

Infrastructure Hardening/Patching
and Digital Forensics
SMK Negeri 7 Semarang



Muhammad Zaky Adzkiya
Rafi Nur Ardiansyah

Memory Forensics

Diberi sebuah memory file. Untuk menganalisa memory dump biasanya orang menggunakan volatility. Karena volatility sudah langsung support windows, kita tidak perlu mengcreate profile sendiri. Kita hanya perlu menjalankan perintah kdbgscan untuk mendapatkan suggestion profile.

```
PS C:\Users\rafim\Desktop\tools\volatility_2.6_win64_standalone> .\vol.exe -f ..\LKS.vmem kdbgscan
Volatility Foundation Volatility Framework 2.6
*****
Instantiating KDBG using: C:\Users\rafim\Desktop\tools\LKS.vmem WinXPSP2x86 (5.1.0 32bit)
Offset (P) : 0x2bfc120
KDBG owner tag check : True
Profile suggestion (KDBGHeader): Win7SP1x64
PsActiveProcessHead : 0x2c35940
PsLoadedModuleList : 0x2c53c90
KernelBase : 0xfffff80002a19000
```

1. Shoulder Surfing

Untuk menemukan password di memory dump windows biasanya kita bisa menggunakan 2 perintah pada volatility yaitu lsadump atau hashdump. Menggunakan perintah lsadump untuk nge dump (decrypted) LSA secrets dari registry. Namun tidak ditemukan password yang sudah di decrypt, lalu menggunakan perintah hashdump untuk dump password hash.

```

Command line : ??[C:\Windows\system32\conhost.exe "82752783919502252562354351821021778553-1750517608-8446107551435525613485839613
PS C:\Users\rafim\Desktop\tools\volatility_2.6_win64_standalone> .\vol.exe -f ..\LKSN.vmem --profile=Win7SP1x64 lsadump
Volatility Foundation Volatility Framework 2.6
DefaultPassword
0x00000000 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
0x00000010 70 90 af d4 e9 f9 61 6d 14 39 70 c6 6a ba b1 49 p....am.9p.j..I

DPAPI_SYSTEM
0x00000000 2c 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
0x00000010 01 00 00 00 69 21 a3 6c b4 05 1d 86 75 8d 99 52 ...i.l...u..R
0x00000020 9c a3 d3 73 5f 2c d6 2c 4c 8b 3d c2 c8 8d 73 45 ...s...L=...SE
0x00000030 e3 4f 91 35 c4 88 11 cc a2 c3 2c d7 00 00 00 00 .0.5.....

PS C:\Users\rafim\Desktop\tools\volatility_2.6_win64_standalone> .\vol.exe -f ..\LKSN.vmem --profile=Win7SP1x64 hashdump
Volatility Foundation Volatility Framework 2.6
Administrator:500:aad3b435b51404eeaad3b435b51404ee:10eca58175d4228ece151e287086e824:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cf0e0d16ae931b73c50d7e0c089c0:::
lksn:1001:aad3b435b51404eeaad3b435b51404ee:6880c767cb7049dbd8d1234925cabb6d:::
HomeGroupUser$:1002:aad3b435b51404eeaad3b435b51404ee:c78a69028265ae8f10aa485e8f19d0bb:::
PS C:\Users\rafim\Desktop\tools\volatility_2.6_win64_standalone>

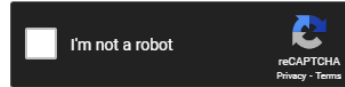
```

Terlihat terdapat user lksn beserta hash password nya, lalu crack password (disini menggunakan tools online). Ternyata dapat ketemu karena menggunakan password yang common.

Free Password Hash Cracker

Enter up to 20 non-salted hashes, one per line:

6880c767cb7049dbd8d1234925cabb6d



Supports: LM, NTLM, md2, md4, md5, md5(md5_hex), md5-half, sha1, sha224, sha256, sha384, sha512, ripeMD160, whirlpool, MySQL 4.1+ (sha1 sha1_bin), QubesV3.1BackupDefaults

Hash	Type	Result
6880c767cb7049dbd8d1234925cabb6d	NTLM	happybirthday

Color Codes: **Green:** Exact match, **Yellow:** Partial match, **Red:** Not found.

Flag **happybirthday**

2. Awal Mula

Di soal ini, kita harus mencari malicious program yang berjalan. Dengan menganalisa perintah cmdscan untuk mengekstrak command history, disini saya mencurigai aplikasi **softwareupdateyey.exe** karena dari nama file nya sudah suspicious. Lalu menggunakan perintah cmdline untuk menampilkan command line argument serta PID pada program

```
PS C:\Users\rafim\Desktop\tools\volatility_2.6_win64_standalone> .\vol.exe -f ..\LKSN.vmem --profile=Win7SP1x64 cmdscan
Volatility Foundation Volatility Framework 2.6
*****
CommandProcess: conhost.exe Pid: 1740
CommandHistory: 0x26d230 Application: cmd.exe Flags: Allocated, Reset
CommandCount: 1 LastAdded: 0 LastDisplayed: 0
FirstCommand: 0 CommandCountMax: 50
ProcessHandle: 0x60
Cmd #0 @ 0x269ab0: .\softwareupdateyey.exe
Cmd #15 @ 0x230158: &
Cmd #16 @ 0x26c3a0: &
*****
CommandProcess: conhost.exe Pid: 1740
CommandHistory: 0x26d560 Application: softwareupdateyey.exe Flags: Allocated
CommandCount: 0 LastAdded: -1 LastDisplayed: -1
FirstCommand: 0 CommandCountMax: 50
ProcessHandle: 0x58
PS C:\Users\rafim\Desktop\tools\volatility_2.6_win64_standalone> _
```

```
*****
softwareupdate pid: 3004
Command line : .\softwareupdateyey.exe
*****
dllhost.exe pid: 1536
```

