CE 340 Project 2

Penetration Test

and

Secure Authentication

User Manual

Group Members

Ege ALTIOK	20190602002
Ozan ŞAHİN	20190602036

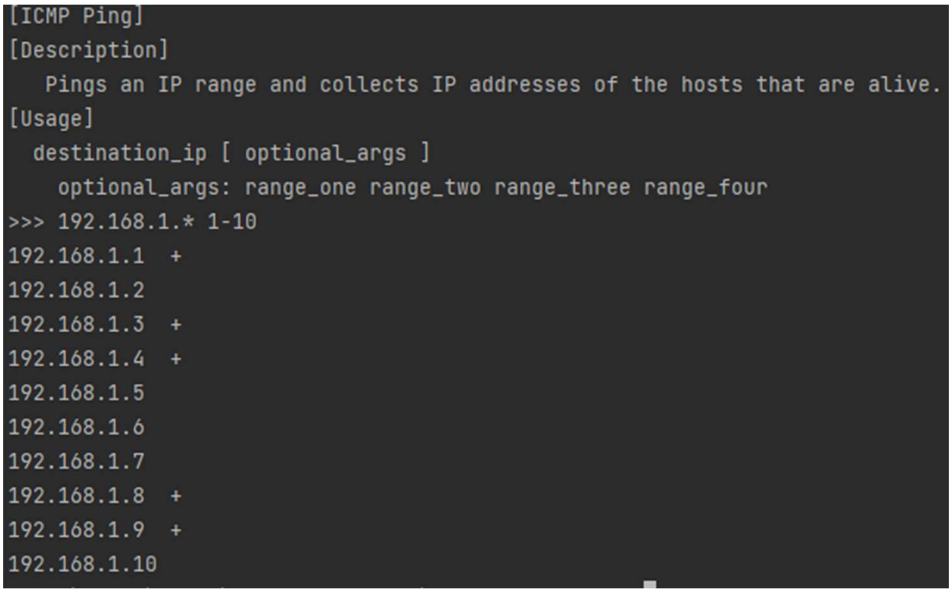
Table of Contents

I. Penetration Test

This section of the manual describes the contents and usage of the **pentest.py** script.

1) imcp_ping

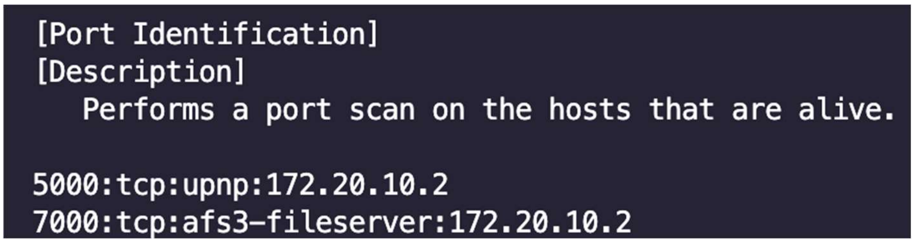
Pings an IP range and collect IP addresses of the hosts that are alive and saves the results in icmp.dat.



```
[ICMP Ping]
[Description]
   Pings an IP range and collects IP addresses of the hosts that are alive.
[Usage]
  destination_ip [ optional_args ]
    optional_args: range_one range_two range_three range_four
>>> 192.168.1.* 1-10
192.168.1.1  +
192.168.1.2
192.168.1.3  +
192.168.1.4  +
192.168.1.5
192.168.1.6
192.168.1.7
192.168.1.8  +
192.168.1.9  +
192.168.1.10
```

2) port_identification

Performs port scan on the live hosts. The scanning finds and identifies ports on each host and save the results in openPorts.dat.

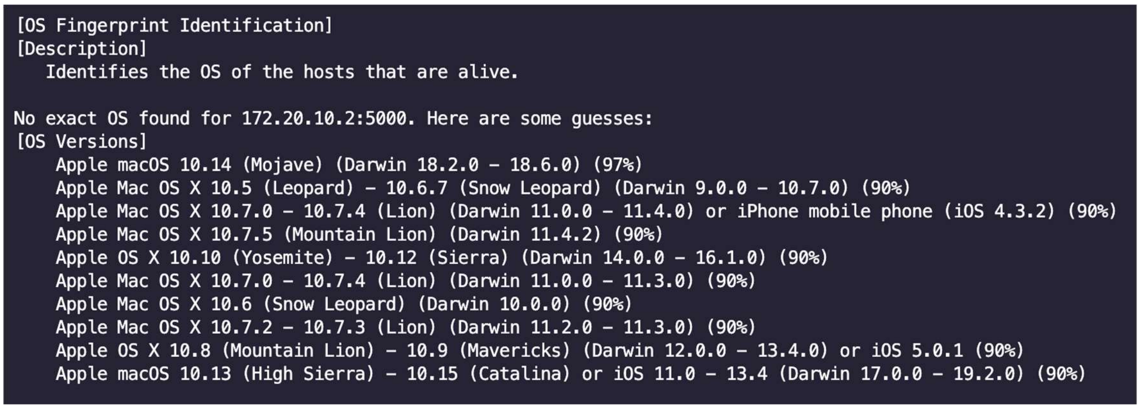


```
[Port Identification]
[Description]
   Performs a port scan on the hosts that are alive.

5000:tcp:upnp:172.20.10.2
7000:tcp:afs3-fileserver:172.20.10.2
```

3) os_fingerprint_identification

Gets the host IPs from the text file and identifies operating systems (OS) and OS versions of the hosts.



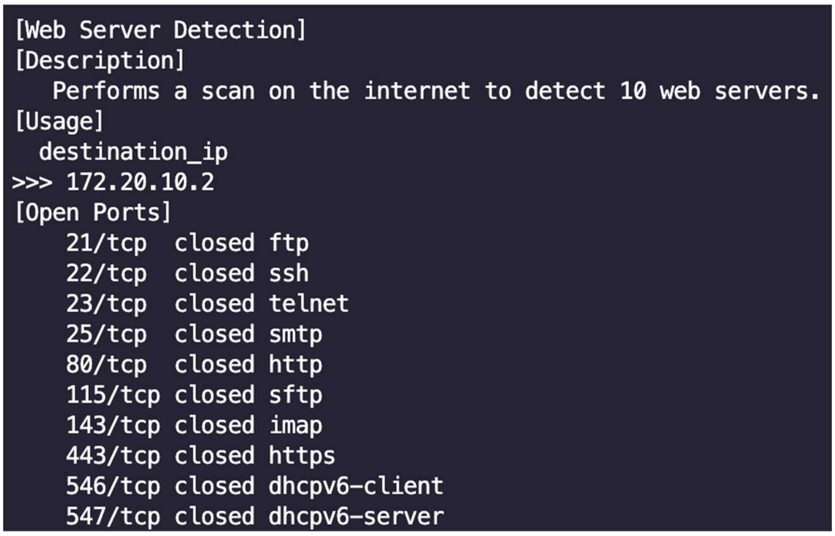
```
[OS Fingerprint Identification]
[Description]
   Identifies the OS of the hosts that are alive.

No exact OS found for 172.20.10.2:5000. Here are some guesses:
[OS Versions]
    Apple macOS 10.14 (Mojave) (Darwin 18.2.0 - 18.6.0) (97%)
    Apple Mac OS X 10.5 (Leopard) - 10.6.7 (Snow Leopard) (Darwin 9.0.0 - 10.7.0) (90%)
    Apple Mac OS X 10.7.0 - 10.7.4 (Lion) (Darwin 11.0.0 - 11.4.0) or iPhone mobile phone (iOS 4.3.2) (90%)
    Apple Mac OS X 10.7.5 (Mountain Lion) (Darwin 11.4.2) (90%)
    Apple OS X 10.10 (Yosemite) - 10.12 (Sierra) (Darwin 14.0.0 - 16.1.0) (90%)
    Apple Mac OS X 10.7.0 - 10.7.4 (Lion) (Darwin 11.0.0 - 11.3.0) (90%)
    Apple Mac OS X 10.6 (Snow Leopard) (Darwin 10.0.0) (90%)
    Apple Mac OS X 10.7.2 - 10.7.3 (Lion) (Darwin 11.2.0 - 11.3.0) (90%)
    Apple OS X 10.8 (Mountain Lion) - 10.9 (Mavericks) (Darwin 12.0.0 - 13.4.0) or iOS 5.0.1 (90%)
    Apple macOS 10.13 (High Sierra) - 10.15 (Catalina) or iOS 11.0 - 13.4 (Darwin 17.0.0 - 19.2.0) (90%)
```

