بروتوكول SSH

اعداد الطلاب:

اوليان رواد كوسه رهف راجي اسطة

الاختصاص: هندسة اتصالات

السنة : الخامسة

بإشراف :الدكتور مهند عيسى


SSH

ملخص عن المشروع:

SSHبروتوكول النقل الآمن:

هو بروتوكول للنقل الآمن للمعلومات، وخدمات الحماية عن بعد أو لتنفيذ أوامر وخدمات أخرى بين حاسوبين متصلين بشبكة التي تربطهما عن طريق قناة أمنة من خلال شبكة غير أمنة وهو مبني على نموذج الخادم/العميل.

سيتم التحدث عن:

تعريف بروتوكول **SSH**

بعض مميزات بروتوكول **SSH**

آلية العمل

الاختلافات الرئيسية بين**SSH** و**TELNET**

تعريف بروتوكول SSH

هو بروتوكول النقل الآمن (Secure Socket Shell)

أو (Secure Shell)

هو بروتوكول شبكيٌّ يوفر للمستخدمين طريق آمن للوصول الآمن للحواسيب عبر الشبكة.

ويشير هذا المصطلح إلى مجموعة الأدوات المساعدة التي تنفذ بروتوكول SSH أيضاً.

يوفر هذا البرتوكول اتصالًا مشفراً بين جهازي حاسب متصلين عبر شبكة مفتوحة كالإنترنت، ويستخدم على نطاقٍ واسعٍ من قبل مسؤولي النظام والشبكة لإدارة الأنظمة والتطبيقات عن بعدٍ ممّا يتيح للمستخدمين قيامهم بتسجيل الدخول إلى مختلف أجهزة الكمبيوتر عبر الشبكة والقيام بتنفيذ الأوامر وعمليات نقل الملفات من جهاز لآخر.

بروتوكول (SSH)

هو بروتوكول مهمته الاهتمام بإدارة الحماية لتنفيذ المراسلات عبر الشبكة ويشمل عمليات التشفير والتوثيق وسلامة البيانات عند تبادلها.

تم تصميم بروتوكول (SSH) كبديل لبروتوكول (TELNET) وغيره من العديد من البروتوكولات التي تعتبر غير آمنة، والتي تقوم بإرسال المعلومات، لاسيما كلمات المرور، كنص عادي(Clear TexT)

غير المشفر، ممّا يجعلها عرضة للاعتراض والكشف عن محتواها وذلك عن طريق استخدام المخترقين لطرق لتحليل الحزم وبرامج (Sniffing).

تتلخص استخداماته فيما يلي :

1) يستخدم لتوفير الوصول الآمن للمستخدمين.

2) نقل الملفات بسهولة وتلقائية بين الأجهزة.

3) إصدار الأوامر عن بعد.
4) القيام بإدارة البنية التحتية للشبكة وتنظيم غيرها العديد من مكونات النظام الهامة.

بعض مميزات بروتوكول SSH:

1) تسجيل الدخول الآمن عن بعد:

على فرض أنَّك قمت بتسجيل الدخول لعدد من أجهزة الكمبيوتر المختلفة، تتيح البروتوكولات مثل (TELNET) للمستخدمين قيامهم بتسجيل الدخول إلى كمبيوتر وذلك من جهاز كمبيوتر آخر. تكمن المشكلة الأكبر في أن هذه البروتوكولات تنقل اسم المستخدم وكلمة المرور في نص عادي عبر الإنترنت ويمكن لأي طرف ثالث اعتراضه والتطفل عليها؛ لذا طُور (SSH) ليتجنب مثل هذه المشاكل عن طريق إرسال هذه المعلومات بطريقةٍ مشفرة فلا يمكن اختراقها والوصول إليها من قبل طرف

خارجي، كما يتم تشفير جلسة العمل بأكملها بالطريقة ذاتها أيضاً.

2) النقل الآمن للملفات:

في حال لديك عدَّة حساباتٍ مختلفةٍ على عدة حواسيب، وتريد نقل ملف من أحدها للآخر، لا توفر برامجُ النقل التقليدية أو البروتوكولات التقليدية النقلَ الآمن لهذه الملفات عبر نقلها خلال الشبكة، أمّا باستخدام SSH فيمكن نقل الملفات بشكلٍ آمنٍ بين الأجهزة.

3) تنفيذ الأوامر عن بعد:

على فرض أنّ أحد مسؤولي النظام هم بحاجة إلى تشغيل نفس الأمر على عدّة أجهزة. بحيث يوفر بروتوكول النقل الآمن إمكانية القيام بهذا الأمر على عدة أجهزة

وذلك مع القيام بتشفير كل أمرٍ أثناء نقله بين هذه الأجهزة.

٥) المفاتيح :

عند استخدام مجموعةٍ من الحسابات فلا بد أن توفر مجموعة من كلمات المرور لها جميعاً، ويتطلب الأمر الكثير لتذكر هذه المجموعة. ليس هذا فحسب، بل تشكل قضية تذكر كلمة السر المرتبطة بكل حساب المشكلة الأكبر. ولا تفيد آلية كتابتها على دفتر خاص نفعاً في بعض الأحيان وخاصةً إن نسيت الاحتفاظ بهذه الورقة في كل مرة. في سبيل إيجاد حلول لهذه المشكلة، برزت فكرة المفاتيح مع بروتوكول النقل الآمن والتي طرحت كبديل عن كلمات المرور.

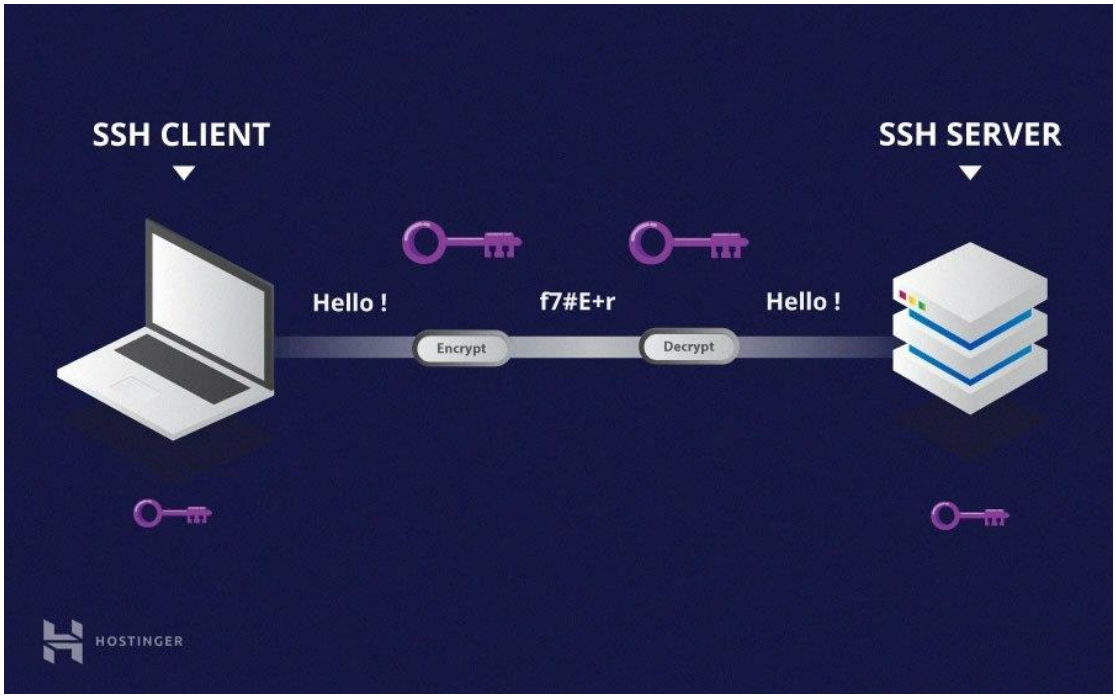
وتشكل هذه المفاتيح مجموعة من البتات المشفرة التي لا يمكن استخدامها إلا بعد إدخال كلمة مرورٍ مناسبة للتعرف على المستخدم. وهكذا يمكن مصادقة جميع

الحسابات بشكل آمن دون الحاجة إلى حفظ العديد من كلمات المرور.

٥)التحكم في الدخول:

يضطر أحدنا في بعض الأحيان إلى السماح لصديق أو أي شخص آخر استخدام حاسبه الشخصي لأغراضٍ معينة، ويمكن السماح لهذا الشخص باستخدام الحساب دون اطلاعه على كلمة المرور الخاصَّة بالمستخدمين، بالإضافة إلى قدرتنا على تحديد صلاحيات الوصول المتاحة له.

آلية العمل:



يتطلب الاتصال عبر الشبكة باستخدام بروتوكول النقل الآمن عمل ثلاث طبقات بشكل متكامل بالشكل الآتي:

طبقة النقل: تعالج هذه الطبقة تبادل مفاتيح التشفير بين الأجهزة، وتدير عملية الاتصال طوال الجلسة.

