Managing Elevated Privileges in the Enterprise Environment

Erik Burgess
@erikburgess_

whois

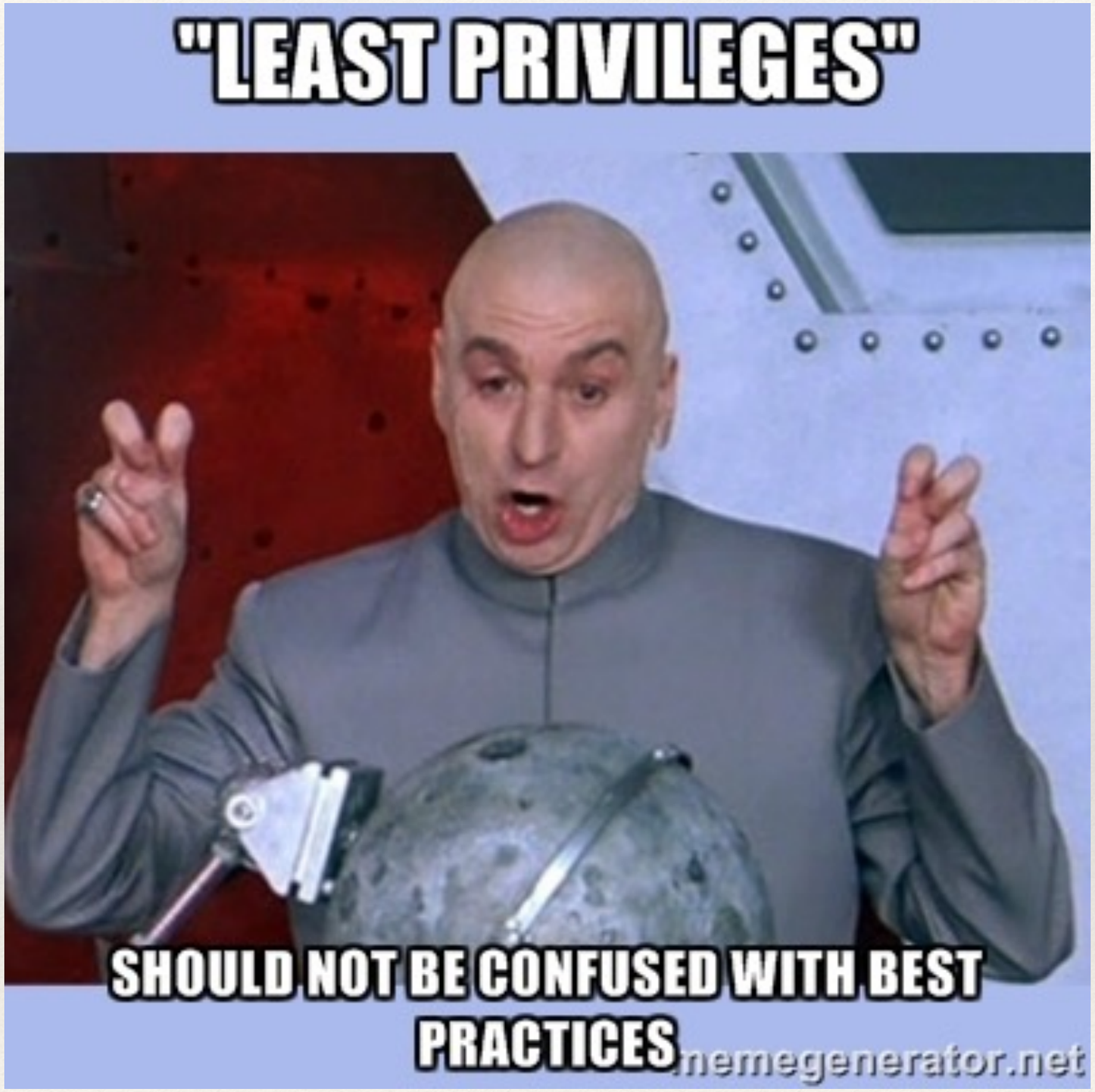
- Industry Veteran
- Many Roles During Career (Help Desk, Servers, Management, Security)
- Experience In Military, Government, Private Sectors
- Lazy Admin a.k.a. Doing More With Less
- Tinkerer, photographer, security enthusiast
- Contact: @erikburgess_

Why THIS talk?

- Too many users operating as admin
- Commercial solutions overly expensive
- Corporate culture needs to change
- Compliancy requirements

Least Privileges

- EP vs. LP vs. Admin Rights
- The principle of least privilege translates to giving people the lowest level of user rights that they can have and still do their jobs. (NIST)
- Elevated Privileges is Privilege Escalation, but….
  - Elevated Privileges often equals Admin Rights
- What about Power User?


