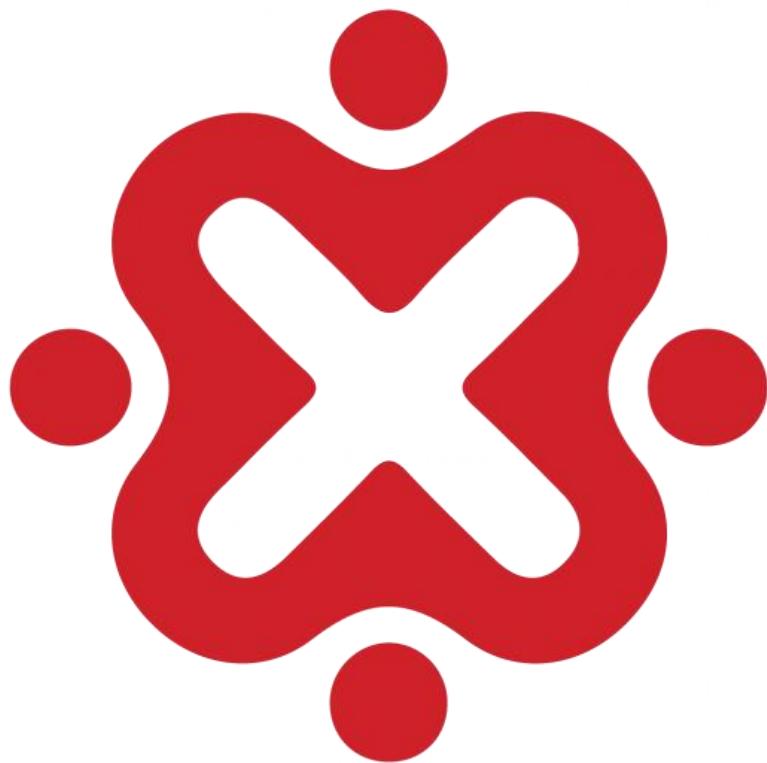




Depok Cybersec

Any progress is better than none



ID-Networkers
Indonesian IT Expert Factory



Introduction Team	5
Summary Findings Each Category	6
Detail Challenge Solved.....	7
Others.....	7
User Guide.....	7
Cryptography	8
Might Guy's Secret.....	8
Rot1Aoka.....	9
Pramuka	10
Classic Cryptography.....	10
Simple Substitution Cipher.....	11
USB Forensic	11
USB Forensic 1	11
USB Forensic 2	12
USB Forensic 3	13
USB Forensic 4	14
USB Forensic 5	14
USB Forensic 6	15
USB Forensic 7	16
USB Forensic 8	17
Windows Forensic	17
Windows Forensic 1	17
Windows Forensic 2	18
Windows Forensic 3	19
Windows Forensic 4	20
Windows Forensic 5	21
Windows Forensic 6	22
Windows Forensic 7	23
Windows Forensic 8	24
Web Exploit	25



Hidden Buy Flag	25
Konoha Breach	26
ID-Networkers	27
Support Force	28
Kue Monster	29
IDN Education.....	30
Beyond Way	31
I'm Not Me, You Are Me.....	32
Circle Clicker.....	33
Xss.....	34
Awesome Website	34
Casino 777.....	35
Welcome Flag	36
Forgot Encode	36
Web 303	38
DOM-Based XSS	38
Unsafe eval()	39
Prototype Pollution Demo	40
JWT Token Manipulation	40
Client-Side Privilege Escalation	41
Timing Attack	42
Unsafe Deserialization	43
Log Analysis	43
Log Analysis 1	43
Log Analysis 2	44
Log Analysis 3	45
Log Analysis 4	46
Log Analysis 5	47
Log Analysis 6	48
Log Analysis 7	49
Log Analysis 8	50
Log Analysis 9	51
Forensic.....	51
Forensic 1	51



Forensic 2	52
------------------	----



Introduction Team

Nama Team : Depok Cybersec

Anggota : Alif Banu Nur Rachman, Raihan Putra Kurniawan, Ahmad Ferdiyansyah.

alifbanu@gmail.com

Teams: Depok Cybersec

101st place

522 points

Members

User Name	Score
Alif Banu Nur Rachman Captain	32
Raihan Putra Kurniawan	280
Ahmad Ferdiyansyah	210

Point : 522



Summary Findings Each Category

Category	Soal Selesai / Dari Soal yang ada	Point
Web Exploit	12/13	120
Other	1/2	10
Welcome Flag	1/1	10
Web 303	7/7	70
Cryptography	5/7	50
Log Analysis	9/9	90
USB Forensic	8/8	80
Browser Forensic	0/10	0
Windows Forensic	8/15	80
Forensic	2/2	12

Pengurangan Nilai : 8 Point



Detail Challenge Solved

Others

User Guide

Deskripsi :

FLAG

Lampiran : none

Solusi :

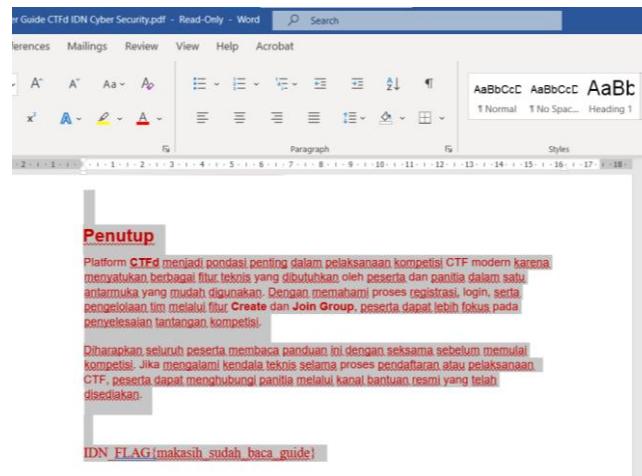
- Membaca seluruh **User Guide**.
- Menemukan format **flag**, lalu coba submit flag Namun **incorrect**.

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

Might Guy's Secret

Deskripsi :

Suatu hari, Might Guy mengirimkan sebuah pesan rahasia ke Konoha HQ. Namun, pesan tersebut dicegat di tengah jalan.

Ini isi pesannya: QGA_OTS{v067j1723qk40f5v33z656afwse60kdf67u9606}

Bersama dengan pesan itu, kamu menemukan secarik kertas bertuliskan: "Giovan Battista Bellaso: 1553M: idnmantab"

Tampaknya Might Guy menggunakan teknik enkripsi klasik namun ampuh

Authtor: Nur Cholis Majid

Lampiran :

Solusi :

- Petunjuk: "Giovan Battista Bellaso: 1553M: idnmantab" dengan jenis chipper Vigenère Cipher dan keynya adalah IDNMANTAB
- Gunakan decoder online



The left panel shows a search result for 'IDNMANTAB' which is a ROT13 cipher. The right panel shows a Vigenère cipher decryption tool with the ciphertext 'QGA_OTS{v067j1723qk40f5v33z656afwse60kdf67u9606}' and the key 'IDNMANTAB'.

Flag: IDN_CTF{c067j1723pc40c5i33n656asdsd60cas67i9606}

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

The left panel shows a search result for 'UPZ_RXMS{B3Y4Z4E4Z_PG1G_94E1t}' which is a ROT13 cipher. The right panel shows a ROT1 cipher decoder with the ciphertext 'VQA_SYNT{C3Z4A4F4A_QH1H_94F1u}'.

- Coba ROT13 untuk seluruh string = correct

The left panel shows a search result for 'IDN_FLAG{P3M4N4S4N_DU1U_94S1H}' which is a ROT13 cipher. The right panel shows a ROT cipher decoder with the ciphertext 'VQA_SYNT{C3Z4A4F4A_QH1H_94F1u}'.

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}

Classic Cryptography

Deskripsi :

Cn knud bqxosnfqzogx. zmc sgd ekzf:
HCM_BSE{xzxx_xnt_zqd_fqdzs}

Author: Rafly Permana

Lampiran :

Solusi :

- Terlihat dari judul “Classic Cryptography” maka kita akan mencoba Caesar Cipher
- Gunakan Decoder Online
- Geser huruf menjadi -1 a-z

The screenshot shows a web-based Caesar cipher decoder. At the top, there's a search bar labeled "RECHERCHE SUR D'CODE PAR MOTS-CLÉS :" with the placeholder "Tapez par exemple 'sudoku'". Below it is a link "PARCOURIR LA LISTE COMPLÈTE DES OUTILS". The main area is titled "Résultats" and shows the decrypted message: "Chiffre de César - Décalage de -1" followed by the letters "Z, A, B, C, D, E, ... X, Y, A, B, C, D, E, F, ... Y, Z". Below this, two arrows point to the right: "→ 25 (↔ 1) IDN_CTF{yayy_you_are_great}" and "← 25 (↔ 1) GBL_ARD{wyww_wms_ypc_epcyr}". To the right, there's a box titled "MESSAGE CHIFFRE PAR CODE CESAR ?" containing the original message "HCM_BSE{xzxx_xnt_zqd_fqdzs}". Below this box is the text "Tester tous les décalages possibles (alphabet de 26 lettres A-Z)". There are two buttons: "► DÉCHIFFRER AUTOMATIQUEMENT" and "DÉCHIFFREMENT MANUEL ET PARAMÈTRES". At the bottom, there's a field "★ DÉCALAGE/CLÉ (NOMBRE) : -1" with a dropdown menu showing "-1" and other options like "0", "1", "2", etc.

Flag : IDN_CTF{yayy_you_are_great}

Copyright © 2025, All rights reserved



Simple Substitution Cipher

Deskripsi :

ORF_EZY{ziol_ol_g_yqsx_wxz_lg_tq_ln}

Author: Rafly Permana

Lampiran :

Solusi :

- Terlihat dari judul "Simple Substitution Cipher", jadi kita akan menggunakan Substitution Chipper
- Dengan Plaintext "abcdefghijklmnopqrstuvwxyz" dan ciphertext "qwertyuiopasdfghjklzxcvbnm"

The screenshot shows a web-based cipher tool interface. It has three main sections: Ciphertext (left), Encode Decode (center), and Plaintext (right).
Ciphertext section: Contains the ciphertext "ORF_EZY{ziol_ol_g_yqsx_wxz_lg_tq_ln}" and a dropdown menu labeled "Ciphertext".
Encode Decode section: Contains the dropdown menu "Alphabetical substitution" and two tables:

- PLAINTEXT ALPHABET: abcdefghijklmnopqrstuvwxyz
- CIPHERTEXT ALPHABET: qwertyuiopasdfghjklzxcvbnm

Below these tables are two dropdown menus:

- CASE STRATEGY: Maintain case
- FOREIGN CHARS: Include Ignore

Plaintext section: Contains the plaintext "IDN_CTF{this_is_o_falu_but_so_ea_sy}" and a dropdown menu labeled "Plaintext".

Flag : IDN_CTF{THIS_IS_O_FALU_BUT_SO_EA_SY}

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

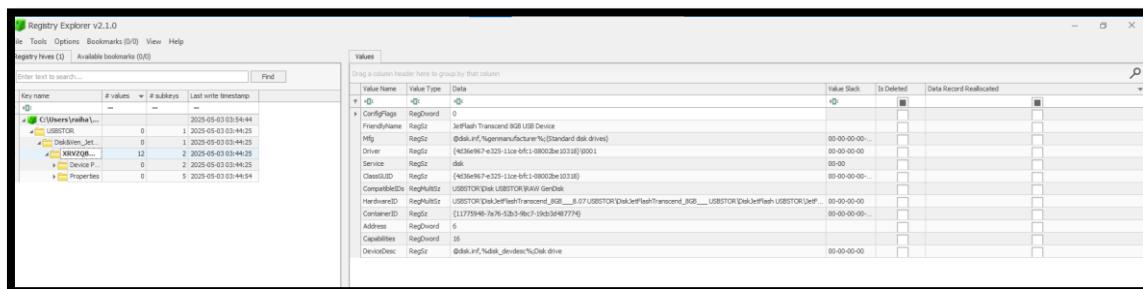
Lampiran : [usb.zip](#)

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 ?

