

السراج عليك و رحمة الله و بركانه

أريد أن أتحدث عن هذا الموضوع اليوم، لأن أغلب المستخدمين العاديين في اللينوكس ليس لديهم معلومات عن هذا الموضوع، و أريد فقط أن أبين ما هو SSH (Secure Shell) و أيضا كيفية استخدامه و ما هي مميزاته و فوائده...

النقاط التي سأحدث عنها:

1. ما هو ال SSH و ما هو عمله
2. لماذا الحاجة له؟
3. الاتصال عبره و التعامل معه
4. نقل الملفات عبر SCP و SFTP
5. نقاط أخيرة أود الحديث عنها

ما هو SSH:

ال SSH أو ال Secure SHell هو عبارة عن بروتوكول شبكة، يستخدم للاتصال بين الأجهزة و التحكم بها عن بعد، ميزة هذا البروتوكول أنه آمن، بعكس باقي البروتوكولات التي تستخدم لهذا الغرض، مثل Telnet و FTP، فهذه البروتوكولات تفتقد للحماية، و قد يقوم أي دخیل باعتراض البيانات المرسلة في الجلسة و تغييرها و بالتالي حدوث مشكلة أمنية في حال كان الاتصال بالطرف الثاني مهم و حساس، و لذلك لو تم استخدام SSH فلن يتمكن أحد من اختراق الجلسة و التغيير فيها...

هذا البروتوكول مستخدم بشكل أساسي و بكثرة على أنظمة Gnu/Linux و Unix، و كما أسلفت هو أكثر أمانا من البروتوكولات الأخرى، و تم تصميمه ليكون بديل ال Telnet و باقي بروتوكولات الاتصال الغير آمنة...

بعض النقاط المهمة عن ال SSH:

- يستخدم التشفير باستخدام المفتاح العام أو المعلن ليقيم بتعريف الطرف البعيد الذي يريد الاتصال به و التصريح له بالاتصال...
- استخدام ال SSH الأساسي هو الدخول للأجهزة التي تحوي على خدمة تعمل و تقبل الاتصالات عبره و لكن أيضا يمكن استخدامه في نقل الملفات باستخدام بروتوكولات مرفقة معه و هي: [SFTP](#) أو [SCP](#) و يمكن أيضا عبره عمل اتصالات X11 للتحكم بسطح المكتب البعيد... و هناك عدة مميزات أخرى له، سأضع لها روابط في النهاية في قسم الروابط...

•المنفذ الأساسي المستخدم لهذا البروتوكول هو 22

• هذا البروتوكول يستخدم بيئة الخادم/العميل، بمعنى أنه لا بد من تواجد خدمة تعمل في الـ Background على الجهاز الآخر البعيد تقوم بقبول الاتصالات ليتم الاتصال عبرها...

حاليا يوجد إصدارين من هذا البروتوكول:

• SSH 1.0: في عام 1995 تم تصميم النموذج الأول لهذا البروتوكول، و كان يحمل اسم SSH-1
• SSH 2.0: في 2006 تم تشكيل فريق اسمه Secsh من قبل IETF (Internet Engineering Task Force) للعمل على البروتوكول الجديد الذي يحمل اسم SSH-2 الآن... و هو المستخدم حاليا.

لماذا الحاجة له؟:

من الطبيعي أن تكون أهم نقطة في هذا الموضوع هي الأمان العالي، فمع وجود أكثر من طريقة للتشفير في الاتصال (Blowfish - triple-DES)، تكون هناك حماية من الهجمات من نوع (الرجل في الوسط) أي بلغة أخرى الدخلاء على الجلسة الحالية، و أيضا مع استخدام تقنية تشفير RSA فلن يكون هناك داعي للقلق عند نقل العرض من الجهاز البعيد للجهاز المحلي المتصل به...

الاتصال عبره و التعامل معه:

أمر الاتصال عبر SSH بسيط جدا- كما هو الحال مع الـ Telnet و غيرها... فقط يتم كتابة الأمر:

```
ssh username@hostname
```

مع استبدال username باسم المستخدم الذي يملك صلاحية الاتصال بالجهاز الهدف و hostname باسم الجهاز الهدف الذي تريد الاتصال به، و سيتم عمل الاتصال بالسيرفر و طلب كلمة المرور...

