On November 8th (15h-room 4.3.30) you will have the first evaluation moment.  
  
You have to make a short presentation about the project idea and planning, 10 minutes maximum. The presentation must include the following topics:  
  
- Identified security problem, including the importance of the security issue/solution; (7 points)  
  
- Data sources. Including the real world scenario to acquire that data; (4 points)  
  
- Test scenario or used datasets; (3 points)  
  
- Data processing (data filtering, data sampling/aggregation and observation processes) applied to raw data (planned, may change later); (3 points)  
  
- Features to extract from processed data (planned, may change later). (3 points)

**Melhorias:**

Tentar procurar CVE’s

**Data source:**

Normal behaviour Capturing packets from a computer that will access different websites in order to define the normal network behavior.

Bad Behaviour: Capturing packets on the same computer where a DNS tunnel will be established between a client and a server (attacker).

**Test Scenario:** Montar o cliente, Dns Server, e o server(atacante). Utilizar a ferramente *Iodine* para estabelecer o túnel.

**Data processsing** : analise pacote a pacote, filtrar tráfego dns tanto udp como tcp porto 53

**Data filtering**: DNS uses both UDP server port 53 and TCP server port 53 for communication.

**Features:**

extra bytes are inserted in the packet header as part of DNS (tamanho pacote)

In traffic analysis, multiple request/response pairs are considered over time. The amount and frequency of requests can give an indication of existing tunneling.

Volume of DNS traffic per IP address

#### Volume of DNS traffic per domain

#### DNS server geographic location