4) web_server_detection

Scans the Internet and discovers 10 web-server addresses, protocols, and ports of each web server. Saves the results in web.dat.

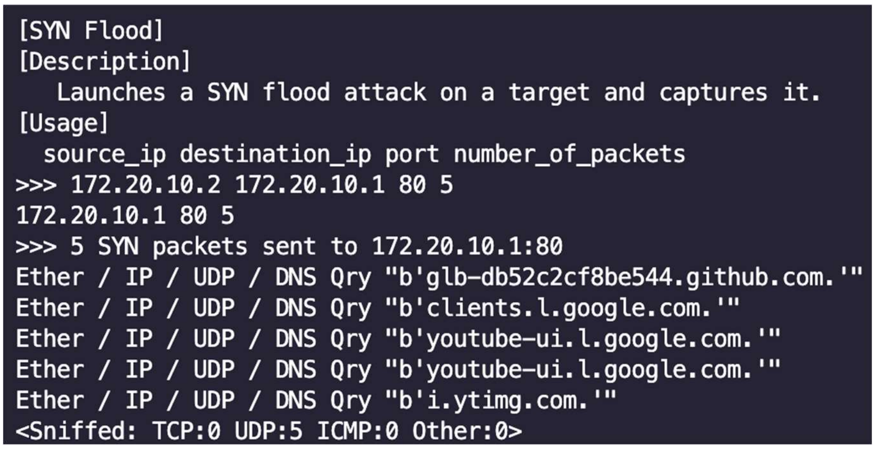
21: (ftp control) 22: (ssh) 23: (telnet) 25: (smtp) 80: (http) 115: (sftp) 143: (imap) 443: (https) 546: (dhcp client) 547: (dhcp server)



```
[Web Server Detection]
[Description]
   Performs a scan on the internet to detect 10 web servers.
[Usage]
  destination_ip
>>> 172.20.10.2
[Open Ports]
    21/tcp  closed ftp
    22/tcp  closed ssh
    23/tcp  closed telnet
    25/tcp  closed smtp
    80/tcp  closed http
    115/tcp closed sftp
    143/tcp closed imap
    443/tcp closed https
    546/tcp closed dhcpv6-client
    547/tcp closed dhcpv6-server
```

5) syn_flood

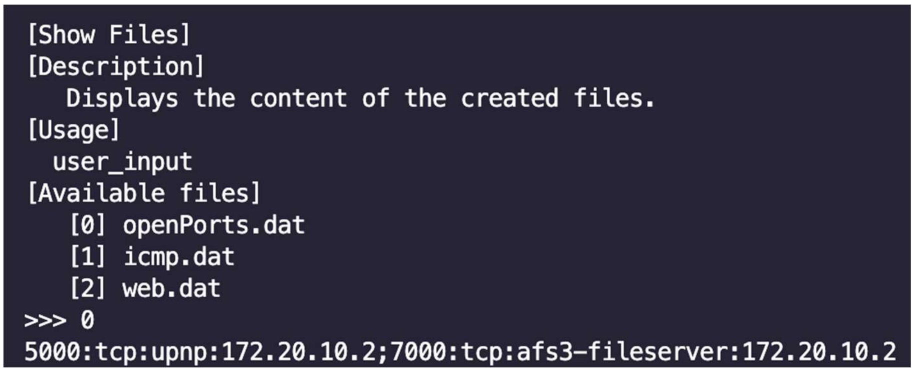
Launches SYN-flood attack to a given destination (IP) and port(s). While attacking, captures and decodes TCP and IP packet headers and saves them in SYNresults.txt.



```
[SYN Flood]
[Description]
   Launches a SYN flood attack on a target and captures it.
[Usage]
  source_ip destination_ip port number_of_packets
>>> 172.20.10.2 172.20.10.1 80 5
172.20.10.1 80 5
>>> 5 SYN packets sent to 172.20.10.1:80
Ether / IP / UDP / DNS Qry "b'glb-db52c2cf8be544.github.com.'"
Ether / IP / UDP / DNS Qry "b'clients.l.google.com.'"
Ether / IP / UDP / DNS Qry "b'youtube-ui.l.google.com.'"
Ether / IP / UDP / DNS Qry "b'youtube-ui.l.google.com.'"
Ether / IP / UDP / DNS Qry "b'i.ytimg.com.'"
<Sniffed: TCP:0 UDP:5 ICMP:0 Other:0>
```

