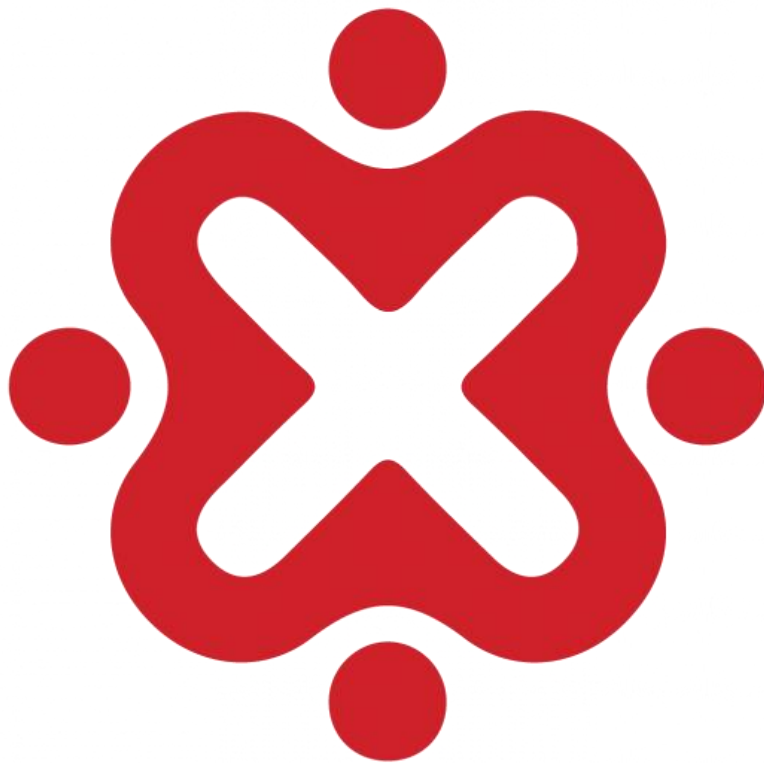




**ID-Networkers**  
Indonesian IT Expert Factory

**Raihan Putra Kurniawan**

Any progress is better than none



**ID-Networkers**  
Indonesian IT Expert Factory



Summary Findings Each Category .....	4
<b>Detail Challenge Solved .....</b>	<b>5</b>
<b>Others.....</b>	<b>5</b>
User Guide.....	5
<b>Cryptography .....</b>	<b>6</b>
Rot1Aoka .....	6
Pramuka .....	7
<b>USB Forensic .....</b>	<b>7</b>
USB Forensic 1 .....	7
USB Forensic 2.....	8
USB Forensic 3.....	9
USB Forensic 4.....	10
USB Forensic 5.....	11
USB Forensic 6.....	11
USB Forensic 7 .....	12
USB Forensic 8.....	13
<b>Windows Forensic.....</b>	<b>14</b>
Windows Forensic 1 .....	14
Windows Forensic 2.....	15
Windows Forensic 3.....	15
Windows Forensic 4.....	17
Windows Forensic 5.....	17
Windows Forensic 6.....	18
Windows Forensic 7.....	19
Windows Forensic 8.....	20
<b>Log Analysis .....</b>	<b>21</b>
Log Analysis 1 .....	21
Log Analysis 2 .....	22
Log Analysis 3 .....	23
Log Analysis 4 .....	24



Log Analysis 5 .....	25
Log Analysis 6 .....	26
Log Analysis 7 .....	27
Log Analysis 8 .....	28
Log Analysis 9 .....	29



## 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

Raihan Putra Kurniawan

280



## Detail Challenge Solved

Others

### User Guide

Deskripsi :

FLAG

Lampiran : none

Solusi :

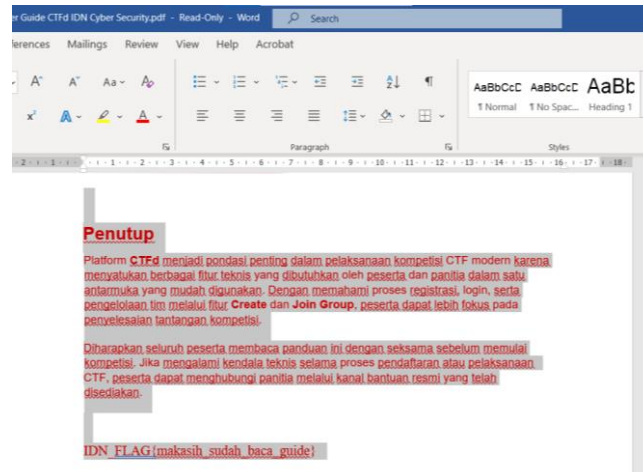
- Membaca seluruh **User Guide**.
- Menemukan format **flag**, lalu coba submit flag Namun **inccorect**.

misalnya `IDN_FLAG{example_flag}` ATAU `IDN_CTF{example_flag}`.

- 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.

Diharapkan seluruh peserta membaca panduan ini dengan seksama sebelum memulai kompetisi. Jika mengalami kendala teknis selama proses pendaftaran atau pelaksanaan CTF, peserta dapat menghubungi panitia melalui kanal bantuan resmi yang telah disediakan.

- 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 Fatty

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 Fatty**

[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 ?



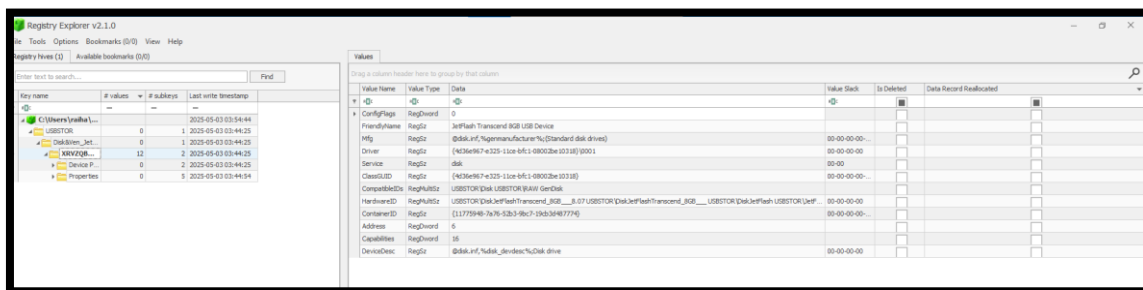
format flag : IDN\_FLAG{Nama\_Device\_Ukuran\_USB\_Device}

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 !

