In [ ]:

```
Training Day 4 Report– 26 June 2025
 Introduction
 Day 4 introduced scanning and enumeration: how to take reconnaissance data an
cover active services, open ports, and software versions while remaining mindf
pacts and authorization.
 Key Concepts Discussed
 We covered the reasons for different scan types, the meaning of open/closed/f
 ports, and the value of service fingerprinting. The trainer discussed the cor
 scanning to avoid service disruption and the legal implications of scanning t
 systems without consent.
 Lab Preparation in Theory
 The class was guided through the conceptual setup for performing controlled s
 isolated environment, including scanning rate throttle plans and logging appr
 discussed how to record scan results and cross-reference service banners with
 databases to prioritize next steps.
 Practical Understanding (Theory)
 Students learned to design a scanning plan: scope, timing, scan types, report
plates, and escalation pathways if critical issues are discovered. We also dis
 defenders detect scanning behavior and how that intelligence is used for resp
 Key Takeaways
 Scanning uncovers actionable intelligence but must be performed with caution.
 service identification accelerates vulnerability research and reduces noise.
 Conclusion
 The foundation for practical scanning is laid; the next session will cover vu
 assessment and interpretation of scan results.
```

In [ ]:

In [ ]:

In [ ]:

In [ ]:

In [ ]: