

اعداد واختبار وتأمين بروتوكول SSH

May 14, 2022

Eng : Ahmed Hamza

Website : <https://ahmed0x59.github.io>

Youtube : <https://www.youtube.com/ahmedhamza0x59>

ما هو بروتوكول النقل الآمن SSH ؟

هو بروتوكول شبكي يوفر للمستخدمين طريق آمن للوصول الى الحواسيب عبر الشبكة ويوفر هذا البروتوكول اتصالاً مشفراً بين جهازي حاسب متصلين عبر شبكة مفتوحة كالإنترنت صمم بروتوكول SSH كبديل لبروتوكول TELNET وغيره من بروتوكولات الاتصال عن بعد الغير الآمنة, والتي ترسل المعلومات كنص عادي Clear Text مما يجعلها عرضة للاعتراض والكشف باستخدام طرق تحليل الحزم وبرامج الـ Sniffing.

مميزات بروتوكول SSH :

- الدخول الآمن إلى حسابك عن بعد (Secure Remote Logins).
- النقل الآمن للملفات (Secure File Transfer).
- التنفيذ الآمن للأوامر عند بعد (Secure Remote Command Execution).

ملخص التطبيق العملي :

1. اعداد بروتوكول SSH على Linux-Server توزيعة Ubuntu
 2. اعداد جدار الحماية Firewall للسماح بالاتصال مع السيرفر عن طريق SSH
 3. اختبار الاتصال مع السيرفر والتأكد من عمل البروتوكول
 4. اختبار اختراق بروتوكول SSH باستخدام هجوم التخمين BruteForce Attack
 5. تأمين بروتوكول SSH باستخدام Public-Key Authentication
 6. النقل الآمن للملفات Secure File Transfer
-

اعداد بروتوكول SSH

Update System & Install openssh-server package

sudo apt update

```
ubuntu@server: ~  
File Edit View Search Terminal Help  
ubuntu@server:~$ sudo apt update  
[sudo] password for ubuntu:  
Hit:1 http://archive.ubuntu.com/ubuntu bionic InRelease  
Get:2 http://archive.ubuntu.com/ubuntu bionic-updates InRelease [88.7 kB]  
Get:3 http://archive.ubuntu.com/ubuntu bionic-backports InRelease [74.6 kB]  
Get:4 http://archive.ubuntu.com/ubuntu bionic-security InRelease [88.7 kB]  
Fetched 252 kB in 3s (83.8 kB/s)  
Reading package lists... Done  
Building dependency tree  
Reading state information... Done  
560 packages can be upgraded. Run 'apt list --upgradable' to see them.  
ubuntu@server:~$
```

sudo apt install openssh-server

```
ubuntu@server: ~  
File Edit View Search Terminal Help  
ubuntu@server:~$ sudo apt install openssh-server  
Reading package lists... Done  
Building dependency tree  
Reading state information... Done  
Suggested packages:  
  molly-guard monkeysphere rssh ssh-askpass  
The following NEW packages will be installed:  
  openssh-server  
0 upgraded, 1 newly installed, 0 to remove and 557 not upgraded.  
Need to get 0 B/332 kB of archives.  
After this operation, 902 kB of additional disk space will be used.  
Preconfiguring packages ...  
Selecting previously unselected package openssh-server.  
(Reading database ... 183445 files and directories currently installed.)  
Preparing to unpack .../openssh-server_1%3a7.6p1-4ubuntu0.7_amd64.deb ...  
Unpacking openssh-server (1:7.6p1-4ubuntu0.7) ...  
Setting up openssh-server (1:7.6p1-4ubuntu0.7) ...  
Processing triggers for man-db (2.8.3-2ubuntu0.1) ...  
Processing triggers for ufw (0.36-0ubuntu0.18.04.1) ...  
Processing triggers for ureadahead (0.100.0-21) ...  
Processing triggers for systemd (237-3ubuntu10.33) ...  
ubuntu@server:~$
```

sudo systemctl start ssh.service

sudo systemctl status ssh.service

```
ubuntu@server: ~  
File Edit View Search Terminal Help  
ubuntu@server:~$ sudo systemctl start ssh.service  
ubuntu@server:~$ sudo systemctl status ssh.service  
● ssh.service - OpenBSD Secure Shell server  
   Loaded: loaded (/lib/systemd/system/ssh.service; disabled; vendor preset: enabled)  
   Active: active (running) since Sat 2022-05-14 16:12:57 UTC; 1min 26s ago  
 Process: 6563 ExecStartPre=/usr/sbin/sshd -t (code=exited, status=0/SUCCESS)  
 Main PID: 6577 (sshd)  
    Tasks: 1 (limit: 2846)  
   CGroup: /system.slice/ssh.service  
           └─6577 /usr/sbin/sshd -D  
  
May 14 16:12:57 toshiba systemd[1]: Starting OpenBSD Secure Shell server...  
May 14 16:12:57 toshiba sshd[6577]: Server listening on 0.0.0.0 port 22.  
May 14 16:12:57 toshiba sshd[6577]: Server listening on :: port 22.  
May 14 16:12:57 toshiba systemd[1]: Started OpenBSD Secure Shell server.  
ubuntu@server:~$
```

اعداد جدار الحماية UFW

اوامر اخرى مهمه للتحقق من خدمة SSH

```
sudo systemctl status ssh.service | sudo systemctl start ssh.service  
sudo systemctl enable ssh.service | sudo systemctl disable ssh.service  
sudo systemctl stop ssh.service | sudo systemctl restart ssh.service
```

اعداد جدار الحماية Firewall للسماح بالاتصال مع السيرفر عن طريق SSH

```
sudo ufw enable | sudo ufw allow ssh | sudo ufw status
```

```
ubuntu@server:~  
File Edit View Search Terminal Help  
ubuntu@server:~$ sudo ufw enable  
Firewall is active and enabled on system startup  
ubuntu@server:~$  
ubuntu@server:~$ sudo ufw allow ssh  
Rule added  
Rule added (v6)  
ubuntu@server:~$  
ubuntu@server:~$ sudo ufw status  
Status: active  
  
To Action From  
-- -- --  
22/tcp ALLOW Anywhere  
22/tcp (v6) ALLOW Anywhere (v6)  
  
ubuntu@server:~$
```

اختبار الاتصال مع السيرفر والتأكد من عمل البروتوكول

التحقق من IP السيرفر عن طريق الامر ifconfig

```
ubuntu@server:~  
File Edit View Search Terminal Help  
ubuntu@server:~$ ifconfig  
enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500  
inet 192.168.1.101 netmask 255.255.255.0 broadcast 192.168.1.255  
inet6 fdcd:a9fa:6580:0:a59e:bc1:2399:a190 prefixlen 64 scopeid 0x0<global>  
inet6 fe80::fcfe:bd68:7301:7da0 prefixlen 64 scopeid 0x20<link>  
ether 08:00:27:6d:c8:c3 txqueuelen 1000 (Ethernet)  
RX packets 973 bytes 322538 (322.5 KB)  
RX errors 0 dropped 0 overruns 0 frame 0  
TX packets 1317 bytes 154591 (154.5 KB)  
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0  
  
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536  
inet 127.0.0.1 netmask 255.0.0.0  
inet6 ::1 prefixlen 128 scopeid 0x10<host>  
loop txqueuelen 1000 (Local Loopback)  
RX packets 476 bytes 44901 (44.9 KB)  
RX errors 0 dropped 0 overruns 0 frame 0  
TX packets 476 bytes 44901 (44.9 KB)  
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0  
  
ubuntu@server:~$
```

اختبار الاتصال مع السيرفر من خلال نظام KALI-LINUX

nmap -Pn -p22 192.168.1.101

```
kali@kali: ~  
File Actions Edit View Help  
kali@kali ~  
└─$ nmap -Pn -p22 192.168.1.101  
Host discovery disabled (-Pn). All addresses will be marked 'up' and scan times will be slower.  
Starting Nmap 7.91 ( https://nmap.org ) at 2022-05-14 12:58 EDT  
Nmap scan report for 192.168.1.101  
Host is up (0.00080s latency).  
  
PORT      STATE SERVICE  
22/tcp    open  ssh  
  
Nmap done: 1 IP address (1 host up) scanned in 0.12 seconds  
  
kali@kali ~  
└─$
```

الاتصال مع السيرفر باستخدام بروتوكول SSH

Username : ubuntu

Password : ubuntu

```
ubuntu@server: ~  
File Actions Edit View Help  
kali@kali ~  
└─$ ssh ubuntu@192.168.1.101  
The authenticity of host '192.168.1.101 (192.168.1.101)' can't be established.  
ECDSA key fingerprint is SHA256:tmgl7WIj9dfqUn/aYUDZiFamd7/15A/9jWmKkPcxt60.  
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes  
Warning: Permanently added '192.168.1.101' (ECDSA) to the list of known hosts.  
ubuntu@192.168.1.101's password:  
Welcome to Ubuntu 18.04.4 LTS (GNU/Linux 4.15.0-74-generic x86_64)  
  
* Documentation:  https://help.ubuntu.com  
* Management:    https://landscape.canonical.com  
* Support:       https://ubuntu.com/advantage  
  
System information as of Sat May 14 17:03:57 UTC 2022  
  
System load:  0.03          Processes:    210  
Usage of /:  18.0% of 48.96GB  Users logged in:  1  
Memory usage: 53%          IP address for enp0s3: 192.168.1.101  
Swap usage:  0%  
  
* Super-optimized for small spaces - read how we shrank the memory  
  footprint of MicroK8s to make it the smallest full K8s around.  
  https://ubuntu.com/blog/microk8s-memory-optimisation  
  
* Canonical Livepatch is available for installation.  
  - Reduce system reboots and improve kernel security. Activate at:  
  https://ubuntu.com/livepatch  
  
568 packages can be updated.  
476 updates are security updates.  
  
New release '20.04.4 LTS' available.  
Run 'do-release-upgrade' to upgrade to it.  
  
Last login: Sat May 14 13:57:18 2022 from 192.168.1.100  
ubuntu@server:~$
```