طبقة المصادقة: هي الطبقة التي تمكن المستخدم من الوصول إلى الحاسب الآخر وذلك باستخدام عدة أساليب متنوعة للحصول على هذه المصادقة. ويعتبر الأسلوب الأكثر شيوعاً واستخداماً هو استخدام كلمة المرور واسم المستخدم.

طبقة الاتصال: هي الطبقة التي تعمل عليها واجهة (SSH) وتشمل تطبيقات الوصول.

□□□□□□□□□□
□□□□□□□□ □□□
(SSH) □ (TELNET):

1) يقدم كلا البروتوكولين الخدمة ذاتها نظرياً والتي تتمثل بالاتصال بالحاسب البعيد.

إلَّا أنَّ وTELNET يمثل بروتوكول تقليدي، في حين يقدم (SSH) ميزات محسنة.

2) لا يوفر (TELNET) أي من الجوانب الأمنية، في حين يعتبر (SSH) أكثر أماناً.

3) تنتقل البيانات في نصٍّ عاديٍّ وهو ما يعرضها لسهولة الاختراق، بينما يستخدم (SSH) التشفير في نقل البيانات.

4) يعمل بروتوكول (TELNET) مع الشبكات الخاصة، ويعمل الآخر مع الشبكات العامة.

5) يتصل (TELNET) عبر المنفذ "Port 23" عبر (TCP/IP)،

ويتصل بروتوكول (SSH) عبر المنفذ "Port 22".

بعض الأسئلة:

أين يقع هذا البروتوكول؟

يقع ضمن الطبقة السابعة من الطبقات المستخدمة في نظام الشبكات(osi layer)

ما الذي يمكن نقله عبر هذا البروتوكول؟

يمكن استخدام ssh لنقل كل من:

1) الأوامر البرمجية
2) البيانات والنصوص

3) الملفات (حيث يتم استخدام sftpوهو في الاساس نسخة مشفرة من بروتوكول(FTP

كيف يتم انشاء قناة مشفرة؟

- تطبيق التشفير المتناظر Symmetrical Encryption

لكي يتم تطبيق التشفير المتناظر يتم تحديد مفتاح لخوارزمية التشفير يتفق الطرفان عليه قبل بدء الاتصال ويستخدم المفتاح لكل من التشفير وفك التشفير الرسائل بين الجهازين.

- تطبيق التشفير الغير متناظر Asymmetrical Encryption

كما لاحظنا عند تطبيق التشفير المتناظر تواجهنا مشكلة تبادل

المفتاح حيث يكون المفتاح غير مشفر ومتاح للجميع ويتم حل هذه المشكلة باستخدام خوارزمية تبادل المفتاح Key Exchange Algorithm حيث يتم استخدام مفتاحين مختلفين: أحدهما عمومي يتفق عليه الطرفين ويمكن مشاركته والاخر خاص بكل جهاز لا يتم مشاركته اطلاقًا فلو قام جهاز العميل (client) بإرسال رسالة عن طريق تشفيرها بالمفتاح العمومي سيتمكن فقط من قراءتها بعد عن طريق فك تشفيرها باستخدام المفتاح الخاص الذي لديه.

كيف يتم التحقق من سلامة البيانات المرسلة؟

لكي يتم التحقق من سلامة البيانات المرسلة نقوم باستخدام الـ HMAC

وهي اختصار لـ Hash-based Message Authentication Codes حيث يتم مع كل رسالة توليد رمز HASH عن طريق استخدام مفتاح التشفير التناظري وهذا الرمز لا يمكن فك تشفيره هو فقط للتأكد من انه لم يتم التلاعب بالبيانات المرسلة بين الجهازين.

كيف يتم التحقق من الهوية؟

التحقق من الهوية Authentication

هناك عدة طرق للتحقق من الهوية منها:

عن طريق كلمة المرور باستخدام المفتاح العام Public-Key Authentication

حيث يقوم جهاز العميل (client) باستخدام اسم مستخدم وكلمة مرور للدخول بالخادم (Server) عن طريق الاتصال المشفر.

