Securing Linux Servers

Miloš Kukoleča
AMRES

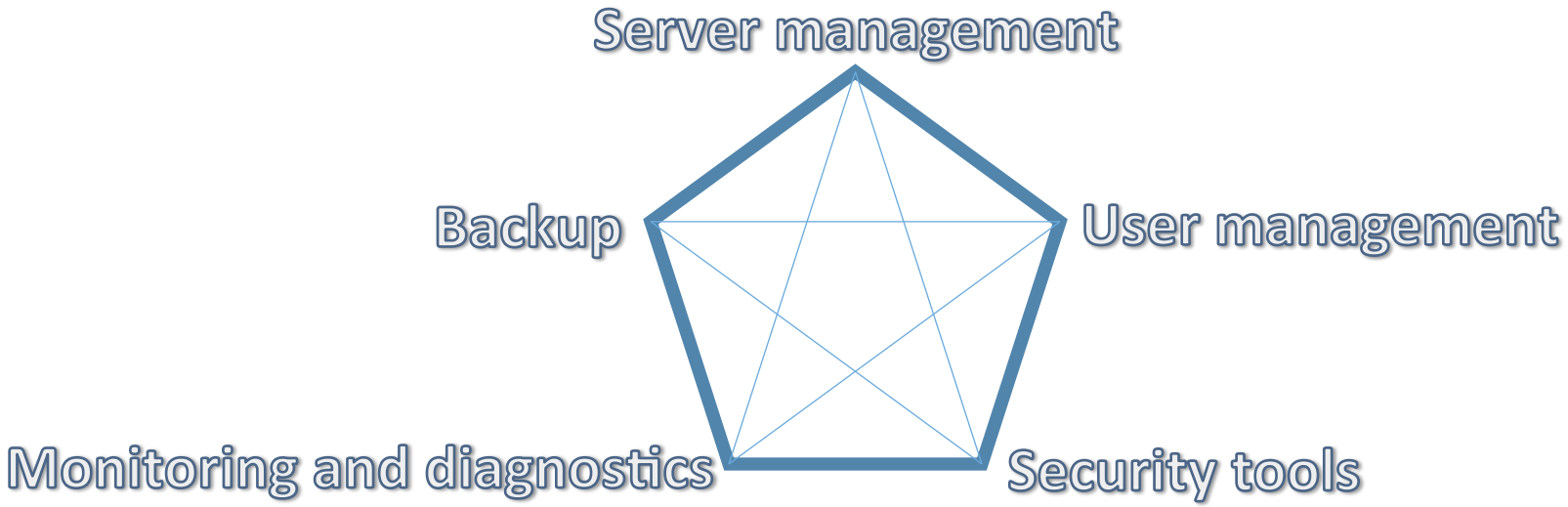
GN3plus Symposium
24 – 25 February 2015
Athens

Motivation

- Majority of production servers in academic environment are run by Linux
- Lack of server security related documents in the academic community
- Security awarenes is not on a high level
- Security challanges are on the rise
- Technical background of academic IT staff is very diverse
  - Advanced sysadmins
  - Beginners

Document planning

- Experience of sysadmins in academic institutions is invaluable
- Knowledge, common problems, solutions and best practices of academic Sysadmins formed this BPD
- Meeting with academic technical community produced a draft for the document



Server (Linux OS) Management

- Suitable installation: standard, specific or minimal ?
- Disabling and removing unnecessary services
- Provide secure communication with the Linux server
  - Remote access
  - File transfer
  - Web access (if needed)
- OS system and services update
- Distribution of production services on available Linux servers
  - „The system is as secure as the most vulnerable service in it!“

User Management

- Usualy the weakest link in the security chain – user ☺
- Create and maintain strict and clear user management policy
  - DO NOT use root account.
  - Enforce policy „ONE USER = ONE ACCOUNT“
  - Enforce secure user password structure
  - Lock or remove unused accounts
  - Use sudo access (if suitable)
- Centralised management of user accounts is a good practice for managing several Linux servers

Security Tools, Monitoring and Diagnostics

- Security for all layers of TCP/IP protocol stack:
  - L2 – arpwatch, antidote
  - L3, L4 – IPtables
  - L5 – SELinux, AppArmor
- Key of successfull Linux management – gathering useful information
- Useful info:
  - Services status
  - Network activity
  - Use of system resources
  - User activity (who, when, where, what...)
- Syslog, Syslog-ng and SNMP are fine tools for monitoring and diagnostics

Backup

- Backup is essential in security related incidents and disaster recovery mechanisms
- Virtual environment makes the backup procedures quite easier
- Non-virtual environment brings the main challenge – what to backup?
- Key is to develop a backup strategy
  - Define the data that should be copied
  - Define the backup technique
  - Define the backup frequency
  - Define the backup cycle
  - Define the time for keeping the backup
  - Define the space needed for storing backups

Conclusions

- BPDs should be written in close collaboration with Sysadmins in academic institutions
- The main aim of „Securing Linux Servers“ BPD is to give general overview of Linux security, not to be used as a Cookbook.
- „Securing Linux Servers“ is a good starting point for a number of spin-off documents which would explain in detail the protection of major network services
- Not to be forgotten – Server protection is not a one-time effort, but a lasting process that continues as long as the server is in use

Thank you and

any questions?