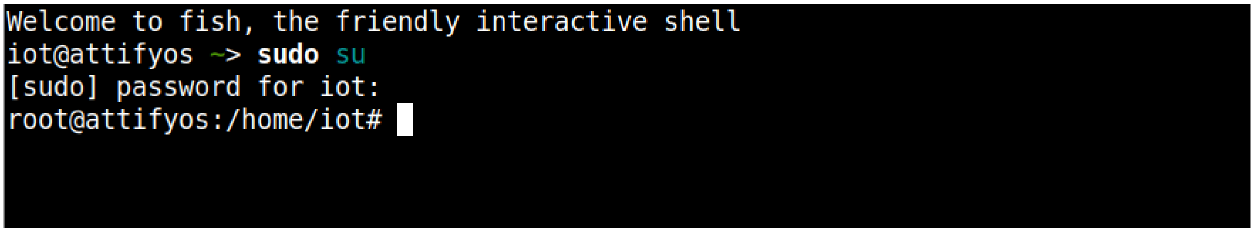
Experiment - 2

Aim : Exploring commands and tools in attify OS

Objective : The practical aims to enhance understanding of Attify OS capabilities for effective security analysis

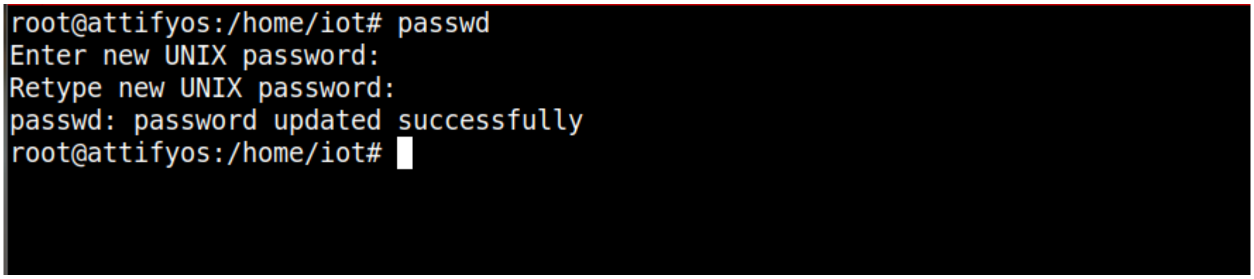
Commands:

1. sudo su : In Attify OS, sudo su grants root access for executing privileged tasks and system configurations.



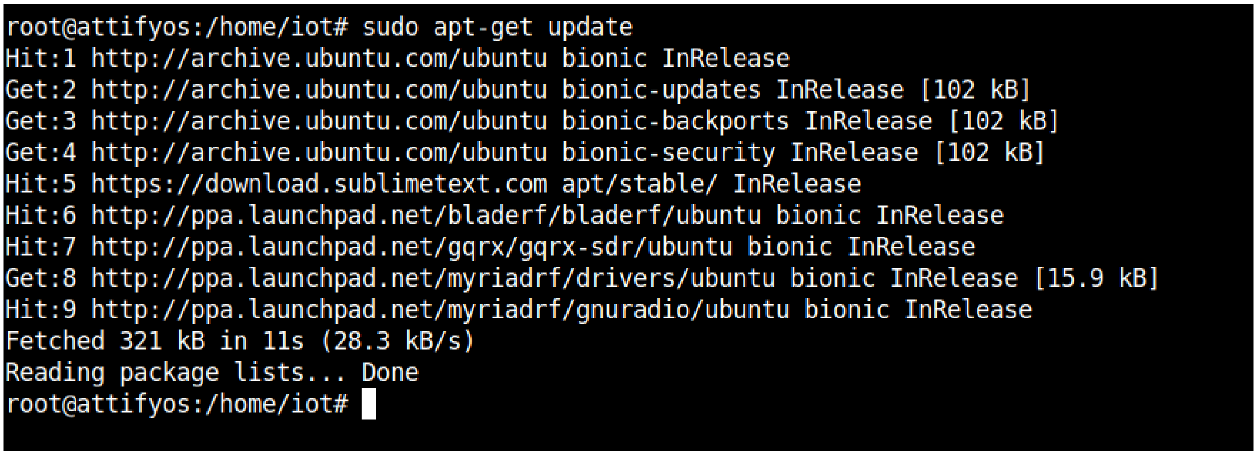
```
Welcome to fish, the friendly interactive shell
iot@attifyos ~> sudo su
[sudo] password for iot:
root@attifyos:/home/iot# 
```

2. passwd : It is used to change the password for the current user or another specified user (requires root privileges).



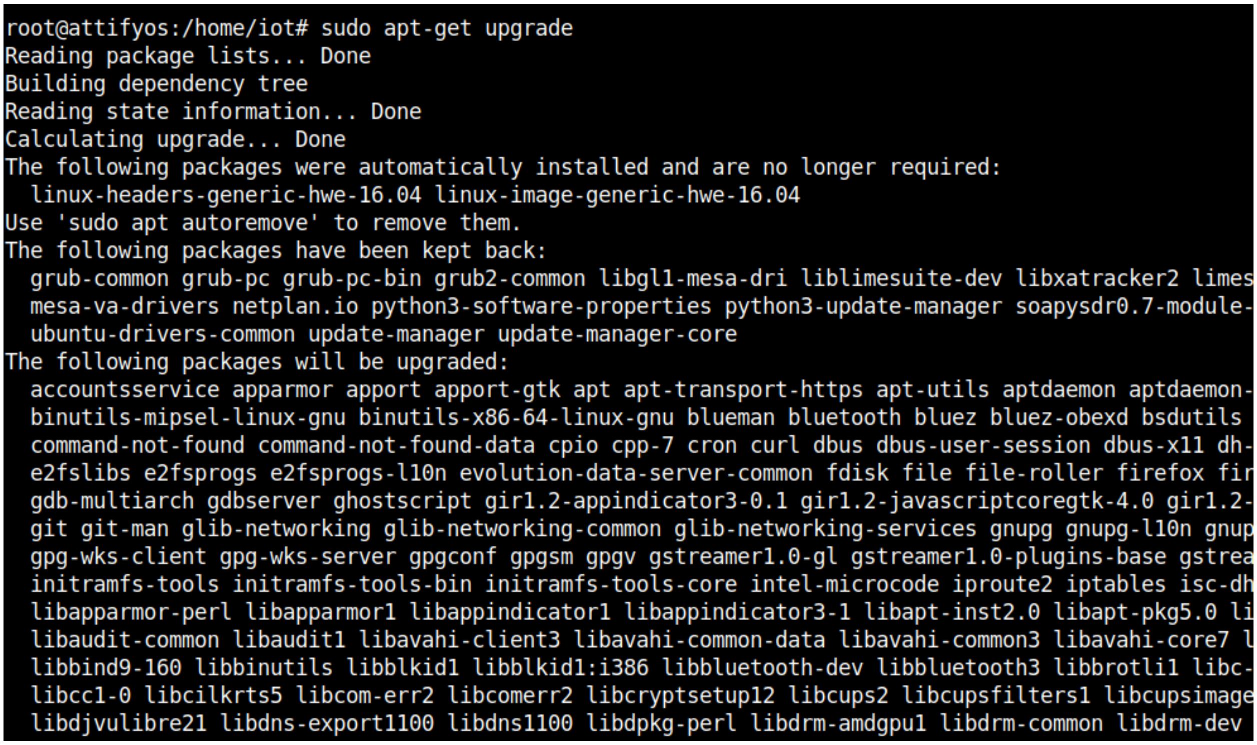
```
root@attifyos:/home/iot# passwd
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
root@attifyos:/home/iot# 
```

