:xx:xx

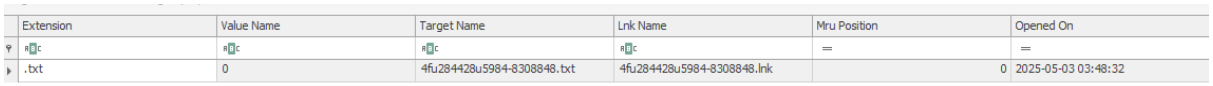
Auhtor: Aditya Firman Nugroho

Lampiran : None

Solusi :

- RecentDocs registry menyimpan file-file terakhir yang dibuka di komputer, termasuk file dari USB.
- Mencoba cari recentdocs registry Explorer di Ntuser.dat .
- Menemukan target name registry “4f624842b5984-8308848.txt “ di path “NTUSER.dat: SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs\.txt “

- Di registry tersebut terdapat informasi " opened On " yang berisi kapan file tersebut dibuka.



Extension	Value Name	Target Name	Lnk Name	Mru Position	Opened On
.txt	0	4fu284428u5984-8308848.txt	4fu284428u5984-8308848.lnk	0	2025-05-03 03:48:32

Flag : IDN_FLAG{ 2025-05-03 03:48:32}

Windows Forensic

Windows Forensic 1

Deskripsi :

Ceritanya, udh ambil hivenya.. mount, trus cari beberapa informasi tambahan lainya !!

(Filenya ada di pertanyaan pertama)

Nama file yang menyimpan credential ?

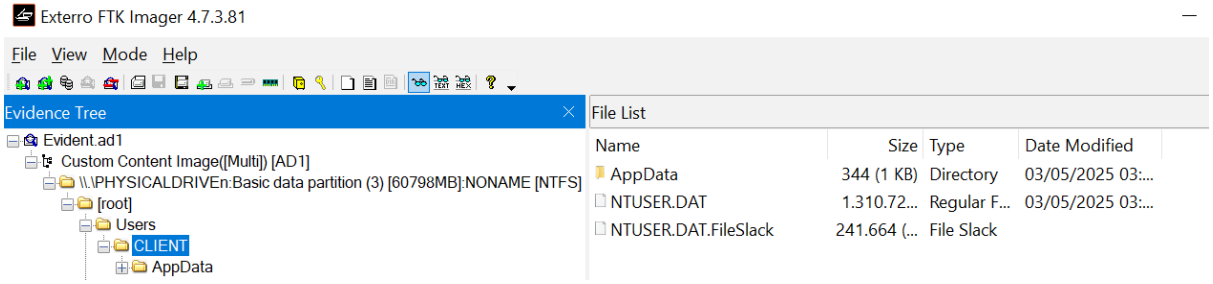
format flag : IDN_FLAG{Jawaban yang disoal} example : xxxxxxxx_xxx.xxx

Auhtor: Aditya Firman Nugroho

Lampiran : Windows.zip

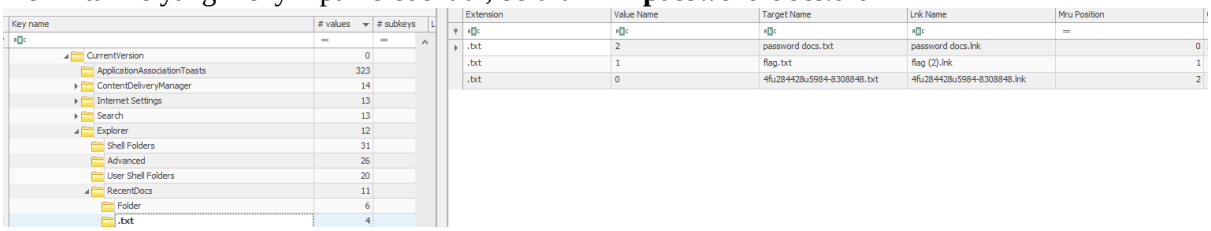
Solusi :

- Mount Evident.ad1 menggunakan **FTK Imager**.
- Masuk ke folder: \Users\CLIENT. Lalu export file **NTUSER.DAT**



- Buka file NTUSER.DAT menggunakan **Registry Explorer**.
- Lalu cari registry RecentDocs. Ketemu di path "NTUSER.DAT: SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs ".

- Didalam folder RecentDocs terdapat folder .txt yang berisi beberapa nama file. Deskripsi meminta file yang menyimpan credential, berarti file "**password docs.txt**".



Key name	# values	# subkeys
CurrentVersion	0	
ApplicationAssociationToasts	323	
ContentDeliveryManager	14	
Internet Settings	13	
Search	13	
Explorer	12	
Shell Folders	31	
Advanced	26	
User Shell Folders	20	
RecentDocs	11	
Folder	6	
.txt	4	

Extension	Value Name	Target Name	Lnk Name	Mru Position
.txt	2	password docs.txt	password docs.lnk	0
.txt	1	flag.txt	flag (2).lnk	1
.txt	0	4fu284428u5984-8308848.txt	4fu284428u5984-8308848.lnk	2

Flag : IDN_FLAG{ password_docs.txt }

Windows Forensic 2

Deskripsi :

> Ceritanya, udh ambil hivenya.. mount, trus cari beberapa informasi tambahan lainya !!
>
> (Filenya ada di pertanyaan pertama)
>
> file yang menyimpan credential, dibuka pada tanggal berapa ?
>
> format flag : IDN_FLAG{Jawaban yang disoal} example : xxxx-xx-xx xx:xx:xx
>
> Auhtor: Aditya Firman Nugroho

Lampiran : None

Solusi :
Di Registry RecentDocs dengan path "NTUSER.DAT: SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs\.txt" terdapat keterangan file "password_docs.txt" dibuka pada " 2025-05-03 07:16:29 ".