اختبار اختراق بروتوكول SSH باستخدام هجوم التخمين

BRUTEFORCE ATTACK

Crack Password [SSH] Using [Hydra Tool]

```
hydra -vV -l ubuntu -P passwords.txt ssh://192.168.1.101
```

```
hydra -vV -L usernames.txt -P passwords.txt ssh://192.168.1.101
```

```
kali@kali: ~/Desktop
File Actions Edit View Help
(kali@kali) - [~/Desktop]
└─$ ls
passwords.txt  usernames.txt

(kali@kali) - [~/Desktop]
└─$ hydra -vV -l ubuntu -P passwords.txt ssh://192.168.1.101

Hydra v9.1 (c) 2020 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2022-05-14 13:25:09
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[DATA] max 16 tasks per 1 server, overall 16 tasks, 118 login tries (l:1/p:118), ~8 tries per task
[DATA] attacking ssh://192.168.1.101:22/
[VERBOSE] Resolving addresses ... [VERBOSE] resolving done
[INFO] Testing if password authentication is supported by ssh://ubuntu@192.168.1.101:22
[INFO] Successful, password authentication is supported by ssh://192.168.1.101:22
[ATTEMPT] target 192.168.1.101 - login "ubuntu" - pass "11111" - 1 of 118 [child 0] (0/0)
[ATTEMPT] target 192.168.1.101 - login "ubuntu" - pass "123456" - 2 of 118 [child 1] (0/0)
[ATTEMPT] target 192.168.1.101 - login "ubuntu" - pass "12345678" - 3 of 118 [child 2] (0/0)
[ATTEMPT] target 192.168.1.101 - login "ubuntu" - pass "abc123" - 4 of 118 [child 3] (0/0)
[ATTEMPT] target 192.168.1.101 - login "ubuntu" - pass "abramov" - 5 of 118 [child 4] (0/0)
[ATTEMPT] target 192.168.1.101 - login "ubuntu" - pass "account" - 6 of 118 [child 5] (0/0)
[ATTEMPT] target 192.168.1.101 - login "ubuntu" - pass "accounting" - 7 of 118 [child 6] (0/0)
[ATTEMPT] target 192.168.1.101 - login "ubuntu" - pass "ad" - 8 of 118 [child 7] (0/0)
[ATTEMPT] target 192.168.1.101 - login "ubuntu" - pass "adm" - 9 of 118 [child 8] (0/0)
[ATTEMPT] target 192.168.1.101 - login "ubuntu" - pass "admin" - 10 of 118 [child 9] (0/0)
[ATTEMPT] target 192.168.1.101 - login "ubuntu" - pass "administrator" - 11 of 118 [child 10] (0/0)
[ATTEMPT] target 192.168.1.101 - login "ubuntu" - pass "adver" - 12 of 118 [child 11] (0/0)
[ATTEMPT] target 192.168.1.101 - login "ubuntu" - pass "advert" - 13 of 118 [child 12] (0/0)
[ATTEMPT] target 192.168.1.101 - login "ubuntu" - pass "advertising" - 14 of 118 [child 13] (0/0)
[ERROR] could not connect to target port 22: Socket error: Connection reset by peer
[ERROR] ssh protocol error
[ERROR] could not connect to target port 22: Socket error: Connection reset by peer
[ERROR] ssh protocol error
[ERROR] ssh protocol error
[ATTEMPT] target 192.168.1.101 - login "ubuntu" - pass "afanasev" - 15 of 118 [child 14] (0/0)
[ATTEMPT] target 192.168.1.101 - login "ubuntu" - pass "agafonov" - 16 of 118 [child 15] (0/0)
[ERROR] could not connect to target port 22: Socket error: Connection reset by peer
[ERROR] ssh protocol error
```

```
kali@kali: ~/Desktop
File Actions Edit View Help
(kali@kali) - [~/Desktop]
└─$ hydra -vV -L usernames.txt -P passwords.txt ssh://192.168.1.101

[ATTEMPT] target 192.168.1.101 - login "ubuntu" - pass "office" - 98 of 122 [child 6] (0/4)
[ATTEMPT] target 192.168.1.101 - login "ubuntu" - pass "ok" - 99 of 122 [child 14] (0/4)
[ATTEMPT] target 192.168.1.101 - login "ubuntu" - pass "oracle" - 100 of 122 [child 15] (0/4)
[ERROR] could not connect to target port 22: Socket error: Connection reset by peer
[ERROR] ssh protocol error
[VERBOSE] Retrying connection for child 15
[RE-ATTEMPT] target 192.168.1.101 - login "ubuntu" - pass "oracle" - 100 of 122 [child 15] (0/4)
[ERROR] could not connect to target port 22: Socket error: Connection reset by peer
[ERROR] ssh protocol error
[VERBOSE] Retrying connection for child 15
[RE-ATTEMPT] target 192.168.1.101 - login "ubuntu" - pass "oracle" - 100 of 122 [child 15] (0/4)
[ATTEMPT] target 192.168.1.101 - login "ubuntu" - pass "password" - 101 of 122 [child 9] (0/4)
[ATTEMPT] target 192.168.1.101 - login "ubuntu" - pass "personal" - 102 of 122 [child 8] (0/4)
[ATTEMPT] target 192.168.1.101 - login "ubuntu" - pass "petgord34truew" - 103 of 122 [child 1] (0/4)
[ATTEMPT] target 192.168.1.101 - login "ubuntu" - pass "post" - 104 of 122 [child 2] (0/4)
[ATTEMPT] target 192.168.1.101 - login "ubuntu" - pass "postmaster" - 105 of 122 [child 7] (0/4)
[ATTEMPT] target 192.168.1.101 - login "ubuntu" - pass "pr" - 106 of 122 [child 10] (0/4)
[ATTEMPT] target 192.168.1.101 - login "ubuntu" - pass "qwerty" - 107 of 122 [child 11] (0/4)
[ATTEMPT] target 192.168.1.101 - login "ubuntu" - pass "rbury" - 108 of 122 [child 13] (0/4)
[ATTEMPT] target 192.168.1.101 - login "ubuntu" - pass "reklama" - 109 of 122 [child 4] (0/4)
[ATTEMPT] target 192.168.1.101 - login "ubuntu" - pass "root" - 110 of 122 [child 5] (0/4)
[ATTEMPT] target 192.168.1.101 - login "ubuntu" - pass "r00t" - 111 of 122 [child 14] (0/4)
[ATTEMPT] target 192.168.1.101 - login "ubuntu" - pass "sale" - 112 of 122 [child 0] (0/4)
[ATTEMPT] target 192.168.1.101 - login "ubuntu" - pass "sales" - 113 of 122 [child 3] (0/4)
[ATTEMPT] target 192.168.1.101 - login "ubuntu" - pass "secretar" - 114 of 122 [child 6] (0/4)
[ATTEMPT] target 192.168.1.101 - login "ubuntu" - pass "sekretar" - 115 of 122 [child 12] (0/4)
[ATTEMPT] target 192.168.1.101 - login "ubuntu" - pass "support" - 116 of 122 [child 15] (0/4)
[ATTEMPT] target 192.168.1.101 - login "ubuntu" - pass "test" - 117 of 122 [child 9] (0/4)
[ATTEMPT] target 192.168.1.101 - login "ubuntu" - pass "ubuntu" - 118 of 122 [child 8] (0/4)
[22][ssh] host: 192.168.1.101 login: ubuntu password: ubuntu
[STATUS] attack finished for 192.168.1.101 (waiting for children to complete tests)
1 of 1 target successfully completed, 1 valid password found
[WARNING] Writing restore file because 7 final worker threads did not complete until end.
[ERROR] 7 targets did not resolve or could not be connected
[ERROR] 0 target did not complete
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2022-05-14 13:25:56

(kali@kali) - [~/Desktop]
└─$
```