6) show

Asks and displays the contents of the files that your tools have created so far.



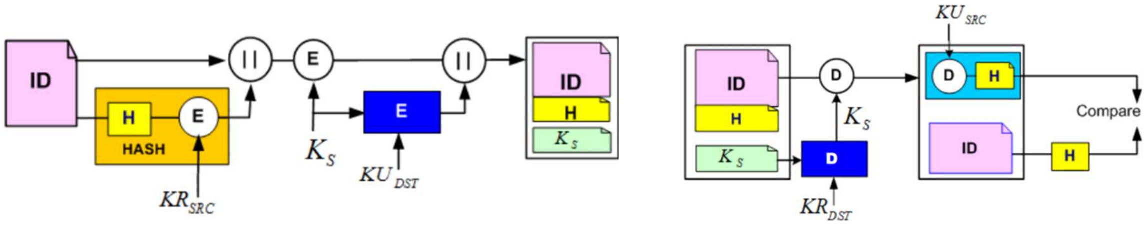
```
[Show Files]
[Description]
   Displays the content of the created files.
[Usage]
  user_input
[Available files]
   [0] openPorts.dat
   [1] icmp.dat
   [2] web.dat
>>> 0
5000:tcp:upnp:172.20.10.2;7000:tcp:afs3-fileserver:172.20.10.2
```

II. Secure Authentication

This section of the manual describes the contents and usage of the **secAuth.py** script.

1) Authentication System

The secure authentication is implemented with both asymmetric key encryption (using RSA) and symmetric key encryption (using Blum Blum Shub session key generation). The block diagram of the system is the following:



(a) Source *(b) Destination*

D = Decrypt	KR = Private Key	H = Hash	| | = Concatenate
E = Encrypt	KU = Public Key	Ks = Session Key	