Flag **3004**

3. Indikator Penyusupan (Bagian 1)

Di bagian ini saya tidak menemukan flag nya, sed 😞. Tapi berikut adalah yang kami dapatkan

```

C:\Users\lksn\AppData\Local\Microsoft\Windows\WebCache\
C:\Users\lksn\AppData\Local\Microsoft\Windows\WebCache\
C:\Users\Public\Music\Sample Music\Kalimba.mp3
C:\Users\Public\Music\Sample Music\Sleep Away.mp3
C:\Users\Public\Music\Sample Music\Maid with the Flaxen Hair.mp3
C:\Users\Public\Pictures\Sample Pictures\Chrysanthemum.jpg
C:\Users\Public\Pictures\Sample Pictures\Desert.jpg
C:\Users\Public\Pictures\Sample Pictures\Hydrangeas.jpg
C:\Users\Public\Pictures\Sample Pictures\Jellyfish.jpg
C:\Users\Public\Pictures\Sample Pictures\Koala.jpg
C:\Users\Public\Pictures\Sample Pictures\Lighthouse.jpg
C:\Users\Public\Pictures\Sample Pictures\Penguins.jpg
C:\Users\Public\Pictures\Sample Pictures\Tulips.jpg
C:\Users\Public\Recorded TV\Sample Media\win7_scenic-demoshort_raw.wtv
C:\Users\Public\Videos\Sample Videos\Wildlife.wmv
1C:\Users\lksn\AppData\Local\Microsoft\Windows\WebCache\
C:\Users\lksn\AppData\Local\Microsoft\Windows\WebCache\
1C:\Users\lksn\AppData\Local\Microsoft\Windows\WebCache\
1C:\Users\lksn\AppData\Local\Microsoft\Windows\WebCache\
C:\Users\lksn\AppData\Local\Microsoft\Windows\WebCache\
(kyruuu DESKTOP-B0VER0Q): [/mnt/c/Users/rafim/Desktop/tools/volatility_2.6_win64_standalone]
strings 3004.dmp | grep C:\\\\

```

sha 512 executable file (bisa pake procdump untuk mendapatkannya)

**0ad04f2eb3f8dcabe15bb19ada6c5165d129126b958a91c397350d954c617b65917c8c6e9759
2508b7988437810c396a6fd680607ae2b7481bbb172407867016**

Path tujuan (asumsi)

curr

C:\Users\lksn\AppData\Local\Temp

C:\ProgramData\Microsoft\Windows\WER\Temp

C:\Users\lksn\AppData\Local\Temp

C:\Users\lksn\AppData\Local\Microsoft\Windows\WebCache

C:\Windows\System32

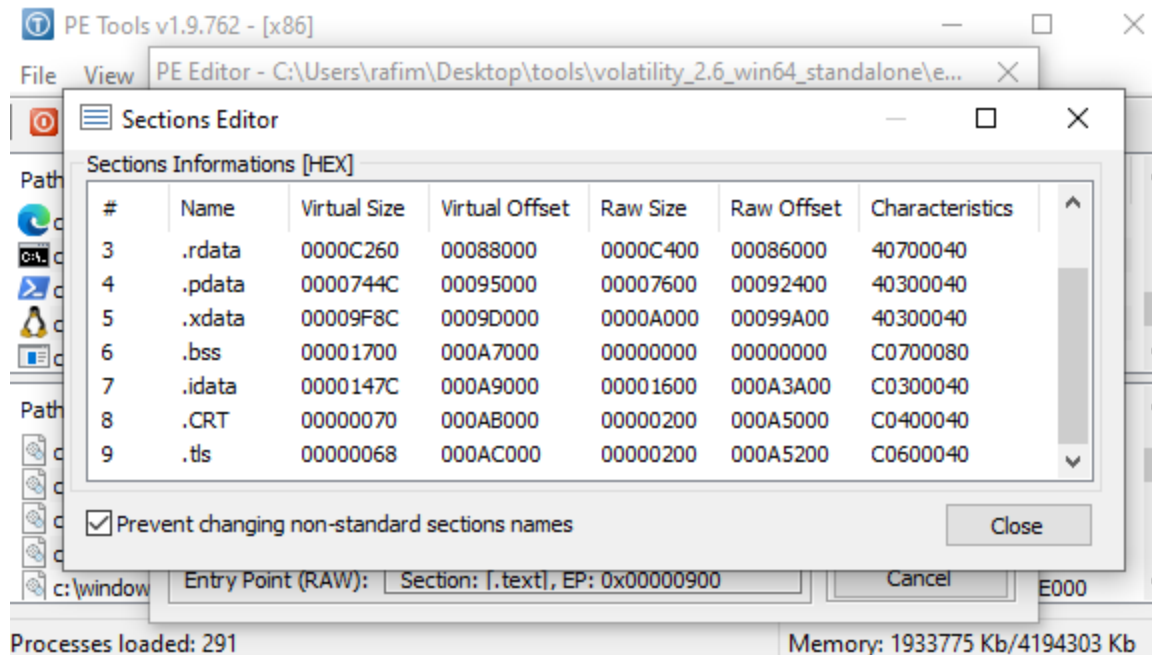
C:\Windows\System32\spp\store\2.0

C:\Windows\System32\spp\store\2.0\cache

4. Indikator Penyusupan (Bagian 2)

Jadi di soal ini di suruh menghitung entropy dan section pada Program Executable (PE). Entropy itu tingkat kerandaman untuk informasi digital. Setelah mencari kesana kemari saya menemukan tools yang luar biasa [petoolse/petools: PE Tools - Portable executable \(PE\) manipulation toolkit \(github.com\)](#). Tools tersebut berfungsi untuk menganalisa Program Executable file.

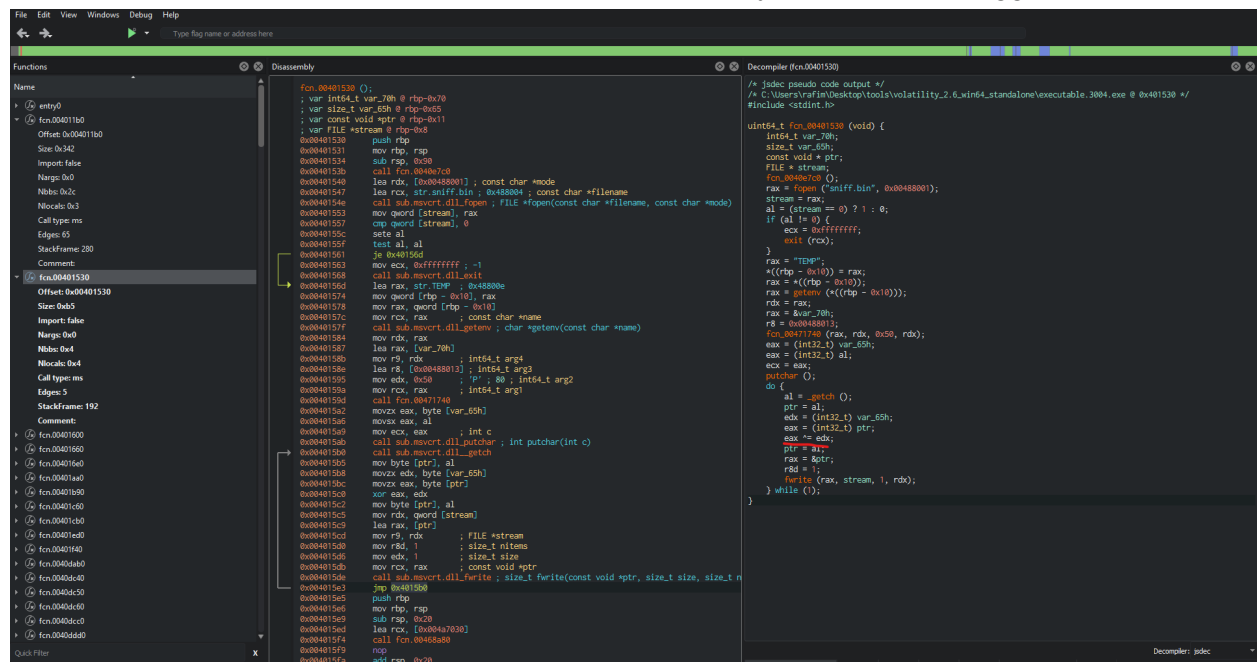
Ternyata entropy file tersebut rata rata 1.936782, karena di suruh dibulatkan maka dapatlah **1.94**



