

- **Firewall & IDPS concepts**
  - History around firewalls
  - Types of Firewalls
  - How firewalls work
  - History around IDPS
  - Types of IDPS
  - How IDPS work
  - Examples of production implementations.
  
- **Cisco Access Control Lists**
  - Installing and using Cisco Packet-tracert simulation tool
  - Implementing a Simple Access Control List
  - Implementing an Extended Access Control List
  - Implementation examples
  
- **Linux IPTABLE**
  - Installing iptables
  - Tables & chains
  - Basic rules creation
  - NAT and redirections
  - Persisting rules
  - Iptables blacklisting
  - Iptables geolocation blocking
  
- **Pfsense**
  - VM Installation
  - System configuration
  - Backup, restore & upgrade
  - Basic rules, aliases
  - Interface grouping
  - Advanced firewall options
  - Port forwards and NAT
  - DHCP, DNS, SNMP and NTP
  - OpenVPN for Remote Access and Site-to-Site
  - Multi WAN, failover, load balancing and policy routing
  - Additional packets, ntopng.

- **Snort**
  - Installation
  - System configuration
  - Operations
  - Rules configuration
  - Keeping rules-up to date
  - Rules syntax and usage
  - Snort as an IPS
  - Rule Optimization
  
- **Suricata**
  - Installation
  - Configuration
  - Rules creation
  - Blacklisting with Suricata
  - Geo-IP blocking with Suricata
  - Log analysis from Suricata
  
- **BRO**
  - Installation
  - Initial configuration
  - Building a Cluster
  - Logs analysis DNS-traffic
  - Logs analysis HTTP-traffic
  
- **P0F**
  - Installing the tool
  - Using it
  - Log analysis
  
- **SecurityOnion**
  - VM Installation
  - System Configuration
  - Using Network-Miner
  - Using SGUIL
  - Exploring data with Kibana

- **Infrastructure security, best practices & strategies**
  - Examples of Firewalls implementations
  - Examples of IDPS implementations
  - Firewall rules clean-up
  - Security best practices
  - Top vendors