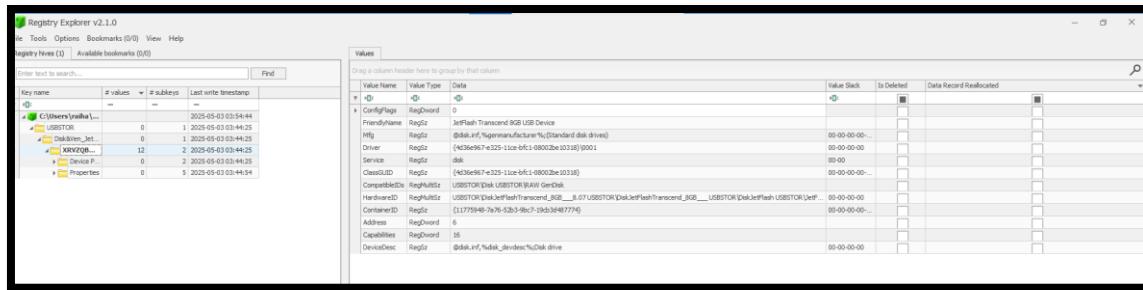
format flag : IDN_FLAG{Jawaban yang disoal}

Auhtor: Aditya Firman Nugroho Author: 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 !

(Filennya ada di pertanyaan pertama)

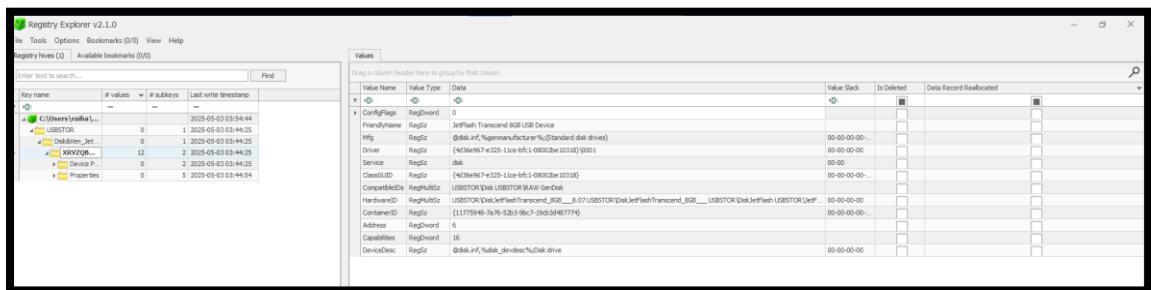
Apa Containder ID USB Yang dipakai Hacker ?

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 !

(Filanya 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**}”.

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

USB Forensic 5

Deskripsi :

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

(Filennya 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 ”

Registry hives (5) Available bookmarks (29/0)			
Values Recent documents			
Drag a column header here to group by that column			
Extension	Value Name	Target Name	
.txt	0	4f624842b5984-8308848.txt	

Flag : IDN_FLAG{4f624842b5984-8308848.txt}

Copyright © 2025, All rights reserved



USB Forensic 7

Deskripsi :

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

(Filanya ada di pertanyaan pertama)

Direktry 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** ”.

The screenshot shows the ShellBags Explorer interface. On the left, there's a tree view of the desktop environment with nodes for Desktop, My Computer, Quick Access, and a folder named E:\. On the right, there's a table with columns: Value, Icon, Shell Type, and MRU Position. A single row is selected, showing the value '-04893u42=b5u024u50u', an icon representing a folder, 'Directory' under Shell Type, and '0' under MRU Position. Below the table, there are tabs for Summary, Details, and Hex, and a summary section at the bottom with the following text:

Name: -04893u42=b5u024u50u
Absolute path: Desktop\E:\\-04893u42=b5u024u50u
Key-Value name path: BagMRU\1-0
Registry last write time: 2025-05-03 03:44:33.581

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	=	=
.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 !!

(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**

Evidence Tree

- Evident.ad1
 - Custom Content Image([Multi]) [AD1]
 - \Physicaldrive1:Basic data partition (3) [60798MB]NONAME [NTFS]
 - [root]
 - Users
 - CLIENT
 - AppData

- 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	Extension	Value Name	Target Name	Link Name	Mru Position
CurrentVersion	0	—	.txt	2	password docs.txt	password docs.lnk	0
ApplicationAssociationToasts	323	—	.txt	1	flag.txt	flag (2).lnk	1
ContentDeliveryManager	14	—	.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 !!

(Filennya 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	=	=
.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 ?

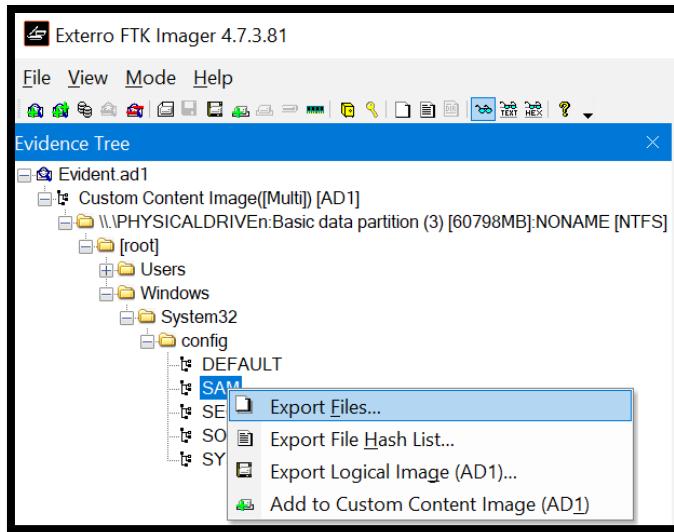
format flag : IDN_FLAG{Jawaban yang disoal}

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 ”.

Key name	# values	# subkeys
C:\Users\railha\OneDrive\Document\ctf\INTUSERDAT	==	==
↳ Unassociated deleted values	2	0
↳ ROOT	0	10 2
C:\Users\railha\OneDrive\Document\ctf\SECURITY	==	==
↳ ROOT	0	3 2
C:\Users\railha\OneDrive\Document\ctf\SAM	==	==
↳ ROOT	0	1 2
↳ SAM	2	3 2
↳ Domains	1	2 2
↳ Builtin	3	3 2
↳ Aliases	1	2 2
↳ Groups	1	1 2
↳ Names	1	0 2
↳ Users	1	1 2
↳ Names	1	0 2
↳ Account	2	3 2
↳ Aliases	1	2 2
↳ Groups	1	2 2
↳ Users	1	0 2

Valid ... User Id Invalid ... Total ... Created On Last... Last... Last... Exp... User Name

Valid	User Id	Invalid	Total	Created On	Last	Last	Last	Exp	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	Invalid	Total	Created On	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

Flag : IDN_FLAG{ Jon }

Windows Forensic 5

Deskripsi :

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

(Filennya ada di pertanyaan pertama)

User yang localgroupnya ada 2, yaitu ?

format flag : IDN_FLAG{Jawaban yang disoal}

Auhor: 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 checked="" type="checkbox"/>	=	=	=	=	=	=	=	=	WDAGUtilityA ccount	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
		504	0	0	2025-05-03 03:27:38	202...								
		<input checked="" type="checkbox"/>												
		1001	0	3	2025-05-03 03:29:00	202...				CLIENT			Administrato rs	
		<input checked="" type="checkbox"/>								Geraldin			<input checked="" type="checkbox"/>	Administrato rs, Users
		<input checked="" type="checkbox"/>	1003	0	0	2025-05-03 07:04:43	202...			Jon				Users
		<input checked="" type="checkbox"/>												

Flag : IDN_FLAG{Geraldin}

Windows Forensic 6

Deskripsi :

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

(Filennya 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"/>	=	=	=	=	=	=	=	=	RBC
<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 !!

(Filennya 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...
=	=	=	=	=	=	=	=	rac
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 !!

(Filennya 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
Unassociated deleted values	—	—
ROOT	0	10 2
SECURITY	0	3 2
USAH	0	1 2
SAM	2	3 2
Domains	1	2 2
Builtin	3	3 2
Aliases	1	21 2

Group Name	Comment	Users
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-1-5-21-2412307826-2007293762-2764304457-1052
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
Guests	Guests have limited 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
Power Users	Power Users are included for backwards compatibility and possess limited administrative powers	
Backup Operators	Backup Operators can override security restrictions for the sole purpose of backing up or restoring files	
Replicator	Supports file replication in a domain	
Remote Desktop Users	Members in this group are granted the right to logon remotely	

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



Web Exploit

Hidden Buy Flag

Deskripsi :

Tim ID-Network baru saja membuat website, tetapi tim internal saja yang dapat masuk ke dalam website tersebut dengan pointing ke website (idn.id), kami menyuruh kalian para (Pentester) untuk mencoba menemukan celah disana dan masuk ke website tersebut. Didalam website tersebut kalian harus membeli sebuah Flag dengan harga 100000000.

Author : Faiz Ahmad Habibi

Lampiran : https://ctf.solusiber.com/buy_the_flag/

Solusi :

- Disini kita memiliki saldo Rp. 100 dan harga untuk flag Rp. 10.000.000.000
- Kita inspect element untuk mengubah value dari yang Rp. 100 menjadi Rp. 10.000.000.00

```
<input type="hidden" name="saldo" value="10000000000">  
<button type="submit">Beli Flag</button>
```

- Karna valuenya sudah di ubah kita coba klik beli flag

Toko Benderaku

Saldo Kamu: Rp100

Premium Product

CTF
CAPTURE THE FLAG

Harga: Rp10.000.000.000

Beli Flag

IDN_FLAG{h3ader_wh1telist_4nd_p4r4m3ter_t4mp3r1ng_v3rry_3zzz}

Flag: IDN_FLAG{h3ader_wh1telist_4nd_p4r4m3ter_t4mp3r1ng_v3rry_3zzz}



Konoha Breach

Deskripsi :

Desa Konoha baru saja meluncurkan sistem data tabel internal untuk para ninja tingkat tinggi. Sistem ini hanya bisa diakses setelah login dengan kredensial resmi admin.

Namun, rumor menyebutkan bahwa sistem ini dibangun tergesa-gesa oleh seorang Chuunin yang baru belajar PHP. Konon, ada celah klasik yang memungkinkan siapa pun melewati sistem login dan mengakses dashboard rahasia tanpa kredensial!

Bocoran pertama yang muncul berisi daftar shinobi aktif dan lokasi markas Anbu. Keamanan Konoha kini dalam bahaya...

Bisakah kamu menyusup ke sistem tanpa login dan menemukan yang tersembunyi?