Flag 1.94_9

5. Finale

Untuk mengetahui apa yang dilakukan program untuk mengenkripsi, saya mereverse program terlebih dahulu. Setelah itu dapat diketahui bahwa file hanya di enkripsi menggunakan **xor**.



Tanpa berpikir panjang saya langsung berasumsi hanya di kunci dengan 1 bytes saja dan langsung mencoba membruteforce kuncinya

```

PS C:\Users\rafim\Downloads> ipython
Python 3.10.8 (tags/v3.10.8:aaaf517, Oct 11 2022, 16:50:30) [MSC v.1933 64 bit (AMD64)]
Type 'copyright', 'credits' or 'license' for more information
IPython 8.4.0 -- An enhanced Interactive Python. Type '?' for help.

In [1]: enc = open('sniff.bin', 'rb').read()

In [2]: enc
Out[2]: b'$\x12\x1bS\x18\x12\x1f\x1a\x12\x1dS\x07\x16\x1f\x12\x1bS\x11\x16\x01\x1b\x12 \x1a\x1fS\x1e\x16\x1d\n\x16\x1f\x16 \x12\x1a\x18\x12\x1dS\x10\x1b\x12\x1f\x1f\x16\x1d\x14\x16S\x15\x1c\x01\x16\x1d \x1a\x10S\x1a\x1d\x1a]S89\x12\x1e\x1aS \x03\x1a\x18\x1a\x01S\x11\x12\x1b\x04\x12S\x18\x12\x1f\x1a\x12\x1dS \x06\x17\x12\x1bS\x1e\x16\x1d\x19\x12\x17\x1aS\x03\x16 \x16\x01\x07\x12S78 =S\n\x12\x1d\x14S\x11\x12\x1a\x18]S<\x1f\x16\x1bS\x18\x12\x01\x16\x1d\x12S\x1a\x07\x06_S\x18\x12\x1e\x1aS\x12\x18\x12\x1dS\x11\x16\x01\x1a\x18\x12\x1dS\x03\x12 \x04\x1c\x01\x17S\n\x12\x1d\x14S\x18\x12\x1f\x1a\x12\x1dS\x10\x12\x01\x1a_S\n\x12\x18\x1d\x1aS78 =\x08\x03GwW\x04C\x01\x17,\x18\x1c\x18,\x11@\x14\x1a\x1d\x1aL,\x07\x12\x03\x1a,\x12\x1e\x12\x1d,\x18G\x1d\x1dL\x0e~'

In [3]: from pwn import xor
...: for i in range(256):
...:     print(xor(enc,i))\
...:

[*] Checking for new versions of pwntools
To disable this functionality, set the contents of C:\Users\rafim\.cache\pwntools-cache-3.10\update to 'never' (old way).
Or add the following lines to ~/.pwn.conf or ~/.config/pwn.conf (or /etc/pwn.conf system-wide):
[update]
interval=never
[*] You have the latest version of Pwntools (4.8.0)

```

Dan dapat flag nya.

```

b'Wah kalian telah berhasil menyelesaikan challenge forensic ini. KJami pikir bahwa kalian sudah menjadi peserta LKSN yang baik. Oleh karena itu, kami akan berikan password yang kalian cari, yakni LKSN{p4$$w0rd_kok_b3gini?_tapi_aman_k4nn?}\n'

```

Flag LKSN{p4\$\$w0rd_kok_b3gini?_tapi_aman_k4nn?}

Disk Image Forensics

1. Ketagihan

1. Ketagihan

100

Laman file: <https://drive.google.com/file/d/1RQ-IT-yW-iCTPqgx8EfVOlGfNIQHU3X/view?usp=sharing>

Password file: peserta_LKSN_terlalu_GG_dan_OP_2k22!

Bagian Pertama

Awal Deskripsi Kasus:

Bobby, merupakan seorang anak SMA yang sangat nakal. Ia pernah masuk ke dalam penjara remaja sejak SMP karena kelakuannya yang suka menjahili temannya hingga berlebihan. Kini, Bobby berulah lagi hingga membuat banyak temannya merasa kesal dengannya hingga dipanggil polisi daerah. Bobby gemar menutupi jejak aksinya dan sangat terencana, oleh karena itu polisi daerah diberikan penugasan untuk mengecek HP Bobby jika ada keanehan atau kekeliruan di dalamnya. Anda, sebagai tim Digital Forensik yang dapat diandalkan diminta untuk melakukan analisa dari hasil akuisisi sebuah **Android Image Phone**.

Pertanyaan:

Apa nama aplikasi browser yang digunakan oleh tersangka?
(nama Android Package Name)

Format: com.apapunini.mbahgugel

Diberikan challenge dengan deskripsi sebagai berikut. Pada deskripsi, kita disuruh untuk menemukan aplikasi browser dari pelaku.

Langsung saja saya search chrome karena browser yang umum digunakan

```
a@lactosilus:/mnt/d/LKSN_FINAL_FORENSIK/data/data$ ls | grep 'chrome'  
com.android.chrome
```

Flag : com.android.chrome

2. Sumber kenakalan

Challenge 14 Solves x

2. Sumber Kenakalan

100

Bagian Kedua

Pihak kepolisian menerka sumber kenakalan remaja Bobby berasal dari kecanduan aplikasi ataupun dari lingkungan pertemanannya. Laman URL apa yang dikunjungi oleh Bobby yang **pertama kali**-nya selain **Google** ?