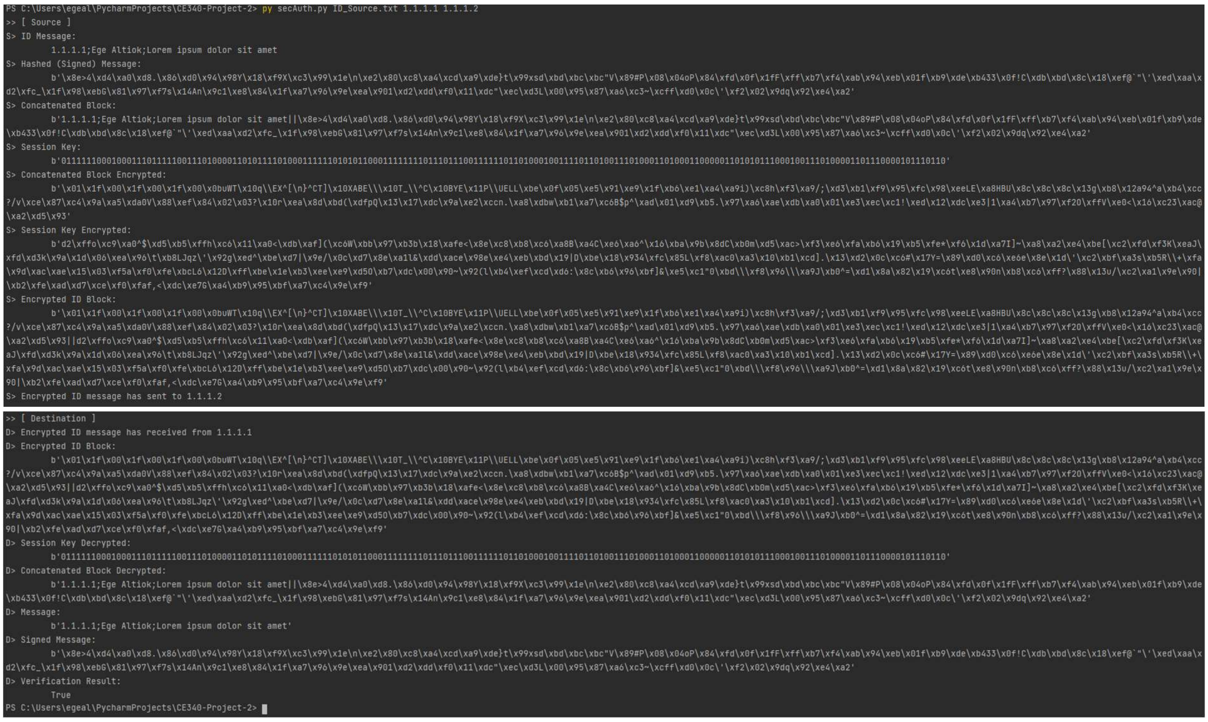
2) Usage

The secAuth.py script can be run in a command line interface using the line below:

>>> [python | py] secAuth.py [file_path] [src_address] [dst_address]

Example code:

>>> py secAuth.py ID.txt 1.1.1.1* 1.1.1.2



```
PS C:\Users\egeal\PycharmProjects\CE340-Project-2> py secAuth.py ID_Source.txt 1.1.1.1 1.1.1.2
>> [ Source ]
S> ID Message:
        1.1.1.1;Ege Altiok;Lorem ipsum dolor sit amet
S> Hashed (Signed) Message:
        b'\x8e>4\xd4\xa0\xd8.\x86\xd0\x94\x98Y\x18\xf9X\xc3\x99\x1e\n\xe2\x80\xc8\xa4\xcd\xa9\xde}t\x99xsd\xbd\xbc\xbc"V\x89#P\x08\x04oP\x84\xfd\x0f\x1fF\xff\xb7\xf4\xab\x94\xeb\x01f\xb9\xde\xb433\x0f!C\xdb\xbd\x8c\x18\xef@`"\'\xed\xaa\x
d2\xfc_\x1f\x98\xebG\x81\x97\xf7s\x14An\x9c1\xe8\x84\x1f\xa7\x96\x9e\xea\x901\xd2\xdd\xf0\x11\xdc"\xec\xd3L\x00\x95\x87\xa6\xc3~\xcff\xd0\x0c\'\xf2\x02\x9dq\x92\xe4\xa2'
S> Concatenated Block:
        b'1.1.1.1;Ege Altiok;Lorem ipsum dolor sit amet||\x8e>4\xd4\xa0\xd8.\x86\xd0\x94\x98Y\x18\xf9X\xc3\x99\x1e\n\xe2\x80\xc8\xa4\xcd\xa9\xde}t\x99xsd\xbd\xbc\xbc"V\x89#P\x08\x04oP\x84\xfd\x0f\x1fF\xff\xb7\xf4\xab\x94\xeb\x01f\xb9\xde
\xb433\x0f!C\xdb\xbd\x8c\x18\xef@`"\'\xed\xaa\xd2\xfc_\x1f\x98\xebG\x81\x97\xf7s\x14An\x9c1\xe8\x84\x1f\xa7\x96\x9e\xea\x901\xd2\xdd\xf0\x11\xdc"\xec\xd3L\x00\x95\x87\xa6\xc3~\xcff\xd0\x0c\'\xf2\x02\x9dq\x92\xe4\xa2'
S> Session Key:
        b'011111100010001110111110011101000011010111101000111111010101100011111111011101110011111101101000100111101101001110100011010001100000110101011100010011101000011011100000101110110'
S> Concatenated Block Encrypted:
        b'\x01\x1f\x00\x1f\x00\x1f\x00\x0buWT\x10q\\EX^[\n}^CT]\x10XABE\\\x10T_\\^C\x10BYE\x11P\\UELL\xbe\x0f\x05\xe5\x91\xe9\x1f\xb6\xe1\xa4\xa9i)\xc8h\xf3\xa9/;\xd3\xb1\xf9\x95\xfc\x98\xeeLE\xa8HBU\x8c\x8c\x8c\x13g\xb8\x12a94^a\xb4\xcc
?/v\xce\x87\xc4\x9a\xa5\xda0V\x88\xef\x84\x02\x03?\x10r\xea\x8d\xbd(\xdfpQ\x13\x17\xdc\x9a\xe2\xccn.\xa8\xdbw\xb1\xa7\xc6B$p^\xad\x01\xd9\xb5.\x97\xa6\xae\xdb\xa0\x01\xe3\xec\xc1!\xed\x12\xdc\xe3|1\xa4\xb7\x97\xf20\xffV\xe0<\x16\xc23\xac@
\xa2\xd5\x93'
S> Session Key Encrypted:
        b'd2\xffo\xc9\xa0^$\xd5\xb5\xffh\xc6\x11\xa0<\xdb\xaf](\xc6W\xbb\x97\xb3b\x18\xafe<\x8e\xc8\xb8\xc6\xa8B\xa4C\xe6\xa6^\x16\xba\x9b\x8dC\xb0m\xd5\xac>\xf3\xe6\xfa\xb6\x19\xb5\xfe*\xf6\x1d\xa7I]~\xa8\xa2\xe4\xbe[\xc2\xfd\xf3K\xeaJ\
xfd\xd3k\x9a\x1d\x06\xea\x96\t\xb8LJqz\'\x92g\xed^\xbe\xd7|\x9e/\x0c\xd7\x8e\xa1l&\xdd\xace\x98e\xe4\xeb\xbd\x19|D\xbe\x18\x934\xfc\x85L\xf8\xac0\xa3\x10\xb1\xcd].\x13\xd2\x0c\xc6#\x17Y=\x89\xd0\xc6\xe6e\x8e\x1d\'\xc2\xbf\xa3s\xb5R\\+\xfa
