استخدام بروتوكول SSH 2

هناك نوعين من بروتوكولات SSH و الاصدار رقم ٢ يحمل العديد من المزايا مثل التصدي لعمليات man-in-the-middle attaks و insertion attacks .

قم بتعديل السطر التالي في ملف الاعدادات حسب التالي:

```
Protocol 2,1
```

ليصبح:

```
Protocol 2
```

تحديد عدد مرات كلمات السر الخاطئة بواسطة SSH

في الوضع الافتراضي فإن الخدمة تقوم باستقبال ٥ محاولات ادخال لكلمة السر للمستخدم، و بتعديل السطر التالي او اضافته نستطيع تغيير هذه القيمة الافتراضية:

```
NumberOfPasswordPrompts 2
```

تحديد المستخدمين القادرين على استعمال SSH

ينصح خبراء الحماية بمنع المستخدم الجذري root من الوصول الى الخادم باستخدام الSSH كاجراء احترازي فقط كون البورتوكول بالأساس يمنع عمليات التجسس كما ذكرنا سابقا. على سبيل المثال في حالة فقدان جهاز خاص عليه كلمة سر الخاصة بالجذر أو غيرها من الأمور غير المتوقعه.

يتم ذلك باضافة او تعديل السطر التالي الى ملف الاعدادات الخاص بالSSH :

```
PermitRootLogin yes
```

ليصبح :

```
PermitRootLogin no
```

ويمكننا تحديد اسماء المستخدمين القادرين على تسجيل الدخول للخادم باضافة السطر التالي الى نفس الملف:

```
AllowUsers grey binary muslim
```

حددنا ٣ مستخدمين فقط قادرين على الوصول لخدمة SSH على الخادم.

استخدام طريقة RSA Public Key لتسجيل الدخول دون الحاجة لكلمة مرور.

تعتبر هذه الطريقة من الطرق الفعالة جدا لمنع هجمات dictionary attacks ، حيث ان الطريقة تعتمد اسلوب التوثيق باستخدام المفتاح العام والخاص Public/Private Key Pair بدلا عن طريقة كلمة السر المعتادة.

تتلخص الطريقة بانشاء مفتاح عام و خاص على جهاز العميل الذي سيستخدم للوصول للخادم باستخدام الامر:

```
ssh-keygen -t rsa
```

يمكنك قبول الاعدادات الافتراضية لانشاء المفاتيح الخاصة بالتدقيق. بعد الانتهاء من الأمر السابق سيقوم الأمر بانشاء ملفين هما

```
~/.ssh/id_rsa
~/.ssh/id_rsa.pub
```