JURNAL RESISTOR
Vol. 1 No 2 – Oktober 2108
p-ISSN 2598-7542 (Print), e-ISSN 2598-9650 (Online)
Available Online at :
http://jurnal.stiki-indonesia.ac.id/index.php/jurnalresistor

IMPLEMENTASI KATOOLIN SEBAGAI PENETRASI *TOOLS* KALI LINUX PADA LINUX UBUNTU 16.04 (STUDI KASUS: REVERSE ENGINEERING FILE .APK)

I Putu Agus Eka Pratama[1], Anak Agung Bagus Arya Wiradarma[2]

1,2 Program Studi Teknologi Informasi, Fakultas Teknik, Universitas Udayana
Denpasar,Bali

e-mail : eka.pratama@unud.ac.id1, 9egungwira5@gmail.com2

Received : Mei, 2018	Accepted : Oktober, 2018	Published : Oktober, 2018

Abstrack

The Linux Operating System is known for its open-source characteristic which means everyone is free to develop Linux with the use of available source code. The result of Linux development is called Linux distribution (Distro). There are various Linux distributions in accordance with their respective uses, one of them is Kali Linux. Kali Linux is a Linux distro that is developed to penetrate the security of computer systems. Kali Linux uses a variety of tools to perform its functions. However, for users who want to use the functionality of Kali Linux without having to change the Linux distro that has been used, the user can use Katoolin. Katoolin can provide the convenience and flexibility for users who want to use Kali Linux as a special Linux distro for the purpose of penetrating computer system security without having to replace the distro that has been used or do a full install of Kali Linux. One case study that can be solved using the Kali Kali Linux based tool on Katoolin is Reverse Engineering. The case study was solved using one of the tools in the Reverse Engineering category named apktool that available on Katoolin.

Keywords: *Kali Linux, Security, Katoolin, Linux Ubuntu, Reverse Engineering*

Abstrak

Sistem Operasi Linux dikenal dengan sifat open-source yang berarti setiap orang bebas untuk mengembangkan Linux dengan pemanfaatan source code yang tersedia. Hasil dari pengembangan Linux disebut dengan distribusi (distro) Linux. Terdapat berbagai macam distro Linux sesuai dengan kegunaannya masing-masing, salah satunya adalah Kali Linux. Kali Linux merupakan distro Linux yang dikhususkan untuk melakukan penetrasi keamanan sistem komputer. Kali Linux menggunakan berbagai macam tools (alat) untuk menjalankan fungsinya. Namun, bagi pengguna yang ingin menggunakan fungsi dari Kali Linux tanpa harus mengganti distro Linux yang telah digunakan, pengguna dapat menggunakan Katoolin. Katoolin dapat menyediakan kemudahan dan fleksibilitas bagi pengguna yang ingin menggunakan Kali Linux sebagai distro Linux yang khusus untuk keperluan penetrasi keamanan sistem komputer tanpa harus mengganti distro yang sudah digunakan ataupun melakukan instalasi penuh dari Kali Linux. Salah satu studi kasus yang dapat diselesaikan dengan menggunakan tools berbasis Kali Linux pada Katoolin adalah Reverse Engineering. Studi kasus tersebut diselesaikan dengan menggunakan salah satu tools dalam kategori Reverse Engineering, yaitu apktool yang tersedia pada Katoolin.

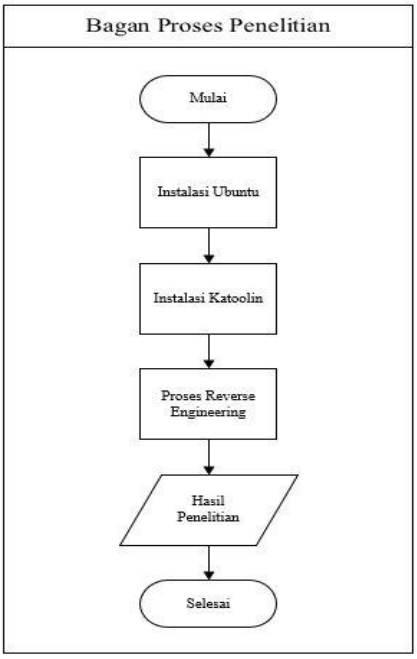
Kata kunci: *Kali Linux, Security, Katoolin, Linux Ubuntu, Reverse Engineering*

1. PENDAHULUAN

Salah satu distro Linux yang dikhususkan untuk kepentingan keamanan adalah Kali Linux. Namun, sering terdapat masalah jika pengguna ingin menguji penetrasi keamanan atau hanya ingin mencoba tools security yang disediakan Kali Linux tetapi pengguna tidak ingin untuk mengganti distro Linux yang sedang digunakan. Solusi dari masalah ini adalah tools yang bernama Katoolin. Katoolin (Kali Linux Tools Installer) merupakan program yang dikembangkan oleh LionSec berbasis Phyton yang dapat menginstal dan menjalankan fungsi dari tools-tools berbasis security pada Kali Linux. Katoolin sangat memudahkan pengguna yang ingin mencoba ataupun menggunakan tools Kali Linux untuk berbagai macam keperluan, yang tentunya tidak jauh dari bidang penetrasi keamanan komputer. Bermacam-macam studi kasus yang diperlukan untuk menggunakan tools Kali Linux dapat diselesaikan dengan menggunakan Katoolin.

