ITMO University

Network Security

Course Workload		Assessment form (examination/ graded test/ ungraded test)
ECTS	Hours	
6	216	Exam

The course targets on basics of the modern methods of supporting security for network services, tuning firewalls and network IDS/IPS systems, detecting attacks and data logging, secured channels of data interaction and tunneling. The course main aims are: • emphasizes on how to tune Linux server to make it more protected against attacks; • learning the principles of network attacks and protection of network services; • introduce some techniques of secured interaction between computers; • working with network protection tools with realistic cases; • analysis of network traffic and detection attacks on it; • configuring some network services; • working with vulnerabilities and risks; • reviewing scenarios of network attacks and how to prevent it.

Course structure:

1. Basic network services, tunneling and secured interaction

1.1. Basic network services: http, dns, dhcp, ssh, pop3/smtp/imap. Tunneling and secured interaction: ssh, vpn, socks5, ssl.

2. Network vulnerabilities, network protection and monitoring tools

2.1. Scanning network on vulnerabilities: vulnerability databases, metasploit, nmap. Network protection and monitoring tools: wireshark, tcpdump, suricata, iptables.

3. Analyzing incidents in network security

3.1. Analyzing incidents in network security: tshark, attack signatures, traffic analysis.