(Filanya ada di pertanyaan pertama)

ClassGUID Pada USB Hacker ?

format flag : IDN\_FLAG{Jawaban yang disoal}

Auhtor: Aditya Firman NugrohoAuthor: Rafly Permana

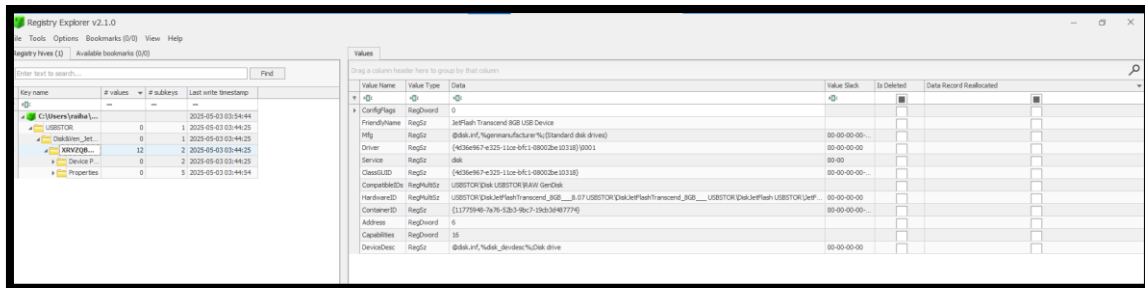




Lampiran : None

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 !

(Filanya 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**}.





## USB Forensic 5

Deskripsi :

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

(Filanya 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 !

(Filanya 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”

Registry hives (5)				Available bookmarks (29/0)		
Enter text to search...				Find		
Key name	# values	# subkeys	Last write timestamp	Values		
WsmSvc	0	1	2025-05-03 03:25	Recent documents		
wfs	0	5	2025-05-03 03:25	Drag a column header here to group by that column		
Windows	0	7	2025-05-03 03:25	Extension	Value Name	Target Name
DWM	12	0	2025-05-03 03:25	*.*	*.*	*.*
AssignedAccessConfiguration	0	0	2025-05-03 03:25	.txt	0	4f624842b5984-8308848.txt
CurrentVersion	0	57	2025-05-03 04:00			
ApplicationAssociationToasts	321	0	2025-05-03 03:46			
ContentDeliveryManager	14	6	2025-05-03 03:46			
Internet Settings	10	10	2025-05-03 03:30			
Search	13	2	2025-05-03 03:55			
Explorer	12	38	2025-05-03 03:46			
Shell Folders	31	0	2025-05-03 03:25			
Advanced	26	0	2025-05-03 03:30			
User Shell Folders	20	0	2025-05-03 03:25			
Taskband	4	1	2025-05-03 03:30			
Accent	3	0	2025-05-03 03:25			
RecentDocs	3	2	2025-05-03 03:46			
.txt	2	0	2025-05-03 03:46			

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 ?

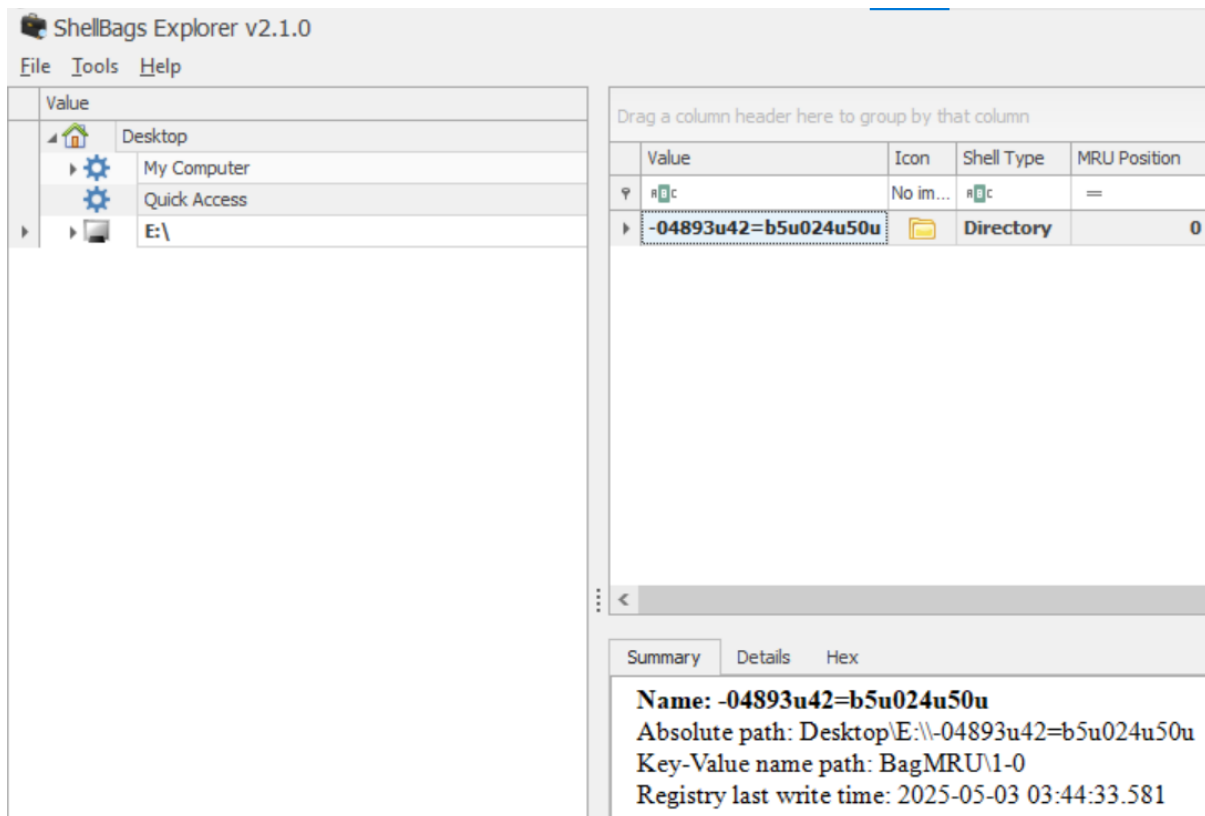
format flag : IDN\_FLAG{Jawaban yang disoal} example : \*:\directory

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 !

(Filanya 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	Link Name	Mr Position	Opened On
c	c	c	c	=	=
.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 lainnya !!

(Filanya ada di pertanyaan pertama)

Nama file yang menyimpan credential ?