Author: Rafly Permana

Lampiran : Isi dari web menggunakan SQL Injection

Solusi :

- Menggunakan Exploitasi SQL Injection, Payload untuk Bypass Login
- Isi Username dengan : ' OR 1=1-- -
- Dan isi Password dengan : password
- Setelah berhasil login, lalu Buka "View Page Source"



Daftar Data PII

Nama Lengkap	Email	No. Telepon	NIK	Alamat
Naruto Uzumaki	naruto@konoha.go	081234567890	1234567890123456	Konoha, Rumah Hokage
Sasuke Uchiha	sasuke@uchiha.org	082345678901	9876543210987654	Konoha, Distrik Uchiha
Sakura Haruno	sakura@medic.konoha	083456789012	1122334455667788	Konoha, Jalan Sakura
Kakashi Hatake	kakashi@konoha.go	081111111111	1001001001001001	Konoha, Jalan Ninja 7
Hinata Hyuga	hinata@hyuga.net	082222222222	2002002002002002	Konoha, Distrik Hyuga
Shikamaru Nara	shikamaru@nara.org	083333333333	3003003003003003	Konoha, Jalan Strategi
Ino Yamanaka	ino@yamanaka.co	084444444444	4004004004004004	Konoha, Toko Bunga Yamanaka
Choji Akimichi	choji@akimichi.food	085555555555	5005005005005005	Konoha, Jalan Kuliner
Rock Lee	lee@taijutsu.konoha	086666666666	6006006006006006	Konoha, Gym Gai Sensei
Tenten	tenten@weapon.konoha	087777777777	7007007007007007	Konoha, Toko Senjata
Neji Hyuga	neji@hyuga.org	088888888888	8008008008008008	Konoha, Markas Hyuga
Might Guy	guy@powerofyouth.konoha	089999999999	9009009009009009	Konoha, Jalan Semangat

Flag : IDN_CTF{cONRats_you_goin_tohe_insideee}

ID-Networkers

Deskripsi :

Sebuah situs publik baru saja diluncurkan ID-Networkers. Tampilannya sederhana dan tidak mencurigakan—hanya halaman beranda dengan ucapan “Selamat Datang di ID- Networkers” dan beberapa tambahan lainnya.

Namun, informasi mengatakan bahwa developer situs ini terlalu percaya pada "aturan" yang ditulis untuk mesin pencari. Mereka menyembunyikan direktori rahasia dengan harapan crawler tidak akan melihatnya...

Tapi kamu bukan crawler, kamu seorang penyusup yang teliti.

Author: Rafly Permana

Solusi :

- Buka Website https://ctf.solusiber.com/robots_dashboard/
- Gunakan text robots.txt setelah slash dashboard
- Akan tampil Dissallow message : asds024nsfd01372021.html
- Copy Dissallow message : asds024nsfd01372021.html , ke slash terakhir



```
User-agent: *
Disallow: /asdsa024nsfd01372021.html
```

Flag : IDN_CTF{@W*_FOuN&_th@_#|**\$N_F|@&}

Support Force

Deskripsi :

Ini klub eksklusif buat agen rahasia. Browser biasa? Maaf, Anda tidak terdaftar. Tapi kalau kamu bisa pura-pura jadi "Agent hackme", pintu rahasia mungkin bakal terbuka buatmu.

Author : Rafly Permana

Lampiran : https://ctf.solusiber.com/support_force/

Solusi :

- Diwebsitenya kita diberi hint untuk lihat browser header, dan dari deskripsi kita disuruh untuk menjadi Agent hackme.
- kita akan memanipulasi headernya tersebut menggunakan chrome ekstention yaitu requestly
- masuk ke requestly > pilih modify headers > masukan URL
https://ctf.solusiber.com/support_force/ > add request header : user-agent dan Value : hackme > safe rule.

The screenshot shows the Chrome DevTools Network tab. The timeline at the top indicates a request took approximately 60ms. Below the timeline, a table lists the request headers for the URL [support_force/](https://ctf.solusiber.com/support_force/). The 'Headers' column is selected. The table includes columns for Name, Headers, Preview, Response, Initiator, Timing, Adblock, and Cookies. Key headers shown include:

Name	Headers	Preview
support_force/	Cookie: PHPSESSID=02415d0a512dd1004fa0200094110e Priority: u=0, i Referer: https://ctf.solusiber.com/ctf/challenges Sec-Ch-Ua: "Chromium";v="136", "Brave";v="136", "Not.A/Brand";v="99" Sec-Ch-Ua-Mobile: ?0 Sec-Ch-Ua-Platform: "Windows" Sec-Fetch-Dest: document Sec-Fetch-Mode: navigate Sec-Fetch-Site: same-origin Sec-Fetch-User: ?1 Sec-Gpc: 1 Upgrade-Insecure-Requests: 1 User-Agent: hackme	Response: PHPSESSID=02415d0a512dd1004fa0200094110e Initiator: https://ctf.solusiber.com/ctf/challenges Timing: 10 ms - 60 ms Adblock: None Cookies: None

At the bottom of the table, it says "1 / 2 requests | 0.9 kB / 1.4 kB transferred".



Access Filtering

IDN_CTF{r7x9_uaSwitch_delta44}

Hint: Check your browser headers. Something isn't quite right...

Flag : IDN_CTF{r7x9_uaSwitch_delta44}

Kue Monster

Deskripsi :

Kamu cuma dikasih kue biasa? Bosen. Upgrade kue-mu jadi kue sultan dan lihat apa yang bisa kamu lakukan! (Jangan makan beneran ya)

Author : Rafly Permana

Lampiran : https://ctf.solusiber.com/kue_monster/

Solusi:

- disini kita diberi hint untuk inspect cookies kita.
- Terlihat juga disini kita menggunakan user guest dan disuruh untuk merubah menjadi admin untuk mendapatkan flagnya
- Masuk ke devtool (F12) > application > cookies > karna kita disuruh merubah user kita pilih user > ubah valuenya dari yang %7B%22role%22%3A%22guest%22%7D Menjadi %7B%22role%22%3A%22admin%22%7D



Name	Value	D..	P..	E..	S..	H..	S..	S..	P..	C..	P..
PHPSESSID	5624f3aba3f2baf...	c...	/	S...	41					M..	
user	%7B%22role%22%... {"role": "guest"}	c...	/...	2...	34					M..	

Cookie Value Show URL-decoded
{"role": "guest"}

- Refresh halaman dan akan muncul flagnya

```
user@ctf-web:~$ whoami
admin
user@ctf-web:~$ cat /flag
IDN_CTF{Y0u_@rE_TH@_C00K|e_M@st$r}

# Hint: Inspect your cookies. Something's not what it seems 🍪
```

Flag : IDN_CTF{Y0u_@rE_TH@_C00K|e_M@st\$r}

IDN Education

Deskripsi :

Siapa sangka file-file tersembunyi di balik input sederhana? Coba kamu buka celahnya, biar file yang terpendam itu bisa keluar. Siapa tahu ada kejutan!

Author : Rafly Permana

Lampiran : https://ctf.solusiber.com/idn_edu/

Solusi :

- Dsini kita diberi hint yaitu LFI
- Kita akan mencoba – coba path yang megekplorasi
https://ctf.solusiber.com/idn_edu/?page=../../../../etc/passwd
- Setelah itu kita mencoba path yang memungkinkan mendapat flag
https://ctf.solusiber.com/idn_edu/?page=../../../../var/www/html/flag.txt



IDN_CTF{l@tisec_r29-loadr}

Flag : IDN_CTF{l@tisec_r29-loadr}

Beyond Way

Deskripsi :

Mungkin kamu nggak pernah diajari buat berjalan keluar dari jalan yang benar... tapi kalau kamu bisa, kamu bakal dapetin sesuatu yang terlarang. Ayo jalanin manipulasi path-nya!



Author : Rafly Permana

Lampiran : https://ctf.solusiber.com/search_free/

Solusi :

- kita disini disuruh untuk manipulasi pathnya
- untuk path awal kita coba masuk
https://ctf.solusiber.com/search_free/?file=../../../../etc/passwd
- coba untuk mencari flagnya dengan mengubah path menjadi
https://ctf.solusiber.com/search_free/?file=../flag.txt



The screenshot shows a red-themed website for Red Mist Technologies. At the top left is a white shield icon with a keyhole. To its right, the company name "Red Mist Technologies" is written in large, bold, white sans-serif font, with "company security" in a smaller font below it. Below the main title is a navigation bar with "About" and "Contact" links. A footer section contains the text "IDN_CTF{tvec-resolver_41}".

Flag: IDN_CTF{tvec-resolver_41}

I'm Not Me, You Are Me

Deskripsi :

Bukan cuma kamu yang punya profil! Coba-coba ganti ID di URL dan lihat apakah kamu bisa jadi orang lain. Mungkin kamu bisa mengakses sesuatu yang seharusnya nggak buatmu!

Author : Rafly Permana

Lampiran : https://ctf.solusiber.com/user_information/

Solusi :

- Kita disini disuruh untuk coba ganti ID yang diberikan
- Kita akan mencoba memasukan id 1

```
Dan terjadi {  
    "id": 1,  
    "username": "luffy",  
    "role": "user",  
    "bio": "Aku ingin menjadi raja bajak laut!"  
}
```

- Kita coba lagi untuk memasukan id 0



```
{  
    "id": 0,  
    "username": "rafly",  
    "role": "admin",  
    "bio": "Aku ingin menjadi hacker!",  
    "flag": "IDN_CTF{Y0u_FF0D_the_heN_admin}"  
}
```

- Flag ditemukan

Flag: IDN_CTF{Y0u_FF0D_the_heN_admin}

Circle Clicker

Deskripsi :

Click Sampai 1000 kali!

Flagnya Di Encode Dengan Encoder yang sama dengan bitcoin dan solana

Author : Mohamad Fattyr

Lampiran : https://ctf.solusiber.com/circle_clicker/

Solusi :

- Hint Click sampai 1000 kali, jadi kita coba click dan ternyata berubah disaat click ke 20
- Buka console dan diberi hint yaitu revealsecret()

```
> revealSecret()  
  
Selamat! Kamu menemukan fungsi rahasia!           circle_clicker/:80  
Bagian pertama flag: 5WJoJxz5CCVWDSE               circle_clicker/:80  
Untuk bagian kedua, coba berpikir sambil bermain click!   circle_clicker/:80  
undefined
```

- Setelah mengetahui bagian pertama flagnya yaitu 5WJoJxz5CCVWDSE, kita menuju ke sources dan mencari kode yang ngacu 5WJoJxz5CCVWDSE, dan ditemukan WJoJxz5CCVWDSEpH4E1n77BT5Fec
- Buka decoder online pilih base 58 karna dari hint kita menggunakan encoder bitcoin dan solana

The screenshot shows a web-based base 58 decoder. At the top, it says "BASE 58" and "DÉCHIFFREMENT DE LA BASE 58". It has dropdown menus for "ALPHABET" (set to "123456789ABC...XYZabc...xyz (Bitcoin BTC)") and "MESSAGE CHIFFRÉ PAR BASE 58" (containing the hex string "5WJoJxz5CCVWDSEpH4E1n77BT5Fec"). Below these are input fields for "RECHERCHE SUR D'CODE PAR MOTS-CLÉS:" (with placeholder "Tapez par exemple 'cesar'") and "PARCOURIR LA LISTE COMPLÈTE DES OUTILS". The results section at the bottom shows the output "IDN_CTF{click_master}".



Flag : IDN_CTF{click_master}

XSS

Deskripsi :

CURI!

Author : Mohamad Fattyr

Lampiran : https://ctf.solusiber.com/super_click/

Solusi :

- Kita diberi hint untuk melihat cookie
- Masuk ke cookie melalui devtools dan menemukan

Name	Value
flag	IDN_FLAG{XSS_C00K13_ST34L3R}
PHPSESSID	5624f3aba3f2baf0041ad2db0894ff6e

Cookie Value Show URL-decoded
IDN_FLAG{XSS_C00K13_ST34L3R}

Flag : IDN_FLAG{XSS_C00K13_ST34L3R}

Awesome Website

Deskripsi :

CARI!!

