



```
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 upgrade -y
Summary:
  Upgrading: 0, Installing: 0, Removing: 0, Not Upgrading: 0

(kali㉿kali)-[~]
$ sudo apt install nmap -y
nmap is already the newest version (7.95+dfsg-3kali1).
Summary:
  Upgrading: 0, Installing: 0, Removing: 0, Not Upgrading: 0

(kali㉿kali)-[~]
$ nmap --version
Nmap version 7.95 ( https://nmap.org )
Platform: x86_64-pc-linux-gnu
Compiled with: liblua-5.4.7 openssl-3.5.0 libssh2-1.11.1 libz-1.3.1 libpcre2-10.45 libpcap-1.10.5 nmap-libdnet-1.12 ipv6
Compiled without:
Available nsock engines: epoll poll select

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

Mouse integration ...

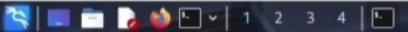
Don't show again

Auto capture keyboard ...

Don't show again

```
To access official Ubuntu documentation, please visit:  
http://help.ubuntu.com/  
no mail.  
msfadmin@metasploitable:~$ ifconfig  
eth0      Link encap:Ethernet HWaddr 08:00:27:1e:a9:63  
          inet addr:192.168.56.104 Bcast:192.168.56.255 Mask:255.255.255.0  
             inet6 addr: fe80::a00:27ff:fe1e:a963/64 Scope:Link  
                UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1  
                RX packets:3 errors:0 dropped:0 overruns:0 frame:0  
                TX packets:30 errors:0 dropped:0 overruns:0 carrier:0  
                collisions:0 txqueuelen:1000  
               RX bytes:1252 (1.2 KB) TX bytes:3924 (3.8 KB)  
               Base address:0xd020 Memory:f0200000-f0220900  
  
lo       Link encap:Local Loopback  
          inet addr:127.0.0.1 Mask:255.0.0.0  
             inet6 addr: ::1/128 Scope:Host  
                UP LOOPBACK RUNNING MTU:16436 Metric:1  
                RX packets:100 errors:0 dropped:0 overruns:0 frame:0  
                TX packets:100 errors:0 dropped:0 overruns:0 carrier:0  
                collisions:0 txqueuelen:0  
               RX bytes:23481 (22.9 KB) TX bytes:23481 (22.9 KB)  
msfadmin@metasploitable:~$ _
```





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
-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 st_5_92_1_and64.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)-[~]
$
```

kali㉿kali: ~

File Machine View Input Devices Help



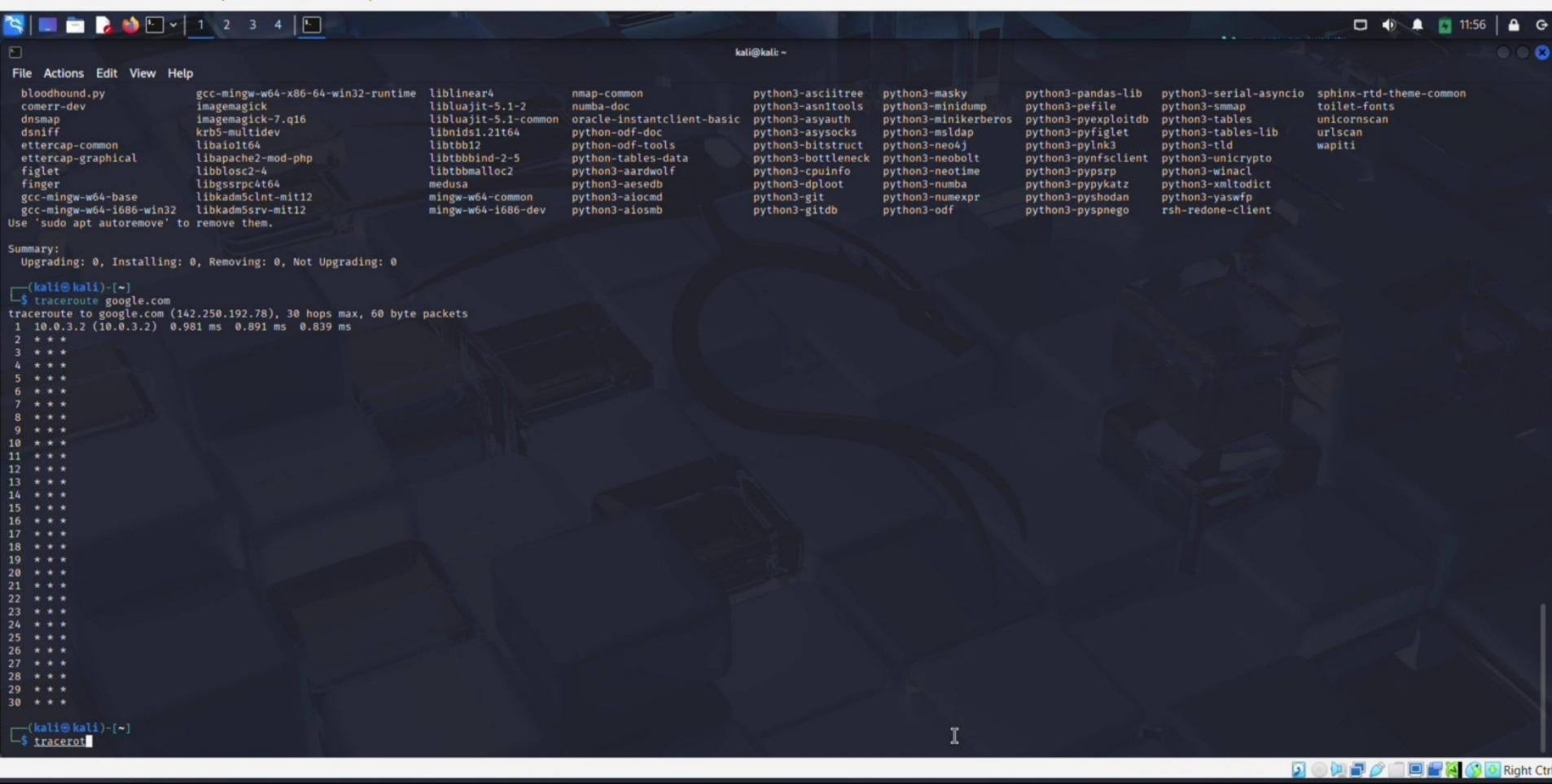
kali㉿kali: ~

```
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 8ubuntu1 (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



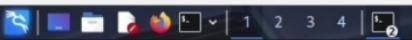
kali@kali:~