Format: <http://inihanyasebatascontohsajaya.com>

Flag Submit

Disini kita disuruh untuk mencari url yang pertama kali dikunjungi pelaku selain Google


```

a@lactosilus:/mnt/d/LKSN_FINAL_FORENSIK/data/data/com.android.chrome/app_chrome/Default$ ls
Account Web Data          Network Action Predictor          Settings
Account Web Data-journal' Network Action Predictor-journal' Shared Storage
Affiliation Database       OS Types                          Shortcuts
Affiliation Database-journal' Passwords                          Shortcuts-journal
Assets                    heavy_ad_intervention_opt_out.db  Synchronization
Bookmarks                 heavy_ad_intervention_opt_out.db-journal  Synchronization-journal
Bookmarks-journal         History                           Synchronization-journal
Cache                     History-journal                   Sync
Certificates              Images                             Sync Data
Cookies                   Local Storage                     Top Sites
Cookies-journal           LOCK                              Top Sites-journal'
Database                  LOG                               TransportSecurity
Database-journal          'Login Data'                     'Visited Links'
Default Preferences       'Login Data-journal'             'Web Data'
Favicons                  LOG.old                          'Web Data-journal'
Favicons-journal          'Network Action Predictor'        WebViews
                           'Network Action Predictor-journal'
                           'Network Persistent State'
                           Private Pages
                           Synchronization
                           Synchronization-journal
                           Synchronization-journal
                           Synchronization-journal
                           Preferences
                           README
                           'Reporting and NEL'
                           'Reporting and NEL-journal'
                           'Safe Browsing Cookies'
                           'Safe Browsing Cookies-journal'
                           Synchronization
                           Synchronization-journal
                           Sync
                           Sync Data
                           Top Sites
                           Top Sites-journal'
                           TransportSecurity
                           'Visited Links'
                           'Web Data'
                           'Web Data-journal'
                           WebViews

```

```

a@lactosilus: /mnt/d/LKSN_FINAL_FORENSIC/data/data/com.android.chrome/app_chrome/Default$ sqlite3 Cookies
SQLite version 3.37.2 2022-01-06 13:25:41
Enter ".help" for usage hints.
sqlite> .tables
cookies      meta
sqlite> .schema cookies
CREATE TABLE cookies(creation_utc INTEGER NOT NULL,host_key TEXT NOT NULL,top_frame_site_key TEXT NOT NULL,name TEXT NOT NULL,value TEXT NOT NULL,encrypted_value BLOB NOT NULL,path TEXT NOT NULL,expires_utc INTEGER NOT NULL,is_secure INTEGER NOT NULL,is_httponly INTEGER NOT NULL,last_access_utc INTEGER NOT NULL,has_expires INTEGER NOT NULL,is_persistent INTEGER NOT NULL,priority INTEGER NOT NULL,samesite INTEGER NOT NULL,source_scheme INTEGER NOT NULL,source_port INTEGER NOT NULL,is_same_party INTEGER NOT NULL,last_update_utc INTEGER NOT NULL);
CREATE UNIQUE INDEX cookies_unique_index ON cookies(host_key, top_frame_site_key, name, path);
sqlite> select * from cookies where host_key = 'account.kompas.com';
1331124605933278|account.kompas.com|AWSALB|sgwKLEWdy5SaeclLW6toBhZ9iXf9+d4qbSFfjsQaYdXkfZofKLnWl1h/aBQz7tRcT5+S8Ub/5+a32LlQmqBCIRj4K8iVKfd+Jvop+Sj9BiA3LxkeJpGaVENC|/|1331185085933278|0|0|1331124605933278|1|1|1|-1|2|443|0|1331124605933390
1331124605933364|account.kompas.com|AWSALBCORS|sgwKLEWdy5SaeclLW6toBhZ9iXf9+d4qbSFfjsQaYdXkfZofKLnWl1h/aBQz7tRcT5+S8Ub/5+a32LlQmqBCIRj4K8iVKfd+Jvop+Sj9BiA3LxkeJpGaVENC|/|1331185085933364|1|0|1331124605933364|1|1|1|0|2|443|0|1331124605933607
sqlite> |

```

Flag :
sgWKELEwdy55aeclIW6ToBhZ9iXi9F+d4qb5FfjsQaYdXkF2ofKnIWl1H/aBOqZ7tRCT5+S8Ub5/
a+32LILqMccBIRj4K8iVKfd+Jvop+Si9BiA3LxkeJpGaVEWC

Challenge

12 Solves

×

4. Korek Menyala

100

Bagian Keempat

Anda mengecek jika laman pencarian teratas yang dicari Bobby pada *browser*-nya mengindikasikan perilaku sosiopat. Apakah hasil pencarian **teratas** saat Bobby sedang menggunakan **search bar browser** -nya?

Format: ini hasil pencariannya guys pakai spasi

Flag

Submit

Challenge meminta kita menemukan pencari paling atas dari pelaku pada search bar browser-nya. Umumnya search bar paling atas adalah terakhir kali kita mencari suatu kata kunci. Lalu saya berasumsi berada pada bagian History

```
a@lactosilus:/mnt/d/LKSN_FINAL_FORENSIK/data/data/com.android.chrome/app_chrome/Default$ sqlite3 History
SQLite version 3.37.2 2022-01-06 13:25:41
Enter ".help" for usage hints.
sqlite> .tables
cluster_keywords      downloads_reroute_info  segments
clusters              downloads_slices       typed_url_sync_metadata
clusters_and_visits   downloads_url_chains   urls
content_annotations  keyword_search_terms  visit_source
context_annotations  meta                  visits
downloads            segment_usage
sqlite> select * from keyword_search_terms;
2|1|cara rakit bom di minecraft|cara rakit bom di minecraft
2|2|cara rakit bom di minecraft|cara rakit bom di minecraft
2|3|cara membully yang baik|cara membully yang baik
2|4|cara membully yang baik|cara membully yang baik
2|5|cara menjadi pembully yang benar|cara menjadi pembully yang benar
2|6|cara menjadi pembully yang benar|cara menjadi pembully yang benar
2|7|kata kata kasar trend 2022|kata kata kasar trend 2022
2|8|kata kata kasar trend 2022|kata kata kasar trend 2022
2|9|farel prayoga|farel prayoga
2|10|farel prayoga|farel prayoga
2|11|cara mencuri sepeda tanpa ketahuan|cara mencuri sepeda tanpa ketahuan
2|12|cara mencuri sepeda tanpa ketahuan|cara mencuri sepeda tanpa ketahuan
2|13|cara mengganggu mental health seseorang|cara mengganggu mental health seseorang
2|14|cara mengganggu mental health seseorang|cara mengganggu mental health seseorang
```