Author : Mohamad Fattyr

Lampiran : https://ctf.solusiber.com/awesome_website/

Solusi :

- Saya membuka sources code
- Lalu menemukan API token yaitu SUROX0ZMQd7VzNCXzNOQ29kM183UjFjazF9
- Encode melalui base64
- Dan menghasilkan flag



The screenshot shows a search interface for tools. In the search bar, it says "Rechercher un outil" and "RECHERCHE SUR D'CODE PAR MOTS-CLÉS : Tapez par exemple 'scrabble'". Below this is a link "PARCOURIR LA LISTE COMPLÈTE DES OUTILS". The results section shows a single result: "SUROX02MQd7...zF9" which is expanded to "IDN_FLAG{W3B_3NCod3_7R1ck1}". On the right, there's a "CODE BASE64" section with sub-sections "DÉCODAGE DE LA BASE64" and "MESSAGE CHIFFRÉ PAR BASE 64". It also includes options for "MODE": "BASE64 (STANDARD RFC 4648)" (selected), "BRUTE-FORCE : TENTATIVE DES VARIANTES BASE64 (VOIR FAQ)", and "SANS CASSE : MAJUSCULES-MINUSCULES SONT ERONÉES/PERD".

Flag: IDN_FLAG{W3B_3NCod3_7R1ck1}

Casino 777

Deksripsi :

Ternyata aplikasi ini menerima input melalui query parameter. Cobalah eksplorasi URL dan manipulasi nilai slot-nya.

mungkin ada sesuatu yang jika sudah lengkap baru merespon

Author : Mohamad Fattyr

Lampiran : https://ctf.solusiber.com/casino_777/

Solusi :

- Buka source code lalu find flag disana terlihat flag terletak di script yaitu

The screenshot shows a portion of a JavaScript file with several lines of code. The flag is embedded within a JSON object. The code includes various variables and functions, but the flag itself is a simple string: "IDN_CTF{M4st3r_0f_H77P_R3qu3st_M4n1pul4t10n!}".

```
while(![]){try{const _0x50ddff=parseInt(_0xfa0b2b(0xcf))/0x1+-parseInt(_0xfa0b2b(0xb7))/0x2+parseInt
,'then','get_flag','random','appendChild','5256318RovBtD','slots','style','getElementById','startsWith'
const _0x3513f3=_0x2753f2,_0x1031b1=document['getElementById'](_0x3513f3(0xc9)),_0x393b5f=document['
'][_0x729024(0xc5)]=_0x729024(0xec),fetch(_0x729024(0xc6))[_0x729024(0xf3)](_0x26689b=>_0x26689b[_0x7
la(0xba)](0x9,_0x28586e||0x1)),Math[_0x4902da(0xb4)](0x1,Math[_0x4902da(0xba)](0x9,_0x62f393||0x1)),M
0c6[0x1]===0x7&&_0x4609c6[0x2]===0x7)_0x47d4ad+=0x1f4,_0x566069[_0x32d74f(0xd5)]=_0x47d4ad,_0x5c1889(
bed,_0x2e481e){const _0x5378aa=_0x3513f3;_0x415051[_0x5378aa(0xd5)]=_0x5b4bed,_0x415051[_0x5378aa(0xf
52be)]try{_0x4791db=JSON[_0x75ec33(0xbff)](_0x5e52be)};catch(_0x4809ea){console[_0x75ec33(0xd2)](_0x75
f0deb)||_0x56e4bd?{'success':![],'flag':'IDN_CTF{M4st3r_0f_H77P_R3qu3st_M4n1pul4t10n!}'}:{'success':!
()<0x168+_0x325baf(0xed),_0x1e3b7a[_0x325baf(0xf9)][_0x325baf(0xe6)]=_0x325baf(0xdc),_0x1e3b7a[_0x325
105])}}},_0x7d0);}const _0x58197c=new URLSearchParams(window[_0x3513f3(0xe0)][_0x3513f3(0xbc)]);_0x5
```

Flag : IDN_CTF{M4st3r_0f_H77P_R3qu3st_M4n1pul4t10n!}



Welcome Flag

Forgot Encode

Deskripsi :

sesorang menggunakan encoding untuk menyimpan rahasianya tapi dia melakukanya sambil berbincang dengan orang lain sehingga dia lupa.

bantu orang tersebut untuk menemukan rahasianya:

Vm0wd2VHUXhUWGhYV0d4VIYwZG9iMVJVU2pSVIZsbDNWMnQwYUZKc2NG
WIZWM1IzWVRBeFdHVkVSbHBoTVZwUVZrUkdXbVF5U2tWWGJHUnBWa1ph
TmxavVvNqUIRNRFZ6VjI1V1ZXSIZXbFZWYWs1dlVsWmtjbFp0Um10TIYxSIIWbT
AxVTJGR1NsbFJiRkpWVm0xb1ExUldXbXRXTVdSMFpFWmtUbUpGY0ZsWFZFSI
hWVEZSZUZOWWJGWmlSa3BoV1d0a2lyUnNiSEZTYlhSciZqQTFTbFI5TVVkvWJ
GcFZWbXhvVjJKSFVqWIViRnByVm1zeFZsZHJPVmRpU0VKWVYxZDRVMMVp0VV
hoaVJtUllZbXMxV1ZadGVFdE5SbkJXVmxSV2FGSXdjRWRaTUdoVFYwWmFjMk5
JUmxWV2JIQXpXWHBLUzFJeVJrZFdiV2hvVFVoQ01sWnRNREZrTWsxM1RWW
mtZVkpXV2xWWIZFNVRWREZhY1ZKcmRGUINI RVI6Vmkek5WZEEdXbFZSYWx
KV1RXcFdjbFI5TVV0VFJsWnpZVWRHVjJWcldtOVdiR1EwVVRGYVZrMVZWazV
TUkVFNQ==

Author: Rafly Permana

Lampiran :

Solusi :

- Gunakan decode base64
- Decode pertama menghasilkan

The screenshot shows a web-based tool for decoding Base64. The input field contains the encoded string: Vm0wd2VHUXhUWGhYV0d4VIYwZG9iMVJVU2pSVIZsbDNWMnQwYUZKc2NG... The output field displays the decoded text: Vm0weGQxTXhXWGxVV0dob1RUSjRVV113V2t0aFJscFZVV3R3YTAXWGVER1phMvpQvkRGWmdySkVxbgRpVkZan1ZUsjRTMDVz25WwJvw1Vvak5vu1Zkc1ZtRmtNV1JYVm01U2FGS11RbfJVMm1Q1RwmtWMR0ZEZkTmJFcF1XVEJXVTFRfENybFZirkphwtkb2RsbHFsbXrVjaA1sLyMudubFpVVmxoV2JHUjZUbFprVmsxVldroVdiSeJYV1d4U1ZtUXhiRmRYYms1wVZteEtNRnBwV1RwaFIwcEdZMghTV0Zac2NIRlVwbHAzWxpKS1IyRkdwbwhoTUhCM1ZtMDfkMk13TVzkYYJWw1VZVE5TVDFacVJrdFRSbEYZv1dzNvdGw1Vra1JwTwPwC1YyMuTR1ZzYudGV2VrwM9wbGQ0UTFaVk1Vvk5SREE5. The tool interface includes sections for 'MESSAGE CHIFFRÉ PAR BASE 64', 'DÉCODAGE DE LA BASE64' (with a radio button selected for 'BASE64 (STANDARD RFC 4648)'), and various encoding/decoding options like 'BRUTE-FORCE', 'SANS CASSE', and 'FORMAT DES RÉSULTATS'.

- Karna masih belum menemukan kita coba decode lagi
- Decode kedua juga masih gagal



Rechercher un outil

★ RECHERCHE SUR D'CODE PAR MOTS-CLÉS :
Tapez par exemple 'scrabble'

★ PARCOURIR LA LISTE COMPLÈTE DES OUTILS

Résultats

```
Vm0weGQxTxhX...EE5
Vm0xd1MxwXlUWghoTTJ4UVVwWkthRlpvUwtwa01XeDFZa
1ZPVDFZd2JEwldivFZ6VTJ4S05sWnVUbUZUJnoRvdrVm
FkMWRXVm5SaFJYQlTRUVmhCTVzkv1dtFdNbEpYWTBWU1Q
xSx1vbFJaYkdodllqRmtkv05JV21GTlZUVlhwbGR6T1Zk
Vk1Vwk9wbHBXWxSVmQxbFdxbk5YVmKMFpVVTVhR0pGY
0hSWFZscHFUV1p3YzJKR2FGVmhhMHB2Vm01d2MwMVdaRV
ZUYTNST1ZqRktTR1F3Vws5WFZUQjRVMjvrV21KSFVsagF
WekZoVld4Q1ZVMUVNRDA9
```

CODE BASE64
Informatique > Codage de Caractères > Code Base64

DÉCODAGE DE LA BASE64

★ MESSAGE CHIFFRÉ PAR BASE 64

```
U1Zkc1ZtRmtNV1jYVm01U2FGs1TrbFJVVm1oQ1RwWmtWMWR0ZEZkTm1F
cf1XveJXVTFReFNYbFZirKphwiTk2RsbfHSbxRrVja1S1yMudubFpV
VmoxV2JHUjZubFprVmsxV1dr0vdiseJYV1d4U1ZtUXhiRmRYYms1wVzt
eeetNRNBWV1JWafIwcEdzMgHtv0zAc2NIR1VwbHawXpkSL1yRkdwbwho
TUhCM1ZtMDFKMk13TV2kYYJWW1VZVE5TVDFacVjrdFRSbeYzv1ldzNvdG
W1Vra1JWtWpWc1YyMuETR1ZyUdgV2rVm9wbGQOUTFavk1Vvk5SRE5
```

★ MODE **BASE64 (STANDARD RFC 4648)**

② BRUTE-FORCE : TENTATIVE DES VARIANTES BASE64 (VOIR FAQ)

○ SANS CASSE : MAJUSCULES-MINUSCULES SONT ERONÉES/PERDUES (BRUTE-FORCE MAX 50 CAR.)

