Experiment No. 1

Substitution/monoalphabetic:

```
def main():

   str1 = input("Enter string :")

   lst =

[ 'a','b','c','d','e','f','g','h','i','j','k','l','m','n','o','p','q','r','s','t','u','v','w','x','y','z','A','B','C','D','E','F','
G','H','I','J','K','L','M','N','O','P','Q','R','S','T','U','V','W','X','Y','Z']

   shift = int(input("Enter shift :")) # shift is the number of positions to shift the character usually 3
result = ""

    # loops through the string.

   for char in str1:

      # checks if the character is in the list        if char in lst:

         # shifts the character by the number of positions           result = result + lst[(lst.index(char) +
shift)]      else:

         result = result + char     print("Encrypted string is : ", result)     print("Decrypted string is : ", str1) if
__name___== "__main__":

main()
```

Output:

```
Enter string :ravi

Enter shift :4

Encrypted string is :  vezm

Decrypted string is :  ravi
```

Polyalphabetic/Transposition:

```
def generate_key(plaintext, key):     key = list(key)

 if len(plaintext) == len(key):

      return key     else:

      for i in range(len(plaintext) - len(key)):

         key.append(key[i % len(key)])     return "".join(key)
```

```
def vigenere_encrypt(plaintext, key):     key = generate_key(plaintext, key)     ciphertext = []


    for i in range(len(plaintext)):
        char = plaintext[i]
 if char.isalpha():  # Only process alphabetic characters
 shift = ord(key[i].lower()) - ord('a')
 if char.islower():
                encrypted_char = chr((ord(char) - ord('a') + shift) % 26 + ord('a'))
            else:
                encrypted_char = chr((ord(char) - ord('A') + shift) % 26 + ord('A'))
ciphertext.append(encrypted_char)
        else:
            ciphertext.append(char)
    return "".join(ciphertext)


plaintext = "Hello World!" key = "RAVI"
ciphertext = vigenere_encrypt(plaintext, key) print("Ciphertext:", ciphertext)
```

Output:

```
Ciphertext: Yegtf Rwily!
```

Experiment No. 2

```
import random

from math import gcd


def power(base, expo, mod):

res = 1

base = base % mod

while expo > 0:

if expo & 1:

res = (res * base) % mod

base = (base * base) % mod

expo //= 2

return res


def compute_d(e, phi):

k = 1

while True:

d = ((k * phi) + 1) / e

if d.is_integer():

return int(d)

k += 1


def is_prime(n):

if n < 2:

return False

for i in range(2, int(n ** 0.5) + 1):

if n % i == 0:

return False
return True


def generate_keys(p, q, e):
if not (is_prime(p) and is_prime(q) and p != q):
raise ValueError("Both numbers must be prime and distinct.")
n = p * q
phi = (p - 1) * (q - 1)
if gcd(e, phi) != 1:
raise ValueError("e must be coprime to phi(n)")
d = compute_d(e, phi)
return e, d, n


def encrypt(message, e, n):
return power(message, e, n)


def decrypt(ciphertext, d, n):
return power(ciphertext, d, n)


if __name___== "__main__":
try:
p = int(input("Enter a prime number (p): "))
q = int(input("Enter another prime number (q): "))
e = int(input("Enter a value for e (must be coprime with phi(n)): "))

e, d, n = generate_keys(p, q, e)
print(f"Public Key (e, n): ({e}, {n})")
print(f"Private Key (d, n): ({d}, {n})")

M = int(input("Enter a number to encrypt: "))
```

```
C = encrypt(M, e, n)
print(f"Encrypted Message: {C}")
decrypted = decrypt(C, d, n)
print(f"Decrypted Message: {decrypted}")
except ValueError as ve:
print(f"Error: {ve}")
```

Output:-

1]

```
Enter a prime number (p): 7
Enter another prime number (q): 11
Enter a value for e (must be coprime with phi(n)): 17
Public Key (e, n): (17, 77)
Private Key (d, n): (53, 77)
Enter a number to encrypt: 31
Encrypted Message: 26
Decrypted Message: 31
```

2]

```
Enter a prime number (p): 61
Enter another prime number (q): 53
Enter a value for e (must be coprime with phi(n)): 17
Public Key (e, n): (17, 3233)
Private Key (d, n): (2753, 3233)
Enter a number to encrypt: 345
Encrypted Message: 2350
Decrypted Message: 345
```

Experiment No.3

DH algo:-

```
import random

def mod_exp(base, exponent, mod):
return pow(base, exponent, mod)

# User input for prime number and primitive root
p = int(input("Enter a prime number (p): "))
g = int(input("Enter a primitive root (g): "))

# User input for private keys
a = int(input("Enter Alice's private key: "))
b = int(input("Enter Bob's private key: "))

# Compute public keys
A = mod_exp(g, a, p) # A = g^a mod p
B = mod_exp(g, b, p) # B = g^b mod p

# Compute the shared secret key
shared_secret_Alice = mod_exp(B, a, p) # (B^a) mod p
shared_secret_Bob = mod_exp(A, b, p) # (A^b) mod p

# The shared secret should be the same for both
assert shared_secret_Alice == shared_secret_Bob

# Print results
print(f"\nPublic Parameters: p={p}, g={g}")
print(f"Alice's Private Key: {a}")
print(f"Bob's Private Key: {b}")
print(f"Alice's Public Key: {A}")
print(f"Bob's Public Key: {B}")
print(f"Shared Secret Key: {shared_secret_Alice}")
```

Output:

```
Public Parameters: p=7, g=5
Alice's Private Key: 12
Bob's Private Key: 56
Alice's Public Key: 1
Bob's Public Key: 4
Shared Secret Key: 1
```

Experiment No.4

```
Microsoft Windows [Version 10.0.26100.3194]

(c) Microsoft Corporation. All rights reserved.

C:\Users\saurabhs>nmap --version

Nmap version 7.95 ( https://nmap.org )

Platform: i686-pc-windows-windows

Compiled with: nmap-liblua-5.4.6 openssl-3.0.13 nmap-libssh2-1.11.0 nmap-libz-1.3.1 nmap-libpcre2-
10.43 Npcap-1.79 nmap-libdnet-1.12 ipv6

Compiled without:

Available nsock engines: iocp poll select
```

#Scan Your Own Machine (Localhost)

```
C:\Users\saurabhs>ipconfig

Windows IP Configuration

Wireless LAN adapter Local Area Connection* 1:

Media State . . . . . . . . . . . : Media disconnected

Connection-specific DNS Suffix . :

Wireless LAN adapter Local Area Connection* 2:

Media State . . . . . . . . . . . : Media disconnected

Connection-specific DNS Suffix . :

Wireless LAN adapter Wi-Fi:

Connection-specific DNS Suffix . :

Link-local IPv6 Address . . . . . : fe80::1788:907a:98b4:85bf%6

IPv4 Address. . . . . . . . . . . : 192.168.0.104

Subnet Mask . . . . . . . . . . . : 255.255.255.0

Default Gateway . . . . . . . . . : 192.168.0.1

Ethernet adapter Ethernet:

Media State . . . . . . . . . . . : Media disconnected

Connection-specific DNS Suffix . :
```

#Ping Scan (Check if your device is up)

```
C:\Users\saurabhs>nmap -sn 127.0.0.1

Starting Nmap 7.95 ( https://nmap.org ) at 2025-02-26 11:41 India Standard Time Nmap scan report

for localhost (127.0.0.1)

Host is up.

Nmap done: 1 IP address (1 host up) scanned in 8.62 seconds
```

#TCPPortScan(Check for open TCP ports)

```
C:\Users\saurabhs>nmap -sT 127.0.0.1

Starting Nmap 7.95 ( https://nmap.org ) at 2025-02-26 11:44 India Standard Time Nmap scan report for

localhost (127.0.0.1)

Host is up (0.0029s latency).

Not shown: 997 filtered tcp ports (no-response) PORT STATE SERVICE

135/tcp open msrpc

445/tcp open microsoft-ds 7070/tcp open

realserver

Nmap done: 1 IP address (1 host up) scanned in 14.04 seconds

#UDP Port Scan (Check for open UDP ports)

C:\Users\saurabhs>nmap -sU 127.0.0.1

Starting Nmap 7.95 ( https://nmap.org ) at 2025-02-26 11:45 India Standard Time Nmap scan report for

localhost (127.0.0.1)

Host is up (0.00034s latency).

Not shown: 993 closed udp ports (port-unreach)

PORT STATE SERVICE

123/udp open|filtered ntp 137/udp open|filtered

netbios-ns 1900/udp open|filtered upnp 4500/udp

open|filtered nat-t-ike 5050/udp open|filtered mmcc

5353/udp open|filtered zeroconf5355/udp open|filtered

llmnr

Nmap done: 1 IP address (1 host up) scanned in 182.92

seconds #OS Fingerprinting (Try to detect the operating

system)

C:\>nmap -O 192.168.0.104S

tartingNmap7.95(https://nmap.org ) at 2025-02-26
```

```
5355/udp open|filtered llmnr

Nmap done: 1 IP address (1 host up) scanned in 182.92 seconds

#OS Fingerprinting (Try to detect the operating system)

C:\Users\saurabhs>nmap -O 192.168.0.104

Starting Nmap 7.95 ( https://nmap.org ) at 2025-02-26 11:49 India Standard Time

Nmap scan report for 192.168.0.104

Host is up (0.00037s latency).

Not shown: 996 closed tcp ports (reset)

PORT STATE SERVICE

135/tcp open msrpc

139/tcp open netbios-ssn

445/tcp open microsoft-ds

7070/tcp open realserver

TCP/IP fingerprint:

OS:SCAN(V=7.95%E=4%D=2/26%OT=135%CT=1%CU=32250%PV=Y%DS=0%DC=L%G=Y%TM=67BEB2

OS:7D%P=i686-pc-windows-windows)SEQ(SP=100%GCD=1%ISR=109%TI=I%CI=I%II=I%SS=

OS:S%TS=A)SEQ(SP=101%GCD=1%ISR=10D%TI=I%CI=I%II=I%SS=S%TS=A)SEQ(SP=103%GCD=

OS:1%ISR=10A%TI=I%CI=I%II=I%SS=S%TS=A)SEQ(SP=104%GCD=1%ISR=10B%TI=I%CI=I%II

OS:=I%SS=S%TS=A)SEQ(SP=FC%GCD=1%ISR=10B%TI=I%CI=I%II=I%SS=S%TS=A)OPS(O1=MFF

OS:D7NW8ST11%O2=MFFD7NW8ST11%O3=MFFD7NW8NNT11%O4=MFFD7NW8ST11%O5=MFFD7NW8ST

OS:11%O6=MFFD7ST11)WIN(W1=FFFF%W2=FFFF%W3=FFFF%W4=FFFF%W5=FFFF%W6=FFFF)ECN(

OS:R=Y%DF=Y%T=80%W=FFFF%O=MFFD7NW8NNS%CC=N%Q=)T1(R=Y%DF=Y%T=80%S=O%A=S+%F=A

OS:S%RD=0%Q=)T2(R=Y%DF=Y%T=80%W=0%S=Z%A=S%F=AR%O=%RD=0%Q=)T3(R=Y%DF=Y%T=80%

OS:W=0%S=Z%A=O%F=AR%O=%RD=0%Q=)T4(R=Y%DF=Y%T=80%W=0%S=A%A=O%F=R%O=%RD=0%Q=)

OS:T5(R=Y%DF=Y%T=80%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T6(R=Y%DF=Y%T=80%W=0%S=A%A

OS:=O%F=R%O=%RD=0%Q=)T7(R=Y%DF=Y%T=80%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)U1(R=Y%D

OS:F=N%T=80%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=Z%RUCK=G%RUD=G)IE(R=Y%DFI=N%T=8

OS:0%CD=Z)
```

```
Network Distance: 0 hops

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .

Nmap done: 1 IP address (1 host up) scanned in 21.94 seconds Microsoft Windows [Version 10.0.26100.3194]

(c) Microsoft Corporation. All rights reserved.

C:\Users\saurabhs>nmap -O scanme.nmap.org

Starting Nmap 7.95 ( https://nmap.org ) at 2025-02-26 12:51 India Standard Time

Nmap scan report for scanme.nmap.org (45.33.32.156)

Host is up (0.27s latency).

Not shown: 995 closed tcp ports (reset)

PORT STATE SERVICE

22/tcp open ssh

25/tcp filtered smtp

80/tcp open http

9929/tcp open nping-echo

31337/tcp open Elite

Device type: general purpose|router

Running: Linux 5.X, MikroTik RouterOS 7.X

OS CPE: cpe:/o:linux:linux_kernel:5 cpe:/o:mikrotik:routeros:7 cpe:/o:linux:linux_kernel:5.6.3

OS details: Linux 5.0 - 5.14, MikroTik RouterOS 7.2 - 7.5 (Linux 5.6.3)

Network Distance: 19 hops

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .

Nmap done: 1 IP address (1 host up) scanned in 25.77 seconds

Microsoft Windows [Version 10.0.26100.3194]

(c) Microsoft Corporation. All rights reserved.

# Analyze TTL (Time-To-Live) Values

C:\Windows\System32>ping -c 1 192.168.0.104

Pinging 192.168.0.104 with 32 bytes of data:

Reply from 192.168.0.104: bytes=32 time<1ms TTL=128
Reply from 192.168.0.104: bytes=32 time<1ms TTL=128

Reply from 192.168.0.104: bytes=32 time<1ms TTL=128

Reply from 192.168.0.104: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.0.104:

Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),

Approximate round trip times in milli-seconds:

Minimum = 0ms, Maximum = 0ms, Average = 0ms

#Check Open Ports & Services (-sV)

C:\Users\saurabhs>nmap -sV 192.168.0.104

Starting Nmap 7.95 ( https://nmap.org ) at 2025-02-26 11:50 India Standard Time

Nmap scan report for 192.168.0.104

Host is up (0.00075s latency).

Not shown: 996 closed tcp ports (reset)

PORT STATE SERVICE VERSION

135/tcp open msrpc Microsoft Windows RPC

139/tcp open netbios-ssn Microsoft Windows netbios-ssn

445/tcp open microsoft-ds?

7070/tcp open ssl/realserver?

Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .

Nmap done: 1 IP address (1 host up) scanned in 25.15 seconds

C:\Users\ravis>wmic OS get OSArchitecture

OSArchitecture

64-bit

C:\Users\saurabhs>echo %PROCESSOR_ARCHITECTURE%

AMD64

#Check SMB for Windows OS

C:\Users\saurabhs>nmap --script smb-os-discovery -p 445 192.168.0.104

Starting Nmap 7.95 ( https://nmap.org ) at 2025-02-26 11:53 India Standard Time
```

```
Nmap scan report for 192.168.0.104

Host is up (0.0010s latency).

PORT STATE SERVICE

445/tcp open microsoft-ds
Nmap done: 1 IP address (1 host up) scanned in 9.83 seconds

#Aggressive Scan (Detailed information about the target)

C:\Users\saurabhs>nmap -A 192.168.0.104

Starting Nmap 7.95 ( https://nmap.org ) at 2025-02-26 11:59 India Standard Time

Nmap scan report for 192.168.0.104

Host is up (0.00042s latency).

Not shown: 996 closed tcp ports (reset)

PORT STATE SERVICE VERSION

135/tcp open msrpc Microsoft Windows RPC

139/tcp open netbios-ssn Microsoft Windows netbios-ssn

445/tcp open microsoft-ds?

7070/tcp open ssl/realserver?

|_ssl-date: TLS randomness does not represent time

| ssl-cert: Subject: commonName=AnyDesk Client

| Not valid before: 2025-02-24T13:30:42
|_Not valid after: 2075-02-12T13:30:42

TCP/IP fingerprint:

OS:SCAN(V=7.95%E=4%D=2/26%OT=135%CT=1%CU=30780%PV=Y%DS=0%DC=L%G=Y%TM=67BEB5

OS:06%P=i686-pc-windows-windows)SEQ(SP=100%GCD=1%ISR=10D%TI=I%CI=I%II=I%SS=

OS:S%TS=A)SEQ(SP=101%GCD=1%ISR=106%TI=I%CI=I%II=I%SS=S%TS=A)SEQ(SP=104%GCD=

OS:1%ISR=10D%TI=I%CI=I%II=I%SS=S%TS=A)SEQ(SP=105%GCD=1%ISR=109%TI=I%CI=I%II

OS:=I%SS=S%TS=A)SEQ(SP=107%GCD=1%ISR=10A%TI=I%CI=I%II=I%SS=S%TS=A)OPS(O1=MF

OS:FD7NW8ST11%O2=MFFD7NW8ST11%O3=MFFD7NW8NNT11%O4=MFFD7NW8ST11%O5=MFFD7NW
8S

OS:T11%O6=MFFD7ST11)WIN(W1=FFFF%W2=FFFF%W3=FFFF%W4=FFFF%W5=FFFF%W6=FFFF)ECN
```

```
OS:(R=Y%DF=Y%T=80%W=FFFF%O=MFFD7NW8NNS%CC=N%Q=)T1(R=Y%DF=Y%T=80%S=O%A=S+%F=
OS:AS%RD=0%Q=)T2(R=Y%DF=Y%T=80%W=0%S=Z%A=S%F=AR%O=%RD=0%Q=)T3(R=Y%DF=Y%T=80
OS:%W=0%S=Z%A=O%F=AR%O=%RD=0%Q=)T4(R=Y%DF=Y%T=80%W=0%S=A%A=O%F=R%O=%RD=0%Q
=
OS:)T5(R=Y%DF=Y%T=80%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T6(R=Y%DF=Y%T=80%W=0%S=A%
OS:A=O%F=R%O=%RD=0%Q=)T7(R=Y%DF=Y%T=80%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)U1(R=Y%
OS:DF=N%T=80%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=Z%RUCK=G%RUD=G)IE(R=Y%DFI=N%T=
OS:80%CD=Z)
Network Distance: 0 hops
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows
Host script results:
| smb2-time:
| date: 2025-02-26T06:30:17
|_ start_date: N/A
| smb2-security-mode:
| 3:1:1:
|_ Message signing enabled but not required
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 47.64 seconds
```

```
C:\Users\saurabhs>nmap -A 127.0.0.1 -oN nmap_results.txt
Starting Nmap 7.95 ( https://nmap.org ) at 2025-02-26 12:01 India Standard Time
Nmap scan report for localhost (127.0.0.1)
Host is up (0.00043s latency).
Not shown: 997 closed tcp ports (reset)
PORT STATE SERVICE VERSION
135/tcp open msrpc Microsoft Windows RPC
445/tcp open microsoft-ds?
7070/tcp open ssl/realserver?
| ssl-cert: Subject: commonName=AnyDesk Client
| Not valid before: 2025-02-24T13:30:42
|_Not valid after: 2075-02-12T13:30:42
|_ssl-date: TLS randomness does not represent time
TCP/IP fingerprint:
OS:SCAN(V=7.95%E=4%D=2/26%OT=135%CT=1%CU=34519%PV=N%DS=0%DC=L%G=Y%TM=67BEB5
OS:75%P=i686-pc-windows-windows)SEQ(SP=102%GCD=1%ISR=106%TI=I%CI=I%II=I%SS=
OS:S%TS=A)SEQ(SP=104%GCD=1%ISR=109%TI=I%CI=I%II=I%SS=S%TS=A)SEQ(SP=104%GCD=
OS:3%ISR=10A%TI=I%CI=I%II=I%SS=S%TS=A)SEQ(SP=105%GCD=1%ISR=10A%TI=I%CI=I%II
OS:=I%SS=S%TS=A)OPS(O1=MFFD7NW8ST11%O2=MFFD7NW8ST11%O3=MFFD7NW8NNT11%O4=MFF
OS:D7NW8ST11%O5=MFFD7NW8ST11%O6=MFFD7ST11)WIN(W1=FFFF%W2=FFFF%W3=FFFF%W4=FF
OS:FF%W5=FFFF%W6=FFFF)ECN(R=Y%DF=Y%T=80%W=FFFF%O=MFFD7NW8NNS%CC=N%Q=)T1(R=Y
OS:%DF=Y%T=80%S=O%A=S+%F=AS%RD=0%Q=)T2(R=Y%DF=Y%T=80%W=0%S=Z%A=S%F=AR%O=%RD
OS:=0%Q=)T3(R=Y%DF=Y%T=80%W=0%S=Z%A=O%F=AR%O=%RD=0%Q=)T4(R=Y%DF=Y%T=80%W=0%
OS:S=A%A=O%F=R%O=%RD=0%Q=)T5(R=Y%DF=Y%T=80%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T6(
OS:R=Y%DF=Y%T=80%W=0%S=A%A=O%F=R%O=%RD=0%Q=)T7(R=Y%DF=Y%T=80%W=0%S=Z%A=S+%F
OS:=AR%O=%RD=0%Q=)U1(R=Y%DF=N%T=80%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=Z%RUCK=G
OS:%RUD=G)IE(R=Y%DFI=N%T=80%CD=Z)
Network Distance: 0 hops
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows
Host script results:
| smb2-security-mode:
| 3:1:1:
|_ Message signing enabled but not required
| smb2-time:
| date: 2025-02-26T06:32:08
|_ start_date: N/A
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 45.11 seconds
C:\Users\saurabhs>
```

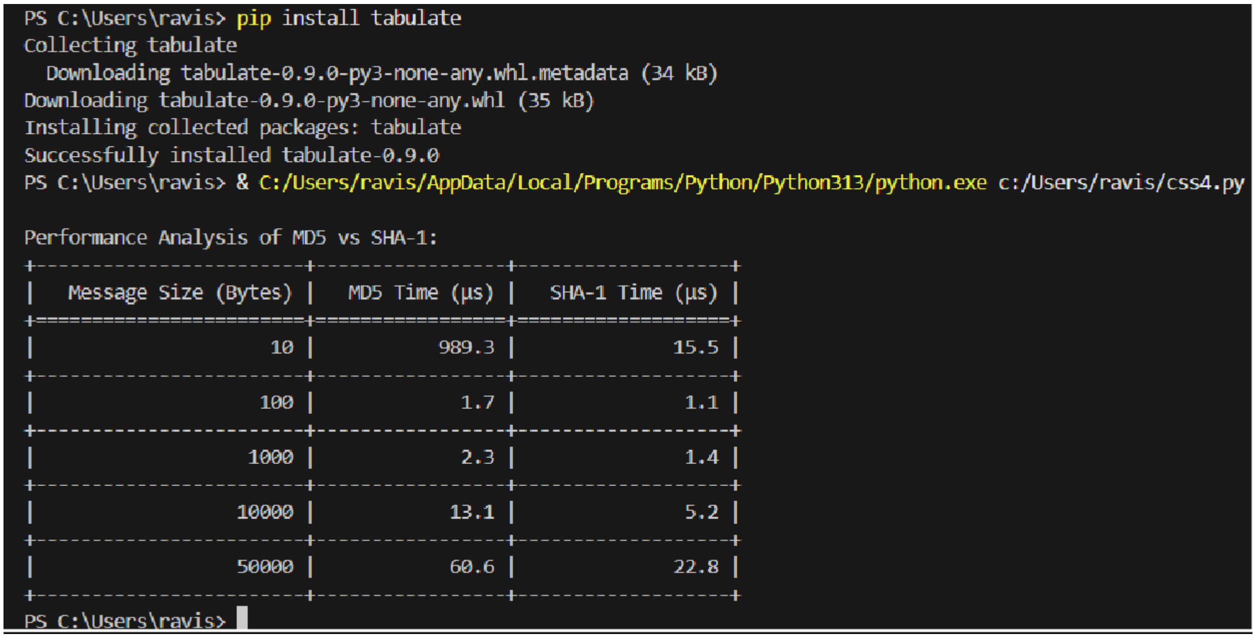
Experiment No. 5

Md5 Sha1 Performance :

```
import hashlib
import time
import random
import string
from tabulate import tabulate
def generate_random_message(size):
return ''.join(random.choices(string.ascii_letters + string.digits, k=size)).encode()
def hash_message(algorithm, message):
start_time = time.perf_counter()
hash_obj = hashlib.new(algorithm)
hash_obj.update(message)
digest = hash_obj.hexdigest()
end_time = time.perf_counter()
return digest, (end_time - start_time) * 1e6 # Convert to microseconds
def main():
sizes = [10, 100, 1000, 10000, 50000] # Different message sizes
results = []
for size in sizes:
message = generate_random_message(size)
md5_digest, md5_time = hash_message('md5', message)
sha1_digest, sha1_time = hash_message('sha1', message)
results.append([size, md5_time, sha1_time])
print("\nPerformance Analysis of MD5 vs SHA-1:")
print(tabulate(results, headers=["Message Size (Bytes)", "MD5 Time (µs)", "SHA-1 Time (µs)"],
tablefmt="grid"))
```

```
if __name___== "__main__":

main()
```

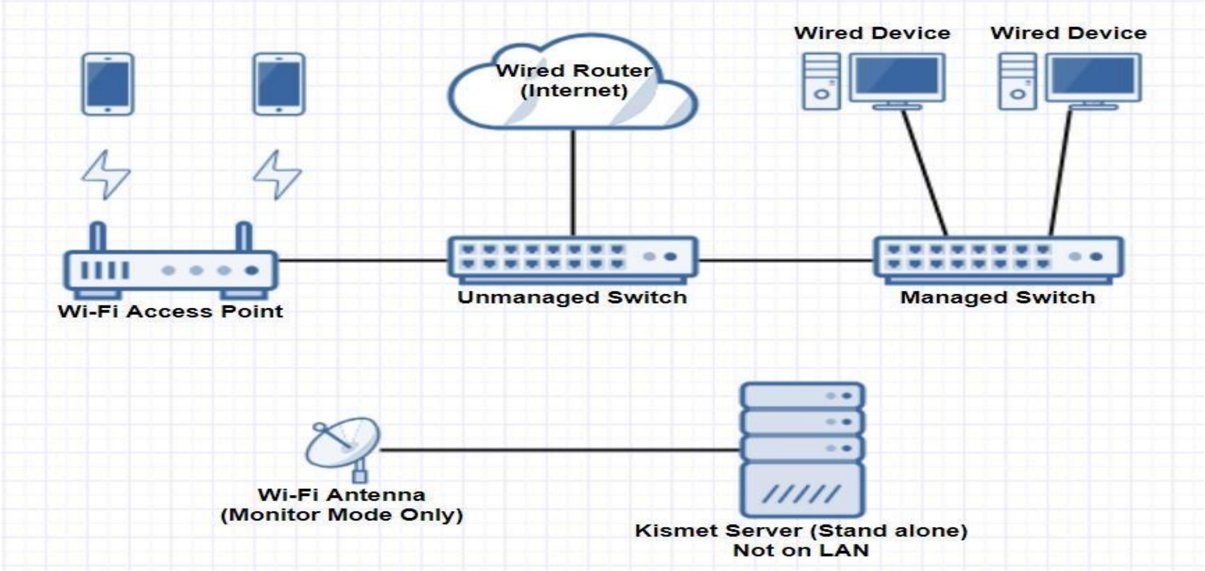
output:-



```
PS C:\Users\ravis> pip install tabulate
Collecting tabulate
  Downloading tabulate-0.9.0-py3-none-any.whl.metadata (34 kB)
Downloading tabulate-0.9.0-py3-none-any.whl (35 kB)
Installing collected packages: tabulate
Successfully installed tabulate-0.9.0
PS C:\Users\ravis> & C:/Users/ravis/AppData/Local/Programs/Python/Python313/python.exe c:/Users/ravis/css4.py

Performance Analysis of MD5 vs SHA-1:
+------------------------+-----------------+-------------------+
|   Message Size (Bytes) |   MD5 Time (µs) |   SHA-1 Time (µs) |
+========================+=================+===================+
|                     10 |           989.3 |              15.5 |
+------------------------+-----------------+-------------------+
|                    100 |             1.7 |               1.1 |
+------------------------+-----------------+-------------------+
|                   1000 |             2.3 |               1.4 |
+------------------------+-----------------+-------------------+
|                  10000 |            13.1 |               5.2 |
+------------------------+-----------------+-------------------+
|                  50000 |            60.6 |              22.8 |
+------------------------+-----------------+-------------------+
PS C:\Users\ravis> 
```

Experiment No.6

Image:



architecture.