في حال كان الاتصال بالسيرفر على منفذ غير المنفذ الافتراضي (22) فيمكن استخدام الأمر التالي:

```
ssh -p [port] username@hostname
```

عند استخدام لينوكس، فإنه يحوي برنامجا موجود مسبقا على النظام للاتصال عبر SSH، كل ما علينا عمله هو فتح الترمينال أو أي برنامج آخر للشل و تنفيذ الأمر السابق مع تغيير اسم المستخدم و كلمة المرور، و سيتم عمل الاتصال بالسيرفر...

في حال لم يكن هناك برنامج مضمن مع النظام (في حال كنت تستخدم ويندوز) فيمكن تحميل هذا البرنامج و استخدامه للاتصال بالسيرفر:

<http://www.chiark.greenend.org.uk/~sgtatham/putty/download.html>

كما ذكرت عند الاتصال بالسيرفر سيسأل عن اسم المستخدم و كلمة المرور، و بعد إدخالها سيقوم السيرفر بنقلك لمجلد الـ Home الخاص بك (الخاص بالمستخدم الذي قام بتسجيل الدخول) و يمكنك سرد محتوياته بالأمر ls كما في الصورة التالية:

[illegible]

و تستطيع الآن التعامل معه كأنك تتعامل مع أي نظام لينوكس آخر، و كل الأوامر ستعمل كما لو أنك تستخدم الجهاز مباشرة...

الأوامر التي يمكن التعامل بها مع السيرفر عند الاتصال ب SSH هي نفسها أوامر الـ لينوكس، و لذلك يجب أن تكون لديك خلفية جيدة عن التعامل مع الـ لينوكس باستخدام الأوامر...

نقل الملفات عبر SCP و SFTP:

SCP تعني Secure Copy و لو ركزنا فيها قليلا سنجدها نفسها CP و لكن مع إضافة S للأمان، و هذا يعني أن الأوامر المستخدمة للنسخ تعمل بنفس مبدأ عمل أوامر CP كما سنلاحظ الآن...

لنقل ملف باستخدام SCP عبر SSH، تكون صيغة الأمر كالتالي: (الموضوع جدا بسيط و لا يحتاج أكثر من أمر واحد)

```
scp [file name] user@server:folder
```

الأمر السابق جدا بسيط:

file name: نستبدلها باسم الملف الكامل الذي نريد نسخه على السيرفر
user@server:folder: نستبدل user باسم المستخدم الذي يملك صلاحية الاتصال عبر ssh و server تكون اسم السيرفر الذي نريد الاتصال به، و folder هو اسم المجلد على السيرفر الذي نريد نسخ الملف إليه...

هذا مثال على الأمر، قمت بنسخ ملف اسمه file.txt إلى السيرفر داخل مجلد اسمه public_html

```
C:\Program Files (x86)\OpenSSH\bin>scp file.txt [redacted]com:public_html
Could not create directory '/home/SalehRam/.ssh'.
The authenticity of host '[redacted].com (66.147.244.181)' can't be established.
RSA key fingerprint is [redacted].
Are you sure you want to continue connecting (yes/no)? y
Please type 'yes' or 'no': yes
Failed to add the host to the list of known hosts (/home/SalehRam/.ssh/known_hosts).
[redacted]s password:
file.txt                                100%   4    0.0KB/s   00:00
C:\Program Files (x86)\OpenSSH\bin>
```

و يمكن أيضا نسخ ملفات من السيرفر البعيد إلى الجهاز المحلي، و ذلك عبر الأمر:

```
scp user@server:path_to_file [destination name on the local pc]
```

المتغيرات في الأمر السابق هي نفسها و لكن مع تغيير بسيط، يكون أمر SCP في البداية ثم يليه مكان الملف الموجود على السيرفر البعيد الذي نريد نسخه، و بعد اسم الملف على الجهاز المحلي الذي نريد نسخه إليه...

