# Week 2: Security Planning and Performance Testing

## 1. Installing Monitoring Tools

**Explanation:**
Installed essential tools (`htop`, `sysstat`, `ifstat`, `nload`) to monitor CPU, memory, disk, and network performance on the server. These tools will be used in later weeks to test system performance under different workloads.

```
  Lynis security scan details:

  Hardening index : 63 [############        ]
  Tests performed : 260
  Plugins enabled : 1

  Components:
  - Firewall               [V]
  - Malware scanner        [X]

  Scan mode:
  Normal [V]    Forensics [ ]    Integration [ ]    Pentest [ ]

  Lynis modules:
  - Compliance status      [?]
  - Security audit         [V]
  - Vulnerability scan     [V]

  Files:
  - Test and debug information      : /var/log/lynis.log
  - Report data                     : /var/log/lynis-report.dat

================================================================================

  Lynis 3.0.9

  Auditing, system hardening, and compliance for UNIX-based systems
  (Linux, macOS, BSD, and others)

  2007-2021, CISOfy - https://cisofy.com/lynis/
  Enterprise support available (compliance, plugins, interface and tools)

================================================================================

  [TIP]: Enhance Lynis audits by adding your settings to custom.prf (see /etc/lynis/default.prf for all settings)

  root@ubuntu:/#
```