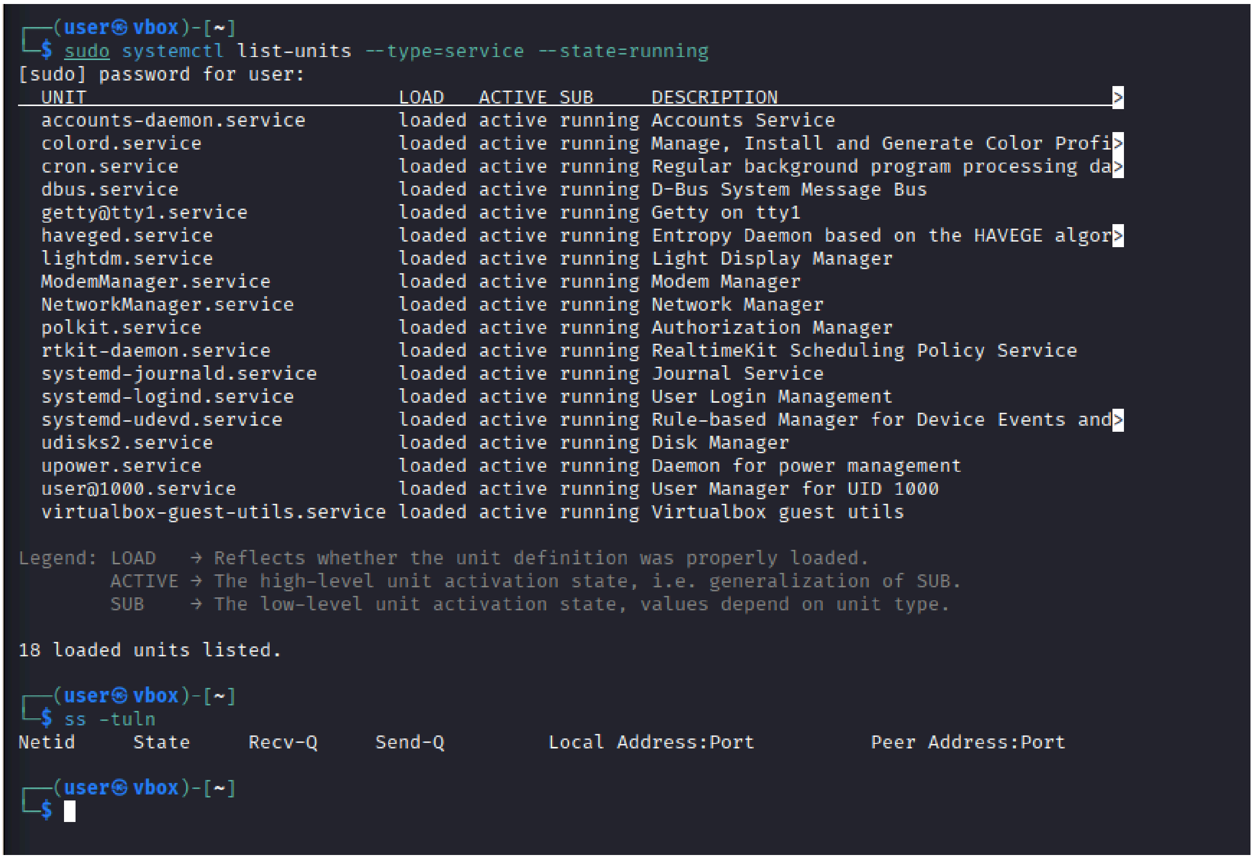
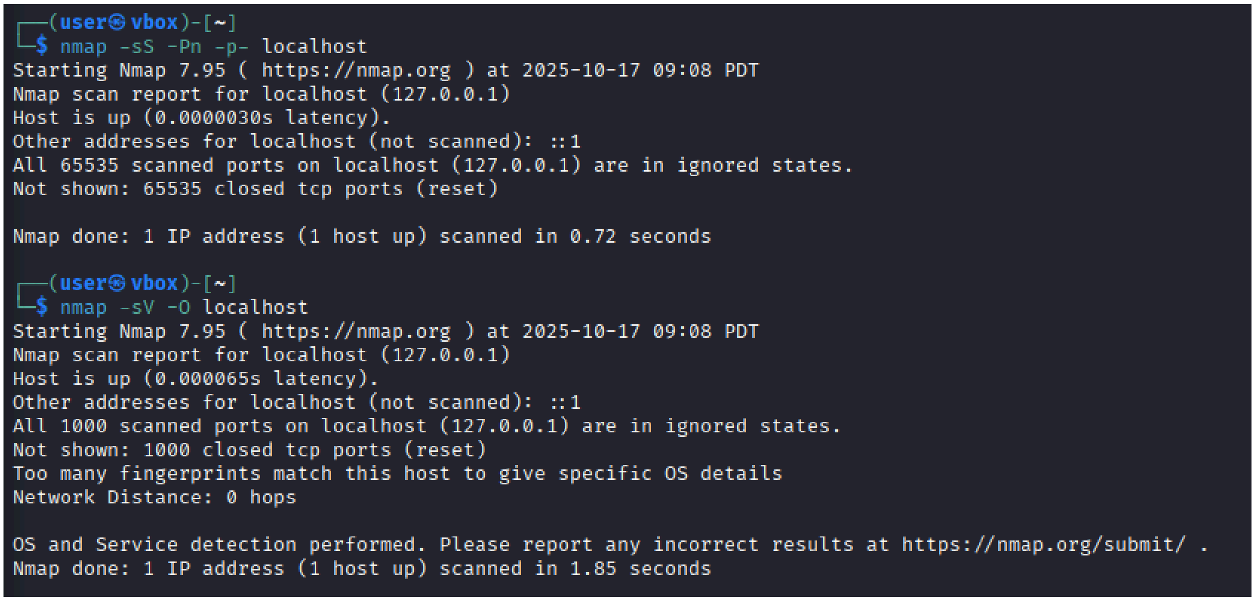
Part A