3. sudo apt-get update : It updates the package list to ensure access to the latest versions and dependencies from configured repositories.

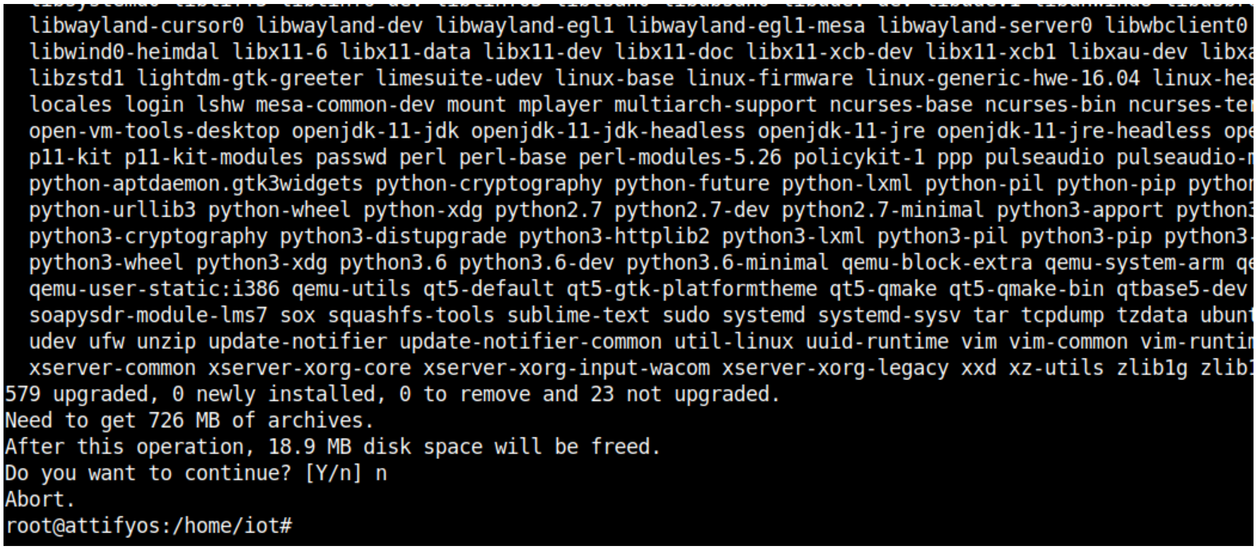


```
root@attifyos:/home/iot# sudo apt-get update
Hit:1 http://archive.ubuntu.com/ubuntu bionic InRelease
Get:2 http://archive.ubuntu.com/ubuntu bionic-updates InRelease [102 kB]
Get:3 http://archive.ubuntu.com/ubuntu bionic-backports InRelease [102 kB]
Get:4 http://archive.ubuntu.com/ubuntu bionic-security InRelease [102 kB]
Hit:5 https://download.sublimetext.com apt/stable/ InRelease
Hit:6 http://ppa.launchpad.net/bladerf/bladerf/ubuntu bionic InRelease
Hit:7 http://ppa.launchpad.net/gqrx/gqrx-sdr/ubuntu bionic InRelease
Get:8 http://ppa.launchpad.net/myriadrf/drivers/ubuntu bionic InRelease [15.9 kB]
Hit:9 http://ppa.launchpad.net/myriadrf/gnuradio/ubuntu bionic InRelease
Fetched 321 kB in 11s (28.3 kB/s)
Reading package lists... Done
root@attifyos:/home/iot#
```

4. sudo apt-get upgrade : It installs the latest available versions of all installed packages while keeping the current configurations intact.

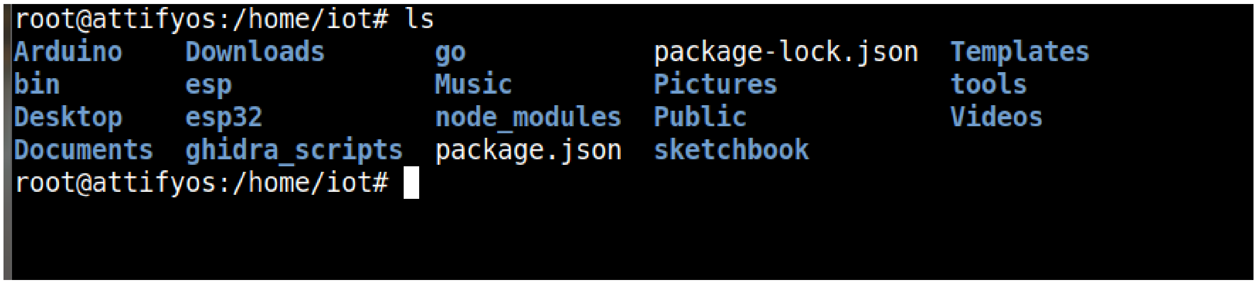


```
root@attifyos:/home/iot# sudo apt-get upgrade
Reading package lists... Done
Building dependency tree
Reading state information... Done
Calculating upgrade... Done
The following packages were automatically installed and are no longer required:
  linux-headers-generic-hwe-16.04 linux-image-generic-hwe-16.04
Use 'sudo apt autoremove' to remove them.
The following packages have been kept back:
  grub-common grub-pc grub-pc-bin grub2-common libgl1-mesa-dri liblimesuite-dev libxatracker2 limes
  mesa-va-drivers netplan.io python3-software-properties python3-update-manager soapysdr0.7-module-
  ubuntu-drivers-common update-manager update-manager-core
The following packages will be upgraded:
  accountsservice apparmor apport apport-gtk apt apt-transport-https apt-utils aptdaemon aptdaemon-
  binutils-mipsel-linux-gnu binutils-x86-64-linux-gnu blueman bluetooth bluez bluez-obexd bsdutils
  command-not-found command-not-found-data cpio cpp-7 cron curl dbus dbus-user-session dbus-x11 dh-
  e2fslibs e2fsprogs e2fsprogs-l10n evolution-data-server-common fdisk file file-roller firefox fir
  gdb-multiarch gdbserver ghostscript gir1.2-appindicator3-0.1 gir1.2-javascriptcoregtk-4.0 gir1.2-
  git git-man glib-networking glib-networking-common glib-networking-services gnupg gnupg-l10n gnup
  gpg-wks-client gpg-wks-server gpgconf gpgsm gpgv gstreamer1.0-gl gstreamer1.0-plugins-base gstrea
  initramfs-tools initramfs-tools-bin initramfs-tools-core intel-microcode iproute2 iptables isc-dh
  libapparmor-perl libapparmor1 libappindicator1 libappindicator3-1 libapt-inst2.0 libapt-pkg5.0 li
  libaudit-common libaudit1 libavahi-client3 libavahi-common-data libavahi-common3 libavahi-core7 l
  libbind9-160 libbinutils libblkid1 libblkid1:i386 libbluetooth-dev libbluetooth3 libbrotli1 libc-
  libcc1-0 libcilkrts5 libcom-err2 libcomerr2 libcryptsetup12 libcups2 libcupsfilters1 libcupsimage
  libdjvulibre21 libdns-export1100 libdns1100 libdpkg-perl libdrm-amdgpu1 libdrm-common libdrm-dev
```



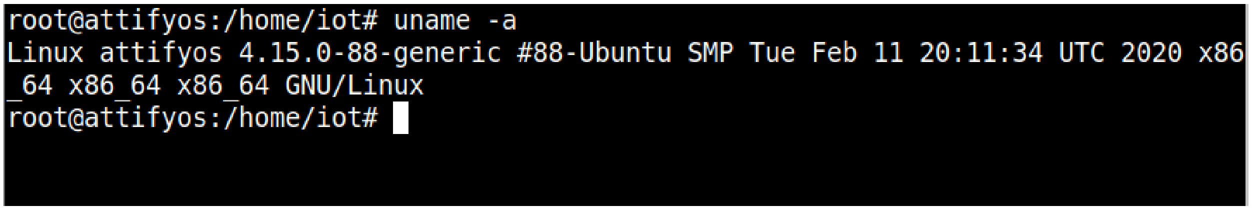
```
  libwayland-cursor0 libwayland-dev libwayland-egl1 libwayland-egl1-mesa libwayland-server0 libwbclient0
  libwind0-heimdal libx11-6 libx11-data libx11-dev libx11-doc libx11-xcb-dev libx11-xcb1 libxau-dev libxa
  libzstd1 lightdm-gtk-greeter limesuite-udev linux-base linux-firmware linux-generic-hwe-16.04 linux-hea
  locales login lshw mesa-common-dev mount mplayer multiarch-support ncurses-base ncurses-bin ncurses-ter
  open-vm-tools-desktop openjdk-11-jdk openjdk-11-jdk-headless openjdk-11-jre openjdk-11-jre-headless ope
  p11-kit p11-kit-modules passwd perl perl-base perl-modules-5.26 policykit-1 ppp pulseaudio pulseaudio-m
  python-aptdaemon.gtk3widgets python-cryptography python-future python-lxml python-pil python-pip python
  python-urllib3 python-wheel python-xdg python2.7 python2.7-dev python2.7-minimal python3-apport python3
  python3-cryptography python3-distupgrade python3-httplib2 python3-lxml python3-pil python3-pip python3-
  python3-wheel python3-xdg python3.6 python3.6-dev python3.6-minimal qemu-block-extra qemu-system-arm qe
  qemu-user-static:i386 qemu-utils qt5-default qt5-gtk-platformtheme qt5-qmake qt5-qmake-bin qtbase5-dev
  soapysdr-module-lms7 sox squashfs-tools sublime-text sudo systemd systemd-sysv tar tcpdump tzdata ubunt
  udev ufw unzip update-notifier update-notifier-common util-linux uuid-runtime vim vim-common vim-runtin
  xserver-common xserver-xorg-core xserver-xorg-input-wacom xserver-xorg-legacy xxd xz-utils zlib1g zlib1
579 upgraded, 0 newly installed, 0 to remove and 23 not upgraded.
Need to get 726 MB of archives.
After this operation, 18.9 MB disk space will be freed.
Do you want to continue? [Y/n] n
Abort.
root@attifyos:/home/iot#
```

5. ls : It lists the files and directories in the current directory.



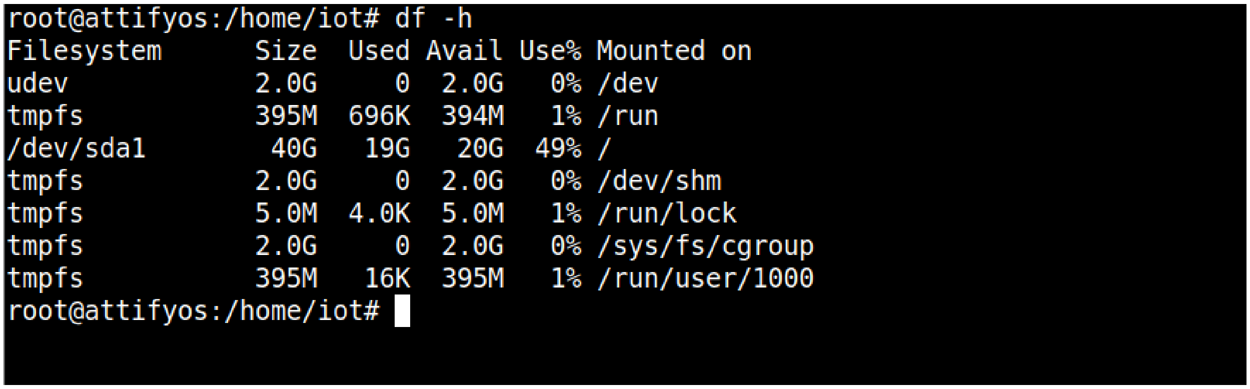
```
root@attifyos:/home/iot# ls
Arduino    Downloads      go            package-lock.json  Templates
bin        esp            Music         Pictures           tools
Desktop    esp32          node_modules  Public             Videos
Documents  ghidra_scripts  package.json  sketchbook
root@attifyos:/home/iot# 
```

6. uname -a: It displays detailed system information, including the kernel name, version, architecture, and more.