2. METODOLOGI PENELITIAN

Metodologi penelitian dimulai dengan melakukan langkah-langkah proses instalasi Katoolin dalam sistem operasi Linux Ubuntu 16.04, dengan asumsi pengguna sudah melakukan instalasi Linux pada komputernya. Setelah melakukan proses instalasi, pengguna akan melakukan percobaan menggunakan salah satu kategori tools berbasis Kali Linux yang dapat diinstal melalui Katoolin pada Linux Ubuntu. Berikut merupakan bagan urutan proses penelitian :



Gambar 1. Bagan Proses Penelitian

Disebabkan oleh tools Kali Linux yang memiliki cukup banyak kategori, pengguna hanya akan mencoba salah satu tools yang akan digunakan sebagai percobaan yang sesuai dengan studi kasus yang telah ditentukan. Studi kasus yang digunakan oleh pengguna adalah studi kasus mengenai reverse engineering, dimana pengguna akan menyelesaikan masalah dari studi kasus tersebut dengan menggunakan tools berbasis Kali Linux yang disediakan oleh Katoolin.

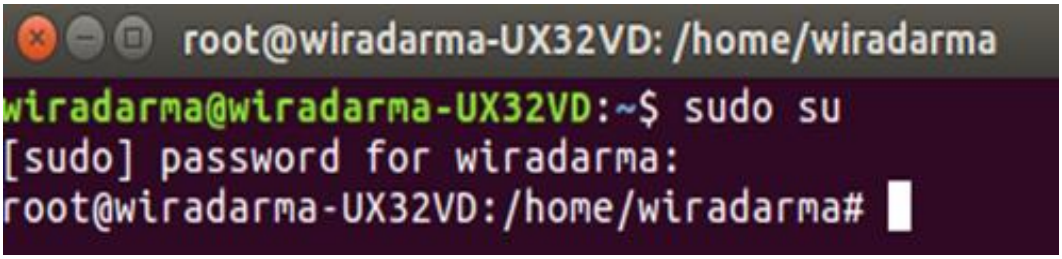
2. HASIL DAN PEMBAHASAN

Berikut merupakan hasil dari penelitian yang telah dilakukan sesuai dengan setiap tahapan yang telah dipaparkan secara rinci pada metodologi penelitian :

3.1 Instalasi Katoolin

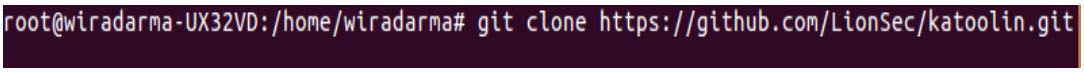
Kode program Katoolin yang menggunakan basis struktur bahasa pemrograman Phyton akan di-instal pada sistem operasi Linux Ubuntu versi 16.04. Berikut merupakan langkah-langkah dari proses instalasi Katoolin :

1. Pengguna menggunakan Terminal pada Linux Ubuntu dan masuk sebagai *super-user* dengan sintaks : *sudo su* Berikut merupakan tampilan login sebagai root.



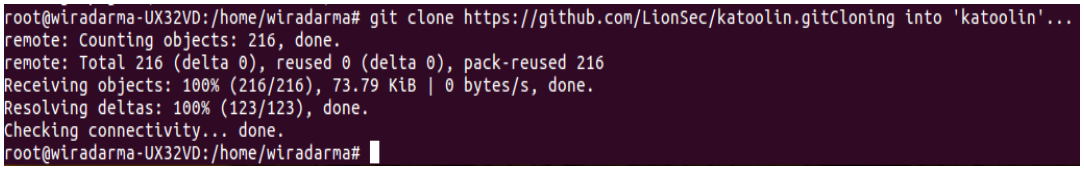
Gambar 2. Login Sebagai *Super-User*

2. Setelah hak akses komputer sudah pada root (*super-user*), lakukan pengunduhan (*clone*) *script* Phyton dari Katoolin pada situs Github melalui Terminal. Proses tersebut dilakukan dengan sintaks : *git clone https://github.com/LionSec/katoolin.git* Berikut merupakan tampilan sintaks *clone script* Phyton Katoolin.



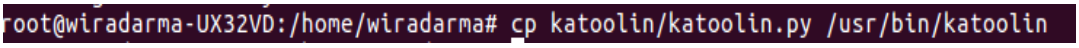
Gambar 3. Sintaks Clone Script Phyton Katoolin

3. Proses pengunduhan dan instalasi Katoolin akan berjalan. Biarkan proses tersebut sampai selesai Berikut merupakan tampilan proses instalasi Katoolin.



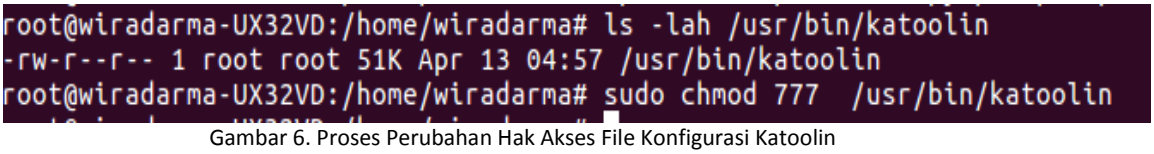
Gambar 4. Proses Instalasi Katoolin

4. Setelah proses pengunduhan dan instalasi Katoolin selesai, maka *copy* file konfigurasi Katoolin yang telah diunduh dengan menggunakan sintaks: *katoolin/katoolin.py /usr/bin/katoolin* Tujuan dari proses *copy* file ini adalah agar file *script* Katoolin berada di dalam direktori konfigurasi Linux Ubuntu pada direktori */usr/bin* Berikut merupakan tampilan proses *copy* file konfigurasi Katoolin.