Extension	Value Name	Target Name	Lnk Name	Mru Position	Opened On
.txt	2	password docs.txt	password docs.lnk	0	2025-05-03 07:16:29
.txt	1	flag.txt	flag (2).lnk	1	
.txt	0	4fu284428u5984-8308848.txt	4fu284428u5984-8308848.lnk	2	

Flag : IDN_FLAG{2025-05-03 07:16:29}

Windows Forensic 3

Deskripsi :

> Ceritanya, udh ambil hivenya.. mount, trus cari beberapa informasi tambahan lainya !!

(Filenya ada di pertanyaan pertama)

User yang dibuat pada tanggal 2025-05-03 07:04:43, Username nya ?

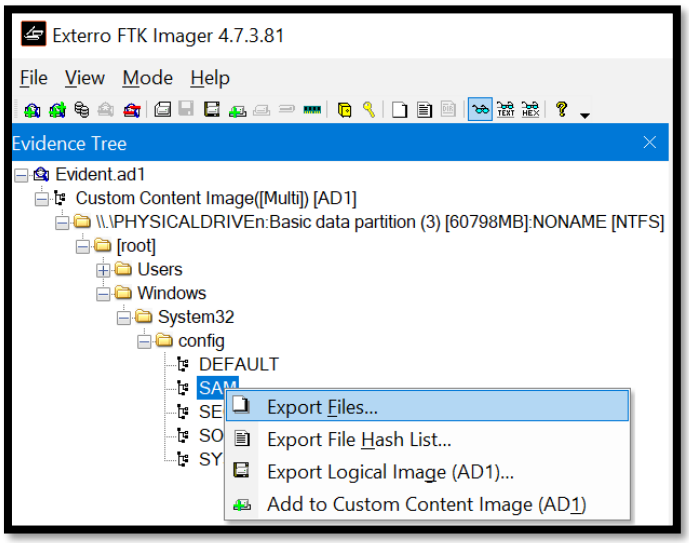
format flag : IDN_FLAG{Jawaban yang disoal}

Auhtor: Aditya Firman Nugroho

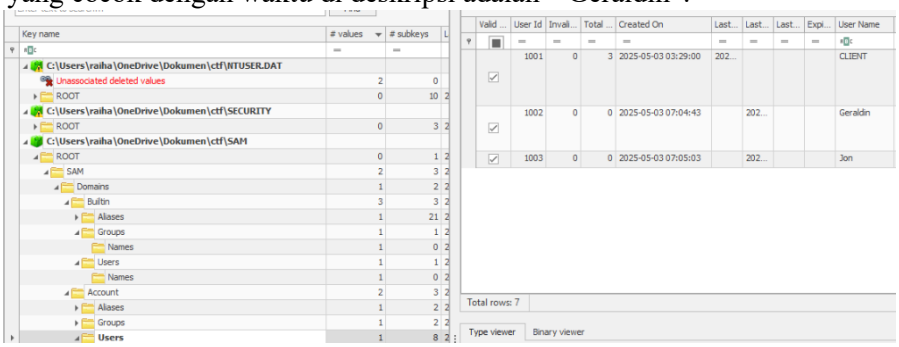
Lampiran : None

Solusi :

- Mount Evident.ad1 menggunakan **FTK Imager**.
- Masuk ke folder: \Windows\System32\Config. Lalu export file **SAM.**



- Buka file SAM menggunakan **Registry Explorer**.
- Cari registry yang berisikan informasi User. Ketemu di path “SAM: SAM\Domains\Account\Users “
- User yang cocok dengan waktu di deskripsi adalah “ Geraldin”.



Flag : IDN_FLAG{Geraldin}

Windows Forensic 4

Deskripsi :

Ceritanya, udh ambil hivenya.. mount, trus cari beberapa informasi tambahan lainya !!

(Filenya ada di pertanyaan pertama)

User yang dibuat pada tanggal 2025-05-03 07:05:03, Username nya ?

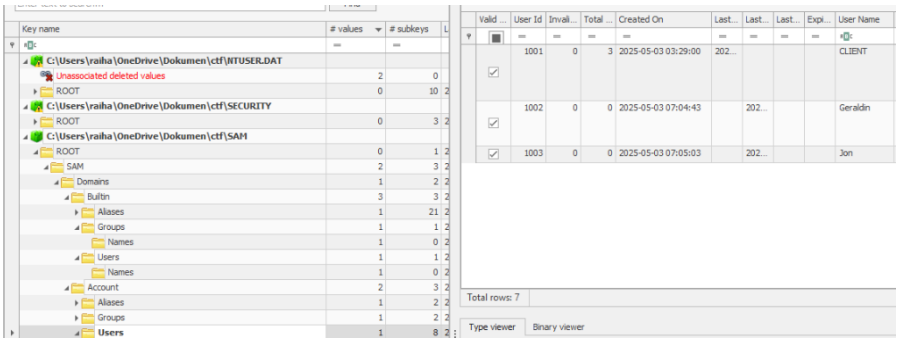
format flag : IDN_FLAG{Jawaban yang disoal}

Auhtor: Aditya Firman Nugroho

Lampiran : None

Solusi :

- Buka file SAM menggunakan **Registry Explorer**.
- Cari registry yang berisikan informasi User. Ketemu di path “SAM: SAM\Domains\Account\Users “
- User yang cocok dengan waktu di deskripsi adalah “Jon”.



Flag : IDN_FLAG{ Jon}

Windows Forensic 5

Deskripsi :

Ceritanya, udh ambil hivenya.. mount, trus cari beberapa informasi tambahan lainya !!

(Filenya ada di pertanyaan pertama)

User yang localgroupnya ada 2, yaitu ?

format flag : IDN_FLAG{Jawaban yang disoal}

Auhtor: Aditya Firman Nugroho

Lampiran : None

Solusi :

- Buka file SAM menggunakan **Registry Explorer**.
- Cari registry yang berisikan informasi User. Ketemu di path “SAM: SAM\Domains\Account\Users “
- User yang local groupnya ada 2 yaitu “ Geraldin”. Ia termasuk dalam group “ administrators “ dan “ Users” .

