

Linux commands | Basics 1

- `ls [-a , -l ..] [file]`
show files and directories
- `pwd`
show current path
- `cd [subdirectory, ..]`
change directory
- `man COMMAND`
manual of command
- `cat TEXTFILE`
show all text in the text file

Linux commands | Basics 2

- touch FILENAME
create new file
- mkdir DIRECTORYNAME
create a new directory
- cp SOURCE DESTINATION
copy file from source to destination
- mv SOURCE DESTINATION
move file from source to destination
- rm SOURCE
remove file from source

Linux commands | Basics 3

- `echo INPUT [>into file;overwirte, >>into file;update]`
print to terminal the string or the variable
- `nano TEXTFILE`
edit file with nano editor (search with `ctrl+w`)
- `vi TEXTFILE`
edit file with vim editor (edit by `i`
escape by `:wq` then enter from command mode)

Linux commands | Users

- `adduser USERNAME`
add user
- `adduser USERNAME sudo`
add this user to sudoers
- `su USERNAME`
change to this user

Linux commands | File Permissions

The number of links to
the file

```
root@kali:~/mydirectory# ls -l myfile  
-rw-r--r-- 1 root root 47 Apr 23 21:15 myfile
```

Owner group and all
users permissions

User and group
own the file

Size in
bytes

Last modified

Linux commands | File Permissions

- `chmod 700 MYFILE`
change permissions of a file

Table 2-1: Linux File Permissions

Integer Value	Permissions	Binary Representation
7	full	111
6	read and write	110
5	read and execute	101
4	read only	100
3	write and execute	011
2	write only	010
1	execute only	001
0	none	000

Linux commands | grep

global expression regular print

- `grep [-i, -w, -A/B/C N] "str" [FILE]`

Find str in the file. Flags : ignore case, words matches only
print after/before/after and before N lines

Pipelines

- `Ls | grep corn`
see all files and directories with 'corn' in it

Linux commands | sed stream editor

- Sed 'OPTIONS' FILENAME

sed 's/Blanckhat/Defcon/' myfile (first appearance in line)

sed 's/Blanckhat/Defcon/g' myfile (all appearance in line-global)

output text file after editing (replace, delete and more)

edit file with /w flag sed 's/Blanckhat/Defcon/w myfile1' myfile

Linux commands | awk

- awk 'pattern' FILNAME
find patterns in a file
- service SERVICENAME COMMAND
service apache2 start

Linux commands | Networks 1

- apt install net-tools
- Ifconfig
get your IP address and gateway for each interface
- route
get your gateway
- netstat -antp
show all programs listening on TCP ports

Linux commands | networks 2

Setting up static IP address

By default define as DHCP (dynamic host configuration protocol)

In order to change it, edit `/etc/network/interfaces`

add this lines: (address as you want, mask and gateway as you saw below)

```
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).
```

```
# The loopback network interface
```

```
auto lo
```

```
iface lo inet loopback
```

```
auto eth0
```

```
iface eth0 inet static
```

```
address 192.168.20.9
```

```
netmask 255.255.255.0
```

```
gateway 192.168.20.1
```

Ubuntu 18.04 and above use [netplan](#) to configure your network, and `/etc/network/interfaces` does not exist anymore. The netplan configuration file should be at `/etc/netplan/`.

Linux commands | networks 3 | netcat

Netcat – the Swiss Army Knife of TCP/IP Connections

nc -h
for help

nc -v IP PORT
check if port in this IP is open

1machine: nc -lvp PORT
open port to listening

2machine: nc IP PORT
hi 1machine → hi 1machine

Linux commands | SSH connection

ssh is a secure shell

You can connect and control remote machine in your terminal.

There is 2 identity ways :

1. Username and password
2. Public Key authentication

ssh REMOTEIP

ssh username@REMOTEIP

Linux commands | SSH connection

When you try connect first time with command `ssh username@REMOTEIP` may appear message like that:

```
(kali㉿kali)-[~]  
$ ssh [REDACTED]  
The authenticity of host '[REDACTED]' can't be established  
ED25519 key fingerprint is SHA256:KEP2epB1Hs/Vxqb3UMti5smqo6zXhX7z2viz64R4PRM  
This key is not known by any other names  
Are you sure you want to continue connecting (yes/no/[fingerprint])? y  
Please type 'yes', 'no' or the fingerprint: yes
```

It means: yes – entrance with password (method 1).
Fingerprint – entrance with keys (method 2).

