Cyber Defense Organization

Fall 2018 - Intro to Windows

PSA

Reset your Chegg account.

https://techcrunch.com/2018/09/26/chegg-resets-40-million-user-passwords-after-data-breach/

Twitter DMs were vulnerable

“If you interacted with an account or business on Twitter that relied on a developer using the AAAPI to provide their services, the bug may have caused some of these interactions to be unintentionally sent to another registered developer”

https://www.cyberscoop.com/twitter-api-bug/

Small Term of the Week: CVSS Score

The Common Vulnerability Scoring System (CVSS) is the industry standard method to evaluate and explain a vulnerability from its security implications perspective.

Scores range from 0 to 10, with 10 being the most severe. (Arbitrary Remote Code Execution).

Example: Shell Shock

CVE-2014-6271

Base Score: 10.0 HIGH

Vector: (AV:N/AC:L/Au:N/C:C/I:C/A:C)

Access Vector (AV): Network
Access Complexity (AC): Low
Authentication (AU): None
Confidentiality (C): Complete
Integrity (I): Complete
Availability (A): Complete

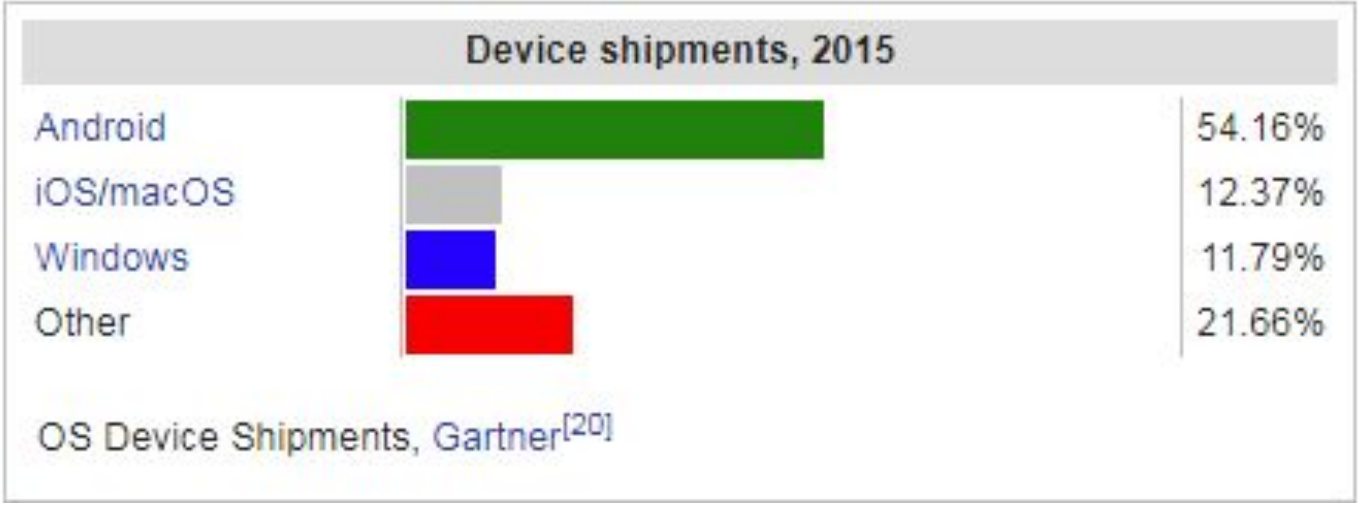
Survey. Which do you think is most popular?

Mac?

Linux?

Windows?

