# Wykrywanie ataków sieciowych - lab 4

## Zadanie 1

Należy zamienić keyword `http_header` na `http_post`.

```
drop tcp any any -> any any (msg:”facebook is blocked”, content:"facebook.com";
http_post; nocase; classtype:policy-violation;
> sid:1;)
```

## Zadanie 2

```
alert udp any any -> any any (msg: “netcat UDP transfer detected”; content:”
tajneDane”; replace: “*********”;)
```

## Zadanie 3

Ponieważ reguła IPS NFQUEUE jest regułą końcową, wszystkie wcześniejsze reguły ACCEPT usuną pakiety z analizy IPS, albo każda decyzja po regułach IPS zostanie zignorowana. Rozwiązaniem tego problemu jest użycie funkcji NF_REPEAT. Reguła ta jest umieszczana na pierwszym miejscu, a IPS wydaje wtedy werdykt NF_REPEAT zamiast NF_ACCEPT dla zaakceptowanych pakietów. Jedyny problemem jest wówczas nieskończona pętla. Można jej jednak łatwo uniknąć, oznaczając pakiety, które zostały już przetworzone przez IPS.