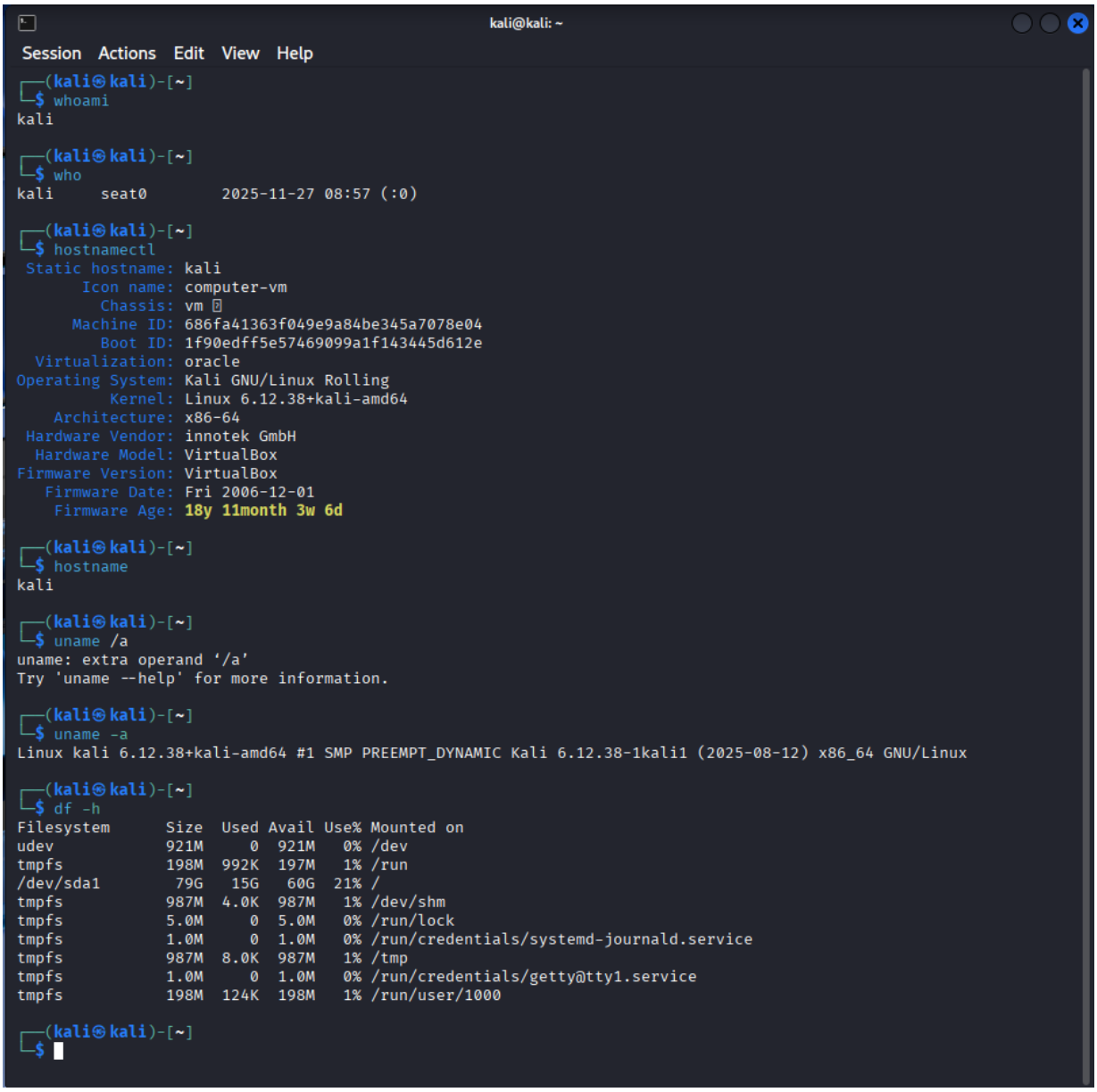
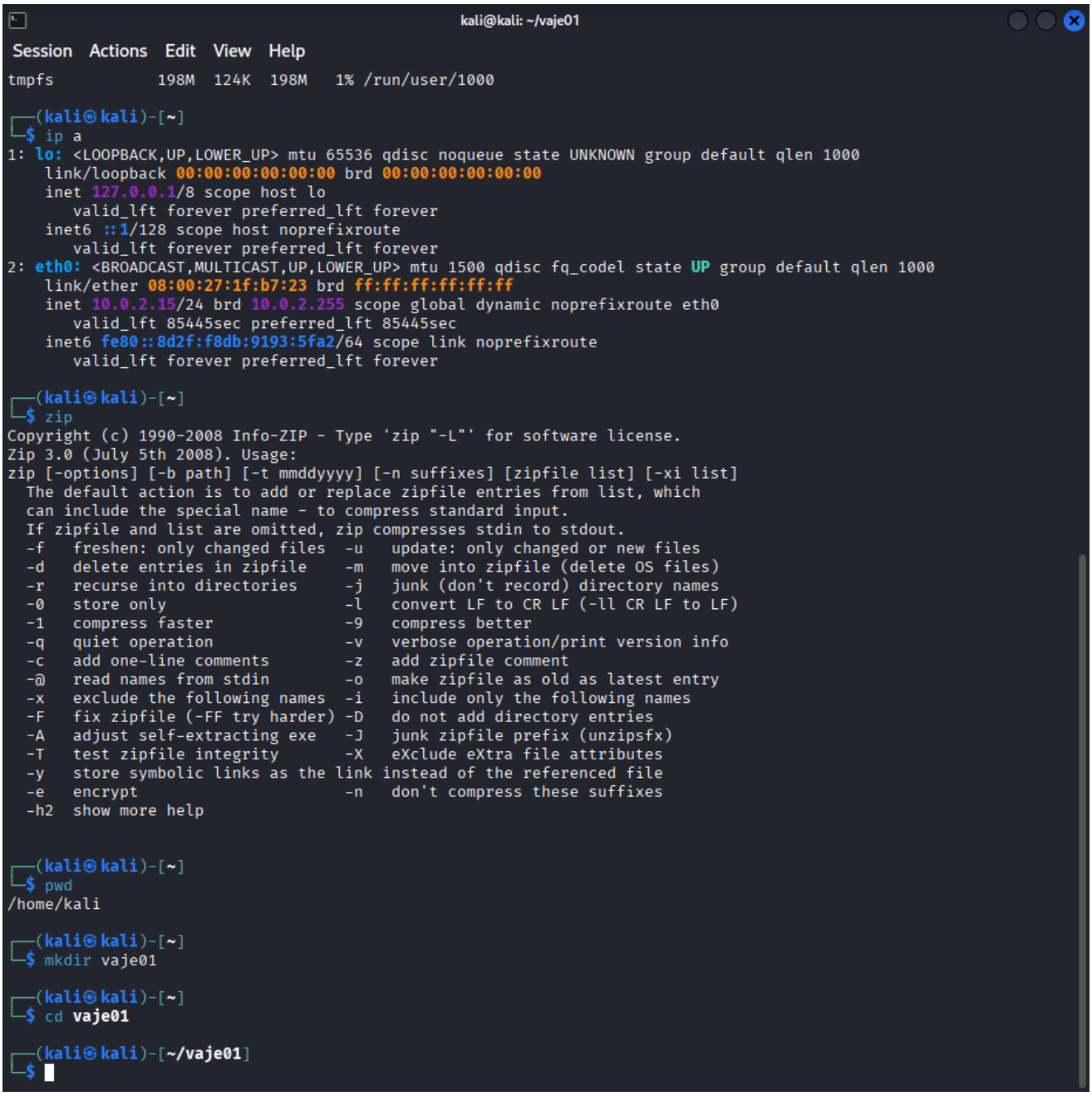
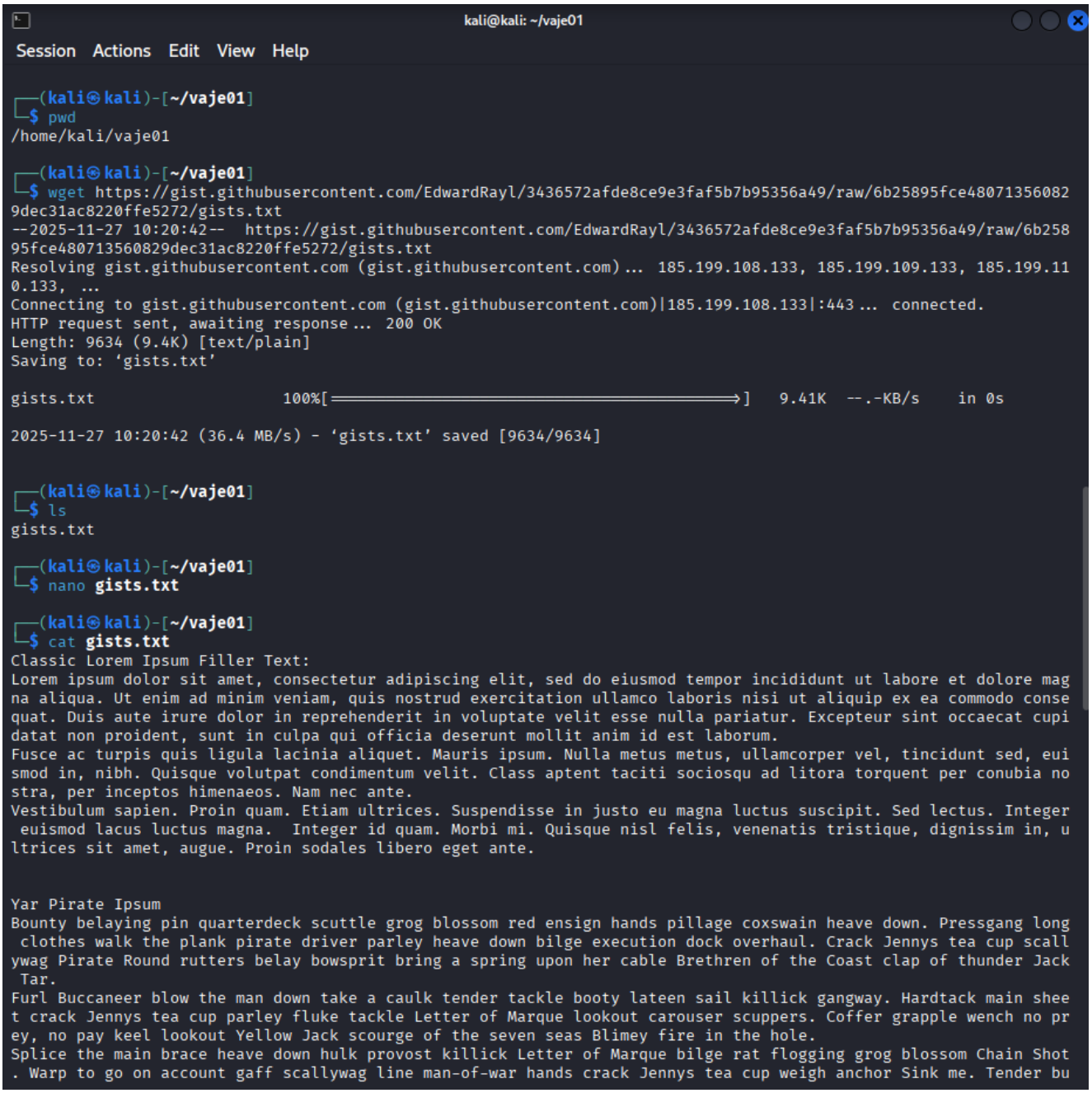
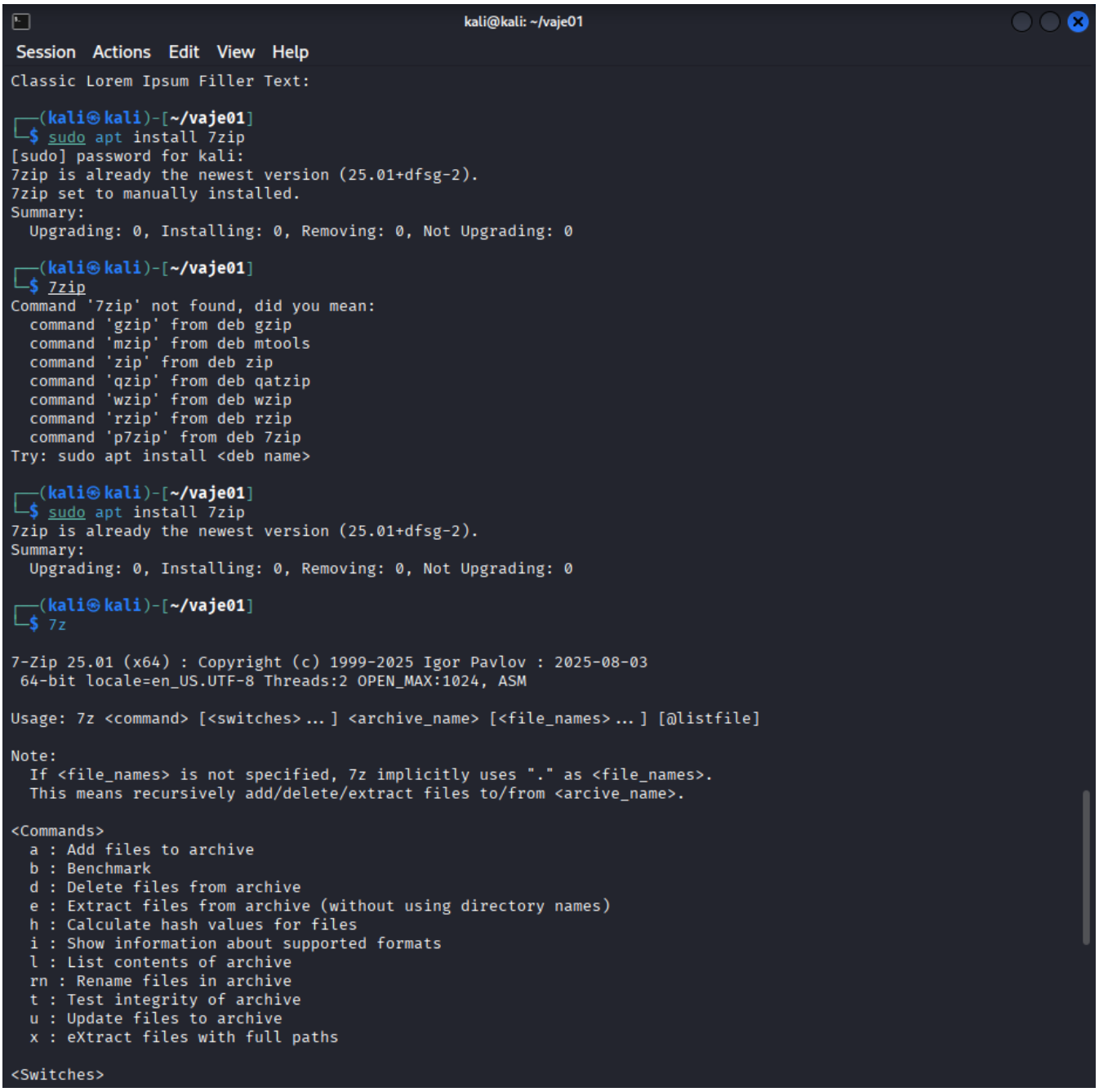
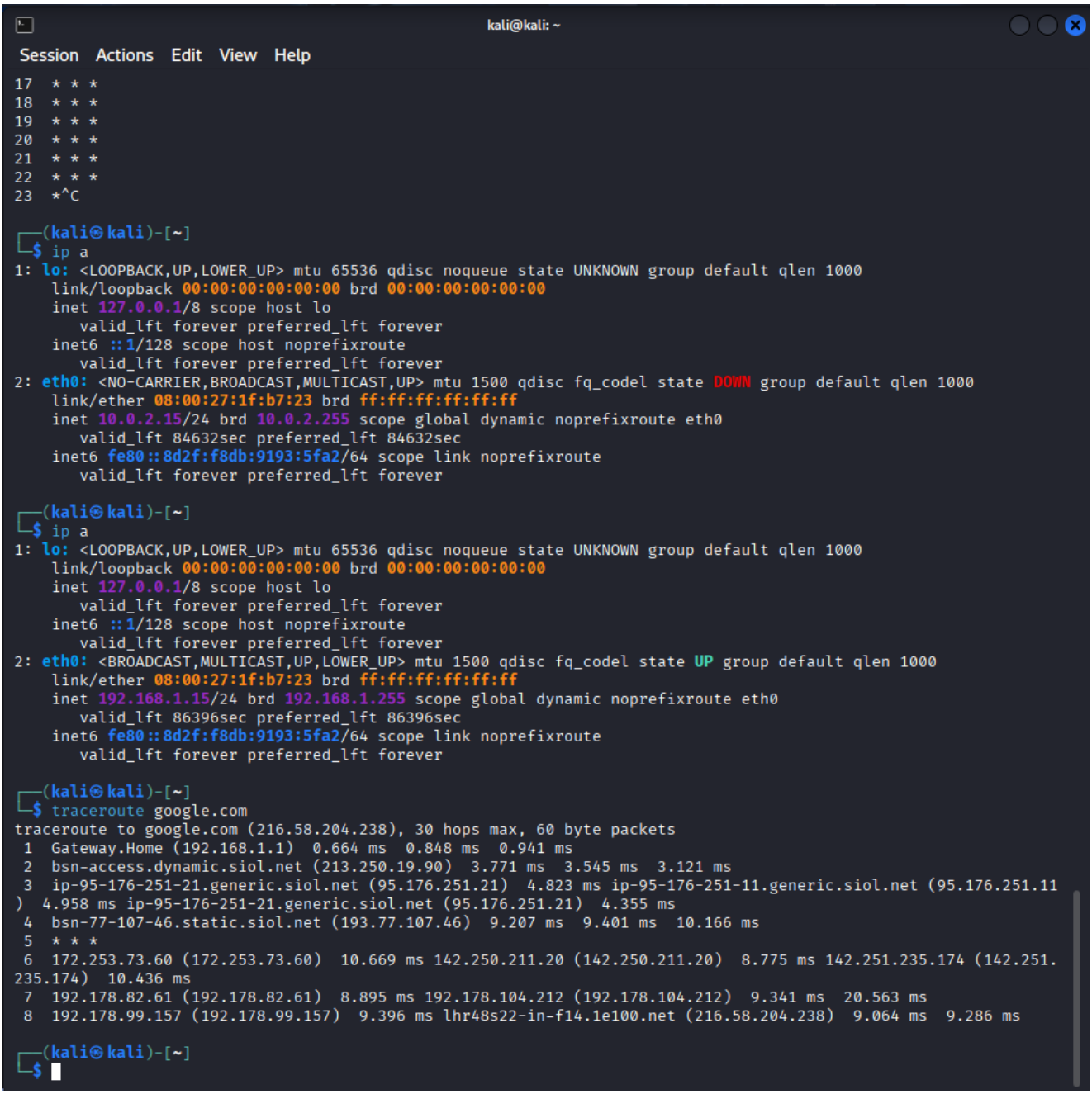
Vaje 01


kali@kali: ~
Session Actions Edit View Help
(kali㉿kali)-[~]
$ whoami
kali
(kali㉿kali)-[~]
$ who
kali seat0 2025-11-27 08:57 (:0)
(kali㉿kali)-[~]
$ hostnamectl
Static hostname: kali
Icon name: computer-vm
Chassis: vm
Machine ID: 686fa41363f049e9a84be345a7078e04
Boot ID: 1f90edff5e57469099a1f143445d612e
Virtualization: oracle
Operating System: Kali GNU/Linux Rolling
Kernel: Linux 6.12.38+kali-amd64
Architecture: x86-64
Hardware Vendor: innotek GmbH
Hardware Model: VirtualBox
Firmware Version: VirtualBox
Firmware Date: Fri 2006-12-01
Firmware Age: 18y 11month 3w 6d
(kali㉿kali)-[~]
$ hostname
kali
(kali㉿kali)-[~]
$ uname /a
uname: extra operand '/a'
Try 'uname --help' for more information.
(kali㉿kali)-[~]
$ uname -a
Linux kali 6.12.38+kali-amd64 #1 SMP PREEMPT_DYNAMIC Kali 6.12.38-1kali1 (2025-08-12) x86_64 GNU/Linux
(kali㉿kali)-[~]
$ df -h
Filesystem Size Used Avail Use% Mounted on
udev 921M 0 921M 0% /dev
tmpfs 198M 992K 197M 1% /run