Trick Question: Android



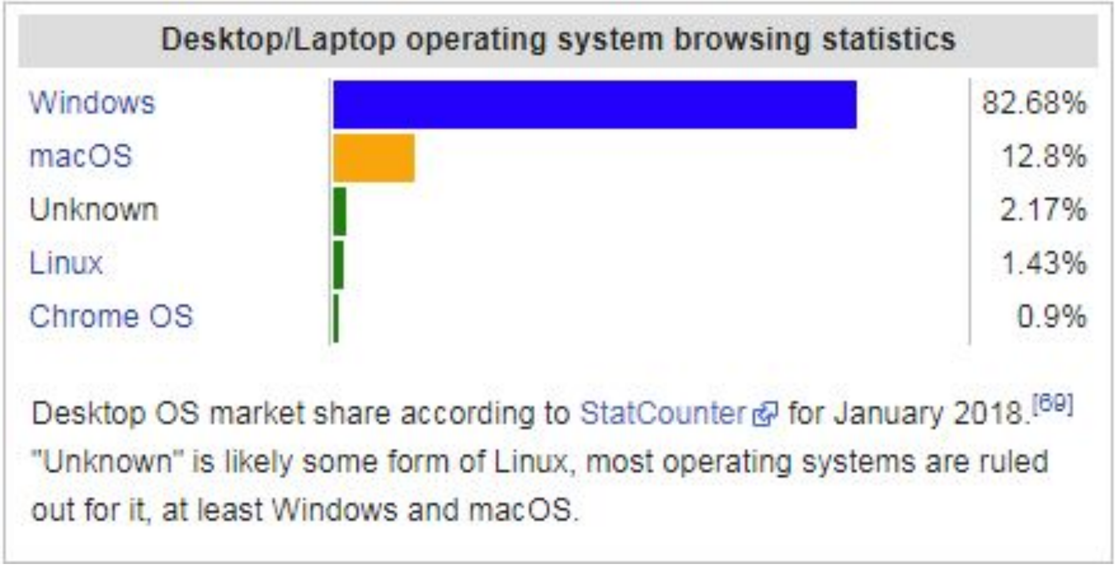
Device shipments, 2015

Android	54.16%
iOS/macOS	12.37%
Windows	11.79%
Other	21.66%

OS Device Shipments, Gartner[20]

Cite:Wikipedia

Desktop Browser



Desktop/Laptop operating system browsing statistics

Windows	82.68%
macOS	12.8%
Unknown	2.17%
Linux	1.43%
Chrome OS	0.9%

Desktop OS market share according to StatCounter for January 2018.[69] "Unknown" is likely some form of Linux, most operating systems are ruled out for it, at least Windows and macOS.

Us chromebook users will slowly take over!

On to Windows proper

What is it?

-Basically a Windows 10 box with a bunch of possibilities built-in.

-Most importantly: It has a GUI. (Take that Linux Servers).

Windows Server 2016

So what can it do? (And let’s look at that)

SMB Server

- FTP Server

- Exchange Server

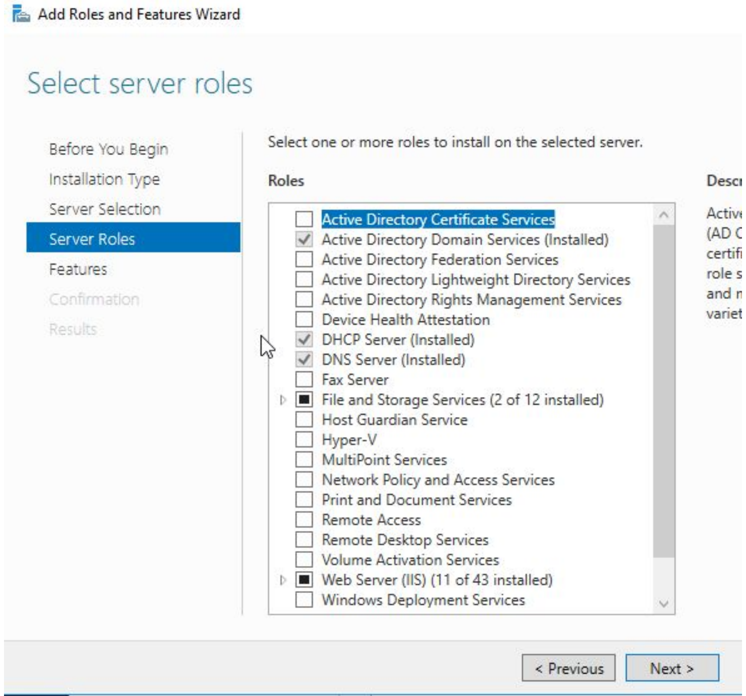
- Application deployment

- Centralized monitoring

- VPN

- DNS

- IIS (web server)



Add Roles and Features Wizard

Select server roles

Before You Begin
Installation Type
Server Selection
Server Roles
Features
Confirmation
Results

Select one or more roles to install on the selected server.

Roles

☐ Active Directory Certificate Services
☑ Active Directory Domain Services (Installed)
☐ Active Directory Federation Services
☐ Active Directory Lightweight Directory Services
☐ Active Directory Rights Management Services
☐ Device Health Attestation
☑ DHCP Server (Installed)
☑ DNS Server (Installed)
☐ Fax Server
■ File and Storage Services (2 of 12 installed)
☐ Host Guardian Service
☐ Hyper-V
☐ MultiPoint Services
☐ Network Policy and Access Services
☐ Print and Document Services
☐ Remote Access
☐ Remote Desktop Services
☐ Volume Activation Services
■ Web Server (IIS) (11 of 43 installed)
☐ Windows Deployment Services

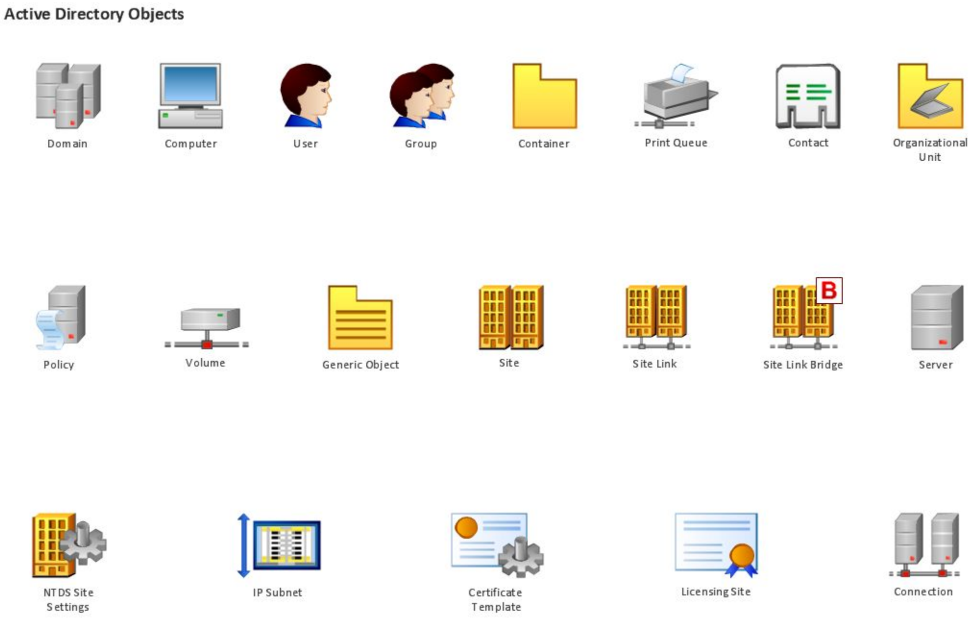
Descr

Active
(AD C
certifi
role s
and r
variet

Most important role: AD

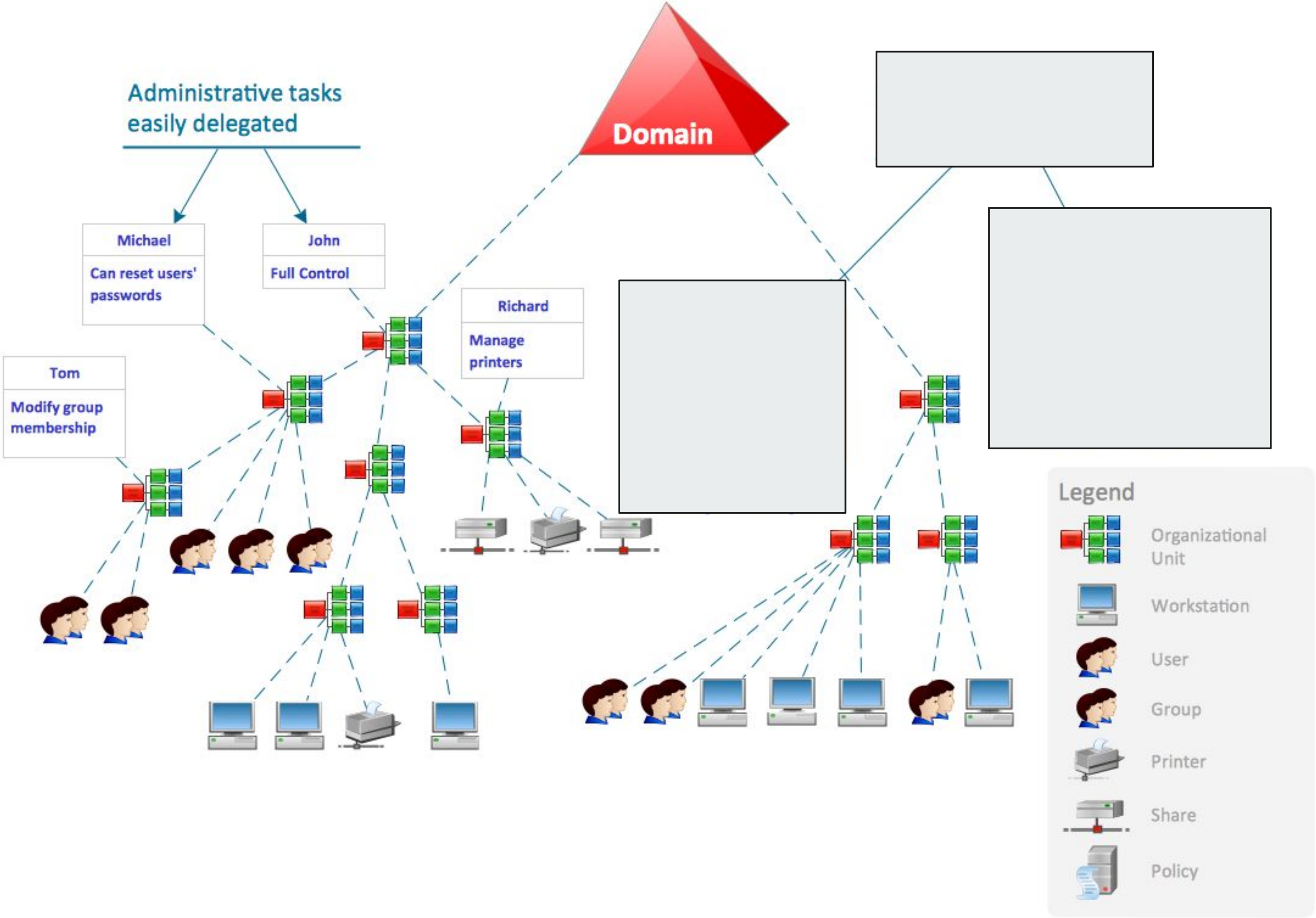
Active Directory is the glue that holds the ~~business~~ world together.

Parts of a domain: the problem



How the heck do you manage all that?

Prepare for messy graphic.