Valid ...	User Id	Invali...	Total ...	Created On	Last...	Last...	Last...	Expi...	User Name	Full ...	Pas...	Groups
☑	504	0	0	2025-05-03 03:27:38		202...			WDAGUtilityAccount			
☑	1001	0	3	2025-05-03 03:29:00	202...				CLIENT			Administrators
☑	1002	0	0	2025-05-03 07:04:43		202...			Geraldin			Administrators, Users
☑	1003	0	0	2025-05-03 07:05:03		202...			Jon			Users

Flag : IDN_FLAG{Geraldin}

Windows Forensic 6

Deskripsi :

Ceritanya,udh ambil hivenya.. mount, trus cari beberapa informasi tambahan lainya !!

(Filenya ada di pertanyaan pertama)

Last Login Time dari User Cli.. ?

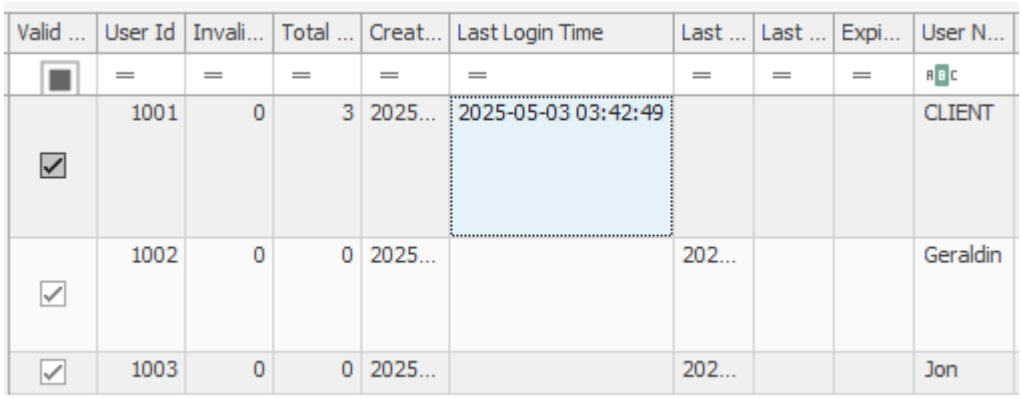
format flag : IDN_FLAG{Jawaban yang disoal} example : xxxx-xx-xx xx:xx:xx

Auhtor: Aditya Firman Nugroho

Lampiran : None

Solusi :

- Buka file SAM menggunakan **Registry Explorer**.
- Cari registry yang berisikan informasi User. Ketemu di path “SAM: SAM\Domains\Account\Users “
- Deskripsi memberikan clue user “ CLI.. “. Yang mendekati clue deskripsi adalah User “ CLIENT “. Last Login Time dari user CLIENT adalah “ 2025-05-03 03:42:49 “ .



Valid ...	User Id	Invali...	Total ...	Creat...	Last Login Time	Last ...	Last ...	Expi...	User N...
☑	1001	0	3	2025...	2025-05-03 03:42:49				CLIENT
☑	1002	0	0	2025...		202...			Geraldin
☑	1003	0	0	2025...		202...			Jon

Flag : IDN_FLAG{2025-05-03 03:42:49}

Windows Forensic 7

Deskripsi :

Ceritanya, udh ambil hivenya.. mount, trus cari beberapa informasi tambahan lainya !!

(Filenya ada di pertanyaan pertama)

User ID dari user dengan 3 huruf ?

format flag : IDN_FLAG{Jawaban yang disoal}

Auhtor: Aditya Firman Nugroho

Lampiran : None

Solusi :

- Buka file SAM menggunakan **Registry Explorer**.

- Cari registry yang berisikan informasi User. Ketemu di path “SAM: SAM\Domains\Account\Users “
- Dari informasi yang ada, user dengan 3 huruf hanya “ Jon “. Dan user ID “ Jon “ adalah “ 1003 “.

User Id	Invali...	Total ...	Creat...	Last Login Time	Last ...	Last ...	Expi...	User N...
1001	0	3	2025...	2025-05-03 03:42:49				CLIENT
1002	0	0	2025...		202...			Geraldin
1003	0	0	2025...		202...			Jon

Flag : IDN_FLAG{1003}

Windows Forensic 8

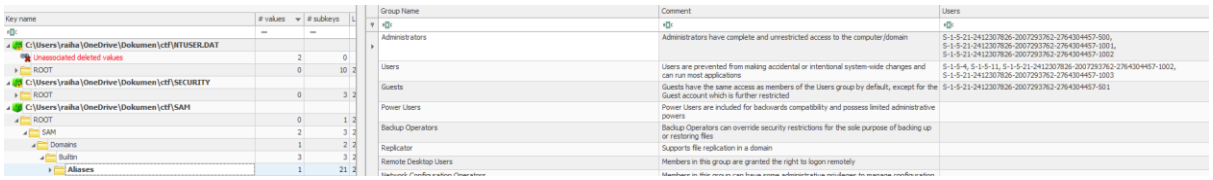
Deskripsi :

> Ceritanya, udh ambil hivenya.. mount, trus cari beberapa informasi tambahan lainya !!
>
> (Filenya ada di pertanyaan pertama)
>
> SID Dari User Guest ?
>
> format flag : IDN_FLAG{Jawaban yang disoal}
>
> Auhtor: Aditya Firman Nugroho

Lampiran : None

Solusi :

- SID (Security Identifier) adalah kode unik yang digunakan oleh Windows untuk mengidentifikasi user, group, dan akun lainnya dalam sistem. Mirip seperti NIK di KTP untuk user account di Windows.
- Buka file SAM menggunakan **Registry Explorer**.
- Cari registry yang berisikan informasi User dan ada SID. Ketemu di path “SAM: SAM\Domains\Builtin\Aliases “.