```
klog:1$#f2ZVMS4K$R9Xk1.CmLdhduE3X9jqP0:14742:0:99999:7:::  
sshd:1:14684:0:99999:7:::  
msfadmin:1:$XN10Zj2c$Rt/zzCw3mLtUWA.ihZjA5:/:14684:0:99999:7:::  
bind:1:14685:0:99999:7:::  
postfix:1:14685:0:99999:7:::  
ftp:1:14685:0:99999:7:::  
postgres:1:$Rw351k.x$MgqZUuO5pAoUvfJhfcYe:/:14685:0:99999:7:::  
mysql:1:14685:0:99999:7:::  
tomcat55:1:14691:0:99999:7:::  
distccd:1:14698:0:99999:7:::  
user:$1$HE5uRxH$0.03693DGoxXiQKpMulgZ0:14699:0:99999:7:::  
service:$1$K3ueJZS76xEL0upr50hp6cjZ3Bu//:14715:0:99999:7:::  
telnetd:1:14715:0:99999:7:::  
proftpd:1:14727:0:99999:7:::  
statd:1:15474:0:99999:7:::  
  
ls /  
bin  
boot  
cdrom  
dev  
etc  
home  
initrd  
initrd.img  
lib  
lost+found  
media  
mnt  
nohup.out  
opt  
proc  
root  
sbin  
srv  
sys  
tmp  
usr  
var  
vmlinuz  
  
ls /home  
ftp  
msfadmin  
service  
user  
cd /tmp  
  
echo "hacked by Asd !">> /tmp/
```



File Machine View Input Devices Help



kali@kali: ~

Hit:1 http://http.kali.org/kali kali-rolling InRelease
963 packages can be upgraded. Run 'apt list --upgradable' to see them.

```
(kali㉿kali)-[~]
$ sudo apt install -y iputils-arping
The following packages were automatically installed and are no longer required:
binutils-mingw-w64-i686  gcc-mingw-w64-i686-win32-runtime  libkdb5-10t64    numba-doc      python3-asn1tools  python3-minidump   python3-pefile    python3-smmmap   toilet-fonts
binutils-mingw-w64-x86-64  gcc-mingw-w64-x86-64-win32     libkrb5-dev      oracle-instantclient-basic  python3-asyauth  python3-minikerberos  python3-pyexploitdb  python3-tables  unicornsanc
bloodhound.py              gcc-mingw-w64-x86-64-win32-runtime  libluajit-5.1-2  python3-odf-doc    python3-asysocks  python3-msldap      python3-pyfiglet  python3-tables-lib  urlscan
comerr-dev                imagemagick       libluajit-5.1-common  python3-odf-tools  python3-bitstruct  python3-neo4j       python3-pylnk3    python3-tld     wapiti
dnsmap                   libmagick-q16      libnids1.21t64    python3-tables-data  python3-bottleneck  python3-neobolt    python3-pynfsclient  python3-unicrypto
dnsniff                  krb5-multidev   libtbb2          python3-aardwolf  python3-cpuinfo   python3-neotime   python3-pypst     python3-winacl
ettercap-common           libtbbt64        libtbbbind-2-5   python3-aesedb    python3-dploot    python3-numexpr   python3-pypykatz  python3-xmltodict
ettercap-graphical        libapache2-mod-php  libtbbmalloc2    python3-aicodm   python3-git       python3-pshtodan  python3-yaswfp
figlet                   libtbb2-2-4      medusa         python3-aiosmb   python3-gitdb     python3-pshtodan  python3-redone-client
finger                   libgssrpc4t64    mingw-w64-common  python3-aioinreg  python3-llvmlite  python3-oscrypto  python3-qasync   smtp-user-enum
gcc-mingw-w64-base        libkadm5clnt-mit12  mingw-w64-dev    python3-arc4     python3-lsassy   python3-pandas   python3-qrcode  sparta-scripts
gcc-mingw-w64-i686-win32  libkadm5srv-mit12  mingw-w64-x86-64-dev  python3-asciitree  python3-masky    python3-pandas-lib  python3-serial-asyncio sphinx-ftd-theme-common
Use 'sudo apt autoremove' to remove them.
```

Upgrading:
 iputils-ping

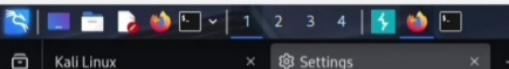
Installing:
 iputils-arping

REMOVING:
 arping

Summary:
 Upgrading: 1, Installing: 1, Removing: 1, Not Upgrading: 962
 Download size: 22.9 kB / 74.9 kB
 Freed space: 31.7 kB

```
Get:1 http://kali.download/kali kali-rolling/main amd64 iputils-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 .../iputils-ping_3%3a20250605-1_amd64.deb ...
Unpacking iputils-ping (3:20250605-1) over (3:20240905-3) ...
Selecting previously unselected package iputils-arping.
Preparing to unpack .../iputils-arping_3%3a20250605-1_amd64.deb ...
Unpacking iputils-arping (3:20250605-1) ...
Setting up iputils-arping (3:20250605-1) ...
Processing triggers for man-db (2.13.1-1) ...
Processing triggers for kali-menu (2025.2.7) ...

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



General

Home

Search

Privacy & Security

Sync

More from Mozilla

Browsing

- Use autoscrolling
- Use smooth scrolling
- Always show scrollbars
- Always use the cursor keys to navigate within pages
- Always underline links
- Search for text when you start typing
- Enable picture-in-picture video controls [Learn more](#)
- Control media via keyboard, headset, or virtual interface [Learn more](#)
- Recommend extensions as you browse [Learn more](#)
- Recommend features as you browse [Learn more](#)

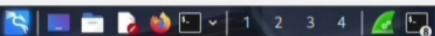
Network Settings

Extensions & Themes

Configure how Firefox connects to the internet. [Learn more](#)

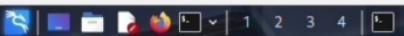
Settings...