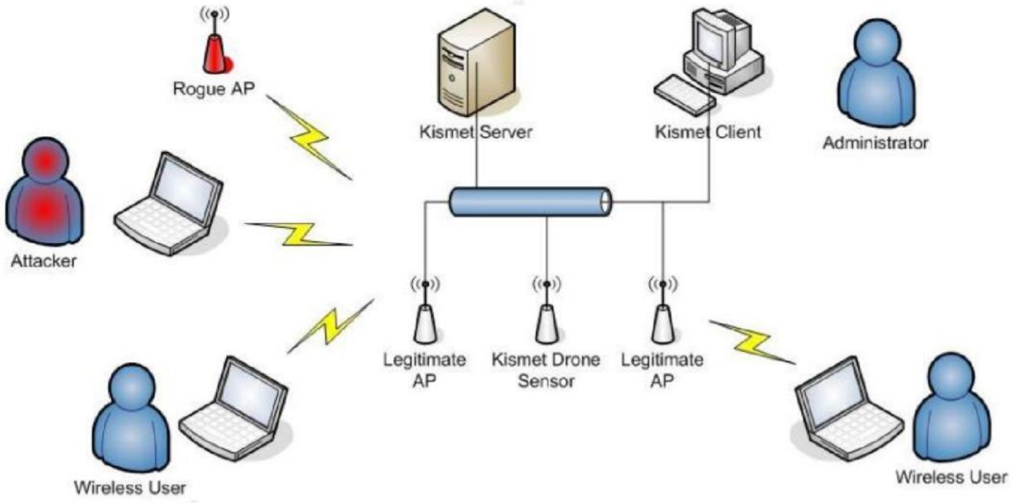
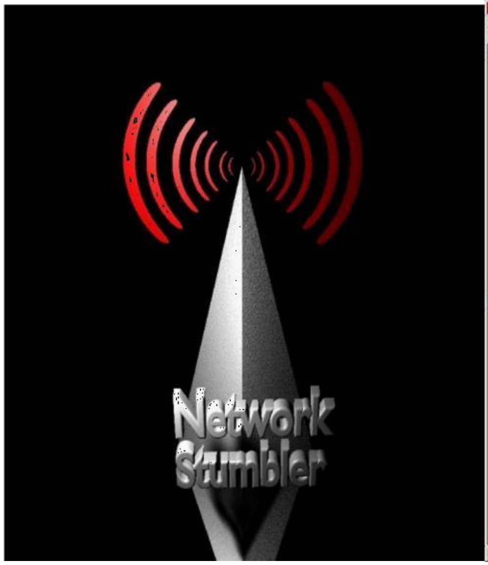
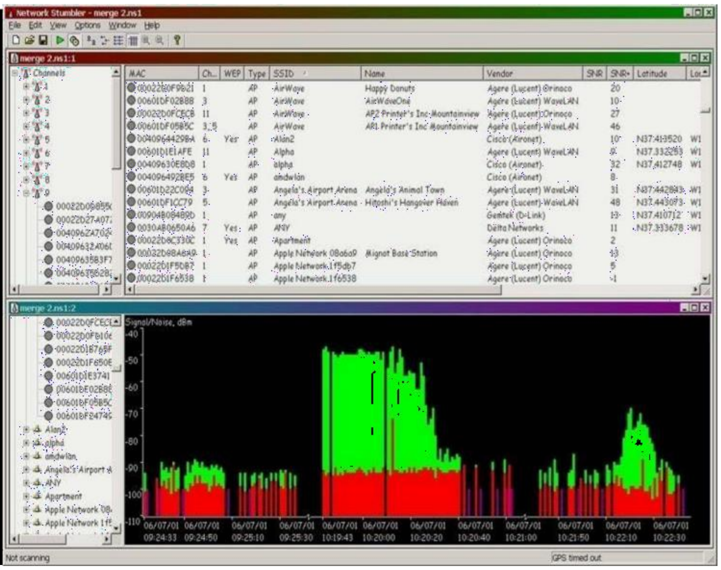


Figure 1 - OpenWRT Kismet IDS Architecture

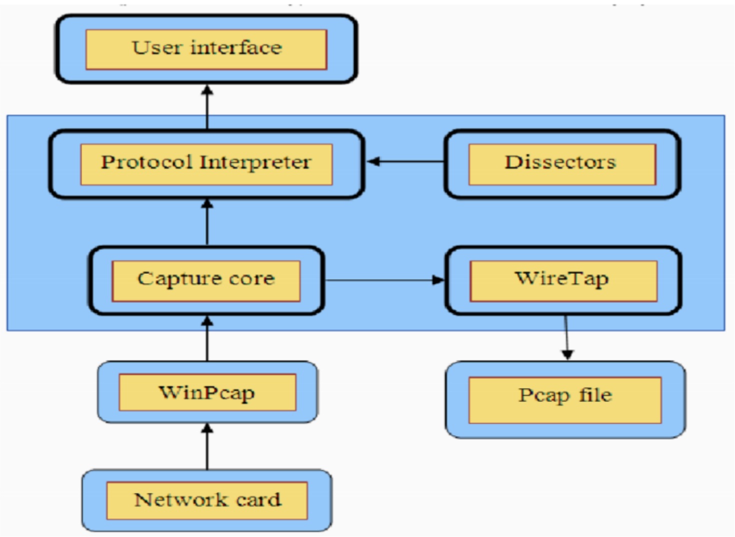


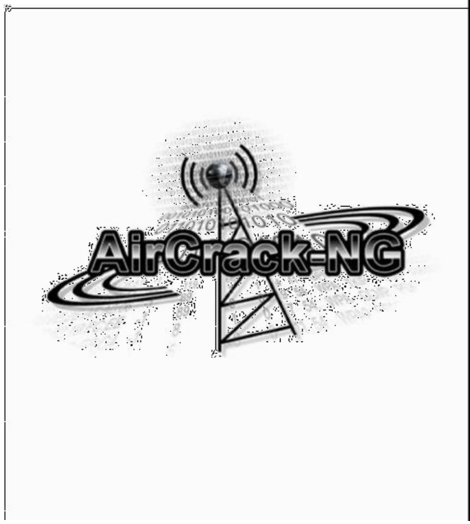


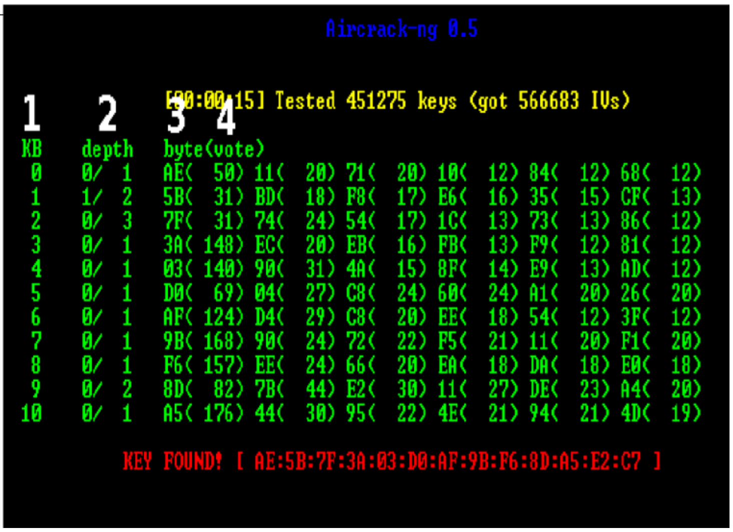
MAC	Ch...	WEP	Type	SSID	Name	Vendor	SNR	SNR+	Latitude	Lo...
00022D0F9B21	1		AP	AirWave	Happy Donuts	Agere (Lucent) Orinoco		20		
00601DF02888	3		AP	AirWave	AirWaveOne	Agere (Lucent) WaveLAN		10		
00022D0FCECB	11		AP	AirWave	AP2 Printer's Inc Mountainview	Agere (Lucent) Orinoco		27		
00601DF05B5C	3, 5		AP	AirWave	AP1 Printer's Inc Mountainview	Agere (Lucent) WaveLAN		46		
00409644298A	6	Yes	AP	Alan2		Cisco (Aironet)		10	N37.413520	W1
00601D1E1AFE	11		AP	Alpha		Agere (Lucent) WaveLAN		9	N37.332253	W1
00409630E8D8	1		AP	alpha		Cisco (Aironet)		32	N37.412748	W1
004096492BE5	6	Yes	AP	andwlan		Cisco (Aironet)		8		
00601D22C094	3		AP	Angela's Airport Arena	Angela's Animal Town	Agere (Lucent) WaveLAN		31	N37.442843	W1
00601DF1CC79	5		AP	Angela's Airport Arena	Hitoshi's Hangover Haven	Agere (Lucent) WaveLAN		48	N37.443073	W1
00904B08489D	1		AP	any		Gemtek (D-Link)		13	N37.410712	W1
0030AB0650A6	7	Yes	AP	ANY		Delta Networks		11	N37.333678	W1
00022D8C330C	1	Yes	AP	Apartment		Agere (Lucent) Orinoco		2		
00022D8BA6A9	1		AP	Apple Network 08a6a9	Mignot Base Station	Agere (Lucent) Orinoco		13		
00022D1F5DB7	1		AP	Apple Network 1f5db7		Agere (Lucent) Orinoco		5		
00022D1F6538	1		AP	Apple Network 1f6538		Agere (Lucent) Orinoco		-1		

```
Channels
  1
  2
  3
  4
  5
  6
  7
  8
  9
    00022D06855
    00022D27A07
    0040962A702
    00409632A06
    004096358F7
    00409635628
```

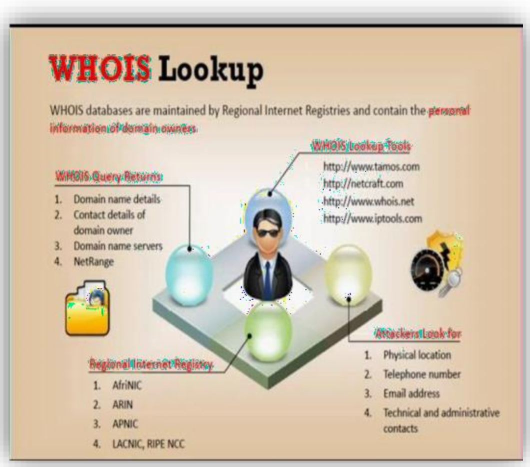
```
    00022D0FCEC
    00022D0FB10
    00022D1B765F
    00022D1F650E
    00601D1E3741
    00601DE02B8
    00601DF05B5C
    00601DF2474
  Alan2
  alpha
  andwlan
  Angela's Airport A
  ANY
  Apartment
  Apple Network 08
  Apple Network 1f
```







```
                          Aircrack-ng 0.5


                 [00:00:15] Tested 451275 keys (got 566683 IVs)

KB    depth   byte(vote)
 0    0/  1   AE(  50) 11(  20) 71(  20) 10(  12) 84(  12) 68(  12)
 1    1/  2   5B(  31) BD(  18) F8(  17) E6(  16) 35(  15) CF(  13)
 2    0/  3   7F(  31) 74(  24) 54(  17) 1C(  13) 73(  13) 86(  12)
 3    0/  1   3A( 148) EC(  20) EB(  16) FB(  13) F9(  12) 81(  12)
 4    0/  1   03( 140) 90(  31) 4A(  15) 8F(  14) E9(  13) AD(  12)
 5    0/  1   D0(  69) 04(  27) C8(  24) 60(  24) A1(  20) 26(  20)
 6    0/  1   AF( 124) D4(  29) C8(  20) EE(  18) 54(  12) 3F(  12)
 7    0/  1   9B( 168) 90(  24) 72(  22) F5(  21) 11(  20) F1(  20)
 8    0/  1   F6( 157) EE(  24) 66(  20) EA(  18) DA(  18) E0(  18)
 9    0/  2   8D(  82) 7B(  44) E2(  30) 11(  27) DE(  23) A4(  20)
10    0/  1   A5( 176) 44(  30) 95(  22) 4E(  21) 94(  21) 4D(  19)

             KEY FOUND! [ AE:5B:7F:3A:03:D0:AF:9B:F6:8D:A5:E2:C7 ]
```



WHOIS Lookup

WHOIS databases are maintained by Regional Internet Registries and contain the personal information of domain owners

WHOIS Query Returns

1. Domain name details
2. Contact details of domain owner
3. Domain name servers
4. NetRange

WHOIS Lookup Tools

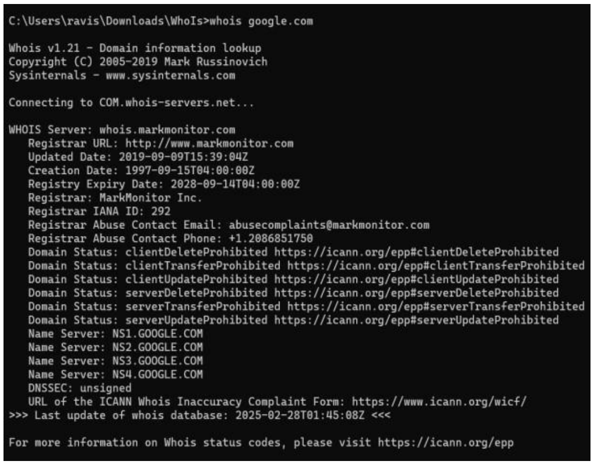
http://www.tamos.com
http://netcraft.com
http://www.whois.net
http://www.iptools.com

Regional Internet Registry

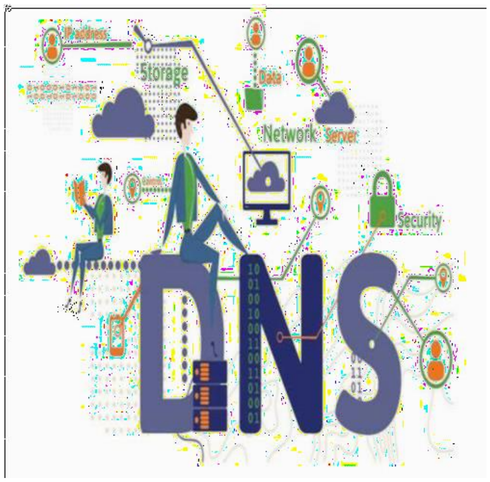
1. AfriNIC
2. ARIN
3. APNIC
4. LACNIC, RIPE NCC

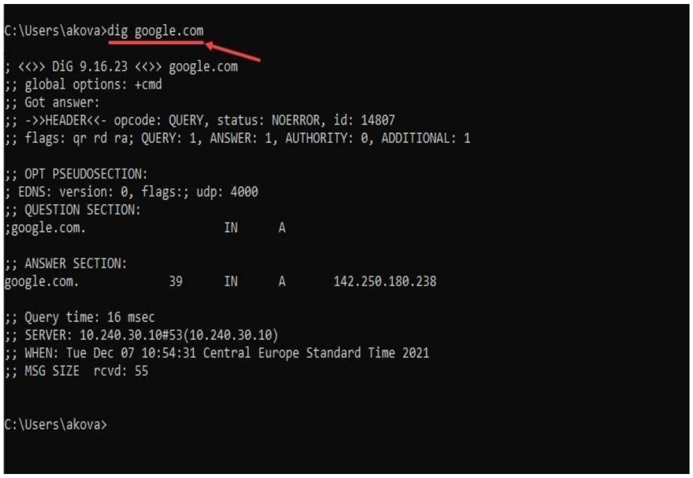
Attackers Look for

1. Physical location
2. Telephone number
3. Email address
4. Technical and administrative contacts

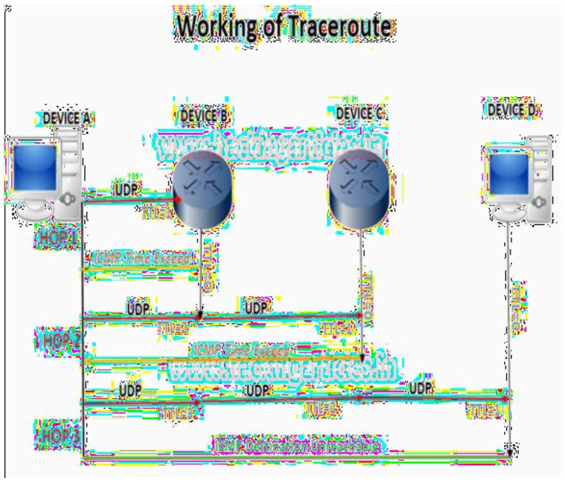


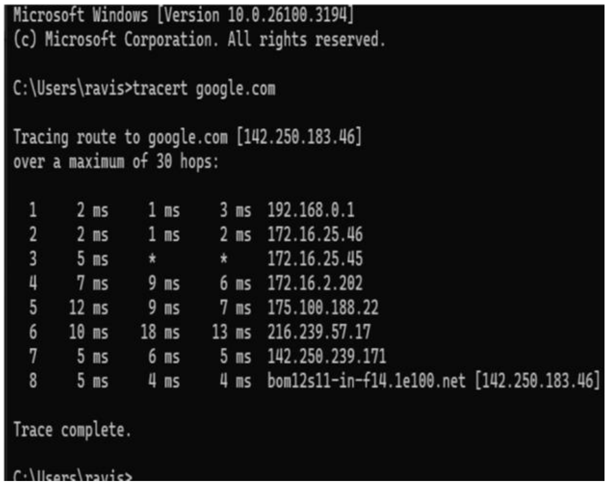
```
C:\Users\ravis\Downloads\WhoIs>whois google.com

Whois v1.21 - Domain information lookup
Copyright (C) 2005-2019 Mark Russinovich
Sysinternals - www.sysinternals.com

Connecting to COM.whois-servers.net...

WHOIS Server: whois.markmonitor.com
   Registrar URL: http://www.markmonitor.com
   Updated Date: 2019-09-09T15:39:04Z
   Creation Date: 1997-09-15T04:00:00Z
   Registry Expiry Date: 2028-09-14T04:00:00Z
   Registrar: MarkMonitor Inc.
   Registrar IANA ID: 292
   Registrar Abuse Contact Email: abusecomplaints@markmonitor.com
   Registrar Abuse Contact Phone: +1.2086851750
   Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited
   Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
   Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited
   Domain Status: serverDeleteProhibited https://icann.org/epp#serverDeleteProhibited
   Domain Status: serverTransferProhibited https://icann.org/epp#serverTransferProhibited
   Domain Status: serverUpdateProhibited https://icann.org/epp#serverUpdateProhibited
   Name Server: NS1.GOOGLE.COM
   Name Server: NS2.GOOGLE.COM
   Name Server: NS3.GOOGLE.COM
   Name Server: NS4.GOOGLE.COM
   DNSSEC: unsigned
   URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
>>> Last update of whois database: 2025-02-28T01:45:08Z <<<

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



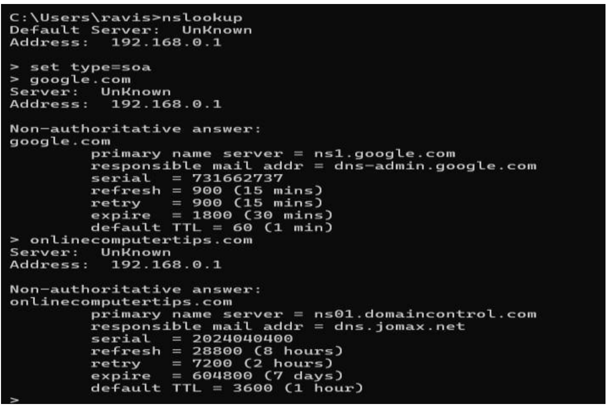


```
C:\Users\akova>dig google.com

; <<>> DiG 9.16.23 <<>> google.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 14807
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4000
;; QUESTION SECTION:
;google.com.                    IN      A

;; ANSWER SECTION:
google.com.             39      IN      A       142.250.180.238

;; Query time: 16 msec
;; SERVER: 10.240.30.10#53(10.240.30.10)
;; WHEN: Tue Dec 07 10:54:31 Central Europe Standard Time 2021
;; MSG SIZE  rcvd: 55


C:\Users\akova>
```





```
Microsoft Windows [Version 10.0.26100.3194]
(c) Microsoft Corporation. All rights reserved.

C:\Users\ravis>tracert google.com

Tracing route to google.com [142.250.183.46]
over a maximum of 30 hops:

  1     2 ms     1 ms     3 ms  192.168.0.1
  2     2 ms     1 ms     2 ms  172.16.25.46
  3     5 ms     *        *     172.16.25.45
  4     7 ms     9 ms     6 ms  172.16.2.202
  5    12 ms     9 ms     7 ms  175.100.188.22
  6    10 ms    18 ms    13 ms  216.239.57.17
  7     5 ms     6 ms     5 ms  142.250.239.171
  8     5 ms     4 ms     4 ms  bom12s11-in-f14.1e100.net [142.250.183.46]

Trace complete.

C:\Users\ravis>
```



```
C:\Users\ravis>nslookup
Default Server:  UnKnown
Address:  192.168.0.1

> set type=soa
> google.com
Server:  UnKnown
Address:  192.168.0.1

Non-authoritative answer:
google.com
        primary name server = ns1.google.com
        responsible mail addr = dns-admin.google.com
        serial  = 731662737
        refresh = 900 (15 mins)
        retry   = 900 (15 mins)
        expire  = 1800 (30 mins)
        default TTL = 60 (1 min)
> onlinecomputertips.com
Server:  UnKnown
Address:  192.168.0.1

Non-authoritative answer:
onlinecomputertips.com
        primary name server = ns01.domaincontrol.com
        responsible mail addr = dns.jomax.net
        serial  = 2024040400
        refresh = 28800 (8 hours)
        retry   = 7200 (2 hours)
        expire  = 604800 (7 days)
        default TTL = 3600 (1 hour)
>
```

Experiment No. 9

#ARP spoofing with nmap:

```
Microsoft Windows [Version 10.0.26100.3194]
(c) Microsoft Corporation. All rights reserved.

C:\Users\ravis>nmap  --version
Nmap version 7.95 ( https://nmap.org )
Platform: i686-pc-windows-windows
Compiled with: nmap-liblua-5.4.6 openssl-3.0.13 nmap-libssh2-1.11.0 nmap-libz-1.3.1
nmaplibpcre210.43 Npcap-1.79 nmap-libdnet-1.12 ipv6  Compiled without:
Available nsock engines: iocp poll select

C:\Users\ravis>ipconfig
Windows IP Configuration
Wireless LAN adapter Local Area Connection* 1:
Media State . . . . . . . . . . . : Media disconnected    Connection-specific
DNS Suffix  . :
Wireless LAN adapter Local Area Connection* 2:
Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :
Wireless LAN adapter Wi-Fi:
   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::1788:907a:98b4:85bf%6
   IPv4 Address. . . . . . . . . . . : 192.168.0.104    Subnet Mask . . . . . . . . . . . : 255.255.255.0    Default
Gateway . . . . . . . . . : 192.168.0.1
Ethernet adapter Ethernet:
   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :
```

#ARP spoofing

```
C:\Windows\System32>nmap -sn 192.168.0.0/24
Starting Nmap 7.95 ( https://nmap.org ) at 2025-03-01 14:06 India Standard Time
Nmap scan report for 192.168.0.1
```

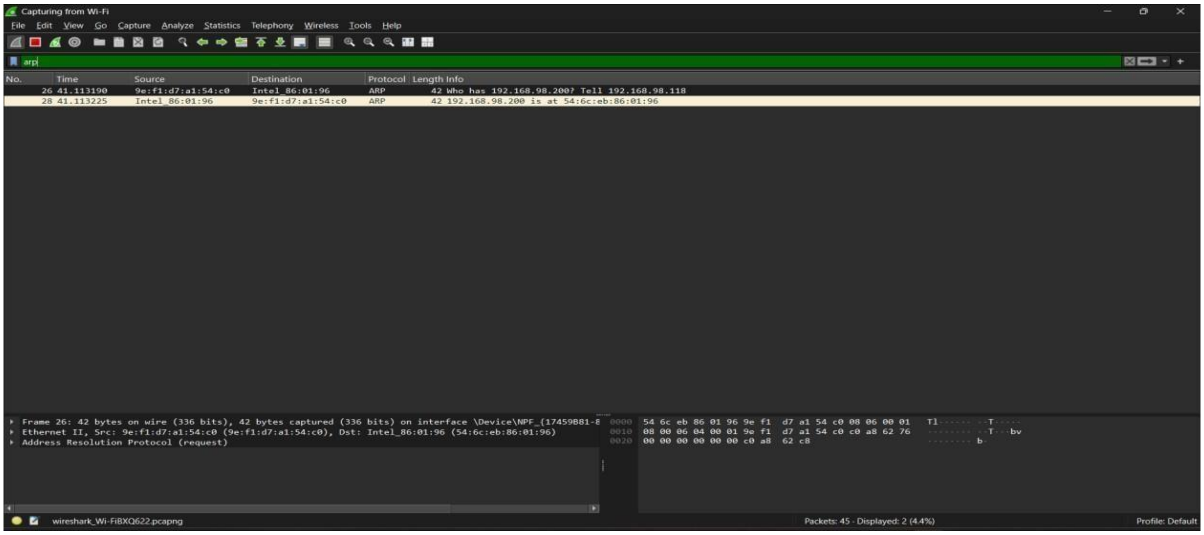
```
Host is up (0.0083s latency).
MAC Address: E8:48:B8:58:AE:18 (TP-Link Limited)
Nmap scan report for 192.168.0.100
Host is up (0.0086s latency).
MAC Address: EC:C8:9C:91:DE:A7 (Hangzhou Hikvision Digital Technology)
Nmap scan report for 192.168.0.104
Host is up.
Nmap done: 256 IP addresses (3 hosts up) scanned in 13.11 seconds
```

#ARP spoofing command