تأمين بروتوكول SSH

تأمين بروتوكول SSH باستخدام Public-Key Authentication

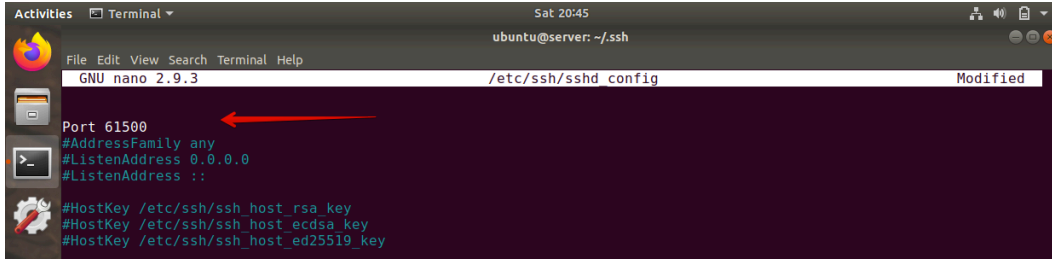
1. استخدم كلمة مرور واسم مستخدم قوية ومعقدة لا يمكن تخمينها
 2. يمكن تغيير رقم البورت الافتراضي من 22 الى اي بورت اخر
 3. الغاء تفعيل الاتصال باستخدام Root
 4. استخدام المفاتيح للاتصال بدلا من الباسوورد Public-Key Auth
- لمنع هجمات القوة الغاشمة لاكتشاف كلمات المرور واسماء المستخدمين

الملف الخاص بالاعدادات لخدمة SSH في المسار التالي :

```
sudo nano /etc/ssh/sshd_config
```

```
sudo systemctl restart ssh.service
```

تغيير رقم البورت الافتراضي من 22 الى 61500



```
GNU nano 2.9.3 /etc/ssh/sshd_config Modified
Port 61500
#AddressFamily any
#ListenAddress 0.0.0.0
#ListenAddress ::
#HostKey /etc/ssh/ssh_host_rsa_key
#HostKey /etc/ssh/ssh_host_ecdsa_key
#HostKey /etc/ssh/ssh_host_ed25519_key
```

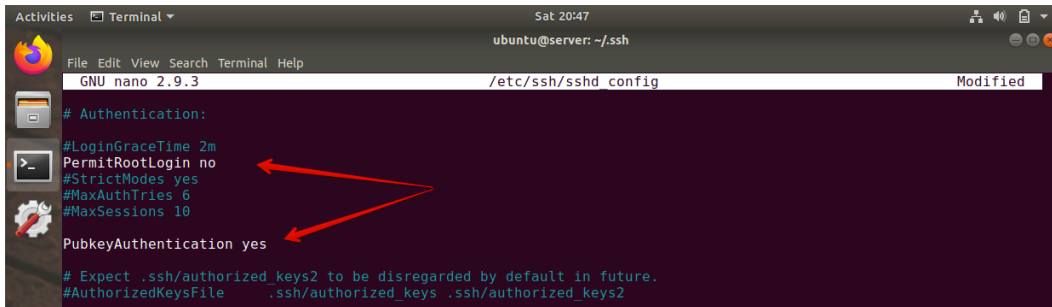
اعداد جدار الحماية Firewall للسماح بالاتصال مع السيرفر عن طريقة بورت 61500

```
sudo ufw allow 61500
```

الغاء تفعيل الاتصال باستخدام صلاحيات Root وتفعيل الاتصال باستخدام المفاتيح بدلا من الباسوورد

```
PermitRootLogin no
```

```
PubkeyAuthentication yes
```



```
GNU nano 2.9.3 /etc/ssh/sshd_config Modified
# Authentication:
#LoginGraceTime 2m
PermitRootLogin no
#StrictModes yes
#MaxAuthTries 6
#MaxSessions 10
PubkeyAuthentication yes
# Expect .ssh/authorized_keys2 to be disregarded by default in future.
#AuthorizedKeysFile .ssh/authorized_keys .ssh/authorized_keys2
```