\x9d\xac\xae\x15\x03\xf5a\xf0\xfe\xbcL6\x12D\xff\xbe\x1e\xb3\xee\xe9\xd50\xb7\xdc\x00\x90~\x92(l\xb4\xef\xcd\xd6:\x8c\xb6\x96\xbf]&\xe5\xc1"0\xbd\\\xf8\x96\\\xa9J\xb0^=\xd1\x8a\x82\x19\xc6t\xe8\x90n\xb8\xc6\xff?\x88\x13u/\xc2\xa1\x9e\x90|
\xb2\xfe\xad\xd7\xce\xf0\xfaf,<\xdc\xe7G\xa4\xb9\x95\xbf\xa7\xc4\x9e\xf9'
S> Encrypted ID Block:
        b'\x01\x1f\x00\x1f\x00\x1f\x00\x0buWT\x10q\\EX^[\n}^CT]\x10XABE\\\x10T_\\^C\x10BYE\x11P\\UELL\xbe\x0f\x05\xe5\x91\xe9\x1f\xb6\xe1\xa4\xa9i)\xc8h\xf3\xa9/;\xd3\xb1\xf9\x95\xfc\x98\xeeLE\xa8HBU\x8c\x8c\x8c\x13g\xb8\x12a94^a\xb4\xcc
?/v\xce\x87\xc4\x9a\xa5\xda0V\x88\xef\x84\x02\x03?\x10r\xea\x8d\xbd(\xdfpQ\x13\x17\xdc\x9a\xe2\xccn.\xa8\xdbw\xb1\xa7\xc6B$p^\xad\x01\xd9\xb5.\x97\xa6\xae\xdb\xa0\x01\xe3\xec\xc1!\xed\x12\xdc\xe3|1\xa4\xb7\x97\xf20\xffV\xe0<\x16\xc23\xac@
\xa2\xd5\x93||d2\xffo\xc9\xa0^$\xd5\xb5\xffh\xc6\x11\xa0<\xdb\xaf](\xc6W\xbb\x97\xb3b\x18\xafe<\x8e\xc8\xb8\xc6\xa8B\xa4C\xe6\xa6^\x16\xba\x9b\x8dC\xb0m\xd5\xac>\xf3\xe6\xfa\xb6\x19\xb5\xfe*\xf6\x1d\xa7I]~\xa8\xa2\xe4\xbe[\xc2\xfd\xf3K\xe
aJ\xfd\xd3k\x9a\x1d\x06\xea\x96\t\xb8LJqz\'\x92g\xed^\xbe\xd7|\x9e/\x0c\xd7\x8e\xa1l&\xdd\xace\x98e\xe4\xeb\xbd\x19|D\xbe\x18\x934\xfc\x85L\xf8\xac0\xa3\x10\xb1\xcd].\x13\xd2\x0c\xc6#\x17Y=\x89\xd0\xc6\xe6e\x8e\x1d\'\xc2\xbf\xa3s\xb5R\\+\
xfa\x9d\xac\xae\x15\x03\xf5a\xf0\xfe\xbcL6\x12D\xff\xbe\x1e\xb3\xee\xe9\xd50\xb7\xdc\x00\x90~\x92(l\xb4\xef\xcd\xd6:\x8c\xb6\x96\xbf]&\xe5\xc1"0\xbd\\\xf8\x96\\\xa9J\xb0^=\xd1\x8a\x82\x19\xc6t\xe8\x90n\xb8\xc6\xff?\x88\x13u/\xc2\xa1\x9e\x
90|\xb2\xfe\xad\xd7\xce\xf0\xfaf,<\xdc\xe7G\xa4\xb9\x95\xbf\xa7\xc4\x9e\xf9'
S> Encrypted ID message has sent to 1.1.1.2
```

```
>> [ Destination ]
D> Encrypted ID message has received from 1.1.1.1
D> Encrypted ID Block:
        b'\x01\x1f\x00\x1f\x00\x1f\x00\x0buWT\x10q\\EX^[\n}^CT]\x10XABE\\\x10T_\\^C\x10BYE\x11P\\UELL\xbe\x0f\x05\xe5\x91\xe9\x1f\xb6\xe1\xa4\xa9i)\xc8h\xf3\xa9/;\xd3\xb1\xf9\x95\xfc\x98\xeeLE\xa8HBU\x8c\x8c\x8c\x13g\xb8\x12a94^a\xb4\xcc
?/v\xce\x87\xc4\x9a\xa5\xda0V\x88\xef\x84\x02\x03?\x10r\xea\x8d\xbd(\xdfpQ\x13\x17\xdc\x9a\xe2\xccn.\xa8\xdbw\xb1\xa7\xc6B$p^\xad\x01\xd9\xb5.\x97\xa6\xae\xdb\xa0\x01\xe3\xec\xc1!\xed\x12\xdc\xe3|1\xa4\xb7\x97\xf20\xffV\xe0<\x16\xc23\xac@
