کار با کلیدهای امنیتی

نوع کاربری: امنیتی

سطح کاربری: مقدماتی، متوسط

نویسنده: سید علی حسینی

پست الکترونیکی: hosseini@iossd.org

تاریخ: ۱۶/۰۳/۸۶

نسخه: ۱۴/۰

منبع: www.gnugpg.org

فهرست

تولید کلید امنیتی 4
نمایش کلیدهای امنیتی 5
کدگذاری بر روی فایلها 6
رمز گشایی فایلهای GPG 7
ورود کلید امنیتی 8
خروج کلید امنیتی 10
ویرایش کلید های امنیتی 12
معرفی کلید های امنیتی دیگر بعنوان کلیدهای معتبر 13

تا به حال خواستین متن یا هر فایل شخصی خودتون رو کد گذاری کنید که توسط افراد دیگری حتی قابل خواندن هم نباشد.

برای این کار ابزار خوبی به نام **GPG** یا **GNU Privacy Guard** در لینوکس وجود دارد (نا گفته نماند که این ابزار برای ویندوز هم تولید شده است). شما بوسیله ابزار قادر خواهید بود کلیه فایلها و حتی ایمیل ارسالی خود را کد گذاری کنید.

حال ما در اینجا آشنایی مختصری با این ابزار خواهیم داشت.

در ابتدا باید بگوییم که هر شخصی می تواند برای خود یک یا چندین کلید امنیتی داشته باشد. این کلید به روش های مختلف گرافیکی و متنی می تواند ساخته شود. در این نسخه از مقاله ما اقدام به آموزش کار با محیط متنی می کنیم.

تولید کلید امنیتی

با وارد کردن دستور زیر شما می توانید اقدام به تولید یک کلید شخصی نمایید.

gpg --gen-key

بعد از اجرای دستور بالا، سیستم سئوالاتی از شما می پرسد که یک به یک به آنها باید پاسخ دهید.

- نوع کلیدی که شما می خواهید ساخته شود؟ که بهتر است حالت پیشفرض را انتخاب کنید.
- حجم و اندازه کلیدی که شما می خواهید بسازید؟ گزینه ۱۰۲۴ یک گزینه خوب برای این سئوال می باشد.
- تعیین مدت زمان اعتبار کلید شما؟ در حالت پیشفرض کلید شما هیچ گاه از بین نمی رود.
- در مرحله بعدی نام واقعی شما توسط سیستم درخواست می شود. که حداقل باید ۵ کاراکتر طول داشته باشد.
- سیستم ایمیل شما را درخواست می کند.
- در صورتی که بخواهید نکته خاصی را در کلید امنیتی خود وارد کنید می‌توانید در این مرحله آن نکته را وارد نمایید.
- در این مرحله کار ورود اطلاعات به پایان رسیده است و اگر شما بخواهید تغییری در اطلاعات خود وارد نمایید می توانید از گزینه هایی که در اختیار شما قرار گرفته استفاده و آنها را ویرایش نمایید. در غیر این صورت با زدن دکمه **O** می‌توانید وارد مرحله بعد شوید.
- در مرحله بعد شما باید برای کلید امنیتی خود یک گذرواژه تعیین نمایید. این مرحله در واقع پایان کار تولید کلید امنیتی می باشد اکنون شما یک کلید امنیتی دارید.

نمایش کلیدهای امنیتی

پس از اینکه شما کلید امنیتی را ساختید. برای اینکه مطمئن شوید که واقعا این کار انجام شده است یا نه می توانید به کمک لیست کردن کلیدهای امنیتی داخل سیستم خود به این واقعیت پی ببرید.

gpg --list-keys $

شاید خروجی شما چیزی شبیه خروجی دستگاه من شود.

root@apache ~]# gpg --list-key]

root/.gnupg/pubring.gpg/

<pub 1024D/C0044DD9 2005-05-31 hosseini <hosseini@iossd.org

sub 1024g/5842C78A 2005-05-31

اگر دقت کنید، خواهید دید که در ابتدای هر سطر در کلمه **PUB** یا **SUB** را می بینید.