Disini saya submit pada index 1 tetapi salah lalu saya lanjut ke 3 dan ternyata benar

Flag : cara membully yang baik

5. Tertata Rapi

Challenge 15 Solves ×

5. Tertata Rapi

100

Bagian Kelima

Bobby ternyata menyimpan rencananya pada sebuah aplikasi *note-taking* khusus. Apa nama aplikasi yang digunakan penyerang untuk melakukan *note taking*? (nama *package name* Android-nya)

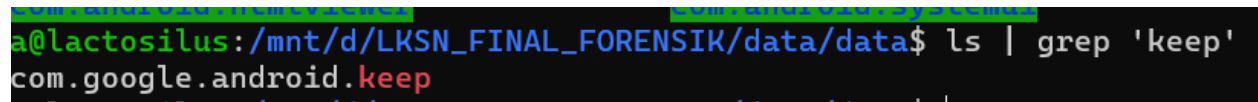
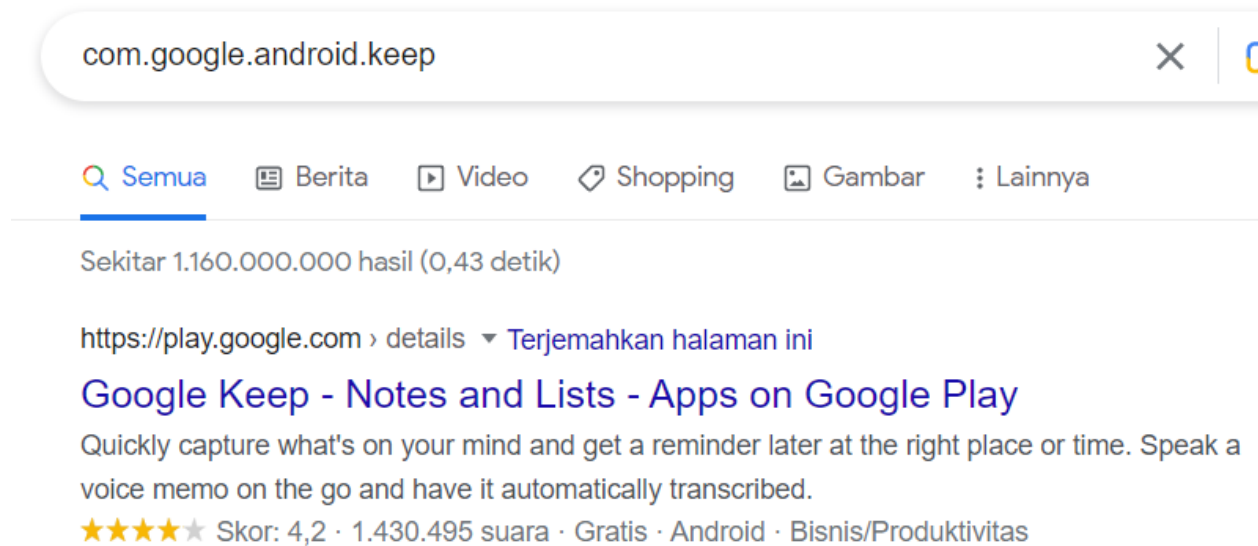
Format: com.lksn.menangsemua

Flag

Submit

Sama seperti soal yang pertama kita disuruh menemukan package name dari note app pelaku

Setelah search” pada google ternyata aplikasi tersebut adalah app note



Flag : com.google.android.keep

6. Akal Licik Anak SMA

Challenge 12 Solves X

6. Akal Licik Anak SMA

100

Bagian Keenam

Bobby telah tertangkap basah oleh Anda karena Anda mengetahui bahwa dia telah menyusun rencana usilnya yang masih dalam aplikasi *note-taking*-nya. Siapakah nama dari korban pertama rencana jahatnya? (huruf kecil semua tanpa spasi)

Format: namabiassa

Flag Submit

Disini kita disuruh untuk menemukan korban pertama dari rencana jahat si pelaku pada notenya. Langsung saja kita cari pada db sqlite nya (keep.db)

```
sqlite> select * from list_item;
1|1|184129bfa4.89a19349b087972c|18XI_SJWuY1ztVCWNWvwZol6JNF83iCV25jXaVXS-RYltdUPCifC4yHpqVWQ_VryEp_N8|1. Mengerjakan pekerjaan penjaskes
2.Pesen nasi padang
3.Pijitin Ayah
4.Maen sepeda
5.Sirem taneman
6.Ngajak Deborah jalan|1. Mengerjakan pekerjaan penjaskes
2.Pesen nasi padang
3.Pijitin Ayah
4.Maen sepeda
5.Sirem taneman
6.Ngajak Deborah jalan|1|0|||0||1666759523526|1666759638564|0|0|7|3||
2|1|184129db021.81d4e42b3f24ce51|10qz9C_BApA3cuIzqj99lyte0kPTgJh_99Tb1hT3TnLg0RmfyXB9AEqPoVL9WnIqJxeqA||2|0|||0||1666759635021|1666759638879|0|0|2|0||
3|1|184129dc7f7.ba6b8517a765da73|13W1lRge8fsmBqH02Vel0175BiUYFMbAwQUKz-A6ffDHk4FeVr8111U_3WbfJ9m3i45sGr||2|0|||0||1666759641120|1666759643164|0|0|2|0||
4|1|184129e6a9.b3b573bfccdcdeaa|1h0WkRdHPmK2adH_5ycOYHUVNeZTJ4FchNk16bzL2q7VyHx3H4mNA_3j_SjpnQSUWvgMf|d4y3Lk_5N|GG123|d4y3Lk_5N|GG123|4|0|||0||166675965
56|1666759770192|0|0|6|2||
5|1|18412a041f3.9c728d3ab64d09d8|1KfFg1dLA6Et3RLTFunV0c3ff58GgJ8kU0uGgqzNusU0UuY5rjSVacn42KldPa_TZoNui|1. Siram tommy pakek air di toilet
2. Kumpulin duit dari temen buat beli bakso kebutuhan sehari-hari
3. Bocorin ban sepeda Laxus
4. tanya jasmine mo kerkol apa engga <3|1. Siram tommy pakek air di toilet
2. Kumpulin duit dari temen buat beli bakso kebutuhan sehari-hari
3. Bocorin ban sepeda Laxus
4. tanya jasmine mo kerkol apa engga <3|5|0|||0||1666759803410|1666759923080|0|0|10|3||
sqlite>
```

i|1. Siram tommy pakek air di toilet

Flag : tommy

7. Bobby Blunder

```
**Category:** Disk Image Forensics - Bully
**Solves:** 12

## Description
>**Bagian Ketujuh**\r\n\r\nKarena masih anak SMA, ternyata Bobby juga bisa
saja teledor menyimpan sesuatu yang sifatnya rahasia dan gampang terekspos
oleh publik karena pihak Anda berhasil mendapatkan sesuatu dari
sana.\r\nBobby telah menyimpan sebuah **backup password** yang ada pada
aplikasi *note-taking* yang sama dengan sebelumnya. Apakah **isi konten**
dari backup passwordnya?\r\n\r\nFormat:  hUrUf@lay

**Hint**
* -

## Solution

### Flag
```