Administrative tasks easily delegated

Domain

Michael

Can reset users' passwords

John

Full Control

Tom

Modify group membership

Richard

Manage printers

Legend

Organizational Unit

Workstation

User

Group

Printer

Share

Policy

The Domain Controller

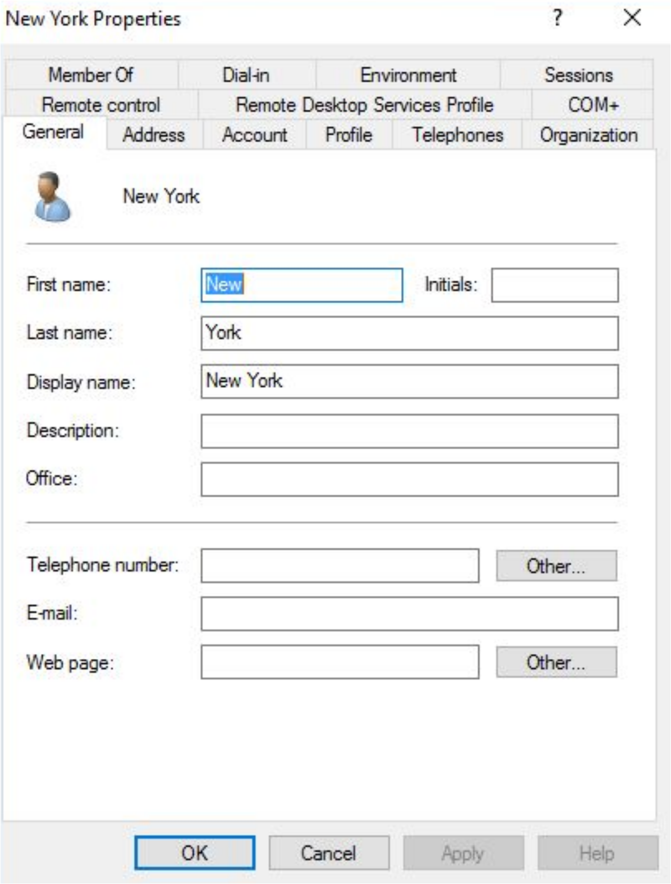
-It can retain information on computers, printers, and users.

-Give permissions to users based on their rank, or even what computer they log in on.

Users

Stores information on user

- Name
- Email
- Phone number
- Address
- Location in organization
- Password (hashed)



New York

First name: New

Initials:

Last name: York

Display name: New York

Description:

Office:

Telephone number:

E-mail:

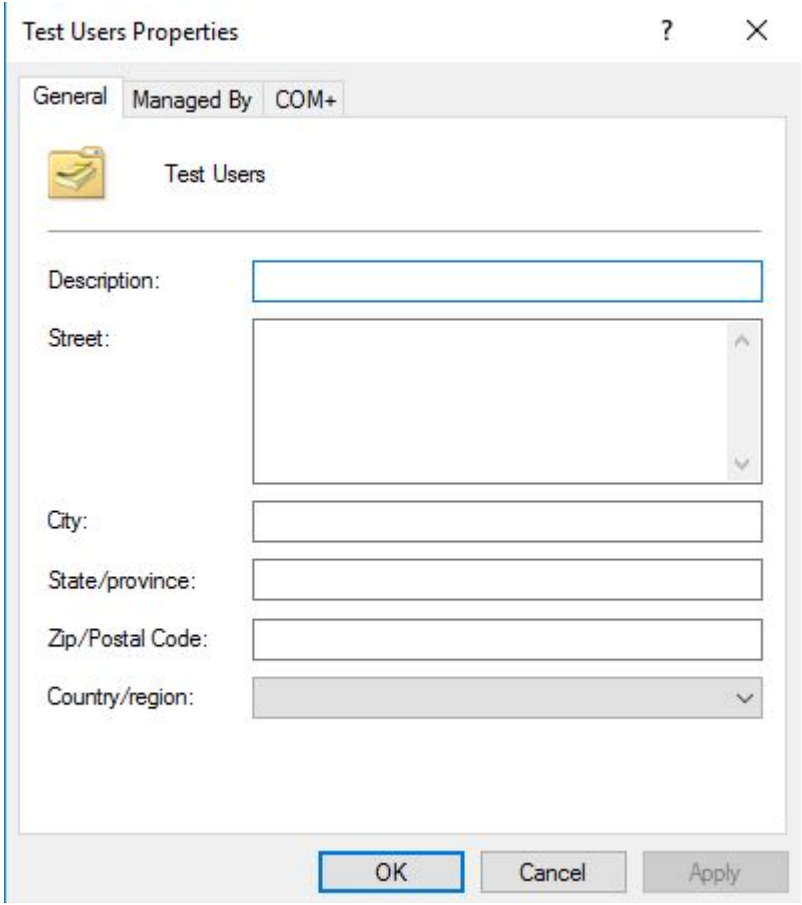
Web page:

Organizational Units

-Allows us to create groups of users, computers, printers etc. and give specific options to them.

-Test users might have one right, while Executive users might have more.