این کلمات نشان دهنده کلید امنیتی **Primary** یا **subordinate** هستند. در سیستم من یک کلید امنیتی با نام حسینی وجود دارد که کلید اصلی سیستم من می باشد.

پس از اینکه از وجود کلید امنیتی خود مطمئن شدید، می بایست برویم سراغ کد گذاری بر روی فایل مورد نظر خود.

کدگذاری بر روی فایلها

برای کد گذاری بر روی یک فایل کافیست از دستور زیر استفاده نمایید.

gpg --encrypt --recipient hosseini foo.txt

یا

gpg -e -r hosseini foo.txt

در پایان اجرای این دستور فایل اصلی شما سر جای خود قرار دارد و تنها یک کپی از آن توسط ابزار **GPG** کدگذاری شده است. فایل جدید شما دارای پسوند **gpg**. می باشد.

رمز گشایی فایلهای GPG

پس از اینکه یک فایل را رمز گذاری نمودید، حال نوبت به آن می رسد که حال همان فایل را رمزگشایی کنید. شما می توانید توسط دستور زیر فایل خود را رمزگشایی نمایید:

gpg --output foo.txt --decrypt foo.txt.gpg

در صورتی که شما دارای کد امنیتی خاص این فایل باشید و همچنین کلمه عبور آنرا در اختیار داشته باشید می توانید این فایل را رمزگشایی نمایید.

ورود کلید امنیتی

زمانی فرا می رسد که ما نیاز داریم فایل خود را برای یکی از دوستان خود ارسال نماییم و چون نمی خواهیم کلمه عبور کلید امینیتمان از دست برود پس بهترین راه این است که از کلید امنیتی دوستمان برای کد گذاری فایل استفاده نماییم.

خوب حالا چه کنیم؟

برای اینکار دوستمان می بایست کلید امنیتی خود را برای ما ارسال نماید تا ما بتوانیم آنرا در سیستم خود وارد کنیم و فایل مورد نظر را رمزگذاری نماییم. روش انجام این کار به طریقه زیر است:

gpg --import /tmp/reza.gpg $

نتیجه:

gpg: key E78DAE88: public key imported

gpg: Total number processed: 1

gpg: imported: 1

دستور بالا کلید امنیتی دوستمان را از مسیر مشخص شده برداشته و وارد سیستم کدگذاری دستگاه ما می کند.

اکنون اگر از سیستم رمزگذاری دستگاه خود لیستی بگیریم می بینیم که کلید امنیتی دوستمان نیز به کلید امنیتی ما اضافه شده است.

gpg --list-keys $

نتیجه:

root/.gnupg/pubring.gpg/

<pub 1024D/C0044DD9 2005-05-31 hosseini <hosseini@iossd.org

sub 1024g/5842C78A 2005-05-31

<pub 1024D/E78DAE88 2003-02-11 reza <reza@iossd.org

sub 1024g/0CF774C4 2003-02-11

خروج کلید امنیتی

برای خارج کردن کلید امنیتی می توانید از دستور زیر استفاده نمایید:

gpg --output /root/hosseini.gpg --export hosseini@iossd.org $

یا

gpg --armor --export ljohn > ljohn.gpg.asc $

در اولین حالت خروجی کار شما فقط یک کلید هگزا دسیمال می باشد

و در حالت دوم خروجی کار شما کد اسکی بوده و به صورت زیر می باشد که در یک فایل با پسوند **asc**. ذخیره می شود.

