# Argomenti NSD:

## Tulumello:

1. Internet architecture and vulnerabilities
    - Punti principali cybersecurity
    - Generalità sulle LANs
    - Routing e IP forwarding
    - DNS
    - Vulnerabilità TCP/IP
2. Ethernet LAN security
    - Ethernet:
        - Trama ethernet
        - Hub,switch e bridge
        - STP
        - Adaptation protocols
    - Vulnerabilità delle LANs ethernet:
        - network and system access
        - traffic confidentiality
        - traffic integrity
    - Contromisure alle vulnerabilità di ethernet
        - router based security
        - access control
        - protocolli di sicurezza (SARP/SEND e MACsec)
        - security monitoring
3. VLANs
    - Vantaggi
    - Membership
    - Tipi di porte/link
    - Sicurezza:
        - MAC flooding
        - VLAN hopping basato sul DTP
        - Double encapsulation VLAN hopping
        - ARP attack
        - STP attack
        - VTP attack
        - CDP attack
        - PVLAN attack
4. 802.1x
    - Generalità
    - Protocolli utilizzati in 802.1x
    - Altre operazioni
    - Autorizzazione
    - Vulnerabilità
    - Soluzione: MACsec key agreement
5. Firewalls
    - A cosa servono
    - Tipologie di firewall (pro e contro)
    - (Netfilter)

6. Filtraggio dei pacchetti
    - LPM
    - CAM
    - Algoritmo bit vector linear search
7. Protocolli di sicurezza
    - Requisiti di sicurezza
    - SSH
    - TLS
    - IPsec
8. Overlay VPN
    - VPN
    - Come implementare VPN
    - Cos'è overlay VPN
    - Problemi (2)
    - OpenVPN:
        - Generalità
        - TUN/TAP
        - PKI
        - Protocollo
9. BGP
    - Protocolli di routing
    - Tipi di messaggi BGP
    - Evitare cicli
    - upstream e downstream peers
    - Annunci manuali
    - Interfaccia loopback
10. MPLS
    - A cosa serve
    - Header
    - Componenti rete MPLS
    - Operazioni
    - Motivazione BGP/MPLS
    - VPN con MPLS
11. BGP security
    - Vulnerabilità TCP/IP+contromisure
    - Vulnerabilità del control plane+contromisure
12. VXLAN
    - Modello gerarchico network datacenter
    - Obiettivi
    - Two tiers topology
    - Three tiers topology
    - Limiti di L2 forwarding
    - VXLAN
        - L2 VNI
        - L3 VNI
        - Load balancing
    - EVPN
        - Generalità

        - Tipi di messaggi
13. Sicurezza in DNS
    - Recap DNS
    - Vulnerabilità DNS
        - DNS spoofing
        - Kaminsky attack
        - DNS tunneling
        - DNS hijacking
        - DoS
        - Botnets-based CPE
        - DNS query confidentiality
    - DNSsec
        - Caratteristiche
        - Meccanismi usati
        - PKI
        - Explicit denial of existence+problema
        - DNSsec white lies
    - DNS over TLS
    - DNS over HTTP

14. DDoS e IDS
    - Classificazione tipi di DoS
    - SYN spoofing
    - Attacchi HTTP
    - Reflection
    - Amplification
    - Attacchi a DNS
    - DDoS+prevenzione
    - Botnets
    - Fast flux (single e double)
    - IDS: tipologie, approcci per la detection, honeypots e Snort