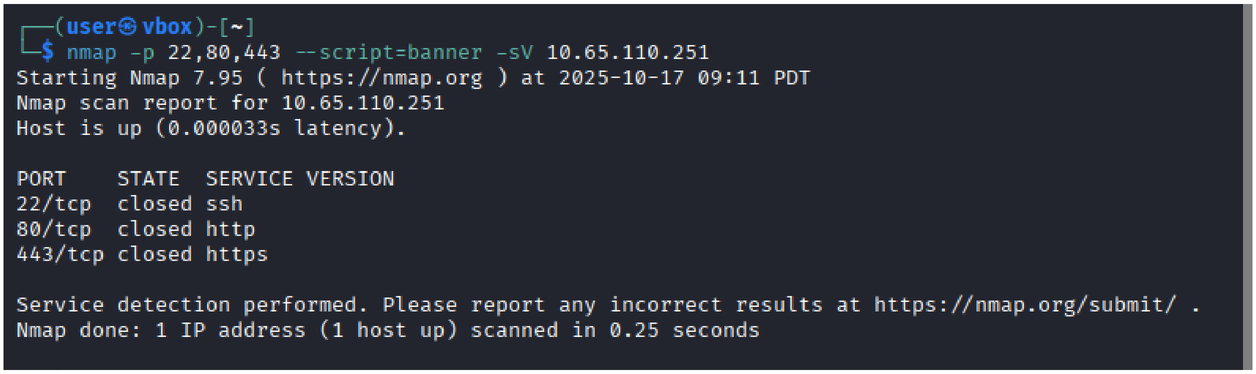


```
┌──(user㉿vbox)-[~]
└─$ sudo systemctl list-units --type=service --state=running
[sudo] password for user:
  UNIT                             LOAD   ACTIVE SUB     DESCRIPTION                                 >
  accounts-daemon.service          loaded active running Accounts Service
  colord.service                   loaded active running Manage, Install and Generate Color Profi>
  cron.service                     loaded active running Regular background program processing da>
  dbus.service                     loaded active running D-Bus System Message Bus
  getty@tty1.service               loaded active running Getty on tty1
  haveged.service                  loaded active running Entropy Daemon based on the HAVEGE algor>
  lightdm.service                  loaded active running Light Display Manager
  ModemManager.service             loaded active running Modem Manager
  NetworkManager.service           loaded active running Network Manager
  polkit.service                   loaded active running Authorization Manager
  rtkit-daemon.service             loaded active running RealtimeKit Scheduling Policy Service
  systemd-journald.service         loaded active running Journal Service
  systemd-logind.service           loaded active running User Login Management
  systemd-udevd.service            loaded active running Rule-based Manager for Device Events and>
  udisks2.service                  loaded active running Disk Manager
  upower.service                   loaded active running Daemon for power management
  user@1000.service                loaded active running User Manager for UID 1000
  virtualbox-guest-utils.service loaded active running Virtualbox guest utils

Legend: LOAD   → Reflects whether the unit definition was properly loaded.
        ACTIVE → The high-level unit activation state, i.e. generalization of SUB.
        SUB    → The low-level unit activation state, values depend on unit type.

18 loaded units listed.

┌──(user㉿vbox)-[~]
└─$ ss -tuln
Netid     State     Recv-Q     Send-Q         Local Address:Port          Peer Address:Port

┌──(user㉿vbox)-[~]
└─$ 
```