Firefox Support



kali@kali

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 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 00:00:27:37:82:0c 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 86367sec preferred_lft 86367sec
        inet6 fd17:625c:f037:3:a1f2:c5af:eddb:440c/64 scope global temporary dynamic
            valid_lft 86369sec preferred_lft 14369sec
        inet6 fd17:625c:f037:3:a00:27ff:fe37:826c/64 scope global dynamic mngtmpaddr noprefixroute
            valid_lft 86369sec preferred_lft 14369sec
        inet6 fe00::a0:27ff:fe37:826c/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=3.86 ms
64 bytes from 192.168.56.104: icmp_seq=2 ttl=255 time=1.71 ms
— 192.168.56.104 ping statistics —
2 packets transmitted, 2 received, 0% packet loss, time 1070ms
rtt min/avg/max/mdev = 1.714/2.786/3.858/1.072 ms
```

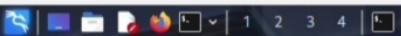
```
(kali㉿kali)-[~]
$ sudo pskill -f tcpdump || true rm -f ~/step6_arp_icmp.pcap
[sudo] password for kali:
sudo: pskill: command not found

(kali㉿kali)-[~]
$ sudo pskill -f tcpdump || true rm -f ~/step6_arp_icmp.pcap
```

```
S | D | P | F | 1 2 3 4 | L |   
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 message.txt -out message.enc -pass pass:TestPass123  
[(kali㉿kali)-~]  
$ openssl enc -d -aes-256-cbc -pbkdf2 -in message.enc -out message_decrypted.txt -pass pass:TestPass123  
[(kali㉿kali)-~]  
$ cat message_decrypted.txt  
This is my OpenSSL encryption test  
[(kali㉿kali)-~]  
$ rm -f message.txt message.enc message_decrypted.t
```

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

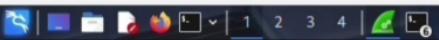
(kali㉿kali)-[~]
$ openssl enc -aes-256-cbc -pbkdf2 -in plain.txt -out secret.enc -pass pass:MyStrongPass123

(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
-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 vt_5_02-1_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_decrypte.txt -pass pass:MyStrongPass123
```

File Machine View Input Devices Help



Capturing from eth1

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help



tcp.port == 443



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	648	Application Data, Application Data
47	90.113068618	2600:1406:5e00:6::1...	fd17:625c:f037:3:73...	TLSv1.3	166	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	f037:3:73...	2600:1406:5e00:6::1...	TCP	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	90.123244140	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	90.570993855	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

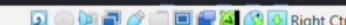
Frame 28: 94 bytes on wire (752 bits), 94 bytes captured (752 bits) on interface eth1, id 0

Ethernet II, Src: 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:f037:3:73b:b565:c292:4ef9, Dst: 2600:1406:5e00:6::17ce:bci

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	06	00	00	e	-N&	^.....
0030	00	00	17	ce	bc	1b	d2	dc	01	bb	aa	94	f7	f5	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	01	03	03	07	7



```
Warning: Never expose this VM to an untrusted network!
Contact: msfdev[at]metasploit.com
Login with msfadmin/msfadmin to get started

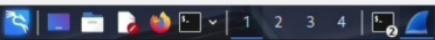
metasploitable login: msfadmin
Password:
Last login: Sat Sep 13 11:40:44 EDT 2025 on ttym1
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/*copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

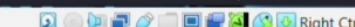
To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ ipconfig
-bash: ipconfig: command not found
msfadmin@metasploitable:~$ _
```





No.	arp icmp	Source	Destination	Protocol	Length	Info
1	arp	PCSSystemtec_d1:5d:66	PCSSystemtec_5f:0e:ab	ARP	42	Who has 192.168.56.100? Tell 192.168.56.106
2	arp_drone	PCSSystemtec_5f:0e:ab	PCSSystemtec_d1:5d:66	ARP	60	192.168.56.100 is at 08:00:27:5f:0e:ab
3	arcnet					
4	arpdp	PCSSystemtec_d1:5d:66	PCSSystemtec_5f:0e:ab	ARP	42	Who has 192.168.56.100? Tell 192.168.56.106
5	armagetrond	PCSSystemtec_d1:5d:66	PCSSystemtec_5f:0e:ab	ARP	60	192.168.56.100 is at 08:00:27:5f:0e:ab
6	arp	PCSSystemtec_1e:a9:66	Broadcast	ARP	60	Who has 192.168.56.100? Tell 192.168.56.104
7	artemis	PCSSystemtec_5f:0e:ab	Broadcast	ARP	60	Who has 192.168.56.106? Tell 192.168.56.100
8	artnet	PCSSystemtec_d1:5d:66	PCSSystemtec_5f:0e:ab	ARP	42	192.168.56.106 is at 08:00:27:d1:5d:66
9	aruba_erm	PCSSystemtec_d1:5d:66	PCSSystemtec_5f:0e:ab	ARP	42	Who has 192.168.56.100? Tell 192.168.56.106
10	aruba_erm_type0	PCSSystemtec_5f:0e:ab	PCSSystemtec_d1:5d:66	ARP	60	192.168.56.100 is at 08:00:27:5f:0e:ab
11	aruba_erm_type1	PCSSystemtec_d1:5d:66	PCSSystemtec_5f:0e:ab	ARP	42	Who has 192.168.56.100? Tell 192.168.56.106
12	aruba_erm_type2					
13	aruba_erm_type3					
14	aruba_erm_type4					
15	aruba_erm_type5					
16	aruba_erm_type6					
17	aruba_jap					

```
> 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)
> Address Resolution Protocol (request)  0000 08 00 27 5f 0e ab 08 00 27 d1 5d 66 08 06 00 01 ..'-'...'.]f ...
  0010 08 00 06 04 00 01 08 00 27 d1 5d 66 c0 a8 38 6a ..'-'...'.]f..8j
  0020 00 00 00 00 00 00 c0 a8 38 64 .....8d
```



