Six Degrees of Domain Admin

Using Graph Theory to Accelerate Red Team Operations

DEF CON 24 – Las Vegas, NV 2016

Andy Robbins - @_wald0 Rohan Vazarkar - @CptJesus Will Schroeder - @harmj0y

About Us – Andy Robbins

- Offensive Network Services Team Lead at Veris Group's Adaptive Threat Division
- Red team and penetration test lead
- Performed hundreds of network penetration tests
- With Brandon Henry, identified critical vulnerability in ACH file processing procedures

About Us – Rohan Vazarkar

- Penetration tester at Veris Group's Adaptive Threat Division
- Co-author and major contributor to many projects, including EyeWitness and Python Empire
- Presenter: BSidesDC, BSidesLV, BSidesDE, Black Hat Arsenal
- Trainer: Black Hat USA 2016

About Us – Will Schroeder

- Researcher at Veris Group's Adaptive Threat Division
- Co-founder of the Veil-Framework, PowerView, PowerUp, Empire/EmPyre
- Active PowerSploit devleoper
- Microsoft PowerShell/CDM MVP
- Speaker and various cons and BlackHat trainer

"Defenders think in lists. Attackers think in graphs. As long as this is true, attackers win."

- John Lambert, General Manager, Microsoft Threat Intelligence Center

Agenda

- The Current State of AD Domain Privilege Escalation
- The Concept of “Derivative Local Admin”
- A Crash Course in Graph Theory
- Stealthy Data Collection with PowerView
- The Release of BloodHound
- Closing Remarks and Future Plans

Prior Work

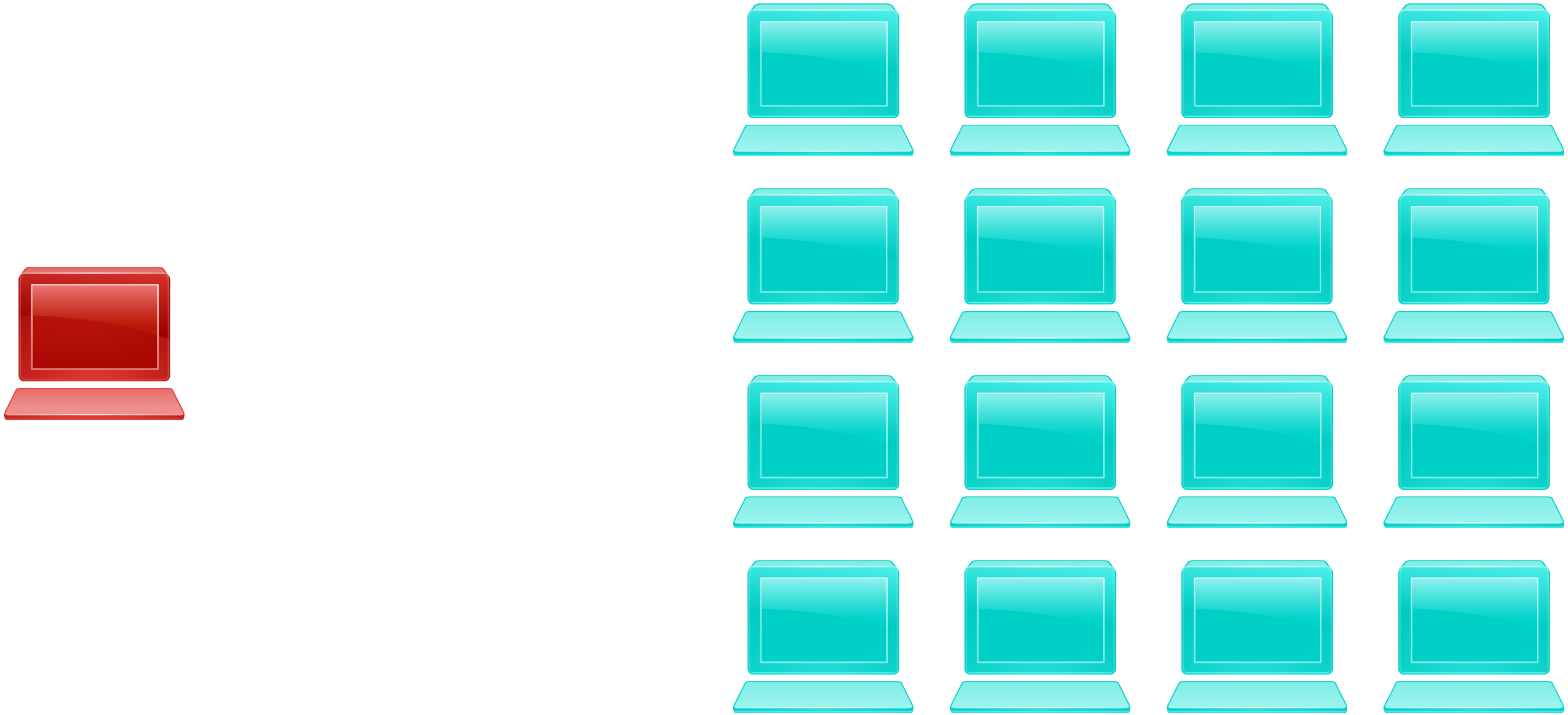
- ”Derivative Local Admin” by Justin Warner (@sixdub) - http://www.sixdub.net/?p=591
- Active Directory Control Paths by Emmanuel Gras and Lucas Bouillot - https://github.com/ANSSI-FR/AD-control-paths
- One of the best AD Security resources - https://adsecurity.org/