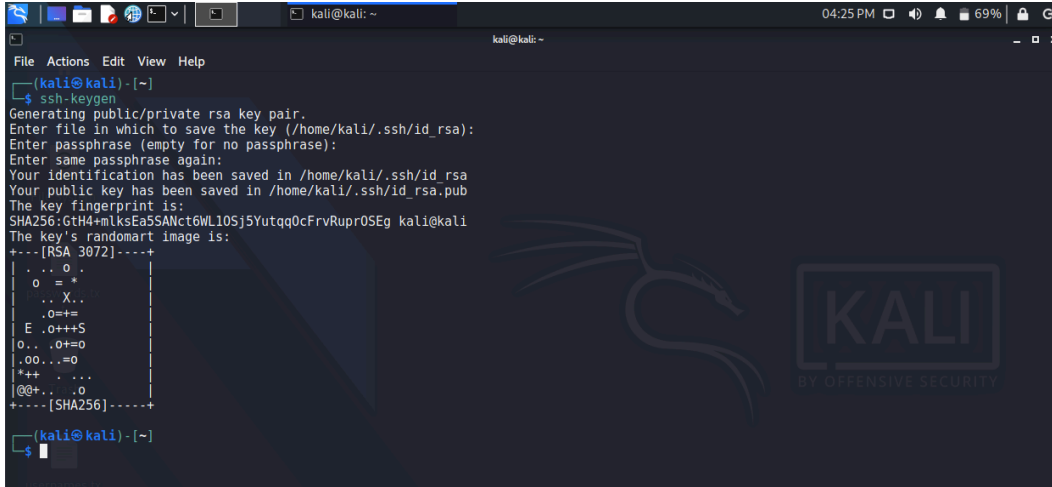
استخدام المفاتيح للاتصال بدلا من الباسورد

PUBLIC-KEY AUTHENTICATION

الدافع لاستخدام مصادقة المفتاح العام على كلمات المرور البسيطة هو الأمان. توفر مصادقة المفتاح العام قوة تشفير لا يمكن أن تقدمها حتى كلمات المرور الطويلة للغاية. تعمل مصادقة المفتاح العام على تحسين الأمان إلى حد كبير لأنها تحرر المستخدمين من تذكر كلمات المرور المعقدة (أو الأسوأ من ذلك ، تدوينها)

عند استخدام مصادقة المفتاح العام نقوم بإنشاء مفتاح عام ومفتاح خاص في جهاز المستخدم وإضافة المفتاح العام إلى السيرفر لنتمكن من الاتصال بالسيرفر عن طريق المفتاح الخاص وأيضا نقوم بإلغاء عملية الاتصال بالسيرفر عن طريق كلمات المرور , يعني السيرفر لن يقبل اي اتصال الا عن طريق المفتاح الخاص الموجود عند المدير او المستخدم المصرح له ويجب الحفاظ على هذا الملف بسرية تامة

اعداد المفاتيح في نظام Kali باستخدام اداة ssh-keygen



```
(kali@kali) ~
└─$ ssh-keygen
Generating public/private rsa key pair.
Enter file in which to save the key (/home/kali/.ssh/id_rsa):
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/kali/.ssh/id_rsa
Your public key has been saved in /home/kali/.ssh/id_rsa.pub
The key fingerprint is:
SHA256:GtH4+mLksEaSSAct6WL10Sj5Yutqq0cFrvRupr05Eg kali@kali
The key's randomart image is:
+---[RSA 3072]----+
|. . . o .
|o = *
|. . X .
|.o+=+
|E .o+++S
|. . . .o+=o
|.oo...=o
|*+ . . . .
|@+ . . . .o
+---[SHA256]----+
(kali@kali) ~
└─$
```

ملاحظة:

يمكن استخدام كلمة مرور للملف الخاص نفسه لزيادة الأمان اكثر , عند اعداد المفاتيح ستخبر بين اعداد كلمة مرور للملف الخاص او تتركه بدون كلمة مرور

اذا قمت بكتابة كلمة مرور للملف الخاص سيتم مطالبتك بكلمة المرور للملف الخاص عند الاتصال بالسيرفر

اذا تركته بدون كلمة المرور لن يتم مطالبتك بكلمة مرور عند الاتصال بالسيرفر باستخدام الملف الخاص

استخدام المفاتيح للاتصال بدلا من الباسورد

PUBLIC-KEY AUTHENTICATION

الآن نقوم بنقل الملف العام id_rsa.pub الى السيرفر باستخدام اداة ssh-copy-id

```
ssh-copy-id -p61500 -i /home/kali/.ssh/id_rsa.pub ubuntu@192.168.1.101
```

ملاحظة :

إذا قمنا بتغيير رقم البورت في ملف الاعدادات يجب تحديد رقم البورت الصحيح عند تنفيذ الأمر

```
kali@kali: ~
└─$ ssh-copy-id -p61500 -i ~/.ssh/id_rsa.pub ubuntu@192.168.1.101
/usr/bin/ssh-copy-id: INFO: Source of key(s) to be installed: "/home/kali/.ssh/id_rsa.pub"
The authenticity of host '[192.168.1.101]:61500 ([192.168.1.101]:61500)' can't be established.
ED25519 key fingerprint is SHA256:0P8JeweTuxfthJlr1IZSHjNVzxsZHe/ec6H80d7bBjA.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
/usr/bin/ssh-copy-id: INFO: attempting to log in with the new key(s), to filter out any that are already installed
/usr/bin/ssh-copy-id: INFO: 1 key(s) remain to be installed -- if you are prompted now it is to install the new keys
ubuntu@192.168.1.101's password:

Number of key(s) added: 1

Now try logging into the machine, with: "ssh -p 61500 'ubuntu@192.168.1.101'"
and check to make sure that only the key(s) you wanted were added.

(kali@kali)~$
```