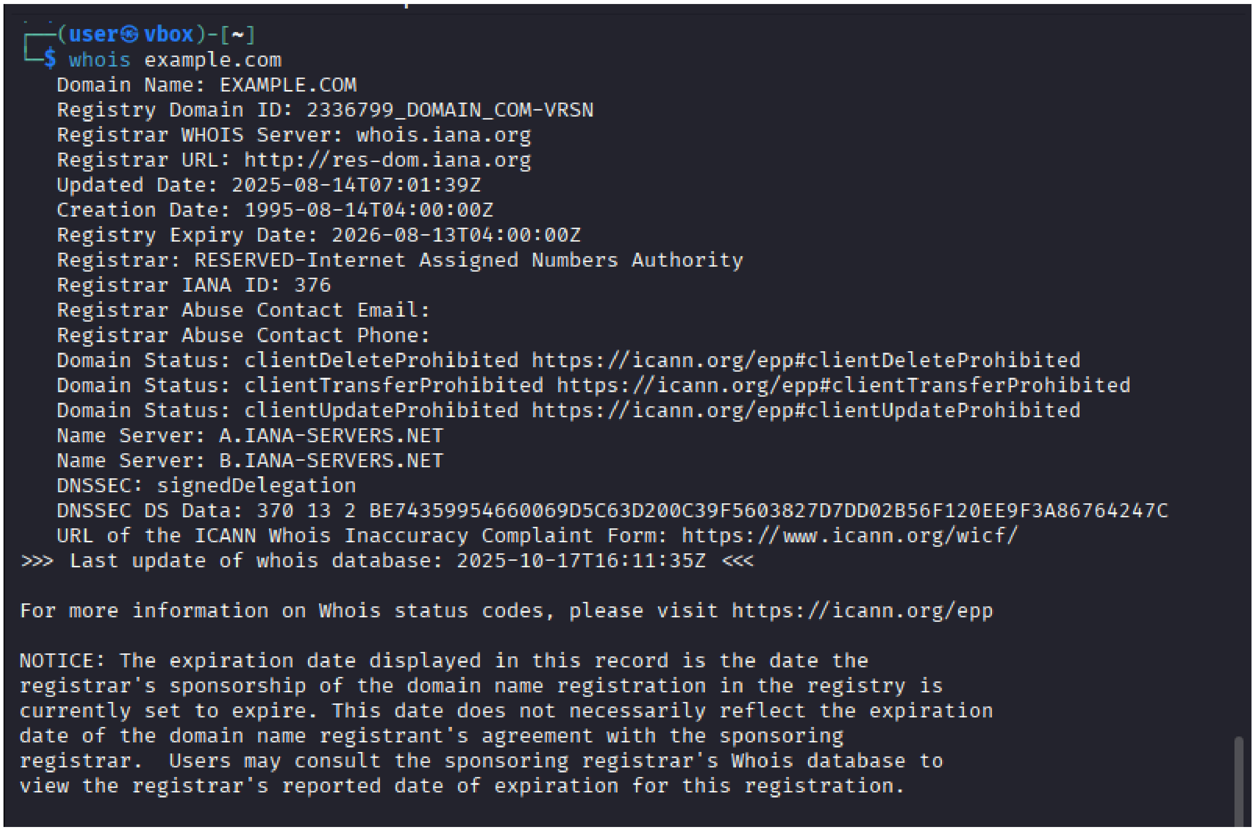
Part B



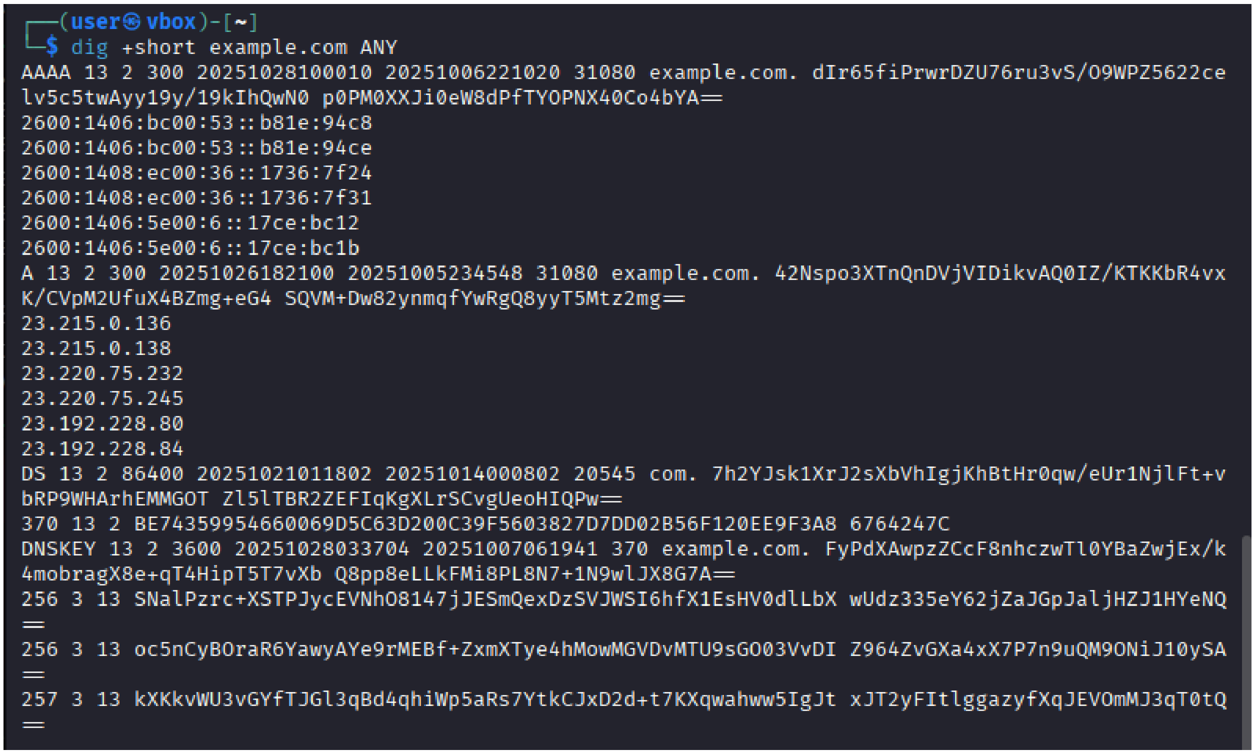
```
┌──(user㉿vbox)-[~]
└─$ nmap -sS -Pn -p- localhost
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-17 09:08 PDT
Nmap scan report for localhost (127.0.0.1)
Host is up (0.0000030s latency).
Other addresses for localhost (not scanned): ::1
All 65535 scanned ports on localhost (127.0.0.1) are in ignored states.
Not shown: 65535 closed tcp ports (reset)

Nmap done: 1 IP address (1 host up) scanned in 0.72 seconds

┌──(user㉿vbox)-[~]
└─$ nmap -sV -O localhost
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-17 09:08 PDT
Nmap scan report for localhost (127.0.0.1)
Host is up (0.000065s latency).
Other addresses for localhost (not scanned): ::1
All 1000 scanned ports on localhost (127.0.0.1) are in ignored states.
Not shown: 1000 closed tcp ports (reset)
Too many fingerprints match this host to give specific OS details
Network Distance: 0 hops

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 1.85 seconds
```



```
┌──(user㉿vbox)-[~]
└─$ nmap -p 22,80,443 --script=banner -sV 10.65.110.251
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-17 09:11 PDT
Nmap scan report for 10.65.110.251
Host is up (0.000033s latency).

PORT    STATE  SERVICE VERSION
22/tcp  closed ssh
80/tcp  closed http
443/tcp closed https

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 0.25 seconds
```



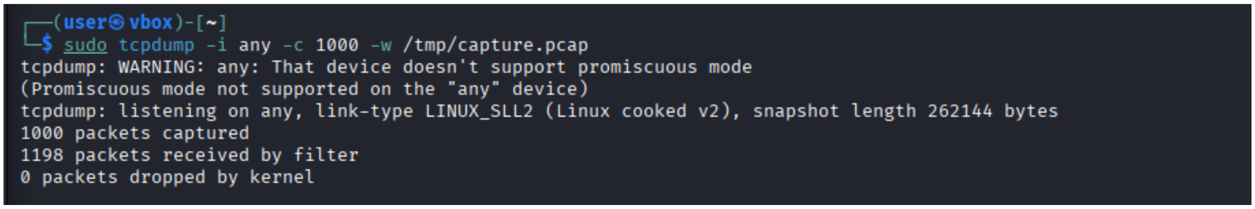
```
┌──(user㉿vbox)-[~]
└─$ whois example.com
   Domain Name: EXAMPLE.COM
   Registry Domain ID: 2336799_DOMAIN_COM-VRSN
   Registrar WHOIS Server: whois.iana.org
   Registrar URL: http://res-dom.iana.org
   Updated Date: 2025-08-14T07:01:39Z
   Creation Date: 1995-08-14T04:00:00Z
   Registry Expiry Date: 2026-08-13T04:00:00Z
   Registrar: RESERVED-Internet Assigned Numbers Authority
   Registrar IANA ID: 376
   Registrar Abuse Contact Email:
   Registrar Abuse Contact Phone:
   Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited
   Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
   Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited
   Name Server: A.IANA-SERVERS.NET
   Name Server: B.IANA-SERVERS.NET
   DNSSEC: signedDelegation
   DNSSEC DS Data: 370 13 2 BE74359954660069D5C63D200C39F5603827D7DD02B56F120EE9F3A86764247C
   URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
>>> Last update of whois database: 2025-10-17T16:11:35Z <<<

For more information on Whois status codes, please visit https://icann.org/epp

NOTICE: The expiration date displayed in this record is the date the
registrar's sponsorship of the domain name registration in the registry is
currently set to expire. This date does not necessarily reflect the expiration
date of the domain name registrant's agreement with the sponsoring
registrar.  Users may consult the sponsoring registrar's Whois database to
view the registrar's reported date of expiration for this registration.
```



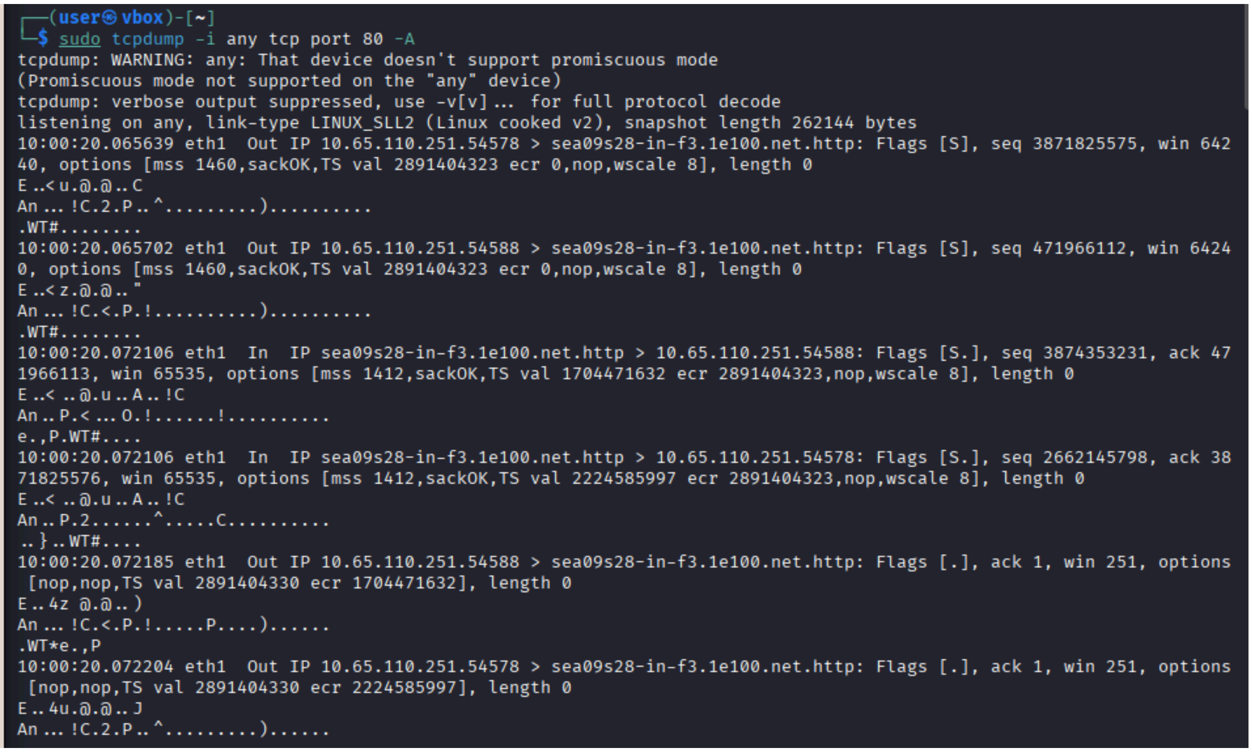
```
┌──(user㉿vbox)-[~]
└─$ dig +short example.com ANY
AAAA 13 2 300 20251028100010 20251006221020 31080 example.com. dIr65fiPrwrDZU76ru3vS/O9WPZ5622ce
lv5c5twAyy19y/19kIhQwN0 p0PM0XXJi0eW8dPfTYOPNX40Co4bYA==
2600:1406:bc00:53::b81e:94c8
2600:1406:bc00:53::b81e:94ce
2600:1408:ec00:36::1736:7f24
2600:1408:ec00:36::1736:7f31
2600:1406:5e00:6::17ce:bc12
2600:1406:5e00:6::17ce:bc1b
A 13 2 300 20251026182100 20251005234548 31080 example.com. 42Nspo3XTnQnDVjVIDikvAQ0IZ/KTKKbR4vx
K/CVpM2UfuX4BZmg+eG4 SQVM+Dw82ynmqfYwRgQ8yyT5Mtz2mg==
23.215.0.136
23.215.0.138
23.220.75.232
23.220.75.245
23.192.228.80
23.192.228.84
DS 13 2 86400 20251021011802 20251014000802 20545 com. 7h2YJsk1XrJ2sXbVhIgjKhBtHr0qw/eUr1NjlFt+v
bRP9WHArhEMMGOT Zl5lTBR2ZEFIqKgXLrSCvgUeoHIQPw==
370 13 2 BE74359954660069D5C63D200C39F5603827D7DD02B56F120EE9F3A8 6764247C
DNSKEY 13 2 3600 20251028033704 20251007061941 370 example.com. FyPdXAwpzZCcF8nhczwTl0YBaZwjEx/k
4mobragX8e+qT4HipT5T7vXb Q8pp8eLLkFMi8PL8N7+1N9wlJX8G7A==
256 3 13 SNalPzrc+XSTPJycEVNhO8147jJESmQexDzSVJWSI6hfX1EsHV0dlLbX wUdz335eY62jZaJGpJaljHZJ1HYeNQ
==
256 3 13 oc5nCyBOraR6YawyAYe9rMEBf+ZxmXTye4hMowMGVDvMTU9sGO03VvDI Z964ZvGXa4xX7P7n9uQM9ONiJ10ySA
==
257 3 13 kXKkvWU3vGYfTJGl3qBd4qhiWp5aRs7YtkCJxD2d+t7KXqwahww5IgJt xJT2yFItlggazyfXqJEVOmMJ3qT0tQ
==
```

All ports are closed, the OS details cannot be scanned as there are too many fingerprints

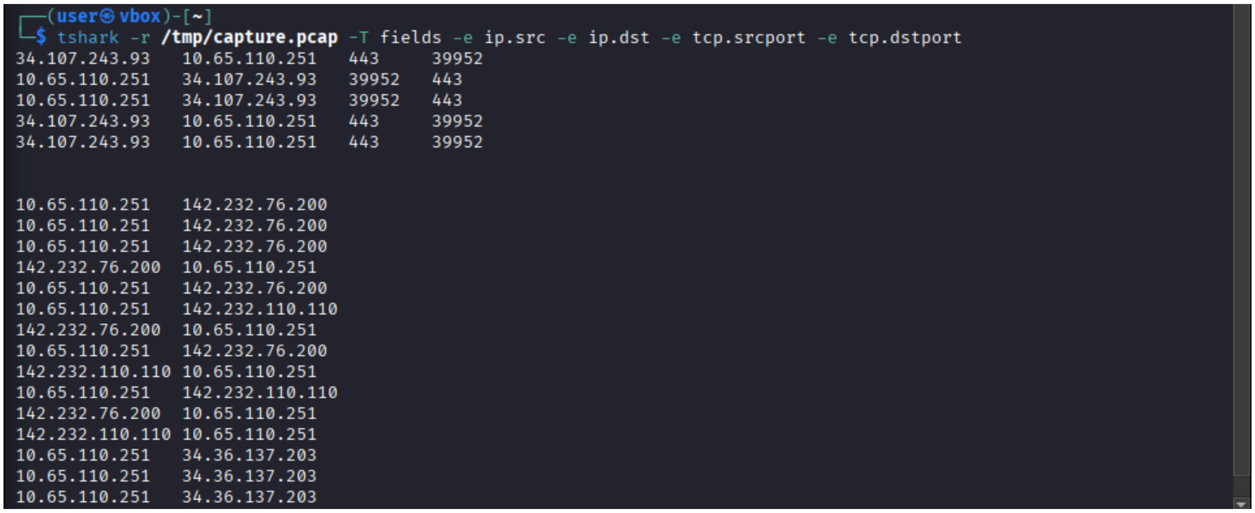
Part C



```
┌──(user㉿vbox)-[~]
└─$ sudo tcpdump -i any -c 1000 -w /tmp/capture.pcap
tcpdump: WARNING: any: That device doesn't support promiscuous mode
(Promiscuous mode not supported on the "any" device)
tcpdump: listening on any, link-type LINUX_SLL2 (Linux cooked v2), snapshot length 262144 bytes
1000 packets captured
1198 packets received by filter
0 packets dropped by kernel
```