The Current State of Active Directory Domain Privilege Escalation

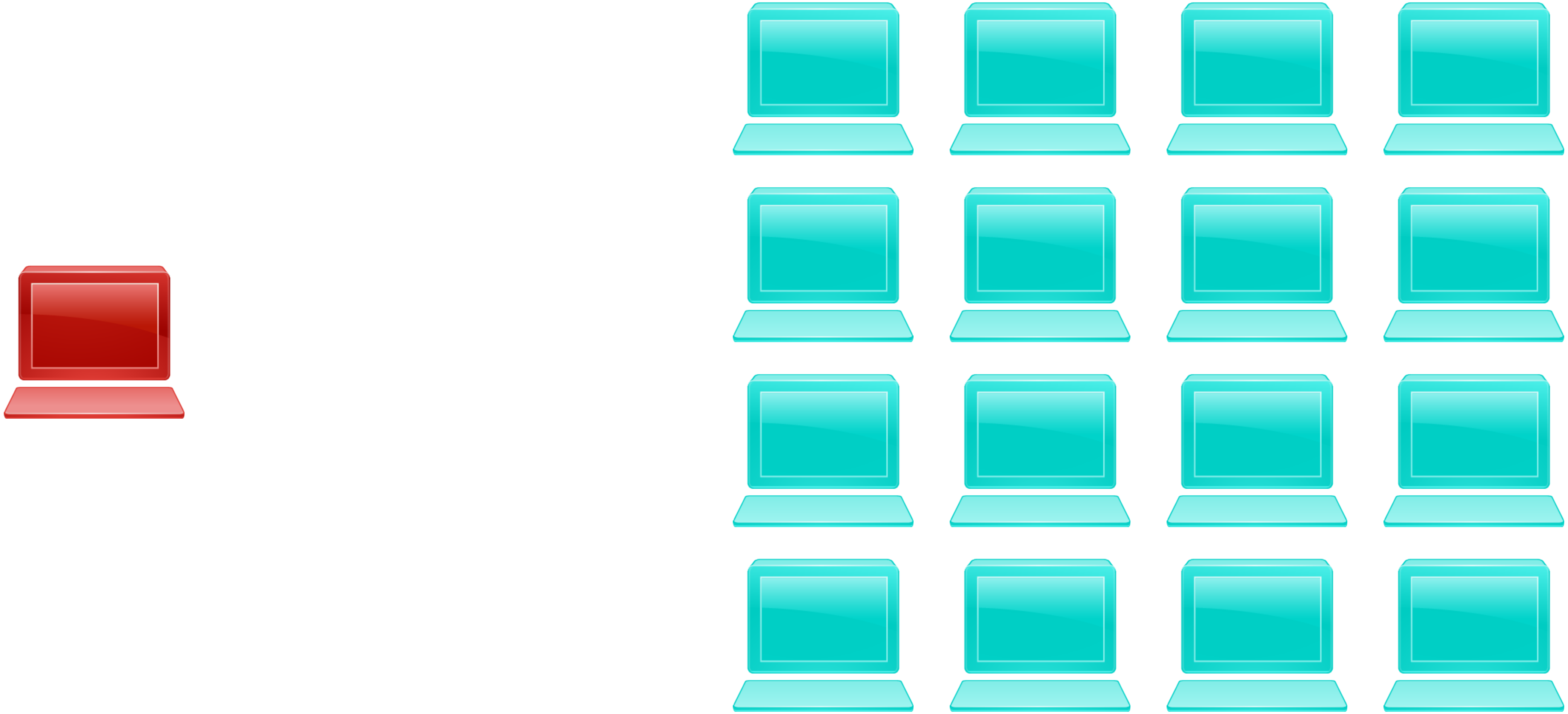
Current State of AD Domain Priv Esc

- Active Directory is ubiquitous.
- LOTS of security research devoted to Active Directory
- Sometimes we get easy buttons! ☺
- Easy buttons have a tendency to disappear.
- The best tradecraft includes, but does not rely on easy buttons