/dev/sda1 79G 15G 60G 21% /
tmpfs 987M 4.0K 987M 1% /dev/shm
tmpfs 5.0M 0 5.0M 0% /run/lock
tmpfs 1.0M 0 1.0M 0% /run/credentials/systemd-journald.service
tmpfs 987M 8.0K 987M 1% /tmp
tmpfs 1.0M 0 1.0M 0% /run/credentials/getty@tty1.service
tmpfs 198M 124K 198M 1% /run/user/1000
(kali㉿kali)-[~]
$

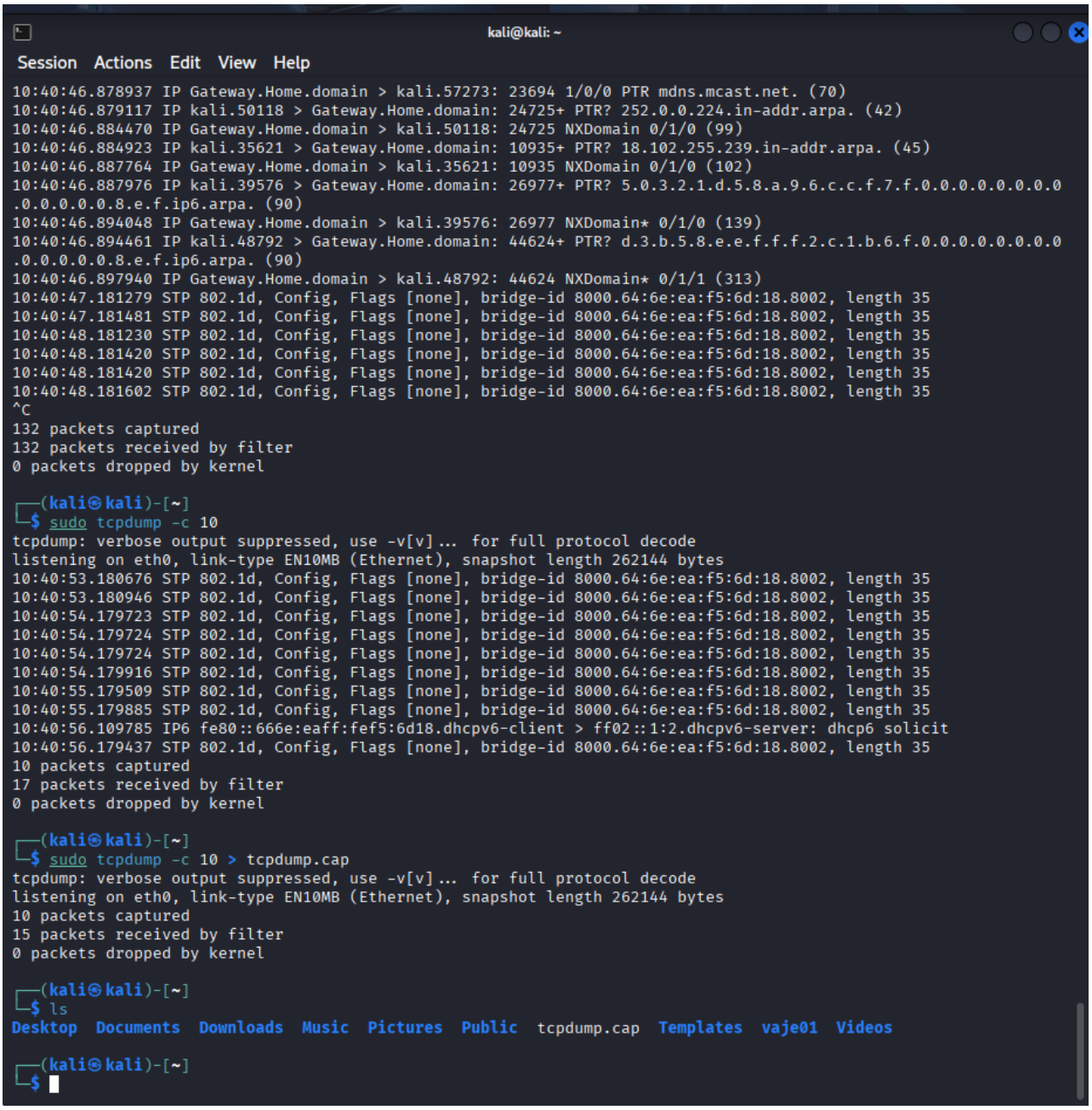

kali@kali: ~/vaje01
Session Actions Edit View Help
tmpfs 198M 124K 198M 1% /run/user/1000
(kali㉿kali)-[~]
$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
inet 127.0.0.1/8 scope host lo
valid_lft forever preferred_lft forever
inet6 ::1/128 scope host noprefixroute
valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
link/ether 08:00:27:1f:b7:23 brd ff:ff:ff:ff:ff:ff
inet 10.0.2.15/24 brd 10.0.2.255 scope global dynamic noprefixroute eth0
valid_lft 85445sec preferred_lft 85445sec
inet6 fe80::8d2f:f8db:9193:5fa2/64 scope link noprefixroute
valid_lft forever preferred_lft forever
(kali㉿kali)-[~]
$ zip
Copyright (c) 1990-2008 Info-ZIP - Type 'zip "-L"' for software license.
Zip 3.0 (July 5th 2008). Usage:
zip [-options] [-b path] [-t mmddyyyy] [-n suffixes] [zipfile list] [-xi list]
The default action is to add or replace zipfile entries from list, which
can include the special name - to compress standard input.
If zipfile and list are omitted, zip compresses stdin to stdout.
-f freshen: only changed files -u update: only changed or new files
-d delete entries in zipfile -m move into zipfile (delete OS files)
-r recurse into directories -j junk (don't record) directory names
-0 store only -l convert LF to CR LF (-ll CR LF to LF)
-1 compress faster -9 compress better
-q quiet operation -v verbose operation/print version info
-c add one-line comments -z add zipfile comment
-@ read names from stdin -o make zipfile as old as latest entry
-x exclude the following names -i include only the following names
-F fix zipfile (-FF try harder) -D do not add directory entries
-A adjust self-extracting exe -J junk zipfile prefix (unzipsfx)
-T test zipfile integrity -X eXclude eXtra file attributes
-y store symbolic links as the link instead of the referenced file
-e encrypt -n don't compress these suffixes
-h2 show more help
(kali㉿kali)-[~]
$ pwd
/home/kali
(kali㉿kali)-[~]
$ mkdir vaje01
(kali㉿kali)-[~]
$ cd vaje01
(kali㉿kali)-[~/vaje01]
$

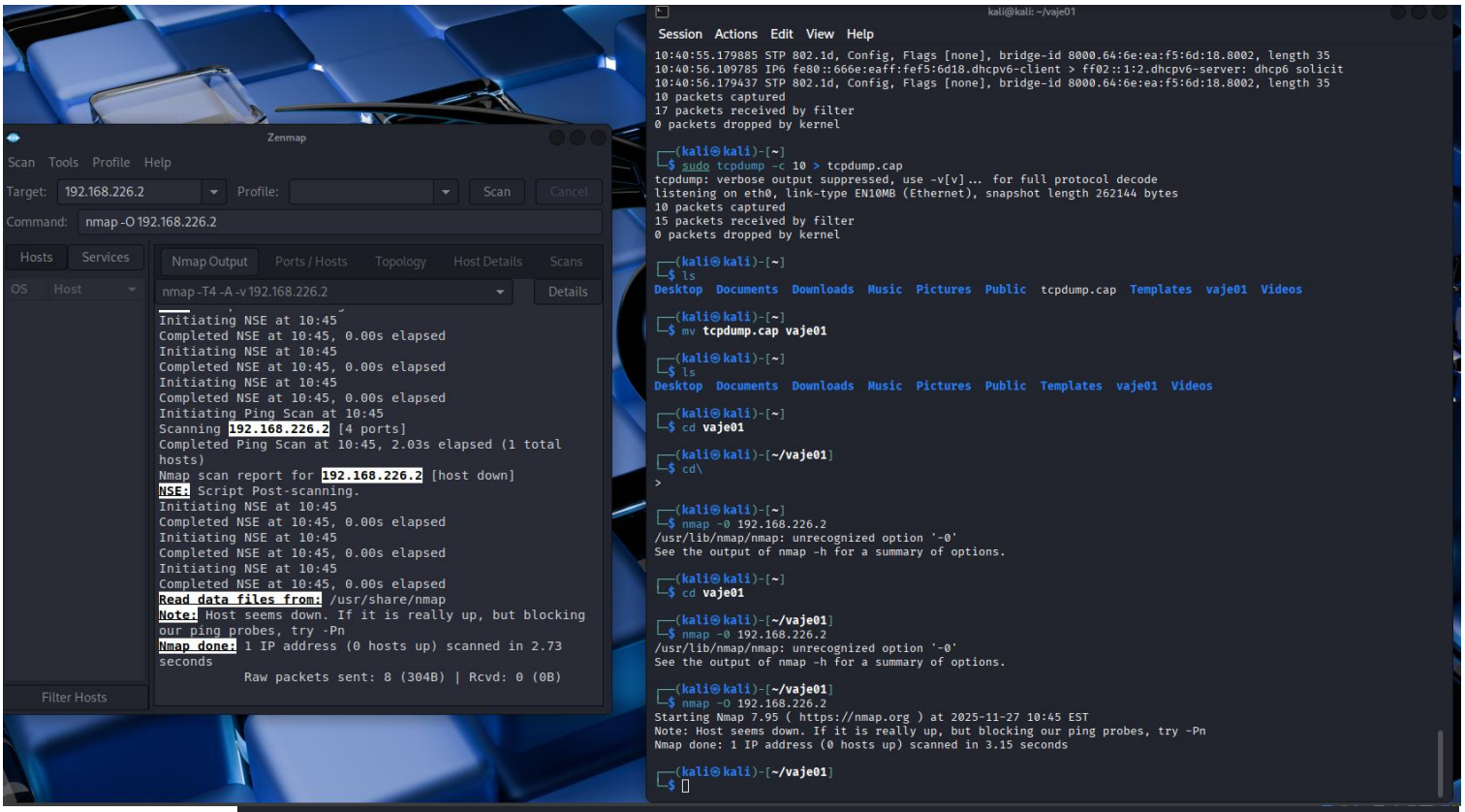

kali@kali: ~/vaje01
Session Actions Edit View Help
┌──(kali㉿kali)-[~/vaje01]
└─$ pwd
/home/kali/vaje01
┌──(kali㉿kali)-[~/vaje01]
└─$ wget https://gist.githubusercontent.com/EdwardRayl/3436572afde8ce9e3faf5b7b95356a49/raw/6b25895fce480713560829dec31ac8220ffe5272/gists.txt
--2025-11-27 10:20:42-- https://gist.githubusercontent.com/EdwardRayl/3436572afde8ce9e3faf5b7b95356a49/raw/6b25895fce480713560829dec31ac8220ffe5272/gists.txt
Resolving gist.githubusercontent.com (gist.githubusercontent.com)... 185.199.108.133, 185.199.109.133, 185.199.110.133, ...
Connecting to gist.githubusercontent.com (gist.githubusercontent.com)|185.199.108.133|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 9634 (9.4K) [text/plain]
Saving to: 'gists.txt'
gists.txt 100%[==========>] 9.41K --.-KB/s in 0s
2025-11-27 10:20:42 (36.4 MB/s) - 'gists.txt' saved [9634/9634]
┌──(kali㉿kali)-[~/vaje01]
└─$ ls
gists.txt
┌──(kali㉿kali)-[~/vaje01]
└─$ nano gists.txt
┌──(kali㉿kali)-[~/vaje01]
└─$ cat gists.txt
Classic Lorem Ipsum Filler Text:
Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat. Duis aute irure dolor in reprehenderit in voluptate velit esse nulla pariatur. Excepteur sint occaecat cupidatat non proident, sunt in culpa qui officia deserunt mollit anim id est laborum.
Fusce ac turpis quis ligula lacinia aliquet. Mauris ipsum. Nulla metus metus, ullamcorper vel, tincidunt sed, euismod in, nibh. Quisque volutpat condimentum velit. Class aptent taciti sociosqu ad litora torquent per conubia nostra, per inceptos himenaeos. Nam nec ante.
Vestibulum sapien. Proin quam. Etiam ultrices. Suspendisse in justo eu magna luctus suscipit. Sed lectus. Integer euismod lacus luctus magna. Integer id quam. Morbi mi. Quisque nisl felis, venenatis tristique, dignissim in, ultrices sit amet, augue. Proin sodales libero eget ante.
Yar Pirate Ipsum
Bounty belaying pin quarterdeck scuttle grog blossom red ensign hands pillage coxswain heave down. Pressgang long clothes walk the plank pirate driver parley heave down bilge execution dock overhaul. Crack Jennys tea cup scallywag Pirate Round rutters belay bowsprit bring a spring upon her cable Brethren of the Coast clap of thunder Jack Tar.
Furl Buccaneer blow the man down take a caulk tender tackle booty lateen sail killick gangway. Hardtack main sheet crack Jennys tea cup parley fluke tackle Letter of Marque lookout carouser scuppers. Coffer grapple wench no prey, no pay keel lookout Yellow Jack scourge of the seven seas Blimey fire in the hole.
Splice the main brace heave down hulk provost killick Letter of Marque bilge rat flogging grog blossom Chain Shot. Warp to go on account gaff scallywag line man-of-war hands crack Jennys tea cup weigh anchor Sink me. Tender bu


kali@kali: ~/vaje01
Session Actions Edit View Help
Classic Lorem Ipsum Filler Text:
┌──(kali㉿kali)-[~/vaje01]
└─$ sudo apt install 7zip
[sudo] password for kali:
7zip is already the newest version (25.01+dfsg-2).
7zip set to manually installed.
Summary:
Upgrading: 0, Installing: 0, Removing: 0, Not Upgrading: 0
┌──(kali㉿kali)-[~/vaje01]
└─$ 7zip
Command '7zip' not found, did you mean:
command 'gzip' from deb gzip
command 'mzip' from deb mtools
command 'zip' from deb zip
command 'qzip' from deb qatzip
command 'wzip' from deb wzip
command 'rzip' from deb rzip
command 'p7zip' from deb 7zip
Try: sudo apt install <deb name>
┌──(kali㉿kali)-[~/vaje01]
└─$ sudo apt install 7zip
7zip is already the newest version (25.01+dfsg-2).