Gambar 5. Proses *Copy* File Konfigurasi Katoolin

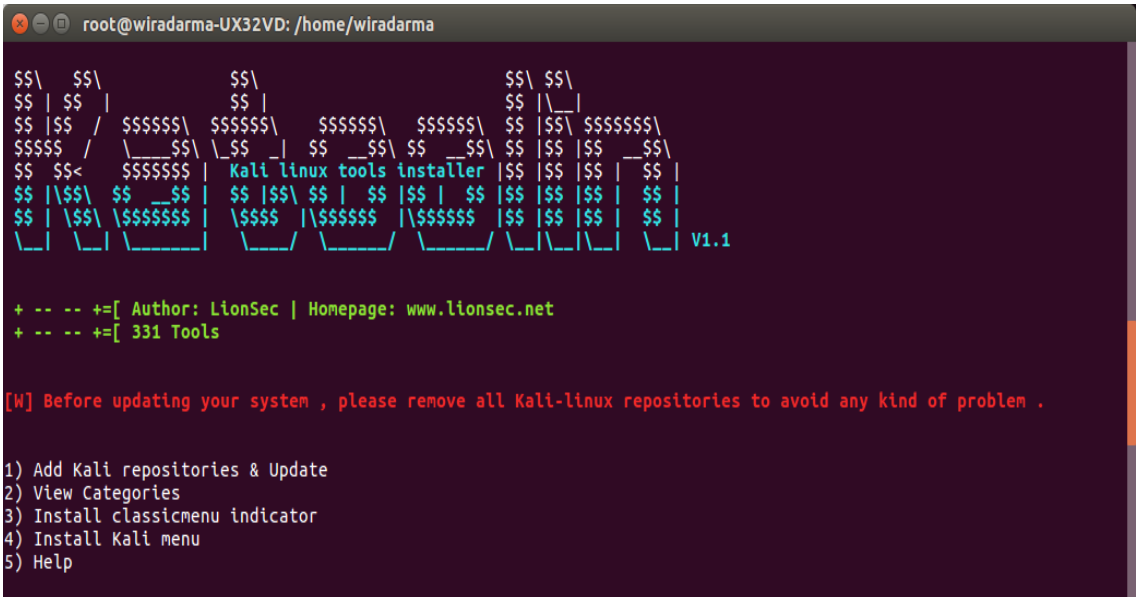
5. Setelah file konfigurasi di-*copy*, lakukan pengecekan hak akses file dengan sintaks : *ls -lah /usr/bin/katoolin* .Terlihat hak akses yang dimiliki pengguna hanya sebatas *read* dan *write* saja. Lakukan pengubahan hak akses file menjadi hak akses tertinggi dengan sintaks : *sudo chmod 777 /usr/bin/katoolin* Berikut merupakan tampilan proses perubahan hak akses file konfigurasi Katoolin:



Gambar 6. Proses Perubahan Hak Akses File Konfigurasi Katoolin

6. Tampilan utama Katoolin sudah dapat diakses dengan menggunakan hak akses *super-user* (sudo) lalu gunakan sintaks : katoolin pada Terminal. Katoolin memiliki beberapa perintah utama sebagai berikut :
   1) Add Kali Repositories & Update
   2) View Categories
   3) Install classicmenu indicator
   4) Install Kali Menu
   5) Help

   Berikut merupakan tampilan menu utama Katoolin:



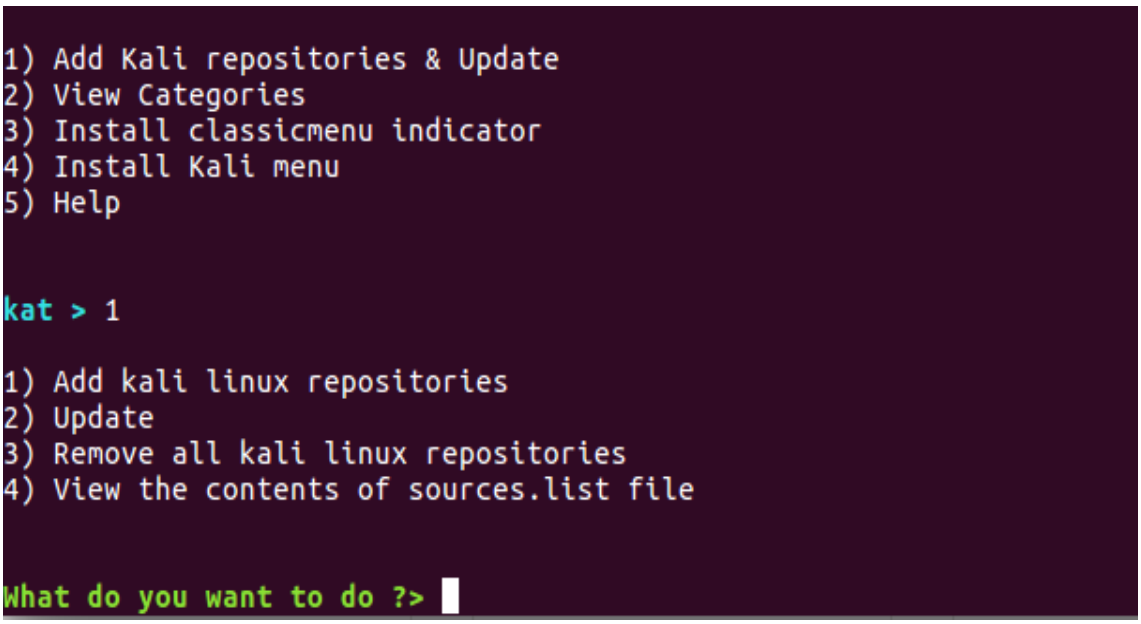
Gambar 7. Tampilan Menu Utama Katoolin

2.2 Percobaan Fungsi Katoolin

Terdapat 5 fungsi utama yang dapat digunakan dalam Katoolin, penjelasan rinci dari fungsi-fungsi tersebut adalah sebagai berikut :