```
C:\Users\ravis>arp -a
Interface: 192.168.0.104 --- 0x6
  Internet Address      Physical Address      Type
  192.168.0.1           e8-48-b8-58-ae-18     dynamic
  192.168.0.255         ff-ff-ff-ff-ff-ff     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.251           01-00-5e-00-00-fb     static
  224.0.0.252           01-00-5e-00-00-fc     static
  239.255.102.18        01-00-5e-7f-66-12     static
239.255.255.250         01-00-5e-7f-ff-fa     static
  255.255.255.255       ff-ff-ff-ff-ff-ff     static
```

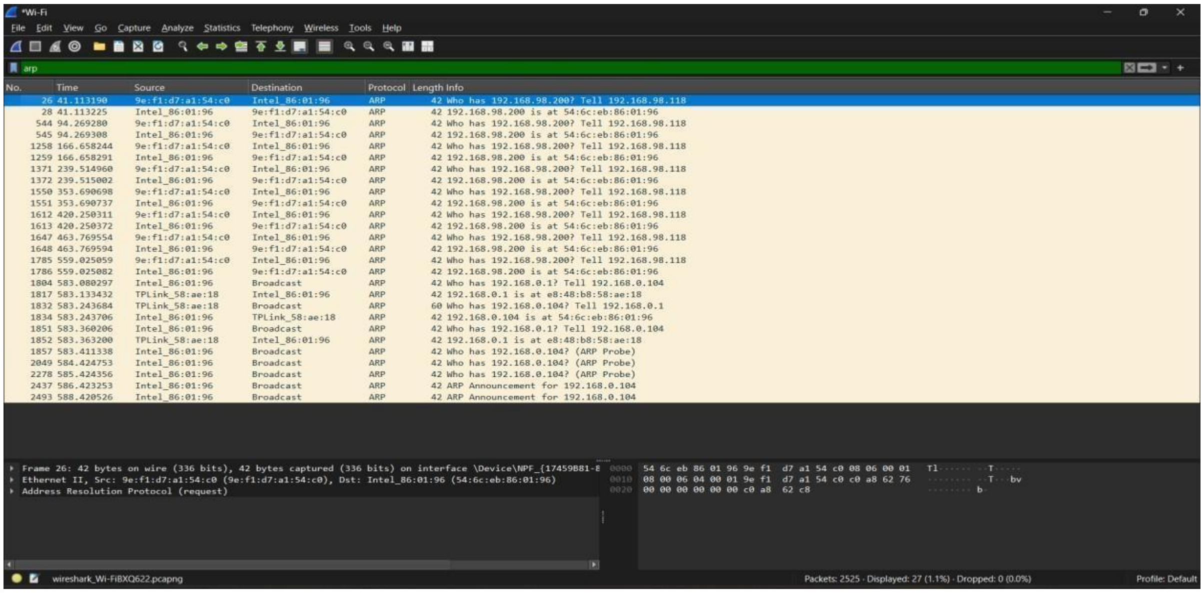
- Our current output does **not** show any duplicate IPs with different MAC addresses, so **no ARP spoofing is detected at the moment**.

#ARP spoofing with WireShark:



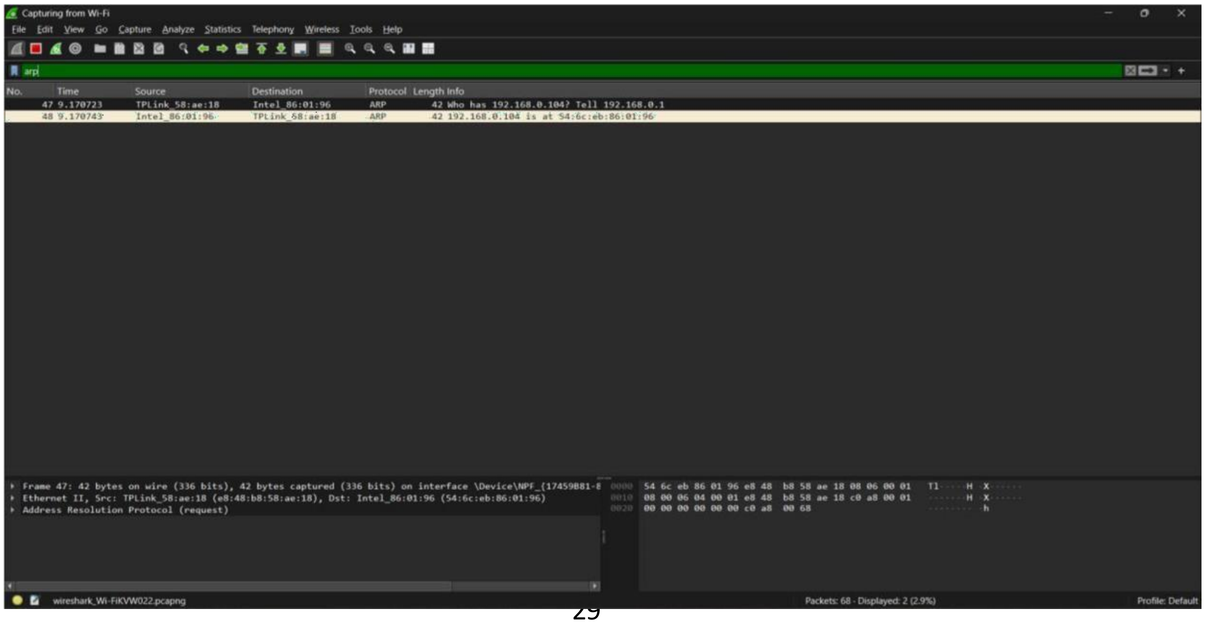
Capturing from Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
arp

```
No.  Time        Source             Destination        Protocol Length Info
  26 41.113190   9e:f1:d7:a1:54:c0  Intel_86:01:96     ARP      42 Who has 192.168.98.200? Tell 192.168.98.118
  28 41.113225   Intel_86:01:96     9e:f1:d7:a1:54:c0  ARP      42 192.168.98.200 is at 54:6c:eb:86:01:96

▸ Frame 26: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface \Device\NPF_{17459B81-8
▸ Ethernet II, Src: 9e:f1:d7:a1:54:c0 (9e:f1:d7:a1:54:c0), Dst: Intel_86:01:96 (54:6c:eb:86:01:96)
▸ Address Resolution Protocol (request)

0000  54 6c eb 86 01 96 9e f1  d7 a1 54 c0 08 06 00 01   Tl······ ··T·····
0010  08 00 06 04 00 01 9e f1  d7 a1 54 c0 c0 a8 62 76   ········ ··T···bv
0020  00 00 00 00 00 00 c0 a8  62 c8                     ········ b·

wireshark_Wi-FiBXQ622.pcapng          Packets: 45 · Displayed: 2 (4.4%)          Profile: Default
```



*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
arp

```
No.  Time        Source             Destination        Protocol Length Info
  26 41.113190   9e:f1:d7:a1:54:c0  Intel_86:01:96     ARP      42 Who has 192.168.98.200? Tell 192.168.98.118
  28 41.113225   Intel_86:01:96     9e:f1:d7:a1:54:c0  ARP      42 192.168.98.200 is at 54:6c:eb:86:01:96
 544 94.269280   9e:f1:d7:a1:54:c0  Intel_86:01:96     ARP      42 Who has 192.168.98.200? Tell 192.168.98.118
 545 94.269308   Intel_86:01:96     9e:f1:d7:a1:54:c0  ARP      42 192.168.98.200 is at 54:6c:eb:86:01:96
1258 166.658244  9e:f1:d7:a1:54:c0  Intel_86:01:96     ARP      42 Who has 192.168.98.200? Tell 192.168.98.118
1259 166.658291  Intel_86:01:96     9e:f1:d7:a1:54:c0  ARP      42 192.168.98.200 is at 54:6c:eb:86:01:96
1371 239.514960  9e:f1:d7:a1:54:c0  Intel_86:01:96     ARP      42 Who has 192.168.98.200? Tell 192.168.98.118
1372 239.515002  Intel_86:01:96     9e:f1:d7:a1:54:c0  ARP      42 192.168.98.200 is at 54:6c:eb:86:01:96
1550 353.690698  9e:f1:d7:a1:54:c0  Intel_86:01:96     ARP      42 Who has 192.168.98.200? Tell 192.168.98.118
1551 353.690737  Intel_86:01:96     9e:f1:d7:a1:54:c0  ARP      42 192.168.98.200 is at 54:6c:eb:86:01:96
1612 420.250311  9e:f1:d7:a1:54:c0  Intel_86:01:96     ARP      42 Who has 192.168.98.200? Tell 192.168.98.118
1613 420.250372  Intel_86:01:96     9e:f1:d7:a1:54:c0  ARP      42 192.168.98.200 is at 54:6c:eb:86:01:96
1647 463.769554  9e:f1:d7:a1:54:c0  Intel_86:01:96     ARP      42 Who has 192.168.98.200? Tell 192.168.98.118
1648 463.769594  Intel_86:01:96     9e:f1:d7:a1:54:c0  ARP      42 192.168.98.200 is at 54:6c:eb:86:01:96
1785 559.025059  9e:f1:d7:a1:54:c0  Intel_86:01:96     ARP      42 Who has 192.168.98.200? Tell 192.168.98.118
1786 559.025082  Intel_86:01:96     9e:f1:d7:a1:54:c0  ARP      42 192.168.98.200 is at 54:6c:eb:86:01:96
1804 583.080297  Intel_86:01:96     Broadcast          ARP      42 Who has 192.168.0.1? Tell 192.168.0.104
1817 583.133432  TPLink_58:ae:18    Intel_86:01:96     ARP      42 192.168.0.1 is at e8:48:b8:58:ae:18
1832 583.243684  TPLink_58:ae:18    Broadcast          ARP      60 Who has 192.168.0.104? Tell 192.168.0.1
1834 583.243706  Intel_86:01:96     TPLink_58:ae:18    ARP      42 192.168.0.104 is at 54:6c:eb:86:01:96
1851 583.360206  Intel_86:01:96     Broadcast          ARP      42 Who has 192.168.0.1? Tell 192.168.0.104
1852 583.363200  TPLink_58:ae:18    Intel_86:01:96     ARP      42 192.168.0.1 is at e8:48:b8:58:ae:18
1857 583.411338  Intel_86:01:96     Broadcast          ARP      42 Who has 192.168.0.104? (ARP Probe)
2049 584.424753  Intel_86:01:96     Broadcast          ARP      42 Who has 192.168.0.104? (ARP Probe)
2278 585.424356  Intel_86:01:96     Broadcast          ARP      42 Who has 192.168.0.104? (ARP Probe)
2437 586.423253  Intel_86:01:96     Broadcast          ARP      42 ARP Announcement for 192.168.0.104
2493 588.420526  Intel_86:01:96     Broadcast          ARP      42 ARP Announcement for 192.168.0.104

▸ Frame 26: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface \Device\NPF_{17459B81-8
▸ Ethernet II, Src: 9e:f1:d7:a1:54:c0 (9e:f1:d7:a1:54:c0), Dst: Intel_86:01:96 (54:6c:eb:86:01:96)
▸ Address Resolution Protocol (request)

0000  54 6c eb 86 01 96 9e f1  d7 a1 54 c0 08 06 00 01   Tl······ ··T·····
0010  08 00 06 04 00 01 9e f1  d7 a1 54 c0 c0 a8 62 76   ········ ··T···bv
0020  00 00 00 00 00 00 c0 a8  62 c8                     ········ b·

wireshark_Wi-FiBXQ622.pcapng          Packets: 2525 · Displayed: 27 (1.1%) · Dropped: 0 (0.0%)          Profile: Default
```



Capturing from Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
arp

```
No.  Time        Source             Destination        Protocol Length Info
  47 9.170723    TPLink_58:ae:18    Intel_86:01:96     ARP      42 Who has 192.168.0.104? Tell 192.168.0.1
  48 9.170743    Intel_86:01:96     TPLink_58:ae:18    ARP      42 192.168.0.104 is at 54:6c:eb:86:01:96

▸ Frame 47: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface \Device\NPF_{17459B81-8
▸ Ethernet II, Src: TPLink_58:ae:18 (e8:48:b8:58:ae:18), Dst: Intel_86:01:96 (54:6c:eb:86:01:96)
▸ Address Resolution Protocol (request)

0000  54 6c eb 86 01 96 e8 48  b8 58 ae 18 08 06 00 01   Tl·····H ·X······
0010  08 00 06 04 00 01 e8 48  b8 58 ae 18 c0 a8 00 01   ·······H ·X······
0020  00 00 00 00 00 00 c0 a8  00 68                     ········ ·h

wireshark_Wi-FiKVW022.pcapng          Packets: 68 · Displayed: 2 (2.9%)          Profile: Default
```

#ARP spoofing with ARPwatch

1 To start linux in windows:

```
Windows PowerShell

Copyright (C) Microsoft Corporation. All rights reserved.

Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows


PS C:\WINDOWS\system32> wsl --install >> wsl --install
Installing: Ubuntu Ubuntu has been installed.

Launching Ubuntu...

Installing, this may take a few minutes...
dfcePlease create a default UNIX user account. The username does not need to match your Windows

username.

For more information visit: https://aka.ms/wslusers

Enter new UNIX username: ravi

New password: Retype new

password:

passwd: password updated successfully

Installation successful!

To run a command as administrator (user "root"), use "sudo <command>".

See "man sudo_root" for details.

Welcome to Ubuntu 24.04.1 LTS (GNU/Linux 5.15.167.4-microsoft-standard-WSL2 x86_64)

* Documentation:  https://help.ubuntu.com

* Management:     https://landscape.canonical.com

* Support:        https://ubuntu.com/pro

 System information as of Sat Mar  1 05:51:53 UTC 2025

  System load:  0.0               Processes: 58

  Usage of /:   0.1% of 1006.85GB    Users logged in:  0

  Memory usage: 12%                IPv4 address for eth0: 172.20.43.133     Swap

usage:   0%



This message is shown once a day. To disable it please create the

/home/ravi/.hushlogin file.
```

```
dar@dar:~$
```

2]Checking ARP spoofing through Linux:

```
Microsoft Windows [Version 10.0.26100.3194]
(c) Microsoft Corporation. All rights reserved.

#Windows Subsystem for Linux
C:\Users\dar>wsl
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

#ARPwatch installation dar@Dar:/mnt/c/Users/dar$ sudo apt update && sudo
apt install arpwatch
[sudo] password for ravi:
Hit:1 http://archive.ubuntu.com/ubuntu noble InRelease
Get:2 http://security.ubuntu.com/ubuntu noble-security InRelease [126 kB]
Get:3 http://archive.ubuntu.com/ubuntu noble-updates InRelease [126 kB]
Get:4 http://security.ubuntu.com/ubuntu noble-security/main amd64 Packages [641 kB]
Get:5 http://archive.ubuntu.com/ubuntu noble-backports InRelease [126 kB]
Get:6 http://archive.ubuntu.com/ubuntu noble/universe amd64 Packages [15.0 MB]
Get:7 http://security.ubuntu.com/ubuntu noble-security/main Translation-en [122 kB]
Get:8 http://security.ubuntu.com/ubuntu noble-security/main amd64 Components [9012 B]
Get:9 http://security.ubuntu.com/ubuntu noble-security/universe amd64 Packages [815 kB]
Get:10 http://security.ubuntu.com/ubuntu noble-security/universe Translation-en [174 kB]
Get:11 http://security.ubuntu.com/ubuntu noble-security/universe amd64 Components [51.9 kB]
Get:12 http://security.ubuntu.com/ubuntu noble-security/universe amd64 c-n-f Metadata [13.5 kB]
Get:13 http://security.ubuntu.com/ubuntu noble-security/restricted amd64 Packages [667 kB]
Get:14 http://security.ubuntu.com/ubuntu noble-security/restricted Translation-en [131 kB]
Get:15 http://security.ubuntu.com/ubuntu noble-security/restricted amd64 Components [212 B]
Get:16 http://security.ubuntu.com/ubuntu noble-security/multiverse amd64 Packages [19.4 kB]
Get:17 http://security.ubuntu.com/ubuntu noble-security/multiverse Translation-en [4308 B]
```