★ FORMAT DES RÉSULTATS **CHAINE DE CARACTÈRES IMPRIMABLES (ASCII/UNICODE)**

○ HEXADÉCIMAL 00-7F-FF

○ DÉCIMAL 0-127-255

○ OCTAL 000-177-377

○ BINAIRE 00000000-11111111

- Kita coba decode untuk ketiga kalinya
- Ternyata masih gagal

Rechercher un outil

★ RECHERCHE SUR D'CODE PAR MOTS-CLÉS :
Tapez par exemple 'scrabble'

★ PARCOURIR LA LISTE COMPLÈTE DES OUTILS

Résultats

```
Vm1wS1YyTxhhM2xQV0ZKaFZUQkpMwx1YkVOT1YwbDZwb
TVzu2xKn1ZuTmfTR3hEwkVad1dwVnRhXBTTvhBMVdwWm
twM1JXY0VST1IyU1RzbGhvYjFkdwnIwmFnVTvx1dzNvd
VMUZOVi1pwY1Rvd1lwWnNxV1j0ZU5aGJFcHRXV1pqTVzw
c2JGaFVha0pvVm5wc01wZEVta3ROVjFKSFQwUk9XVTB4U
25kwMjHulhaVzFhWxCVU1EMD0=
```

CODE BASE64
Informatique > Codage de Caractères > Code Base64

DÉCODAGE DE LA BASE64

★ MESSAGE CHIFFRÉ PAR BASE 64

```
Vm0xd1MxwXlUWghoTTJ4UVVwWkthRlpvUwtwa01XeDFZa1ZPVDFZd2JE
W1divFZ6VTJ4S05sWnVUbUZUJnoRvdrVmFkMWRXVm5SaFJYQlTRUVmhC
TV2kv1dtFdnbEPyWtbWU1qxSx1vbFJaYkdodllqRmtkv05JV21G1ZU
V1hbwGR6T1ZkV1Vwk9wbHBXWxSVmQxbfdxbk5YVmKMFpVVTVhR0pG
Y0hSwFZscHFUV1p3YzJKR2FGVmhhMHB2Vm01d2MwMVdaRVZUYTNST1Zq
RktTR1F3Vws5WFZUQjRVMjvrV21KSFVsagFWekZoVld4Q1ZVMUVNRDA9
```

★ MODE **BASE64 (STANDARD RFC 4648)**

② BRUTE-FORCE : TENTATIVE DES VARIANTES BASE64 (VOIR FAQ)

○ SANS CASSE : MAJUSCULES-MINUSCULES SONT ERONÉES/PERDUES (BRUTE-FORCE MAX 50 CAR.)

★ FORMAT DES RÉSULTATS **CHAINE DE CARACTÈRES IMPRIMABLES (ASCII/UNICODE)**

○ HEXADÉCIMAL 00-7F-FF

○ DÉCIMAL 0-127-255

- Decode lagi

Rechercher un outil

★ RECHERCHE SUR D'CODE PAR MOTS-CLÉS :
Tapez par exemple 'scrabble'

★ PARCOURIR LA LISTE COMPLÈTE DES OUTILS

Résultats

```
Vm1wS1YyTxhh...D0=
VmpKV2Mxa31PwfjhvtBjd1lubENOv16vm5s1J6vnnaS
GxDZEZwWVtaEpSMXA1wZkv2RwcEROR2RTY1hob1duCH
ZaMU5Wws5WU1FNvZVbTuwYzsWVRteE9hbEptWVZjMvp
sbFhuakJoVnpsMvdEsktNV1JHT0ROWU0xSndZbGRXZW1a
U1BUMD0=
```

CODE BASE64
Informatique > Codage de Caractères > Code Base64

DÉCODAGE DE LA BASE64

★ MESSAGE CHIFFRÉ PAR BASE 64

```
Vm1wS1YyTxhhM2xQV0ZKaFZUQkpMwx1YkVOT1YwbDZwbTVzU2xKn1ZuTmf
TR3hEwkVad1dwVnRhXBTTvhBMVdwWmTwM1JXY0VST1IyU1RzbGhvYjFkdw
NIwmFnVTvx1dzNvdMUZOVi1pwY1Rvd1lwWnNxV1j0ZU5aGJFcHRXV1pqT
V2wC2JGaFVha0pvVm5wc01wZEVta3ROVjFKSFQwUk9XVTB4U25kwMjHulha
VzFhWxCVU1EMD0=
```

★ MODE **BASE64 (STANDARD RFC 4648)**

② BRUTE-FORCE : TENTATIVE DES VARIANTES BASE64 (VOIR FAQ)

○ SANS CASSE : MAJUSCULES-MINUSCULES SONT ERONÉES/PERDUES (BRUTE-FORCE MAX 50 CAR.)

★ FORMAT DES RÉSULTATS **CHAINE DE CARACTÈRES IMPRIMABLES (ASCII/UNICODE)**

○ HEXADÉCIMAL 00-7F-FF

- Decode lagi



Rechercher un outil

★ RECHERCHE SUR D'CODE PAR MOTS-CLÉS :
Tapez par exemple 'scrabble'

★ PARCOURIR LA LISTE COMPLÈTE DES OUTILS

Résultats

VmpKV2Mxa31PwFJhVTBjd1ubENOV016Vm5s1J6VnNaSGxDZEZwWVvtaEp
SMXA1WZkV2RWCEr0R2RTY1hob1duchZaMUSWWs5WU1FNVZvbTUwYZsW
Rte9hbEptWZjMvpsbFhUakJoVnpsMVdESktNV1JHT0ROWU0xSndZbGRXZ
W1a18UMD0=

➤ VjJwc1kyOXRaU0IwYn1CNWIzVn1JRzVsZH1CdFpYUmhJR
1p5YVdWdVpDNGdSbxh0nvpZ1NVuk9YME5VUm50aV1YTm
x0a1JmYVc1Z11XTjBhVz1WDJKMWRGODNYM1JwYldWemZ
RPT0=

➤ Kita coba decode sampai berhasil disini terlihat decoder semakin sedikit

Rechercher un outil

★ RECHERCHE SUR D'CODE PAR MOTS-CLÉS :
Tapez par exemple 'scrabble'

★ PARCOURIR LA LISTE COMPLÈTE DES OUTILS

Résultats

V2VsY29tZSB0..Q==

Welcome to your new meta friend. Flag:
IDN_CTF{base64_in_action_but_7_times}

➤ Setelah 7 kali decode akhirnya menemukan flagnya

Flag : IDN_CTF{base64_in_action_but_7_times}

Web 303

DOM-Based XSS

Deskripsi :

Flagnya Di Encode Dengan Encoder yang sama dengan bitcoin dan solana

**Author: Rafly Permana **

Lampiran : https://ctf.solusiber.com/web_101/lab1/

Solusi :

- Disini kita langsung masuk ke sources dan mencari flagnya dikarenakan flag terletak pada script
- Ditemukan code 27oFx9NE945YFuBYFshct2G4Mi3hmKpS7UTWS87yKMn
- Lakukan decoder menggunakan base 58



The screenshot shows a web application interface for decoding messages from base 58. The main title is "DÉCHIFFREMENT DE LA BASE 58". Below it, under "Mathématiques > Arithmétique > Base 58", there are two dropdown menus: "ALPHABET" set to "123456789ABC...XYZabc...xyz (Bitcoin BTC)" and "MESSAGE CHIFFRÉ PAR BASE 58" set to "27oFx9NE945YFuBYFshct2G4Mi3hmKpS7UTWS87yKMn". The results section displays the decoded message "IDN_CTF{dom_based_xss_executed}".

Flag : IDN_CTF{dom_based_xss_executed}

Unsafe eval()

Deskripsi :

Flagnya Di Encode Dengan Encoder yang sama dengan bitcoin dan solana

**Author: Rafly Permana **

Lampiran : https://ctf.solusiber.com/web_101/lab2/

Solusi :

- Disini kita langsung masuk ke sources dan mencari flagnya dikarenakan flag terletak pada script
- Ditemukan code 8K1iQbpVVMPdiYxaREW9wJvvCmBnKZnNn9VguPSy71veTjEc
- Lakukan decoder menggunakan base 58

The screenshot shows a web application interface for decoding messages from base 58. The main title is "DÉCHIFFREMENT DE LA BASE 58". Below it, under "Mathématiques > Arithmétique > Base 58", there are two dropdown menus: "ALPHABET" set to "123456789ABC...XYZabc...xyz (Bitcoin BTC)" and "MESSAGE CHIFFRÉ PAR BASE 58" set to "8K1iQbpVVMPdiYxaREW9wJvvCmBnKZnNn9VguPSy71veTjEc". The results section displays the decoded message "IDN_CTF{you_used_eval_successfully}".

Flag : IDN_CTF{you_used_eval_successfully}



Prototype Pollution Demo

Deskripsi :

Flagnya Di Encode Dengan Encoder yang sama dengan bitcoin dan solana

**Author: Rafly Permana **

Lampiran : https://ctf.solusiber.com/web_101/lab3/

Solusi :

- Disini kita langsung masuk ke sources dan mencari flagnya dikarenakan flag terletak pada script
- Ditemukan code ZGW9mAgck8zohQPm4DeKSaKYAFRft9nPpb88Hj7nWrDtPcgyS
- Lakukan decoder menggunakan base 58

The screenshot shows a web application for decoding messages from Base 58. The main panel has fields for 'ALPHABET' (set to 123456789ABC...XYZabc...xyz (Bitcoin BTC)) and 'MESSAGE CHIFFRÉ PAR BASE 58' (containing the hex string ZGW9mAgck8zohQPm4DeKSaKYAFRft9nPpb88Hj7nWrDtPcgyS). Below the message field, there are options for 'FORMAT DES RÉSULTATS' (set to CHAINE DE CARACTÈRES IMPRIMABLES) and a preview area.

Flag : IDN_CTF{prototype_pollution_success}

JWT Token Manipulation

Deskripsi :

Flagnya Di Encode Dengan Encoder yang sama dengan bitcoin dan solana

**Author: Rafly Permana **

Lampiran : https://ctf.solusiber.com/web_101/lab4/

Solusi :

- Disini kita langsung masuk ke sources dan mencari flagnya dikarenakan flag terletak pada script
- Ditemukan code FgUreh9sJv91wCs9a98YnG7VDuumwf96zBUnieQzY
- Lakukan decoder menggunakan base 58



The screenshot shows a search interface for 'IDN_CTF{jwt_token_manipulated}'. The results section displays the flag.

Rechercher un outil

RECHERCHE SUR D'CODE PAR MOTS-CLÉS : Tapez par exemple 'sudoku'

PARCOURIR LA LISTE COMPLÈTE DES OUTILS

Résultats

IDN_CTF{jwt_token_manipulated}

BASE 58

DÉCHIFFREMENT DE LA BASE 58

ALPHABET 123456789ABC...XYZabc...xyz (Bitcoin BTC)

MESSAGE CHIFFRÉ PAR BASE 58 FgUr eh9s Jv91wCs9a98YnG7VDuumwf96zBUnieQzY

FORMAT DES RÉSULTATS CHAÎNE DE CARACTÈRES IMPRIMABLES (ASCII/UNICODE)

Flag : IDN_CTF{jwt_token_manipulated}

Client-Side Privilege Escalation

Deskripsi :

Flagnya Di Encode Dengan Encoder yang sama dengan bitcoin dan solana

**Author: Rafly Permana **

Lampiran : https://ctf.solusiber.com/web_101/lab5/

Solusi :

- Ubah role pada console menggunakan localStorage.setItem('user_role', 'admin');
- Ditemukan code
2DvT8boTciwZu4ZctauqBoqJaMKWk8xbK5mAmgPqCTjQ9NX2xGEggGHXFA
- Lakukan decoder menggunakan base 58

The screenshot shows a search interface for 'IDN_FLAG{client_side_privilege_escalation}'. The results section displays the flag.

Rechercher un outil

RECHERCHE SUR D'CODE PAR MOTS-CLÉS : Tapez par exemple 'tirage au'

PARCOURIR LA LISTE COMPLÈTE DES OUTILS

Résultats

IDN_FLAG{client_side_privilege_escalation}

BASE 58

DÉCHIFFREMENT DE LA BASE 58

ALPHABET 123456789ABC...XYZabc...xyz (Bitcoin BTC)

MESSAGE CHIFFRÉ PAR BASE 58 2DvT8boTciwZu4ZctauqBoqJaMKWk8xbK5mAmgPqCTjQ9NX2xGEggGHXFA

FORMAT DES RÉSULTATS CHAÎNE DE CARACTÈRES IMPRIMABLES (ASCII/UNICODE)

Flag : IDN_FLAG{client_side_privilege_escalation}



Timing Attack

Deskripsi :

Flagnya Di Encode Dengan Encoder yang sama dengan bitcoin dan solana

**Author: Rafly Permana **

Lampiran : https://ctf.solusiber.com/web_101/lab4/

Solusi :

- Disini kita langsung masuk ke sources dan menemukan passwordnya yaitu password123

Lab 6: Timing Attack

Guess the secret password. The slower the response, the closer your guess.

password123

Guess

Correct! Flag:
NmMm6LByWzRL5zYUYocFN2qt1Lv7WDhkiLf6zqN2mVLuA

- Lakukan decoder menggunakan base 58

BASE 58

Mathématiques > Arithmétique > Base 58

DÉCHIFFREMENT DE LA BASE 58

★ ALPHABET | 123456789ABC...XYZabc...xyz (Bitcoin BTC) ▾

★ MESSAGE CHIFFRÉ PAR BASE 58 ?

