```
In [ ]: Training Day 3 Report– 25 June 2025
         Introduction
         Day 3covered reconnaissance – the practice of gathering as much information a
         about a target before any direct interaction. Reconnaissance is often split i
         methods that do not touch the target and active methods that do, and both wer
         in terms of ethics and scope.
         Key Concepts Discussed
         We discussed Open-Source Intelligence (OSINT), including public web searches,
         registration records, DNS records, and social media signals. Theoretical adva
         limitations of passive enumeration were weighed against the potential for det
         performing active discovery.
         Lab Preparation in Theory
         A theoretical plan was given for using DNS queries and WHOIS lookups, identif
         subdomains through historical services, and collecting publicly available doc
         reveal system details. The class examined how to structure findings with time
         source references.
         Practical Understanding (Theory)
         Weexplored the ethics of data collection, including respecting robots.txt and
        ing private information. Discussion included how to prioritize targets based o
         impact and likely presence of vulnerabilities, preparing a reconnaissance che
         lab work.
         Key Takeaways
         Reconnaissance sets the stage for efficient testing; thorough documentation a
         awareness distinguish professional testing from malicious probing.
         Conclusion
         Tomorrow we will move from reconnaissance to scanning and enumeration, applyi
         network fundamentals to identify hosts and services.
```