-----BEGIN PGP PUBLIC KEY BLOCK-----

(Version: GnuPG v1.0.7 (OpenBSD

mQGiBD5H/vURBACHhxmStFpXFLgIZU3PrLDbso6puxn8onDVcARojwKd3J1PdffG

S3XzQDcReNbvQ8XgU210tX69SoUaGihfnRz/7I9YlpPwzBp1CmzWVp7qkk+mjQaC

GhxJ1YOEnykWjyJQunSDwmoLWCiI7HZpXJHZjVfbvv5x2xVYyMbEsKtK5wCg8J0K

9QNs4y7F17+liuqhGhjy7esD/jQYKkGsHaWgnrHhI8kLpCgSx65FY2dd8UJMAGZZ

YFPyWwuAwUeonNEHD/I7T6ajhpFzu5sFAYdQNdcu0MjSBf/VNOiPqQbtKWn7OvPw

tpX0y7sDSDfhQa0c7O1iAV5O/gSWoV1i9LdxGbsOGlQNovIqbOvvVsiS7dK6brhC

ieZ6A/9PwTaVlEsjR7GDC94HKPs9b84rQ/4boNA58GyY7aHmdIF6B8s7aiNruXNL

nVQ47dhtxDqhqtEU4CAnfMxiW9z8Ef4CRMDZIbNX16Q4byn3IJzbrDT9Fhq3kUw4

I/I0uiZMN3X6gPuq65dGiGXq9J8lN2AIYpZ+D3cvoBXMV6GEG7QgTGl0dGxlIEpv

aG4gPGxqb2huQHNoZXJ3b29kLm5ldD6IWQQTEQIAGQUCPkf+9QQLBwMCAxUCAwMW

AgECHgECF4AACgkQHnUc+lVwnqsj1wCfbOCuG+LqnWEvUwJwFteU3kIAItoAoMf8

VtZDfBP2l5k+C7iMNJhfp6ziuQENBD5H/wcQBACt6sWIxnhPboYtEItNbHNzvijU

qXIF+EK+KIaiIOAoikPH2fYdL6c4nGINmddGtkrGAHec0uvZC7zdJG1TLp6uUQ7a

AxHuw0FIDgJqG3kLHucOstJ0hZe//nFd16B/Ag+H9mT7Hr+ZpAX7sfytpNb/Dr+6

53rZAfG6hC+DvWJxVwADBQP/Zrl8rInc/9YtNIeU/vefiV6KHBBbltM69IrNmVGp

AXtfWwtDYIArU5P+7KEhH8bYOdePirXa044SYmMr1Afq2vX0ooUdpyG3sV2u7/w0

6MieoOUCQ7kdZZMVcsLjcBxGBi1xxsIuODi/vw/P/xWVMsv/CaUxwuKlHPTLT+J5

UtCIRgQYEQIABgUCPkf/BwAKCRAedRz6VXCeq6rmAJ9hk3qdVzjEg/uN6wQeU9Bj

=FnamqgCgpuLMZIUiUkMHpK0IpCrjfmyXebc

EHgv=

-----END PGP PUBLIC KEY BLOCK-----

ویرایش کلید های امنیتی

برای ویرایش کلید امنیتی که در حال استفاده از می باشید باید از دستور زیر استفاده کنید:

gpg --no-greeting --edit-key C0044DD9 $

خروجی شما چنین خواهد بود:

.Secret key is available

pub 1024D/C0044DD9 created: 2005-05-31 expires: never trust: u/u

sub 1024g/5842C78A created: 2005-05-31 expires: never

<Hosseini <hosseini@iossd.org .(**1**)

<Command

بعد از نمایش کلید های امنیتی موجود در سیستم، شما وارد یک محیط کامندی می شود که منتظر ورود دستور شما می باشد.

معرفی کلید های امنیتی دیگر بعنوان کلیدهای معتبر

برای معرفی کردن یک کلید امنیتی که توسط شما وارد سیستم امنیتی شده است بعنوان یک کلید مطمئن و معتبر می بایست آن کلید را ویرایش نماییم. پس می بایست از دستور ویرایش کلید به صورت زیر استفاده نماییم.

gpg --no-greeting --edit-key C0044DD9 $

برای ادامه کار و ادامه ورود دستورات مربوط به معتبر بودن یک کلید می توانیم از کلیدهای زیر استفاده کنیم:

trust: A/B

حرف کلیدی **A** در صورتی در مقابل دستور **trust** قرار می گیرد که بخواهیم این کلید صاحب اصلی کلید باشد. و در صورتی که بخواهیم غیر از این حالت را برای کلید انتصاب کنیم از کلیدهای زیر به ازای حرف **B** استفاده می نماییم:

-	**No owner trust assigned / not yet calculated**
e	**Trust calculation has failed; probably due to an expired key**
q	**Not enough information for calculation (unknown)**
n	**Never trust this key**
m	**Marginally trusted**
f	**Fully trusted**
u	**Ultimately trusted**