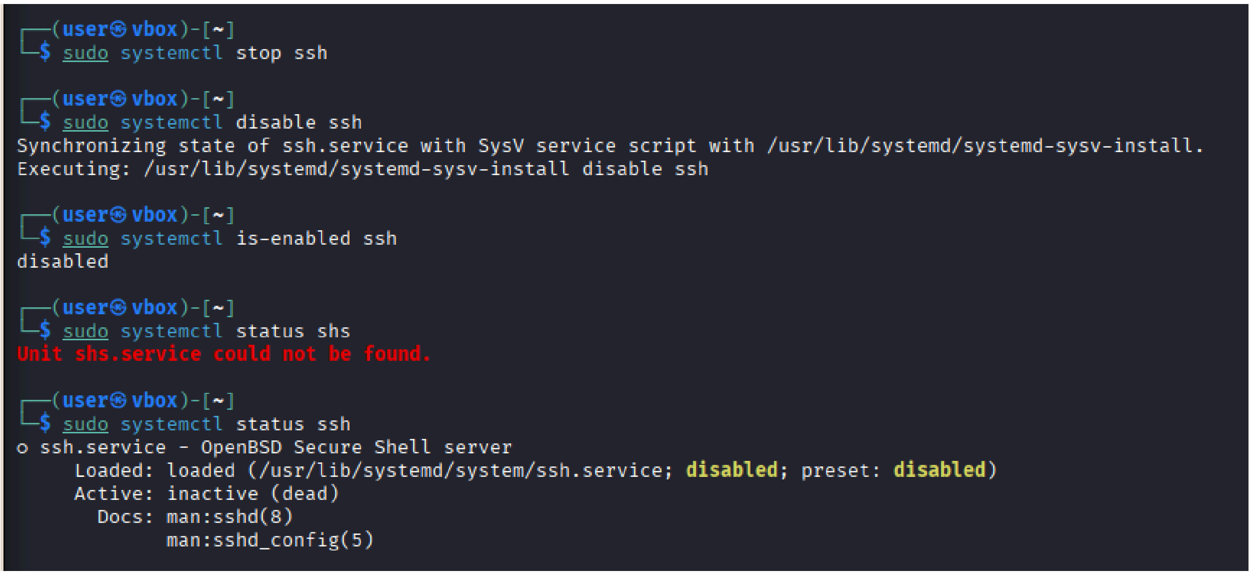


```
┌──(user㉿vbox)-[~]
└─$ sudo tcpdump -i any tcp port 80 -A
tcpdump: WARNING: any: That device doesn't support promiscuous mode
(Promiscuous mode not supported on the "any" device)
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on any, link-type LINUX_SLL2 (Linux cooked v2), snapshot length 262144 bytes
10:00:20.065639 eth1  Out IP 10.65.110.251.54578 > sea09s28-in-f3.1e100.net.http: Flags [S], seq 3871825575, win 642
40, options [mss 1460,sackOK,TS val 2891404323 ecr 0,nop,wscale 8], length 0
E..<u.@.@..C
An...!C.2.P..^.........)..........
.WT#........
10:00:20.065702 eth1  Out IP 10.65.110.251.54588 > sea09s28-in-f3.1e100.net.http: Flags [S], seq 471966112, win 6424
0, options [mss 1460,sackOK,TS val 2891404323 ecr 0,nop,wscale 8], length 0
E..<z.@.@.."
An...!C.<.P.!..........)..........
.WT#........
10:00:20.072106 eth1  In  IP sea09s28-in-f3.1e100.net.http > 10.65.110.251.54588: Flags [S.], seq 3874353231, ack 47
1966113, win 65535, options [mss 1412,sackOK,TS val 1704471632 ecr 2891404323,nop,wscale 8], length 0
E..<..@.u..A..!C
An..P.<...O.!......!..........
e.,P.WT#....
10:00:20.072106 eth1  In  IP sea09s28-in-f3.1e100.net.http > 10.65.110.251.54578: Flags [S.], seq 2662145798, ack 38
71825576, win 65535, options [mss 1412,sackOK,TS val 2224585997 ecr 2891404323,nop,wscale 8], length 0
E..<..@.u..A..!C
An..P.2......^.....C..........
..}..WT#....
10:00:20.072185 eth1  Out IP 10.65.110.251.54588 > sea09s28-in-f3.1e100.net.http: Flags [.], ack 1, win 251, options
 [nop,nop,TS val 2891404330 ecr 1704471632], length 0
E..4z @.@..)
An...!C.<.P.!.....P....)......
.WT*e.,P
10:00:20.072204 eth1  Out IP 10.65.110.251.54578 > sea09s28-in-f3.1e100.net.http: Flags [.], ack 1, win 251, options
 [nop,nop,TS val 2891404330 ecr 2224585997], length 0
E..4u.@.@..J
An...!C.2.P..^.........)......
```

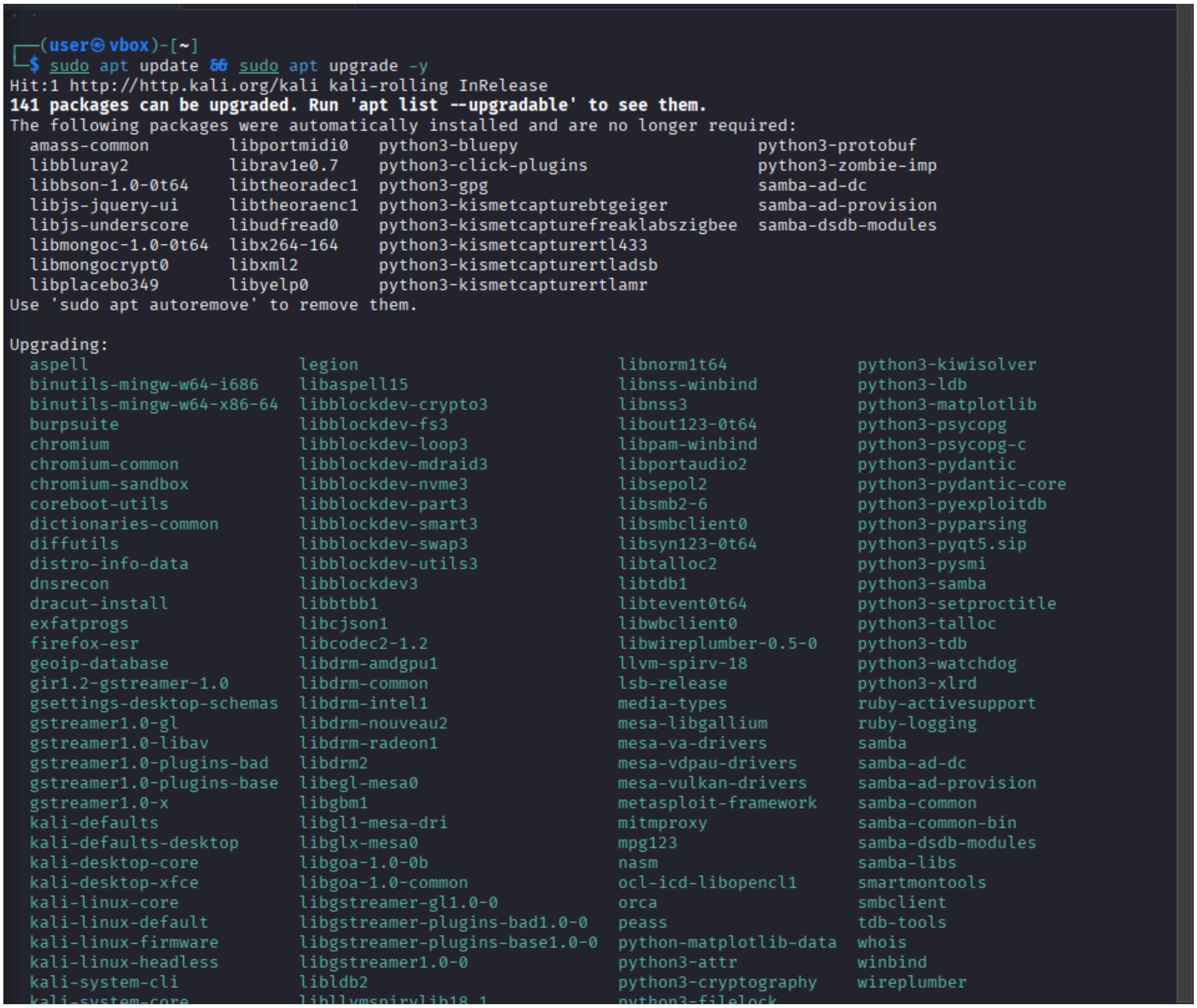


```
┌──(user㉿vbox)-[~]
└─$ tshark -r /tmp/capture.pcap -T fields -e ip.src -e ip.dst -e tcp.srcport -e tcp.dstport
34.107.243.93   10.65.110.251   443     39952
10.65.110.251   34.107.243.93   39952   443
10.65.110.251   34.107.243.93   39952   443
34.107.243.93   10.65.110.251   443     39952
34.107.243.93   10.65.110.251   443     39952


10.65.110.251   142.232.76.200
10.65.110.251   142.232.76.200
10.65.110.251   142.232.76.200
142.232.76.200  10.65.110.251
10.65.110.251   142.232.76.200
10.65.110.251   142.232.110.110
142.232.76.200  10.65.110.251
10.65.110.251   142.232.76.200
142.232.110.110 10.65.110.251
10.65.110.251   142.232.110.110
142.232.76.200  10.65.110.251
142.232.110.110 10.65.110.251
10.65.110.251   34.36.137.203
10.65.110.251   34.36.137.203
10.65.110.251   34.36.137.203
```