NmMm6LByWzRL5zYUYocFN2qt1Lv7WDhkiLf6zqN2mVLuA

★ FORMAT DES

★ CHAINE DE CARACTÈRES IMPRIMABLES

Rechercher un outil

★ RECHERCHE SUR D'CODE PAR MOTS-CLÉS :
Tapez par exemple 'tirage au'

★ PARCOURIR LA LISTE COMPLÈTE DES OUTILS

Résultats

IDN_CTF{timing_attack_successful}



Unsafe Deserialization

Deskripsi :

Flagnya Di Encode Dengan Encoder yang sama dengan bitcoin dan solana

**Author: Rafly Permana **

Lampiran : https://ctf.solusiber.com/web_101/lab4/

Solusi :

- Disini kita langsung masuk ke sources dan mencari flagnya dikarenakan flag terletak pada script
- Ditemukan code 4e9THmJfgagHkvXRC2T99EoKiSvisvU8PqSyvB3Fz3hnbKxJCNNeEYk
- Lakukan decoder menggunakan base 58

The screenshot shows a web application for decoding Base 58 messages. At the top, there's a decorative banner with the word 'D CODE'. Below it is a search bar labeled 'Rechercher un outil' with a placeholder 'Tapez par exemple l' tirage au' and a search icon. There's also a link 'PARCOURIR LA LISTE COMPLÈTE DES OUTILS'. The main area is titled 'Résultats' and displays the decoded message: 'IDN_CTF{unsafe_deserialization_executed}'. To the right, there's a sidebar titled 'BASE 58' with navigation links 'Mathématiques > Arithmétique > Base 58'. It shows the input message '4e9THmJfgagHkvXRC2T99EoKiSvisvU8PqSyvB3Fz3hnbKxJCNNeEYk' and two dropdown menus: 'ALPHABET' set to '123456789ABC...XYZabc...xyz (Bitcoin BTC)' and 'MESSAGE CHIFFRÉ PAR BASE 58' with a question mark icon. At the bottom, there are options for 'FORMAT DES RÉSULTATS' (radio button selected) and 'CHAINE DE CARACTÈRES IMPRIMABLES (ASCII/UNICODE)'.

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

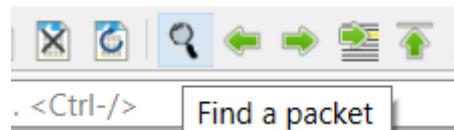
Lampiran : [incident response .pcapng](#)

Solusi :

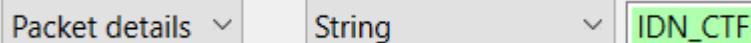
- Buka file pcap menggunakan wireshark.
- Lalu coba gunakan fitur “ **find a packet**”.



Capture Analyze Statistics



- Gunakan opsi “ packet Details ” dan “ string ” lalu cari text “ IDN_CTF ”



- Menemukan packet yang berisi text html yang berisikan “IDN_CTF” .

Packet details String IDN_CTF

No. Time Source Destination Protocol Length Info

99247 52.664456 192.168.10.244 TCP 74 80 + 46542 [SYN, ACK] Seq=1 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM TStamp=712163285 TSecr=597661114

99248 52.664459 192.168.10.244 192.168.10.153 TCP 74 [TCP Retransmission] 80 + 46542 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM TStamp=712163285 TSecr=597661114

99249 52.664631 192.168.10.153 192.168.10.244 TCP 66 46542 + 80 [ACK] Seq=1 Ack=1 Win=32128 Len=0 TStamp=597661114 TSecr=712163285

99250 52.664634 192.168.10.153 192.168.10.244 TCP 66 [TCP Dup, RCK 99249#1] 46542 + 80 [ACK] Seq=1 Ack=1 Win=32128 Len=0 TStamp=597661114 TSecr=712163285

99251 52.664749 192.168.10.153 192.168.10.244 HTTP 158 GET /yesterday.html HTTP/1.1

99252 52.664753 192.168.10.153 192.168.10.244 TCP 158 [TCP Retransmission] 46542 + 80 [PSH, ACK] Seq=1 Ack=1 Win=32128 Len=92 TStamp=597661114 TSecr=712163285

99253 52.664893 192.168.10.153 192.168.10.244 HTTP 208 GET /dashboard/es/cardinalauth HTTP/1.1

99254 52.664898 192.168.10.153 192.168.10.244 TCP 208 [TCP Retransmission] 46542 + 80 [PSH, ACK] Seq=11036 Ack=39286 Win=45824 Len=142 TStamp=597661114 TSecr=712163285

99255 52.665309 192.168.10.153 192.168.10.244 TCP 567 HTTP/1.1 299 OK (text/html)

99256 52.665309 192.168.10.153 192.168.10.244 TCP 567 [TCP Retransmission] 80 + 46542 [PSH, ACK] Seq=1 Ack=1 Win=65535 Len=501 TStamp=712163286 TSecr=597661114

99257 52.665484 192.168.10.153 192.168.10.244 TCP 66 46542 + 80 [ACK] Seq=93 Ack=502 Win=31872 Len=0 TStamp=597661115 TSecr=712163286

99258 52.665597 192.168.10.153 192.168.10.244 TCP 66 [TCP Dup, RCK 99257#1] 46542 + 80 [ACK] Seq=93 Ack=502 Win=31872 Len=0 TStamp=597661115 TSecr=712163286

99259 52.665598 192.168.10.153 192.168.10.244 HTTP 553 HTTP/1.1 404 Not Found (text/html)

99260 52.665789 192.168.10.244 192.168.10.153 TCP 551 [TCP Retransmission] 80 + 46528 [PSH, ACK] Seq=9286 Ack=11178 Win=64768 Len=485 TStamp=712163286 TSecr=597661114

99261 52.665813 192.168.10.153 192.168.10.244 TCP 66 46542 + 80 [PSH, ACK] Seq=93 Ack=502 Win=31872 Len=0 TStamp=597661115 TSecr=712163286

99262 52.665817 192.168.10.153 192.168.10.244 TCP 66 [TCP Retransmission] 46542 + 80 [PSH, ACK] Seq=93 Ack=502 Win=31872 Len=0 TStamp=597661115 TSecr=712163286

99263 52.665852 192.168.10.244 192.168.10.153 TCP 66 46542 [ACK] Seq=93 Ack=502 Win=31872 Len=0 TStamp=597661115

> Frame 99255: 567 bytes on wire (4596 bits), 567 bytes captured (4536 bits) on interface \Device\NPF_{6A7...}
> Ethernet II, Src: Intel_Bab2_72 (28:7f:c8:b2:72), Dst: Intel_Bab2_72 (28:7f:c8:b2:72)
> Internet Protocol Version 4, Src: 192.168.10.244, Dst: 192.168.10.153
> Transmission Control Protocol, Src Port: 80, Dst Port: 46542, Seq: 1, Ack: 93, Len: 501
> Hypertext Transfer Protocol
> Line-based text data: text/html (11 lines)

```

<!DOCTYPE html>
<html lang="en">
<head>
<meta charset="UTF-8" />
<meta name="viewport" content="width=device-width, initial-scale=1.0" />
<title>Dashboard - Admin</title>
</head>
<body>
<p>IDN_CTF{Re30N3C}</p>
</body>
</html>

```

0:0 0 39 65 63 32 22 0d 0a 41 63 63 65 79 74 2d 52 0eca2*-- Accept-R
0:0 0 61 6e 67 65 73 3a 20 62 79 74 65 73 0d 0a 43 6f anges: b ytes: Co
0:10 0 61 6e 67 65 73 3a 20 62 79 74 65 73 0d 0a 43 6f ntent-Le ngth: 24
0:110 0 6e 74 65 6d 74 2d 4c 65 6e 67 74 68 3a 20 32 3d
0:120 0 39 0d 0a 43 6e 74 65 6d 74 2d 58 79 70 65 3a
0:130 0 74 65 78 74 65 68 74 6d 6c 0d 0a 0d 0a 3c 23
0:140 0 40 0d 43 6c 2d 58 74 6d 6c 0d 0a 0d 0a 3c 23
0:150 0 68 74 6c 2c 61 6c 6e 67 74 22 65 6e 22 0d
0:160 0 09 3c 68 65 61 64 3e 0d 0a 09 09 3c 6d 65 74
0:170 0 61 20 63 68 61 72 73 65 74 3d 22 55 54 46 2d 38
0:180 0 22 20 2f 3d 0d 0a 09 09 3c 6d 65 74 61 20 6e 61
0:190 0 6d 65 3d 22 76 65 77 70 6f 72 24 22 20 63 6f
0:1a0 0 6d 65 3d 22 76 65 77 70 6f 72 24 22 20 63 6f
0:1b0 0 69 63 66 2d 77 69 64 74 68 2c 20 69 6e 69
0:1c0 0 61 6c 2d 73 63 61 6c 65 3d 31 33 30 22 20 2f 3a
0:1d0 0 09 09 3c 74 69 74 6c 65 3e 44 61 73 68 62
0:1e0 0 6f 61 72 64 20 2d 41 64 6d 69 3c 74 69
0:1f0 0 74 6c 73 63 6d 0a 09 3c 2f 68 65 61 64 3e 0d 0a
0:200 0 6d 65 3d 22 76 65 77 70 6f 72 24 22 20 63 6f
0:210 0 44 6c 73 63 6d 0a 09 3c 2f 68 65 61 64 3e 0d 0a
0:220 0 70 3a 0d 0a 09 3c 2f 62 6d 64 79 3e 0d 0a 3c 2f
0:230 0 68 74 6d 6c 3e 0d 0a