Flag : IDN_FLAG{ S-1-5-21-2412307826-2007293762-2764304457-501}

Log Analysis

Log Analysis 1

Deskripsi :

pada file pcap dibawah, hacker mencoba untuk melakukan sesuatu yang berhubungan dengan recon pada service, silahkan cari...

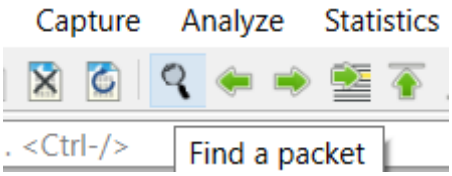
Format Flag : IDN_CTF{jawaban}

Author : Aditya Firman Nugroho

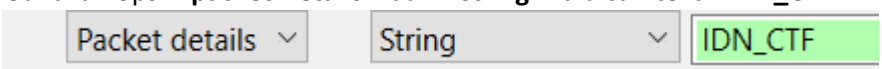
Lampiran : incident respone .pcapng

Solusi :

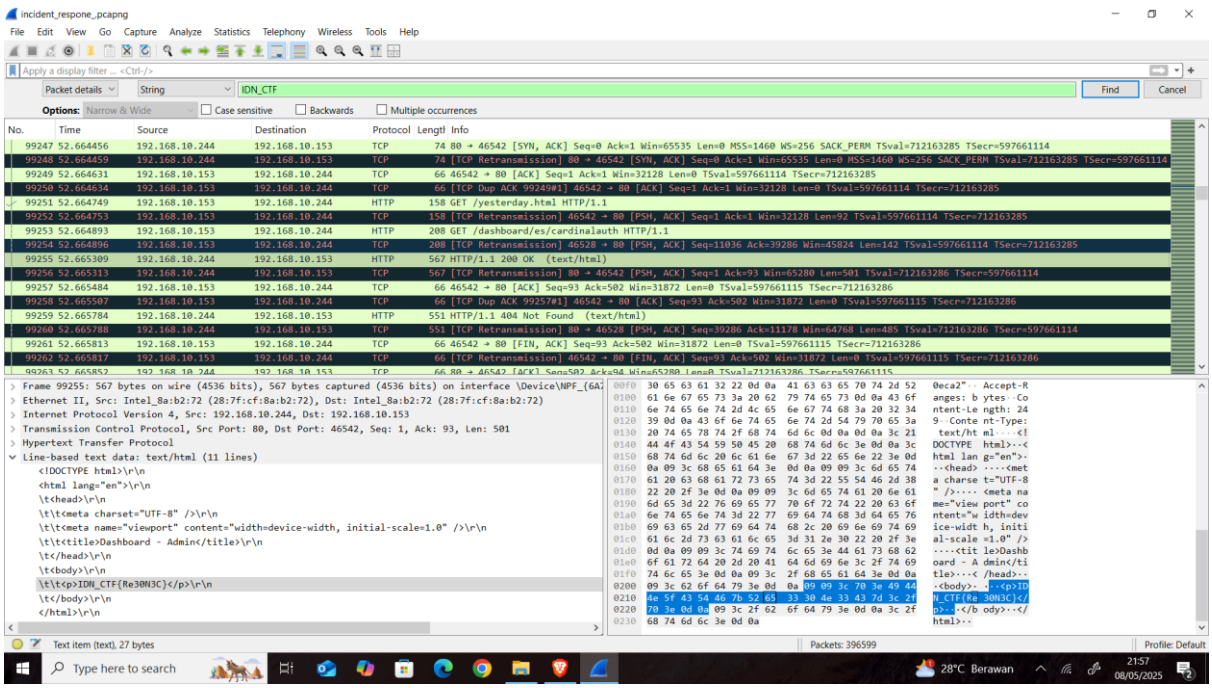
- Buka file pcap menggunakan wireshark.
- Lalu coba gunakan fitur **" find a packet".**



- Gunakan opsi **" packet Details "** dan **" string "** lalu cari text **" IDN_CTF"**



- Menemukan packet yang berisi text html yang berisikan **"IDN_CTF"** .



Flag : IDN_CTF{Re30N3C}

Log Analysis 2

Deskripsi :

awas, hati-hati, pelan-pelan, ada .....

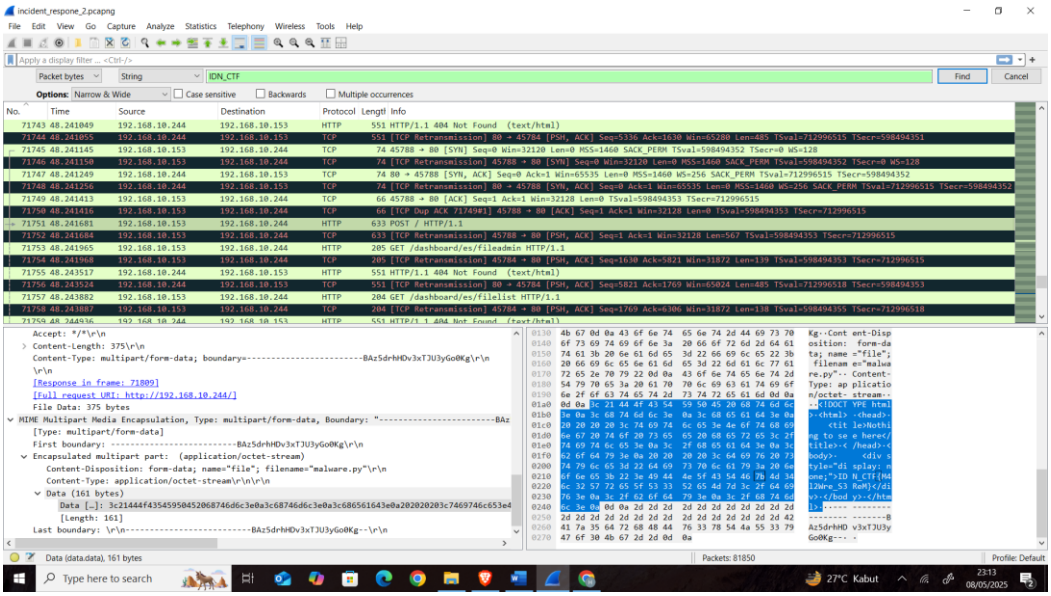
Format Flag : IDN_CTF{jawaban}

Author : Aditya Firman Nugroho

Lampiran : incident_respone_2.pcapng

Solusi :