Linux commands | SSH connection

1. username and password

Now, you can enter with username and password of target machine.

```
(kali@kali)-[~]  
$ ssh -oHostKeyAlgorithms=+ssh-dss georgia@  
georgia@1's password:  
Linux ubuntu 2.6.27-7-generic #1 SMP Fri Oct 24 06:42:44 UTC 2008 i686  
  
The programs included with the Ubuntu system are free software;  
the exact distribution terms for each program are described in the  
individual files in /usr/share/doc/*/copyright.  
  
Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by  
applicable law.  
  
To access official Ubuntu documentation, please visit:  
http://help.ubuntu.com/  
Last login: Sat Dec 15 15:49:22 2012 from  
georgia@ubuntu:~$  
identity added: /home/kali/.ssh/id_rsa (kali@kali)
```

Linux commands | SSH connection

[Last page I added the flag “-oHostKeyAlgorithms=+ssh-dss”

to ssh command as mention [here](#). Dou to old version of ubuntu.]

We have connection to georgia!

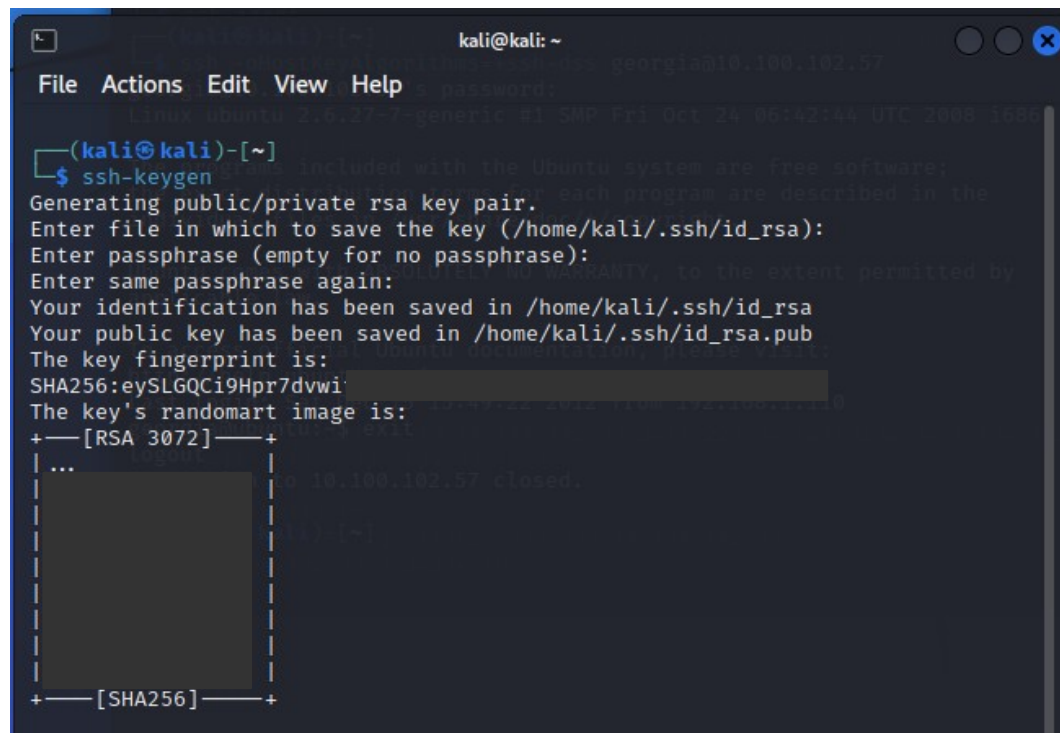
Linux commands | SSH connection

2. pubkey method:

Set (before entrance) your pubkey by:
ssh-keygen

passphrase is optional.

Now your private/public key saved as
hash256 in /.ssh/id_rsa.pub



```
kali@kali: ~  
File Actions Edit View Help  
georgis@10.100.102.57  
password:  
Linux ubuntu 2.6.27-7-generic #1 SMP Fri Oct 24 06:42:44 UTC 2008; i686  
included with the Ubuntu system are free software;  
(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:eySLGQC9Hpr7dvw...  
The key's randomart image is:  
+--[RSA 3072]--+  
| ...  
+-----[SHA256]-----
```

Linux commands | SSH connection

To copy your public key to your server, run: `ssh-copy-id username@REMOTEIP`

```
(kali㉿kali)-[~]  
$ ssh-copy-id -oHostKeyAlgorithms=+ssh-dss georgia@10.100.102.60  
/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  
georgia@10.100.102.60's password:  
  
(kali㉿kali)-[~]  
$ ssh-copy-id -oHostKeyAlgorithms=+ssh-dss georgia@10.100.102.60  
/usr/bin/ssh-copy-id: INFO: Source of key(s) to be installed: "/home/kali/.ssh/id_rsa.pub" 10.100.102.60  
The authenticity of host '10.100.102.60' can't be established.  
DSA key fingerprint is SHA256:WlGEO+/YI1hPU.  
Please type 'yes', 'no' or the fingerprint: SHA256:WlGEO+/YI1hPU  
/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  
georgia@10.100.102.60's password: █
```

Linux commands | SSH connection

We have connection to georgia, with no password!