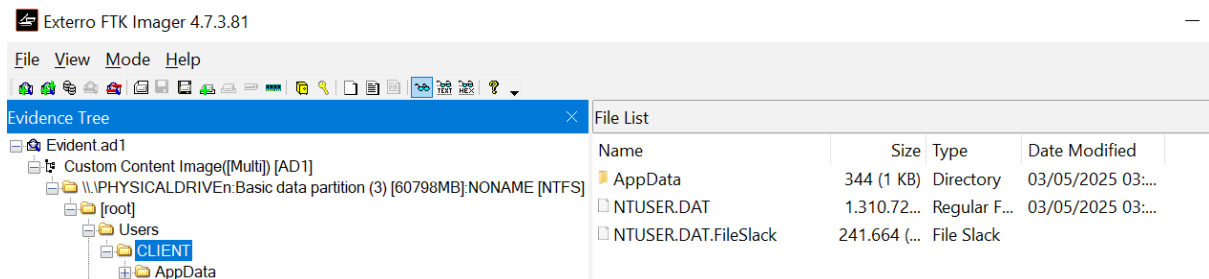
format flag : IDN\_FLAG{Jawaban yang disoal} example : xxxxxxxx\_xxx.xxx

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	323
ApplicationAssociationToasts	14	13
ContentDeliveryManager	13	12
Search	12	31
Explorer	26	20
Shell Folders	11	6
Advanced	4	
User Shell Folders		
RecentDocs		
Folder		
.txt		

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 lainnya !!

(Filanya 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 lainnya !!



(Filanya ada di pertanyaan pertama)

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

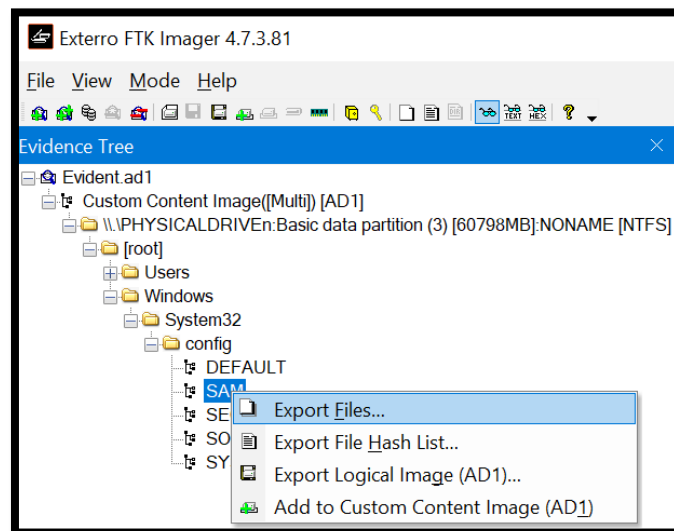
format flag : IDN\_FLAG{Jawaban yang disoal}

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”.

Key name	# values	# subkeys	Valid	User Id	Invali	Total	Created On	Last...	Last...	Last...	Expi...	User Name
C:\Users\raihia\OneDrive\Dokumen\ctf\INTUSER.DAT	2	0										
Unassociated deleted values	2	0										
ROOT	0	10										
C:\Users\raihia\OneDrive\Dokumen\ctf\SECURITY	0	10										
ROOT	0	3										
C:\Users\raihia\OneDrive\Dokumen\ctf\SAM	0	1										
ROOT	0	1										
SAM	2	3										
Domains	1	2										
Builtin	3	3										
Aliases	1	2										
Groups	1	1										
Names	1	0										
Users	1	1										
Names	1	0										
Account	2	3										
Aliases	1	2										
Groups	1	2										
Users	1	8										

Valid	User Id	Invali	Total	Created On	Last...	Last...	Last...	Expi...	User Name
<input checked="" type="checkbox"/>	1001	0	3	2025-05-03 03:29:00	202...				CLIENT
<input checked="" type="checkbox"/>	1002	0	0	2025-05-03 07:04:43	202...				Geraldin
<input checked="" type="checkbox"/>	1003	0	0	2025-05-03 07:05:03	202...				Jon
Total rows: 7									
Type viewer Binary viewer									

Flag : IDN\_FLAG{Geraldin}





## Windows Forensic 4

Deskripsi :

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

(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”.

Valid	User Id	Inval.	Total	Created On	Last.	Last.	Last.	Expl.	User Name
<input checked="" type="checkbox"/>	1001	0	3	2025-05-03 03:29:00	202...				CLIENT
<input checked="" type="checkbox"/>	1002	0	0	2025-05-03 07:04:43	202...				Geraldin
<input checked="" type="checkbox"/>	1003	0	0	2025-05-03 07:05:03	202...				Jon

Flag : IDN\_FLAG{ Jon }

## Windows Forensic 5

Deskripsi :

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

(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
▼	<input type="checkbox"/>	=	=	=	=	=	=	=	=	hgc	hgc	hgc	hgc
	<input checked="" type="checkbox"/>	504	0	0	2025-05-03 03:27:38		202...			WDAGUtilityA ccount			
	<input checked="" type="checkbox"/>	1001	0	3	2025-05-03 03:29:00	202...				CLIENT			Administrato rs
▶	<input checked="" type="checkbox"/>	1002	0	0	2025-05-03 07:04:43		202...			Geraldin			Administrato rs, Users
	<input checked="" type="checkbox"/>	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 lainnya !!

(Filanya 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...
<input type="checkbox"/>	=	=	=	=	=	=	=	=	ABC
<input checked="" type="checkbox"/>	1001	0	3	2025...	2025-05-03 03:42:49				CLIENT
<input checked="" type="checkbox"/>	1002	0	0	2025...		202...			Geraldin
<input checked="" type="checkbox"/>	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 lainnya !!

(Filanya 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...
=	=	=	=	=	=	=	=	A B C
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 lainnya !!

(Filanya 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 “.

Key name	# values	# subkeys	Group Name	Comment	Users
C:\Users\raisha (OneDrive\Documents)\cf\USER.DAT	2	0	Administrators	Administrators have complete and unrestricted access to the computer (domain)	S-1-5-21-2412307826-2007293762-2764304457-500, S-1-5-21-2412307826-2007293762-2764304457-501, S-1-5-21-2412307826-2007293762-2764304457-502
ROOT	0	10	Users	Users are prevented from making accidental or intentional system-wide changes and can run most applications	S-1-5-4, S-1-5-11, S-1-5-21-2412307826-2007293762-2764304457-1002, S-1-5-21-2412307826-2007293762-2764304457-1003
C:\Users\raisha (OneDrive\Documents)\cf\SECURITY	0	3	Guests	Guests have the same access as members of the Users group by default, except for the Guest account which is further restricted	S-1-5-21-2412307826-2007293762-2764304457-501
ROOT	0	3	Power Users	Power Users are included for backwards compatibility and possess limited administrative powers	
C:\Users\raisha (OneDrive\Documents)\cf\SAM	0	1	Backup Operators	Backup Operators can override security restrictions for the sole purpose of backing up or restoring files	
ROOT	2	3	Replicator	Supports file replication in a domain	
Domains	1	2	Remote Desktop Users	Members in this group are granted the right to logon remotely	
Builtin	3	3			
Aliases	1	21			



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...

