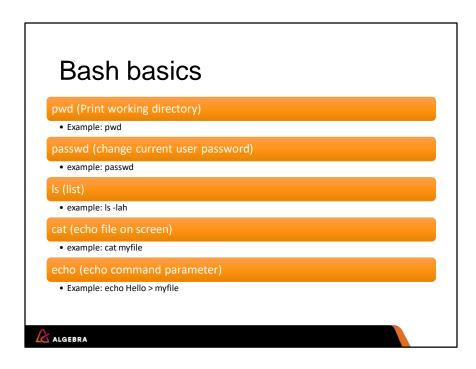


Bash basics

Finding files

- find
 - Searches through everything
 - Example: find / -name myfile
- locate
 - First use updatedb to build local database of all the files on the system, or nothing will be shown in screen
 - Example: locate myfile
- which
 - Searches the folders in the \$PATH variable
 - Example: which nc





Bash basics

grep (search for string inside another string)

• Example: cat myfile | grep something

cut (extract columns of data)

• Example: cat myfile | cut –f 2 –d ":"

tr (remove specific characters)

• Example: tr –d "x"

sed (replace specific part of the string)

• Example: sed s/day/night/oldfile >newfile

ALGEBRA

Bash basics

- It's all about piping
 - Using | to pass the output of one command as an input to another
- Example: output contents of the file "myfile" search for lines with string "user" in the file and show only these lines, then show the lines without 001 and save it to file hello

cat myfile | grep user | grep -v 001 > hello



Linux basic troubleshooting commands

ifconfig – identify and configure IP and MAC

• Example: ifconfig eth0 192.168.100.100/24

ip – identify and configure IP and MAC

• Example: ip address

arp – identify IP to MAC mappings

• Example: arp

netstat - identify open ports and established connections

• Example: netstat-tupan



Linux basic troubleshooting commands

route - show routing table

• Example: route

traceroute – identify routers between nodes

• Example: traceroute

smbclient – establish SMB connection

- example: smbclient-W DEMO.LAB-U Username //Computername/c\\$
- \\\Compuername\\sharename or //computername/sharename

rpcclient – powerufull enumeration tool

• Example: rpcclient-u USERNAME IP



Linux basic troubleshooting commands

service – start, stop, pause the service

• Example: service apache2 start

systemctl – start, stop pause service

• Example: systemctl start apache2

update-rc.d – start service automatically after reboot

• Example: update-rc.d apache2 enable

journalctl - system logs for troubleshooting

• Example: journalctl-f



Linux basic commands

Configure IP settings permanently - DHCP

- Edit file /etc/network/interfaces
- Change entry point for the adapter or add new entry if it does not exist.
 - auto eth0
 - iface eth0 inet dhcp

Use ifup eth0 and ifdown eth0 commands to reinitialize the NIC if needed

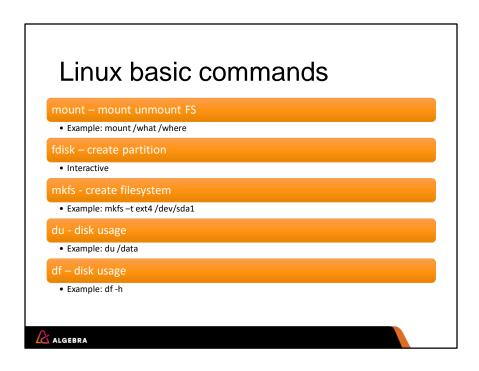


Linux basic commands

Configure IP settings permanently – manual IP

- Edit file /etc/network/interfaces
- Change entry point for the adapter or add new entry if it does not exist.
 - auto eth0
 - iface eth0 inet static
 - address 192.168.100.100
 - netmask 255.255.255.0
 - gateway 192.168.100.254





Linux basic commands

ps - process list

• Example: ps -ef

top – process CPU/memory usage

Example: top



Start and configure apache

apt-get install apache2 if not installed

- Default document location on Kali /var/www/html
- Default configuration location on Kali /etc/apache2
- Default logs location on Kali /var/log/apache2

Start apache service

• service apache2 start or systemctl start apache2

Stop apache service

• service apache2 stop or systemctl stop apache2

Check status

• service apache2 status or systemctl status apache2



Start and configure ssh

You can use username/password combination to access ssh, but this is not recommended, especially not with root user.