Summary:
Upgrading: 0, Installing: 0, Removing: 0, Not Upgrading: 0
┌──(kali㉿kali)-[~/vaje01]
└─$ 7z
7-Zip 25.01 (x64) : Copyright (c) 1999-2025 Igor Pavlov : 2025-08-03
64-bit locale=en_US.UTF-8 Threads:2 OPEN_MAX:1024, ASM
Usage: 7z <command> [<switches>...] <archive_name> [<file_names>...] [@listfile]
Note:
If <file_names> is not specified, 7z implicitly uses "." as <file_names>.
This means recursively add/delete/extract files to/from <arcive_name>.
<Commands>
a : Add files to archive
b : Benchmark
d : Delete files from archive
e : Extract files from archive (without using directory names)
h : Calculate hash values for files
i : Show information about supported formats
l : List contents of archive
rn : Rename files in archive
t : Test integrity of archive
u : Update files to archive
x : eXtract files with full paths
<Switches>


kali@kali: ~
Session Actions Edit View Help
17 * * *
18 * * *
19 * * *
20 * * *
21 * * *
22 * * *
23 *^C
┌──(kali㉿kali)-[~]
└─$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
inet 127.0.0.1/8 scope host lo
valid_lft forever preferred_lft forever
inet6 ::1/128 scope host noprefixroute
valid_lft forever preferred_lft forever
2: eth0: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc fq_codel state DOWN group default qlen 1000
link/ether 08:00:27:1f:b7:23 brd ff:ff:ff:ff:ff:ff
inet 10.0.2.15/24 brd 10.0.2.255 scope global dynamic noprefixroute eth0
valid_lft 84632sec preferred_lft 84632sec
inet6 fe80::8d2f:f8db:9193:5fa2/64 scope link noprefixroute
valid_lft forever preferred_lft forever
┌──(kali㉿kali)-[~]
└─$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
inet 127.0.0.1/8 scope host lo
valid_lft forever preferred_lft forever
inet6 ::1/128 scope host noprefixroute
valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
link/ether 08:00:27:1f:b7:23 brd ff:ff:ff:ff:ff:ff
inet 192.168.1.15/24 brd 192.168.1.255 scope global dynamic noprefixroute eth0
valid_lft 86396sec preferred_lft 86396sec
inet6 fe80::8d2f:f8db:9193:5fa2/64 scope link noprefixroute
valid_lft forever preferred_lft forever
┌──(kali㉿kali)-[~]
└─$ traceroute google.com
traceroute to google.com (216.58.204.238), 30 hops max, 60 byte packets
1 Gateway.Home (192.168.1.1) 0.664 ms 0.848 ms 0.941 ms
2 bsn-access.dynamic.siol.net (213.250.19.90) 3.771 ms 3.545 ms 3.121 ms
3 ip-95-176-251-21.generic.siol.net (95.176.251.21) 4.823 ms ip-95-176-251-11.generic.siol.net (95.176.251.11
) 4.958 ms ip-95-176-251-21.generic.siol.net (95.176.251.21) 4.355 ms
4 bsn-77-107-46.static.siol.net (193.77.107.46) 9.207 ms 9.401 ms 10.166 ms
5 * * *
6 172.253.73.60 (172.253.73.60) 10.669 ms 142.250.211.20 (142.250.211.20) 8.775 ms 142.251.235.174 (142.251.
235.174) 10.436 ms
7 192.178.82.61 (192.178.82.61) 8.895 ms 192.178.104.212 (192.178.104.212) 9.341 ms 20.563 ms
8 192.178.99.157 (192.178.99.157) 9.396 ms lhr48s22-in-f14.1e100.net (216.58.204.238) 9.064 ms 9.286 ms
┌──(kali㉿kali)-[~]
└─$


┌──(kali㉿kali)-[~]
└─$ strings /bin/ls | head
!/lib64/ld-linux-x86-64.so.2
_ITM_deregisterTMCloneTable
__gmon_start__
_ITM_registerTMCloneTable
fgetfilecon_raw
fgetfilecon
freecon
lgetfilecon
lgetfilecon_raw
_IO_stdin_used


kali@kali: ~
Session Actions Edit View Help
10:40:46.878937 IP Gateway.Home.domain > kali.57273: 23694 1/0/0 PTR mdns.mcast.net. (70)
10:40:46.879117 IP kali.50118 > Gateway.Home.domain: 24725+ PTR? 252.0.0.224.in-addr.arpa. (42)
10:40:46.884470 IP Gateway.Home.domain > kali.50118: 24725 NXDomain 0/1/0 (99)
10:40:46.884923 IP kali.35621 > Gateway.Home.domain: 10935+ PTR? 18.102.255.239.in-addr.arpa. (45)
10:40:46.887764 IP Gateway.Home.domain > kali.35621: 10935 NXDomain 0/1/0 (102)
10:40:46.887976 IP kali.39576 > Gateway.Home.domain: 26977+ PTR? 5.0.3.2.1.d.5.8.a.9.6.c.c.f.7.f.0.0.0.0.0.0.0.0
.0.0.0.0.0.8.e.f.ip6.arpa. (90)
10:40:46.894048 IP Gateway.Home.domain > kali.39576: 26977 NXDomain* 0/1/0 (139)
10:40:46.894461 IP kali.48792 > Gateway.Home.domain: 44624+ PTR? d.3.b.5.8.e.e.f.f.f.2.c.1.b.6.f.0.0.0.0.0.0.0.0
.0.0.0.0.0.8.e.f.ip6.arpa. (90)
10:40:46.897940 IP Gateway.Home.domain > kali.48792: 44624 NXDomain* 0/1/1 (313)
10:40:47.181279 STP 802.1d, Config, Flags [none], bridge-id 8000.64:6e:ea:f5:6d:18.8002, length 35
10:40:47.181481 STP 802.1d, Config, Flags [none], bridge-id 8000.64:6e:ea:f5:6d:18.8002, length 35
10:40:48.181230 STP 802.1d, Config, Flags [none], bridge-id 8000.64:6e:ea:f5:6d:18.8002, length 35
10:40:48.181420 STP 802.1d, Config, Flags [none], bridge-id 8000.64:6e:ea:f5:6d:18.8002, length 35
10:40:48.181420 STP 802.1d, Config, Flags [none], bridge-id 8000.64:6e:ea:f5:6d:18.8002, length 35
10:40:48.181602 STP 802.1d, Config, Flags [none], bridge-id 8000.64:6e:ea:f5:6d:18.8002, length 35