File Machine View Input Devices Help



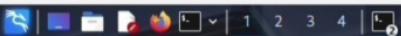
kali@kali: ~

(kali㉿kali)-[~]

\$ pwd
/home/kali

(kali㉿kali)-[~]
\$ ls -l /tmp

File Machine View Input Devices Help



kali@kali:~

```
(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)-[~]
$
```

File Machine View Input Devices Help

```
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_9.02-1_and64.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
e32c0fbef13ba88636f74bbd1f2cb0efa88f8e0a1322c0ec4975daf3d5d4646 hash.txt
(kali㉿kali)-[~]
└$ rm -f hash.txt
(kali㉿kali)-[~]
└$ openssl genrsa -out myprivate.key 2048
(kali㉿kali)-[~]
└$ ls -lmy privat
```

File Machine View Input Devices Help



kali㉿kali: ~

```
64 bytes from 192.168.56.104: icmp_seq=4 ttl=255 time=2.72 ms
64 bytes from 192.168.56.104: icmp_seq=5 ttl=255 time=2.30 ms
64 bytes from 192.168.56.104: icmp_seq=6 ttl=255 time=1.68 ms temporary dynamic
64 bytes from 192.168.56.104: icmp_seq=7 ttl=255 time=1.15 ms
64 bytes from 192.168.56.104: icmp_seq=8 ttl=255 time=1.44 ms temporary dynamic
64 bytes from 192.168.56.104: icmp_seq=9 ttl=255 time=1.88 ms
64 bytes from 192.168.56.104: icmp_seq=10 ttl=255 time=1.26 ms

— 192.168.56.104 ping statistics —
10 packets transmitted, 10 received, 0% packet loss, time 9027ms
rtt min/avg/max/mdev = 1.153/2.789/12.511/3.273 ms
```

```
[(kali㉿kali)-~] $ sudo apt install -y arping >/dev/null || true
```

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

binutils-mingw-w64-i686	gcc-mingw-w64-i686-win32-runtime	libkdbs5-10t64	numba-doc	python3-asn1tools	python3-minidump	python3-pefile	python3-smmmap	toilet-fonts
binutils-mingw-w64-x86-64	gcc-mingw-w64-x86-64-win32	libkrb5-dev	oracle-instantclient-basic	python3-asyauth	python3-minikerberos	python3-pyexploitdb	python3-tables	unicornscan
bloodhound.py	gcc-mingw-w64-x86-64-win32-runtime	liblLuaJIT-5.1-2	python3-odf-doc	python3-asyncsocks	python3-msldap	python3-pyfiglet	python3-tables-lib	wapiti
comerr-dev	imagemagick	liblLuaJIT-5.1-common	python3-odf-tools	python3-bitsruct	python3-neo4j	python3-pylink3	python3-tld	
dnsmasq	imagemagick-7.q16	liblbind1.21t64	python3-tables-data	python3-bottleneck	python3-neobolt	python3-pynfsclient	python3-unicrypto	
dsniff	krb5-multidev	liblai0t64	python3-aardwolf	python3-cpuinfo	python3-neotime	python3-pysrplib	python3-winacl	
ettercap-common	liblbb1	liblbbbind-2-5	python3-aesedb	python3-dploot	python3-numba	python3-pypykatz	python3-xmldict	
ettercap-graphical	liblapache2-mod-php	liblbbmalloc2	python3-aiocmd	python3-git	python3-numexpr	python3-psychan	python3-yawsfp	
figlet	liblbbosc2-4	medusa	python3-aiosmb	python3-gitdb	python3-odf	python3-pysnego	rsh-redone-client	
finger	liblgsrprc4t64	mingw-w64-common	python3-aiowinreg	python3-lvmlite	python3-oscrypto	python3-qasync	smtp-user-enum	
gcc-mingw-w64-base	liblakadm5clnt-mit12	mingw-w64-dev	python3-arc4	python3-lsassy	python3-pandas	python3-qrcode	sparta-scripts	
gcc-mingw-w64-i686-win32	liblakadm5rv-mit12	mingw-w64-x86-64-dev	python3-asciitree	python3-masky	python3-pandas-lib	python3-serial-asyncio	sphinx-rtd-theme-common	

Use 'sudo apt autoremove' to remove them.

```
Upgrading: arping
arping
Upgrading 1 package, 0 newly installed, 0 to remove and 963 not upgraded.
Summary:
```

Upgrading: 1, Installing: 0, Removing: 0, Not Upgrading: 963

Download size: 0 B / 33.1 kB

Space needed: 0 B / 97.4 GB available

```
(Reading database ... 381037 files and directories currently installed.)
Preparing to unpack .../arping_2.26-1_amd64.deb ...
Unpacking arping (2.26-1) over (2.25-1) ...
Setting up arping (2.26-1) ...
Processing triggers for kali-menu (2025.2.7) ...
Processing triggers for man-db (2.13.1-1) ...
```

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

arping: Unable to get the IPv4 address of interface eth0:
arping: libnet_get_ipaddr4(): ioctl(): Cannot assign requested addressarping: Use -S to specify address manually.

```
[(kali㉿kali)-~] $ arping --version
```

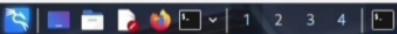


```
File Actions Edit View Help
    color: #38488f;
    text-decoration: none;
}
@media (max-width: 700px) {
    div {
        margin: 0 auto; referer_ift forever
        width: auto; t norefreshroute
    }
}

```

```
[kali㉿kali:~] $ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback brd 00:00:00:00:00:00 state UNKNOWN
    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,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 00:02:27:d1:66:bd brd ff:ff:ff:ff:ff:ff
3: eth1: <NO-CARRIER,BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 00:02:27:37:82:b6 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:fe4f/64 scope global temporary dynamic
            valid_lft 86377sec preferred_lft 14377sec
        inet6 fd17:625c:f037:3:a0:27ff:fe37:826c/64 scope global dynamic mngtmpaddr noprefixroute
            valid_lft 86377sec preferred_lft 14377sec
```

```
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
```



kali@kali: ~

File Actions Edit View Help

(kali㉿kali)-[~]
\$ sudo dhclient

Mouse integration ...

