Gaining Access: Escalating Privileges

Dale Meredith
MCT | CEI | CEH | MCSA | MCSE
Cyber Security Expert

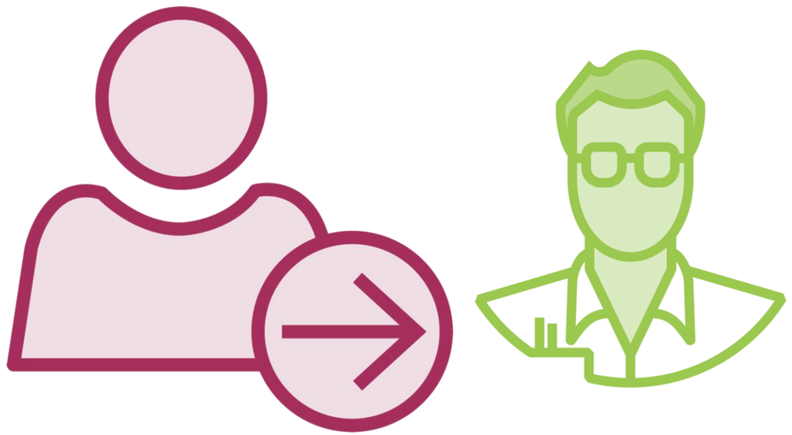
dalemeredith.com | Twitter: @dalemeredith | Linkedin: dalemeredith|

It's true, I had hacked into a lot of companies, and took copies of the source code to analyze it for security bugs. If I could locate security bugs, I could become better at hacking into their systems. It was all towards becoming a better hacker.

Kevin Mitnick

Now What?

So We've Made It In...Now What?



Remember how we came in?

Never make assumptions

Next step? Look around

- Configuration mistakes
- Design errors
- Layouts
- Programming flaws

Four Methods for Escalation

Pwn the admin/root account

Take advantage of vulnerabilities

- Remember our overall goal is “data”

Fire up a “tool”

Have a user do it for you!

Types of Escalation

Vertical Escalation

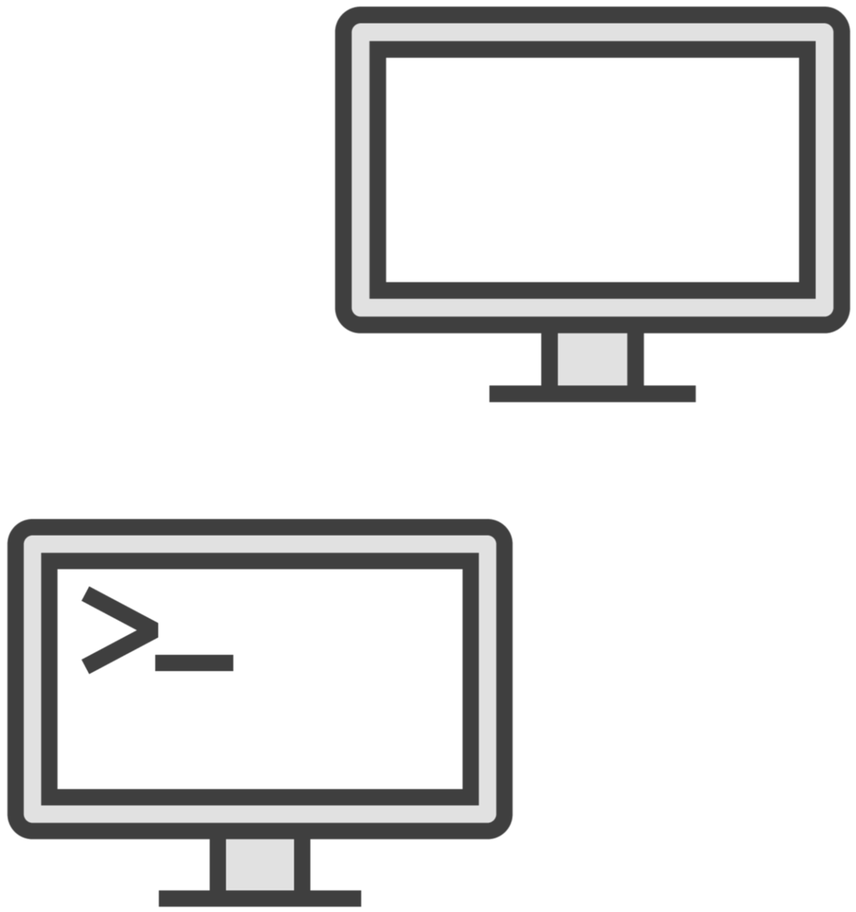
The user gets admin-level access

Create users

Configure system settings

Extract data

Offline Access Will Kill You!



All the time in the world

Simple exploits are gapping holes

Demo

HiveNightmare: Escalating privileges

Horizontal Escalation

Horizontal Escalation

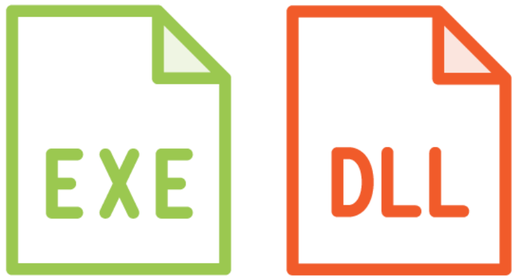
Same access, but with a different user account

