Key words added.

Do NOT try to go through everything within 10 minutes

1. Network Security Threats

Confidentiality, Integrity, Availability
Sniffing
IP adresser, Whois
Example programs: ping, traceroute, Nmap - port scanning, service detection, OS detection
“Security Problems in the TCP/IP Protocol Suite” April, 1989
Problems described in the original:
sequence number spoofing, routing attacks, source address spoofing,
authentication attacks, DNS problems, SNMP, eavesdropping and host-spoofing ARP spoofing

- similar attacks exist today
  DDoS
  Example programs: Nmap, hping3

2. Traffic inspection and firewalls

Filtering
IP header fields: source IP, source port, destination IP, destination port, protocols TCP, UDP, ICMP
VPN protocols
stateless Filtering, stateful inspection, session data, netflow
IEEE 802.1q VLANs
Example platforms Debian med UFW, Opensense, OpenBSD PF, Checkpoint, Cisco ASA , Meraki,
Firepower, Fortinet, Juniper SRX, Palo Alto,Big-IP F5
IEEE 802.1x
Example Elastiflow

3. Encrypting the network

symmetric key, public key,
AES, DES, 3DES
TLS, VPN, IPsec

4. Virtual Private Networks

IPsec
Wireguard
TLS VPN
Example programs: sslscan til TLS og ikescan til IPsec/IKE

5. Wifi Security

IEEE 802.11
"Robust Security Network" (RSN), 802.11i

Sniffing, man in the middle
WEP, WPA, WPA2, WPA3, WPS
WPA PSK vs WPA Enterprise
IEEE 802.1x
Authentication Protocols RADIUS, PAP, CHAP, EAP
Examples: aircrack-ng.org airodump

6. Network Management

DNS, DHCP, NTP, ICMP
SNMP versions and security
Secure Shell (SSH)
Examples LibreNMS, Smokeping, BIND, Unbound, RANCID, Oxidized
Advanced: Jump hosts, VLAN, port security, IEEE 802.1x, Ansible
Husk input fra NSRC

7. Network Intrusion Detection

Intrusion Detection Systems (IDS)
Intrusion Prevention System (IPS)
Zeek, Suricata, IDS rules
Dashboards
Sources: passive DNS, malware domains, IP reputation, Netflow
Indicator of Compromise (IoC)
Network Security Monitoring
ENISA Forensics examples

8. Network Forensics

Centralized syslog
Netflow
Session data, full packet capture, packet string data
Indicator of Compromise (IoC)

9. DNS and Email Security

DNS: records NS, A, AAAA, MX
DNSSEC, IMAPS
SMTP Start TLS (STARTTLS)
SPF, DKIM, DMARC
DANE
DNS over Transport Layer Security (TLS) (DoT), RFC 7858
DNS Queries over HTTPS (DoH) RFC 8484
Phishing, sphear phishing, malware
Example programs: sslscan