Don't show again

```
kali@kali: ~
```

File Actions Edit View Help

```
</div>
</body>
</html> Connection #0 to host example.com left intact
```

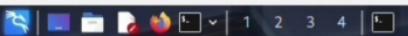
```
(kali㉿kali)-[~]
$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
        inet 127.0.0.1/8 scope host lo
            valid_lft forever preferred_lft forever
            inet6 ::1/128 scope host 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:d1:66 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 81554sec preferred_lft 81554sec
        inet6 fd17:625c:f037:3:736b:b565:c292:4ef9/64 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 fe00::a0:27ff: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
64 bytes from 8.8.8.8: icmp_seq=4 ttl=255 time=77.3 ms

--- 8.8.8 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3056ms
rtt min/avg/max/mdev = 72.602/80.296/98.048/10.404 ms

(kali㉿kali)-[~]
$ sudo tcpdump -i eth1 arp -c 5
[sudo] password for kali:
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on eth1, link-type EN10MB (Ethernet), snapshot length 262144 bytes
17:58:16.881076 ARP, Request who-has 10.0.3.2 tell 10.0.3.15, length 28
17:58:16.881843 ARP, Reply 10.0.3.2 is-at 52:55:0a:00:03:02 (oui Unknown), length 50
```

File Machine View Input Devices Help



kali㉿kali: ~

File Actions Edit View Help

```
Setting up nmap (7.95+dfsg-3kali1) ...
Setcap worked! Adding configuration to environment
Processing triggers for man-db (2.13.1-1) ...
Processing triggers for kali-menu (2025.2.7) ...
```

```
(kali㉿kali)-[~]
$ nmap --version
Nmap version 7.95 ( https://nmap.org )
Platform: x86_64-pc-linux-gnu
Compiled with: liblua-5.4.7 openssl-3.5.0 libssh2-1.11.1 libz-1.3.1 libpcre2-10.45 libpcap-1.10.5 nmap-libdnet-1.12 ipv6
Compiled without:
Available nsock engines: epoll poll select
```

```
(kali㉿kali)-[~]
$ nmap localhost
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-11 12:20 IST
Nmap scan report for localhost (127.0.0.1)
Host is up (0.0000020s 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)
```

Nmap done: 1 IP address (1 host up) scanned in 0.16 seconds

```
(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)-[~]
$ nmap 10.0.2.2
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-11 12:21 IST
Nmap scan report for 10.0.2.2
Host is up (0.000060s latency).
All 1000 scanned ports on 10.0.2.2 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
```

Nmap done: 1 IP address (1 host up) scanned in 5.66 seconds

```
(kali㉿kali)-[~]
$ nmap 192.168.1.1
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-11 12:21 IST
Nmap scan report for 192.168.1.1
Host is up (0.0026s latency).
All 1000 scanned ports on 192.168.1.1 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
```

Nmap done: 1 IP address (1 host up) scanned in 4.86 seconds

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

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

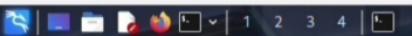
(kali㉿kali)-[~]
$ cat received.txt
cat: received.txt: No such file or directory

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

(kali㉿kali)-[~]
$
```

```
kali@kali: ~
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)-[~]
$
```

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 st_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
)***RMeY'2*
```

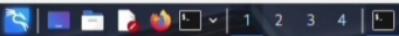
(kali㉿kali)-[~]

```
$ 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)-[~]
$
```



kali@kali: ~

```
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 message.txt -out message.enc -pass pass:TestPass123
[(kali㉿kali)-~]
$ openssl enc -d -aes-256-cbc -pbkdf2 -in message.enc -out message_decrypted.txt -pass pass:TestPass123
[(kali㉿kali)-~]
$
```

File Machine View Input Devices Help



kali㉿kali:~

```
File Actions Edit View Help
[_clock-skew: mean: 59m58s, deviation: 2h00m00s, median: -1s
[_nbstat: NetBIOS name: METASPLOITABLE, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)

TRACEROUTE (using port 80/tcp)
HOP RTT ADDRESS
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
```

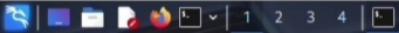
```
(kali㉿kali)-[~]
$ sudo nmap -sV 192.168.56.104 | tee nmap_scan.txt
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-13 22:57 IST
Nmap scan report for 192.168.56.104
Host is up (0.0036s latency).

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 rexecd
513/tcp   open  login       Netkit rshd
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

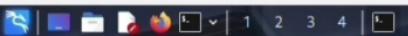
(kali㉿kali)-[~]
$ cat nmap_scan.txt
```



kali@kali: ~

```
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 message.txt -out message.enc -pass pass:TestPass123
[(kali㉿kali)-~]
$ openssl enc -d -aes-256-cbc -pbkdf2 -in secret.enc -out plain_decrypted.txt -pass pass:MyStrongPass123
```

File Machine View Input Devices Help



kali㉿kali: ~

File Actions Edit View Help

```
[(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	libkdbs5-10t64	mingw-w64-x86-64-dev
binutils-mingw-w64-x86-64	gcc-mingw-w64-x86-64-win32	libkrb5-dev	ndiff
bloodhound.py	gcc-mingw-w64-x86-64-win32-runtime	liblinear4	nmap-common
comerr-dev	imagemagick	libluajit-5.1-2	numba-doc
dnsmap	imagemagick-7.q16	libnids1.21t64	oracle-instantclient-basic
dsniff	krb5-multidev	libtbb2	python-odf-doc
ettercap-common	libaiolit64	libtbb2bind-2-5	python-odf-tools
ettercap-graphical	libapache2-mod-php	libtbbmalloc2	python-tables-data
figlet	libgsrpc4t64	medusa	python3-aardwolf
finger	mingw-w64-base	mingw-w64-common	python3-aesedb
gcc-mingw-w64-base	libkadm5clnt-mit12	mingw-w64-dev	python3-aicmd
gcc-mingw-w64-i686-win32	libkadm5srv-mit12		python3-aiosmb

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
```

wget: missing URL
Usage: wget [OPTION] ... [URL] ...
Try 'wget --help' for more options.

```
[(kali㉿kali)-~]$ wget http://archive.ubuntu.com/ubuntu/pool/universe/s/sl/sl_5.02-1_amd64.deb
```

--2025-09-07 20:26:18-- http://archive.ubuntu.com/ubuntu/pool/universe/s/sl/sl_5.02-1_amd64.deb

Resolving archive.ubuntu.com (archive.ubuntu.com) ... 185.125.140.83, 91.189.91.81, 185.125.190.82, ...