1. Add Kali Repositories & Update

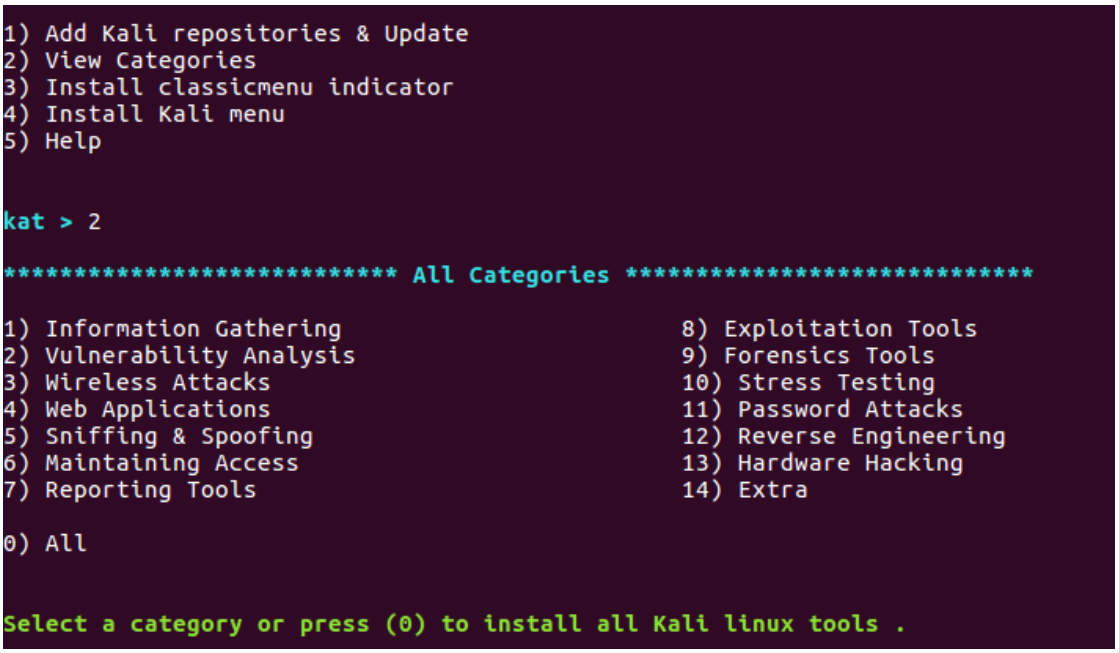
Menu Katoolin yang pertama adalah fungsi untuk menambahkan *repository* dari Kali Linux. Fungsi ini wajib dijalankan oleh pengguna ketika baru meng-*install* Katoolin. Dengan menambahkan repository dari Kali Linux maka pengguna dapat menggunakan tools-tools yang disediakan. Terdapat pula sub menu untuk melakukan update, menghapus semua repositories dari Kali Linux dan melihat isi dari file source.list yang berisikan dengan sumber-sumber yang digunakan untuk meng-instal repositories dari Kali Linux. Berikut merupakan tampilan fungsi *Add Kali Repositories & Update* yang dijalankan pada terminal Linux Ubuntu 16.04 :



Gambar 8. Tampilan Menu *Add Kali Repositories & Update*

2. View Categories

Menu Katoolin yang kedua adalah fungsi untuk melihat dari kategori-kategori dari *tools* berbasis Kali Linux yang dapat di-instal dan dijalankan. Terdapat 14 kategori yang tersedia. Kategori tersebut mencakup kategori-kategori penting dalam hal *security.* Didalam kategori tersebut, masing-masing mempunyai *tools* yang fungsinya sesuai dengan kategori yang telah dibagi. Berikut merupakan tampilan fungsi *View Categories* yang dijalankan pada terminal Linux Ubuntu 16.04 :



Gambar 9. Tampilan Menu *View Categories*

***3.* Install classicmenu indicator**

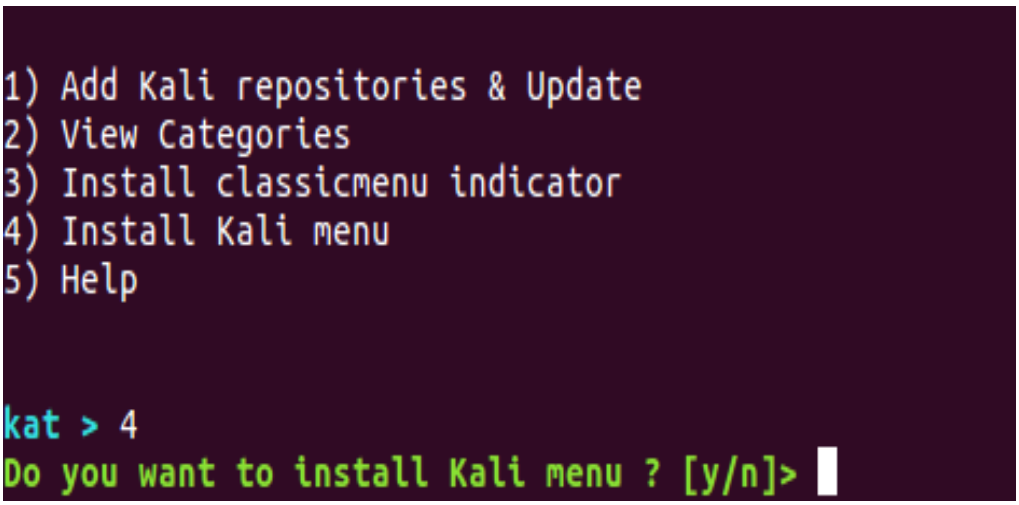
Menu Katoolin yang ketiga adalah fungsi untuk meng-install indikator yang berfungsi untuk menunjukkan tampilan dari menu klasik Ubuntu yang dapat diakses dari panel bagian atas. Tampilan klasik menu akan menunjukkan pengguna tampilan klasik berbasis GNOME yang berguna bagi pengguna yang lebih memilih untuk menggunakan tampilan klasik dari tampilan dashboard Ubuntu Unity. Berikut merupakan tampilan fungsi Install classicmenu indicator yang dijalankan pada terminal Linux Ubuntu 16.04

