



## Penetration Testing Report

For

**“EyeSaaaaaaAmPeeeeeeeeee”**

S.NO.	Title	#
1.	Challenge Category	Network Security
2.	Challenge Related Files	N/A
3.	File Link / Target IP	N/A

## PROCEDURE

1. Notice that when dst of packet is == 10.40.0.23 its always ICMP packet
2. Means Flag is Hidden in ICMP data packets
3. Analyze more to get a pattern in packets

```
~/final/Network_mid/question/solve.py - Sublime
File Edit Selection Find View Goto Tools Project Preferences Help
solve.py x
1  #!/usr/bin/env python3
2
3  from scapy.all import *
4  from scapy.layers.inet import IP, ICMP
5
6  cap = rdpcap('test.pcapng')
7  print('Done reading capture')
8
9  print(cap)
10
11 results = ''
12
13
14 def decode(data):
15     decoded = ''.join(chr(int(data[i:i + 8], 2)) for i in range(0, len(data), 8))
16     return decoded
17
18
19 for pkt in cap:
20     if ICMP in pkt:
21         dst = pkt[IP].dst
22         if dst == '192.168.1.5':
23             t = pkt[ICMP].type
24             print(t)
25             results += ['0', '1'][t == 8]
26
27 print(results)
28
29 print(f'Got flag data: {decode(results)}')
30
```

## Flags:

S.No.	Flag - No.	Flag
1.	Flag 1	HE{Trying_to_Get_ICMP_huh}