TTKS0700 Data Security Testing

Lab 04. Configurations

Jarmo Nevala, 10.09.2019

Lab 04. Configurations

System configurations

- GOAL
  - To understand basics of the CONFIGURATIONS audits / checklists

- In this document
  - RED color = TASK
  - BLUE color = TIP
  - Green color = Example

Lab 04. Configurations

Audit system configurations

- System hardening guidelines
- Benchmarks
- Best practices

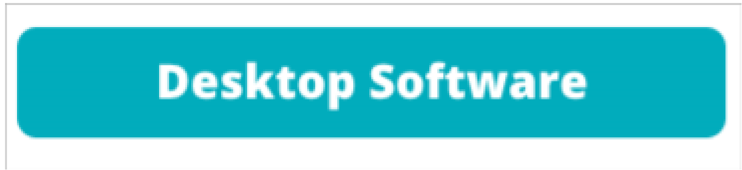
Lab 04. Configurations

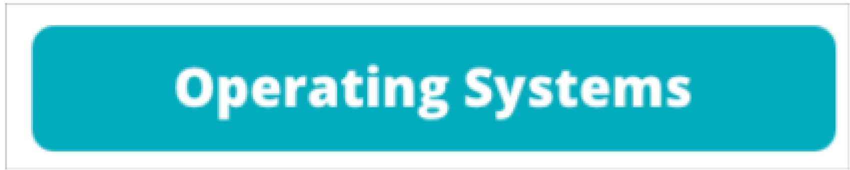
CIS BENCHMARK

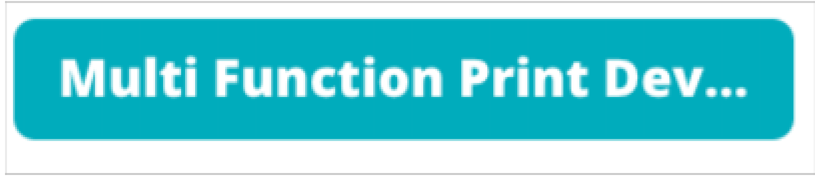
- “CIS Controls and CIS Benchmarks are global industry best practices endorsed by leading IT security vendors and governing bodies.”
- Proven guidelines will enable you to safeguard operating systems, software and networks that are most vulnerable to cyber attacks.
- They are continuously verified by a volunteer IT community to combat evolving cybersecurity challenges.
- 100+ configuration guidelines for various technology groups to safeguard systems against today’s evolving cyber threats.
- Source: https://www.cisecurity.org/cybersecurity-best-practices/

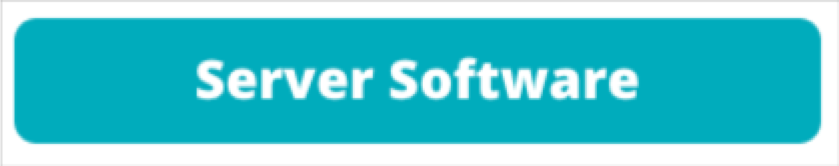
Lab 04. Configurations

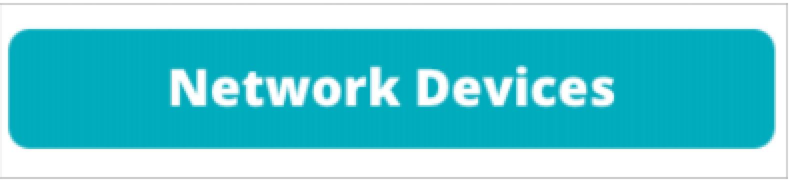
CIS BENCHMARK

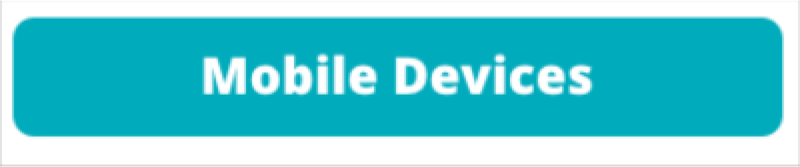


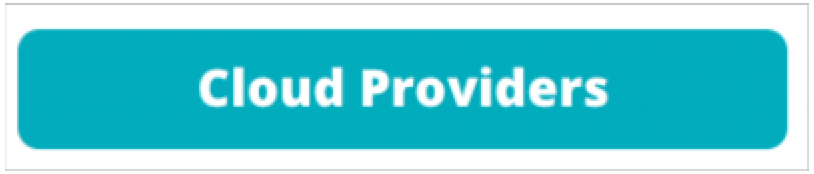












Lab 04. Configurations

CIS BENCHMARK

- There is also commercial tool to check compliance (CIS-CAT-PRO)
- Free CIS-CAT-LITE version supports very limited amount of operating systems

- https://www.cisecurity.org/cybersecurity-tools/cis-cat-pro/
- https://learn.cisecurity.org/cis-cat-landing-page
  - Use school email or www.10minutemail.com (or similar)

Lab 04. Configurations

Vendor Best Practises

- Some examples of vendor based best practices and hardening guidelines

- https://wiki.centos.org/HowTos/OS_Protection
- https://www.microsoft.com/en-us/download/details.aspx?id=53353

Lab 04. Configurations

Task 1.

- Find suitable CIS Benchmarks for Windows and Linux versions in target environment (registration is needed for downloads).
- Select one area (second level header 1.1, 1.2, 2.1 etc.) from each guide and check the configurations
  - Notice that there are LEVEL-1 and LEVEL-2 –settings. Find out what these LEVELS mean.

Lab 04. Configurations

Task 2.

- Audit pfsense –firewall RULES using following checklist https://www.sans.org/media/score/checklists/FirewallChecklist.pdf (Select applicable parts from the checklist) jamk.fi

Jyväskylän ammattikorkeakoulu
JAMK University of Applied Sciences