Challenge pada kali, pelaku memiliki backup password yang disimpan dalam notenya. Sebelumnya, pada challenge ke 6, kita telah melihat credential dari si pelaku dengan format huruf alay

```
5.Sirem taneman
6.Ngajak Deborah jalan|1|0|||0||1666759523526|1666759638564|0|0|7|3||
2|1|184129db021.81d4e43b3f24ce51|1Qqz9C_BApA3cuIzqj99Lyte0kPTgJh_99TbLhT3TnLg0RmfyXB9AEqPoVL9HrIqJxeqA|||2|0|||0||16667
59635021|1666759638879|0|0|2|0||
3|1|184129dc7f7.ba6b8517a765da73|13W11Rge8fsmBqH02VeL0175BiUYFMbAwQUKz-A6ffDhK4FeVr8I11U_3WbfJ9mi45sGr|||3|0|||0||16667
59641129|1666759643164|0|0|2|0||
4|1|184129e6ac9.b3b573bfccdcdeaa|1hoWkRdHPmK2adH_5yc0YHUVNeZTJ4FchNk16bzL2q7VyHx3H4mNA_3j_SjpnQSUWvgMf|d4y3Lk_5N@GG123|d
4y3Lk_5N@GG123|4|0|||0||1666759682856|1666759770192|0|0|6|2||
5|1|18412a041f3.9c728d3ab64d09d8|1KFfg1dLA6Et3RLTFunV0c3ff58GgJ8kU0uUy5rjSVacn42KldPa_TZoNui|1. Siram tommy pa
kek air di toilet
2. Kumpulin duit dari temen buat beli bakso kebutuhan sehari-hari
3. Bocorin ban sepeda Laxus
4. tanya jasmine mo kerkol apa engga <3|1. Siram tommy pakek air di toilet
2. Kumpulin duit dari temen buat beli bakso kebutuhan sehari-hari
3. Bocorin ban sepeda Laxus
4. tanya jasmine mo kerkol apa engga <3|5|0|||0||1666759803410|1666759923080|0|0|10|3||
sqlite>
```

```
Mf | d4y3Lk_5N@GG123 | d
```

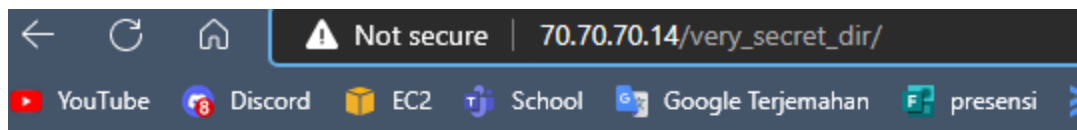
Flag : d4y3Lk_5N@GG123

Patching

Patching

Pertama tama kami merubah permission pada `very_secret_dir`, karena direktori itu milik root yang berada pada direktori web dan juga itu adalah direktori rahasia, seharusnya tidak semua orang bisa melihat direktori itu.

```
root@ubuntu20:/var/www/html# ls -la
total 32
drwxr-xr-x 3 root    root    4096 Oct 25 00:10 .
drwxr-xr-x 4 root    root    4096 Oct 25 00:09 ..
-r-xr-xr-x 1 www-data www-data 522 Apr 29 2021 .backup_config.php
-rw-r--r-- 1 www-data www-data 11327 Jun 30 2021 index.html
-rw-r--r-- 1 www-data www-data 43 Oct 25 00:10 robots.txt
drwxr-xr-x 2 root    root    4096 Jun 21 16:28 very_secret_dir
root@ubuntu20:/var/www/html# chmod 700 very_secret_dir/
root@ubuntu20:/var/www/html# ls -la
total 32
drwxr-xr-x 3 root    root    4096 Oct 25 00:10 .
drwxr-xr-x 4 root    root    4096 Oct 25 00:09 ..
-r-xr-xr-x 1 www-data www-data 522 Apr 29 2021 .backup_config.php
-rw-r--r-- 1 www-data www-data 11327 Jun 30 2021 index.html
-rw-r--r-- 1 www-data www-data 43 Oct 25 00:10 robots.txt
drwx----- 2 root    root    4096 Jun 21 16:28 very_secret_dir
root@ubuntu20:/var/www/html#
```



Forbidden

You don't have permission to access this resource.

Apache/2.4.46 (Ubuntu) Server at 70.70.70.14 Port 80

Selanjutnya kami Mendisable Anonymous login pada vsftpd untuk mencegah orang jahat mengunduh data yang ada pada server.

```
# addresses; then you must run two copies of vsftpd
# files.
listen_ipv6=YES
#
# Allow anonymous FTP? (Disabled by default).
anonymous_enable=NO
anon_root=/var/ftp/pub
#
# Uncomment this to allow local users to log in.
local_enable=YES
#
# Uncomment this to enable any form of FTP write co
```

Lalu kami mengubah password sysadm karena password terlalu mudah dan common,

Credential baru

sysadm:D6K@8Bg%16G0

Setelah mengecek lagi terdapat laman php. Menggunakan fungsi **real_escape_string** pada php untuk escape special character sehingga bisa mencegah sql injection pada web yang tersedia di **IPV6**. referensi [PHP: mysqli::real_escape_string - Manual](#)

```
<?php
session_start();
if(isset($_SESSION['userid'])) {
    header("location: index.php");
    exit();
}
include("../conf/db.php");
if(isset($_POST['login'])) {
    $query = "SELECT user_name,user_password FROM tb_users WHERE user_name=? AND user_password=? LIMIT 1";
    if($act = $db->prepare($query)) {
        $username = $db->real_escape_string($_POST['username']);
        $password = $db->real_escape_string($_POST['password']);
        $act->bind_param("ss",$username,$password);
        $act->execute();
        $res = $act->get_result();
        if($res->num_rows > 0) {
            $_SESSION['userid'] = $res->fetch_assoc()['user_name'];
            header("location: index.php");
            exit();
        } else {
            header("location: login.php");
            exit();
        }
    }
    $act->close();
} else {
    echo "b";
}
}
```