Gambar 10. Tampilan Menu *Install Classicmenu Indicator*

***4.* Install Kali Menu**

Menu Katoolin yang keempat adalah fungsi untuk meng-install menu Kali Linux. Fungsi ini dapat meng-install keseluruhan dari menu yang terdapat pada Kali Linux pada sistem operasi pengguna. Pengguna dapat

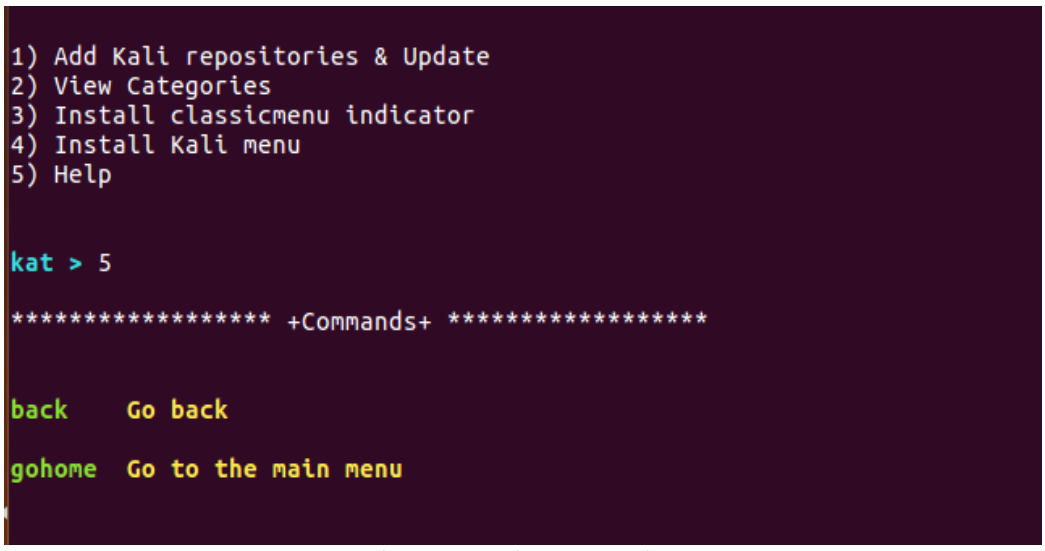
menggunakan keseluruhan menu dari Kali Linux jika dibutuhkan, dan pengguna tidak hanya ingin melakukan instalasi terhadap tools-tools-nya saja. Berikut merupakan tampilan fungsi Install Kali menu yang dijalankan pada terminal Linux Ubuntu 16.04



Gambar 11. Tampilan Menu *Install Kali Menu*

5. **Help**

Menu Katoolin yang kelima atau fungsi terakhir adalah fungsi untuk bantuan. Fungsi ini akan menunjukkan pengguna perintah-perintah yang dapat digunakan pengguna dalam menggunakan Katoolin. Berikut merupakan tampilan fungsi Help yang dijalankan pada terminal Linux Ubuntu 16.04 :



Gambar 12. Tampilan Fungsi Help

a. Instalasi Tools Katoolin (Studi Kasus : *Reverse Engineering* pada File .apk (*Android Package Tool*))

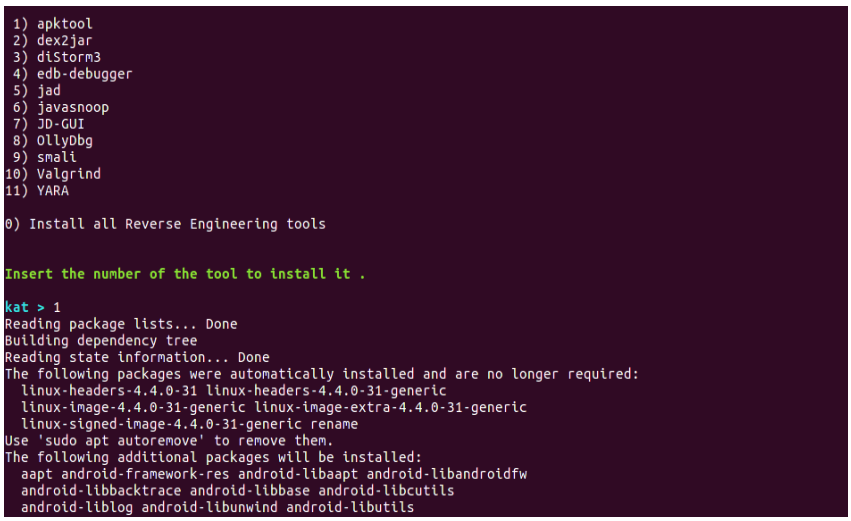
Sistem operasi Kali Linux menyediakan berbagai macam kategori *tools* yang dapat digunakan oleh pengguna sesuai dengan keperluan. Pada penelitian ini, pengguna diasumsikan mengerjakan studi kasus *Reverse Engineering*. *Reverse engineering* adalah suatu proses untuk mencari dan menemukan sistem dari suatu teknologi, fungsi dan operasi yang bekerja di balik suatu desain dan komponen atau objek melalui sebuah proses analisa yang mendalam pada setiap komponen struktur dari desain atau objek yang diteliti. Proses *reverse engineering* pada umunya menjadi salah satu

proses dalam *hacking*. Pengguna akan memakai tools *apktool* dalam kategori *Reverse Engineering* pada Katoolin. Berikut merupakan langkah instalasinya :