تم اضافة ملف العام الخاص بنظام kali الى السيرفر في ملف authorized_keys وهو الملف الذي يوجد به المفاتيح المصرح لها بالاتصال مع السيرفر الان نقوم بالاتصال بالسيرفر باستخدام المفتاح الخاص والتعديل على ملف الاعدادات لالغاء الاتصال بالسيرفر عن طريق كلمات المرور يعني السيرفر لن يقبل اي اتصال الا عن طريق المفتاح الخاص

```
ssh ubuntu@192.168.1.101 -p61500 -i /home/kali/.ssh/id_rsa
```

```
ubuntu@server: ~
└─$ ssh ubuntu@192.168.1.101 -p61500 -i /home/kali/.ssh/id_rsa
Welcome to Ubuntu 18.04.4 LTS (GNU/Linux 4.15.0-74-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage

System information as of Sat May 14 20:49:54 UTC 2022

System load: 0.39          Processes:                210
Usage of /:   18.0% of 48.96GB   Users logged in:        1
Memory usage: 54%          IP address for enp0s3:  192.168.1.101
Swap usage:  0%

 * Super-optimized for small spaces - read how we shrank the memory
  footprint of MicroK8s to make it the smallest full K8s around.
  https://ubuntu.com/blog/microk8s-memory-optimisation

 * Canonical Livepatch is available for installation.
  - Reduce system reboots and improve kernel security. Activate at:
  https://ubuntu.com/livepatch

568 packages can be updated.
476 updates are security updates.

New release '20.04.4 LTS' available.
Run 'do-release-upgrade' to upgrade to it.

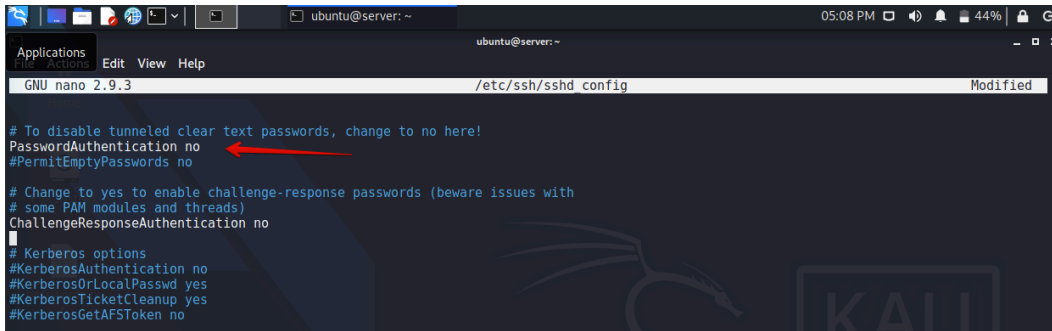
Last login: Sat May 14 20:38:58 2022 from 192.168.1.104
ubuntu@server:~$
```


استخدام المفاتيح للاتصال بدلا من الباسوورد

PUBLIC-KEY AUTHENTICATION

الآن نقوم بالتعديل على ملف الاعدادات والغاء الاتصال بالسيرفر عن طريق كلمات المرور

PasswordAuthentication no



```
ubuntu@server: ~
Applications Edit View Help
File Actions /etc/ssh/sshd config Modified
GNU nano 2.9.3
# To disable tunneled clear text passwords, change to no here!
PasswordAuthentication no
#PermitEmptyPasswords no
# Change to yes to enable challenge-response passwords (beware issues with
# some PAM modules and threads)
ChallengeResponseAuthentication no
# Kerberos options
#KerberosAuthentication no
#KerberosOrLocalPasswd yes
#KerberosTicketCleanup yes
#KerberosGetAFSToken no
```

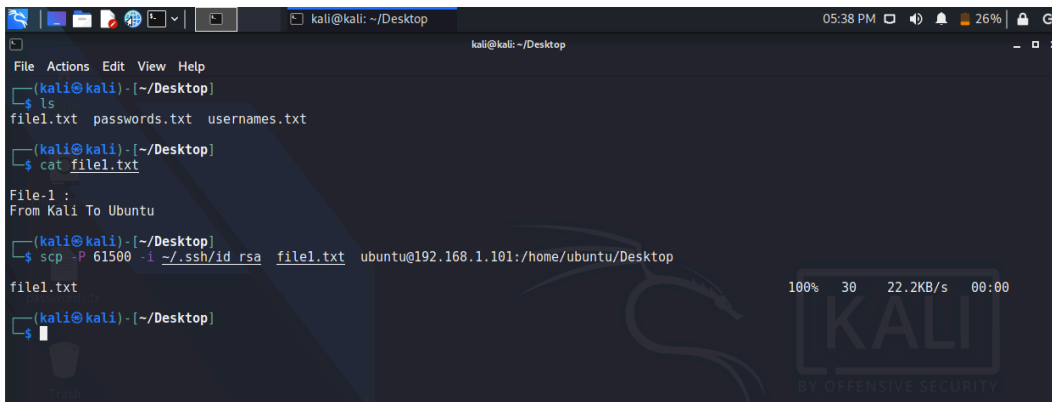
عند اجراء اي تعديل على ملف الاعدادات يجب ان نقوم باعادة تشغيل الخدمة من جديد
ubuntu@server:~\$ sudo systemctl reload ssh

