Lab topics

Deadlines match the reported order

- Network attacks
  1. ARP Poisoning + TCP session hijacking
  2. Denial of Service (ICMP flood, SYN, UDP, .., RST)
  3. MitM attacks
  4. DNS cache poisoning
  5. Kaminsky attack
- Software attacks
  6. XSS+CSRF+phishing
  7. Buffer Overflows
  8. SQLi + defenses
- Defenses
  9. FW (stateless) → allows/blocks/redirects/forwards packets depending on pre-defined rules
  10. FW (stateful) → FW whose rules consider connection states
  11. NIDS – Snort → network sensor that detects possible attacks by matching pre-defined signatures with network traffic
  12. NIDS – Bro → like above but more expressive languag (can define more complex signatures)