1. Pengguna memulai Katoolin dan menuju menu *View Categories*, setelah itu akan terlihat kategori *tools* yang disediakan dan pengguna memillih nomor 12 untuk
2. melihat *tools* dalam kategori *Reverse Engineering*. Terdapat 11 tools pada kategori *Reverse Engineering*, untuk menginstall *apktool* pengguna meng-input angka 1 sesuai dengan urutan *tools* pada kategori *Reverse Engineering* dalam Katoolin. Berikut merupakan tampilan kategori *Reverse Engineering* dan macam-macam *tools* yang terdapat didalamnya

Gambar 13. Kategori *Reverse Engineering* pada Katoolin

3. Katoolin akan melakukan proses instalasi dari tools apktool. Berikut merupakan tampilan proses instalasi dari *tools apktool* :



Gambar 14. Proses Instalasi apktool pada Katoolin

4. Katoolin akan memberi notifikasi pada pengguna saat melakukan instalasi mengenai ukuran dari *apktool*. Pengguna akan mendapat pilihan akan menlajutkan

proses instalasi atau tidak. Berikut merupakan tampilan notifikasi ukuran *apktool* oleh Katoolin :

```
After this operation, 234 MB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:1 http://ftp.yzu.edu.tw/Linux/kali kali-rolling/main amd64 android-framework-res all 1:7.0.0+r33-1 [12,9 MB]
Get:12 http://mirrors.neusoft.edu.cn/kali kali-rolling/main amd64 libpng16-16 amd64 1.6.34-1 [287 kB]
Get:2 http://ftp.yzu.edu.tw/Linux/kali kali-rolling/main amd64 android-liblog amd64 1:7.0.0+r33-2 [18,1 kB]
Get:3 http://ftp.yzu.edu.tw/Linux/kali kali-rolling/main amd64 android-libcutils amd64 1:7.0.0+r33-2 [24,4 kB]
Get:4 http://ftp.yzu.edu.tw/Linux/kali kali-rolling/main amd64 android-libbase amd64 1:7.0.0+r33-2 [20,5 kB]
Get:5 http://ftp.yzu.edu.tw/Linux/kali kali-rolling/main amd64 p7zip amd64 16.02+dfsg-6 [376 kB]
Get:6 http://ftp.yzu.edu.tw/Linux/kali kali-rolling/main amd64 p7zip-full amd64 16.02+dfsg-6 [1.164 kB]
Get:7 http://ftp.yzu.edu.tw/Linux/kali kali-rolling/main amd64 android-libunwind amd64 7.0.0+r1-4 [50,4 kB]
Get:8 http://ftp.yzu.edu.tw/Linux/kali kali-rolling/main amd64 android-libbacktrace amd64 1:7.0.0+r33-2 [33,6 kB]
Get:9 http://ftp.yzu.edu.tw/Linux/kali kali-rolling/main amd64 android-libutils amd64 1:7.0.0+r33-2 [50,6 kB]
Get:10 http://ftp.yzu.edu.tw/Linux/kali kali-rolling/main amd64 android-libziparchive amd64 1:7.0.0+r33-2 [21,4 kB]
Get:11 http://ftp.yzu.edu.tw/Linux/kali kali-rolling/main amd64 android-libandroidfw amd64 1:7.0.0+r33-1 [98,3 kB]
Get:13 http://ftp.yzu.edu.tw/Linux/kali kali-rolling/main amd64 android-libaapt amd64 1:7.0.0+r33-1 [264 kB]
Get:14 http://ftp.yzu.edu.tw/Linux/kali kali-rolling/main amd64 libprotobuf-lite10 amd64 3.0.0-9.1 [126 kB]
```

Gambar 15. Notifikasi Ukuran *apktool* Oleh Katoolin

5. Proses instalasi dari *apktool* telah selesai. Pengguna dapat menjalankan *apktool* dengan meng-inputkan command “apktool” pada Terminal, lalu akan terlihat menu utama dari *apktool*. Menu utama *apktool* memperlihatkan cara-cara dan command yang dapat digunakan oleh pengguna beserta dengan fungsinya masing-masing. Berikut merupakan tampilan utama *apktool* :

```
root@wiradarma-UX32VD:/home/wiradarma# apktool
Apktool v2.3.2-dirty - a tool for reengineering Android apk files
with smali v2.2.3-dev and baksmali v2.2.3-dev
Copyright 2014 Ryszard Wiśniewski <brut.alll@gmail.com>
Updated by Connor Tumbleson <connor.tumbleson@gmail.com>

usage: apktool
 -advance,--advanced   prints advance information.
 -version,--version    prints the version then exits
usage: apktool if|install-framework [options] <framework.apk>
 -p,--frame-path <dir>   Stores framework files into <dir>.
 -t,--tag <tag>          Tag frameworks using <tag>.
usage: apktool d[ecode] [options] <file_apk>
 -f,--force              Force delete destination directory.
 -o,--output <dir>       The name of folder that gets written. Default is apk.out
 -p,--frame-path <dir>   Uses framework files located in <dir>.
 -r,--no-res             Do not decode resources.
 -s,--no-src             Do not decode sources.
 -t,--frame-tag <tag>    Uses framework files tagged by <tag>.
usage: apktool b[uild] [options] <app_path>
 -f,--force-all          Skip changes detection and build all files.
 -o,--output <dir>       The name of apk that gets written. Default is dist/name.apk
 -p,--frame-path <dir>   Uses framework files located in <dir>.

For additional info, see: http://ibotpeaches.github.io/Apktool/
For smali/baksmali info, see: https://github.com/JesusFreke/smali
```