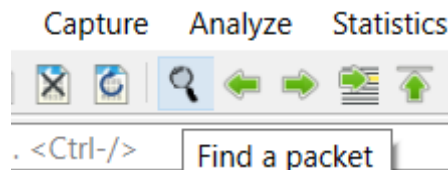
Format Flag : IDN\_CTF{jawaban}

**Author : Aditya Firman Nugroho**

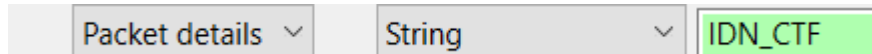
Lampiran : incident\_response\_pcapng

Solusi :

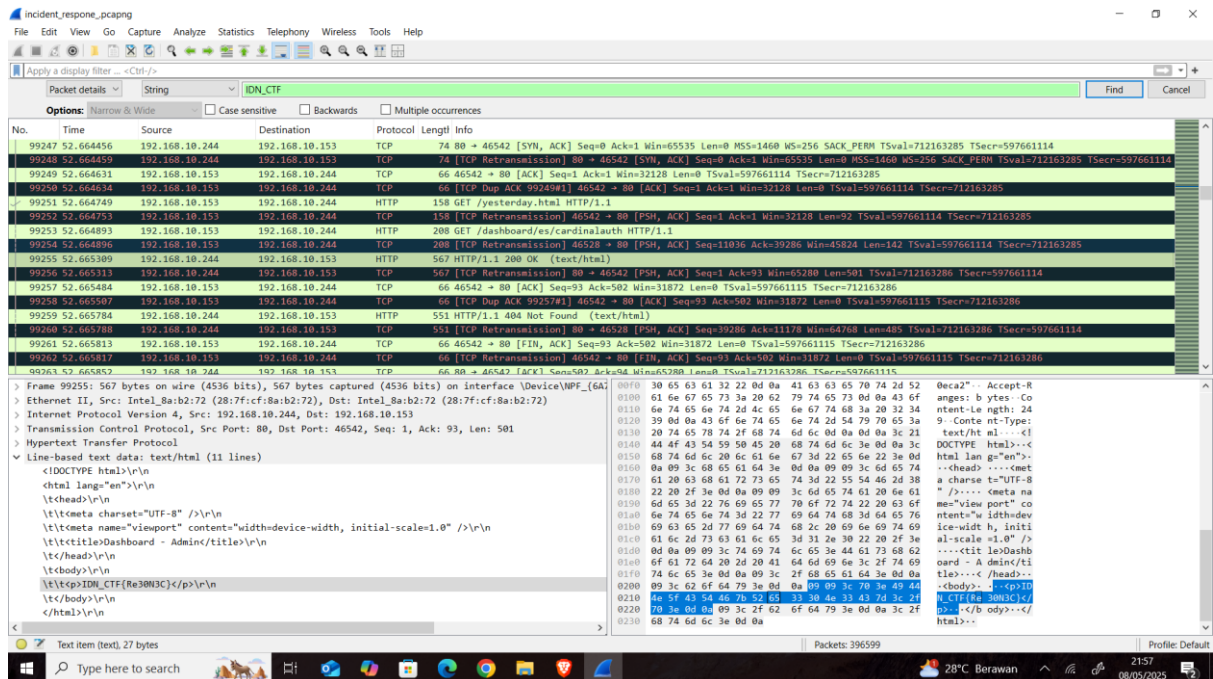
- Buka file pcap menggunakan wireshark.
- Lalu coba gunakan fitur “ **find a packet**”.



- 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 .....

