

Exam 13.06.2017

2 Part Exam

Oral

- **Based on work with pcap file**

Written in Moodle

- **Necessary additions will follow**

Organisation

- **To participate you will need to show id**
- **Will assign Pcap semi randomly.**
- **Pick pcap from directory with assigned number.**
- **Analyze it and**
- **Answer the questions**
and Show results to me (Protect)

Pcaps

- **Short description what is going on in this Pcap (Be aware files can be malicious !)**
 - How many protocols are in the pcap
 - How many protocols are used by machine downloading the file
- **What file/files were exchanged by machine that does most downloading ?**
 - Where from files game?
 - Protocols used
 - Any authentication information?
- **What was server name -if any**
- **Any P2p activity ?**
- **Where file was located**
- **Sha256 value for file**

Additional information

Routing rules for A

- **ISP 2 Default route is ISP3**
- **ISP 1 have established BGP relationship with ISP2, ISP3**
- **ISP3 have BGP relationship with ISP 4, ISP 2, ISP1**
- **Directly connected non ISP routers talk OSPF**

Routing rules for B

- **ISP 1 Default route is ISP2 but transactions with ISP3 are done directly**
- **ISP3 have established BGP relationship with ISP2, ISP1 , ISP4**
- **ISP 3 have announced more specific route to subnet E**
- **Directly connected non ISP routers talk OSPF**