- Helps keep an avalanche of people and things organized

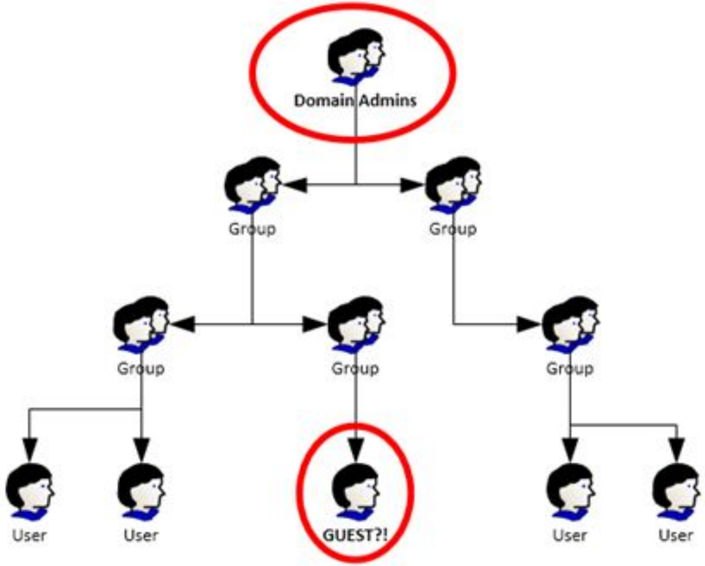


Nesting

Groups can be in groups. Yeah.

At this point you should preplan the domain around existing hierarchy.

Leads to inheritance rules which make me cry...especially when group policy.



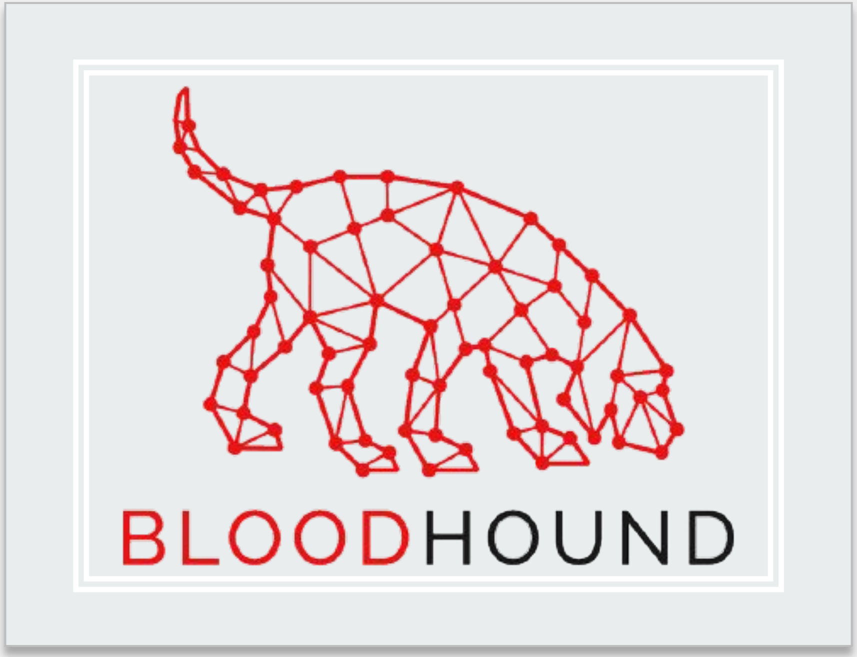
Recap.

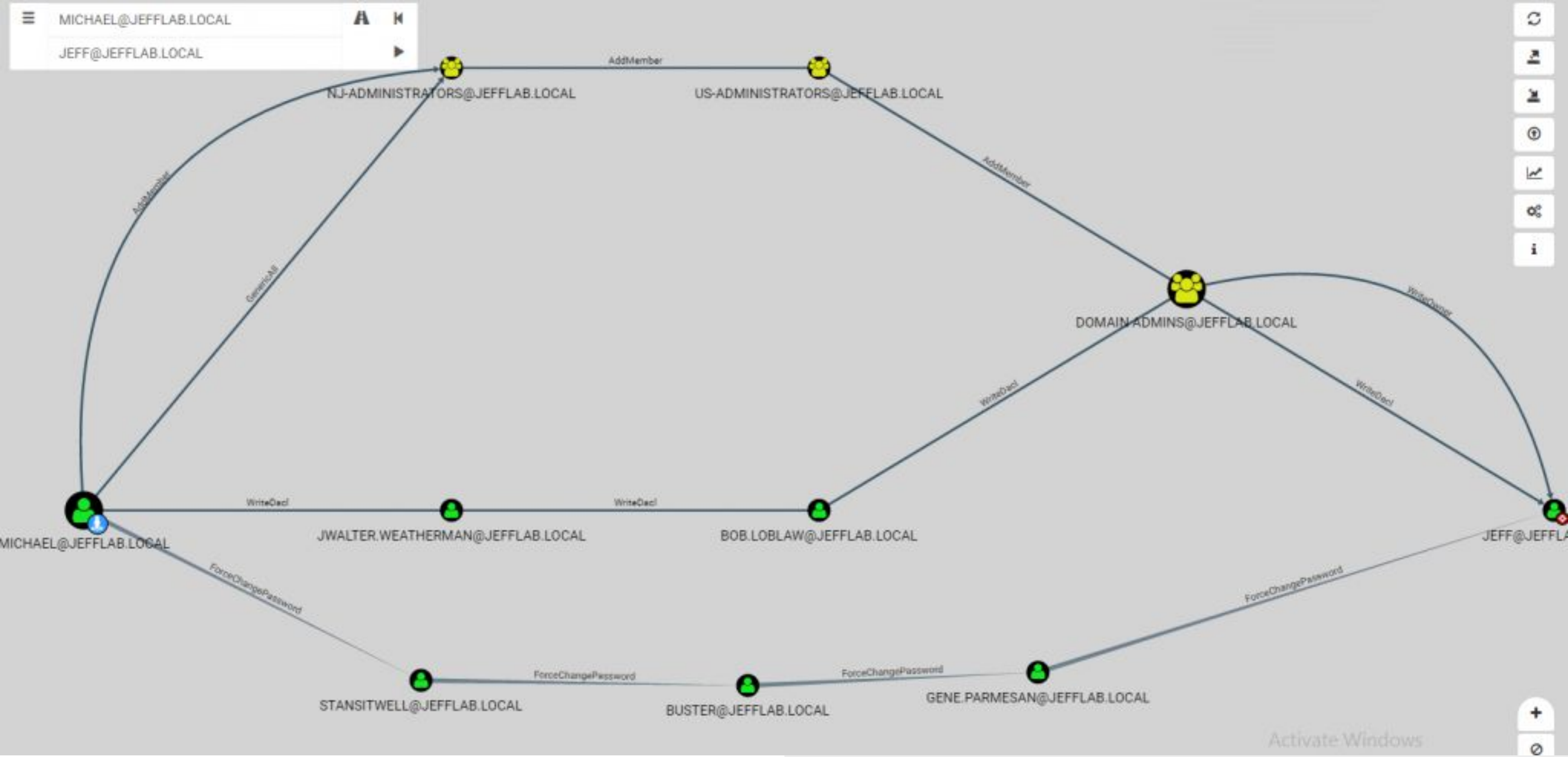
-Domains control network

- OU’s store information on things (objects)
- Groups contain objects
- Groups go in groups
- Windows is GUI frontend for a command line

Explore Active Directory

Tonight we will be using methods to understand and view this system.





MICHAEL@JEFFLAB.LOCAL

JEFF@JEFFLAB.LOCAL

Spectrum

Windows Server

Sense of Security

Password:

Cyberdeforg1!

Kali:
root / toor

Neo4j / toor

Links for nerds who look at these slides after.

https://github.com/BloodHoundAD/BloodHound

https://github.com/GoFetchAD/GoFetch

https://github.com/sense-of-security/ADRecon

https://bloodhoundgang.herokuapp.com/

Cya Next week!

Send your resume and a writing sample to mlim@albany.edu

Follow us on Twitter? Add on myInvolvement?

President of Center for Internet Security, Steve Spano
Tuesday night, 7:15PM in BB129

Gap week!

Introduction to Linux Security

- **Friday 3pm BB123**