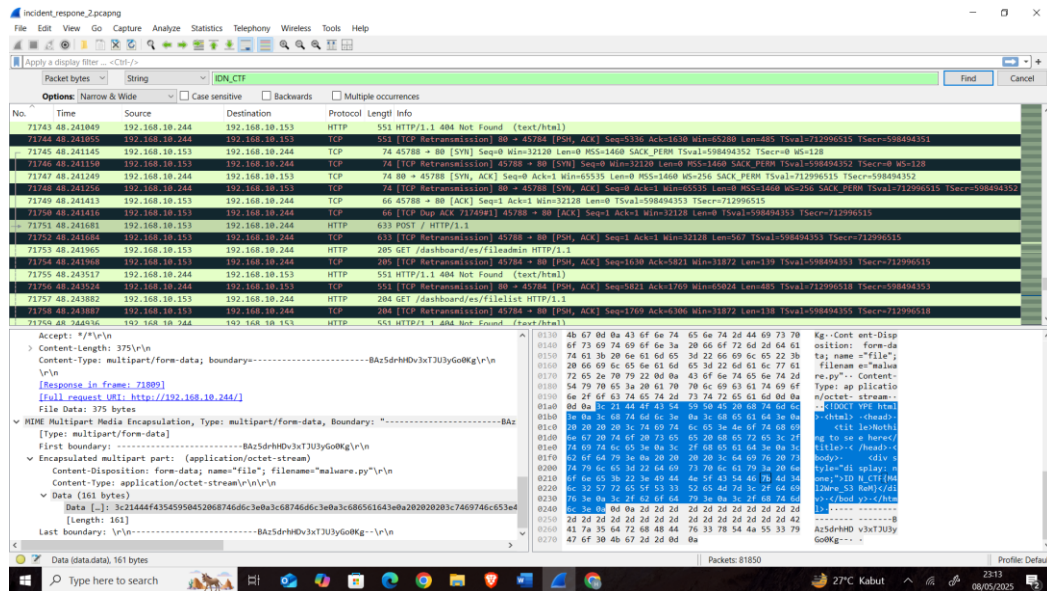
Format Flag : IDN\_CTF{jawaban}

Author : Aditya Firman Nugroho

Lampiran : [incident\\_response\\_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.









```
C:\Users\Kurniawan\Downloads\auth.log - Notepad++
File Edit Search View Encoding Language Settings Tools Macro Run Plugins Window ?
auth.log
241 Apr 27 13:04:50 test sshd[19006]: Failed password for invalid user football from 192.168.18.6 port 54508 ssh2
242 Apr 27 13:04:50 test sshd[19002]: Connection closed by invalid user 123123 192.168.18.6 port 54490 [preauth]
243 Apr 27 13:04:50 test sshd[19012]: Failed password for invalid user carlos from 192.168.18.6 port 54540 ssh2
244 Apr 27 13:04:50 test sshd[18990]: Connection closed by invalid user angel 192.168.18.6 port 54376 [preauth]
245 Apr 27 13:04:50 test sshd[19008]: Connection closed by invalid user secret 192.168.18.6 port 54516 [preauth]
246 Apr 27 13:04:50 test sshd[19012]: Connection closed by invalid user carlos 192.168.18.6 port 54540 [preauth]
247 Apr 27 13:04:50 test sshd[19003]: Connection closed by invalid user football 192.168.18.6 port 54492 [preauth]
248 Apr 27 13:04:50 test sshd[19006]: Connection closed by invalid user football 192.168.18.6 port 54508 [preauth]
249 Apr 27 13:04:50 test sshd[18995]: Connection closed by invalid user justin 192.168.18.6 port 54432 [preauth]
250 Apr 27 13:04:50 test sshd[18998]: Connection closed by invalid user justin 192.168.18.6 port 54448 [preauth]
251 Apr 27 13:04:51 test sshd[18994]: Connection closed by invalid user liverpool 192.168.18.6 port 54418 [preauth]
252 Apr 27 13:04:51 test sshd[18991]: Connection closed by invalid user jordan 192.168.18.6 port 54388 [preauth]
253 Apr 27 13:04:51 test sshd[19010]: Connection closed by invalid user andrea 192.168.18.6 port 54530 [preauth]
254 Apr 27 13:04:51 test sshd[19000]: Connection closed by invalid user loveme 192.168.18.6 port 54456 [preauth]
255 Apr 27 13:05:06 test sshd[4810]: exited MaxStartups throttling after 00:00:27, 16 connections dropped
256 Apr 27 13:05:10 test sshd[19014]: Accepted password for ghxyss from 192.168.18.6 port 52320 ssh2
257 Apr 27 13:05:10 test sshd[19014]: pam_unix(sshd:session): session opened for user ghxyss(uid=1000) by (uid=0)
258 Apr 27 13:05:10 test systemd-logind[872]: New session 4 of user ghxyss.
259 Apr 27 13:05:16 test sshd[19072]: Received disconnect from 192.168.18.6 port 52320:11: disconnected by user
260 Apr 27 13:05:16 test sshd[19072]: Disconnected from user ghxyss 192.168.18.6 port 52320
261 Apr 27 13:05:16 test sshd[19014]: pam_unix(sshd:session): session closed for user ghxyss
```

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.

log_analysis_5.pcapng						
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help						
http.response.code != 403 && http.response.code != 404						
No.	Time	Source	Destination	Protocol	Length	Info
26092	102.202830	192.168.18.230	192.168.18.6	HTTP	647	HTTP/1.1 301 Moved Permanently (text/html)



