الآن يجب ان نقوم بانشاء ملف على جهاز الخادم الذي سيستقبل اتصال SSH يدعى
```
~/.ssh/authorized_keys
```
ونلصق داخله المفتاح الأساسي الذي تم انشاؤه في ملف id_rsa.pub على جهاز العميل.
كما يجب تغيير الصلاحيات للملف على النحو التالي:
```
chmod 600 ~/.ssh/authorized_keys
```
للتأكد من استعمال طريقة الPublic/Private key authentication تأكد من وجود الأسطر التالية مفعلة داخل ملف الاعدادات على الخادم:
```
RSAAuthentication yes
PubkeyAuthentication yes
AuthorizedKeysFile %h/.ssh/authorized_keys
```
واذا أردت منع عمليات التوثيق باستخدام كلمات السر و الاعتماد فقط على طريق المفتاح العام والخاص سنقوم بتغيير القيمة yes الى no في السطر التالي في ملف الاعدادات:
```
PasswordAuthentication no
```

ماذا عن الجدار الناري؟

ان الجدار الناري Firewall في أنظمة اللينوكس تتميز بمرونة فائقة تميزها عن عن غيرها من الجدران النارية، إن تنفيذ امرين كالتالي كفيلين بمنع المستخدم في حالة ادخال كلمة مرور خاطئة من محاولة الدخول مرة أخرى إلا بعد مرور دقيقة واحدة:
```
iptables -A INPUT -p tcp -m state --syn --state NEW --dport 22 -m limit --
limit 1/minute --limit-burst 1 -j ACCEPT

iptables -A INPUT -p tcp -m state --syn --state NEW --dport 22 -j REJECT --
reject-with tcp-reset
```

الخاتمة

لعلك لاحظت عزيزي القارئ أن هناك طرق عديدة تساعد على رفع مستوى الحماية و الأمان على خادمك ،وقد تطرقنا لبعضها و ما اعتبره الأهم ربما في وجهة نظري، ولكن تذكر عزيزي أنه ما دام خادمك موصول بالانترنت فأنت لست بامان أبدا من المخترقين!!.