عن طريق استخدام التشفير الغير متناظر

حيث يتم تسجيل الدخول دون الحاجة الى كلمة مرور

- المراجع:
- https://www.matrix219.com/index/2017/06/30/%D8%A8%D8%B1%D9%88%D8%AA%D9%88%D9%83%D9%88%D9%84-ssh/

- https://e3arabi.com/%D8%A7%D9%84%D8%AA%D9%82%D9%86%D9%8A%D8%A9/%D9%85%D8%A7-%D9%87%D9%88-%D8%A8%D8%B1%D9%88%D8%AA%D9%88%D9%83%D9%88%D9%84-%D8%A7%D9%84%D9%86%D9%82%D9%84-%D8%A7%D9%84%D8%A2%D9%85%D9%86-/ssh%D8%9F
- https://www.matrix219.com/m/index

الجزء العملي:

مقدمة عن الكود:

كيفية تحميل ملف باستخدام SSH في Python تحميل ملف باستخدام SSH يضبط ملف محلي إلى دليل بعيد على اتصال آمن

الكود:

```
"host = "demo.wftpserver.com
port = 2222
"password = "demo-user
"username = "demo-user


()ssh = paramiko.SSHClient
```

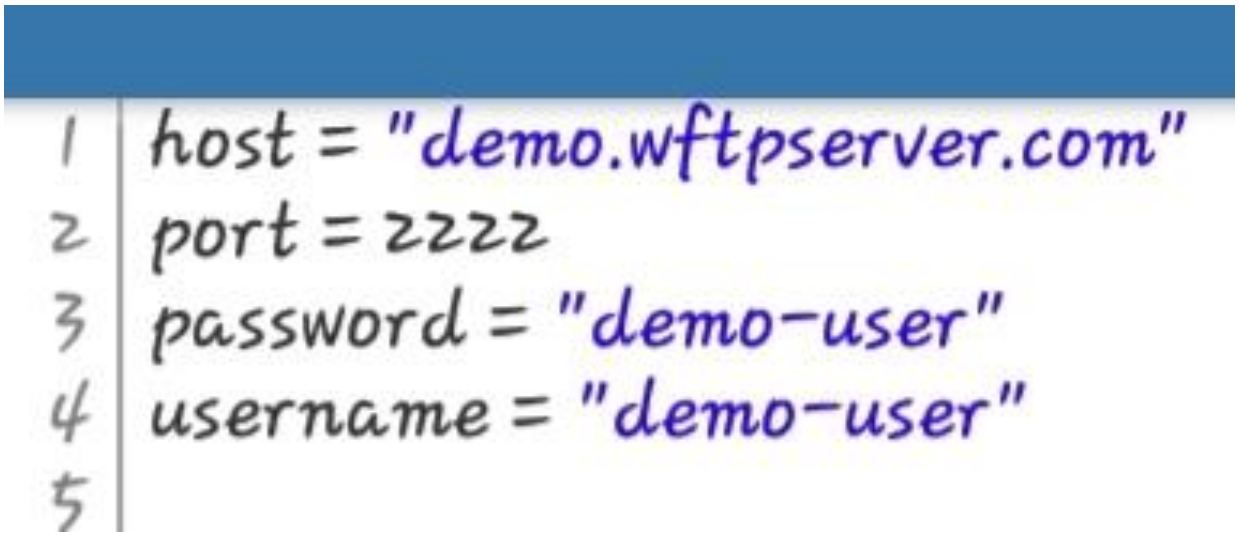
```
ssh.set_missing_host_key_policy(
paramiko.AutoAddPolicy())
ssh.connect(host, port, username,
password)

()sftp = ssh.open_sftp

"path = "/upload/src.py
"localpath = "src.py
sftp.put(localpath, path)

()sftp.close
()ssh.close
```

شرح تعليمات الكود:



```
1 host = "demo.wftpserver.com"
2 port = 2222
3 password = "demo-user"
4 username = "demo-user"
5
```

عرفنا بارامترات وادخلنا موقع الجهاز ورقم المنفذ وكلمة السر واسم المستخدم.

```
6 ssh = paramiko.SSHClient()
```

USE paramiko.SSHClient() TO UPLOAD A FILE USING SSH

استخدمنا مكتبة paramiko لتحميل ملف باستخدام ssh

Paramiko هو اتصال الآمن عن بعد وتنفيذ ودعم التوثيق ووضع المفتاح.

