System Administration for InfoSec Pros

Antranig Vartanian — 26/02/2025 — OWASP Yerevan

whoami

- Antranig Vartanian
- I blog @ antranigv.am && անդրանիկ.հայ
- Started as a SysAdmin
- Became InfoSec Professional by accident
- I disagree with most SysAdmins/NetAdmin
- I also disagree with most InfoSec Professionals
- My goal is simple: *Stop doing stupid things*
- My motto is simple: *Boring is always better*

Why this talk

- I started talking with “people”
- Turns out “working as sysadmin” and “working in InfoSec” are similar
  - We keep doing stupid things
  - We keep expecting good results
  - We keep trying to fix problems that have been solved for ~20 years
  - “Certified SysAdmin” and “Certified InfoSec (org)” is very common
  - Yet, certified sysadmins know nothing, certified infosec orgs get hacked
- I really wanted to show how simple both InfoSec and SysAdm is

Basics of System Administration

- Your mission
    - Keep shit running (uptime)
    - Keep shit fast (performance)
    - Keep shit secure (security)
- Your scope
    - ***EVERYTHING***
- Your Challenge
    - Shit changes fast

Basics of System Administration

- You care about one thing and one thing only: ***the user***
- You work for the user, you live for the user, you dream about the user
- The user has no stereotype
  - The user can be smart, dumb, nice, mean, fast, slow, rich, poor, educated, young, old, persistent, flexible or a former sysadmin
- All users like good sysadmins
- All bad sysadmin hate users
- Happy users == Functioning Organization

Basics of System Administration

- If you’re not learning, then you’re not working
- You can’t know everything
- You can’t do everything alone
- You need helpers
    - Your junior sysadmin
    - Your community
    - Your scripts
- You *will* have problems
- You need to *understand* the problems if you want to solve them

Basic Concepts

- Responsibilities: Users, Groups, Configuration, Maintenance
- Systems: Operating Systems, Network Systems
  - Operating Systems: Windows, Unix(-like)
  - Network Systems: Routers, Switches
- Hardware vs Software
- Access Control
- Service Management
- Automation

The hard truth(s) about System Administration

- If you do everything right: no one will notice you
- If you do everything wrong: everyone will blame you
- If you do a stupid mistake: you will get breached

The good facts about System Administration

- If you try hard enough, everything is system administration
- Automating 99% of your tasks will boost your users/organization
- DevOps? SRE? Cloud? It’s basically fancy term for SysAdmin
- InfoSec? It’s basically a limited scope of SysAdmin

Keep things stupid simple

- Isolate everything
- ACL for everyone
- Backup always
- Restore almost always

Boring is always better

- You don’t need “latest and greatest”
- You need “old ~~as fuck~~ and mature”
- You don’t need “products”
- You need “protocols”
- You need manual pages
- You need documentation

Battle-Tested Technologies

- Operating System: FreeBSD
- File System: ZFS
- System Isolation: Jails
- Network Isolation: VLANs
- ACLs: Firewalls
- Documentation: Wiki

Demo: FreeBSD

Demo: ZFS

Demo: Jails

Demo: pf

illuria

Demo: Wikis

Demo: Community

illuria

Discussion: Enterprise™

illluria

No Surprises

Know Your Shit

Be nice

Never blame

Thank you!

https://illuria.com/

https://illuria.am/

https://antranigv.am/

https://անդրանիկ.հայ/