A Tale of Two Networks



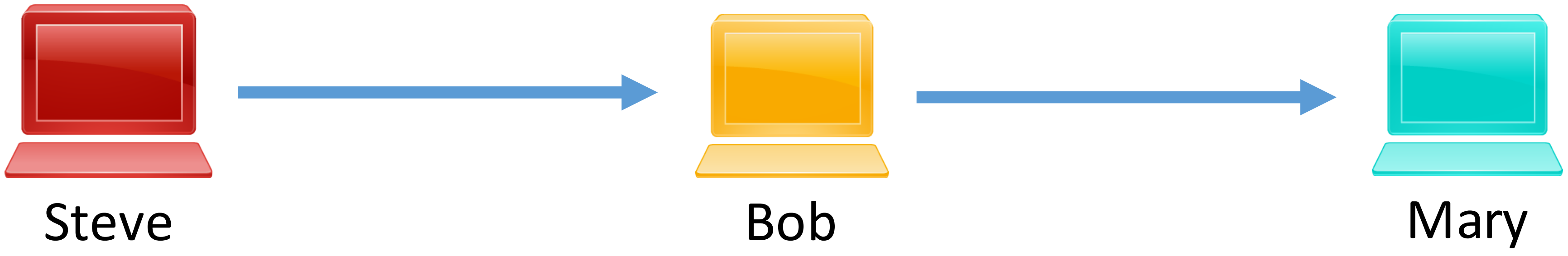
A Tale of Two Networks



The Concept of “Derivative Local Admin”

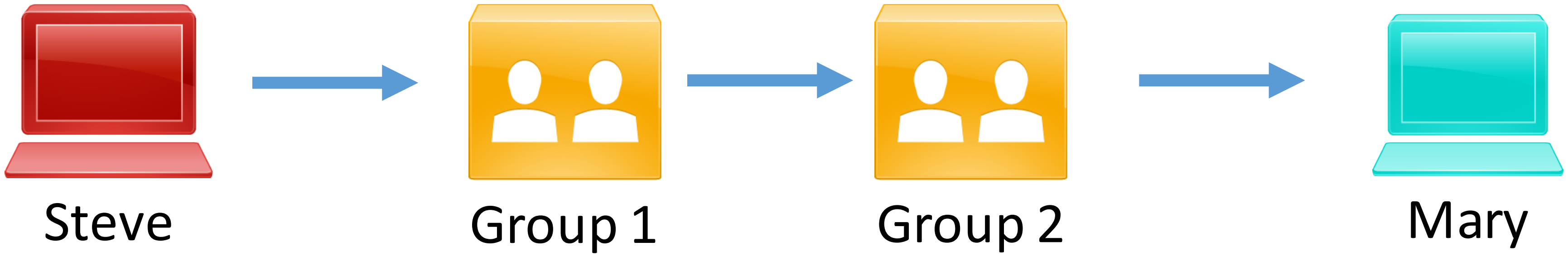
Derivative Local Admin

- The chaining or linking of administrator rights through compromising other privileged accounts
- Also referred to as a “Snowball attack” by Microsoft Research as early as 2009
  - “Derivative Local Admin” first coined in this blog post: sixdub.net/asdf

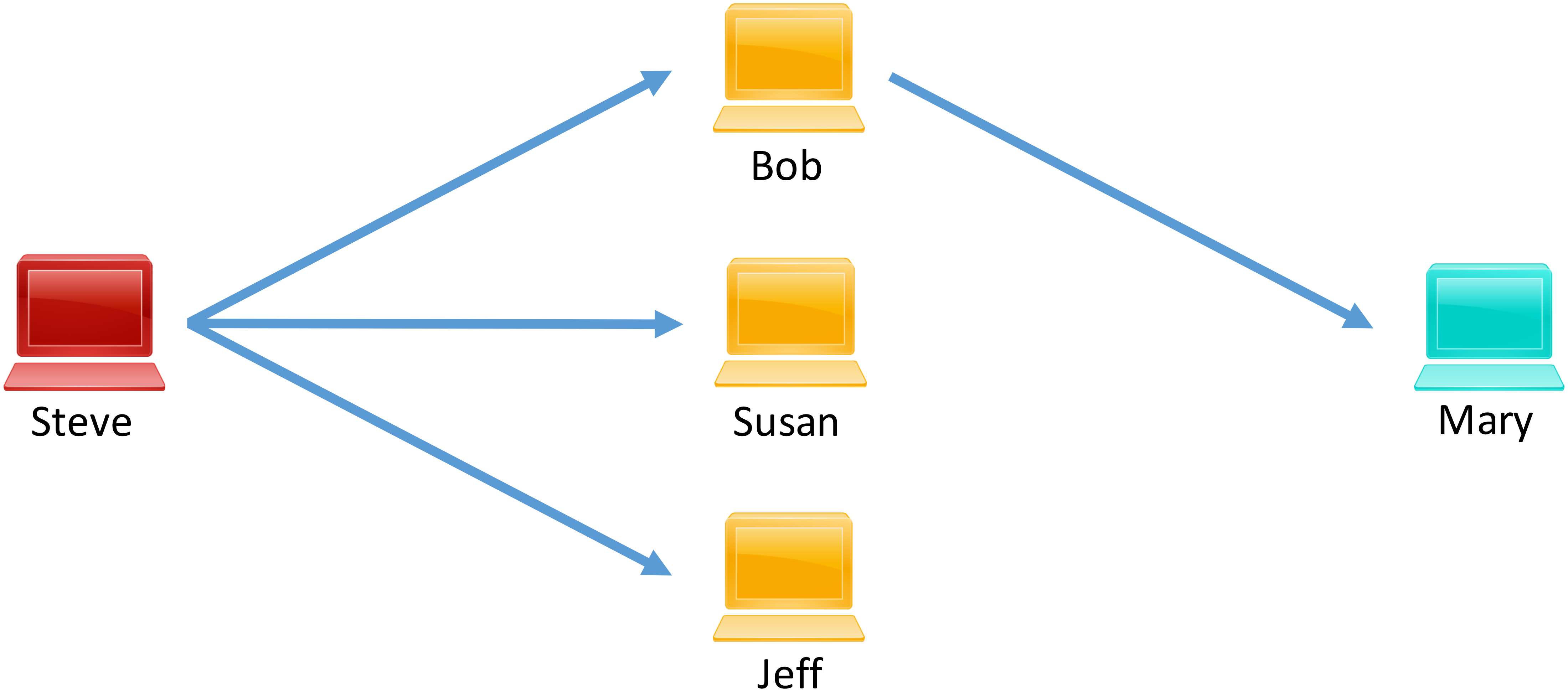


Derivative Local Admin

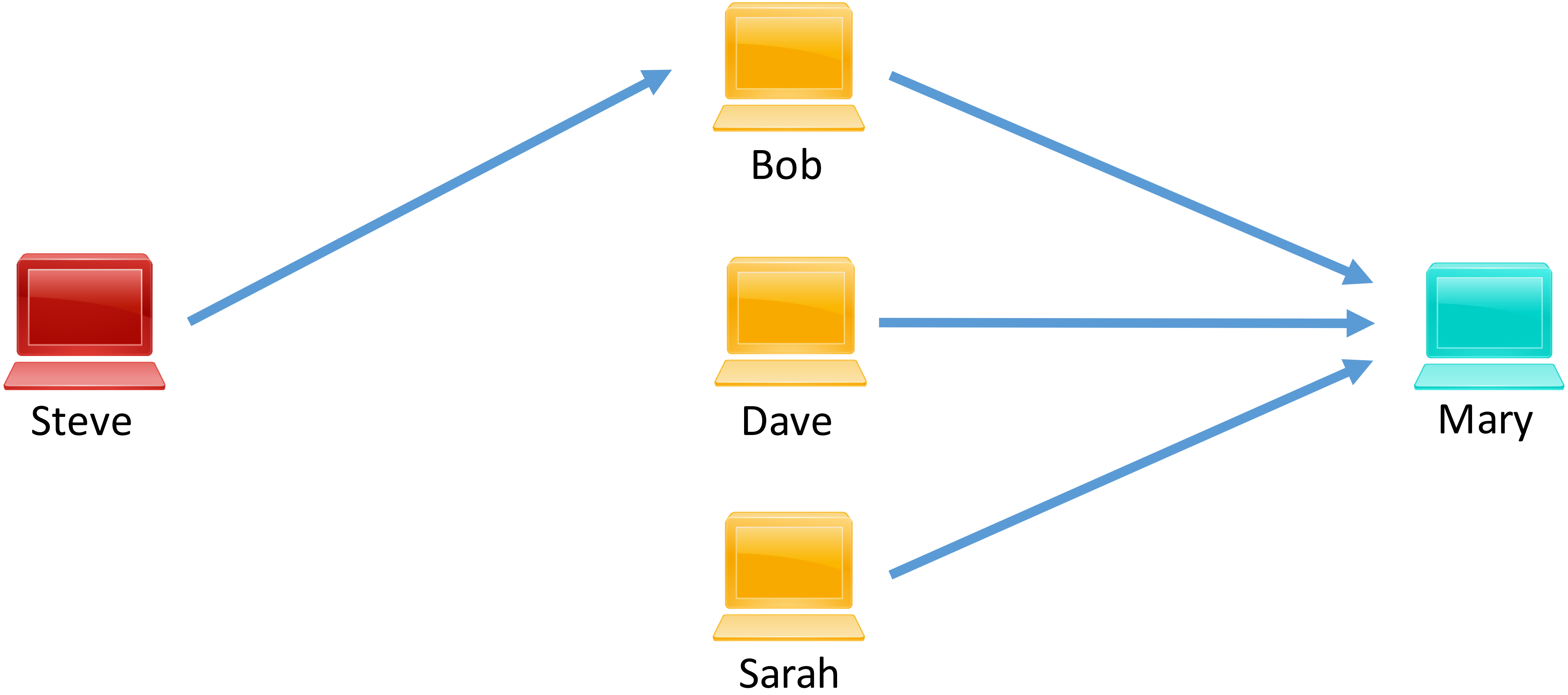
- This often occurs due to runaway nested groups, making it difficult to determine who the effective admins are on a given system.