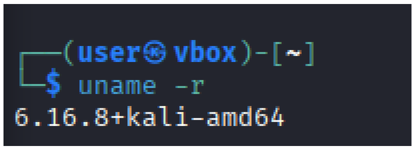
Part D



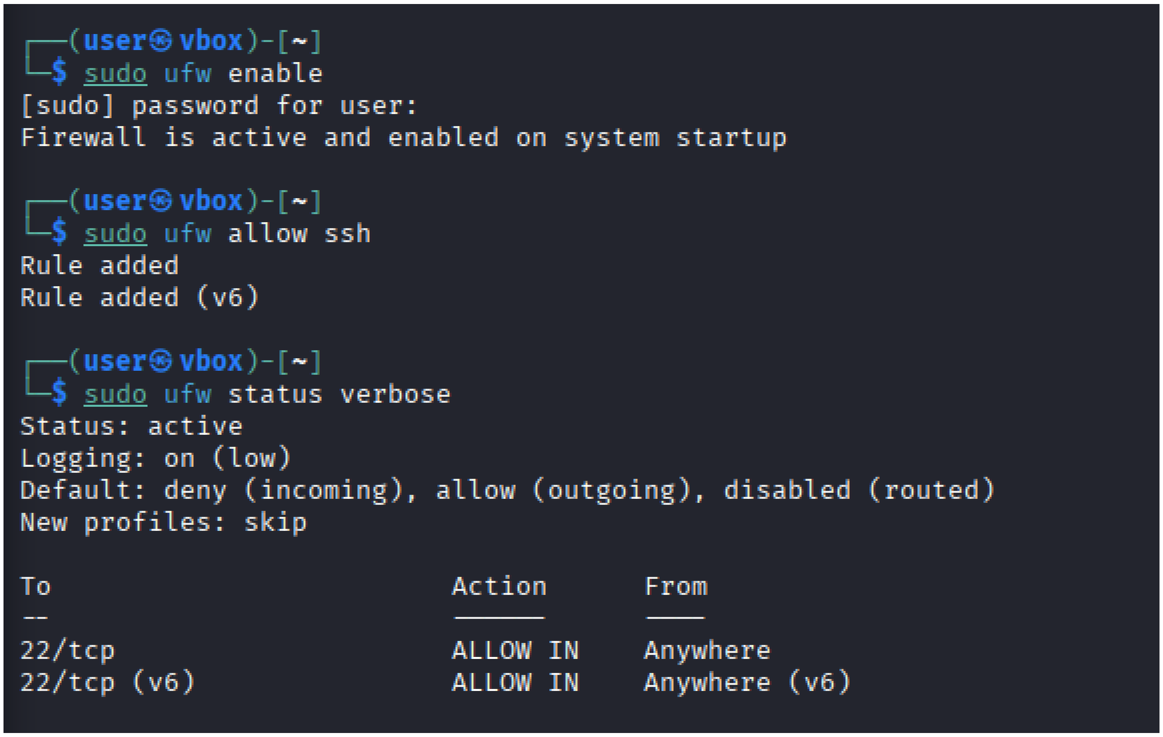
```
┌──(user㉿vbox)-[~]
└─$ sudo systemctl stop ssh

┌──(user㉿vbox)-[~]
└─$ sudo systemctl disable ssh
Synchronizing state of ssh.service with SysV service script with /usr/lib/systemd/systemd-sysv-install.
Executing: /usr/lib/systemd/systemd-sysv-install disable ssh

┌──(user㉿vbox)-[~]
└─$ sudo systemctl is-enabled ssh
disabled

┌──(user㉿vbox)-[~]
└─$ sudo systemctl status shs
Unit shs.service could not be found.

┌──(user㉿vbox)-[~]
└─$ sudo systemctl status ssh
○ ssh.service - OpenBSD Secure Shell server
     Loaded: loaded (/usr/lib/systemd/system/ssh.service; disabled; preset: disabled)
     Active: inactive (dead)
       Docs: man:sshd(8)
             man:sshd_config(5)
```



```
┌──(user㉿vbox)-[~]
└─$ sudo apt update && sudo apt upgrade -y
Hit:1 http://http.kali.org/kali kali-rolling InRelease
141 packages can be upgraded. Run 'apt list --upgradable' to see them.
The following packages were automatically installed and are no longer required:
  amass-common        libportmidi0   python3-bluepy                        python3-protobuf
  libbluray2          librav1e0.7    python3-click-plugins                 python3-zombie-imp
  libbson-1.0-0t64    libtheoradec1  python3-gpg                           samba-ad-dc
  libjs-jquery-ui     libtheoraenc1  python3-kismetcapturebtgeiger         samba-ad-provision
  libjs-underscore    libudfread0    python3-kismetcapturefreaklabszigbee  samba-dsdb-modules
  libmongoc-1.0-0t64  libx264-164    python3-kismetcapturertl433
  libmongocrypt0      libxml2        python3-kismetcapturertladsb
  libplacebo349       libyelp0       python3-kismetcapturertlamr
Use 'sudo apt autoremove' to remove them.

Upgrading:
  aspell                     legion                          libnorm1t64             python3-kiwisolver
  binutils-mingw-w64-i686    libaspell15                     libnss-winbind          python3-ldb
  binutils-mingw-w64-x86-64  libblockdev-crypto3             libnss3                 python3-matplotlib
  burpsuite                  libblockdev-fs3                 libout123-0t64          python3-psycopg
  chromium                   libblockdev-loop3               libpam-winbind          python3-psycopg-c
  chromium-common            libblockdev-mdraid3             libportaudio2           python3-pydantic
  chromium-sandbox           libblockdev-nvme3               libsepol2               python3-pydantic-core
  coreboot-utils             libblockdev-part3               libsmb2-6               python3-pyexploitdb
  dictionaries-common        libblockdev-smart3              libsmbclient0           python3-pyparsing
  diffutils                  libblockdev-swap3               libsyn123-0t64          python3-pyqt5.sip
  distro-info-data           libblockdev-utils3              libtalloc2              python3-pysmi
  dnsrecon                   libblockdev3                    libtdb1                 python3-samba
  dracut-install             libbtbb1                        libtevent0t64           python3-setproctitle
  exfatprogs                 libcjson1                       libwbclient0            python3-talloc
  firefox-esr                libcodec2-1.2                   libwireplumber-0.5-0    python3-tdb
  geoip-database             libdrm-amdgpu1                  llvm-spirv-18           python3-watchdog
  gir1.2-gstreamer-1.0       libdrm-common                   lsb-release             python3-xlrd
  gsettings-desktop-schemas  libdrm-intel1                   media-types             ruby-activesupport
  gstreamer1.0-gl            libdrm-nouveau2                 mesa-libgallium         ruby-logging
  gstreamer1.0-libav         libdrm-radeon1                  mesa-va-drivers         samba
  gstreamer1.0-plugins-bad   libdrm2                         mesa-vdpau-drivers      samba-ad-dc
  gstreamer1.0-plugins-base  libegl-mesa0                    mesa-vulkan-drivers     samba-ad-provision
  gstreamer1.0-x             libgbm1                         metasploit-framework    samba-common
  kali-defaults              libgl1-mesa-dri                 mitmproxy               samba-common-bin
  kali-defaults-desktop      libglx-mesa0                    mpg123                  samba-dsdb-modules
  kali-desktop-core          libgoa-1.0-0b                   nasm                    samba-libs
  kali-desktop-xfce          libgoa-1.0-common               ocl-icd-libopencl1      smartmontools
  kali-linux-core            libgstreamer-gl1.0-0            orca                    smbclient
  kali-linux-default         libgstreamer-plugins-bad1.0-0   peass                   tdb-tools
  kali-linux-firmware        libgstreamer-plugins-base1.0-0  python-matplotlib-data  whois
  kali-linux-headless        libgstreamer1.0-0               python3-attr            winbind
  kali-system-cli            libldb2                         python3-cryptography    wireplumber
  kali-system-core           libllvmspirvlib18.1             python3-filelock
```

