

```
Shell x + Q P Publish
~/home: ls -l

~/workspace$ ^[[200~PS1='hola mundo $ '~
PS1='hola mundo $ '~bash: PS1=hola mundo $ ~: command not found
~/workspace$ ~PS1='hola mundo $ '~
bash: ~PS1=hola mundo $ ~: command not found
~/workspace$ PS1='hola mundo $'
hola mundo $
hola mundo $PS1='\u@\w$ '
runner@~/workspace$
runner@~/workspace$ PS1='\[\033[0;32m\]\u\[\033[0m\]@\[\033[0;34m\]\w\[\033[0m\]
: $ '
runner@~/workspace: $ PS1='\[\033[1;35m\]\t \d\[\033[0m\] $ '
13:19:28 Mon Oct 06 $ PS1='\[\033[1;35m\]\t \d\[\033[0m\] $ '
13:22:03 Mon Oct 06 $ PS1='\[\033[1;32m\]^C
13:23:17 Mon Oct 06 $ PS1='\[\033[1;32m\]\t \d\[\033[0m\] $ '
13:23:53 Mon Oct 06 $ date
Mon Oct 6 01:24:06 PM UTC 2025
13:24:06 Mon Oct 06 $ echo hola
hola
13:24:14 Mon Oct 06 $ echo %PATH
%PATH
13:25:10 Mon Oct 06 $ echo $Path

13:25:29 Mon Oct 06 $ echo $PATH
/nix/store/bap4d0lpcrhpwmpb8ayjcgkmvfj62lnq-bash-interactive-5.1-p16/bin:/nix/st
ore/pr5n59mb4jzmfxf6kanwxly0l07p861fg-patchelf-0.15.0/bin:/nix/store/dq0xwmsk1g0i
2ayg6pb7y87na2knzylh-gcc-wrapper-11.3.0/bin:/nix/store/lgf2flfqnpqbr1b4p4qz2f72y
42bs56r-gcc-11.3.0/bin:/nix/store/57xv61c5zi8pphjbcwxjlgc34p61ic9-glibc-2.35-16
3-bin/bin:/nix/store/a7gvj343m05j2s32xcnwr35v31ynlypr-coreutils-9.1/bin:/nix/sto
re/1d6ian3r8kdzspw8hacjhl3xkp40g1lj-binutils-wrapper-2.39/bin:/nix/store/039g378
vc3pc3dvi9dzdlrd0i4q93qwf-binutils-2.39/bin:/nix/store/p1qrn27c0q3x0338vy02v67jb
c8zk0ar-tree-2.0.4/bin:/nix/store/kblplvpffcfnozprj80vh41xchjx4jag-wget-1.21.3/b
in:/nix/store/nk3jcpqk04xbil6gk61dck9vcdcabxy-wkhtmltopdf-bin-0.12.6-3/bin:/nix
/store/1a0aw657n2v799swjffjncskjc859g6kk-imagemagick-7.1.0-52-dev/bin:/nix/store/
hl5lsmyf6alwj91nv8kmg2iz1lbnxym9-curl-7.86.0-dev/bin:/nix/store/39m0xn31z7n44wfl
fxqq7fbjh1ik6xq7-brotli-1.0.9/bin:/nix/store/0lm4ygsln65xi9pkw2kw29qiqqd80hz-li
bkrb5-1.20-dev/bin:/nix/store/r7gl900my2fw6k33nxh2r7rv8nv0s25-libkrb5-1.20/bin:/
nix/store/n8jl8q7kk4a03n4gjiymy4y4hpcp2apm-nghttp2-1.49.0-bin/bin:/nix/store/hf
kdbq95wsm9a0zf2hz51ads25h657hx-libidn2-2.3.2-bin/bin:/nix/store/fq47cv26nb87hwz2
678r6i8ym5b57lwf-openssl-3.0.7-bin/bin:/nix/store/mb0pcxkmrg0f6k0zaywlnvpk9q3j5a
ns-zstd-1.5.2-bin/bin:/nix/store/w10in9diaqrcqqxi5lg20n3q2jfpk6pq-zstd-1.5.2/bin
:/nix/store/52fbv6j49khca4cfvwm35fqd984w2520-curl-7.86.0-bin/bin:/nix/store/a8mh
cagrsly7c7mpjrpsnaahk4aax056-bzip2-1.0.8-bin/bin:/nix/store/v2lzl6dkp9f5kjva1sz
a5d3hfr2k8jg-freetype-2.12.1-dev/bin:/nix/store/ifswwxzvkvjyv7rq6i1a90vsw3n6ia1n
-libpng-apng-1.6.37-dev/bin:/nix/store/wwqnsjrk9ws6dfp5chxb6r3wcawbra1y-libjpeg-
turbo-2.1.4-bin/bin:/nix/store/zlcnmq14jz5x9439jf937mvayyl63da-xz-5.2.7-bin/bin
:/nix/store/3k4dxm0j11b2gr59ws8g5wr6v75vywml-libtiff-4.4.0-bin/bin:/nix/store/k0
```

```

  ▾ /home:mkdir hello.txt
/nix/store/a7gvj343m05j2s32xcnwr35v31nlypr-coreutils-9.1/bin/date
13:26:10 Mon Oct 06 $ pwd
/home/runner/workspace
13:28:07 Mon Oct 06 $ cd home
bash: cd: home: No such file or directory
13:28:11 Mon Oct 06 $ cd /home
13:28:21 Mon Oct 06 $ pwd
/home
13:28:24 Mon Oct 06 $ cd ..
13:28:31 Mon Oct 06 $ pwd
/
13:28:34 Mon Oct 06 $ cd ./home
13:28:39 Mon Oct 06 $ pwd
/home
13:28:44 Mon Oct 06 $ cd runner
13:28:50 Mon Oct 06 $ pwd
/home/runner
13:28:54 Mon Oct 06 $ ../../bin/echo hola
hola
13:29:06 Mon Oct 06 $ echo $HOME
/home/runner
13:29:34 Mon Oct 06 $ cd ~
13:29:42 Mon Oct 06 $ pwd
/home/runner
13:29:44 Mon Oct 06 $ cd home
bash: cd: home: No such file or directory
13:30:06 Mon Oct 06 $ cd /home
13:30:12 Mon Oct 06 $ ls -l
total 0
drwxrwxrwx 1 runner runner 46 Oct  6 13:06 runner
13:30:30 Mon Oct 06 $ echo hello > hello.txt
bash: hello.txt: Read-only file system
13:33:22 Mon Oct 06 $ cat hello.txt
cat: hello.txt: No such file or directory
13:33:32 Mon Oct 06 $ echo hello > hello.txt
bash: hello.txt: Read-only file system
13:33:39 Mon Oct 06 $ echo hello > hello.txt
bash: hello.txt: Read-only file system
13:34:25 Mon Oct 06 $
13:34:26 Mon Oct 06 $
13:34:26 Mon Oct 06 $
13:34:26 Mon Oct 06 $ cat < hello.txt > hello2.txt
bash: hello.txt: No such file or directory
13:35:28 Mon Oct 06 $ mkdir hello.txt
mkdir: cannot create directory 'hello.txt': Read-only file system
13:35:51 Mon Oct 06 $ █

```

```

-rwxr-xr-x 1 root root 31584 Sep 26 2024 watch
-rwxr-xr-x 1 root root 55824 Apr 5 2024 wc
-rwxr-xr-x 1 root root 35224 Dec 5 2024 wdctl
-rwxr-xr-x 1 root root 31576 Dec 5 2024 whereis
lrwxrwxrwx 1 root root 23 Mar 31 2024 which -> /etc/alternatives/whi
ch
-rwxr-xr-x 1 root root 1080 Mar 31 2024 which.debianutils
-rwxr-xr-x 1 root root 59928 Apr 5 2024 who
-rwxr-xr-x 1 root root 35336 Apr 5 2024 whoami
lrwxrwxrwx 1 root root 7 Dec 5 2024 x86_64 -> setarch
-rwxr-xr-x 1 root root 63912 Apr 8 2024 xargs
-rwxr-xr-x 1 root root 5167 Apr 8 12:47 xsubpp
-rwxr-xr-x 1 root root 89008 Mar 31 2025 xz
lrwxrwxrwx 1 root root 2 Mar 31 2025 xzcat -> xz
lrwxrwxrwx 1 root root 6 Mar 31 2025 xzcmp -> xzdiff
-rwxr-xr-x 1 root root 7422 Mar 31 2025 xzdiff
lrwxrwxrwx 1 root root 6 Mar 31 2025 xzegrep -> xzgrep
lrwxrwxrwx 1 root root 6 Mar 31 2025 xzfgrep -> xzgrep
-rwxr-xr-x 1 root root 10333 Mar 31 2025 xzgrep
-rwxr-xr-x 1 root root 1813 Mar 31 2025 xzless
-rwxr-xr-x 1 root root 2190 Mar 31 2025 xzmore
-rwxr-xr-x 1 root root 35208 Apr 5 2024 yes
lrwxrwxrwx 1 root root 8 Apr 8 2024 ypdomainname -> hostname
-rwxr-xr-x 1 root root 1984 Apr 8 2024 zcat
-rwxr-xr-x 1 root root 1678 Apr 8 2024 zcmp
-rwxr-xr-x 1 root root 6460 Apr 8 2024 zdiff
-rwxr-xr-x 1 root root 31008 Jan 28 2025 zdump
-rwxr-xr-x 1 root root 29 Apr 8 2024 zegrep
-rwxr-xr-x 1 root root 29 Apr 8 2024 zfgrep
-rwxr-xr-x 1 root root 2081 Apr 8 2024 zforce
-rwxr-xr-x 1 root root 8103 Apr 8 2024 zgrep
-rwxr-xr-x 1 root root 70193 Apr 8 12:47 zipdetails
-rwxr-xr-x 1 root root 2206 Apr 8 2024 zless
-rwxr-xr-x 1 root root 1842 Apr 8 2024 zmore
-rwxr-xr-x 1 root root 4577 Apr 8 2024 znew
13:36:28 Mon Oct 06 $ ls -l | tail -n1
-rwxr-xr-x 1 root root 4577 Apr 8 2024 znew
13:36:35 Mon Oct 06 $ curl --head --silent google.com | grep Length
Content-Length: 219
13:37:03 Mon Oct 06 $ cd ~/workspace
13:37:22 Mon Oct 06 $ curl -o logo_wikimedia.png https://upload.wikimedia.org/wi
kipedia/commons/6/63/Wikipedia-logo.png
% Total % Received % Xferd Average Speed Time Time Time Current
Dload Upload Total Spent Left Speed
100 38692 100 38692 0 0 245k 0 --:--:-- --:--:-- --:--:-- 246k
13:37:31 Mon Oct 06 $

```



ESP  
LAA



8:37 a.m.  
6/10/2025

## Taller

```
~ /workspace/hacker-lab: echo \"Iniciando el escaneo...\"

13:38:46 Mon Oct 06 $ cd ~/workspace
13:38:52 Mon Oct 06 $ mkdir hacker-lab
cd hacker-lab
13:39:02 Mon Oct 06 $ touch scanner.sh
13:39:14 Mon Oct 06 $ #!/bin/bash

# Escaneo de archivos sospechosos en el sistema
echo "Iniciando el escaneo..."

# Busca archivos que contengan la palabra 'password'
grep -ril "password" /etc /var

# Busca archivos con permisos de ejecución para todos
find /var -type f -perm -111 2>/dev/null

echo "Escaneo completado."
Iniciando el escaneo...