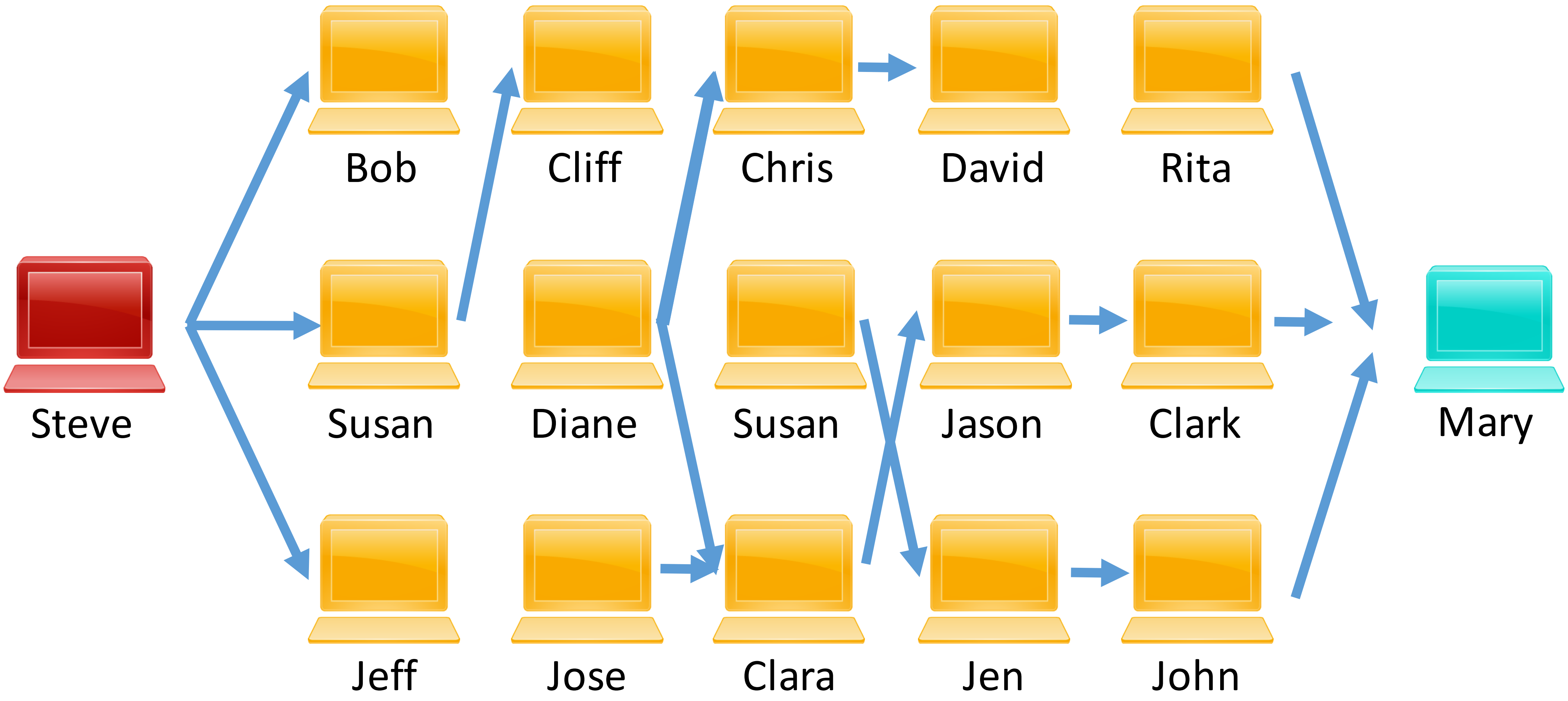
Derivative Local Admin – Forward Escalation



Derivative Local Admin – Reverse Analysis



Derivative Local Admin – The Combinatorial Explosion



Challenges with this approach

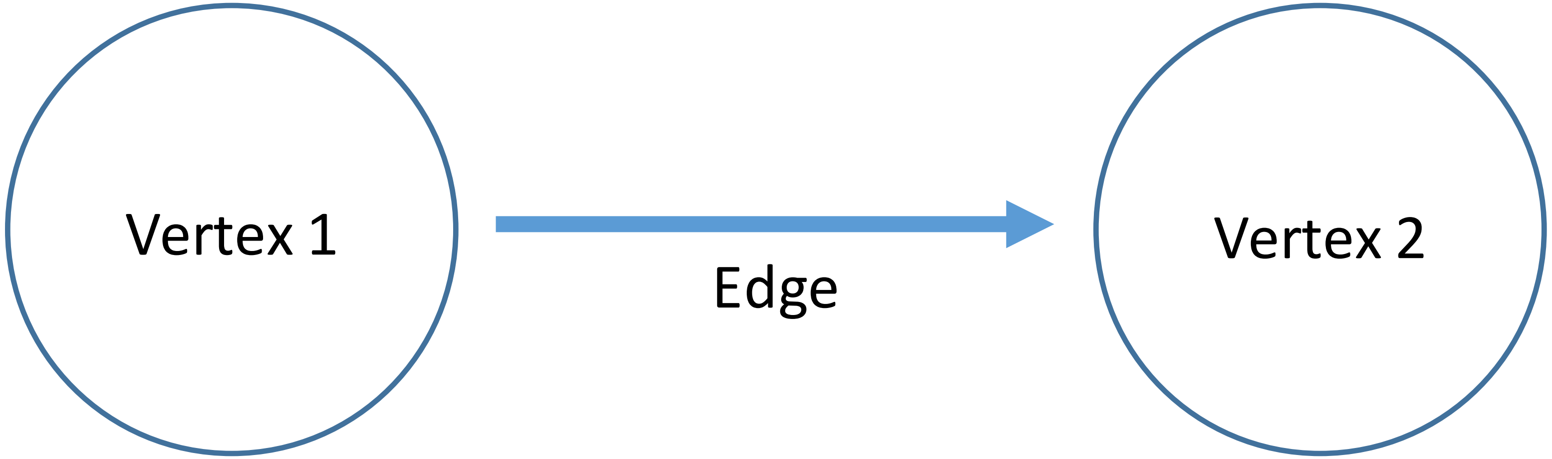
- Doesn’t scale
- Extremely time consuming and tedious
- May not identify the shortest (and certainly not all) path possible
- Domain Admin might not be necessary
- Limited situational awareness

A Crash Course in Graph Theory

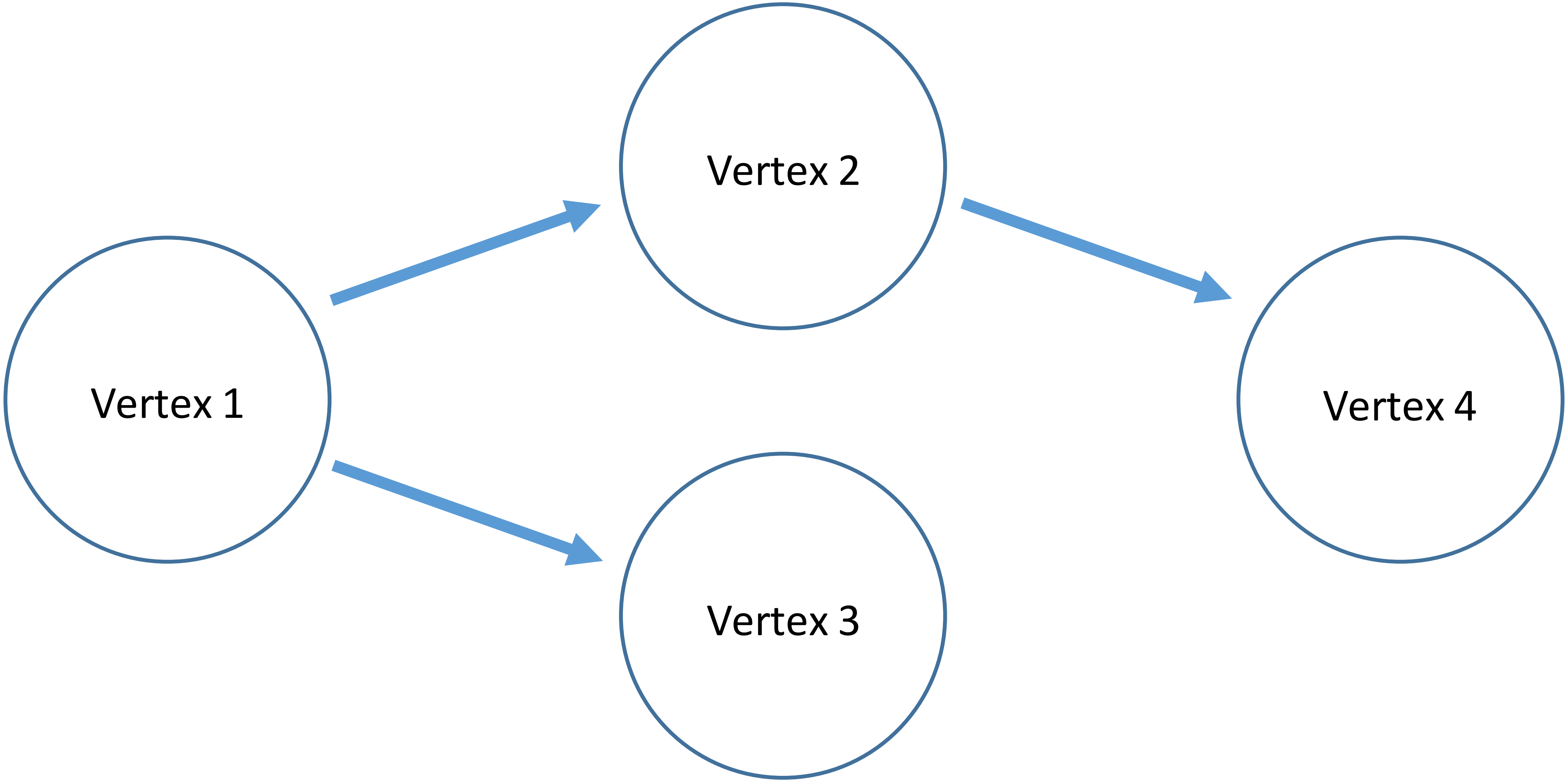
Graph Theory Crash Course

- Graphs are comprised of vertices (or nodes) and edges (or relationships).
- Vertices that share an edge are said to be “adjacent”
- Edges can be directed (or “one-way”) or undirected (or “bidirectional”)
- A path is a set of vertices and edges linking one vertex to another, whether those vertices are adjacent or not