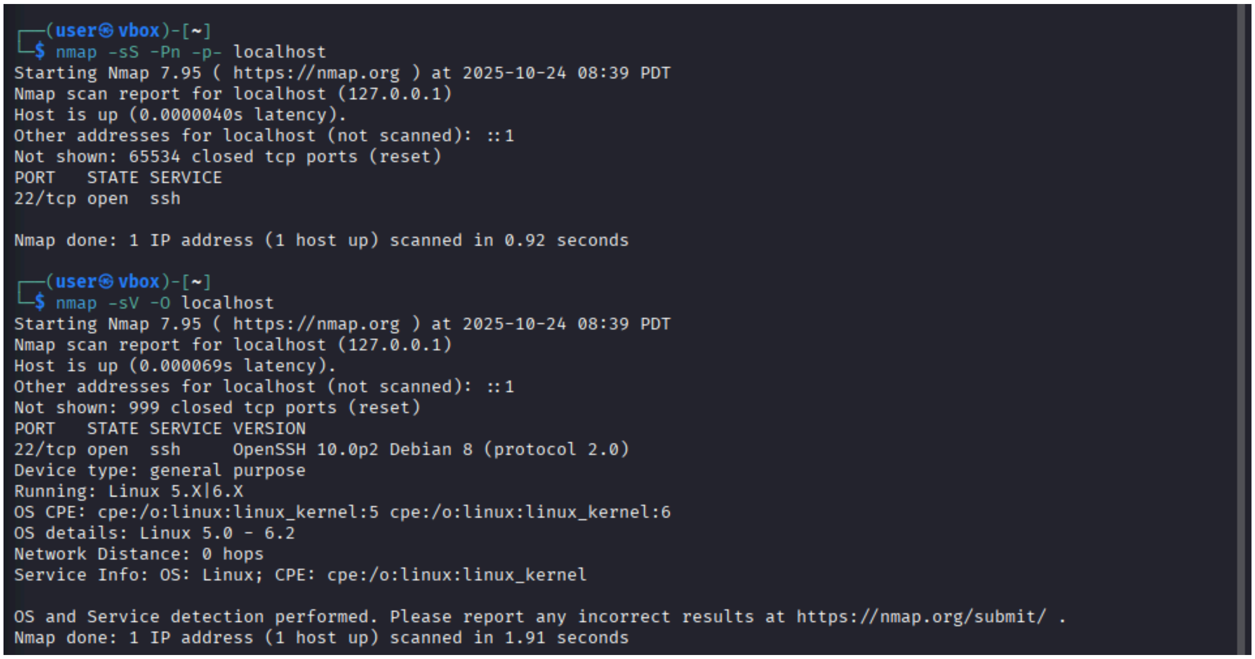


```
┌──(user㉿vbox)-[~]
└─$ uname -r
6.16.8+kali-amd64
```



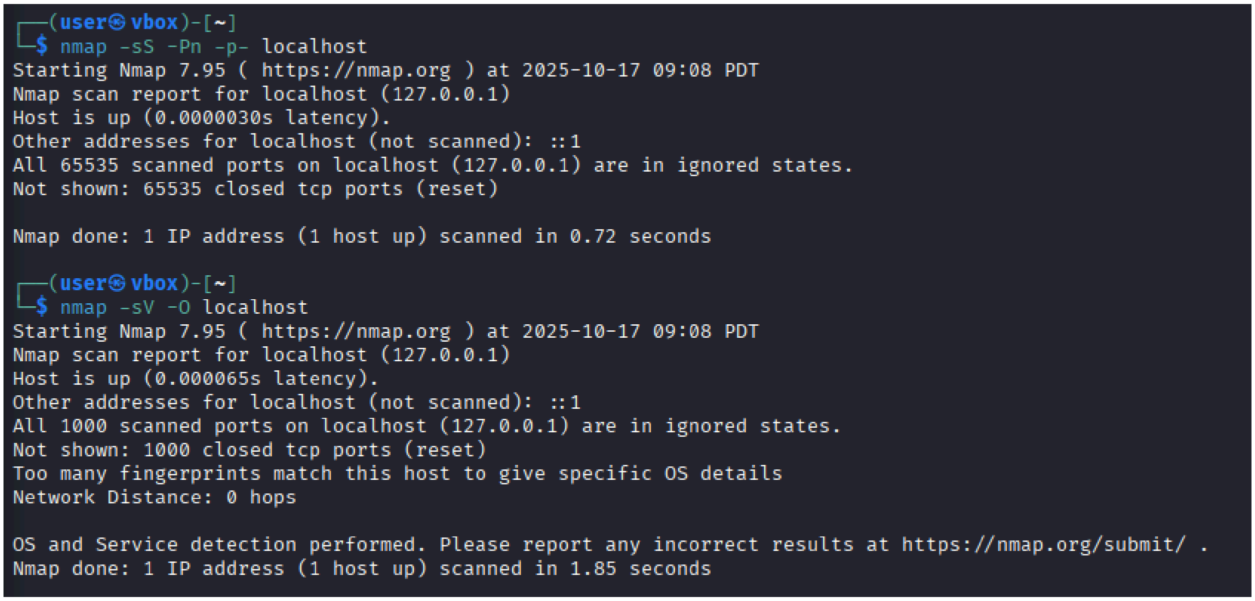
```
┌──(user㉿vbox)-[~]
└─$ sudo ufw enable
[sudo] password for user:
Firewall is active and enabled on system startup

┌──(user㉿vbox)-[~]
└─$ sudo ufw allow ssh
Rule added
Rule added (v6)

┌──(user㉿vbox)-[~]
└─$ sudo ufw status verbose
Status: active
Logging: on (low)
Default: deny (incoming), allow (outgoing), disabled (routed)
New profiles: skip

To                         Action      From
--                         ------      ----
22/tcp                     ALLOW IN    Anywhere
22/tcp (v6)                ALLOW IN    Anywhere (v6)
```