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

log\_analysis\_5.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

No.	Time	Source	Destination	Protocol	Length	Info
17099	75.042842	192.168.18.230	192.168.18.17	FTP	60	Request: PASV
17101	75.043896	192.168.18.17	192.168.18.230	FTP	105	Response: 227 Entering Passive Mode (192,168,18,17,84,162).
17103	75.044211	192.168.18.230	192.168.18.17	FTP	68	Request: STOR malware
17113	75.045625	192.168.18.17	192.168.18.230	FTP	76	Response: 150 Ok to send data.
17119	75.046935	192.168.18.17	192.168.18.230	FTP	78	Response: 226 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"**.

```
*C:\Users\Kurniawan\Downloads\log1.txt - Notepad++
File Edit Search View Encoding Language Settings Tools Macro Run Plugins Window ?

log1.txt
1 192.168.10.15 - [21/Apr/2024:08:12:31 +0700] "GET /index.html HTTP/1.1" 200 4523 "http://example.com/" "Mozilla/5.0 (Windows NT 10.0; Win64; x64)"
2 192.168.10.20 - [21/Apr/2024:08:12:36 +0700] "POST /login.php HTTP/1.1" 302 154 "http://example.com/login" "Mozilla/5.0 (Windows NT 10.0; Win64; x64)"
3 203.0.113.101 - [21/Apr/2024:08:12:40 +0700] "GET /favicon.ico HTTP/1.1" 404 199 "-" "Mozilla/5.0 (compatible; Googlebot/2.1; http://www.google.com/bot.html)"
4 198.51.100.23 - [21/Apr/2024:08:13:12 +0700] "GET /admin HTTP/1.1" 403 721 "-" "Mozilla/5.0 (X11; Linux x86_64)"
5 10.0.0.9 - [21/Apr/2024:08:13:42 +0700] "GET /api/data?id=1234 HTTP/1.1" 200 985 "http://example.com/" "curl/7.68.0"
6 192.168.10.15 - [21/Apr/2024:08:14:05 +0700] "GET /downloads/manual.pdf HTTP/1.1" 200 253467 "http://example.com/manual" "Mozilla/5.0 (Windows NT 10.0; Win64; x64)"
7 198.51.100.45 - [21/Apr/2024:08:14:38 +0700] "POST /wp-login.php HTTP/1.1" 200 5423 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36"
8 203.0.113.101 - [21/Apr/2024:08:15:03 +0700] "GET /robots.txt HTTP/1.1" 200 68 "-" "Mozilla/5.0 (compatible; bingbot/2.0; http://www.bing.com/bingbot.htm)"
9 10.0.0.9 - [21/Apr/2024:08:15:42 +0700] "GET /search?q=test HTTP/1.1" 200 1234 "http://example.com/" "curl/7.68.0"
10 192.168.10.20 - [21/Apr/2024:08:16:10 +0700] "GET / HTTP/1.1" 200 3421 "http://example.com/" "Mozilla/5.0 (Windows NT 10.0; Win64; x64)"
11 203.0.113.101 - [21/Apr/2024:08:16:54 +0700] "GET /index.php?user=admin' OR '1'='1 HTTP/1.1" 200 5432 "-" "Mozilla/5.0 (X11; Linux x86_64)"
12 198.51.100.23 - [21/Apr/2024:08:17:22 +0700] "GET /config.php.bak HTTP/1.1" 404 213 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64)"
13 192.168.10.15 - [21/Apr/2024:08:17:50 +0700] "GET /admin/dashboard HTTP/1.1" 403 701 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64)"
14 198.51.100.45 - [21/Apr/2024:08:18:19 +0700] "POST /xmlrpc.php HTTP/1.1" 404 123 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64)"
15 10.0.0.9 - [21/Apr/2024:08:18:50 +0700] "GET /api/data?id=../etc/passwd HTTP/1.1" 403 279 "-" "curl/7.68.0"
16 203.0.113.101 - [21/Apr/2024:08:19:15 +0700] "GET /uploads/../../../../etc/passwd HTTP/1.1" 403 213 "-" "Mozilla/5.0 (X11; Linux x86_64)"
17 198.51.100.23 - [21/Apr/2024:08:19:45 +0700] "GET /ring.php?id=1 UNION SELECT password FROM users HTTP/1.1" 500 1234 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64)"
18 192.168.10.15 - [21/Apr/2024:08:20:13 +0700] "POST /login.php HTTP/1.1" 403 710 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64)"
19 198.51.100.45 - [21/Apr/2024:08:20:47 +0700] "POST /login.php HTTP/1.1" 200 900 "-" "Mozilla/5.0 (compatible; Googlebot/2.1; http://www.google.com/bot.html)"
20 10.0.0.9 - [21/Apr/2024:08:21:18 +0700] "GET /test.php?param=<script>alert('xss')</script> HTTP/1.1" 200 1234 "-" "curl/7.68.0"
21 192.168.10.20 - [21/Apr/2024:08:21:44 +0700] "GET /hidden/.env HTTP/1.1" 404 212 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64)"
22 203.0.113.101 - [21/Apr/2024:08:22:09 +0700] "GET /wp-admin/ HTTP/1.1" 403 300 "-" "Mozilla/5.0 (X11; Linux x86_64)"
23 198.51.100.23 - [21/Apr/2024:08:22:40 +0700] "GET /backup.zip HTTP/1.1" 404 180 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64)"
24 192.168.10.15 - [21/Apr/2024:08:23:12 +0700] "GET /admin HTTP/1.1" 403 710 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64)"
25 198.51.100.45 - [21/Apr/2024:08:23:42 +0700] "POST /upload.php HTTP/1.1" 500 934 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64)"
26 10.0.0.9 - [21/Apr/2024:08:24:10 +0700] "GET /api/data?file=../../../../etc/passwd HTTP/1.1" 403 278 "-" "curl/7.68.0"
27 203.0.113.101 - [21/Apr/2024:08:24:44 +0700] "GET /admin/config HTTP/1.1" 403 700 "-" "Mozilla/5.0 (X11; Linux x86_64)"
28 198.51.100.23 - [21/Apr/2024:08:25:15 +0700] "GET /app/config.bak HTTP/1.1" 404 221 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64)"
29 192.168.10.20 - [21/Apr/2024:08:25:48 +0700] "GET /search?q=adminpanel HTTP/1.1" 200 1234 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64)"
30 203.0.113.101 - [21/Apr/2024:08:26:11 +0700] "GET /login.php HTTP/1.1" 200 1342 "-" "Mozilla/5.0 (X11; Linux x86_64)"
31 198.51.100.45 - [21/Apr/2024:08:26:45 +0700] "POST /comment.php HTTP/1.1" 200 1210 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64)"
32 10.0.0.9 - [21/Apr/2024:08:27:12 +0700] "GET /search?q=<script>eval(code())</script> HTTP/1.1" 200 1300 "-" "curl/7.68.0"
33 192.168.10.15 - [21/Apr/2024:08:27:45 +0700] "GET /admin/delete.php HTTP/1.1" 403 720 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64)"
34 198.51.100.23 - [21/Apr/2024:08:28:15 +0700] "GET /test.php?debug=true HTTP/1.1" 200 910 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64)"

Search results - (5 hits)
Search "500" (5 hits in 1 file of 1 searched) [Normal: Word]
Line 1: 198.51.100.23 - [21/Apr/2024:08:19:45 +0700] "GET /ring.php?id=1 UNION SELECT password FROM users HTTP/1.1" 500 1234 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64)"
Line 25: 198.51.100.45 - [21/Apr/2024:08:23:42 +0700] "POST /upload.php HTTP/1.1" 500 934 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64)"
Line 47: 198.51.100.23 - [21/Apr/2024:08:34:50 +0700] "GET /search?q=42743bDROF+TABLE+users43b-- HTTP/1.1" 500 1234 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64)"
Line 51: 198.51.100.45 - [21/Apr/2024:08:36:38 +0700] "POST /upload.php HTTP/1.1" 500 940 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64)"
Line 96: 198.51.100.45 - [21/Apr/2024:08:40:12 +0700] "GET /index.php?id=105 UNION ALL SELECT username, password FROM users-- HTTP/1.1" 500 1543 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64)"
```