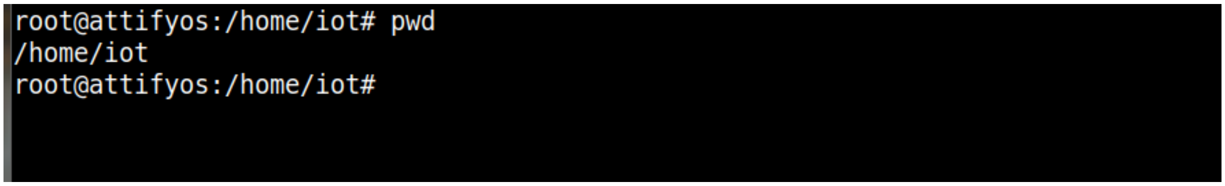
```
root@attifyos:/home/iot# uname -a
Linux attifyos 4.15.0-88-generic #88-Ubuntu SMP Tue Feb 11 20:11:34 UTC 2020 x86
_64 x86_64 x86_64 GNU/Linux
root@attifyos:/home/iot# 
```

7. df -h : It shows the disk space usage of all mounted file systems in a human-readable format.



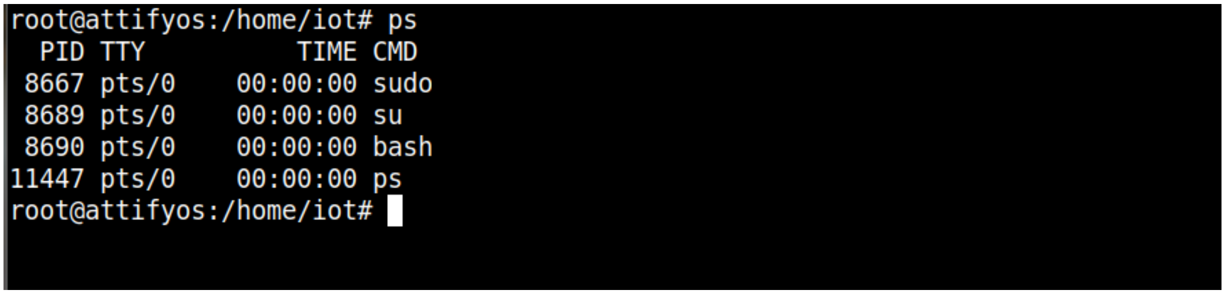
```
root@attifyos:/home/iot# df -h
Filesystem      Size  Used Avail Use% Mounted on
udev            2.0G     0  2.0G   0% /dev
tmpfs           395M  696K  394M   1% /run
/dev/sda1        40G   19G   20G  49% /
tmpfs           2.0G     0  2.0G   0% /dev/shm
tmpfs           5.0M  4.0K  5.0M   1% /run/lock
tmpfs           2.0G     0  2.0G   0% /sys/fs/cgroup
tmpfs           395M   16K  395M   1% /run/user/1000
root@attifyos:/home/iot# 
```

8. pwd : It prints the current working directory's full path.



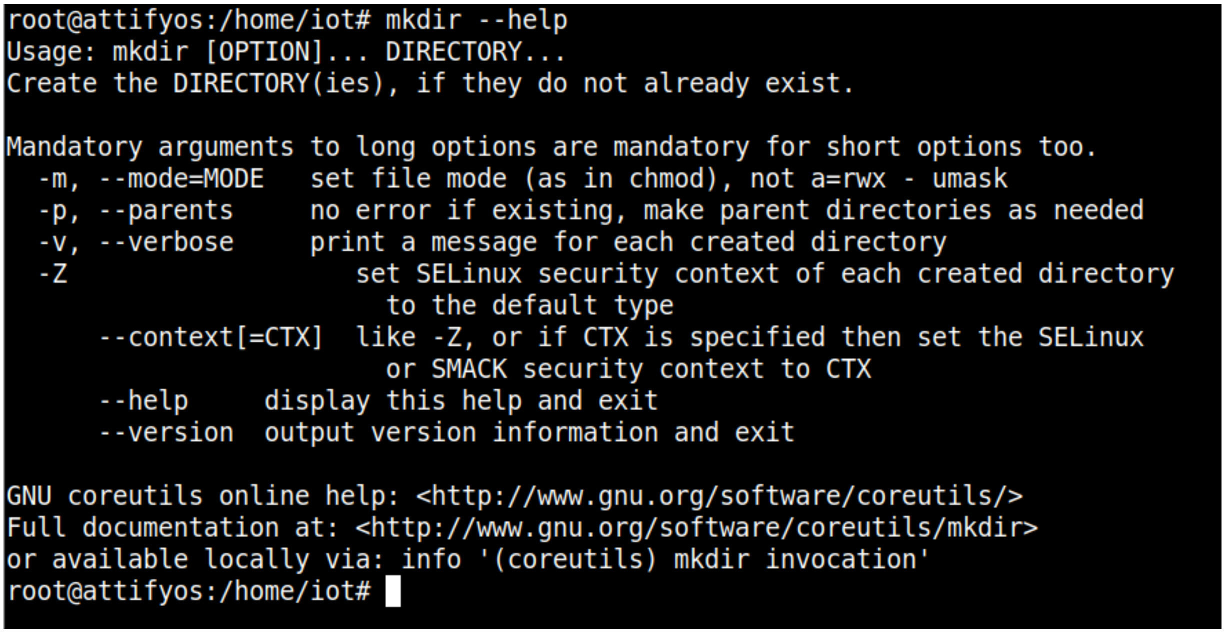
```
root@attifyos:/home/iot# pwd
/home/iot
root@attifyos:/home/iot#
```

9. ps : It displays a snapshot of the currently running processes on the system.