Part E



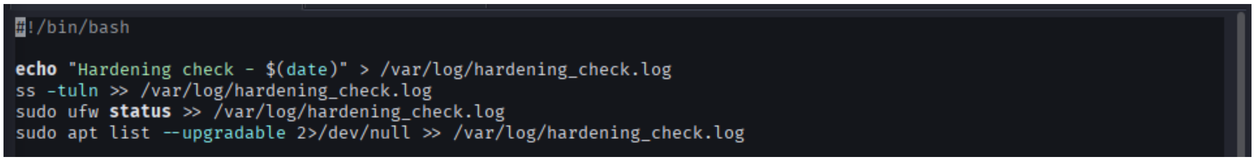
```
┌──(user㉿vbox)-[~]
└─$ nmap -sS -Pn -p- localhost
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-24 08:39 PDT
Nmap scan report for localhost (127.0.0.1)
Host is up (0.0000040s latency).
Other addresses for localhost (not scanned): ::1
Not shown: 65534 closed tcp ports (reset)
PORT   STATE SERVICE
22/tcp open  ssh

Nmap done: 1 IP address (1 host up) scanned in 0.92 seconds

┌──(user㉿vbox)-[~]
└─$ nmap -sV -O localhost
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-24 08:39 PDT
Nmap scan report for localhost (127.0.0.1)
Host is up (0.000069s latency).
Other addresses for localhost (not scanned): ::1
Not shown: 999 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 10.0p2 Debian 8 (protocol 2.0)
Device type: general purpose
Running: Linux 5.X|6.X
OS CPE: cpe:/o:linux:linux_kernel:5 cpe:/o:linux:linux_kernel:6
OS details: Linux 5.0 - 6.2
Network Distance: 0 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 1.91 seconds
```

Before:

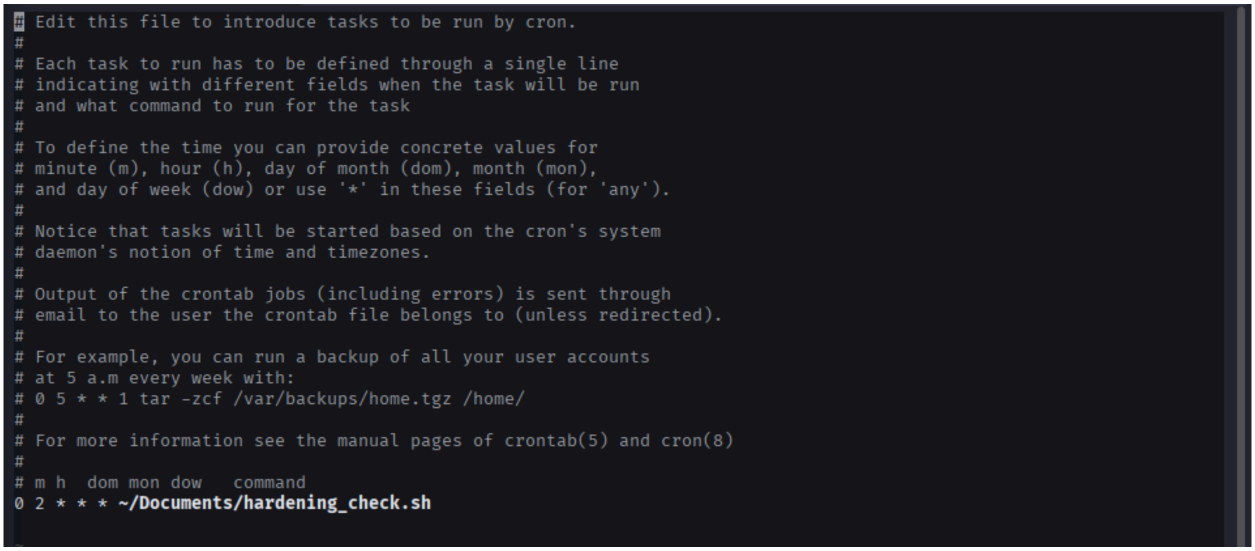


```
┌──(user㉿vbox)-[~]
└─$ nmap -sS -Pn -p- localhost
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-17 09:08 PDT
Nmap scan report for localhost (127.0.0.1)
Host is up (0.0000030s latency).
Other addresses for localhost (not scanned): ::1
All 65535 scanned ports on localhost (127.0.0.1) are in ignored states.
Not shown: 65535 closed tcp ports (reset)

Nmap done: 1 IP address (1 host up) scanned in 0.72 seconds

┌──(user㉿vbox)-[~]
└─$ nmap -sV -O localhost
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-17 09:08 PDT
Nmap scan report for localhost (127.0.0.1)
Host is up (0.000065s latency).
Other addresses for localhost (not scanned): ::1
All 1000 scanned ports on localhost (127.0.0.1) are in ignored states.
Not shown: 1000 closed tcp ports (reset)
Too many fingerprints match this host to give specific OS details
Network Distance: 0 hops

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 1.85 seconds
```

Part F



```
#!/bin/bash

echo "Hardening check - $(date)" > /var/log/hardening_check.log
ss -tuln >> /var/log/hardening_check.log
sudo ufw status >> /var/log/hardening_check.log
sudo apt list --upgradable 2>/dev/null >> /var/log/hardening_check.log
```



```
# Edit this file to introduce tasks to be run by cron.
#
# Each task to run has to be defined through a single line
# indicating with different fields when the task will be run
# and what command to run for the task
#
# To define the time you can provide concrete values for
# minute (m), hour (h), day of month (dom), month (mon),
# and day of week (dow) or use '*' in these fields (for 'any').
#
# Notice that tasks will be started based on the cron's system
# daemon's notion of time and timezones.
#
# Output of the crontab jobs (including errors) is sent through
# email to the user the crontab file belongs to (unless redirected).
#
# For example, you can run a backup of all your user accounts
# at 5 a.m every week with:
# 0 5 * * 1 tar -zcf /var/backups/home.tgz /home/
#
# For more information see the manual pages of crontab(5) and cron(8)
#
# m h  dom mon dow   command
0 2 * * * ~/Documents/hardening_check.sh
```