In [ ]:
```
Training Day 24 Report– 16 July 2025
 Introduction
 Day 24 focused on rootkits and stealth techniques that allow attackers to hid
 at userland or kernel levels.
 Key Concepts Discussed
 We discussed the distinction between user-mode and kernel-mode rootkits, tech
 tampering with system calls, and why traditional detection can be bypassed.
 Lab Preparation in Theory
 The class covered integrity verification approaches, trusted boot models, and
 steps to maintain system integrity indicators in production.
 Practical Understanding (Theory)
 Weexplored defense strategies including secure boot, measured boot, and regul
 scanning, as well as incident plans if a rootkit is suspected.
 Key Takeaways
 Rootkits pose significant detection challenges; proactive integrity controls
 processes reduce the risk.
 Conclusion
 Next we turn to security governance and policy topics.
```