^C
132 packets captured
132 packets received by filter
0 packets dropped by kernel
┌──(kali㉿kali)-[~]
└─$ sudo tcpdump -c 10
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), snapshot length 262144 bytes
10:40:53.180676 STP 802.1d, Config, Flags [none], bridge-id 8000.64:6e:ea:f5:6d:18.8002, length 35
10:40:53.180946 STP 802.1d, Config, Flags [none], bridge-id 8000.64:6e:ea:f5:6d:18.8002, length 35
10:40:54.179723 STP 802.1d, Config, Flags [none], bridge-id 8000.64:6e:ea:f5:6d:18.8002, length 35
10:40:54.179724 STP 802.1d, Config, Flags [none], bridge-id 8000.64:6e:ea:f5:6d:18.8002, length 35
10:40:54.179724 STP 802.1d, Config, Flags [none], bridge-id 8000.64:6e:ea:f5:6d:18.8002, length 35
10:40:54.179916 STP 802.1d, Config, Flags [none], bridge-id 8000.64:6e:ea:f5:6d:18.8002, length 35
10:40:55.179509 STP 802.1d, Config, Flags [none], bridge-id 8000.64:6e:ea:f5:6d:18.8002, length 35
10:40:55.179885 STP 802.1d, Config, Flags [none], bridge-id 8000.64:6e:ea:f5:6d:18.8002, length 35
10:40:56.109785 IP6 fe80::666e:eaff:fef5:6d18.dhcpv6-client > ff02::1:2.dhcpv6-server: dhcp6 solicit
10:40:56.179437 STP 802.1d, Config, Flags [none], bridge-id 8000.64:6e:ea:f5:6d:18.8002, length 35
10:40:56.179437 STP 802.1d, Config, Flags [none], bridge-id 8000.64:6e:ea:f5:6d:18.8002, length 35
10 packets captured
17 packets received by filter
0 packets dropped by kernel
┌──(kali㉿kali)-[~]
└─$ sudo tcpdump -c 10 > tcpdump.cap
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), snapshot length 262144 bytes
10 packets captured
15 packets received by filter
0 packets dropped by kernel
┌──(kali㉿kali)-[~]
└─$ ls
Desktop Documents Downloads Music Pictures Public tcpdump.cap Templates vaje01 Videos
┌──(kali㉿kali)-[~]
└─$




```
┌──(kali㉿kali)-[~/vaje01]
└─$ nmap -O 192.168.226.2
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-27 10:45 EST
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 3.15 seconds

┌──(kali㉿kali)-[~/vaje01]
└─$ nmap -p 1-65535 -T4 192.168.226.2
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-27 10:48 EST
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 2.07 seconds

┌──(kali㉿kali)-[~/vaje01]
└─$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:1f:b7:23 brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.15/24 brd 192.168.1.255 scope global dynamic noprefixroute eth0
       valid_lft 85405sec preferred_lft 85405sec
    inet6 fe80::8d2f:f8db:9193:5fa2/64 scope link noprefixroute
       valid_lft forever preferred_lft forever

┌──(kali㉿kali)-[~/vaje01]
└─$ nmap -p 1-65535 -T4 192.168.1.15
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-27 10:48 EST
Nmap scan report for kali (192.168.1.15)
Host is up (0.0000040s latency).
All 65535 scanned ports on kali (192.168.1.15) are in ignored states.
Not shown: 65535 closed tcp ports (reset)

Nmap done: 1 IP address (1 host up) scanned in 0.79 seconds

┌──(kali㉿kali)-[~/vaje01]
└─$
```

```
┌──(kali㉿kali)-[~/vaje01]
└─$ dnsenum google.com
dnsenum VERSION:1.3.1

-----   google.com   -----


Host's addresses:
__________________

google.com.                              293      IN    A        142.250.180.142


Name Servers:
______________

ns4.google.com.                          247522   IN    A        216.239.38.10
ns1.google.com.                          72759    IN    A        216.239.32.10
ns2.google.com.                          78016    IN    A        216.239.34.10
ns3.google.com.                          82246    IN    A        216.239.36.10


Mail (MX) Servers:
___________________

smtp.google.com.                         292      IN    A        108.177.119.26
smtp.google.com.                         292      IN    A        108.177.119.27
smtp.google.com.                         292      IN    A        108.177.127.26
smtp.google.com.                         292      IN    A        108.177.96.26
smtp.google.com.                         292      IN    A        108.177.96.27


Trying Zone Transfers and getting Bind Versions:
_________________________________________________


Trying Zone Transfer for google.com on ns1.google.com ...
AXFR record query failed: corrupt packet

Trying Zone Transfer for google.com on ns2.google.com ...
AXFR record query failed: corrupt packet
^C

┌──(kali㉿kali)-[~/vaje01]
└─$ lbd google.com

lbd - load balancing detector 0.4 - Checks if a given domain uses load-balancing.
                                    Written by Stefan Behte (http://ge.mine.nu)
                                    Proof-of-concept! Might give false positives.

Checking for DNS-Loadbalancing: NOT FOUND
Checking for HTTP-Loadbalancing [Server]:
 gws
```