- gunakan fitur **“ find a packet”.** Gunakan opsi **“ packet Details “** dan **“ string “** lalu cari text **“ IDN_CTF”** .
- Tidak ketemu, lalu coba keywords lain.
- Masih tidak ketemu juga. mulai mengamati lalu lintas jaringan, mungkin flag adalah nama serangannya.
- Lalu coba lagi gunakan fitur **“ find a packet”.** namun gunakan opsi **“ packet bytes “** dan **“ string “** lalu cari text **“ IDN_CTF”.** Ketemu.



Flag : IDN_CTF{M4l2Wre_S3ReM}

Log Analysis 3

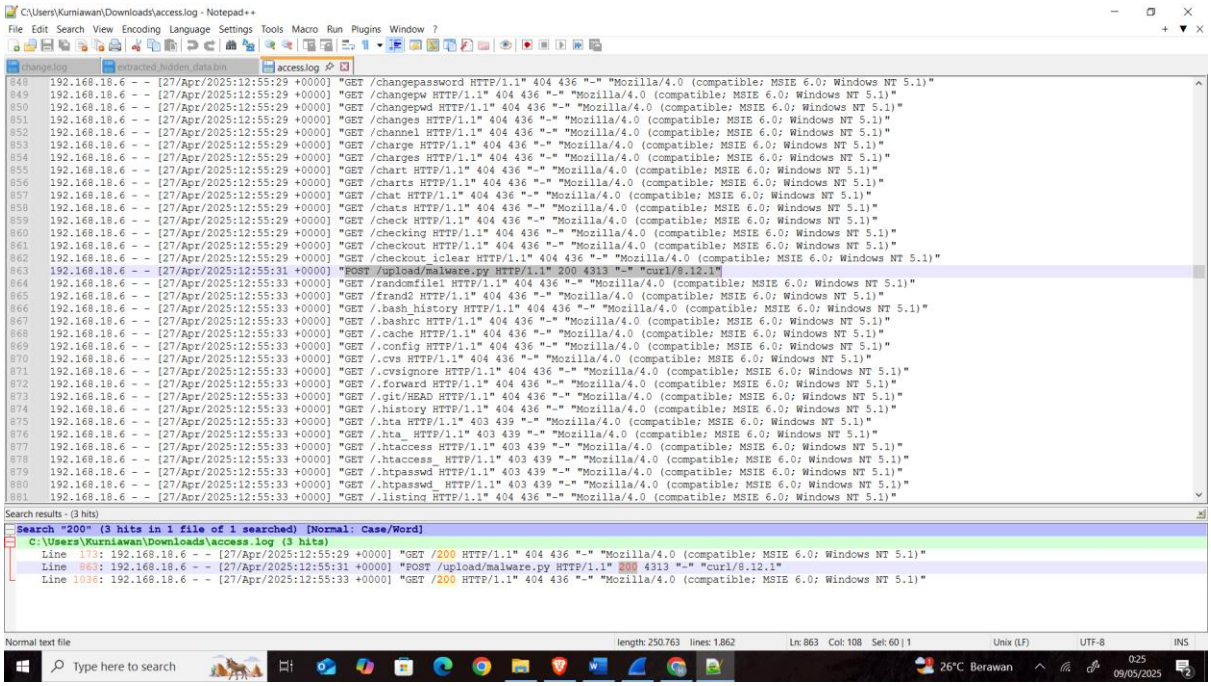
Deskripsi :

analisis log acces.log ini, file ip yang dimasukan pada system ? Format Flag : IDN_CTF{jawaban} Author : Aditya Firman Nugroho

Lampiran : access.log

Solusi :

- Menggunakan aplikasi Notepad++ untuk membuka file lognya.
- Gunakan fitur Find untuk mencari kata kunci **"200",** karena kode **HTTP 200** menandakan akses berhasil.
- Dari hasil pencarian, ditemukan bahwa file **malware.py** berhasil dikirim ke endpoint /upload menggunakan metode POST.



Flag : IDN_CTF{malware.py}

Log Analysis 4

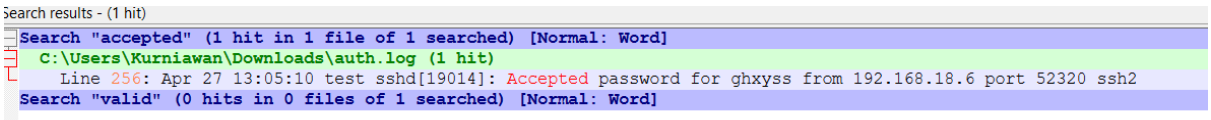
Deskripsi :

> analis log auth.log, user apa yang sukses masuk ke dalam system ?
>
> Format Flag : IDN_CTF{user}
>
> Author : Aditya Firman Nugroho

