1번 문제 과정

- 룰 파일 생성

```
vim /etc/suricata/rules/local.rules
```

- 룰 추가

```
alert dns any any -> any any (msg:"DNS message detected"; dns.query;
content:".com";sid:9999;)
```

- 룰 파일을 사용해서 Suricata 파일 읽기

```
suricata -r 2025-01-22-traffic-analysis-exercise.pcap -l . -S /etc/
suricata/rules/local.rules
```

- rrname 중복 없이 순서대로 나열

```
jq 'select(.alert.signature_id==9999) | .dns.queries[]?.rrname'
eve.json | sort | uniq
```

1번 문제 정답

1-1.

```
alert dns any any -> any any (msg:"DNS message detected"; dns.query;
content:".com";sid:9999;)
```

1-2.

```
"assets[.]msn[.]com"
```

2번 문제 과정

- 룰 추가

```
alert http any any => any any (msg:"GET request approved"; http.method; content:"GET"; http.stat_code; content:"200"; sid:999;)
```

- 룰 파일을 사용해서 Suricata 파일 읽기

```
suricata -r 2025-01-22-traffic-analysis-exercise.pcap -l . -S /etc/suricata/rules/local.rules
```

- URL들 중복 없이 순서대로 나열

```
jq 'select(.alert.signature_id==999).http.url' eve.json | sort | uniq
```

2번 문제 정답

2-1.

```
alert http any any => any any (msg:"GET request approved"; http.method; content:"GET"; http.stat_code; content:"200"; sid:999;)
```

2-2.

```
"/1517096937"
"/api/file/get-file/264872"
"/api/file/get-file/29842.ps1"
"/api/file/get-file/TeamViewer"
"/c/msdownload/update/others/2025/01/42681408_eba72ad8cac00ea04690b09c0ff175074bb281e9.cab"
```

```
"/c/msdownload/update/others/
2025/01/42681409_9e243120ff356d59920855fa02c873fcbcf678c6.cab"
"/c/msdownload/update/others/
2025/01/42681502_106431d428d2c49b06bf00d7ab662ff53edb4726.cab"
"/connecttest.txt"
"/din.aspx?
s=00000000&id=0&client=DynGate&rnd=15187500&p=10000001"
"/din.aspx?
s=00000000&id=0&client=DynGate&rnd=216758732&p=10000001"
"/din.aspx?
s=00000000&id=0&client=DynGate&rnd=418412399&p=10000001"
"/din.aspx?
s=00000000&id=0&client=DynGate&rnd=427975263&p=10000001"
"/din.aspx?
s=00000000&id=0&client=DynGate&rnd=5384120&p=10000001"
"/din.aspx?s=91930119&id=0&client=DynGate&p=10000002"
"/din.aspx?s=91930135&id=0&client=DynGate&p=10000002"
"/din.aspx?s=91930144&id=0&client=DynGate&p=10000002"
"/din.aspx?s=91930165&id=0&client=DynGate&p=10000002"
"/din.aspx?s=91930189&id=0&client=DynGate&p=10000002"
"/dout.aspx?
s=91930119&p=10000001&client=DynGate&data=FyQSkgCjHqkys5MkoZ6
ZGhycGJuamZMkoh6YEyY3s7O0tzOemJMmoKGemDwYGDIYMRuZGxowm-
5ovmLIwnBoYGrIxmxucMbKxr5iamJuYHJscmZuTJqSiHpg8GBgyGDEbmRs-
aMJuaL5iyMJwaGBqyMZsbnDGysa+YmpibmBybHJmbkyepnqu0txuTKx6al-
xgXG5obnBAoqQ=="
"/dout.aspx?
s=91930135&p=10000001&client=DynGate&data=FyQSkgCjHqkys5MkoZ6
ZGhycGJuamZMkoh6YEyY3s7O0tzOemJMmoKGemDwYGDIYMRuZGxowm-
5ovmLIwnBoYGrIxmxucMbKxr5iamJuYHJscmZuTJqSiHpg8GBgyGDEbmRs-
aMJuaL5iyMJwaGBqyMZsbnDGysa+YmpibmBybHJmbkyepnqu0txuTKx6al-
xgXG5obnBAoqQ=="
```