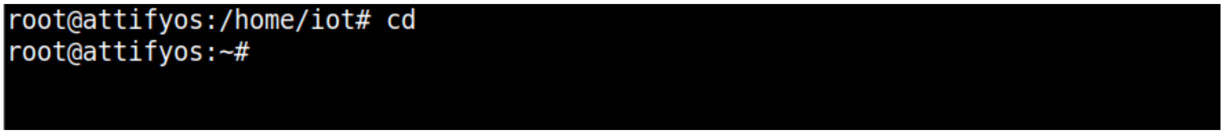
```
root@attifyos:/home/iot# ps
  PID TTY          TIME CMD
 8667 pts/0    00:00:00 sudo
 8689 pts/0    00:00:00 su
 8690 pts/0    00:00:00 bash
11447 pts/0    00:00:00 ps
root@attifyos:/home/iot# 
```

10. mkdir : It is used to create a new directory.



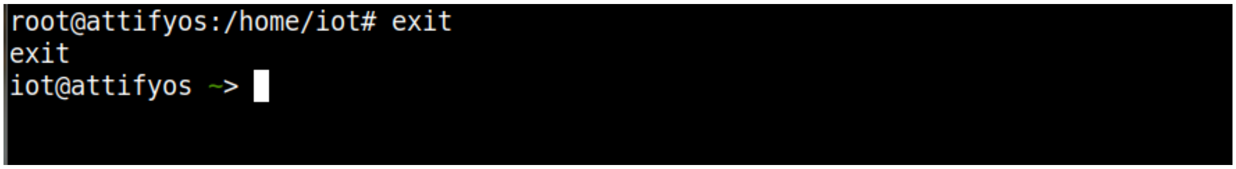
```
root@attifyos:/home/iot# mkdir --help
Usage: mkdir [OPTION]... DIRECTORY...
Create the DIRECTORY(ies), if they do not already exist.

Mandatory arguments to long options are mandatory for short options too.
  -m, --mode=MODE   set file mode (as in chmod), not a=rwx - umask
  -p, --parents     no error if existing, make parent directories as needed
  -v, --verbose     print a message for each created directory
  -Z                   set SELinux security context of each created directory
                         to the default type
      --context[=CTX]  like -Z, or if CTX is specified then set the SELinux
                         or SMACK security context to CTX
      --help     display this help and exit
      --version  output version information and exit

GNU coreutils online help: <http://www.gnu.org/software/coreutils/>
Full documentation at: <http://www.gnu.org/software/coreutils/mkdir>
or available locally via: info '(coreutils) mkdir invocation'
root@attifyos:/home/iot# 
```

11. cd : It is used to change the current working directory.



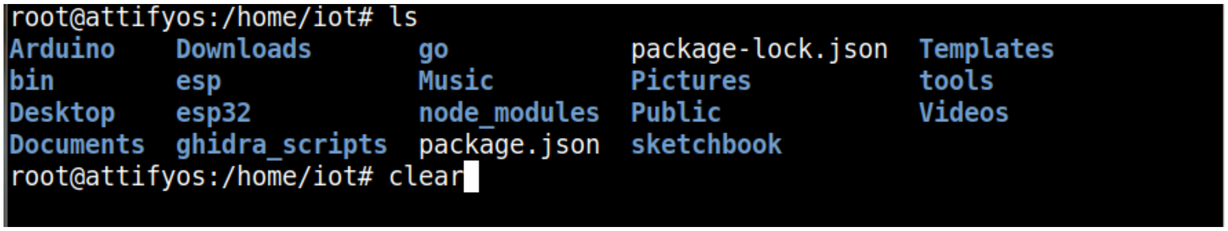
```
root@attifyos:/home/iot# cd
root@attifyos:~#
```

12. exit : It is used to close the current terminal session or log out from the root user when in a sudo su session.



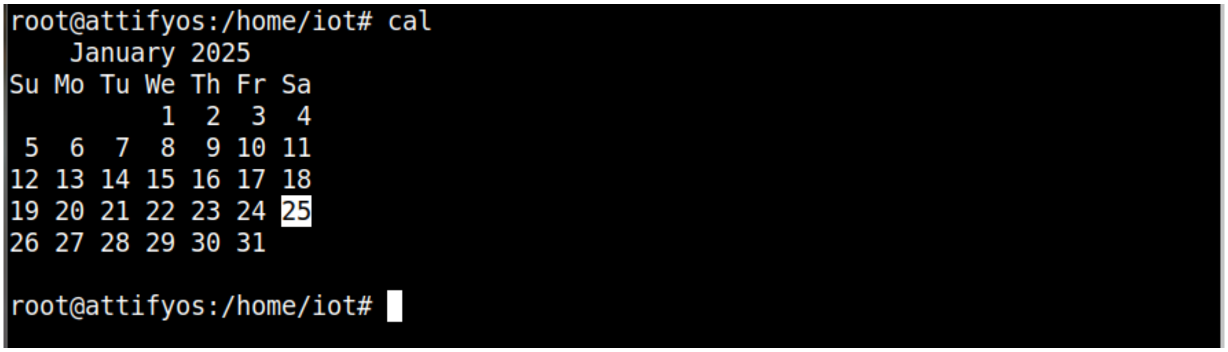
```
root@attifyos:/home/iot# exit
exit
iot@attifyos ~> 
```

13. clear : It clears the terminal screen, removing all previous output for a clean workspace.



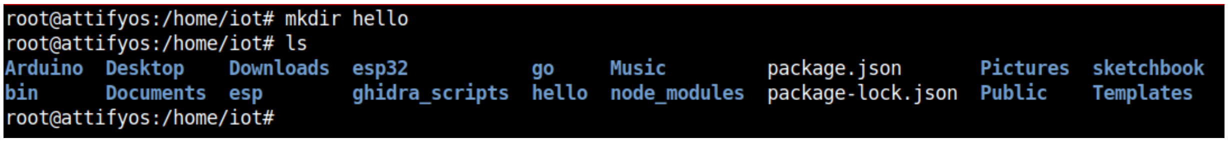
```
root@attifyos:/home/iot# ls
Arduino    Downloads      go            package-lock.json  Templates
bin        esp            Music         Pictures           tools
Desktop    esp32          node_modules  Public             Videos
Documents  ghidra_scripts package.json  sketchbook
root@attifyos:/home/iot# clear
```

14. cal : It displays a calendar of the current month. You can also specify a year or month for a different calendar view.