\xa2\xd5\x93||d2\xffo\xc9\xa0^$\xd5\xb5\xffh\xc6\x11\xa0<\xdb\xaf](\xc6W\xbb\x97\xb3b\x18\xafe<\x8e\xc8\xb8\xc6\xa8B\xa4C\xe6\xa6^\x16\xba\x9b\x8dC\xb0m\xd5\xac>\xf3\xe6\xfa\xb6\x19\xb5\xfe*\xf6\x1d\xa7I]~\xa8\xa2\xe4\xbe[\xc2\xfd\xf3K\xe
aJ\xfd\xd3k\x9a\x1d\x06\xea\x96\t\xb8LJqz\'\x92g\xed^\xbe\xd7|\x9e/\x0c\xd7\x8e\xa1l&\xdd\xace\x98e\xe4\xeb\xbd\x19|D\xbe\x18\x934\xfc\x85L\xf8\xac0\xa3\x10\xb1\xcd].\x13\xd2\x0c\xc6#\x17Y=\x89\xd0\xc6\xe6e\x8e\x1d\'\xc2\xbf\xa3s\xb5R\\+\
xfa\x9d\xac\xae\x15\x03\xf5a\xf0\xfe\xbcL6\x12D\xff\xbe\x1e\xb3\xee\xe9\xd50\xb7\xdc\x00\x90~\x92(l\xb4\xef\xcd\xd6:\x8c\xb6\x96\xbf]&\xe5\xc1"0\xbd\\\xf8\x96\\\xa9J\xb0^=\xd1\x8a\x82\x19\xc6t\xe8\x90n\xb8\xc6\xff?\x88\x13u/\xc2\xa1\x9e\x
90|\xb2\xfe\xad\xd7\xce\xf0\xfaf,<\xdc\xe7G\xa4\xb9\x95\xbf\xa7\xc4\x9e\xf9'
D> Session Key Decrypted:
        b'011111100010001110111110011101000011010111101000111111010101100011111111011101110011111101101000100111101101001110100011010001100000110101011100010011101000011011100000101110110'
D> Concatenated Block Decrypted:
        b'1.1.1.1;Ege Altiok;Lorem ipsum dolor sit amet||\x8e>4\xd4\xa0\xd8.\x86\xd0\x94\x98Y\x18\xf9X\xc3\x99\x1e\n\xe2\x80\xc8\xa4\xcd\xa9\xde}t\x99xsd\xbd\xbc\xbc"V\x89#P\x08\x04oP\x84\xfd\x0f\x1fF\xff\xb7\xf4\xab\x94\xeb\x01f\xb9\xde
\xb433\x0f!C\xdb\xbd\x8c\x18\xef@`"\'\xed\xaa\xd2\xfc_\x1f\x98\xebG\x81\x97\xf7s\x14An\x9c1\xe8\x84\x1f\xa7\x96\x9e\xea\x901\xd2\xdd\xf0\x11\xdc"\xec\xd3L\x00\x95\x87\xa6\xc3~\xcff\xd0\x0c\'\xf2\x02\x9dq\x92\xe4\xa2'
D> Message:
        b'1.1.1.1;Ege Altiok;Lorem ipsum dolor sit amet'
D> Signed Message:
        b'\x8e>4\xd4\xa0\xd8.\x86\xd0\x94\x98Y\x18\xf9X\xc3\x99\x1e\n\xe2\x80\xc8\xa4\xcd\xa9\xde}t\x99xsd\xbd\xbc\xbc"V\x89#P\x08\x04oP\x84\xfd\x0f\x1fF\xff\xb7\xf4\xab\x94\xeb\x01f\xb9\xde\xb433\x0f!C\xdb\xbd\x8c\x18\xef@`"\'\xed\xaa\x
d2\xfc_\x1f\x98\xebG\x81\x97\xf7s\x14An\x9c1\xe8\x84\x1f\xa7\x96\x9e\xea\x901\xd2\xdd\xf0\x11\xdc"\xec\xd3L\x00\x95\x87\xa6\xc3~\xcff\xd0\x0c\'\xf2\x02\x9dq\x92\xe4\xa2'
D> Verification Result:
        True
PS C:\Users\egeal\PycharmProjects\CE340-Project-2> ▮
```

***Warning:** The contents of the ID.txt given to the script must include the source address in the beginning of the file for validating the source address.

Example ID.txt: 1.1.1.1;Ege Altiok;Lorem ipsum dolor sit amet