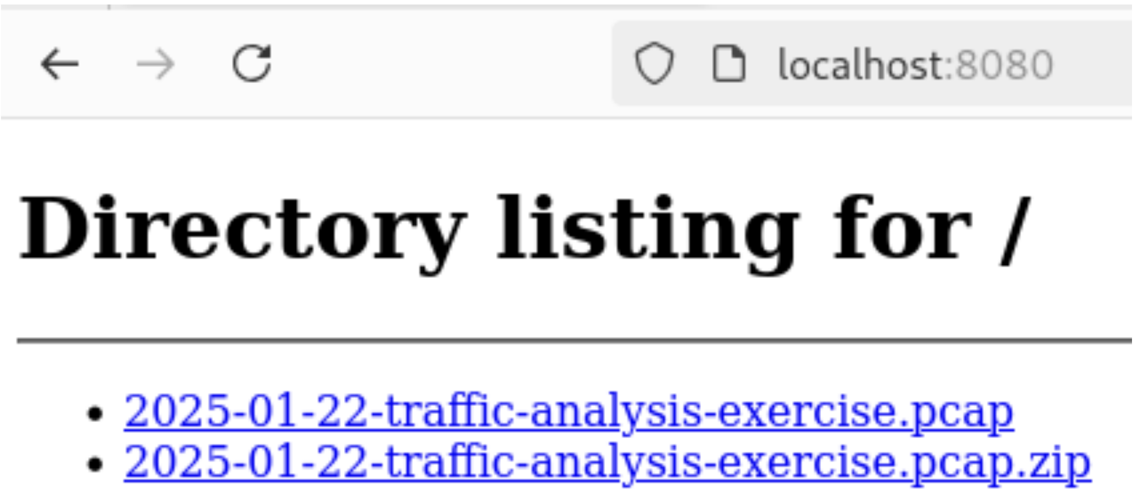
```
"/dout.aspx?
s=91930144&p=10000001&client=DynGate&data=FyQSkgCjHqkys5MkoZ6
ZGhycGJuamZMkoh6YEyY3s7O0tzOemJMmoKGemDwYGDIYMRuZGxowm-
5ovmLIwnBoYGrIxmxucMbKxr5iamJuYHJscmZuTJqSiHpg8GBgyGDEbmRs-
aMJuaL5iyMJwaGBqyMZsbnDGysa+YmpibmBybHJmbkyepnqu0txuTKx6al-
xgXG5obnBAoqQ=="
"/dout.aspx?
s=91930165&p=10000001&client=DynGate&data=FyQSkgCjHqkys5MkoZ6
ZGhycGJuamZMkoh6YEyY3s7O0tzOemJMmoKGemDwYGDIYMRuZGxowm-
5ovmLIwnBoYGrIxmxucMbKxr5iamJuYHJscmZuTJqSiHpg8GBgyGDEbmRs-
aMJuaL5iyMJwaGBqyMZsbnDGysa+YmpibmBybHJmbkyepnqu0txuTKx6al-
xgXG5obnBAoqQ=="
"/dout.aspx?
s=91930189&p=10000001&client=DynGate&data=FyQSkgCjHqkys5MkoZ6
ZGhycGJuamZMkoh6YEyY3s7O0tzOemJMmoKGemDwYGDIYMRuZGxowm-
5ovmLIwnBoYGrIxmxucMbKxr5iamJuYHJscmZuTJqSiHpg8GBgyGDEbmRs-
aMJuaL5iyMJwaGBqyMZsbnDGysa+YmpibmBybHJmbkyepnqu0txuTKx6al-
xgXG5obnBAoqQ=="
"/filestreamingservice/files/2a0d597c-a09c-4400-be86-87596dd2e696?
P1=1737884967&P2=404&P3=2&P4=W7WOpOZ6ahXXhvqsFdcWAJHdZVPv-
8SRh1FficfbizECNzzxIRLbCNa6F6JoXegoy4yxszlyc4ZC4KfWUOr2RSA%3d%3
d"
"/filestreamingservice/files/2ed1297e-f6c9-4355-aec4-433ea371b116?
P1=1737884967&P2=404&P3=2&P4=DQ%2frdpZetb6%2bCA7SUqmOgjEU-
a0b3x%2f0slORjy3dXLFk%2fx6KtXqpmjgm4wKw8TSyht7Eu00wi6QlvL9zKq-
BzIFw%3d%3d"
```