Lay blame else where

DLL Hijacking

DLL Hijacking

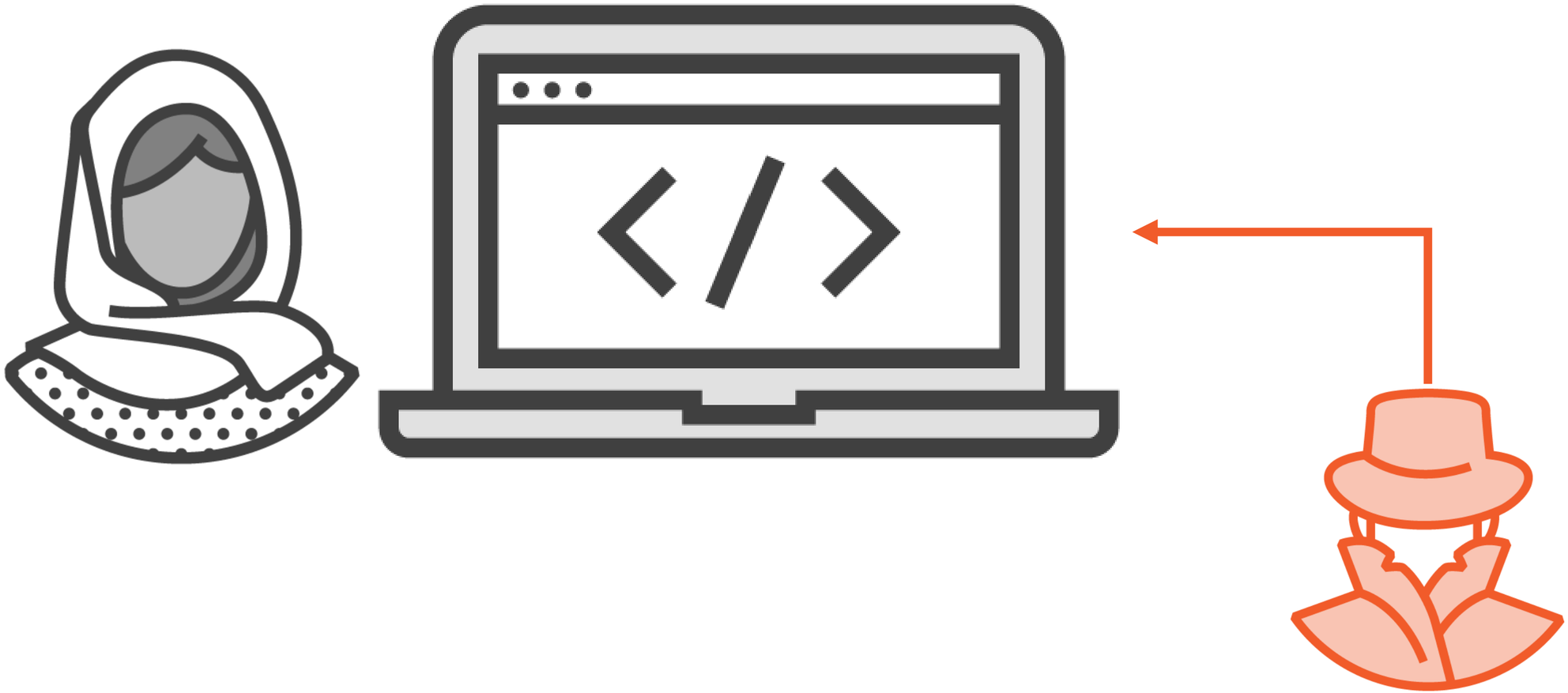
DLL Hijacking



DLL Hijacking

DLL Hijacking

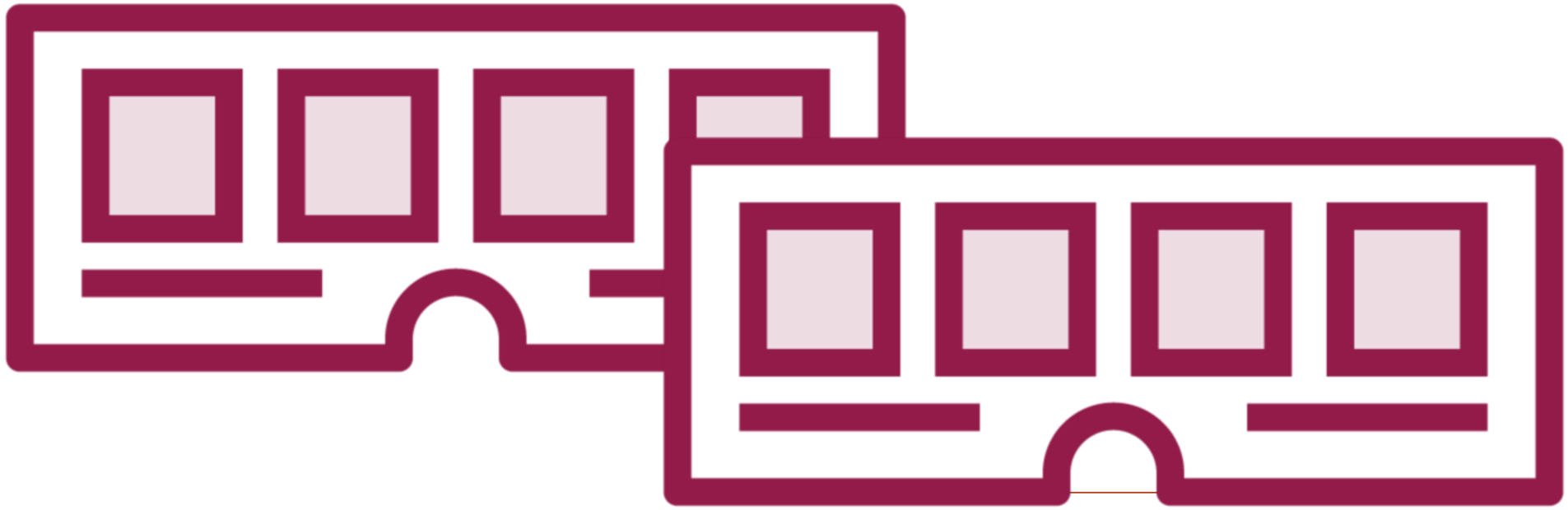
DLL Hijacking



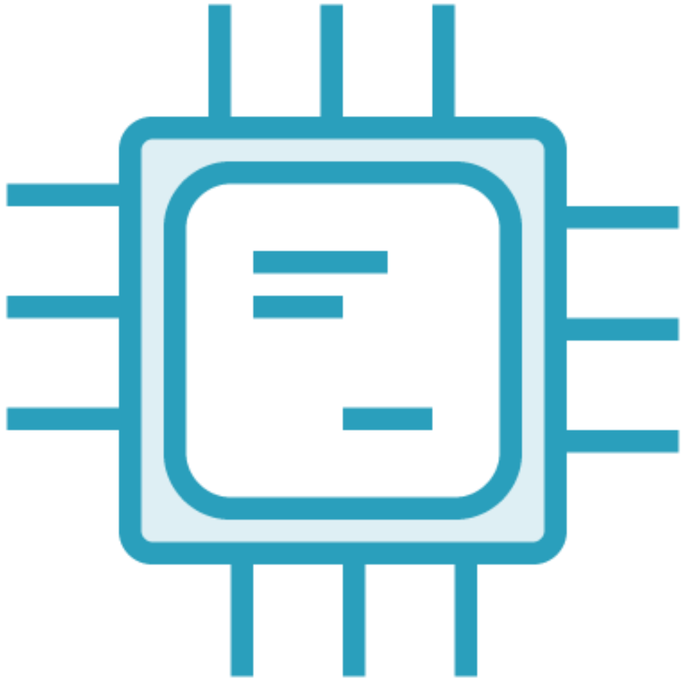
Windows Isn't The Only One

Spectre and Meltdown

Spectre and Meltdown

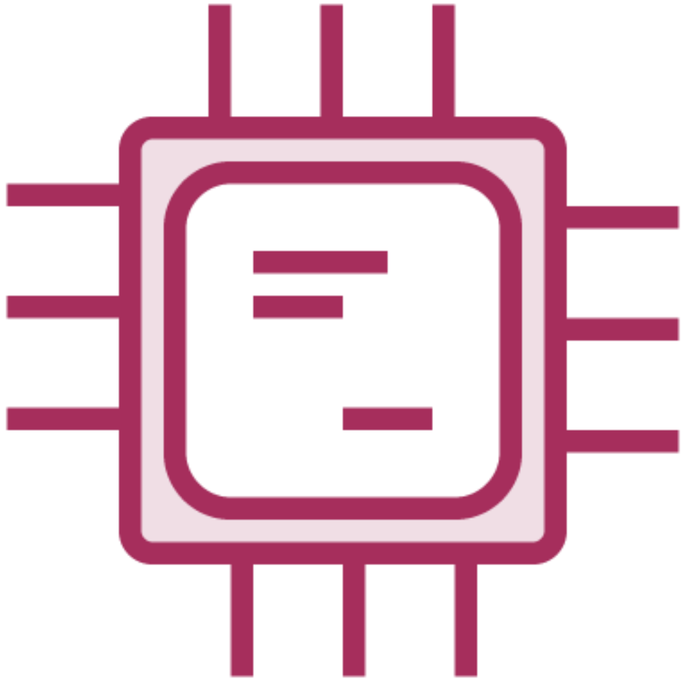


Spectre and Meltdown



- Apple
- AMD
- ARM
- Intel
- Samsung
- Qualcomm

Spectre and **Meltdown**



Apple

Intel

ARM

Other Issues

But Wait, There's More

- Application Shimming
- File System Permission Weakness
- Launch Daemon
- Path Interception
- Scheduled Tasks
- Access Token

But Wait, There's More

Setuid and Setgid

Web Shell

Buffer Overflows

Plist Modification

Countermeasures

How Do I Slow Them Down?

Encryption

Least privileges

Updates, updates, updates

Limit interactive logon

Service accounts don't need all rights

Limit the extent of code that runs "high"

How Do I Slow Them Down?

Privilege separation approach

Test OS and app coding meticulously

Multi-factor = good

Stress tests

Next Up:

Maintaining Access: Executing Applications