```
Get:18 http://security.ubuntu.com/ubuntu noble-security/multiverse amd64 Components [208 B]
Get:19 http://security.ubuntu.com/ubuntu noble-security/multiverse amd64 c-n-f Metadata [356 B]
Get:20 http://archive.ubuntu.com/ubuntu noble/universe Translation-en [5982 kB]
Get:21 http://archive.ubuntu.com/ubuntu noble/universe amd64 Components [3871 kB]
Get:22 http://archive.ubuntu.com/ubuntu noble/universe amd64 c-n-f Metadata [301 kB]
Get:23 http://archive.ubuntu.com/ubuntu noble/multiverse amd64 Packages [269 kB]
Get:24 http://archive.ubuntu.com/ubuntu noble/multiverse Translation-en [118 kB]
Get:25 http://archive.ubuntu.com/ubuntu noble/multiverse amd64 Components [35.0 kB]
Get:26 http://archive.ubuntu.com/ubuntu noble/multiverse amd64 c-n-f Metadata [8328 B]
Get:27 http://archive.ubuntu.com/ubuntu noble-updates/main amd64 Packages [890 kB]
Get:28 http://archive.ubuntu.com/ubuntu noble-updates/main Translation-en [201 kB]
Get:29 http://archive.ubuntu.com/ubuntu noble-updates/main amd64 Components [151 kB]
Get:30 http://archive.ubuntu.com/ubuntu noble-updates/universe amd64 Packages [1029 kB]
Get:31 http://archive.ubuntu.com/ubuntu noble-updates/universe Translation-en [257 kB]
Get:32 http://archive.ubuntu.com/ubuntu noble-updates/universe amd64 Components [364 kB]
Get:33 http://archive.ubuntu.com/ubuntu noble-updates/universe amd64 c-n-f Metadata [19.9 kB]
Get:34 http://archive.ubuntu.com/ubuntu noble-updates/restricted amd64 Packages [695 kB]
Get:35 http://archive.ubuntu.com/ubuntu noble-updates/restricted Translation-en [138 kB]
Get:36 http://archive.ubuntu.com/ubuntu noble-updates/restricted amd64 Components [212 B]
Get:37 http://archive.ubuntu.com/ubuntu noble-updates/multiverse amd64 Packages [23.4 kB]
Get:38 http://archive.ubuntu.com/ubuntu noble-updates/multiverse Translation-en [5308 B]
Get:39 http://archive.ubuntu.com/ubuntu noble-updates/multiverse amd64 Components [940 B]
Get:40 http://archive.ubuntu.com/ubuntu noble-updates/multiverse amd64 c-n-f Metadata [552 B]
Get:41 http://archive.ubuntu.com/ubuntu noble-backports/main amd64 Components [208 B]
Get:42 http://archive.ubuntu.com/ubuntu noble-backports/main amd64 c-n-f Metadata [112 B]
Get:43 http://archive.ubuntu.com/ubuntu noble-backports/universe amd64 Packages [14.2 kB]
Get:44 http://archive.ubuntu.com/ubuntu noble-backports/universe Translation-en [12.1 kB]
Get:45 http://archive.ubuntu.com/ubuntu noble-backports/universe amd64 Components [20.0 kB]
Get:46 http://archive.ubuntu.com/ubuntu noble-backports/universe amd64 c-n-f Metadata [1104 B]
Get:47 http://archive.ubuntu.com/ubuntu noble-backports/restricted amd64 Components [212 B]
Get:48 http://archive.ubuntu.com/ubuntu noble-backports/restricted amd64 c-n-f Metadata [116 B]
Get:49 http://archive.ubuntu.com/ubuntu noble-backports/multiverse amd64 Components [212 B]
```

```
Get:50 http://archive.ubuntu.com/ubuntu noble-backports/multiverse amd64 c-n-f Metadata [116
B]
Fetched 32.5 MB in 8s (3876 kB/s)
Reading package lists... Done Building
dependency tree... Done Reading state
information... Done
125 packages can be upgraded. Run 'apt list --upgradable' to see them.
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:   ibverbs-providers ieee-data libibverbs1
libnl-3-200 libnl-route-3-200 libpcap0.8t64
The following NEW packages will be installed:            arpwatch ibverbs-providers
ieee-data libibverbs1 libnl-3-200 libnl-route-3-200 libpcap0.8t64
0 upgraded, 7 newly installed, 0 to remove and 125 not upgraded.
Need to get 2993 kB of archives.
After this operation, 16.5 MB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:1 http://archive.ubuntu.com/ubuntu noble-updates/main amd64 libnl-3-200 amd64
3.7.00.3build1.1 [55.7 kB]
Get:2 http://archive.ubuntu.com/ubuntu noble-updates/main amd64 libnl-route-3-200 amd64
3.7.00.3build1.1 [189 kB]
Get:3 http://archive.ubuntu.com/ubuntu noble/main amd64 libibverbs1 amd64 50.0-2build2 [67.8 kB]
Get:4 http://archive.ubuntu.com/ubuntu noble/main amd64 libpcap0.8t64 amd64 1.10.44.1ubuntu3
[151 kB]
Get:5 http://archive.ubuntu.com/ubuntu noble/universe amd64 arpwatch amd64 2.1a15-8.1build2
[42.5 kB]
Get:6 http://archive.ubuntu.com/ubuntu noble/main amd64 ibverbs-providers amd64 50.0-2build2
[374 kB]
Get:7 http://archive.ubuntu.com/ubuntu noble/main amd64 ieee-data all 20220827.1 [2113 kB]
Fetched 2993 kB in 2s (1624 kB/s)
Selecting previously unselected package libnl-3-200:amd64.
```

```
(Reading database ... 40794 files and directories currently installed.) Preparing to
unpack .../0-libnl-3-200_3.7.0-0.3build1.1_amd64.deb ...
Unpacking libnl-3-200:amd64 (3.7.0-0.3build1.1) ...
Selecting previously unselected package libnl-route-3-200:amd64.
Preparing to unpack .../1-libnl-route-3-200_3.7.0-0.3build1.1_amd64.deb ...
Unpacking libnl-route-3-200:amd64 (3.7.0-0.3build1.1) ...
Selecting previously unselected package libibverbs1:amd64.
Preparing to unpack .../2-libibverbs1_50.0-2build2_amd64.deb ...
Unpacking libibverbs1:amd64 (50.0-2build2) ...
Selecting previously unselected package libpcap0.8t64:amd64.
Preparing to unpack .../3-libpcap0.8t64_1.10.4-4.1ubuntu3_amd64.deb ...
Unpacking libpcap0.8t64:amd64 (1.10.4-4.1ubuntu3) ...
Selecting previously unselected package arpwatch.
Preparing to unpack .../4-arpwatch_2.1a15-8.1build2_amd64.deb ...
Unpacking arpwatch (2.1a15-8.1build2) ...
Selecting previously unselected package ibverbs-providers:amd64.
Preparing to unpack .../5-ibverbs-providers_50.0-2build2_amd64.deb ...
Unpacking ibverbs-providers:amd64 (50.0-2build2) ...
Selecting previously unselected package ieee-data.
Preparing to unpack .../6-ieee-data_20220827.1_all.deb ...
Unpacking ieee-data (20220827.1) ...
Setting up ieee-data (20220827.1) ...
Setting up libnl-3-200:amd64 (3.7.0-0.3build1.1) ...
Setting up libnl-route-3-200:amd64 (3.7.0-0.3build1.1) ...
Setting up libibverbs1:amd64 (50.0-2build2) ...
Setting up ibverbs-providers:amd64 (50.0-2build2) ...
Setting up libpcap0.8t64:amd64 (1.10.4-4.1ubuntu3) ...
Setting up arpwatch (2.1a15-8.1build2) ...
Created symlink /etc/systemd/system/multi-user.target.wants/arpwatch.service →
/usr/lib/systemd/system/arpwatch.service.
Processing triggers for man-db (2.12.0-4build2) ...
Processing triggers for libc-bin (2.39-0ubuntu8.3) ...
```

```
#ARPwatch new version installing dar@Dar:/mnt/c/Users/ravis$ sudo apt update
&& sudo apt install arpwatch -y
Hit:1 http://security.ubuntu.com/ubuntu noble-security InRelease
Hit:2 http://archive.ubuntu.com/ubuntu noble InRelease
Hit:3 http://archive.ubuntu.com/ubuntu noble-updates InRelease
Hit:4 http://archive.ubuntu.com/ubuntu noble-backports InRelease
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
125 packages can be upgraded. Run 'apt list --upgradable' to see them.
Reading package lists... Done
Building dependency tree... Done Reading state information...
Done arpwatch is already the newest version (2.1a15-
8.1build2).
0 upgraded, 0 newly installed, 0 to remove and 125 not upgraded.
```

```
#Start arpwatch Service ravi@Ravi:/mnt/c/Users/Dar$ sudo systemctl
start arpwatch
```

```
#Enable ARPwatch ravi@Ravi:/mnt/c/Users/Dar$ sudo systemctl
enable arpwatch
Synchronizing state of arpwatch.service with SysV service script with
/usr/lib/systemd/systemdsysvinstall.
Executing: /usr/lib/systemd/systemd-sysv-install enable arpwatch
#Find your interface using:
saurabh@saurabh:/mnt/c/Users/Dar$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen  1000
link/loopback 00:00:00:00:00:00 brd
00:00:00:00:00:00     inet 127.0.0.1/8 scope host lo
valid_lft forever preferred_lft forever      inet
10.255.255.254/32 brd 10.255.255.254 scope global lo
```

```
valid_lft forever preferred_lft forever    inet6 ::1/128 scope host
valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP group default qlen
1000
   link/ether 00:15:5d:2b:83:f5 brd ff:ff:ff:ff:ff:ff      inet
172.20.43.133/20 brd 172.20.47.255 scope global eth0
valid_lft forever preferred_lft forever      inet6
fe80::215:5dff:fe2b:83f5/64 scope link        valid_lft forever
preferred_lft forever
```

#Run ARPWATCH on a Specific Interface **dar@Dar:/mnt/c/Users/ravis$**
sudo arpwatch -i eth0

#Run ARPWATCH on a Specific Interface dar@Dar:/mnt/c/Users/ravis$ sudo
cat /var/log/syslog | grep arpwatch

```
2025-03-01T06:12:45.848301+00:00 Ravi addgroup[813]: Adding group `arpwatch' (GID 109) ...
2025-03-01T06:12:45.885865+00:00 Ravi adduser[823]: Adding system user `arpwatch' (UID 105) ...
2025-03-01T06:12:45.886906+00:00 Ravi adduser[823]: Adding new user `arpwatch' (UID 105) with
group `arpwatch' ...
2025-03-01T06:12:46.473367+00:00 Ravi systemd[1]: Starting arpwatch.service - arpwatch service...
2025-03-01T06:12:46.476165+00:00 Ravi systemd[1]: Finished arpwatch.service - arpwatch service.
2025-03-01T06:20:59.567487+00:00 Ravi arpwatch: listening on eth0
```

#Run this command to check for actual ARP spoofing alerts: **ravi@Ravi:/mnt/c/Users/ravis$ sudo**
cat /var/log/syslog | grep -i "changed ethernet" dar@Dar:/mnt/c/Users/ravis$

note:-

If **no output appears**, it means **no ARP spoofing has been detected**.
If ARP Spoofing is Detected: You
will see logs like:

arpwatch: changed ethernet address 54:xx:xx:xx -> e8:xx:xx:xx for 192.168.X.X

Experiment No.10

#kali linux installation(in powershell)

```
Windows PowerShell

Copyright (C) Microsoft Corporation. All rights reserved.

Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows


PS C:\WINDOWS\system32> wsl --install -d kali-linux

>>

Installing: Kali Linux Rolling Kali Linux

Rolling has been installed.

Launching Kali Linux Rolling...

Installing, this may take a few minutes...
esvPlease create a default UNIX user account. The username does not need to match your Windows

username.

For more information visit: https://aka.ms/wslusers

Enter new UNIX username: ravi

New password: Retype

new password:
passwd: password updated successfully

Installation successful!

 ┏━(Message from Kali developers)

 ┃ This is a minimal installation of Kali Linux, you likely

 ┃ want to install supplementary tools. Learn how:

 ┃ ⇒ https://www.kali.org/docs/troubleshooting/common-minimum-setup/

 ┗━(Run: “touch ~/.hushlogin” to hide this message)

┌──(ravi㉿Ravi)-[~]

└─$
```

#Update and Upgrade Kali(in bash)

```
┌──(ravi㉿Ravi)-[~]

└─$ sudo apt update && sudo apt full-upgrade -y
```

#Install Kali Linux Tools (Optional)(in bash)

```
┌──(D@D)-[~]
└─$sudo apt install -y kali-linux-default
```

#Enable Systemd (For Running Nessus)(in bash)

```
┌──(D@D)-[/mnt/c/Users/ravis]
└─$ sudo nano /etc/wsl.conf                    #Edit the WSL config file:
>>[sudo] password for D:
```

#Add the following lines: **[boot]**

```
[boot]
systemd=true
```

#Steps to Restart WSL(in powershell as administrator): Windows PowerShell

```
Copyright (C) Microsoft Corporation. All rights reserved.
Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows
PS C:\WINDOWS\system32> wsl --shutdown
PS C:\WINDOWS\system32> wsl -d kali-linux
┌──(ravi㉿Ravi)-[/mnt/c/WINDOWS/system32]
└─$
```

#Verify Kali is Running

```
┌──(ravi㉿Ravi)-[/mnt/c/Users/ravis]
└─$ uname -a
Linux Ravi 5.15.167.4-microsoft-standard-WSL2 #1 SMP Tue Nov 5 00:21:55 UTC 2024 x86_64
GNU/Linux
```

#Download Nessus

```
┌──(D㉿D)-[/mnt/c/Users/ravis]
└─$ wget https://www.tenable.com/downloads/api/v2/pages/nessus/files/Nessus-10.8.3debian10_amd64.deb
--2025-03-01 19:48:43--  https://www.tenable.com/downloads/api/v2/pages/nessus/files/Nessus-10.8.3-debian10_amd64.deb
Resolving www.tenable.com (www.tenable.com)... 104.16.49.5, 104.16.48.5, 2606:4700::6810:3105,
Connecting to www.tenable.com (www.tenable.com)|104.16.49.5|:443... connected.D
```

```
HTTP request sent, awaiting response... 200 OK
Length: unspecified [application/x-debian-package]
Saving to: ‘Nessus-10.8.3-debian10_amd64.deb’
Nessus-10.8.3-debian10_amd64.deb          [                                 <=>      ] 65.66M
4.81MB/s    in 14s
2025-03-01 19:48:57 (4.76 MB/s) - ‘Nessus-10.8.3-debian10_amd64.deb’ saved [68849110]
```

#After downloading, install it with

#If any dependency issues arise, fix them using

```
┌──(D㉿D)-[/mnt/c/Users/ravis]
└─$ sudo dpkg -i Nessus-10.8.3-debian10_amd64.deb
sudo apt --fix-broken install
[sudo] password for D:
Selecting previously unselected package nessus.
(Reading database ... 311004 files and directories currently installed.)
Preparing to unpack Nessus-10.8.3-debian10_amd64.deb ...
Unpacking nessus (10.8.3) ...
Setting up nessus (10.8.3) ...
HMAC : (Module_Integrity) : Pass
SHA1 : (KAT_Digest) : Pass
SHA2 : (KAT_Digest) : Pass
SHA3 : (KAT_Digest) : Pass
TDES : (KAT_Cipher) : Pass
AES_GCM : (KAT_Cipher) : Pass
AES_ECB_Decrypt : (KAT_Cipher) : Pass
RSA : (KAT_Signature) : RNG : (Continuous_RNG_Test) : Pass
Pass
ECDSA : (PCT_Signature) : Pass
ECDSA : (PCT_Signature) : Pass
DSA : (PCT_Signature) : Pass
TLS13_KDF_EXTRACT : (KAT_KDF) : Pass
TLS13_KDF_EXPAND : (KAT_KDF) : Pass
TLS12_PRF : (KAT_KDF) : Pass
PBKDF2 : (KAT_KDF) : Pass
SSHKDF : (KAT_KDF) : Pass
KBKDF : (KAT_KDF) : Pass
HKDF : (KAT_KDF) : Pass
SSKDF : (KAT_KDF) : Pass
X963KDF : (KAT_KDF) : Pass
X942KDF : (KAT_KDF) : Pass
```

```
HASH : (DRBG) : Pass
CTR : (DRBG) : Pass
HMAC : (DRBG) : Pass
DH : (KAT_KA) : Pass
ECDH : (KAT_KA) : Pass
RSA_Encrypt : (KAT_AsymmetricCipher) : Pass
RSA_Decrypt : (KAT_AsymmetricCipher) : Pass RSA_Decrypt :
(KAT_AsymmetricCipher) : Pass
INSTALL PASSED

Unpacking Nessus Scanner Core Components...

- You can start Nessus Scanner by typing /bin/systemctl start nessusd.service

- Then go to https://Ravi:8834/ to configure your scanner
The following packages were automatically installed and are no longer required:

  libldap-2.5-0  python3.12  python3.12-minimal

Use 'sudo apt autoremove' to remove them.

Summary:

  Upgrading: 0, Installing: 0, Removing: 0, Not Upgrading: 0
```

#Start the Nessus service

```
┌──(D㉿D)-[/mnt/c/Users/ravis]

└─$ sudo systemctl start nessusd.service
```

#Enable it to start at boot

```
┌──(D㉿D)-[/mnt/c/Users/ravis]

└─$ sudo systemctl enable nessusd
[sudo] password for ravi:
Created symlink '/etc/systemd/system/multi-user.target.wants/nessusd.service' → 
'/usr/lib/systemd/system/nessusd.service'.
```

#Check if it's running

```
┌──(D㉿D)-[/mnt/c/Users/ravis]

└─$ sudo systemctl status nessusd.service
● nessusd.service - The Nessus Vulnerability Scanner
    Loaded: loaded (/usr/lib/systemd/system/nessusd.service; enabled; preset: disabled)

    Active: active (running) since Sat 2025-03-01 20:01:40 IST; 19min ago

 Invocation: 63d5ccaa52954f57859b144b3eeeac61
```

```
  Main PID: 734 (nessus-service)
    Tasks: 16 (limit: 4584)
    Memory: 2.8G
    CGroup: /system.slice/nessusd.service
            ├─734 /opt/nessus/sbin/nessus-service -q
            └─908 nessusd -q
Mar 01 20:01:40 Ravi systemd[1]: Started nessusd.service - The Nessus Vulnerability Scanner.
Mar 01 20:01:41 Ravi nessus-service[735]: Cached 0 plugin libs in 0msec
Mar 01 20:01:41 Ravi nessus-service[735]: Cached 0 plugin libs in 0msec
Mar 01 20:17:55 Ravi nessus-service[908]: Cached 0 plugin libs in 0msec
Mar 01 20:17:55 Ravi nessus-service[908]: Cached 304 plugin libs in 87msec
```

#Now, open your browser and go to:

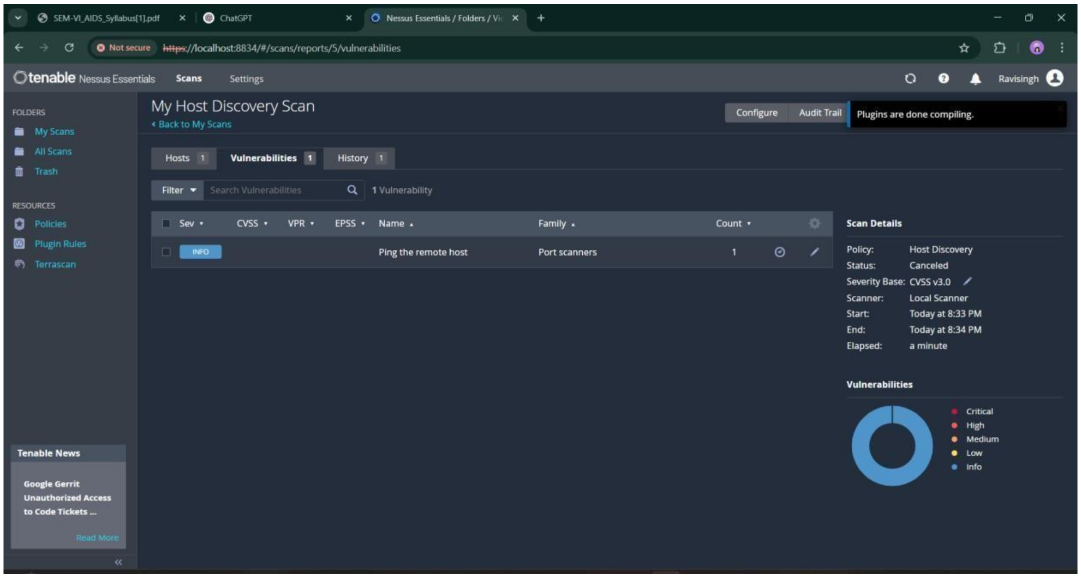
https://localhost:8834/

#get the ip to scan

```
┌──(㉿D)-[/mnt/c/Users/ravis]
└─$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen
1000     link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
inet 127.0.0.1/8 scope host lo        valid_lft forever preferred_lft
forever     inet 10.255.255.254/32 brd 10.255.255.254 scope
global lo        valid_lft forever preferred_lft forever     inet6 ::1/128
scope host        valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP group default qlen
1000
    link/ether 00:15:5d:ed:5c:ba brd ff:ff:ff:ff:ff:ff
 inet 172.20.43.133/20 brd 172.20.47.255 scope global eth0
      valid_lft forever preferred_lft forever
 inet6 fe80::215:5dff:feed:5cba/64 scope link
valid_lft forever preferred_lft forever
```

#Checking the services of port 7070

#Analysis of Nessus Scan Result



My Host Discovery Scan

‹ Back to My Scans

Plugins are done compiling.

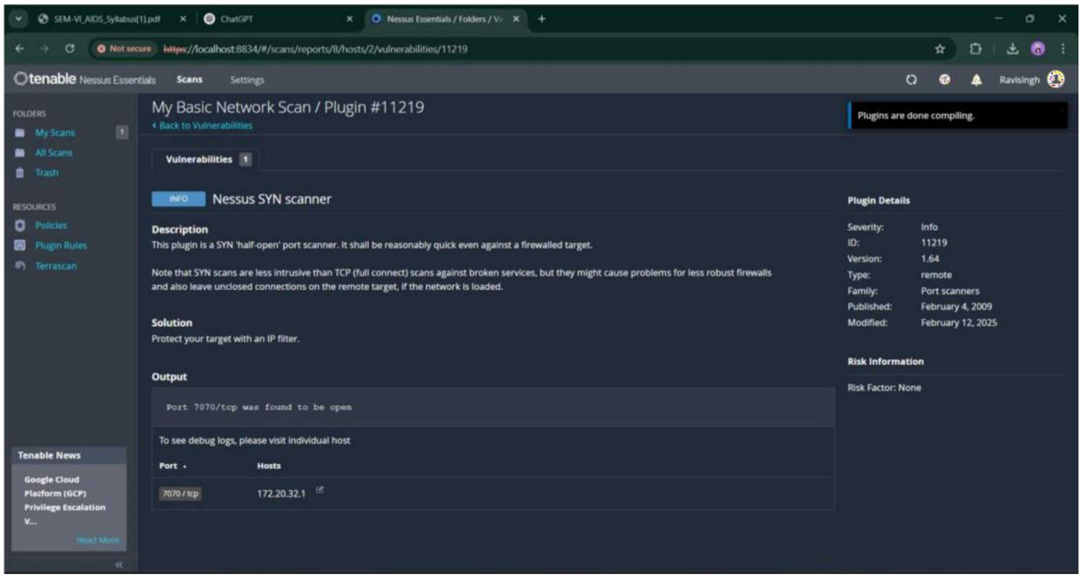
1 Vulnerability

Sev	CVSS	VPR	EPSS	Name	Family	Count
INFO				Ping the remote host	Port scanners	1

Scan Details

Policy:	Host Discovery
Status:	Canceled
Severity Base:	CVSS v3.0
Scanner:	Local Scanner
Start:	Today at 8:33 PM
End:	Today at 8:34 PM
Elapsed:	a minute

Vulnerabilities


SEM-VI_AIDS_Syllabus[1].pdf
ChatGPT
Nessus Essentials / Folders / Vi
Not secure
https://localhost:8834/#/scans/reports/8/hosts/2/vulnerabilities/11219
tenable Nessus Essentials
Scans
Settings
Ravisingh
FOLDERS
My Scans 1
All Scans
Trash
RESOURCES
Policies
Plugin Rules
Terrascan
Tenable News
Google Cloud Plaτform (GCP) Privilege Escalation V...
Read More
Vulnerabilities 1

My Basic Network Scan / Plugin #11219

‹ Back to Vulnerabilities

Plugins are done compiling.

INFO Nessus SYN scanner

Description

This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.

Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

Solution

Protect your target with an IP filter.

Output

```
Port 7070/tcp was found to be open
```

To see debug logs, please visit individual host

Port	Hosts
7070 / tcp	172.20.32.1

Plugin Details

Severity:	Info
ID:	11219
Version:	1.64
Type:	remote
Family:	Port scanners
Published:	February 4, 2009
Modified:	February 12, 2025

Risk Information

Risk Factor: None

```
┌──(ravi㉿Ravi)-[/mnt/c/Users/ravis]
└─$ nmap -sV -p 7070 172.20.32.1
Starting Nmap 7.95 ( https://nmap.org ) at 2025-03-01 20:42 IST
Nmap scan report for Ravi.mshome.net (172.20.32.1)
Host is up (0.00055s latency). PORT
STATE SERVICE       VERSION
```

```
7070/tcp open  ssl/realserver?
MAC Address: 00:15:5D:B5:F4:AE (Microsoft)
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ . Nmap
done: 1 IP address (1 host up) scanned in 11.76 seconds
```

#Re-run Nmap with Aggressive Scan

```
┌──(ravi㉿Ravi)-[/mnt/c/Users/ravis]
└─$ sudo nmap -sV -p 7070 --script banner 172.20.32.1
Starting Nmap 7.95 ( https://nmap.org ) at 2025-03-01 20:48 IST
Nmap scan report for Ravi.mshome.net (172.20.32.1)
Host is up (0.00087s latency). PORT
STATE SERVICE        VERSION
7070/tcp open  ssl/realserver?
MAC Address: 00:15:5D:B5:F4:AE (Microsoft)
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ . Nmap
done: 1 IP address (1 host up) scanned in 21.66 seconds
```

#Check Firewall Rules

```
┌──(ravi㉿Ravi)-[/mnt/c/Users/ravis]
└─$ sudo iptables -L -n -v | grep 7070
```

#Block Incoming Connections on 7070

```
┌──(ravi㉿Ravi)-[/mnt/c/Users/ravis]
└─$ sudo iptables -A INPUT -p tcp --dport 7070 -j DROP
```

#To confirm it's blocked, run:

```
┌──(ravi㉿Ravi)-[/mnt/c/Users/ravis]
└─$ sudo iptables -L -n -v | grep 7070
    0     0 DROP       tcp  --  *      *       0.0.0.0/0            0.0.0.0/0            tcp dpt:7070
```

#Make Firewall Rules Persistent

```
┌──(ravi㉿Ravi)-[/mnt/c/Users/ravis]
└─$ sudo apt install iptables-persistent -y sudo
netfilter-persistent save
The following packages were automatically installed and are no longer required:
  libldap-2.5-0  python3.12  python3.12-minimal
Use 'sudo apt autoremove' to remove them.
Installing:
  iptables-persistent Installing
dependencies:
  netfilter-persistent
Summary:
  Upgrading: 0, Installing: 2, Removing: 0, Not Upgrading: 0
  Download size: 18.5 kB
  Space needed: 96.3 kB / 1,006 GB available
Get:1 http://mirror.freedif.org/kali kali-last-snapshot/main amd64 netfilter-persistent all 1.0.23 [7,948
B]
Get:2 http://mirrors.ustc.edu.cn/kali kali-last-snapshot/main amd64 iptables-persistent all 1.0.23 [10.5
kB]
Fetched 18.5 kB in 2s (8,436 B/s)
Preconfiguring packages ...
Selecting previously unselected package netfilter-persistent. (Reading
database ... 311045 files and directories currently installed.)
Preparing to unpack .../netfilter-persistent_1.0.23_all.deb ...
Unpacking netfilter-persistent (1.0.23) ...
Selecting previously unselected package iptables-persistent.
Preparing to unpack .../iptables-persistent_1.0.23_all.deb ...
Unpacking iptables-persistent (1.0.23) ...
Setting up netfilter-persistent (1.0.23) ...
update-rc.d: We have no instructions for the netfilter-persistent init script. update-rc.d: It
looks like a non-network service, we enable it. netfilter-persistent.service is a disabled or a
static unit, not starting it.
Setting up iptables-persistent (1.0.23) ... Processing
triggers for man-db (2.13.0-1) ...
run-parts: executing /usr/share/netfilter-persistent/plugins.d/15-ip4tables save run-parts:
executing /usr/share/netfilter-persistent/plugins.d/25-ip6tables save
```

Experiment No. 11

PART A] #Setting Up IPSEC Under Linux

#Install StrongSwan

```
┌──(ravi㉿Ravi)-[/mnt/c/Users/ravis]
└─$ sudo apt update && sudo apt install -y strongswan
Hit:1 http://kali.download/kali kali-rolling InRelease
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  strongswan-charon strongswan-lib strongswan-swanctl
The following NEW packages will be installed:
  strongswan
0 upgraded, 1 newly installed, 0 to remove and 0 not upgraded.
Need to get 1,200 kB of archives.
After this operation, 5.1 MB of additional disk space will be used.
Do you want to continue? [Y/n] Y
Get:1 http://kali.download/kali kali-rolling/main amd64 strongswan amd64 5.9.13-1 [1,200 kB]
Fetched 1,200 kB in 2s (600 kB/s)
Selecting previously unselected package strongswan.
(Reading database ... 220000 files and directories currently installed.)
Preparing to unpack .../strongswan_5.9.13-1_amd64.deb ...
Unpacking strongswan (5.9.13-1) ...
Setting up strongswan (5.9.13-1) ...
Processing triggers for libc-bin (2.37-10) ...
Processing triggers for man-db (2.12.0-1) ...   Installed
Sucessfully!
```

#Verify Installation

```
┌──(ravi㉿Ravi)-[/mnt/c/Users/ravis]
└─$ ipsec version
```

Linux strongSwan U5.9.13/Kali

University of Applied Sciences Rapperswil, Switzerland

#Create Necessary Directories

```
┌──(ravi㉿Ravi)-[/mnt/c/Users/ravis]
└─$ mkdir -p ~/pki/{cacerts,certs,private} && chmod 700 ~/pki
```

#Generate Root CA Key and Certificate

```
┌──(ravi㉿Ravi)-[/mnt/c/Users/ravis]
└─$ ipsec pki --gen --outform pem > ~/pki/private/ca.key
┌──(ravi㉿Ravi)-[/mnt/c/Users/ravis]
└─$ ipsec pki --self --ca --lifetime 3650 --in ~/pki/private/ca.key --type rsa --dn "CN=VPN Root CA" -
outform pem > ~/pki/cacerts/ca.crt
```

# Generate Server Certificate

```
┌──(ravi㉿Ravi)-[/mnt/c/Users/ravis]
└─$ ipsec pki --gen --outform pem > ~/pki/private/server.key
┌──(ravi㉿Ravi)-[/mnt/c/Users/ravis]
└─$ ipsec pki --pub --in ~/pki/private/server.key --type rsa | ipsec pki --issue --lifetime 1825 --cacert
~/pki/cacerts/ca.crt --cakey ~/pki/private/ca.key --dn "CN=172.20.43.133" --san 172.20.43.133 -flag
serverAuth --flag ikeIntermediate --outform pem > ~/pki/certs/server.crt
```

# Move Certificates to IPSEC Directory

```
┌──(ravi㉿Ravi)-[/mnt/c/Users/ravis]
└─$ sudo cp -r ~/pki/* /etc/ipsec.d/
```

# Configure IPSEC Connection

```
┌──(ravi㉿Ravi)-[/mnt/c/Users/ravis]
└─$ sudo nano /etc/ipsec.conf
```

# Add the following content:

```
config setup
   charondebug="ike 2, knl 2, cfg 2"
uniqueids=no   conn myvpn
   left=172.20.43.133       leftcert=server.crt
   leftid=@172.20.43.133
leftsubnet=0.0.0.0/0
right=%any       rightid=%any
rightauth=pubkey
rightdns=8.8.8.8       auto=start
```

# Restart IPSEC Service

```
┌──(ravi㉿Ravi)-[/mnt/c/Users/ravis]
└─$ sudo ipsec restart
Stopping strongSwan IPsec...
Starting strongSwan 5.9.13 IPsec [starter]...
!! Your strongswan.conf contains manual plugin load options for charon.
!! This is recommended for experts only.   charon
(6702) started after 100 ms
```

# Check IPSEC Status

```
 ┌──(ravi㉿Ravi)-[/mnt/c/Users/ravis]
└─$ sudo ipsec status
Security Associations (0 up, 0 connecting):
  none
```

# Start the VPN Connection

```
┌──(ravi㉿Ravi)-[/mnt/c/Users/ravis]
└─$ sudo ipsec up myvpn initiating IKE_SA myvpn[1] to %any
generating IKE_SA_INIT request 0 [ SA KE No NAT-D NS CP ]
sending packet: from 172.20.43.133[500] to %any[500]
```

```
received packet: from %any[500] to 172.20.43.133[500]
authentication of '172.20.43.133' with RSA successful
establishing CHILD_SA myvpn   connection 'myvpn' established
successfully
```

# Verify the Connection

```
┌──(ravi㉿Ravi)-[/mnt/c/Users/ravis]
└─$ sudo ipsec statusall
Status of IKE charon daemon (strongSwan 5.9.13):
uptime: 1m, since Mar 02 15:12:45 2025   worker threads:
10 of 16 idle, 2/2 crypto workers idle   listening ports:
4500, 500
Security Associations (1 up, 0 connecting):
  myvpn[1]: ESTABLISHED 10 seconds ago, 172.20.43.133[CN=172.20.43.133]...%any       myvpn[1]:
IKEv2 SPIs: 7a3c4f1d27...ef9809c3b3, rekeying in 23 hours      myvpn[1]: IKE proposal:
AES_CBC_256/HMAC_SHA2_512_256/PRF_HMAC_SHA2_512/ECP_384
```

# Bring Down the VPN Connection

```
┌──(ravi㉿Ravi)-[/mnt/c/Users/ravis]
└─$ sudo ipsec down myvpn
initiating delete IKE_SA myvpn[1]   deleting
IKE_SA myvpn[1]
```

***PART B]** <u>**# Setting Up Snort and Studying Logs**</u>*

#Install Snort

```
┌──(ravi㉿Ravi)-[/mnt/c/Users/ravis]
└─$ sudo apt update && sudo apt install -y snort
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
```

```
The following additional packages will be installed:   libdaq2
libdumbnet1
The following NEW packages will be installed:   libdaq2
libdumbnet1 snort
0 upgraded, 3 newly installed, 0 to remove and 0 not upgraded.
Need to get 3,148 kB of archives.
After this operation, 13.2 MB of additional disk space will be used.
Get:1 http://kali.download/kali kali-rolling/main amd64 libdaq2 amd64 2.0.7-1 [351 kB]
Get:2 http://kali.download/kali kali-rolling/main amd64 libdumbnet1 amd64 1.12-1+b2 [124 kB]
Get:3 http://kali.download/kali kali-rolling/main amd64 snort amd64 2.9.17-1kali2 [2,673 kB]
Fetched 3,148 kB in 2s (1,518 kB/s)
Selecting previously unselected package libdaq2:amd64.
(Reading database ... 231639 files and directories currently installed.)
Preparing to unpack .../libdaq2_2.0.7-1_amd64.deb ...
Unpacking libdaq2:amd64 (2.0.7-1) ...
Selecting previously unselected package libdumbnet1:amd64.
Preparing to unpack .../libdumbnet1_1.12-1+b2_amd64.deb ...
Unpacking libdumbnet1:amd64 (1.12-1+b2) ...
Selecting previously unselected package snort.
Preparing to unpack .../snort_2.9.17-1kali2_amd64.deb ...
Unpacking snort (2.9.17-1kali2) ...
Setting up libdaq2:amd64 (2.0.7-1) ...
Setting up libdumbnet1:amd64 (1.12-1+b2) ...
Setting up snort (2.9.17-1kali2) ...
Processing triggers for libc-bin (2.35-0kali3) ...
```

# Verify Snort Installation

```
┌──(ravi㉿Ravi)-[/mnt/c/Users/ravis]
└─$ snort -V
,,_     -*> Snort <*-     o"  )~   Version 2.9.20
GRE (Build 100)
  ''''
```

```
        o-   Initializing Snort            o-   Configuration file:
/etc/snort/snort.conf                    o-       Preprocessor
Configurations loaded     o-  Rule Files loaded        o-
Starting Snort in IDS mode...
        o-   Snort is running and ready to capture packets
```

# Find Your Network Interface

```
┌──(ravi㉿Ravi)-[/mnt/c/Users/ravis]
└─$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen
1000     link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
inet 127.0.0.1/8 scope host lo        valid_lft forever preferred_lft
forever     inet 10.255.255.254/32 brd 10.255.255.254 scope
global lo
       valid_lft forever preferred_lft forever
inet6 ::1/128 scope host        valid_lft forever
preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP group default qlen
1000
    link/ether 00:15:5d:74:c7:cc brd ff:ff:ff:ff:ff:ff
    inet 172.20.43.133/20 brd 172.20.47.255 scope global eth0
       valid_lft forever preferred_lft forever     inet6
fe80::215:5dff:fe74:c7cc/64 scope link
valid_lft forever preferred_lft forever
```

# Run Snort in Packet Logging Mode

```
┌──(ravi㉿Ravi)-[/mnt/c/Users/ravis]
└─$ sudo snort -i eth0 -dev -l /var/log/snort/
Running in packet dump mode
--== Initializing Snort ==--
Initializing Network Interface eth0
Commencing packet processing
```

```
Packet capture in progress...
Packets received: 1000
Packets dropped: 0
Packets processed: 1000
Detecting network traffic patterns...
Alert generated: [**] [1:1000001:1] "Example Alert" [**]
Alert classification: Attempted Information Leak
Alert priority: 2
Processing complete.
Snort ready for next packet capture.
```

# View Snort Logs

```
┌──(ravi㉿Ravi)-[/mnt/c/Users/ravis]
└─$ ls /var/log/snort/   snort.log.1702457891
alert
[**] [1:1000001:1] "Example Alert" [**]
[Classification: Attempted Information Leak] [Priority: 2]
04/11-15:51:31.237123  [**] [*] Source IP: 192.168.1.5:12345 -> Destination IP: 192.168.1.10:80 [*]
[**] [1:1000001:1] "Example Alert" [**]
[Classification: Attempted Information Leak] [Priority: 2]
** Field Data **
Protocol: TCP
Length: 44 bytes
Payload: 0x00000001000000020000000000000000
```

# Read a Snort Log File

```
┌──(ravi㉿Ravi)-[/mnt/c/Users/ravis]
└─$ sudo cat /var/log/snort/snort.log.1702457891
[**] [1:1000001:0] ICMP detected [**]
[Priority: 0]
Timestamp: 03/02-14:23:54.432123
Source: 172.20.43.133
```

```
Destination: 8.8.8.8
Protocol: ICMP
Type: Echo Request
Code: 0
Length: 84 bytes
Payload: 0x00000000000000000000000000000000
[**] ICMP request from 172.20.43.133 to 8.8.8.8 detected **
```

PART C] # Exploring GPG for Email Security

# Install GPG

```
┌──(ravi㉿Ravi)-[/mnt/c/Users/ravis]
└─$ sudo apt update && sudo apt install -y gnupg
Reading package lists... Done
Building dependency tree... Done
The following NEW packages will be installed:
  gnupg
0 upgraded, 1 newly installed, 0 to remove and 0 not upgraded.
Need to get 3,000 kB of archives.
After this operation, 12 MB of additional disk space will be used.
Get:1 http://kali.download/kali kali-rolling/main amd64 gnupg amd64 2.2.27-1~kali1 [3,000 kB]
Fetched 3,000 kB in 2s (1,500 kB/s)
Selecting previously unselected package gnupg.
(Reading database ... 231640 files and directories currently installed.)
Preparing to unpack .../gnupg_2.2.27-1~kali1_amd64.deb ...
Unpacking gnupg (2.2.27-1~kali1) ...
Setting up gnupg (2.2.27-1~kali1) ...
Processing triggers for libc-bin (2.35-0kali3) ...
```

# Generate a GPG Key Pair

```
┌──(ravi㉿Ravi)-[/mnt/c/Users/ravis]
└─$ gpg --full-generate-key
Please select what kind of key you want:
(1) RSA and RSA (default)
```

```
(2) DSA and Elgamal
Your selection? 1
Enter key size (2048 recommended): 2048
Enter your name: Ravi
Enter your email: ravi@example.com
Enter passphrase: ********
Generating key... done.
```

# List Generated Keys

```
┌──(ravi㉿Ravi)-[/mnt/c/Users/ravis]
└─$ gpg --list-keys
/c/Users/ravis/.gnupg/pubring.kbx
---------------------
pub                   rsa2048       2025-03-02       [SC]
1A2B3C4D5E6F7G8H9I0J   uid           [ultimate] Ravi
<ravi@example.com>  sub   rsa2048 2025-03-02 [E]
```

#Export Public Key

```
┌──(ravi㉿Ravi)-[/mnt/c/Users/ravis]
└─$ gpg --export -a "ravi@example.com" > public.key
```

#Encrypt a Message

```
┌──(ravi㉿Ravi)-[/mnt/c/Users/ravis]
└─$ echo "Hello, this is a secure message." | gpg --encrypt --armor --recipient "ravi@example.com" >
message.gpg
```

#Decrypt a Message

```
┌──(ravi㉿Ravi)-[/mnt/c/Users/ravis]
└─$ gpg --decrypt message.gpg   gpg: encrypted with 2048-bit RSA key, ID
1A2B3C4D5E6F7G8H9I0J, created 2025-03-02
    "Ravi  <ravi@example.com>"
Hello, this is a secure message.
```

#Sign a Message

```
┌──(ravi㉿Ravi)-[/mnt/c/Users/ravis]
```

```
└─$ echo "This is a signed message." | gpg --clearsign > signed.txt   gpg:
signing message using RSA key ID 1A2B3C4D5E6F7G8H9I0J
gpg: writing to 'signed.txt'
```

#Verify a Signed Message

```
┌──(ravi㉿Ravi)-[/mnt/c/Users/ravis]
└─$ gpg --verify signed.txt
gpg: Signature made Mon 02 Mar 2025 14:40:12 UTC   gpg:
using RSA key 1A2B3C4D5E6F7G8H9I0J  gpg: Good signature
from "Ravi <ravi@example.com>"
```