CERT-IS Seminar

designed By. 스마일게이트

INDEX

0x02

Socket Programming

편지를 보내기 위한 가정

1. 편지를 받을 주소
2. 우편함

데이터를 보내기 위한 가정

1. 데이터를 받을 주소(IP)
2. PORT

02 Socket Programming

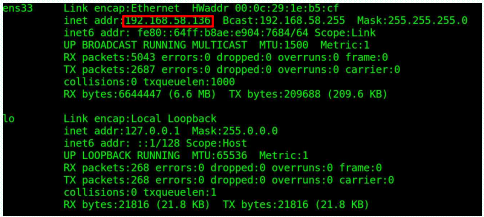
Socket?

대충 65000개 이상 있는 그림

편지 : xx아파트 102동 304호

네트워크 : 123.45.67.89 : 8080

ctrl + alt + t 눌러서 cmd창 뜨면 ifconfig



편지 : xx아파트 102동 304호

네트워크 : 123.45.67.89 : 8080

PORT를 열기 위해서는 프로그램을 짜거나 사용한다.
우선 nc(netcat)을 사용하여 포트를 열어보기로 하자.

ctrl + alt + t 눌러서 cmd창 nc -lvp 숫자
ex) nc -lvp 4949

```
root@ubuntu:/home# nc -lvp 4949
Listening on [0.0.0.0] (family 0, port 4949)
```

```
sakuya@ubuntu:~$ netstat -ano |grep 4949
tcp        0      0 0.0.0.0:4949            0.0.0.0:*               LISTEN      off (0.00/0/0)
```


편지 : xx아파트 102동 304호

네트워크 : 123.45.67.89 : 8080

ctrl + alt + t -> nc IP 아까입력한 숫자 엔터
ex)nc 1.2.3.4 4949
쓰고싶은말 엔터
종료시 ctrl+c

```
root@ubuntu:/home# nc -lvp 4949
Listening on [0.0.0.0] (family 0, port 4949)
```

```
sakuya@ubuntu:~$ netstat -ano |grep 4949
tcp        0      0 0.0.0.0:4949            0.0.0.0:*               LISTEN      off (0.00/0/0)
```

생각대로 안되면 nc 127.0.0.1 숫자

nc는 내가 원하는 처리를 해주기 어려움
그래서 프로그램을 만들어서 처리해 주도록 하자

vi network.py

```
from socket import *

IP = "127.0.0.1"
PORT = 4949
s = socket()
s.bind((IP,PORT))
s.listen(10)
while 1:
    (cs,addr) = s.accept()
    print(addr[0] + cs.recv(1024))
```

작성후 esc, :wq 엔터

python3 network.py

ctrl + alt + T , nc 127.0.0.1 포트번호

보낼 메세지후 엔터 엔터..


```
1  from socket import * #include 같은거
2
3  IP = "127.0.0.1"     # 우리집 주소 (102동)
4  PORT = 4949          # 우리집 호실 (304호)
5  s = socket ()        # 편지함을 만들었다
6  s.bind((IP,PORT))    # 편지함을 설치했다
7  s.listen(10)         # 편지함이 받을 준비가 됐다
8  while 1:
9      (cs,addr) = s.accept()          #편지가 오면
10     print(addr[0] + cs.recv(1024))  #내용을 읽는다
```

이제까지 만든건 서버(편지함)이고

편지를 쓰는 프로그램(클라이언트)을 만들어보자

데이터를 전송하는 프로그램을 만든다

vi sender.py

```
from socket import *

IP = "127.0.0.1"
PORT = 4949
s = socket()
s.connect((IP,PORT))

while(1):
    data = input(">> ")
    s.send(data)
```

network.py와 같게

작성후 esc, :wq 엔터

python3 network.py&

python3 sender.py

보낼 메세지후 엔터 엔터..