Packets: 396599 Profile: Default

Flag : IDN_CTF{Re30N3C}

Log Analysis 2

Deskripsi :

awas, hati-hati, pelan-pelan, ada

Format Flag : IDN_CTF{jawaban}

Author : Aditya Firman Nugroho

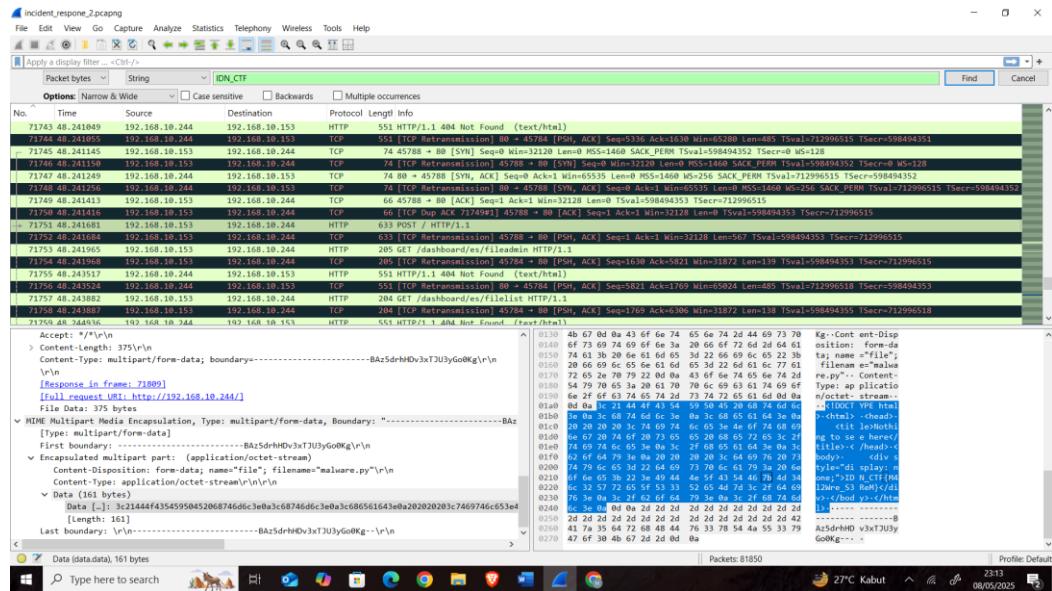
Lampiran : [incident response 2.pcapng](#)

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\access.log - Notepad++
File Edit Search View Encoding Language Settings Tools Macro Run Plugins Window ?
File Open Save Save As Find Replace Go To Encoding Tools Plugins Window Help
accesslog > [x]
changes.log extractor hidden.log accesslog > [x]
848 192.168.18.6 - - [27/Apr/2025:12:55:29 +0000] "GET /change password HTTP/1.1" 404 436 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"
849 192.168.18.6 - - [27/Apr/2025:12:55:29 +0000] "GET /changepw HTTP/1.1" 404 436 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"
850 192.168.18.6 - - [27/Apr/2025:12:55:29 +0000] "GET /changepw HTTP/1.1" 404 436 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"
851 192.168.18.6 - - [27/Apr/2025:12:55:29 +0000] "GET /change HTTP/1.1" 404 436 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"
852 192.168.18.6 - - [27/Apr/2025:12:55:29 +0000] "GET /charge HTTP/1.1" 404 436 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"
853 192.168.18.6 - - [27/Apr/2025:12:55:29 +0000] "GET /chart HTTP/1.1" 404 436 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"
854 192.168.18.6 - - [27/Apr/2025:12:55:29 +0000] "GET /charts HTTP/1.1" 404 436 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"
855 192.168.18.6 - - [27/Apr/2025:12:55:29 +0000] "GET /chart HTTP/1.1" 404 436 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"
856 192.168.18.6 - - [27/Apr/2025:12:55:29 +0000] "GET /charts HTTP/1.1" 404 436 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"
857 192.168.18.6 - - [27/Apr/2025:12:55:29 +0000] "GET /chat HTTP/1.1" 404 436 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"
858 192.168.18.6 - - [27/Apr/2025:12:55:29 +0000] "GET /chats HTTP/1.1" 404 436 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"
859 192.168.18.6 - - [27/Apr/2025:12:55:29 +0000] "GET /checkin HTTP/1.1" 404 436 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"
860 192.168.18.6 - - [27/Apr/2025:12:55:29 +0000] "GET /checking HTTP/1.1" 404 436 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"
861 192.168.18.6 - - [27/Apr/2025:12:55:29 +0000] "GET /checkout HTTP/1.1" 404 436 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"
862 192.168.18.6 - - [27/Apr/2025:12:55:29 +0000] "GET /checkout iclear HTTP/1.1" 404 436 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"
863 192.168.18.6 - - [27/Apr/2025:12:55:31 +0000] "POST /upload/malware.py HTTP/1.1" 200 4313 "-" "curl/8.12.1"
864 192.168.18.6 - - [27/Apr/2025:12:55:33 +0000] "GET /randomfile HTTP/1.1" 404 436 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"
865 192.168.18.6 - - [27/Apr/2025:12:55:33 +0000] "GET /frand2 HTTP/1.1" 404 436 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"
866 192.168.18.6 - - [27/Apr/2025:12:55:33 +0000] "GET /.bash_history HTTP/1.1" 404 436 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"
867 192.168.18.6 - - [27/Apr/2025:12:55:33 +0000] "GET /.baehir HTTP/1.1" 404 436 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"
868 192.168.18.6 - - [27/Apr/2025:12:55:33 +0000] "GET /.bashrc HTTP/1.1" 404 436 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"
869 192.168.18.6 - - [27/Apr/2025:12:55:33 +0000] "GET /.config HTTP/1.1" 404 436 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"
870 192.168.18.6 - - [27/Apr/2025:12:55:33 +0000] "GET /.cova HTTP/1.1" 404 436 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"
871 192.168.18.6 - - [27/Apr/2025:12:55:33 +0000] "GET /.cvsignore HTTP/1.1" 404 436 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"
872 192.168.18.6 - - [27/Apr/2025:12:55:33 +0000] "GET /.forward HTTP/1.1" 404 436 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"
873 192.168.18.6 - - [27/Apr/2025:12:55:33 +0000] "GET /.git/HEAD HTTP/1.1" 404 436 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"
874 192.168.18.6 - - [27/Apr/2025:12:55:33 +0000] "GET /.history HTTP/1.1" 404 436 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"
875 192.168.18.6 - - [27/Apr/2025:12:55:33 +0000] "GET /.hta HTTP/1.1" 403 439 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"
876 192.168.18.6 - - [27/Apr/2025:12:55:33 +0000] "GET /.hta HTTP/1.1" 403 439 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"
877 192.168.18.6 - - [27/Apr/2025:12:55:33 +0000] "GET /.htaccess HTTP/1.1" 404 436 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"
878 192.168.18.6 - - [27/Apr/2025:12:55:33 +0000] "GET /.htaccess HTTP/1.1" 404 439 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"
879 192.168.18.6 - - [27/Apr/2025:12:55:33 +0000] "GET /.htpasswd HTTP/1.1" 403 439 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"
880 192.168.18.6 - - [27/Apr/2025:12:55:33 +0000] "GET /.htpasswd MDW7/1.1" 403 439 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"
881 192.168.18.6 - - [27/Apr/2025:12:55:33 +0000] "GET /.listind HTTP/1.1" 404 436 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"

Search results - (3 hits)
Search "200" (3 hits in 1 file of 1 searched) [Normal: Case/Word]
C:\Users\Kurniawan\Downloads\access.log (3 hits)
Line 173: 192.168.18.6 - - [27/Apr/2025:12:55:29 +0000] "GET /200 HTTP/1.1" 404 436 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"
Line 863: 192.168.18.6 - - [27/Apr/2025:12:55:31 +0000] "POST /upload/malware.py HTTP/1.1" 200 4313 "-" "curl/8.12.1"
Line 1036: 192.168.18.6 - - [27/Apr/2025:12:55:33 +0000] "GET /200 HTTP/1.1" 404 436 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"

Normal text file
Type here to search 26°C Berawan 025 09/05/2025
length: 250.762 lines: 1.862 ln: 863 Col: 108 Sel: 60 | F INS

```

Flag : IDN_CTF{malware.py}

Log Analysis 4

Deskripsi :

analisis 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.

```

Search results - (1 hit)
Search "accepted" (1 hit in 1 file of 1 searched) [Normal: Word]
C:\Users\Kurniawan\Downloads\auth.log (1 hit)
Line 256: Apr 27 13:05:10 test sshd[19014]: Accepted password for ghyss from 192.168.18.6 port 52320 ssh2
Search "valid" (0 hits in 0 files of 1 searched) [Normal: Word]

```

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



The screenshot shows the Notepad++ application window with the file 'auth.log' open. The log file contains several entries from an SSH server, mostly showing failed password attempts from various invalid users like 'football', 'carlos', 'angel', etc., from IP 192.168.18.6. There are also successful logins for a user named 'ghxyss'. The last few entries show a session opening and closing for this user.

```
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
262 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.

The screenshot shows the Wireshark interface with a single captured packet selected. The packet details pane shows a request from source IP 192.168.18.230 to destination IP 192.168.18.6. The protocol is HTTP, and the length is 647 bytes. The info column shows the response code 301 Moved Permanently (text/html). A display filter is applied in the top bar: `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**.

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 mengeksplorasi endpoint dengan teknik SQL Injection, menghasilkan internal server error. Apa nama file yang ditargetkan dalam eksplorasi tersebut?

IDN_CTF{jawaban}

Author: Rafly Permana

Lampiran : [log1.txt](#)

Solusi :

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

```

1. 198.10.15. - - [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. 192.168.10.23. - - [21/Apr/2024:08:12:42 +0700] "GET /index.php HTTP/1.1" 403 720 "Mozilla/5.0 (Windows NT 10.0; Win64; x64)" "curl/7.68.0"
5. 10.0.0.9. - - [21/Apr/2024:08:12:42 +0700] "GET /index.php 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/2024:08:13:03 +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/2024:08:15:15 +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 HTTP/1.1" 200 5432 "-" "Mozilla/5.0 (X11; Linux x86_64)" "curl/7.68.0"
12. 198.51.100.23. - - [21/Apr/2024:08:17:22 +0700] "GET /config.php HTTP/1.1" 404 213 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64)"
13. 192.168.10.15. - - [21/Apr/2024:08:17:22 +0700] "GET /admin/dashboard HTTP/1.1" 403 701 "Mozilla/5.0 (Windows NT 10.0; Win64; x64)"
14. 192.168.10.20. - - [21/Apr/2024:08:17:22 +0700] "GET /index.php HTTP/1.1" 403 704 "Mozilla/5.0 (Windows NT 10.0; Win64; x64)"
15. 10.0.0.9. - - [21/Apr/2024:08:18:50 +0700] "GET /datafile/ HTTP/1.1" 403 279 "http://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" $00 1234 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64)"
18. 192.168.10.15. - - [21/Apr/2024:08:20:13 +0700] "GET /admin.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/2024:08:21:11 +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/2024:08:22:47 +0700] "GET /wp-admin/ HTTP/1.1" 404 303 "-" "Mozilla/5.0 (X11; Linux x86_64)"
23. 198.51.100.23. - - [21/Apr/2024:08:22:47 +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/2024:08:22:47 +0700] "GET /admin/index.php HTTP/1.1" 403 717 "-" "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" 403 934 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64)"
26. 10.0.0.9. - - [21/Apr/2024:08:23:42 +0700] "GET /datafile/ HTTP/1.1" 403 278 "http://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/2024:08:27:11 +0700] "GET /search?q=<script>evil_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" 403 726 "-" "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]
C:\Users\Kurniawan\Downloads\log1.txt (5 hits)

Line 17: 198.51.100.23. - - [21/Apr/2024:08:19:45 +0700] "GET /rini.php?id=1 UNION SELECT password FROM users HTTP/1.1" $00 1234 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64)"
Line 25: 198.51.100.45. - - [21/Apr/2024:08:19:45 +0700] "POST /upload.php HTTP/1.1" 500 934 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64)"
Line 47: 198.51.100.23. - - [21/Apr/2024:08:34:59 +0700] "GET /search?q=<?php?eval($_POST['?']);?> HTTP/1.1" $00 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 80: 198.51.100.45. - - [21/Apr/2024:08:40:12 +0700] "GET /index.php?fid=105 UNION SELECT username, password FROM users-- HTTP/1.1" $00 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.