"LEAST PRIVILEGES"
SHOULD NOT BE CONFUSED WITH BEST PRACTICES
memegenerator.net

User Damage

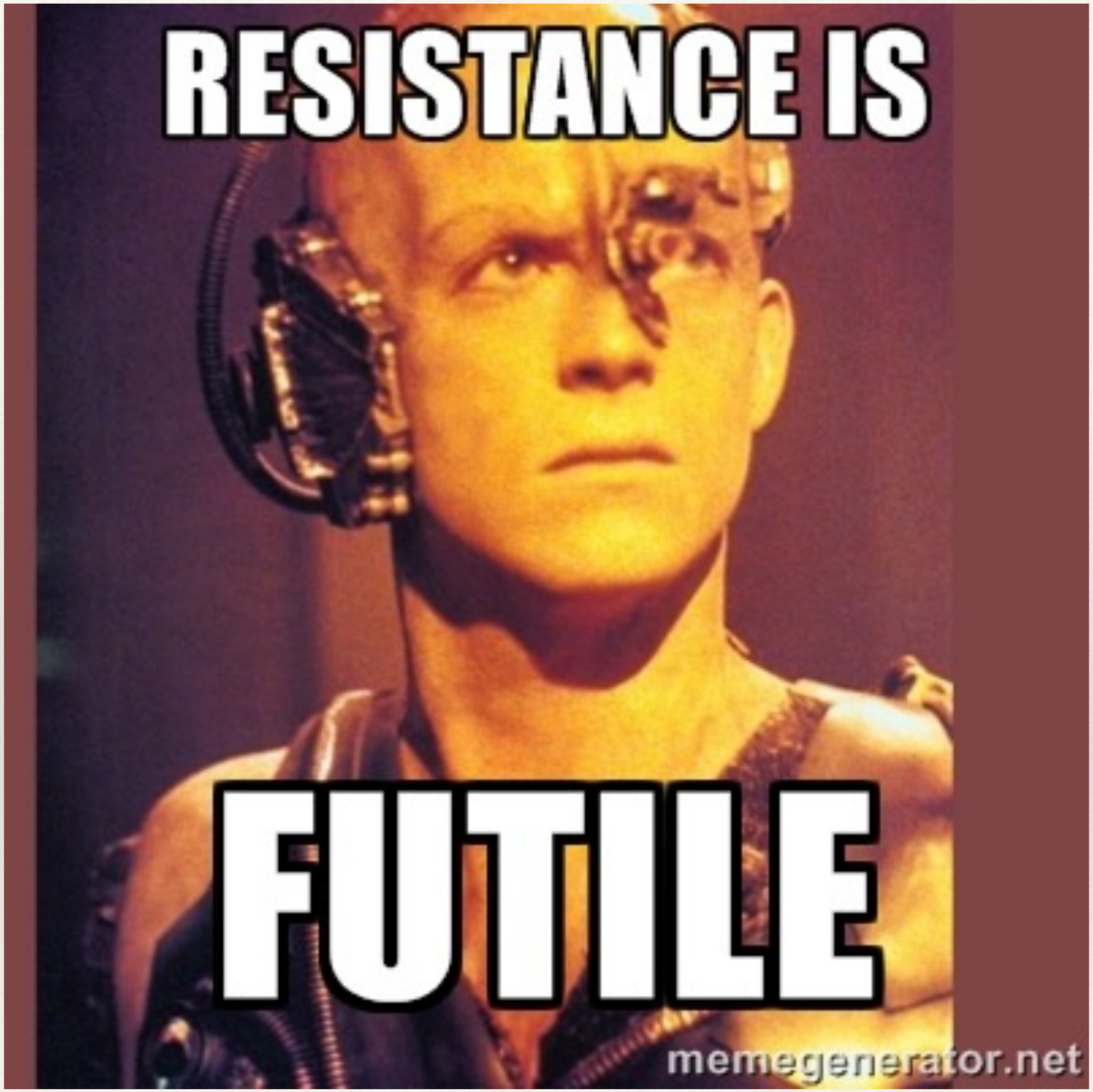
- Virus/Malware
- Broken Systems
- File Deletion
- Unwanted Applications
- More Work for SA's / Higher Cost

Getting Started

- Management Approval / Sell to Users
- Identify Trouble Users/Applications
  - Surveys, Testing, Tickets
- Implement EP Workflow
  - Approve / Track / Verify
  - User Rules and Responsibilities
- Pilot Test
- Remove Existing EP from Unapproved Users
- User Training

User Challenges

- Believe It's Their Personal Machine
- They Are Too Important and/or Busy
- Will Run And Hide At The Sight Of An SA
- Learn What Works And They All Use It
- Do Not Abide By Rules And Regulations
- Vindictive Users
- Never-ending Battle