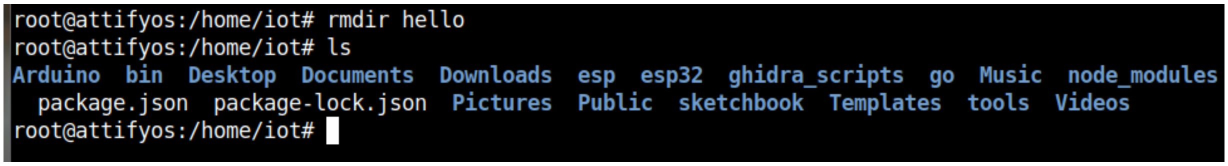
```
root@attifyos:/home/iot# cal
    January 2025
Su Mo Tu We Th Fr Sa
          1  2  3  4
 5  6  7  8  9 10 11
12 13 14 15 16 17 18
19 20 21 22 23 24 25
26 27 28 29 30 31

root@attifyos:/home/iot# 
```

15. mkdir : It is used to create a new directory.



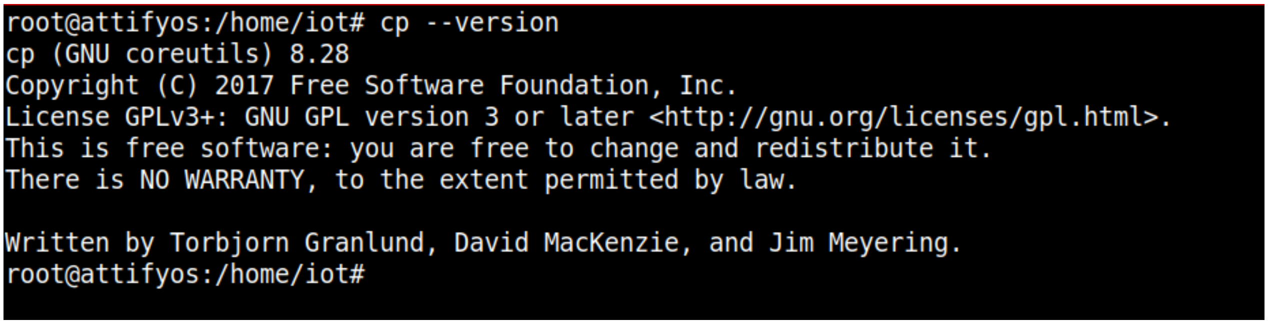
```
root@attifyos:/home/iot# mkdir hello
root@attifyos:/home/iot# ls
Arduino  Desktop    Downloads  esp32          go     Music         package.json       Pictures   sketchbook
bin      Documents  esp        ghidra_scripts  hello  node_modules  package-lock.json  Public     Templates
root@attifyos:/home/iot#
```

16. rmdir : It is used to remove an empty directory.



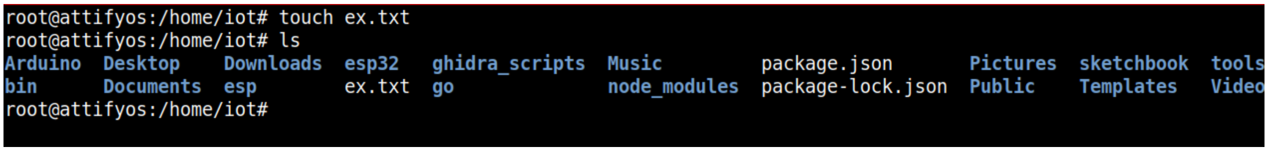
```
root@attifyos:/home/iot# rmdir hello
root@attifyos:/home/iot# ls
Arduino  bin  Desktop  Documents  Downloads  esp  esp32  ghidra_scripts  go  Music  node_modules
  package.json  package-lock.json  Pictures  Public  sketchbook  Templates  tools  Videos
root@attifyos:/home/iot# 
```

17. cp : It is used to copy files or directories from one location to another.



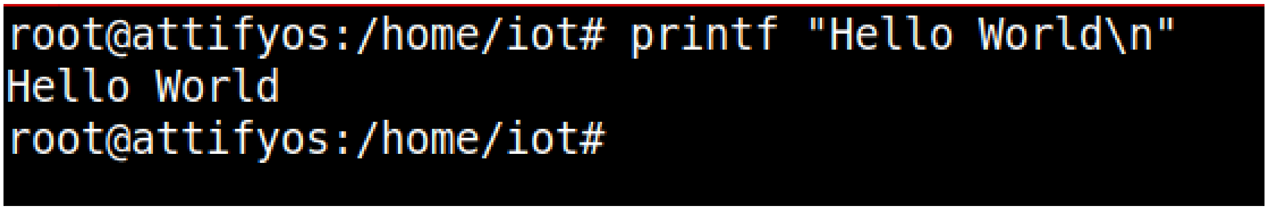
```
root@attifyos:/home/iot# cp --version
cp (GNU coreutils) 8.28
Copyright (C) 2017 Free Software Foundation, Inc.
License GPLv3+: GNU GPL version 3 or later <http://gnu.org/licenses/gpl.html>.
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law.

Written by Torbjorn Granlund, David MacKenzie, and Jim Meyering.
root@attifyos:/home/iot#
```

18. touch : It is used to create an empty file or update the timestamp of an existing file.



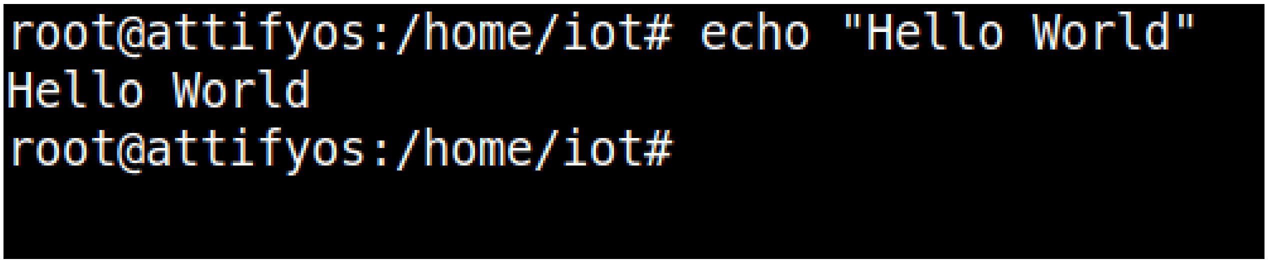
```
root@attifyos:/home/iot# touch ex.txt
root@attifyos:/home/iot# ls
Arduino  Desktop    Downloads  esp32   ghidra_scripts  Music         package.json       Pictures  sketchbook  tools
bin      Documents  esp        ex.txt  go              node_modules  package-lock.json  Public    Templates   Video
root@attifyos:/home/iot#
```

19. printf : It is used to print formatted output to the terminal, allowing control over the text's appearance, such as width, precision, and alignment.