- 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**.

```
11 203.0.114.10 - - [22/Apr/2024:09:19:10 +0700] "GET /index.php?user=guest" DROP TABLE users;-- HTTP/1.1" 500 6000 "-" "Mozilla/5.0 (X11; Linux x86_64)"
12 198.51.101.15 - - [22/Apr/2024:09:19:45 +0700] "GET /config.php.bak HTTP/1.1" 404 220 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64)"
13 10.10.10.1 - - [22/Apr/2024:09:20:12 +0700] "GET /admin/dashboard HTTP/1.1" 403 710 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64)"
14 198.51.101.23 - - [22/Apr/2024:09:20:50 +0700] "POST /xmlrpc.php HTTP/1.1" 404 128 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64)"
15 192.168.100.5 - - [22/Apr/2024:09:21:15 +0700] "GET /api/v2/data?id=../../..../etc/passwd HTTP/1.1" 403 280 "-" "curl/7.70.0"
16 203.0.114.10 - - [22/Apr/2024:09:21:50 +0700] "GET /uploads/../../..../etc/passwd HTTP/1.1" 403 220 "-" "Mozilla/5.0 (X11; Linux x86_64)"
17 198.51.101.15 - - [22/Apr/2024:09:22:20 +0700] "GET /sqltest.php?id=1 UNION SELECT password FROM users HTTP/1.1" 500 1300 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64)"
18 10.10.10.1 - - [22/Apr/2024:09:22:55 +0700] "GET /admin.php HTTP/1.1" 403 715 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64)"
19 198.51.101.23 - - [22/Apr/2024:09:23:33 +0700] "POST /login.php HTTP/1.1" 200 910 "-" "Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)"
20 192.168.100.5 - - [22/Apr/2024:09:24:05 +0700] "GET /test.php?param=<script>alert('test')</script> HTTP/1.1" 200 1250 "-" "curl/7.70.0"
21 10.10.10.2 - - [22/Apr/2024:09:24:38 +0700] "GET /hidden/.env HTTP/1.1" 404 215 "-" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7)"
22 203.0.114.10 - - [22/Apr/2024:09:25:12 +0700] "GET /wp-admin/ HTTP/1.1" 403 305 "-" "Mozilla/5.0 (X11; Linux x86_64)"
23 198.51.101.15 - - [22/Apr/2024:09:25:45 +0700] "GET /backup.zip HTTP/1.1" 404 185 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64)"
24 10.10.10.1 - - [22/Apr/2024:09:26:20 +0700] "GET /admin HTTP/1.1" 403 715 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64)"
25 198.51.101.23 - - [22/Apr/2024:09:26:55 +0700] "POST /upload.php HTTP/1.1" 500 950 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64)"
26 192.168.100.5 - - [22/Apr/2024:09:27:26 +0700] "GET /api/v2/data?file=../../..../etc/passwd HTTP/1.1" 403 280 "-" "curl/7.70.0"
27 203.0.114.10 - - [22/Apr/2024:09:27:58 +0700] "GET /admin/config HTTP/1.1" 403 705 "-" "Mozilla/5.0 (X11; Linux x86_64)"
28 198.51.101.15 - - [22/Apr/2024:09:28:28 +0700] "GET /app/config.bak HTTP/1.1" 404 225 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64)"
29 10.10.10.2 - - [22/Apr/2024:09:28:59 +0700] "GET /search?q=admin+panel HTTP/1.1" 200 1240 "-" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7)"
30 203.0.114.10 - - [22/Apr/2024:09:29:33 +0700] "GET /login.php HTTP/1.1" 200 1350 "-" "Mozilla/5.0 (X11; Linux x86_64)"
31 198.51.101.23 - - [22/Apr/2024:09:30:04 +0700] "POST /comment.php HTTP/1.1" 200 1300 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64)"
32 192.168.100.5 - - [22/Apr/2024:09:30:33 +0700] "GET /search?q=<script>eval(code)(</script> HTTP/1.1" 200 1310 "-" "curl/7.70.0"
33 10.10.10.1 - - [22/Apr/2024:09:31:05 +0700] "GET /admin/delete.php HTTP/1.1" 403 725 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64)"
34 198.51.101.15 - - [22/Apr/2024:09:31:36 +0700] "GET /test.php?debug=true HTTP/1.1" 200 920 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64)"
35 203.0.114.10 - - [22/Apr/2024:09:32:05 +0700] "GET /wp-config.php- HTTP/1.1" 404 145 "-" "Mozilla/5.0 (X11; Linux x86_64)"
36 10.10.10.2 - - [22/Apr/2024:09:32:35 +0700] "GET /login.php?redirect=2Fadmin HTTP/1.1" 200 1550 "-" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7)"
37 198.51.101.23 - - [22/Apr/2024:09:33:08 +0700] "POST /administrator/index.php HTTP/1.1" 403 905 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64)"
38 192.168.100.5 - - [22/Apr/2024:09:33:39 +0700] "GET /?id=105420UNION%20SELECT%201,2,3 HTTP/1.1" 200 1350 "-" "curl/7.70.0"
39 10.10.10.1 - - [22/Apr/2024:09:34:08 +0700] "GET /dashboard.php HTTP/1.1" 403 708 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64)"
40 198.51.101.15 - - [22/Apr/2024:09:34:40 +0700] "GET /oldbackup.tar.gz HTTP/1.1" 404 140 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64)"
41 203.0.114.10 - - [22/Apr/2024:09:35:12 +0700] "GET /api/v2/users HTTP/1.1" 200 1250 "-" "Mozilla/5.0 (X11; Linux x86_64)"
```





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 “.

```
"user" (28 hits in 1 file of 1 searched) [Normal]
-----
C:\Users\Kurniawan\Downloads\log3.txt (28 hits)
ne 2: Apr 22 12:01:25 server1 sshd[2345]: Failed password for invalid user admin from 203.0.113.45 port 60222 ssh2
ne 4: Apr 22 12:01:30 server1 sshd[2345]: Failed password for invalid user root from 203.0.113.45 port 60223 ssh2
ne 6: Apr 22 12:01:35 server1 sshd[2345]: Failed password for invalid user test from 203.0.113.45 port 60224 ssh2
ne 8: Apr 22 12:01:40 server1 sshd[2347]: Accepted password for user1 from 198.51.100.23 port 51432 ssh2
ne 9: Apr 22 12:01:42 server1 sshd[2347]: pam_unix(sshd:session): session opened for user user1 by (uid=0)
ne 10: Apr 22 12:02:01 server1 sudo: user1 : TTY=pts/1 ; PWD=/home/user1 ; USER=root ; COMMAND=/bin/cat /etc/passwd
ne 11: Apr 22 12:02:05 server1 sudo: pam_unix(sudo:session): session opened for user user1 by user1(uid=0)
ne 12: Apr 22 12:02:07 server1 sudo: pam_unix(sudo:session): session closed for user root
```

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

```
C:\Users\Kurniawan\Downloads\log3.txt - Notepad++
File Edit Search View Encoding Language Settings Tools Macro Run Plugins Window ?
log3.txt
1 Apr 22 12:01:23 server1 kernel: [UFW BLOCK] IN=eth0 OUT= MAC=00:0c:29:68:22:db:00:50:56:c0:00:01:08:00 SRC=198.51.100.12 DST=192.168.1.10 LEN=60 TOS=0x00 PREC=0x00 TTL=55 ID=54321 DF PRO
2 Apr 22 12:01:25 server1 sshd[2345]: Failed password for invalid user admin from 203.0.113.45 port 60222 ssh2
3 Apr 22 12:01:27 server1 kernel: [UFW BLOCK] IN=eth0 OUT= MAC=00:0c:29:68:22:db:00:50:56:c0:00:01:08:00 SRC=203.0.113.45 DST=192.168.1.10 LEN=52 TOS=0x00 PREC=0x00 TTL=49 ID=32154 PRO
4 Apr 22 12:01:30 server1 sshd[2345]: Failed password for invalid user root from 203.0.113.45 port 60223 ssh2
5 Apr 22 12:01:32 server1 kernel: [UFW BLOCK] IN=eth0 OUT= MAC=00:0c:29:68:22:db:00:50:56:c0:00:01:08:00 SRC=203.0.113.45 DST=192.168.1.10 LEN=52 TOS=0x00 PREC=0x00 TTL=49 ID=32155 PRO
6 Apr 22 12:01:35 server1 sshd[2345]: Failed password for invalid user test from 203.0.113.45 port 60224 ssh2
7 Apr 22 12:01:38 server1 kernel: [UFW BLOCK] IN=eth0 OUT= MAC=00:0c:29:68:22:db:00:50:56:c0:00:01:08:00 SRC=198.51.100.99 DST=192.168.1.10 LEN=60 TOS=0x00 PREC=0x00 TTL=54 ID=54322 DF
8 Apr 22 12:01:40 server1 sshd[2347]: Accepted password for user1 from 198.51.100.23 port 51432 ssh2
9 Apr 22 12:01:42 server1 sshd[2347]: pam_unix(sshd:session): session opened for user user1 by (uid=0)
10 Apr 22 12:02:01 server1 sudo: user1 : TTY=pts/1 ; PWD=/home/user1 ; USER=root ; COMMAND=/bin/cat /etc/passwd
11 Apr 22 12:02:05 server1 sudo: pam_unix(sudo:session): session opened for user user1 by user1(uid=0)
12 Apr 22 12:02:07 server1 sudo: pam_unix(sudo:session): session closed for user root
13 Apr 22 12:02:10 server1 kernel: [UFW BLOCK] IN=eth0 OUT= MAC=00:0c:29:68:22:db:00:50:56:c0:00:01:08:00 SRC=192.0.2.33 DST=192.168.1.10 LEN=60 TOS=0x00 PREC=0x00 TTL=53 ID=6754 DF PRO
14 Apr 22 12:02:12 server1 sshd[2350]: Failed password for invalid user guest from 192.0.2.33 port 60225 ssh2
15 Apr 22 12:02:14 server1 kernel: [UFW BLOCK] IN=eth0 OUT= MAC=00:0c:29:68:22:db:00:50:56:c0:00:01:08:00 SRC=66.249.65.102 DST=192.168.1.10 LEN=60 TOS=0x00 PREC=0x00 TTL=56 ID=23456 DF
16 Apr 22 12:02:20 server1 systemd[1]: Starting Daily Cleanup of Temporary Directories...
17 Apr 22 12:02:25 server1 systemd[1]: Started Daily Cleanup of Temporary Directories.
18 Apr 22 12:03:05 server1 kernel: [UFW BLOCK] IN=eth0 OUT= MAC=00:0c:29:68:22:db:00:50:56:c0:00:01:08:00 SRC=192.0.2.50 DST=192.168.1.10 LEN=52 TOS=0x00 PREC=0x00 TTL=64 ID=4402 PROTO=
19 Apr 22 12:03:08 server1 sshd[2360]: Failed password for root from 192.0.2.50 port 60226 ssh2
20 Apr 22 12:03:10 server1 kernel: [UFW BLOCK] IN=eth0 OUT= MAC=00:0c:29:68:22:db:00:50:56:c0:00:01:08:00 SRC=192.0.2.50 DST=192.168.1.10 LEN=52 TOS=0x00 PREC=0x00 TTL=64 ID=4403 PROTO=
21 Apr 22 12:03:15 server1 sshd[2360]: Failed password for root from 192.0.2.50 port 60227 ssh2
22 Apr 22 12:03:18 server1 kernel: [UFW BLOCK] IN=eth0 OUT= MAC=00:0c:29:68:22:db:00:50:56:c0:00:01:08:00 SRC=192.0.2.51 DST=192.168.1.10 LEN=60 TOS=0x00 PREC=0x00 TTL=64 ID=4404 DF PRO
23 Apr 22 12:03:20 server1 sshd[2365]: Accepted password for admin from 192.0.2.51 port 60228 ssh2
24 Apr 22 12:03:23 server1 sshd[2365]: pam_unix(sshd:session): session opened for user admin by (uid=0)
25 Apr 22 12:03:45 server1 sudo: admin : TTY=pts/2 ; PWD=/root ; USER=root ; COMMAND=/usr/bin/vi /etc/ssh/sshd_config
26 Apr 22 12:04:01 server1 sudo: pam_unix(sudo:session): session opened for user root by admin(uid=0)
27 Apr 22 12:04:15 server1 sudo: pam_unix(sudo:session): session closed for user root
28 Apr 22 12:04:25 server1 systemd[1]: Starting Cleanup of Temporary Files...
29 Apr 22 12:04:30 server1 systemd[1]: Started Cleanup of Temporary Files.
30 Apr 22 12:15:32 server1 kernel: [UFW BLOCK] IN=eth0 OUT= MAC=00:0c:29:68:22:db:00:50:56:c0:00:01:08:00 SRC=198.51.100.77 DST=192.168.1.10 LEN=64 TOS=0x00 PREC=0x00 TTL=52 ID=48753 DF
31 Apr 22 12:15:35 server1 nrd[1476]: listen normally on 192.168.1.10 UDP 123
Search results - (28 hits)
-----
"user" (28 hits in 1 file of 1 searched) [Normal]
-----
C:\Users\Kurniawan\Downloads\log3.txt (28 hits)
ne 2: Apr 22 12:01:25 server1 sshd[2345]: Failed password for invalid user admin from 203.0.113.45 port 60222 ssh2
ne 4: Apr 22 12:01:30 server1 sshd[2345]: Failed password for invalid user root from 203.0.113.45 port 60223 ssh2
ne 6: Apr 22 12:01:35 server1 sshd[2345]: Failed password for invalid user test from 203.0.113.45 port 60224 ssh2
ne 8: Apr 22 12:01:40 server1 sshd[2347]: Accepted password for user1 from 198.51.100.23 port 51432 ssh2
ne 9: Apr 22 12:01:42 server1 sshd[2347]: pam_unix(sshd:session): session opened for user user1 by (uid=0)
ne 10: Apr 22 12:02:01 server1 sudo: user1 : TTY=pts/1 ; PWD=/home/user1 ; USER=root ; COMMAND=/bin/cat /etc/passwd
ne 11: Apr 22 12:02:05 server1 sudo: pam_unix(sudo:session): session opened for user user1 by user1(uid=0)
ne 12: Apr 22 12:02:07 server1 sudo: pam_unix(sudo:session): session closed for user root
```

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** “.

```
*C:\Users\Kurniawan\Downloads\log4.txt - Notepad++
File Edit Search View Encoding Language Settings Tools Macro Run Plugins Window ?
log4.txt
1 2024-04-23T14:05:12Z server1 sshd[1523]: Accepted publickey for alice from 192.168.0.5 port 58922 ssh2: RSA SHA256:AbCdEfGhIjKlMnOpQrStUvWxYz1234567890
2 2024-04-23T14:05:15Z server1 sudo: pam_unix(sudo:session): session opened for user root by alice(uid=0)
3 2024-04-23T14:06:01Z server1 kernel: [12345.678901] audit: type=1400 audit(1682251561.123:45): apparmor="DENIED" operation="open" profile="/usr/bin/curl" name="/etc/shadow" pid=1567
4 2024-04-23T14:06:03Z server1 curl[1567]: curl: (13) Permission denied reading key from file /etc/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}