• Default server configuration file on /etc/ssh/sshd_conf

Create folders to hold ssh keys

- mkdir /root/.ssh
- chmod 0700 /root/.ssh

Create ssh key pair (use pass for better sec.)

• ssh-keygen

Copy id_rsa (private key) to system you will connect to Kali from and DELETE the private key on Kali!!



Start and configure ssh cont.

rename id_rsa.pub (public key) to authorized_keys

Change file permissions

chmod 0600 authorized_keys

Start ssh server service

- service ssh start (NOTICE! In this case service is not called sshd / it's called ssh)
- systemctl start ssh

Stop, status as explained on apache2 slides



Start and configure tftp

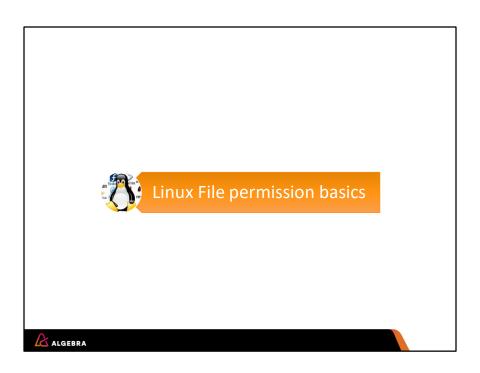
Install tftp server

- apt-get install atftpd
- Defaut document location /srv/tftp

Start tftp service

 service atftpd start or systemctl start atftpd





```
Linux file permission basics
     • d – folder, can also be:
      • Simbolic link (I), setuid/setgid (s), sticky bit permissions (t)
     • rwx - read write execute
     • First rwx set - owner permissions
     • Second rwx set – group permissions
     • Third rwx set - all users (world) permissions
         .i:/home/robert/.ssh# ls -lah
              2 robert robert 4.0K Jan 19 20:45 .
drwxd-xr-x 16 robert root
                                  4.0K Jan 17 09:00
                                    13K Jan 19 20:45 1
               1 root
                          root
                                    394 Sep 14 01:31 authorized keys
                 robert robert
   ALGEBRA
```

https://www.linux.com/learn/understanding-linux-file-permissions

Linux file permission basics

_ w_

_w x

r___

 r_x

rw_

rwx

rwx:

- 0 non of the permissions turned on
- 1 execute permission turned on
- 2 write permission turned on
- 3 write execute permission turned on
- 4 read permission turned on
- 5 read and execute permissions turned on
- 6 read and write permissions turned on
- 7 read, write and execute permission turned on

ALGEBRA

Linux file permission basics

Examples:

- chmod 0700 (_ rwx ____)
- chmod 0600 (_ rw_ ___ _)
- chmod 764 (_rwx rw_ r_ _)
- Leading zero doesn't have to be used in this cases it represents first underscore.
 It this is d or l it will be different number.



Linux passwords and users

/etc/passwd

/etc/shadow

- Password salted on most of todays Linux distributions
- \$1 MD5
- \$2 Blowfish
- \$2a ExBlowfish
- \$5 SHA-256
- \$6 SHA-512



Linux passwords and users

- robert:\$6\$qnLY7dsW\$EwK35OV7RTbydgqB3BKQ1o KL9zQaAeUnEj4ci4iAciwlhmGBiwAe5h4Fv3bYXkiV1 W0T9zY0k67eKurnZEkSB1:17186:0:99999:7:::
 - Name, Hash type,
 - Salt, Hash
 - Last password change
 - Minimum, Maximum
 - Warn, Inactive, Expire



challenge: Try to crack this password - Good luck ;-)