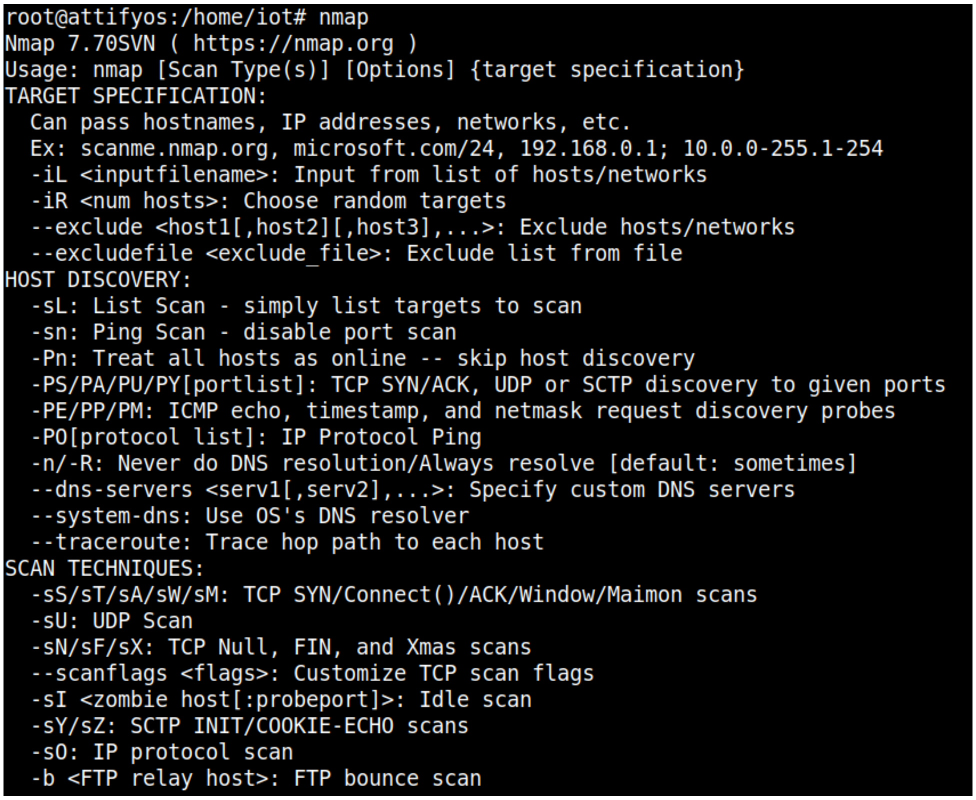
```
root@attifyos:/home/iot# printf "Hello World\n"
Hello World
root@attifyos:/home/iot#
```

20. echo : It is used to display a line of text or a variable's value in the terminal.



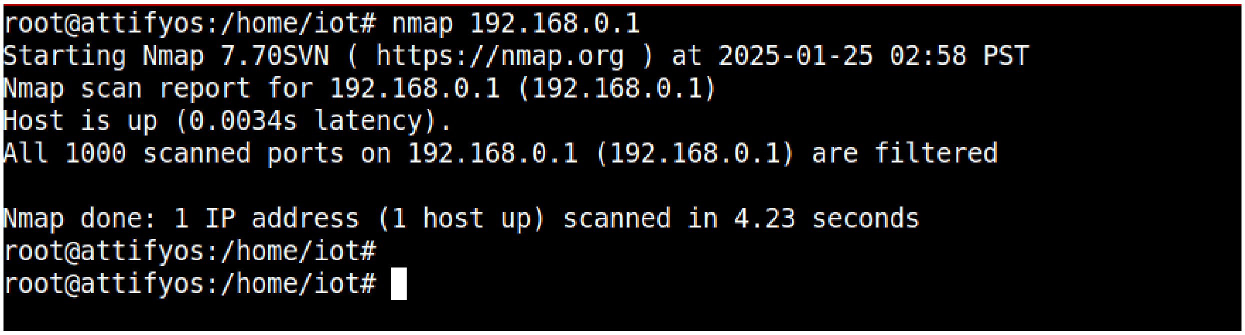
```
root@attifyos:/home/iot# echo "Hello World"
Hello World
root@attifyos:/home/iot#
```

21. nmap : It is a network scanning tool used to discover hosts, services, and vulnerabilities on a network.



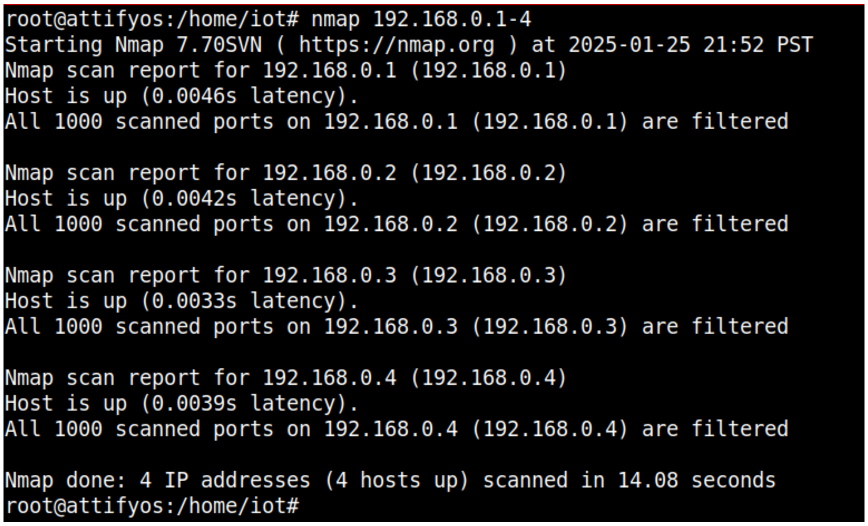
```
root@attifyos:/home/iot# nmap
Nmap 7.70SVN ( https://nmap.org )
Usage: nmap [Scan Type(s)] [Options] {target specification}
TARGET SPECIFICATION:
  Can pass hostnames, IP addresses, networks, etc.
  Ex: scanme.nmap.org, microsoft.com/24, 192.168.0.1; 10.0.0-255.1-254
  -iL <inputfilename>: Input from list of hosts/networks
  -iR <num hosts>: Choose random targets
  --exclude <host1[,host2][,host3],...>: Exclude hosts/networks
  --excludefile <exclude_file>: Exclude list from file
HOST DISCOVERY:
  -sL: List Scan - simply list targets to scan
  -sn: Ping Scan - disable port scan
  -Pn: Treat all hosts as online -- skip host discovery
  -PS/PA/PU/PY[portlist]: TCP SYN/ACK, UDP or SCTP discovery to given ports
  -PE/PP/PM: ICMP echo, timestamp, and netmask request discovery probes
  -PO[protocol list]: IP Protocol Ping
  -n/-R: Never do DNS resolution/Always resolve [default: sometimes]
  --dns-servers <serv1[,serv2],...>: Specify custom DNS servers
  --system-dns: Use OS's DNS resolver
  --traceroute: Trace hop path to each host
SCAN TECHNIQUES:
  -sS/sT/sA/sW/sM: TCP SYN/Connect()/ACK/Window/Maimon scans
  -sU: UDP Scan
  -sN/sF/sX: TCP Null, FIN, and Xmas scans
  --scanflags <flags>: Customize TCP scan flags
  -sI <zombie host[:probeport]>: Idle scan
  -sY/sZ: SCTP INIT/COOKIE-ECHO scans
  -sO: IP protocol scan
  -b <FTP relay host>: FTP bounce scan
```