```
C:\Users\Kurniawan\Downloads\log2.txt - Notepad++
File Edit Search View Encoding Language Settings Tools Macro Run Plugins Window ?

log2.txt
1 203.0.114.10 - [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)"
1 198.51.101.15 - [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)"
1 10.10.1.10 - [22/Apr/2024:09:20:12 +0700] "GET /admin/dashboard HTTP/1.1" 403 710 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64)"
1 198.51.101.23 - [22/Apr/2024:09:20:50 +0700] "POST /xampp/php HTTP/1.1" 404 128 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64)"
1 192.168.100.5 - [22/Apr/2024:09:21:15 +0700] "GET /api/v2/data/ide/./././.etc/passwd HTTP/1.1" 403 280 "-" "curl/7.70.0"
1 203.0.114.10 - [22/Apr/2024:09:21:15 +0700] "GET /uploads/./././.etc/passwd HTTP/1.1" 403 220 "-" "Mozilla/5.0 (X11; Linux x86_64)"
1 198.51.101.15 - [22/Apr/2024:09:22:21 +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)"
1 10.10.1.10 - [22/Apr/2024:09:22:55 +0700] "GET /admin.php HTTP/1.1" 403 715 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64)"
1 198.51.101.23 - [22/Apr/2024:09:23:30 +0700] "POST /login.php HTTP/1.1" 200 910 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64)" "GET /index.php HTTP/1.1" 200 1250 "-" "curl/7.70.0"
1 198.168.100.5 - [22/Apr/2024:09:24:05 +0700] "GET /index.php?user=guest HTTP/1.1" 200 1250 "-" "curl/7.70.0"
1 10.10.1.10 - [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)"
1 203.0.114.10 - [22/Apr/2024:09:25:12 +0700] "GET /wp-admin HTTP/1.1" 403 305 "-" "Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/118.0.604.124 Safari/537.36"
1 198.51.101.15 - [22/Apr/2024:09:25:45 +0700] "GET /backup.zip HTTP/1.1" 404 185 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64)"
1 10.10.1.10 - [22/Apr/2024:09:26:20 +0700] "GET /admin HTTP/1.1" 403 715 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64)"
1 198.51.101.23 - [22/Apr/2024:09:26:55 +0700] "POST /upload.php HTTP/1.1" 500 95 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64)"
1 192.168.100.5 - [22/Apr/2024:09:27:25 +0700] "GET /api/v2/data/ide/./././.etc/passwd HTTP/1.1" 403 280 "-" "curl/7.70.0"
1 203.0.114.10 - [22/Apr/2024:09:27:58 +0700] "GET /admin/config HTTP/1.1" 403 705 "-" "Mozilla/5.0 (X11; Linux x86_64)"
1 198.51.101.15 - [22/Apr/2024:09:28:21 +0700] "GET /admin/config HTTP/1.1" 404 225 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64)"
1 10.10.1.10 - [22/Apr/2024:09:28:56 +0700] "GET /wp-admin/administrator/index.php HTTP/1.1" 200 1240 "-" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7)"
1 203.0.114.10 - [22/Apr/2024:09:29:33 +0700] "GET /login.php HTTP/1.1" 200 1350 "-" "Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/118.0.604.124 Safari/537.36"
1 198.51.101.23 - [22/Apr/2024:09:30:04 +0700] "POST /wp-login.php HTTP/1.1" 200 1300 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64)"
1 192.168.100.5 - [22/Apr/2024:09:30:33 +0700] "GET /search?q=script%2fevil_code%2fscript HTTP/1.1" 200 1310 "-" "curl/7.70.0"
1 10.10.1.10 - [22/Apr/2024:09:31:05 +0700] "GET /admin/delete.php HTTP/1.1" 403 275 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64)"
1 198.51.101.15 - [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)"
1 203.0.114.10 - [22/Apr/2024:09:32:05 +0700] "GET /wp-config.php HTTP/1.1" 404 145 "-" "Mozilla/5.0 (X11; Linux x86_64)"
1 36.10.10.1.2 - [22/Apr/2024:09:32:35 +0700] "GET /login.php?redirect=2&admin HTTP/1.1" 200 1550 "-" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7)"
1 198.51.101.23 - [22/Apr/2024:09:33:09 +0700] "POST /administrator/index.php HTTP/1.1" 403 905 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64)"
1 192.168.100.5 - [22/Apr/2024:09:33:38 +0700] "GET /index.php?user=guest HTTP/1.1" 200 1350 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64)"
1 198.51.101.15 - [22/Apr/2024:09:34:01 +0700] "GET /dashboard.php HTTP/1.1" 404 708 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64)"
1 201.0.114.10 - [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)"
Line 1: 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"
Line 10: 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)"
Line 26: 192.168.100.5 - [22/Apr/2024:09:27:26 +0700] "GET /api/v2/datafile/./././.etc/passwd HTTP/1.1" 403 280 "-" "curl/7.70.0"
Line 42: 192.168.100.20 - [22/Apr/2024:09:35:45 +0700] "GET /test.php?file=././././.etc/shadow HTTP/1.1" 403 282 "-" "curl/7.70.0"
Line 46: 10.10.10.1.10 - [22/Apr/2024:09:38:55 +0700] "GET /test.php?query=././././.etc/passwd HTTP/1.1" 403 282 "-" "curl/7.70.0"
Line 60: 192.168.100.5 - [22/Apr/2024:09:48:50 +0700] "GET /test.php?param=././././.etc/shadow HTTP/1.1" 403 282 "-" "curl/7.70.0"

Search results - (23 hits)
Search ? - (23 hits in 1 file of 1 searched) [Normal]
C:\Users\Kurniawan\Downloads\log2.txt - (23 hits)

Line 1: 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"
Line 10: 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)"
Line 26: 192.168.100.5 - [22/Apr/2024:09:27:26 +0700] "GET /api/v2/datafile/./././.etc/passwd HTTP/1.1" 403 280 "-" "curl/7.70.0"
Line 42: 192.168.100.20 - [22/Apr/2024:09:35:45 +0700] "GET /test.php?file=././././.etc/shadow HTTP/1.1" 403 282 "-" "curl/7.70.0"
Line 46: 10.10.10.1.10 - [22/Apr/2024:09:38:55 +0700] "GET /test.php?query=././././.etc/passwd HTTP/1.1" 403 282 "-" "curl/7.70.0"
Line 60: 192.168.100.5 - [22/Apr/2024:09:48:50 +0700] "GET /test.php?param=././././.etc/shadow HTTP/1.1" 403 282 "-" "curl/7.70.0"
```



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]
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 3 : Apr 22 12:01:25 server1 sshd[2345]: Failed password for invalid user root from 203.0.113.45 port 60223 ssh2
ne 4 : Apr 22 12:01:35 server1 sshd[2345]: Failed password for invalid user test from 203.0.113.45 port 60224 ssh2
ne 5 : Apr 22 12:01:40 server1 sshd[2347]: Accepted password for user1 from 198.51.100.23 port 51432 ssh2
ne 6 : Apr 22 12:01:42 server1 sshd[2347]: pam_unix(sshd:session): session opened for user user1 by (uid=0)
ne 7 : Apr 22 12:02:01 server1 sudo:  user1 : TTY=pts/1 ; FWD=/home/user1 ; USER=root ; COMMAND=/bin/cat /etc/passwd
ne 8 : Apr 22 12:02:05 server1 sudo: pam_unix(sudo:session): session opened for user root by user1(uid=0)
ne 9 : Apr 22 12:02:07 server1 sudo: pam_unix(sudo:session): session closed for user root
ne 10 : Apr 22 12:02:07 server1 sudo:  user1 : TTY=pts/1 ; FWD=/home/user1 ; USER=root ; COMMAND=/bin/cat /etc/passwd
ne 11 : Apr 22 12:02:07 server1 sudo: pam_unix(sudo:session): session opened for user root 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 12:01:25 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 12:01:25 server1 sshd[2345]: Failed password for invalid user root from 203.0.113.45 port 60223 ssh2
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 sshd[2345]: [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
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 sshd[2347]: [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
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 ; FWD=/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 root 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 PRO
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 12:02:30 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=TCP/HTTP
19. Apr 22 12:03:08 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=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=60227 ssh2
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=192.0.2.50 DST=60228 ssh2
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 ; FWD=/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 12:04:18 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 PRO
31. Apr 22 12:15:35 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 PRO

Search results : (28 hits)
"user" (28 hits in 1 file of 1 searched) [Normal]
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 3 : Apr 22 12:01:35 server1 sshd[2345]: Failed password for invalid user root from 203.0.113.45 port 60223 ssh2
ne 4 : Apr 22 12:01:35 server1 sshd[2345]: Failed password for invalid user test from 203.0.113.45 port 60224 ssh2
ne 5 : Apr 22 12:01:40 server1 sshd[2347]: Accepted password for user1 from 198.51.100.23 port 51432 ssh2
ne 6 : Apr 22 12:01:42 server1 sshd[2347]: pam_unix(sshd:session): session opened for user user1 by (uid=0)
ne 7 : Apr 22 12:02:01 server1 sudo:  user1 : TTY=pts/1 ; FWD=/home/user1 ; USER=root ; COMMAND=/bin/cat /etc/passwd
ne 8 : Apr 22 12:02:05 server1 sudo: pam_unix(sudo:session): session opened for user root by user1(uid=0)
ne 9 : 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}

Forensic

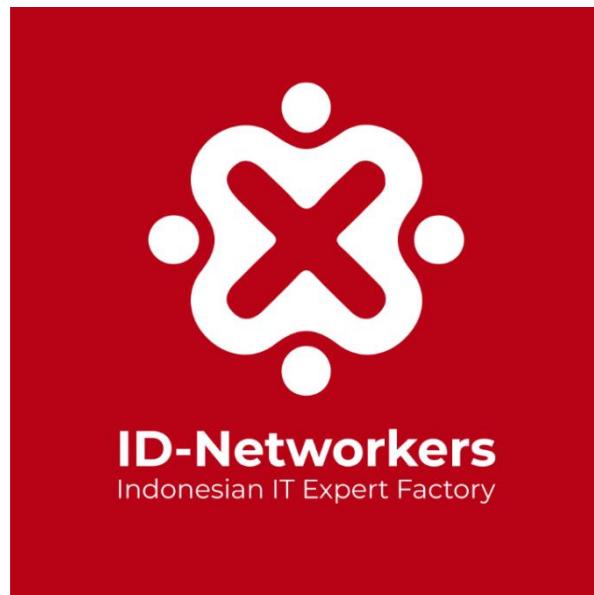
Forensic 1

Deskripsi :

ngomongin crypto, selain encryption itu ada apa lagi ya ?

material.png

Author: Aditya Firman Nugroho



Lampiran : Material.png

Solusi :

- Download file Material tersebut
- untuk melihat, memodifikasi, dan menghapus metadata (data informasi tentang file) dalam berbagai jenis file seperti gambar
- Cari di kolom Comment pada data foto nya

Flag : IDN_CTF{W0W_wh4T_K03NC1D3CE}

Forensic 2

Deskripsi :

Qris

2 kali

Author : Mohamad Fattyr

Solusi :

- Scan Kode QRIS menggunakan aplikasi Scanner
- Akan tampil kode U1VST1gwWk1RVWQ3VmOU04xOWxORk0zWDFJaE9VaFVmUT09



- Segera decode menggunakan base decode 64
- Akan tampil kode lagi SUROX0ZMQUd7VjNSN19lNFM3X1lhOUhUfQ==
- Kemudian ulangi decode lagi dan akan tampil Flag nya

Flag : IDN_FLAG{V3R7_e4S7_R!9HT}