Gambar 16. Tampilan Utama *apktool*

3.4 Implementasi Tools Katoolin (Studi Kasus : Reverse Engineering pada File APK (Android Package Tool))

Proses implementasi salah satu tools Katoolin dengan kategori Reverse Engineering yaitu apktool akan dilakukan sesuai dengan fungsinya. Fungsi dari apktool adalah melakukan ekstrak file berformat .apk dimana file .apk merupakan format file yang digunakan untuk mendistribusikan dan memasang aplikasi ke ponsel dengan sistem operasi Android. Apktool akan mampu memecah file .apk menjadi bagian-bagian file dan folder yang berfungsi untuk membangun aplikasi Android terkait.

Pada studi kasus ini, pengguna akan menggunakan apktool untuk melakukan ekstrak file .apk dari salah satu aplikasi Android. Setelah berhasil melakukan ekstrak file .apk , pengguna akan dapat melihat dan mempelajari file-file yang menjadi sumber untuk membangun aplikasi berbasis Android tersebut. Berikut langkah-langkah implementasi tools apktool pada Katoolin :

1. Pengguna menjalankan apktool. Berikut merupakan tampilan utama apktool :

```
root@wiradarma-UX32VD:/home/wiradarma# apktool
Apktool v2.3.2-dirty - a tool for reengineering Android apk files
with smali v2.2.3-dev and baksmali v2.2.3-dev
Copyright 2014 Ryszard Wiśniewski <brut.alll@gmail.com>
Updated by Connor Tumbleson <connor.tumbleson@gmail.com>

usage: apktool
 -advance,--advanced   prints advance information.
 -version,--version    prints the version then exits
usage: apktool if|install-framework [options] <framework.apk>
 -p,--frame-path <dir>   Stores framework files into <dir>.
 -t,--tag <tag>          Tag frameworks using <tag>.
usage: apktool d[ecode] [options] <file_apk>
 -f,--force              Force delete destination directory.
 -o,--output <dir>       The name of folder that gets written. Default is apk.out
 -p,--frame-path <dir>   Uses framework files located in <dir>.
 -r,--no-res             Do not decode resources.
 -s,--no-src             Do not decode sources.
 -t,--frame-tag <tag>    Uses framework files tagged by <tag>.
usage: apktool b[uild] [options] <app_path>
 -f,--force-all          Skip changes detection and build all files.
 -o,--output <dir>       The name of apk that gets written. Default is dist/name.apk
 -p,--frame-path <dir>   Uses framework files located in <dir>.

For additional info, see: http://ibotpeaches.github.io/Apktool/
For smali/baksmali info, see: https://github.com/JesusFreke/smali
```