Connecting to archive.ubuntu.com (archive.ubuntu.com)|185.125.190.83|:80 ... connected.

HTTP request sent, awaiting response ... 200 OK

Length: 12708 (12K) [application/vnd.debian.binary-package]

Saving to: 'sl_5.02-1_amd64.deb'

sl_5.02-1_amd64.deb

2025-09-07 20:26:19 (357 MB/s) - 'sl_5.02-1_amd64.deb' saved [12708/12708]

```
[(kali㉿kali)-~]$ sudo dpkg -i sl_5.02-1_amd64.deb
```

smtp-user-enum
sparta-scripts
sphinx-rtd-theme-common
toilet-fonts
unicornscan
urlscan
wapiti

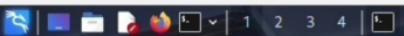


File Machine View Input Devices Help

```
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 vt_3.02-1_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
e32c0bfeba13ba88636f74bbd1f2cb0efa88f8e0a1322c0ec4975daf3d5d4646 hash.txt
(kali㉿kali)-[~]
$ rm -f hash.txt
(kali㉿kali)-[~]
```

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 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 00:00:27:37:82:0c 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 86367sec preferred_lft 86367sec
        inet6 fd17:625c:f037:3:a1f2:c5af:eddb:440c/64 scope global temporary dynamic
            valid_lft 86369sec preferred_lft 14369sec
        inet6 fd17:625c:f037:3:a00:27ff:fea7:826c/64 scope global dynamic mngtmpaddr noprefixroute
            valid_lft 86369sec preferred_lft 14369sec
        inet6 fe00::a0:27ff:fea7:826c/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=3.86 ms
64 bytes from 192.168.56.104: icmp_seq=2 ttl=255 time=1.71 ms
— 192.168.56.104 ping statistics —
2 packets transmitted, 2 received, 0% packet loss, time 1070ms
rtt min/avg/max/mdev = 1.714/2.786/3.858/1.072 ms
```

```
(kali㉿kali)-[~]
$ sudo pkill -f tcpdump || true
```

```
File Actions Edit View Help
</html>
* Connection #0 to host example.com left intact
(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
        link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
        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 08:00:27:37:82:6c 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:ae9/64 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::a0:27ff:fe37:826c/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
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)-[~]
$ 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

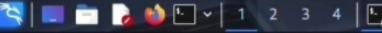
(kali㉿kali)-[~]
$ ping -c 4 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=255 time=98.0 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=255 time=72.6 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=255 time=73.3 ms
64 bytes from 8.8.8.8: icmp_seq=4 ttl=255 time=77.3 ms

— 8.8.8.8 ping statistics —
4 packets transmitted, 4 received, 0% packet loss, time 3056ms
rtt min/avg/max/mdev = 72.602/80.296/98.048/10.404 ms

(kali㉿kali)-[~]
$ sudo tcpdump -i eth1 arp -c 5
[sudo] password for kali:
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on eth1, link-type EN10MB (Ethernet), snapshot length 262144 bytes
17:58:16.881076 ARP, Request who-has 10.0.3.2 tell 10.0.3.15, length 28
17:58:16.881843 ARP, Reply 10.0.3.2 is-at 52:55:0a:00:03:02 (oui Unknown), length 50
17:59:56.716963 ARP, Request who-has 10.0.3.2 tell 10.0.3.15, length 28
17:59:56.717386 ARP, Reply 10.0.3.2 is-at 52:55:0a:00:03:02 (oui Unknown), length 50
```

Screenshot taken

View image



kali@kali: ~

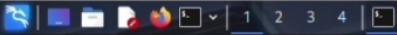


File Actions Edit View Help

```
(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
16:38:06.678795 ARP, Request who-has 192.168.56.104 tell 192.168.56.100, length 46
  valid_lifETIME forever, wire_length 46
24: 0x00000000000000000000000000000000 broadcast, lower_layer_type 1500, source fa:ad:ef:state UP group default qlen 1000
  link/ether 00:00:00:00:00:00 brd ff:ff:ff:ff:ff:ff
? 0x00000000000000000000000000000000 broadcast, lower_layer_type 1500, source fa:ad:ef:state UP group default qlen 1000
  link/ether 00:00:27:37:42:0c brd ff:ff:ff:ff:ff:ff
inet br-lan brd 255.255.255.0/24 scope global dynamic noprefixroute eth0
  valid_lft 85740sec preferred_lft 85740sec
inet6 fe80::2e0:1ff:fe00:1/64 brd fe80::ff:ff:ff:ff:ff:ff scope global temporary dynamic
  valid_lft 86374sec preferred_lft 14234sec
  valid_lft 86374sec preferred_lft 14234sec
inet6 :: brd ::/64 scope link noprefixroute
  valid_lft forever preferred_lft forever

└── (br-lan) [~]
  ↳ in route
default via 192.168.56.1 dev eth0 proto dhcp src 192.168.56.1 metric 100
  dev eth0 proto kernel scope link src 192.168.56.1 metric 100