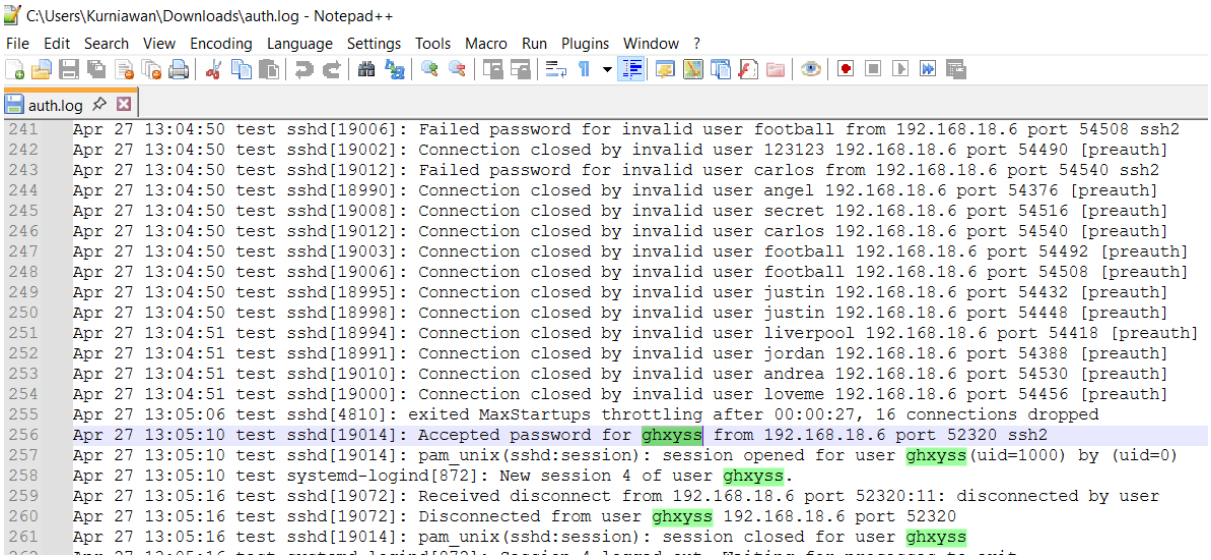
Lampiran : auth.log

Solusi :

- Gunakan aplikasi notepad, lalu gunakan fitur findnya untuk mencari keyword **“ valid “** (match whole word only) tidak ditemukan.
- Lalu cari keyword **“ accepted “,** ditemukan.



- Dari keyword itu ditemukan **“ghxyss”**. Selanjutnya di line berikutnya dapat mengetahui bahwa itu merupakan nama user dan berhasil masuk ke system.



Flag : IDN_CTF{ghxyss}

Log Analysis 5

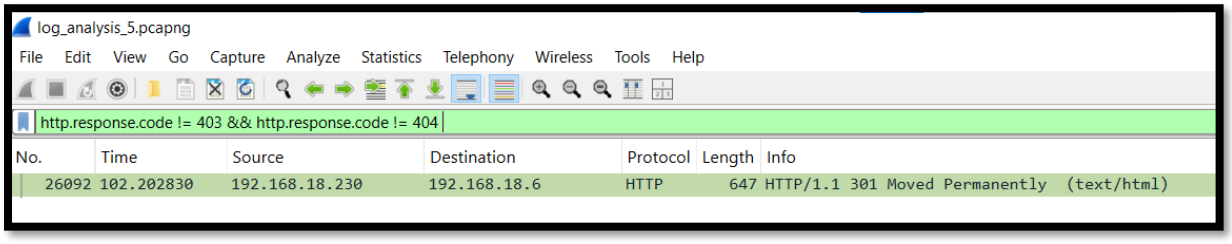
Deskripsi :

> "dengan service ... file ... di dalam server " - administrator
>
> Format Flag : IDN_CTF{service:file}
>
> Author : Aditya Firman Nugroho

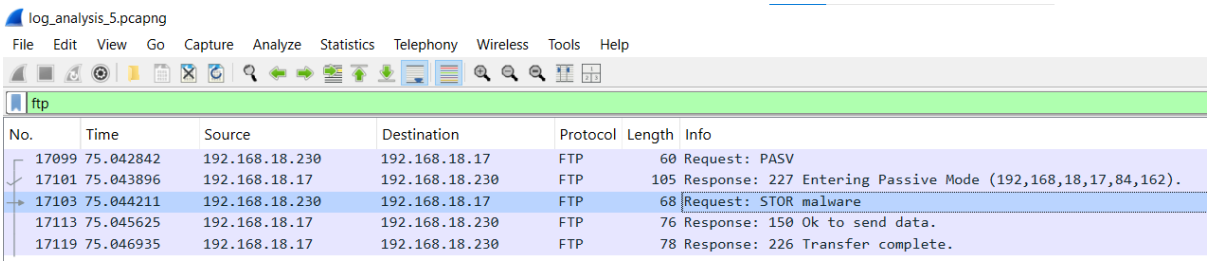
Lampiran : log_analysis_5.pcapng

Solusi :

- Dari deskripsi bisa diartikan men-upload file ke server, untuk upload file biasanya menggunakan service **HTTP dan FTP**.
- Gunakan fitur **"display filter"** , input keyword **HTTP.** Data yang ditampilkan masih banyak dan **HTTP response** nya banyak yang sama yaitu **not found**, lalu gunakan keyword filter tambahan **" http.response.code != 403 && http.response.code != 404".** Hasilnya tidak ada yang berhasil masuk.



- mencoba gunakan filter dengan keyword **FTP**. Lalu menemukan perintah **STOR**. Dan di line selanjutnya menunjukkan **transfer complete**.