tor를 통해 데이터를 전송하는 프로그램을 만든다

tor를 깔아야함..
apt-get install tor

```
root@sakuya-Izayoi:/home/sakuya# apt-get install tor
Reading package lists... Done
Building dependency tree
Reading state information... Done
tor is already the newest version (0.3.2.10-1).
0 upgraded, 0 newly installed, 0 to remove and 68 not upgraded.
```


tor를 통해 데이터를 전송하는 프로그램을 만든다

설치가 완료되면 tor& 입력후 엔터

```
root@sakuya-Izayoi:/home/sakuya# tor
Nov 10 00:01:10.614 [notice] Tor 0.3.2.10 (git-0edaa32732ec8930) running on Linux with Libevent 2.1.8-
 5.2.2, and Libzstd 1.3.3.
Nov 10 00:01:10.614 [notice] Tor can't help you if you use it wrong! Learn how to be safe at https://w
Nov 10 00:01:10.614 [notice] Read configuration file "/etc/tor/torrc".
Nov 10 00:01:10.619 [warn] Skipping obsolete configuration option 'ControlListenAddress'
Nov 10 00:01:10.619 [notice] Scheduler type KIST has been enabled.
Nov 10 00:01:10.619 [notice] Opening Socks listener on 127.0.0.1:9050
Nov 10 00:01:10.619 [notice] Opening Control listener on 127.0.0.1:9051
Nov 10 00:01:10.000 [notice] Parsing GEOIP IPv4 file /usr/share/tor/geoip.
Nov 10 00:01:10.000 [notice] Parsing GEOIP IPv6 file /usr/share/tor/geoip6.
Nov 10 00:01:10.000 [warn] You are running Tor as root. You don't need to, and you probably shouldn't.
Nov 10 00:01:10.000 [notice] Bootstrapped 0%: Starting
Nov 10 00:01:11.000 [notice] Starting with guard context "default"
Nov 10 00:01:11.000 [notice] Bootstrapped 80%: Connecting to the Tor network
```


데이터를 전송하는 프로그램을 만든다

vi sender.py

```
import socket
import socks

socks.setdefaultproxy(socks.PROXY_TYPE_SOCKS5,"127.0.0.1",9050)
socket.socket = socks.socksocket

URL = "Onion Protocol URL"
SERVICE_PORT = 1234
IP = URL

s = socket.socket()
s.connect((IP,PORT))
r = s.recv(4096)
s.send("data")
```


돼는지 안돼는지 어케 아냐구요?

그게 과제입니다

vafy5px7jhsqgq35.onion : 80 에 접속해서 출력하는 문자열을

스크린샷 찍어서 조교에게 제출하세요.
코드도 스크린샷을 찍어서 제출하거나 파일을 제출해주시면 됩니다.

parsing

받은 데이터를 특정한 기준으로 가공해서 원하는 데이터를 얻는방법

```
data = """
ID: Sakuya
Nick: Sakuya
Password: Sakuya
----------
ID: Newbie
Nick: Hacker
Password: IDK
"""


splited = data.split("----------")
print("FIRST : \n" + splited[0])
print("SECOND : \n" + splited[1])
```

```
root@sakuya-Izayoi:/home/sakuya# python3 cust_protocol.py
FIRST :

ID: Sakuya
Nick: Sakuya
Password: Sakuya

SECOND :

ID: Newbie
Nick: Hacker
Password: IDK
```


parsing

어떤것을 기준으로 자르느냐에 따라
데이터 처리를 위한 코드 길이가 달라짐..

나만의 프로토콜을 만들어서 통신에 적용을 해보자.

내가 코딩능력이 부족하면 선배나 저에게 도움을 요청하세요.

과제로 제출해 주시면 되겠습니다.

1.담당조교에게 개인메세지

2.파일 업로드후 댓글에 !report 입력

02 Socket Programming

Report

1.담당조교에게 개인메세지

2.파일 업로드후 댓글에 !report 입력

3. 업로드가 성공하면 제출완료라고 알려줌.


```
root@e3f7f778d371:/home/discord/report# ls
Sakuya#5626
root@e3f7f778d371:/home/discord/report# find
.
./Sakuya#5626
./Sakuya#5626/report1.png
root@e3f7f778d371:/home/discord/report#
```

Socket Prog.

End Of Document