22. nmap 192.168.0.1 : It scans the IP address 192.168.0.1 to discover open ports, services, and potential vulnerabilities on the device or network at that address.



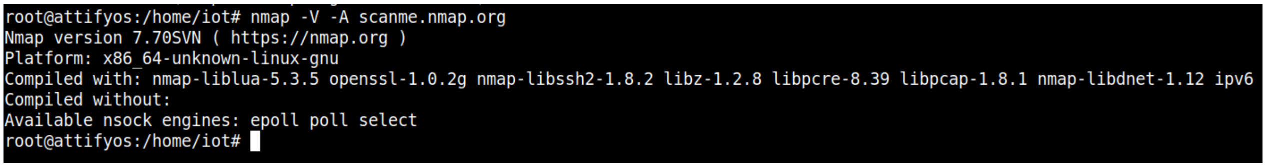
```
root@attifyos:/home/iot# nmap 192.168.0.1
Starting Nmap 7.70SVN ( https://nmap.org ) at 2025-01-25 02:58 PST
Nmap scan report for 192.168.0.1 (192.168.0.1)
Host is up (0.0034s latency).
All 1000 scanned ports on 192.168.0.1 (192.168.0.1) are filtered

Nmap done: 1 IP address (1 host up) scanned in 4.23 seconds
root@attifyos:/home/iot#
root@attifyos:/home/iot# 
```

23. nmap 192.168.0.1-4 : It scans the IP range from 192.168.0.1 to 192.168.0.4, checking for open ports and services on all devices within that range.



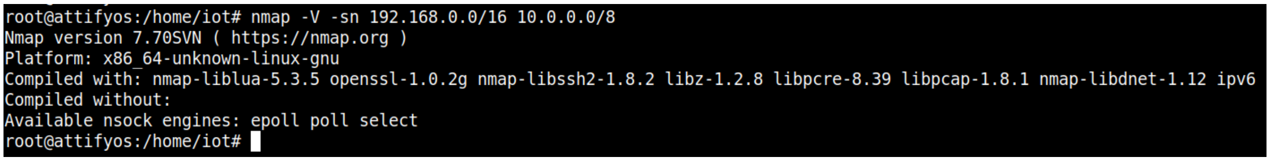
```
root@attifyos:/home/iot# nmap 192.168.0.1-4
Starting Nmap 7.70SVN ( https://nmap.org ) at 2025-01-25 21:52 PST
Nmap scan report for 192.168.0.1 (192.168.0.1)
Host is up (0.0046s latency).
All 1000 scanned ports on 192.168.0.1 (192.168.0.1) are filtered

Nmap scan report for 192.168.0.2 (192.168.0.2)
Host is up (0.0042s latency).
All 1000 scanned ports on 192.168.0.2 (192.168.0.2) are filtered

Nmap scan report for 192.168.0.3 (192.168.0.3)
Host is up (0.0033s latency).
All 1000 scanned ports on 192.168.0.3 (192.168.0.3) are filtered

Nmap scan report for 192.168.0.4 (192.168.0.4)
Host is up (0.0039s latency).
All 1000 scanned ports on 192.168.0.4 (192.168.0.4) are filtered

Nmap done: 4 IP addresses (4 hosts up) scanned in 14.08 seconds
root@attifyos:/home/iot#
```

24. nmap -V -A scanme.nmap.org : It performs a detailed scan on scanme.nmap.org. The -V option displays the Nmap version, and the -A option enables aggressive scanning, which includes OS detection, version detection, script scanning, and traceroute.



```
root@attifyos:/home/iot# nmap -V -A scanme.nmap.org
Nmap version 7.70SVN ( https://nmap.org )
Platform: x86_64-unknown-linux-gnu
Compiled with: nmap-liblua-5.3.5 openssl-1.0.2g nmap-libssh2-1.8.2 libz-1.2.8 libpcre-8.39 libpcap-1.8.1 nmap-libdnet-1.12 ipv6
Compiled without:
Available nsock engines: epoll poll select
root@attifyos:/home/iot# █
```

25. nmap -V -sn 192.168.0.0/16 10.0.0.0/8 : It performs a **ping scan** (-sn) to discover active hosts in the IP ranges 192.168.0.0/16 and 10.0.0.0/8, without scanning for open ports. The -V option displays the Nmap version.



```
root@attifyos:/home/iot# nmap -V -sn 192.168.0.0/16 10.0.0.0/8
Nmap version 7.70SVN ( https://nmap.org )
Platform: x86_64-unknown-linux-gnu
Compiled with: nmap-liblua-5.3.5 openssl-1.0.2g nmap-libssh2-1.8.2 libz-1.2.8 libpcre-8.39 libpcap-1.8.1 nmap-libdnet-1.12 ipv6
Compiled without:
Available nsock engines: epoll poll select
root@attifyos:/home/iot# █
```

Conclusion:

Exploring and Mastery of these commands allows for effective vulnerability identification, firmware analysis, and network traffic monitoring, empowering researchers to strengthen IoT security and mitigate potential threats.