3번 문제 과정

- HTTP 서버 역할하는 파이썬 코드 실행

```
python3 -m http.server 8080
```

- HTTP 서버 연결 확인



Directory listing for /

- 2025-01-22-traffic-analysis-exercise.pcap
- 2025-01-22-traffic-analysis-exercise.pcap.zip

- HTTP 패킷 전부 차단하는 룰 추가

```
drop http any any -> 127.0.0.1 any (msg:"Packet dropped..."; sid:1;)
```

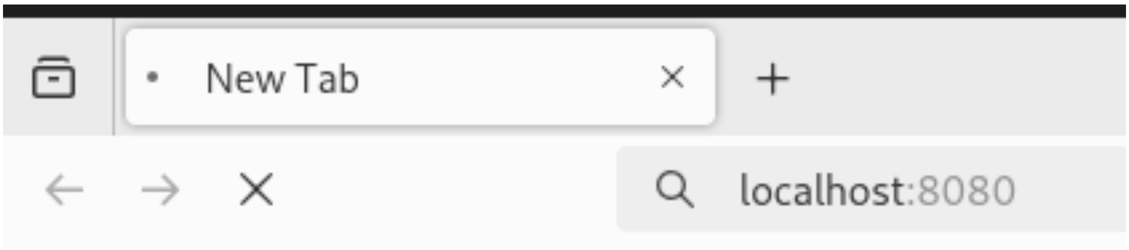
- iptables 설정

```
sudo iptables -I OUTPUT -j NFQUEUE --queue-num 0
sudo iptables -I INPUT -j NFQUEUE --queue-num 0
```

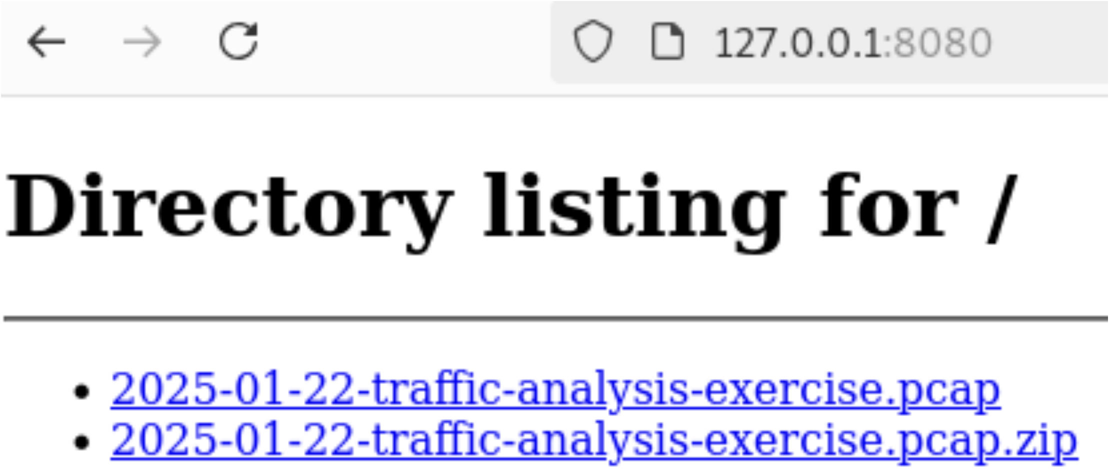
- Suricata IPS 모드로 실행

```
sudo suricata -c /etc/suricata/suricata.yaml -q 0 -S /etc/suricata/
rules/local.rules
```

- HTTP 서버 연결 확인



- 룰 제거하고 Suricata 다시 실행
- HTTP 서버 연결 확인



Directory listing for /

- 2025-01-22-traffic-analysis-exercise.pcap
- 2025-01-22-traffic-analysis-exercise.pcap.zip

- iptable 원상복구

```
sudo iptables -D OUTPUT 1
sudo iptables -D INPUT 1
```