Flag : IDN_CTF{ftp:malware}

Log Analysis 6

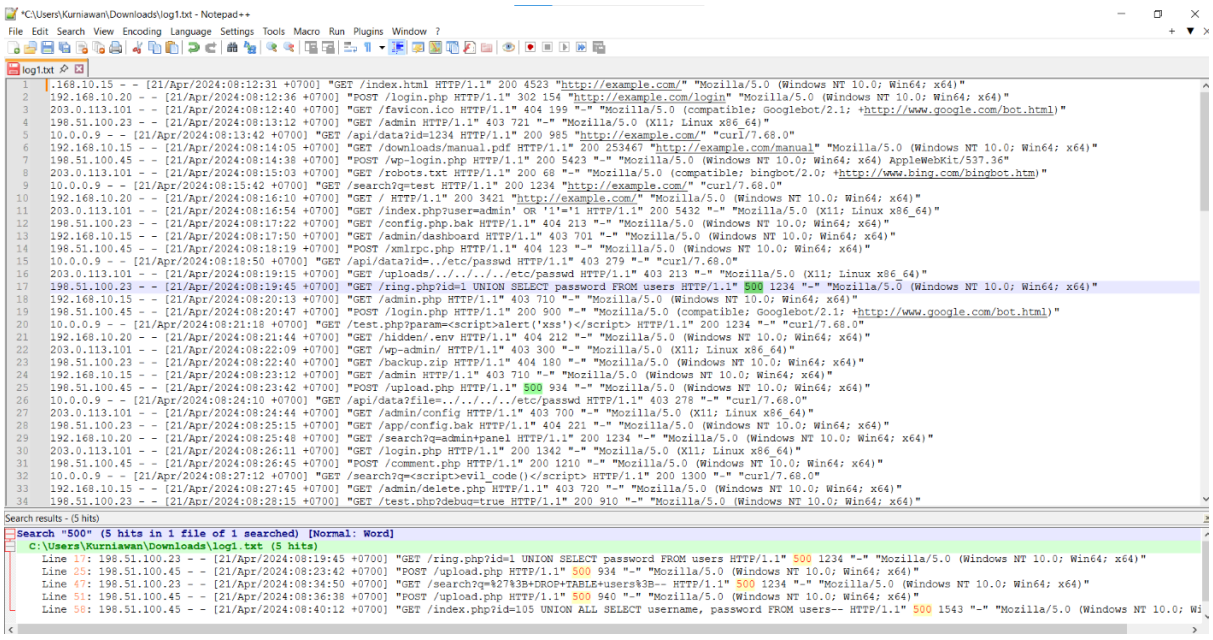
Deskripsi :

> Seseorang mencoba mengeksploitasi endpoint dengan teknik SQL Injection, menghasilkan internal server error. Apa nama file yang ditargetkan dalam eksploitasi tersebut?
>
> IDN_CTF{jawaban}
>
> Author: Rafly Permana

Lampiran : log1.txt

Solusi :

- kode **internal server error = 500**
- gunakan fitur **find** untuk mencari keyword **"500".**



- Terdapat query **UNION SELECT**, teknik umum dalam **SQL Injection** Dan **Target kolom sensitive** yaitu **password FROM users.**
- **" GET /ring.php? "** menunjukkan bahwa file **ring.php** adalah **endpoint** yang diminta.

Flag : IDN_CTF{ring.php}

Log Analysis 7

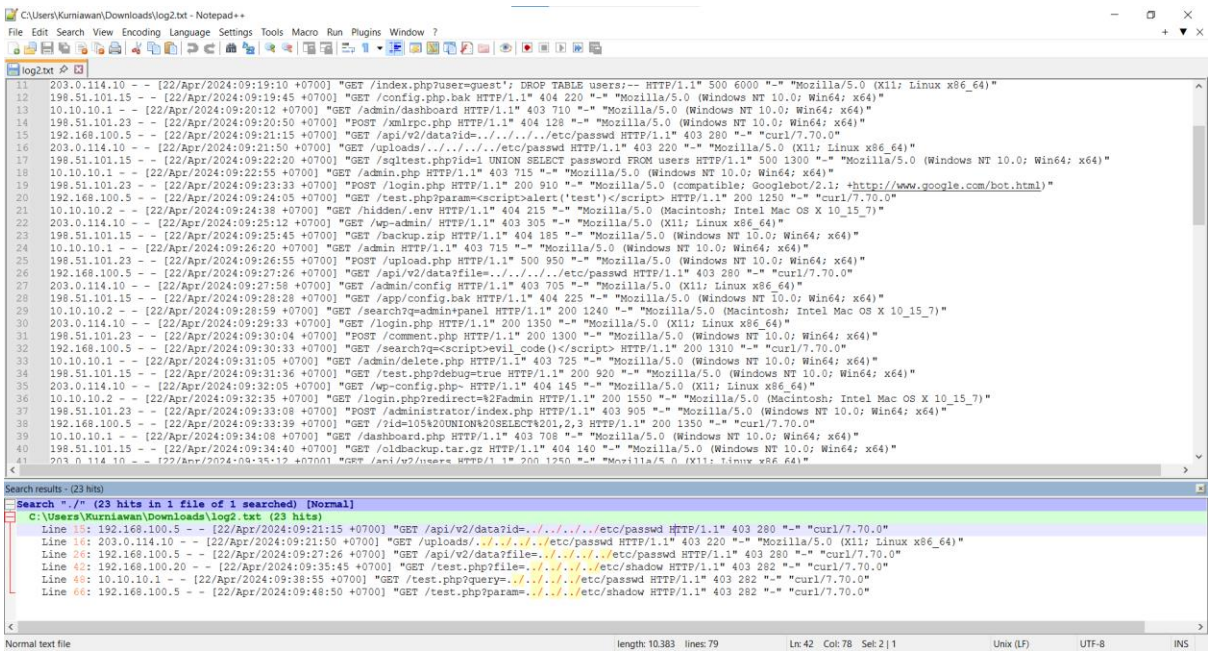
Deskripsi :

> Ada upaya eksploitasi menggunakan path traversal dalam permintaan ke endpoint API. Apa parameter lengkap yang digunakan penyerang?
>
> IDN_CTF{jawaban}
>
> Author: Rafly Permana

Lampiran : log2.txt

Solusi :

- **Path traversal** biasanya path yang mengandung path **..** , // , **../../../** .
- Menggunakan fitur **find** untuk mencari **pattern path traversal**.
- Ditemukan beberapa line yang mengandung **pattern** path traversal dan yang paling **sensitive** adalah **../../../../etc/passwd**.