يمكن أيضا نسخ مجلدات من و إلى السيرفر و ذلك عبر الأمر التالي:

```
scp -r user@server:path_to_file [destination folder name on the local pc]
لنسخ مجلد من السيرفر إلى الجهاز المحلي
scp -r [source folder name on the local pc]
لنسخ مجلد من الجهاز المحلي إلى السيرفر user@server:destination_folder
```

بالنسبة لنقل الملفات عبر SFTP:

فالموضوع مماثل تماما لـ SCP و صيغة الأمر:

```
sftp username@hostname
```

عند تنفيذ الأمر السابق، سيتم طلب كلمة المرور للمستخدم الذي تم إدخاله، و عند إدخالها سيقوم النظام بالدخول للسيرفر البعيد و بدء تلقي الأوامر، و صيغة الأوامر تكون كالتالي:
أولا، لتكون على علم أين أنت يجب معرفة مكان العمل الحالي على كل من السيرفر البعيد و الجهاز المحلي، و للقيام بذلك، نقوم بتنفيذ الأمرين التاليين:

```
pwd // يعرض مكان العمل الحالي على السيرفر البعيد
```

```
lpwd // يعرض مكان العمل الحالي على الجهاز المحلي
```

و لتتمكن من الوصول للمكان الذي تريده على السيرفر البعيد، تستطيع استخدام الأمر التالي لتغيير المسار:

```
[cd [remote_directory
```

و مثله أيضا على الجهاز المحلي نستخدم الأمر التالي لتغيير المسار الحالي (مكان العمل):

```
[lcd [local_directory
```

لنسخ ملف من السيرفر البعيد إلى الجهاز المحلي (سيتم نسخ الملف في مكان العمل الحالي):

```
[get [remote_file_name
```

و كمثال عليه، أريد أن أقوم بنسخ ملف اسمه file.txt من السيرفر فيكون الأمر كالتالي:

```
get file.txt
```

عند تنفيذ الأمر السابق سيتم نسخ الملف من السيرفر إلى الجهاز المحلي في مكان العمل الحالي..

و لوضع ملف ما من الجهاز المحلي على السيرفر البعيد، يتم تنفيذ هذا الأمر:

```
put [local_file_name]
```

سيتم عند تنفيذ الأمر السابق نسخ الملف المطلوب من الجهاز إلى السيرفر البعيد و وضعه في مسار المجلد الحالي

يوجد عدة أوامر أخرى يجب معرفتها، و هي كالتالي:

```
ls // تعرض الملفات الموجودة داخل دليل على السيرفر البعيد
```

```
lls // تعرض الملفات الموجودة داخل المجلد الحالي على الجهاز المحلي
```

```
mkdir // يقوم بعمل مجلد جديد على السيرفر داخل المجلد الحالي
```

```
mkdir //المجلد الجديد داخل المجلد الحالي على الجهاز المحلي
rename //يقوم بعمل إعادة تسمية لملف على السيرفر البعيد
rm //يقوم بحذف ملف من السيرفر البعيد
rmdir //يقوم بحذف مجلد من السيرفر البعيد
exit //يقوم بإنهاء الجلسة الحالية و قطع الإتصال
```

يوجد عدة أوامر أخرى، و لكنني لن أتطرق لها، فالموضوع هو فقط عبارة عن توضيح لهذه التقنية و كيفية استخدامها بدون أن أدخلك في تفاصيل الأمان و طرق توليد المفاتيح الخاصة بها و غيرها من التفاصيل المتقدمة قليلا...

نقاط أخيرة أود الحديث عنها:

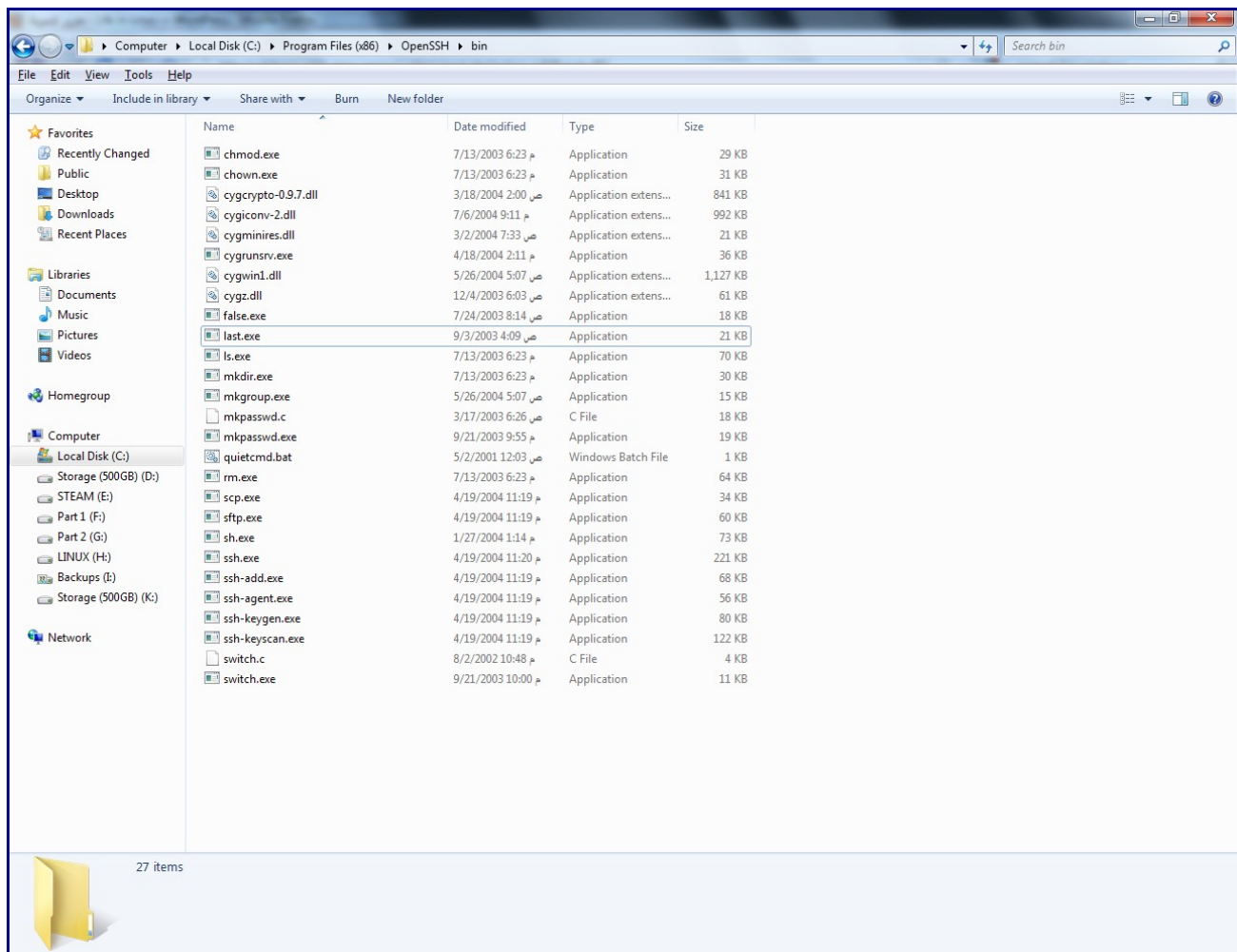
كما لاحظتم، فإن التعامل مع SSH و SCP تقريبا يعني التعامل مع اللينوكس، لأن كل الأوامر المستخدمة فيها هي في الواقع أوامر في نظام اللينوكس، حتى أمر النسخ في SCP، هو نفسه تماما الأمر CP لكن مع إضافة الـ S و تغير شكل أحد عوامل الأمر، حيث يكون أحد عوامله هو السيرفر البعيد، الذي تكون كتابته دائما بالطريقة user@server، و لذلك لا بد من معرفة الأوامر الأساسية على الأقل للتمكن من التعامل مع هذه البروتوكولات و تصبح قادر على استخدامها...

أود الإشارة أيضا إلى بعض الأشياء التي استخدمتها في هذا الدرس:

• استخدمت لتشغيل الـ SSH على الويندوز برنامج OpenSSH for Windows و

يمكن الوصول لصفحته من [هنا](#)

• عند تثبيت OpenSSH for Windows سيتم عمل مجلد داخل دليل تثبيته اسمه bin يحوي الملفات اللازمة لتشغيل SSH و SCP كما تلاحظون في الصورة التالية:



• للاتصال بسيرفر عبر SSH من داخل ويندوز، يفضل تحميل برنامج PuTTY من هنا