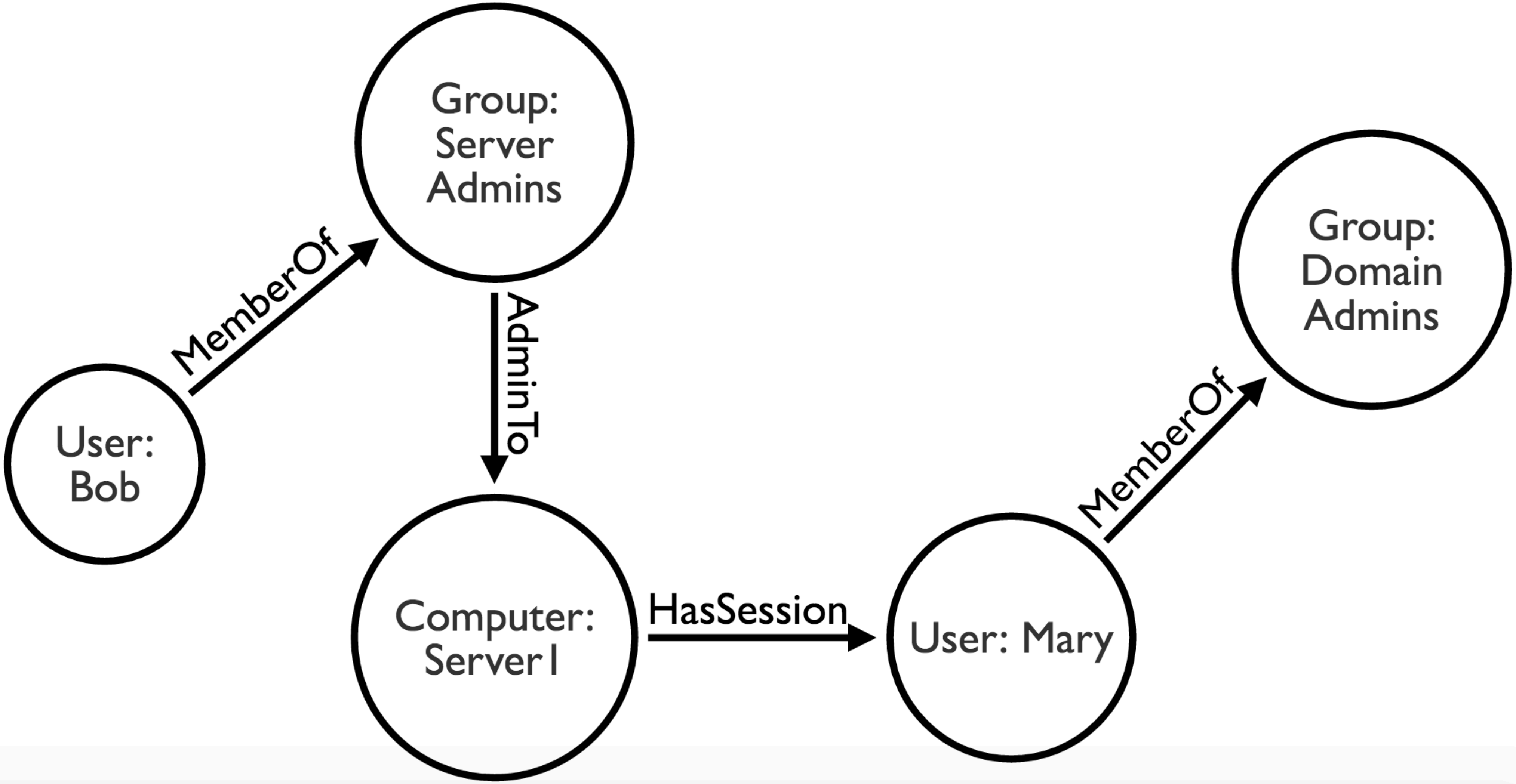
Graph Theory Crash Course



Graph Theory Crash Course



BloodHound Graph Design



Stealthy Data Collection with PowerView

Thanks?

- *“The best tool these days for understanding windows networks is Powerview [1].”*

-Phineas Fisher
http://pastebin.com/raw/0SNSvyjJ

PowerView

- A pure PowerShell v2.0 domain/network situational awareness tool
  - Fully self-contained and loadable in memory
  - Now part of PowerSploit™ (not really trademarked)
- Built to automate large components of the tradecraft on our red team engagements
- Collects the data that BloodHound is built on

Who’s Logged In Where?

- We deem this “user hunting”

- **Invoke-UserHunter** is built on:
  - **Get-NetSession –** who has sessions with a remote machine
  - **Get-NetLoggedOn** – who’s logged in on what machine
  - **Get-LoggedOnLocal –** who’s logged in on a machine (with remote registry)

- “Stealth” approach:
  - Enumerate commonly trafficked servers (i.e. file servers) and remote session information for each

Who Can Admin What?

- Did you know that Windows allows any domain-authenticated user to enumerate the members of a **local** group on a **remote** machine?
  - Either through the NetLocalGroupGetMembers() Win32 API call or the WinNT service provider

- PowerView:
  - **Get-NetLocalGroup –ComputerName IP [-API]**

Who Can Admin What (GPO Edition)?

- Let’s correlate what GPOs set the local administrators group with with OUs/sits these GPOs are applied to
  - Lets us determine who has admin rights where based on GPO settings
  - This isn’t a super simple process…

- PowerView’s **Find-GPOLocation** will enumerate this for a specific target or dump all relationships by default

Who's in What Groups?

- Not too crazy, just enumerate all groups and all members of each group through LDAP/ADSI searches

- **Get-NetGroup | Get-NetGroupMember**

- That's it!

Bringing it All Together

- The BloodHound ingestor is a customized version of PowerView with the following two functions added:
  - **Export-BloodHoundData** – exports PowerView data objects to the BloodHound Neo4j batch RESTful API
  - **Get-BloodHoundData** – automates the data ingestion and pipes results to Export-BloodHoundData

- We have a PowerShell v2.0 ingestion tool that:
  - Doesn’t need administrator rights to pull lots of data
  - Directly ingests data into BloodHound

The Release of BloodHound

The Release of BloodHound

- Easy-to-use, intuitive web interface for interacting with a graph database
- Built with Linkurious.js
- Lots of fun capabilities that Rohan will demo right now

BLOODHOUND

Closing Remarks and Future Plans

Future Plans

- Increase the scope of elements modeled in the BloodHound graph, including AD object ACLs, GPOs, and more
- Continued research on the applications of graph theory to Active Directory security
- Defense-centric capability
- Continuing maturation of data collection, ingestion, and analysis methods

Closing Remarks

- As defensive postures improve, attack paths will increasingly rely on environmental misconfigurations, and poor implementations of least privilege and administrator account hygiene
- Graph theory enables rapid attack path analysis
- BloodHound is a free and open source Active Directory domain privilege escalation capability which utilizes graph theory

Go Get BloodHound!

- https://www.github.com/adaptivethreat/bloodhound

- Contact Us:
- Andy Robbins -- @_wald0
- Rohan Vazarkar -- @CptJesus
- Will Schroeder -- @harmj0y