Penetration Testing Report

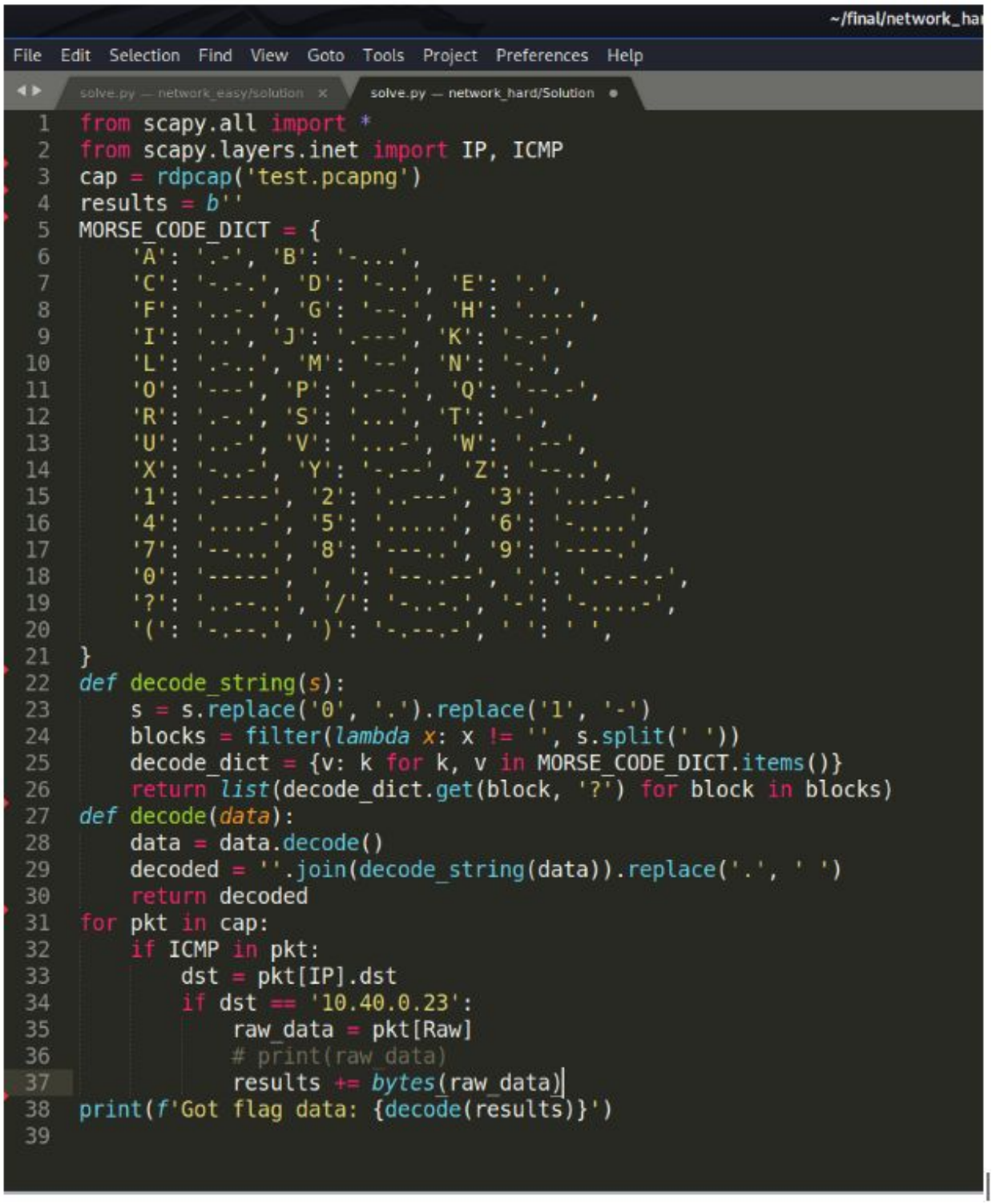
For

“Super Secret Code (But Old)”

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**
2. **Extra binary data is there in packet**
3. **Extract all such data in order**
4. **Morse decode That either by hand or by script At will give the flag.**


~/final/network_ha
File Edit Selection Find View Goto Tools Project Preferences Help
solve.py — network_easy/solution
solve.py — network_hard/Solution
from scapy.all import *
from scapy.layers.inet import IP, ICMP
cap = rdpcap('test.pcapng')
results = b''
MORSE_CODE_DICT = {
'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': '--..',
'1': '.----', '2': '..---', '3': '...--',
'4': '....-', '5': '.....', '6': '-....',
'7': '--...', '8': '---..', '9': '----.',
'0': '-----', ', ': '--..--', '.': '.-.-.-',
'?': '..--..', '/': '-..-.', '-': '-....-',
'(': '-.--.', ')': '-.--.-', ' ': ' ',
}
def decode_string(s):
s = s.replace('0', '.').replace('1', '-')
blocks = filter(lambda x: x != '', s.split(' '))
decode_dict = {v: k for k, v in MORSE_CODE_DICT.items()}
return list(decode_dict.get(block, '?') for block in blocks)
def decode(data):
data = data.decode()
decoded = ''.join(decode_string(data)).replace('.', ' ')
return decoded
for pkt in cap:
if ICMP in pkt:
dst = pkt[IP].dst
if dst == '10.40.0.23':
raw_data = pkt[Raw]
# print(raw_data)
results += bytes(raw_data)
print(f'Got flag data: {decode(results)}')

Flags:

S.No.	Flag - No.	Flag
1.	Flag 1	HE{SO-MOORSE-WAS-EMBEDED-IN-PCAP}