



In []: Training Day 28 Report- 20 July 2025

Introduction

Day 28 examined VPNs, secure remote access, and the balance between usability security for remote workers and services.

Key Concepts Discussed

We contrasted IPsec and TLS-based VPNs and explored split tunneling risks. The emphasis was on the importance of strong authentication and certificate management for remote access solutions.

Lab Preparation in Theory

The class discussed how to design and test remote access configurations in environments and how to validate access controls and logging.

Practical Understanding (Theory)

We reviewed multi-factor authentication for VPNs, endpoint posture checks before access, and monitoring remote sessions for anomalous behavior.

Key Takeaways

Secure remote access requires layered controls including strong auth, endpoint security, and session monitoring.

Conclusion

Following remote access, we will discuss cloud security fundamentals