└── (br-lan) [~]
```



kali@kali: ~

20:27

Home



Applications

Dash

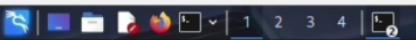
System

() () () () () () () () ()
() () () () () () () () ()
D () () () () () () () () ()
H H H H H H H H H H
I I I I I I I I I I
= = = = = = = = = =
D D D D D D D D D D
A A A A A A A A A A

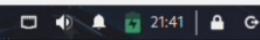
o o o o o o o o o o
= = = = = = = = = =
D D D D D D D D D D
Y Y Y Y Y Y Y Y Y Y

I I I I I I I I I I
D D D D D D D D D D
D D D D D D D D D D

File Machine View Input Devices Help



kali@kali: ~



File Actions Edit View Help
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
```

```
[(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  
64 bytes from 192.168.56.104: icmp_seq=8 ttl=255 time=4.10 ms  
64 bytes from 192.168.56.104: icmp_seq=9 ttl=255 time=3.19 ms  
64 bytes from 192.168.56.104: icmp_seq=10 ttl=255 time=2.84 ms  
--- 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  
ARPING 192.168.56.104 from 10.0.3.15 eth0  
Unicast reply from 192.168.56.104 [08:00:27:1E:A9:63] 3.060ms  
Unicast reply from 192.168.56.104 [08:00:27:1E:A9:63] 5.045ms  
Unicast reply from 192.168.56.104 [08:00:27:1E:A9:63] 2.898ms  
Unicast reply from 192.168.56.104 [08:00:27:1E:A9:63] 1.950ms  
Unicast reply from 192.168.56.104 [08:00:27:1E:A9:63] 2.124ms  
Sent 5 probes (1 broadcast(s))  
Received 5 response(s)
```

```
[(kali㉿kali)-~] $ sudo pkill tcpdump  
tcpdump: /lib/stub/_tcpdump: No such file or directory
```

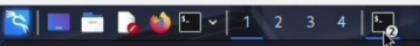
```
[(kali㉿kali)-~] $
```

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 ...
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: ~
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 test" | nc 127.0.0.1 4444
(kali㉿kali)-[~]
$ 
```

File Machine View Input Devices Help



kali@kali: ~

```
File Actions Edit View Help
└$ 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 21:36:0C:00:00:00 grep --color=auto
```

```
(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 count [1--count]
64 bytes from 192.168.56.104: icmp_seq=7 ttl=255 time=2.07 ms [1--seconds]
64 bytes from 192.168.56.104: icmp_seq=8 ttl=255 time=4.10 ms [emptytype]
64 bytes from 192.168.56.104: icmp_seq=9 ttl=255 time=3.19 ms [outlbound]
64 bytes from 192.168.56.104: icmp_seq=10 ttl=255 time=2.84 ms [inlbound]
— 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
ARPING 192.168.56.104 from 10.0.3.15 eth0
Unicast reply from 192.168.56.104 [08:00:27:1E:A9:63] 3.060ms
Unicast reply from 192.168.56.104 [08:00:27:1E:A9:63] 5.045ms
Unicast reply from 192.168.56.104 [08:00:27:1E:A9:63] 2.898ms
Unicast reply from 192.168.56.104 [08:00:27:1E:A9:63] 1.950ms
Unicast reply from 192.168.56.104 [08:00:27:1E:A9:63] 2.124ms
Sent 5 probes (1 broadcast(s))
Received 5 response(s)
```

```
(kali㉿kali)-[~]
└$ sudo tcpdump -n -i eth0 -w ./tcpdump.pcap
tcpdump: listening on eth0, link-type Pcap (raw IP), capture size 65535 bytes (1638.8 KB)
tcpdump: warning: /tmp/tcpdump.pcap: file must be created by root or root-equivalent user
tcpdump: warning: /tmp/tcpdump.pcap: file must be created by root or root-equivalent user
(kali㉿kali)-[~]
└$ ps -ef | grep tcpdump
kali      17730    7635  0 21:43 pts/1    00:00:00 grep --color=auto tcpdump
```

```
(kali㉿kali)-[~]
└$
```

File Machine View Input Devices Help



```
kali㉿kali: ~
```

```
2049/tcp open  nfs
2121/tcp open  cproxy-ftp
3306/tcp open  mysql
5432/tcp open  postgresql
5900/tcp open  vnc
6000/tcp open  X11
6667/tcp open  irc
8009/tcp open  ajp13
8180/tcp open  unknown

Nmap done: 1 IP address (1 host up) scanned in 11.37 seconds
```

```
(kali㉿kali)-[~]
$ sudo nmap -sV 192.168.56.104
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-13 22:53 IST
Nmap scan report for 192.168.56.104
Host is up (0.0042s 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 Bubuntu1 (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 rexecd
513/tcp   open  login?      Netkit rshd
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 23.23 seconds
```

```
(kali㉿kali)-[~]
$ sudo nmap -A 192.168.56.104
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-13 22:54 IST
```

File Machine View Input Devices Help



kali@kali: ~

File Actions Edit View Help

```
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]:Google  
Organizational Unit Name (eg, section) []:  
Common Name (e.g. server FQDN or YOUR name) []:Kuwar Pratap Dubey  
Email Address []:47ashutoshdubey@gmail.com
```

```
Please enter the following 'extra' attributes  
to be sent with your certificate request  
A challenge password []:kali  
An optional company name []:IN
```

```
[(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]:IN  
State or Province Name (full name) [Some-State]:Delhi  
Locality Name (eg, city) []:Dehi  
Organization Name (eg, company) [Internet Widgits Pty Ltd]:Mylab  
Organizational Unit Name (eg, section) []:  
Common Name (e.g. server FQDN or YOUR name) []:kali  
Email Address []:
```

```
Please enter the following 'extra' attributes  
to be sent with your certificate request  
A challenge password []:kali  
An optional company name []:kali
```

```
[(kali㉿kali)-~]$ openssl x509 -req -days 365 -in myrequest.csr -signkey myprivate.key -out mycertificate.crt  
Certificate request self-signature ok  
subject=C=IN, ST=Delhi, L=Dehi, O=Mylab, CN=kali
```

```
[(kali㉿kali)-~]$
```

```
File Actions Edit View Help
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_mdd6.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*****RM♦y^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_mdd6.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)-[~]
└─$
```

File Machine View Input Devices Help



kali@kali: ~

```
(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.

