In [ ]:

```
Training Day 2 Report– 24 June 2025
 Introduction
 OnDay2wefocused on networking fundamentals which underpin nearly all cybersec
 work. Understanding how systems communicate, how packets traverse networks, a
 how addressing works is essential for effective reconnaissance and later expl
 trainer framed networking knowledge as both an investigative tool and as a se
 signals.
 Key Concepts Discussed
 Weexamined the OSI and TCP/IP models, explaining layered responsibilities fro
ical connectivity through application protocols. IP addressing and subnetting 
ered, with emphasis on how address allocation affects discovery and segmentati
 distinctions between TCP and UDP, common port numbers, and basic packet flow 
cepts were clarified.
 Lab Preparation in Theory
 The theoretical lab plan included configuring virtual network interfaces, cre
 subnets for test VMs, and simulating simple client-server setups. We discusse
 to safely capture traffic on an isolated network and how to interpret packet 
 identify protocols and services.
 Practical Understanding (Theory)
 We reviewed common network troubleshooting commands and their purposes concep
ally: how ICMP helps test reachability, what traceroute reveals about path hop
 how ARP relates to local link mapping. The class discussed how these concepts
 reconnaissance and how defenders can monitor for abnormal traffic patterns.
 Key Takeaways
 Networking models help structure thought when analyzing systems. Basic addres
 ports, and protocol knowledge allow ethical hackers to map target environment
rately while defenders can use the same knowledge to detect unusual behaviors.
 Conclusion
 Network fundamentals were reinforced as a building block for scanning and rec
sance. The next class will focus on reconnaissance techniques and OSINT.
```