Call paramiko.SSHClient() to create a new SSHClient

انشاء sshclient(العميل)

```
ssh.
set_missing_host_key_policy(paramiko.
AutoAddPolicy())
```

Call paramiko.SSHClient.set_missing_host_key_policy(policy) with policy as paramiko.AutoAddPolicy() to allow the Python script to SSH to a remote server with unknown SSH keys

نقوم بتعيين سياسة لاستخدامها عند الاتصال بالخوادم بدون مفتاح مضيف معروف.

```
8 | ssh.connect(host, port, username,
  | password)
9 |
```

Call paramiko.SSHClient.connect(host, port, username, password) to connect the client to the server host:port with the credentials username and password

توصيل العميل بالخادم باستخدام اسم المستخدم و كلمة المرور

```
9  |
10 | sftp = ssh.open_sftp()
11 |
```

Call paramiko.SSHClient.open_sftp() to return a paramiko.SFTPClient and open an SFTP connection on the remote server.

استخدام SFTP لفتح اتصال مع الخادم عن بعد

```
11
12 path = "/upload/src.py"
13 localpath = "src.py"
14 sftp.put(localpath, path)
15
```

Call paramiko.SFTPClient.put(localpath, targetpath) to upload the local

file at localpath to the target path at targetpath

تحميل الملف الى الهدف

SFTP (بروتوكول نقل الملفات SSH، المعروف أيضا باسم بروتوكول نقل الملفات السرية)

إنه بروتوكول نقل الملفات الآمن، وسيلة أمان لنقل الملفات من خلال الشبكة؛

إنه يضمن نقل آمن للبيانات باستخدام تدفقات البيانات الخاصة والتأمين.

يتطلب SFTP مصادقة المستخدمين العميلين من خلال الخادم.

ويجب إجراء نقل البيانات من خلال قناة آمنة (SSH)، أي لا يتم نقل كلمة مرور النص أو بيانات الملف العادي.

يسمح بمجموعة متنوعة من العمليات إلى الملفات البعيدة، مثل بروتوكول نظام الملفات عن بعد.

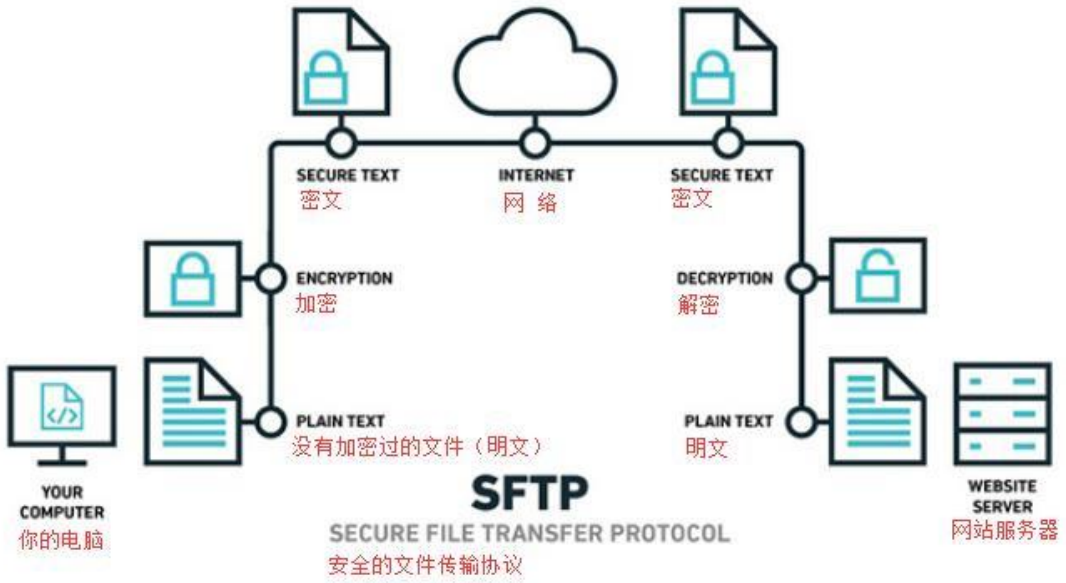
يسمح SFTP بالشفاء من عملية مثل الإيقاف المؤقت وقائمة الدليل، وقائمة الدليل، وحذف الملف البعيد.

بمعنى:(التعليمة الاولى تفتح ftp

والثانية تنقل المسار المحلي الى المسار الموجود على ssh

يعني سحب وافلات الملف

استخدمنا ftp لان ssh وسيلة اتصال اما نقل الملفات تتم عن طريق ftp)




```
15
16 sftp.close()
17 ssh.close()
```

Call paramiko.SFTPClient.close()
and paramiko.SSHClient.close()
.to close the connections

اغلاق الاتصال