النقل الآمن للملفات SECURE FILE TRANSFER

Transfer file1.txt From kali To Ubuntu :

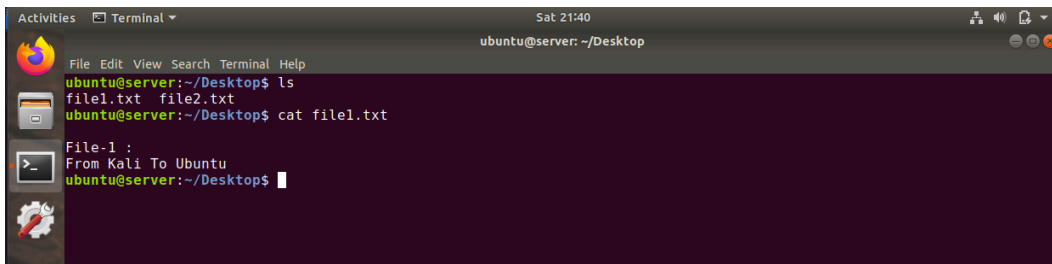
نقل ملف file1.txt من الكالي الى السيرفر

```
scp -P 61500 -i /home/kali/.ssh/id_rsa file1.txt ubuntu@192.168.1.101:/home/ubuntu/Desktop
```



```
kali@kali: ~/Desktop
File Actions Edit View Help
(kali@kali) - [~/Desktop]
└─$ ls
file1.txt passwords.txt usernames.txt
(kali@kali) - [~/Desktop]
└─$ cat file1.txt
File-1 :
From Kali To Ubuntu
(kali@kali) - [~/Desktop]
└─$ scp -P 61500 -i ~/.ssh/id_rsa file1.txt ubuntu@192.168.1.101:/home/ubuntu/Desktop
file1.txt
(kali@kali) - [~/Desktop]
└─$
```

تم استلام الملف file1.txt بنجاح في السيرفر



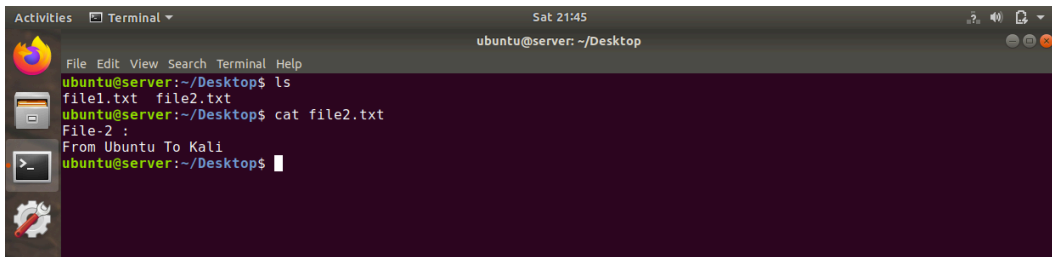
```
ubuntu@server: ~/Desktop
File Edit View Search Terminal Help
ubuntu@server:~/Desktop$ ls
file1.txt file2.txt
ubuntu@server:~/Desktop$ cat file1.txt
File-1 :
From Kali To Ubuntu
ubuntu@server:~/Desktop$
```

النقل الآمن للملفات SECURE FILE TRANSFER

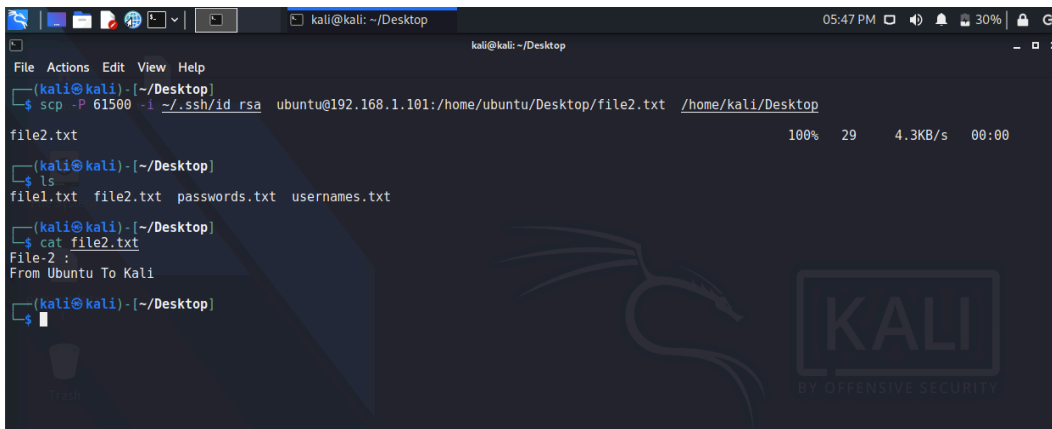
Transfer file2.txt From Ubuntu To Kali :

سحب ملف من السيرفر الى نظام الكالي :

```
scp -P 61500 -i /home/kali/.ssh/id_rsa ubuntu@192.168.1.101:/home/ubuntu/Desktop/file2.txt /home/kali/Desktop
```



