In [ ]:

```
Training Day 20 Report– 12 July 2025
 Introduction
 Day 20 examined endpoint threats such as keyloggers, malware, and the role of
 detection and response (EDR) systems in modern security architectures.
 Key Concepts Discussed
 We discussed types of endpoint threats, behavioral indicators of compromise,
 trade-offs between usability and security for endpoint controls.
 Lab Preparation in Theory
 The class covered how to instrument endpoints with monitoring agents, how to
 suspicious hosts, and the importance of controlled analysis environments for
 potential malware.
 Practical Understanding (Theory)
 Defensive postures such as allowlisting, application control, and least-privi
 were explored as preventive measures. The trainer stressed incident response
 for endpoints.
 Key Takeaways
 Endpoint hardening and monitoring are critical to early detection and contain
 Conclusion
 Following endpoints, the course will cover malware analysis and safe handling
```