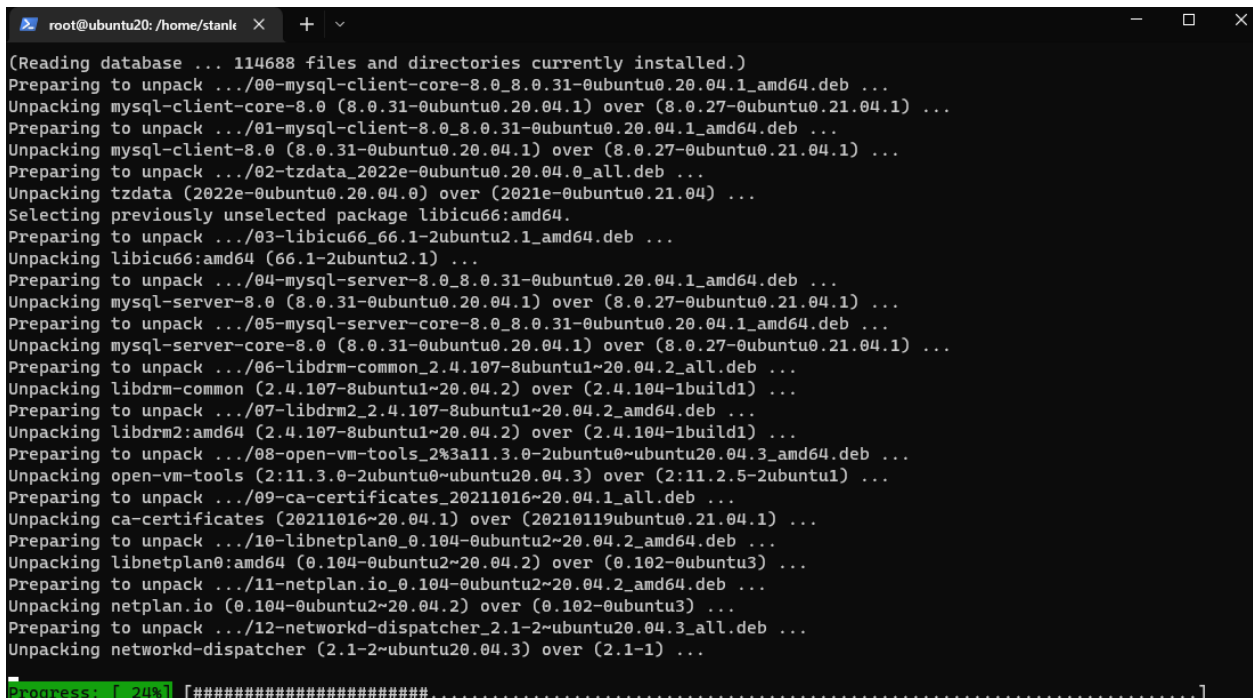
Pada direktori sysadm pada ftp terdapat backup konfigurasi iptable, walaupun sudah di enkripsi namun bisa ter decode dengan klu pada gambar yang ada pada web di port 80.

Platform Hardening

Update Repository

Karena repository sebelumnya tidak bisa di gunakan saya mengganti repo dengan repo yang lebih aman, setelah itu melakukan update. Sebenarnya ada sedikit error namun dapat diatasi karena bantuan stack overflow [Apt: Can't upgrade packages, and system still showing 16.04 / Xenial sources. after upgrade to 18.04 / Bionic - Ask Ubuntu](#)

```
# deb-src http://archive.ubuntu.com/ubuntu hirsute-security
root@ubuntu20:/usr/src# rm /etc/apt/sources.list
root@ubuntu20:/usr/src# vim /etc/apt/sources.list
```



```
root@ubuntu20:/home/stanl... X + v
(Reading database ... 114688 files and directories currently installed.)
Preparing to unpack .../00-mysql-client-core-8.0_8.0.31-0ubuntu0.20.04.1_amd64.deb ...
Unpacking mysql-client-core-8.0 (8.0.31-0ubuntu0.20.04.1) over (8.0.27-0ubuntu0.21.04.1) ...
Preparing to unpack .../01-mysql-client-8.0_8.0.31-0ubuntu0.20.04.1_amd64.deb ...
Unpacking mysql-client-8.0 (8.0.31-0ubuntu0.20.04.1) over (8.0.27-0ubuntu0.21.04.1) ...
Preparing to unpack .../02-tzdata_2022e-0ubuntu0.20.04.0_all.deb ...
Unpacking tzdata (2022e-0ubuntu0.20.04.0) over (2021e-0ubuntu0.21.04) ...
Selecting previously unselected package libicu66:amd64.
Preparing to unpack .../03-libicu66_66.1-2ubuntu2.1_amd64.deb ...
Unpacking libicu66:amd64 (66.1-2ubuntu2.1) ...
Preparing to unpack .../04-mysql-server-8.0_8.0.31-0ubuntu0.20.04.1_amd64.deb ...
Unpacking mysql-server-8.0 (8.0.31-0ubuntu0.20.04.1) over (8.0.27-0ubuntu0.21.04.1) ...
Preparing to unpack .../05-mysql-server-core-8.0_8.0.31-0ubuntu0.20.04.1_amd64.deb ...
Unpacking mysql-server-core-8.0 (8.0.31-0ubuntu0.20.04.1) over (8.0.27-0ubuntu0.21.04.1) ...
Preparing to unpack .../06-libdrm-common_2.4.107-8ubuntu1~20.04.2_all.deb ...
Unpacking libdrm-common (2.4.107-8ubuntu1~20.04.2) over (2.4.104-1build1) ...
Preparing to unpack .../07-libdrm2_2.4.107-8ubuntu1~20.04.2_amd64.deb ...
Unpacking libdrm2:amd64 (2.4.107-8ubuntu1~20.04.2) over (2.4.104-1build1) ...
Preparing to unpack .../08-open-vm-tools_2%3a11.3.0-2ubuntu0~ubuntu20.04.3_amd64.deb ...
Unpacking open-vm-tools (2:11.3.0-2ubuntu0~ubuntu20.04.3) over (2:11.2.5-2ubuntu1) ...
Preparing to unpack .../09-ca-certificates_20211016~20.04.1_all.deb ...
Unpacking ca-certificates (20211016~20.04.1) over (20210119ubuntu0.21.04.1) ...
Preparing to unpack .../10-libnetplan0_0.104-0ubuntu2~20.04.2_amd64.deb ...
Unpacking libnetplan0:amd64 (0.104-0ubuntu2~20.04.2) over (0.102-0ubuntu3) ...
Preparing to unpack .../11-netplan.io_0.104-0ubuntu2~20.04.2_amd64.deb ...
Unpacking netplan.io (0.104-0ubuntu2~20.04.2) over (0.102-0ubuntu3) ...
Preparing to unpack .../12-networkd-dispatcher_2.1-2-ubuntu20.04.3_all.deb ...
Unpacking networkd-dispatcher (2.1-2-ubuntu20.04.3) over (2.1-1) ...
Progress: [ 24%] [#####]
```

```
Scanning linux images...

Running kernel seems to be up-to-date.

No services need to be restarted.

No containers need to be restarted.

No user sessions are running outdated binaries.
```

Update kernel & kernel Module Sign

Untuk update kernel kami melihat referensi dari [Compile Kernel - OnnoWiki \(onnocenter.or.id\)](#) dan kami melakukan sedikit modifikasi pada `/usr/src/linux/certs` untuk kernel module sign nya

Bisa pake command ini

wget

<https://gist.githubusercontent.com/github-kyruuu/e7778b38824c4edfea69d68c528389a7/raw/c7990b2aa2dc8d862bda38fde46671e34ba43b0f/x509.genkey>

```
openssl req -new -nodes -utf8 -sha256 -days 36500 -batch -x509 \
-config x509.genkey -outform PEM -out signing_key.pem \
-keyout signing_key.pem
```

Waktu compile memang memerlukan waktu yang lama 😊

```
root@ubuntu20:~# uname -r
5.15.74
```

Lalu terlihat pada **/proc/keys** sudah terdapat **Secure Boot Signing Key**

```
1b2928ba I--Q--- 1 perm 3f030000 0 0 keyring _ses: 2
1be779d1 I--Q--- 1 perm 0b0b0000 0 0 user invocation_id: 16
1c66bbb4 I--Q--- 1 perm 3f030000 0 0 keyring _ses: 2
1d826a3b I--Q--- 1 perm 0b0b0000 0 0 user invocation_id: 16
202b02ac I----- 1 perm 1f030000 0 0 asymmetri SMK Negeri 7 Semarang: Secure Boot Signing Key: 1cb25658b13e2
60f2e7e6987a6a7bfff7ffa57fcc: X509.rsa ffa57fcc []
20c5f60d I--Q--- 1 perm 3f030000 0 0 keyring _ses: 2
219e8f32 I--Q--- 1 perm 3f030000 0 0 keyring _ses: 2
223885e2 I----- 1 perm 1f030000 0 0 keyring .dns_resolver: empty
```

Kernel Module Loading enforcement

Ini berfungsi agar module baru tidak bisa ter input (tidak bisa pake command insmod)

```
root@ubuntu20:~# echo 1 > /proc/sys/kernel/modules_disabled
root@ubuntu20:~# _
```

SUID Executables

File bertipe **s** merupakan file yang unik karena dapat beroperasi/berjalan sebagai root dan dapat dijalankan oleh semua user. Maka kita harus berhati hati dengan file ini, untuk list semua file yang memiliki tipe s bisa di lihat sebagai berikut ...

```
root@ubuntu20:~# find / -perm -u=s -type f 2>/dev/null
/usr/bin/gpasswd
/usr/bin/fusermount
/usr/bin/chfn
/usr/bin/newgrp
/usr/bin/chsh
/usr/bin/umount
/usr/bin/su
/usr/bin/pkexec
/usr/bin/mount
/usr/bin/passwd
/usr/bin/sudo
```

Binary pkexec berfungsi untuk execute command sebagai user lain jika ini memiliki tipe s maka akan gawat darurat, karena semua user akan bisa mengakses sebagai root. Maka kita perlu menghapus tipe s pada binary ini

```
root@ubuntu20:~# chmod /usr/bin/pkexec -s
root@ubuntu20:~#
```

SSH Attack Surface Reduction

Untuk mereduksi serangan bertipe bruteforce attack pada ssh kita menggunakan konfigurasi seperti di bawah

```
# PermitTTY no
# ForceCommand cvs server
PasswordAuthentication no_
AllowUsers stanley
-- INSERT --
```

Dengan begitu User yang mau login ssh harus menggunakan public key

Credential Hardening

Identify and Protect Privileged Accounts

Check yang punya uid 0

```
root@ubuntu20:~# cat /etc/passwd | awk -F: '($3 == 0) { print $1 }'
```

root

Ternyata yang memiliki uid 0 hanya root

Strong Password Enforcement

```
# install libpam
```

```
sudo apt install libpam-cracklib
```

Konfigurasi pada `/etc/pam.d/common-password`

- `retry=3` : Prompts user at most 1 time before returning with error.
- `minlen=8` : The minimum acceptable size for the new password.
- `uccredit=-1` : The password must contain at least 1 uppercase characters.
- `dcredit=-1` : The new password must contain at least 1 digits.
- `ocredit=-1` : The new password must contain at least 1 symbols.

```
# here are the per-package modules (the "Primary" block)
password requisite pam_cracklib.so retry=3 minlen=8 ucredit=-1 dcredit=-1 ocredit=-1
password [success=1 default=ignore] pam_unix.so obscure use_authtok try_first_pass sha512
# here's the fallback if no module succeeds
password requisite pam_deny.so
# prime the stack with a positive return value if there isn't one already;
# this avoids us returning an error just because nothing sets a success code
# since the modules above will each just jump around
password required pam_permit.so
# and here are more per-package modules (the "Additional" block)
# end of pam-auth-update config
```

Dengan begitu kita bisa menyuruh semua user untuk mengganti password, karena sudah ada libpam, maka password yang di buat user akan jauh lebih aman. Bayangkan jika user hanya

menginputkan password misal **password**. Maka akan mudah di tebak dan tidak memerlukan waktu yang lama untuk meng crack password tsb.

How Secure is Your Password?

Take the Password Test

Tip: It's often better to have longer passwords than shorter, more complex ones

Show password: ☐

password

Very Weak

8 characters containing: Lower case Upper case Numbers Symbols

Time to crack your password:

0 seconds

How Secure is Your Password?

Take the Password Test

Tip: It's often better to have longer passwords than shorter, more complex ones

Show password: ☒

v3R12yStr0n9P4ssw0rD

Very Strong

20 characters containing: Lower case Upper case Numbers Symbols

Time to crack your password:

360 years

– Thank You –