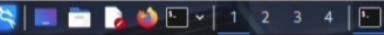
(kali㉿kali)-[~]
$ ls -l myprivate.key
-rw——— 1 kali kali 1704 Sep 11 20:26 myprivate.key

(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]:Google
Organizational Unit Name (eg, section) []:A
Common Name (e.g. server FQDN or YOUR name) []:Kumar Pratap Dubey
Email Address []:47ashutoshdubey@gmail.com

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:kali
An optional company name []:IN

(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]:IN
State or Province Name (full name) [Some-State]:Delhi
Locality Name (eg, city) []:
```

File Machine View Input Devices Help



kali㉿kali: ~

Not After : Sep 11 15:06:35 2026 GMT
Subject: C=IN, ST=Delhi, L=Dehi, O=Mylab, CN=kali
Subject Public Key Info:
 Public Key Algorithm: rsaEncryption
 Public-Key: (2048 bit)
 Modulus:
 00:e1:eb:db:51:9d:f6:f5:fc:68:6b:f6:c4:37:0c:
 53:ad:be:18:af:48:87:0c:d3:49:dd:f2:27:88:40:
 f8:8f:6c:fb:59:70:18:eb:dc:0e:36:e2:40:7f:61:
 ee:73:6c:e7:22:c7:80:fb:f2:aa:1e:5c:2c:8f:0b:
 60:03:58:22:5a:23:ec:5a:b8:74:30:18:54:fa:ca:
 42:7b:9d:4c:fd:a7:b6:f6:cfc:ea:ea:e5:e0:60:4f:
 7f:db:67:91:fa:f3:b3:ff:3b:9e:c5:df:72:bb:ac:
 c3:6d:73:03:29:ac:0c:d4:97:a2:e1:b0:6a:d0:24:
 27:06:f8:4c:2a:db:70:65:e9:9b:33:d3:34:51:0f:
 66:93:fc:41:31:23:a3:13:80:a0:d9:5a:1d:85:dd:
 3a:c3:26:d9:24:e2:eb:0f:91:d8:dc:6d:e6:89:51:
 fe:ab:c5:dc:02:e7:db:99:89:c4:49:59:d2:67:7e:
 c2:af:d5:0f:ac:20:f3:c5:eb:75:02:ea:6c:74:b7:
 9c:4f:6e:50:7a:55:35:4f:ac:18:22:4f:1f:60:b6:
 11:e9:64:a2:75:61:8e:e7:b9:d1:f1:ca:21:fe:e5:
 3a:1e:ad:87:a4:e5:30:a5:f3:fb:8a:4e:41:39:d3:
 a0:0c:2b:37:e0:56:aa:96:83:41:8f:5c:95:24:a7:
 a4:c1
 Exponent: 65537 (0x10001)

X509v3 extensions:

X509v3 Subject Key Identifier:

EC:9F:9C:A0:58:DD:21:AD:A8:30:92:DA:9B:9A:F6:67:29:88:6F:29

Signature Algorithm: sha256WithRSAEncryption

Signature Value:

45:42:32:5c:9b:e3:49:1e:7f:dd:a8:69:54:7c:87:ff:56:0f:
00:c6:24:21:39:2f:a0:01:69:70:aa:69:2b:9d:bb:55:dc:3b:
f0:79:57:ta:2:c9:6a:fd:18:79:e1:20:d5:81:60:43:45:09:f2:
6f:df:bd:7a:95:14:b0:a8:88:b0:ea:e7:51:b7:ec:6e:36:54:44:
6f:0d:61:75:fc:e4:e0:25:06:3e:5d:03:3d:9c:57:43:9a:53:
0f:68:c1:94:3b:ed:83:12:83:09:d1:8b:89:c5:cd:ce:e1:2a:
da:98:83:54:61:71:25:19:a8:91:de:ae:99:2e:30:64:17:e1:
32:aa:0d:bd:e5:83:31:c3:76:e1:dc:19:22:5e:5a:18:d4:df:
60:e7:e0:0d:03:c0:1a:77:23:aa:c6:1e:66:00:6a:39:5a:dc:
04:45:b5:3f:57:df:22:87:e2:e0:9d:6f:fd:da:73:95:81:aa:
c8:13:b5:b8:d1:2e:66:64:62:77:87:e6:f2:52:17:2e:0b:b8:1f:
f2:f5:06:95:39:76:12:dc:63:bd:e7:45:4c:cd:1:0:c0:11:d5:
45:bd:3f:61:e7:c6:78:77:8c:fced:46:i3:c3:f7:3e:22:02:
8d:73:a0:f9:8f:79:a5:c8:ec:ee:b4:b8:16:8e:84:c5:ac:00:
03:84:98:3b

(kali㉿kali)-[~]\$ rm -f myprivate.key myrequest.csr mycertificate.crt

(kali㉿kali)-[~]\$

File Machine Help



New Group 1



Details

General

Name: Kali Linux
Operating System: Debian (64-bit)
Groups: New Group 1

System

Base Memory: 4194 MB
Processors: 5
Boot Order: Floppy, Optical, Hard Disk
Acceleration: Nested Paging, KVM Paravirtualization

Display

Video Memory: 128 MB
Graphics Controller: VMSVGA
Remote Desktop Server Port: 3389
Recording: Disabled

Storage

Controller: IDE
IDE Primary Device 0: [Optical Drive] Empty
Controller: SATA
SATA Port 0: Kali Linux.vdi (Normal, 120.26 GB)

Audio

Host Driver: Default
Controller: ICH AC97

Network

Adapter 1: Intel PRO/1000 MT Desktop (Host-only Adapter, 'VirtualBox Host-Only Ethernet Adapter')
Adapter 2: Intel PRO/1000 MT Desktop (NAT)

USB

USB Controller: OHCI, EHCI
Device Filters: 0 (0 active)

Shared folders

None

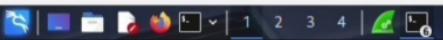
Description

None

Preview



File Machine View Input Devices Help



kali@kali: ~

17:38

```
(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
;; 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
[sudo] password for kali:
Sorry, try again.
[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
```