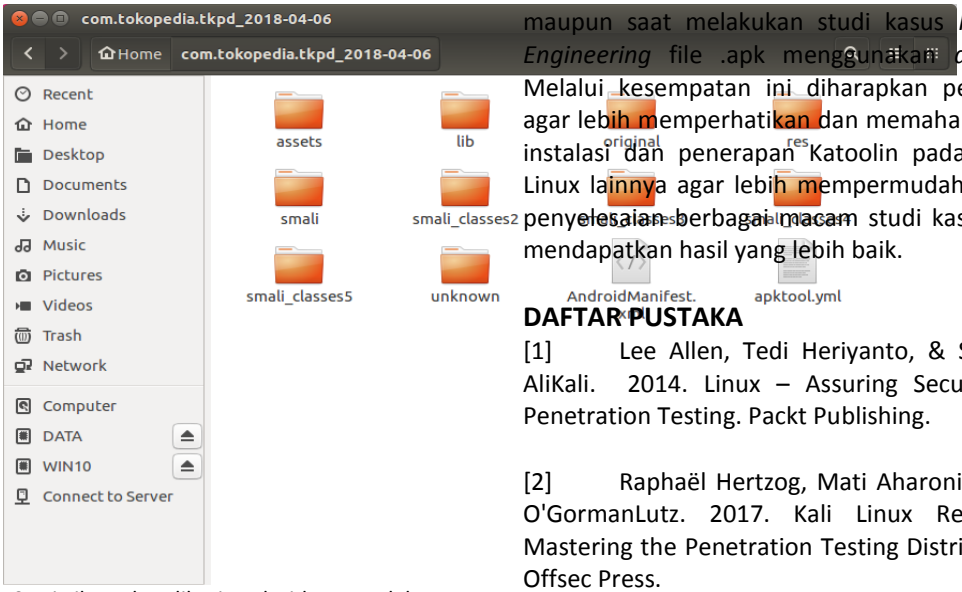
Gambar 17. Tampilan Utama *apktool*

2. Piasumsikan pengguna sudah mempunyai file .apk yang akan diekstrak dengan *apktool*. Gunakan perintah : *apktool d /direktori-file/nama-file* . Berikut merupakan tampilan proses pada *apktool* saat sedang melakukan fungsinya sebagai *tools reverse engineering*, yaitu mengekstrak file .apk menjadi bagian dari file-file yang membangun .apk atau aplikasi Android tersebut :

```
root@wiradarma-UX32VD:/home/wiradarma# apktool d /home/wiradarma/Downloads/com.tokopedia.tkpd_2018-04-06.apk
I: Using Apktool 2.3.2-dirty on com.tokopedia.tkpd_2018-04-06.apk
I: Loading resource table...
I: Decoding AndroidManifest.xml with resources...
I: Loading resource table from file: /root/.local/share/apktool/framework/1.apk
I: Regular manifest package...
I: Decoding file-resources...
W: Cant find 9patch chunk in file: "drawable-mdpi-v4/notification_bg_normal_pressed.9.png". Renaming it to *.png.
W: Cant find 9patch chunk in file: "drawable-xhdpi-v4/bubble_mask.9.png". Renaming it to *.png.
W: Cant find 9patch chunk in file: "drawable-mdpi-v4/notification_bg_low_normal.9.png". Renaming it to *.png.
W: Cant find 9patch chunk in file: "drawable-mdpi-v4/bg_speech_bubble_r90.9.png". Renaming it to *.png.
S: Could not decode file, replacing by FALSE value: raw/keep.xml
W: Cant find 9patch chunk in file: "drawable-mdpi-v4/notification_bg_low_pressed.9.png". Renaming it to *.png.
W: Cant find 9patch chunk in file: "drawable-xhdpi-v4/bubble_shadow.9.png". Renaming it to *.png.
W: Cant find 9patch chunk in file: "drawable-mdpi-v4/notification_bg_normal.9.png". Renaming it to *.png.
I: Decoding values */* XMLs...
I: Baksmaling classes.dex...
I: Baksmaling classes2.dex...
I: Baksmaling classes3.dex...
I: Baksmaling classes4.dex...
I: Baksmaling classes5.dex...
I: Copying assets and libs...
I: Copying unknown files...
I: Copying original files...
root@wiradarma-UX32VD:/home/wiradarma#
```

Gambar 18. Perintah Ekstrak File .apk pada Apktool dan Proses Ektrasi

3. Setelah *apktool* selesai melakukan ekstraksi file .apk dari suatu aplikasi Android, maka folder yang berisi sumber file-file, baik itu kode program, gambar, ataupun file lainnya yang dibutuhkan untuk membangun dan menjalankan aplikasi Android tersebut dapat diakses oleh pengguna. Pengguna dapat melakukan identifikasi maupun perubahan dari source code tersebut untuk membangun suatu aplikasi yang sesuai dengan keinginan pengguna berdasarkan sumber dari .apk yang telah diekstrak. Jika diperlukan, pengguna dapat menggunakan aplikasi *Android Studio* untuk membangun sebuah aplikasi Andoid. Berikut merupakan tampilan file dan folder yang dihasilkan dari proses *reverse engineering* file .apk pada *apktool* :



Gambar 19. Isi File .apk Aplikasi Android yang Telah Diekstrak dengan Apktool

4. KESIMPULAN

Kesimpulan yang dapat diambil dari penelitian ini adalah dengan menggunakan Katoolin, pengguna yang ingin mencoba dan menggunakan tools-tools dengan fungsi penetrasi keamanan sistem komputer yang disediakan oleh distro Kali Linux dapat dipermudah dengan Katoolin. Katoolin dapat memudahkan pengguna yang sudah menggunakan distro Linux dan tidak ingin menggantinya semata-mata hanya untuk menggunakan tools yang terdapat pada Kali Linux. Fleksibilitas yang diciptakan Katoolin bagi pengguna distro Linux lainnya membuat Katoolin menjadi alternatif bagi pengguna yang gemar memakai sistem operasi Linux dalam bidang security, tanpa harus mengganti atau meng-instal secara penuh distro Linux yang sudah dikhususkan dalam bidang security, yaitu Kali Linux.

Hasil penelitian dan implementasi Katoolin sebagai penetrasi tools Kali Linux pada Linux Ubuntu 16.04 yang dilakukan telah berjalan dengan lancar, meskipun masih terdapat beberapa kendala dalam langkah instalasi maupun saat melakukan studi kasus *Reverse Engineering* file .apk menggunakan *apktool*. Melalui kesempatan ini diharapkan pembaca agar lebih memperhatikan dan memahami cara instalasi dan penerapan Katoolin pada distro Linux lainnya agar lebih mempermudah dalam penyelesaian berbagai macam studi kasus dan mendapatkan hasil yang lebih baik.

DAFTAR PUSTAKA

[1] Lee Allen, Tedi Heriyanto, & Shakeel AliKali. 2014. Linux – Assuring Security by Penetration Testing. Packt Publishing.

[2] Raphaël Hertzog, Mati Aharoni, & Jim O'GormanLutz. 2017. Kali Linux Revealed: Mastering the Penetration Testing Distribution. Offsec Press.

[3] Wang, Wego. 2010. Reverse Engineering: Technology of Reinvention. CRC Press, Taylor & Francis Group.

[4] Friesinger, Günther, & Herwig, Jana. 2012. TheArt of Reverse Engineering: Open - Dissect –Rebuild. Department of Art Funding, City of Vienna, Austria.

[5] I Kadek Susila Satwika, I Made Sukafona. 2018. Analisis Coverage Dan Quality Of Service Jaringan WiFi 2,4 GHz Di STMIK STIKOM Indonesia. Jurnal Resistor STIMIK STIKOM Indonesia. Vol. 1 No. 1 Hal. 1-7 2018.

[6] Caroline Layadi, Moh Fajar, Hasniati, Izmy Alwiah Musdar. 2018. Analisis Data Pada Jaringan Sensor Nirkabel Menggunakan Metode Support Vector Machine. Jurnal Resistor STIMIK STIKOM Indonesia. Vol. 1 No. 1 Hal. 8-15 2018.

[7] Amrita, Nair. 2016. Katoolin: Installing Kali Linux Tools on a Debian-based OS. https://opensourceforu.com/2016/11/katoolin-installing-kali-linux-tools-debian-based-os/ .Diakses 11 April 2018.