Flag : IDN_CTF{../../../../etc/passwd}

Log Analysis 8

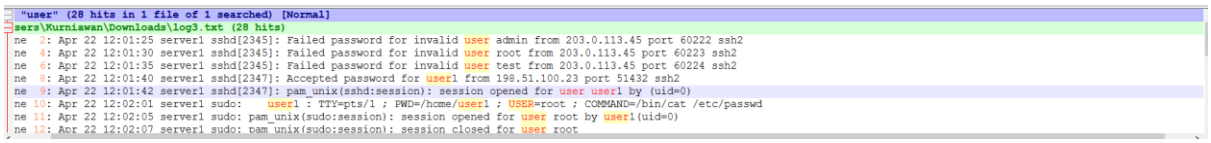
Deskripsi :

> Pada tanggal 22 April, salah satu user berhasil mendapatkan akses root melalui SSH. Berdasarkan log, berikan IP address asli dari user tersebut.
>
> IDN_CTF{jawaban}
>
> Author: Rafly Permana

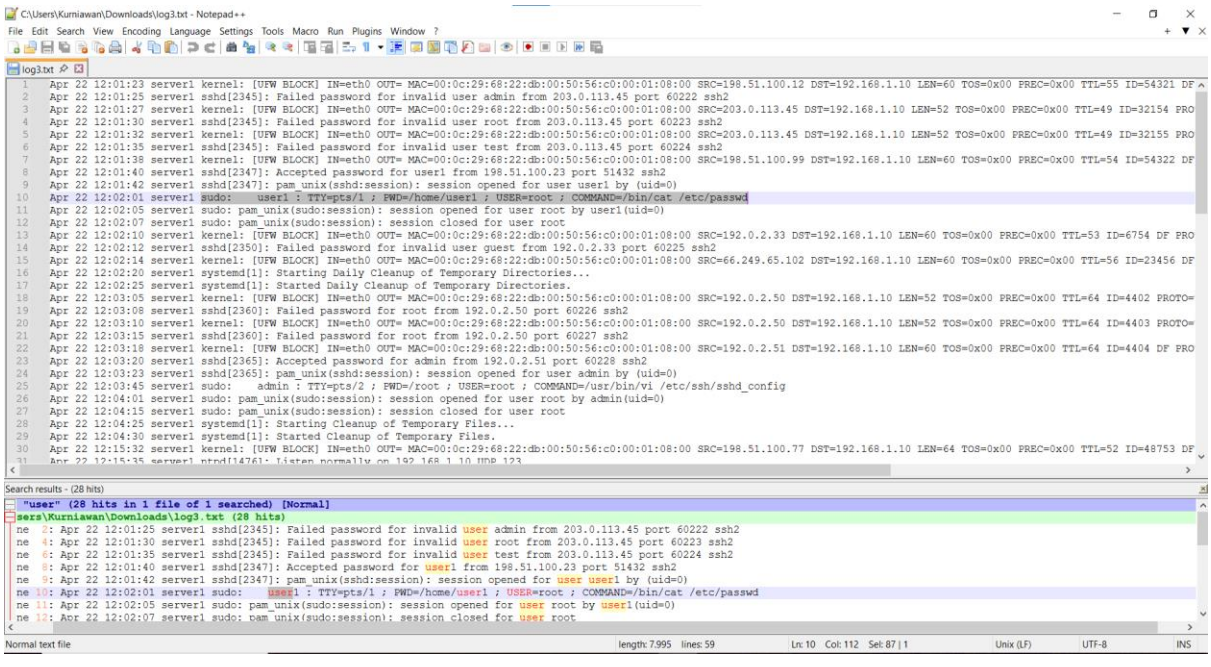
Lampiran : log3.txt

Solusi :

- Gunakan fitur find untuk mencari keyword " **USER** ".



- Di line yang berisi **user1** , terdapat informasi bahwa **user1** mendapatkan akses **root**.
- IP Adress **user1** adalah : **198.51.100.23**



Flag : IDN_CTF{198.51.100.23}

Log Analysis 9

Deskripsi :

Pengguna manakah yang berhasil mendapatkan akses root, mencoba membaca file shadow menggunakan curl, namun ditolak oleh AppArmor? Sebutkan IP-nya dan hash publik RSA yang digunakan saat login.

pisahkan jawaban dengan koma (,) Contoh: user,10.10.10.9,BASE64:Jinasidn023nnandd

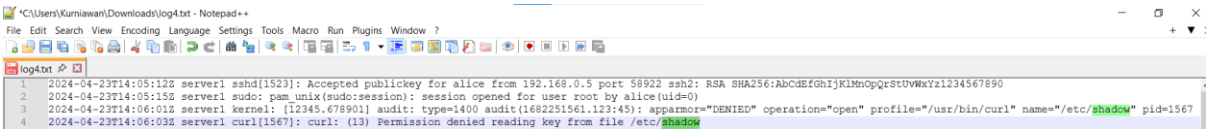
IDN_CTF{jawaban}

Author: Rafly Permana

Lampiran : log4.txt

Solusi :

- Cari baris yang mengandung " **shadow** ".



- Dari baris yang ditemukan. mendapatkan informasi bahwa ada yang mencoba membaca file **shadow** menggunakan **curl** namun ditolak oleh **AppArmor**.
- sebelum baris itu hanya user **Alice** saja yang tercatat **login**. Dan pada baris 2, user **alice** mendapatkan akses **root**.

Flag : IDN_CTF{alice,192.168.0.5,SHA256:AbCdEfGhIjKlMnOpQrStUvWxYz1234567890}