/etc/login.defs
/nix/store/8b4vn1iyn6kqiisjvlmv67d1c0p3j6wj-gnugrep-3.11/bin/grep: /etc/shadow-:
Permission denied
/etc/default/useradd
/etc/security/pwhistory.conf
/nix/store/8b4vn1iyn6kqiisjvlmv67d1c0p3j6wj-gnugrep-3.11/bin/grep: /etc/security
/opasswd: Permission denied
/nix/store/8b4vn1iyn6kqiisjvlmv67d1c0p3j6wj-gnugrep-3.11/bin/grep: /etc/gshadow:
Permission denied
/etc/debconf.conf
/nix/store/8b4vn1iyn6kqiisjvlmv67d1c0p3j6wj-gnugrep-3.11/bin/grep: /etc/.pwd.loc
k: Permission denied
/etc/pam.d/chpasswd
/etc/pam.d/other
/etc/pam.d/newusers
/etc/pam.d/su
/etc/pam.d/su-l
/etc/pam.d/common-password
/etc/pam.d/chsh
/etc/pam.d/login
/etc/pam.d/chfn
/etc/pam.d/passwd
/nix/store/8b4vn1iyn6kqiisjvlmv67d1c0p3j6wj-gnugrep-3.11/bin/grep: /etc/gshadow-
: Permission denied
/nix/store/8b4vn1iyn6kqiisjvlmv67d1c0p3j6wj-gnugrep-3.11/bin/grep: /etc/shadow:
Permission denied
/nix/store/8b4vn1iyn6kqiisjvlmv67d1c0p3j6wj-gnugrep-3.11/bin/grep: /etc/ssl/priv
ate: Permission denied
/etc/ssl/openssl.cnf
```

```
Shell x + Q + Publish
~/workspace/hacker-lab: echo "\"Iniciando el escaneo...\"" > scan_report.txt

/var/lib/dpkg/info/xz-utils.postinst
/var/lib/dpkg/info/perl.postrm
/var/lib/dpkg/info/git.postinst
/var/lib/dpkg/info/fonts-dejavu-core.preinst
/var/lib/dpkg/info/fonts-dejavu-core.prerm
/var/lib/dpkg/info/perl.preinst
/var/lib/dpkg/info/locales.prerm
/var/lib/dpkg/info/libgssapi-krb5-2:amd64.postrm
/var/lib/dpkg/info/fontconfig-config.preinst
/var/lib/dpkg/info/fontconfig-config.prerm
/var/lib/dpkg/info/locales.postrm
/var/lib/dpkg/info/ca-certificates.postrm
/var/lib/dpkg/info/libgssapi-krb5-2:amd64.postinst
/var/lib/dpkg/info/xz-utils.prerm
/var/lib/dpkg/info/perl.prerm
/var/lib/dpkg/info/git.preinst
/var/lib/dpkg/info/locales.config
/var/lib/dpkg/info/ca-certificates.config
/var/lib/dpkg/info/perl.postinst
/var/lib/dpkg/info/fontconfig.postinst
/var/lib/dpkg/info/openssl.postinst
/var/lib/dpkg/info/fonts-dejavu-core.postrm
/var/lib/dpkg/info/ca-certificates.postinst
/var/lib/dpkg/info/locales.postinst
/var/lib/dpkg/info/git.prerm
Escaneo completado.
13:39:38 Mon Oct 06 $ chmod +x scanner.sh
13:40:18 Mon Oct 06 $ ./scanner.sh
13:40:25 Mon Oct 06 $ #!/bin/bash

echo "Iniciando el escaneo..." > scan_report.txt

# Busca archivos que contengan la palabra 'password'
grep -rils "password" /etc /var >> scan_report.txt &

# Busca archivos con permisos de ejecución para todos
find /var -type f -perm -111 2>/dev/null >> scan_report.txt &

echo "Escaneo completado. Revisa el archivo scan_report.txt para los resultados."
"
[1] 839
[2] 840
Escaneo completado. Revisa el archivo scan_report.txt para los resultados.
[2]+ Exit 1 find /var -type f -perm -111 2> /dev/null >> scan_report.txt
13:40:56 Mon Oct 06 $
```