Xarxa Classe:
10.200.243.0/24

DNS SOA

Bind9 zone "cryptosec.net"

Apache2 Web Server

OpenSSL CA "cryptosec" --> cacert.pem --> cryptosec_cert.pem

Static conf netplan
DNS primary = 10.200.243.164
DNS secondary: 10.200.240.10

10.200.243.164
enp0s3

DNS EDT:
10.200.240.10

DNSSEC

switch

gateway
10.200.243.1

router

Internet

Intercepts connection & attacks

10.200.243.X

eth0

Kali

Dynamic conf / Hacking tools (MITM)
- Ettercap
- SET (Social Engineering Tool)
- Bettercap
- Nmap
- John (Password Cracker)
- SSLStrip
- Wireshark
- ...

DNSSEC

Static conf netplan
DNS forwarder = 10.200.243.164
DNS secondary: 10.200.240.10

10.200.243.168
enp0s3

192.168.3.1
enp0s8

switch

DNS Forwarder (Router)

Bind9 forwarder to "cryptosec.net"

Internal Network ("Cryptosec" 192.168.3.0/24 via enp0s8)

DHCP 192.168.3.100 - 192.168.3.200 ; DNS 192.168.3.1

Iptables - NAT 192.168.3.0/24 (Masquerade)

Wazuh: Host Intrusion Detection

.100
Client Linux Lite

.101
Client Debian

.102
Client Windows

Dynamic conf - DHCP by Router

Gateway: 192.168.3.1
DNS: 192.168.3.1

Automatic DNS

Request & Offer "dhclient"

Xarxa cryptosec:
192.168.3.0/24