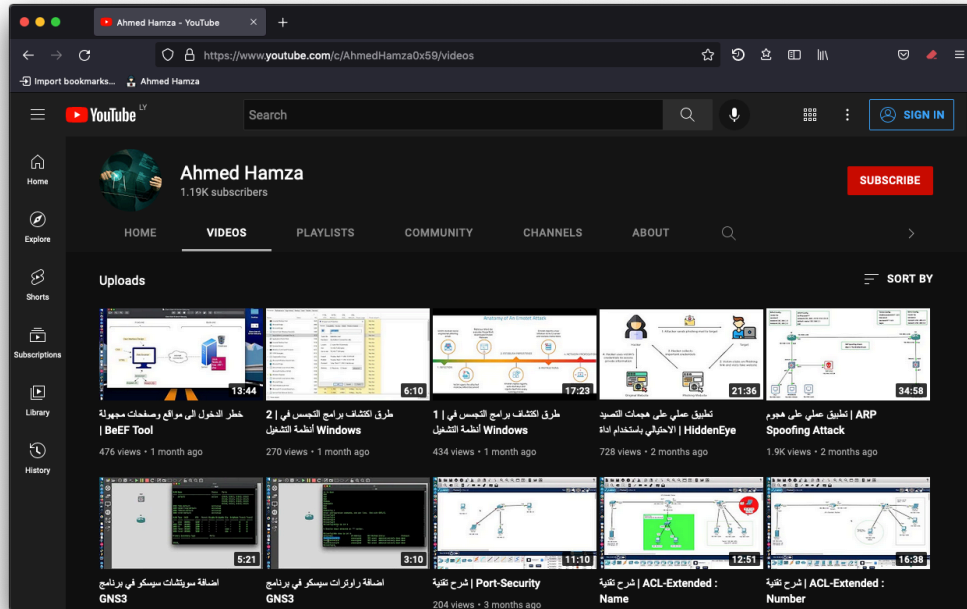
```
ubuntu@server:~/Desktop$ ls
file1.txt file2.txt
ubuntu@server:~/Desktop$ cat file2.txt
File-2 :
From Ubuntu To Kali
ubuntu@server:~/Desktop$
```



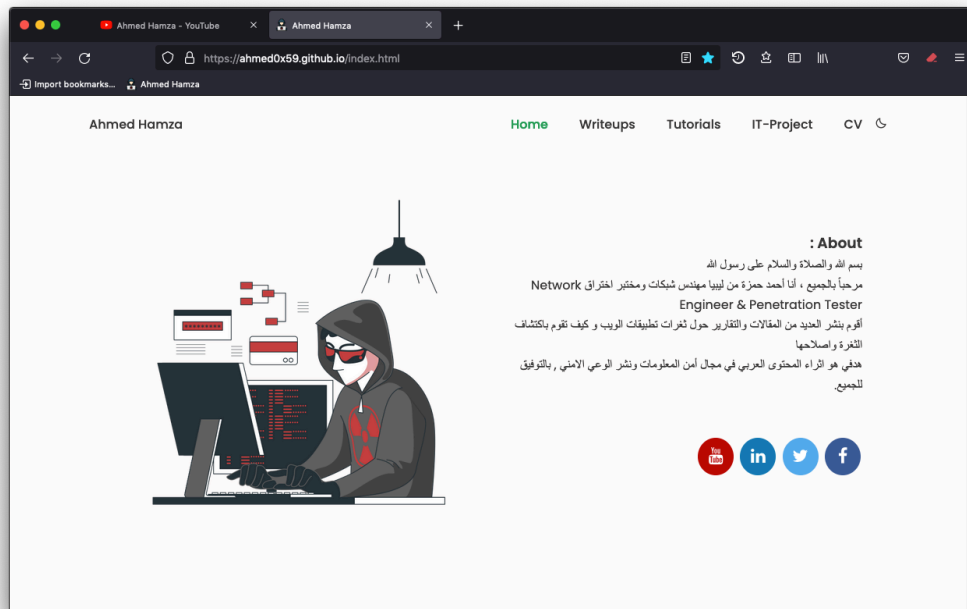
```
kali@kali: ~/Desktop
(kali@kali) ~/Desktop
$ scp -P 61500 -i ~/.ssh/id_rsa ubuntu@192.168.1.101:/home/ubuntu/Desktop/file2.txt /home/kali/Desktop
file2.txt 100% 29 4.3KB/s 00:00
(kali@kali) ~/Desktop
$ ls
file1.txt file2.txt passwords.txt usernames.txt
(kali@kali) ~/Desktop
$ cat file2.txt
File-2 :
From Ubuntu To Kali
(kali@kali) ~/Desktop
$
```

شرح التطبيق العملي كامل في اليوتيوب

<https://www.youtube.com/c/AhmedHamza0x59/videos>



<https://ahmed0x59.github.io>



المراجع

<https://linuxhandbook.com/ssh-basics>

<https://linuxhandbook.com/enable-ssh-ubuntu>

<https://linuxhandbook.com/add-ssh-public-key-to-server>

<https://linuxhandbook.com/scp-command>

<https://linuxize.com/post/how-to-enable-ssh-on-ubuntu-20-04>

<https://itsfoss.com/set-up-ssh-ubuntu>

<https://www.ssh.com/academy/ssh/protocol>

<https://www.ssh.com/academy/ssh/openssh>

<https://www.ssh.com/academy/ssh/public-key-authentication>

<https://www.openssh.com>

<https://ubuntu.com/server/docs/service-openssh>