RESISTANCE IS
FUTILE
memegenerator.net

Solutions

- Third-Party Commercial Solutions
- EP On Demand
- Open-Source Tools
- Secondary Local or Domain Admin Account
- Windows UAC (User Account Control)
- Roll Your Own

Limiting Access

- Sudo / WinSudo
- Install Applications in User Space
- Directory / Registry Permissions
- Ability to Manipulate Services
- Authorization Database (OSX)

Editing Service Permissions

- sc query
- sc sdshow
- whoami /user
- sc sdset

C:\> sc sdshow FTPSVC

C:\> sc sdset FTPSVC D:(A;;CCLCSWRPWPDTLOCRRC;;;SY)
(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)
(A;;CCLCSWLOCRRC;;;IU)(A;;CCLCSWLOCRRC;;;SU)
(A;;RPWPDTLO;;;S-1-5-21-3566490150-1616182022-3231533333-1003)S:
(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD)

DEMO

- Service Permissions

Typical Scenario

- User says application X isn't working.
- Work is critical/time sensitive. Management involved.
- EP granted system-wide for a single application.
- User never has time for admin to troubleshoot.

Workflow / Tracking

Systems EP is needed on

* System Name

System ECN

* When is EP no longer needed? (Date Picker BROKEN)

07/04/2015

* System Operating System

Select

* Justification for EP

* Select the corresponding System Security Plan the user is requesting Elevated Privileges on. Most systems will fall under the AETD Laboratory Systems

Select

+ Add

*

I have read and agree to the User Acknowledgement Statement

Windows Custom

- WinSudo
- Patching Agent
- Scripting
- Logging

Windows Scripts

- Leveraged Patching Agent
  - AutoEP Scripts Run Every ~2 Hours
- Consists of a PowerShell script and three text files
  - Global Admins, Ignored Accounts, EP Users
- Can Use Either AD Groups or Users

Windows Script File Format

- Two .txt Files and a .csv

#Erik's VMs
domain\eburgess,Windows7VM
domain\eburgess,Windows8VM

#computername, username, expiration date
windows7vm,domain\eburgess,02/09/2013*
windows8vm,domain\eburgess

* Expiration Date Ignored

DEMO

- Windows AutoEP Scripting Demo

WinSudo

- Custom Build
- Good for Granting EP to a Single Application
- Can Validate File Checksums
- Automatically Updates System Config ~24 Hours
- User Can Manually Update

DEMO

- WinSudo Demo

Linux / OSX Custom

- Sudo
- Patching Agent
- Scripting
- Authorization Database (Mac Only)
- Logging

Authorization Database

- Sqlite database that controls access rights to various commands.
- Energy, Network, Printers, App Store Updates, Time Zone, Time Machine, Xcode
- Can unlock many other things

AuthDB Example

```
# Unlock Energy Saver preference pane.

security authorizationdb read system.preferences.energysaver > /tmp/system.preferences.energysaver.plist

/usr/libexec/PlistBuddy -c "set group staff"  /tmp/system.preferences.energysaver.plist
        security authorizationdb write system.preferences.energysaver < /tmp/
system.preferences.energysaver.plist
```

DEMO

- AuthDB Demo

Monitoring

- Log, log, log
- Visualize where possible
- Can track changes to admin groups

DEMO

- Splunk Dashboard Demo

Easing The Burden

- Automated Patching
- Centralized Software Installations
  - SIP Portal / AD & GPOs / SCCM / WSUS (Windows)
  - Munki / Spacewalk (OSX / Linux)
  - Updates & Approved Applications

Positive Effects

- Potentially Fewer Security Incidents
- Better Security
  - Helps Stop Malware, Limits Data Access When Compromised, Protects Data From Users
- Can Help With Data Classification
- Culture Can Spread

Negative Effects

- Culture Change
- Cranky Users
- Potentially More Help Desk Tickets
- Security Team Getting a Bad Rap

EP Justifications

* **Justification for EP**

I currently have 2 computers (1 desktop, 1 laptop). I am replacing both systems with a new laptop. IT has taken the laptop but left me with the desktop until it is determined that nothing else is needed from that system. I will need EP on my new system ASAP so I can relinquish the old desktop.

EP Justifications

*** Justification for EP**

My wavefront sensing and control work involves extensive numerical and scientific computing work. The tools and software package required for this work generally require elevated privileges for installation, maintenance, and configuration. Because of the large number of tools, their specialized nature, and frequent need for updates and configuration requiring all EP operations to be done by the regular system administrator would be an unreasonable burden on their time. Software tools include parallel computing libraries (mpi4py), compilers (mingw and MSVC), various python distributions (including Anaconda and the official Python distribution), integrated development environments (PyCharm), as well as profilers and debuggers.

Q & A