I <3 Your AD

OFFENSIVE AD AUDITING – A HOW-TO

>Whoami_

- Red Teamer for 10 years
- Recovering Blue Teamer
- Consultant reviewing numerous environments

- Pot Stirrer (nano for life)

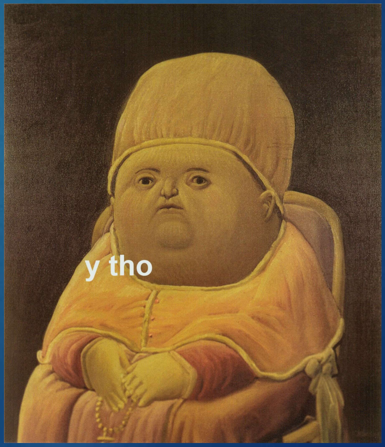
Tweeter:
@jarrodcoulter

Talk Outline

- Y Tho?
- How Tho?
- Show Me Bro
- Cool, But I Can’t Bro
- Recap
- Questions, Yo

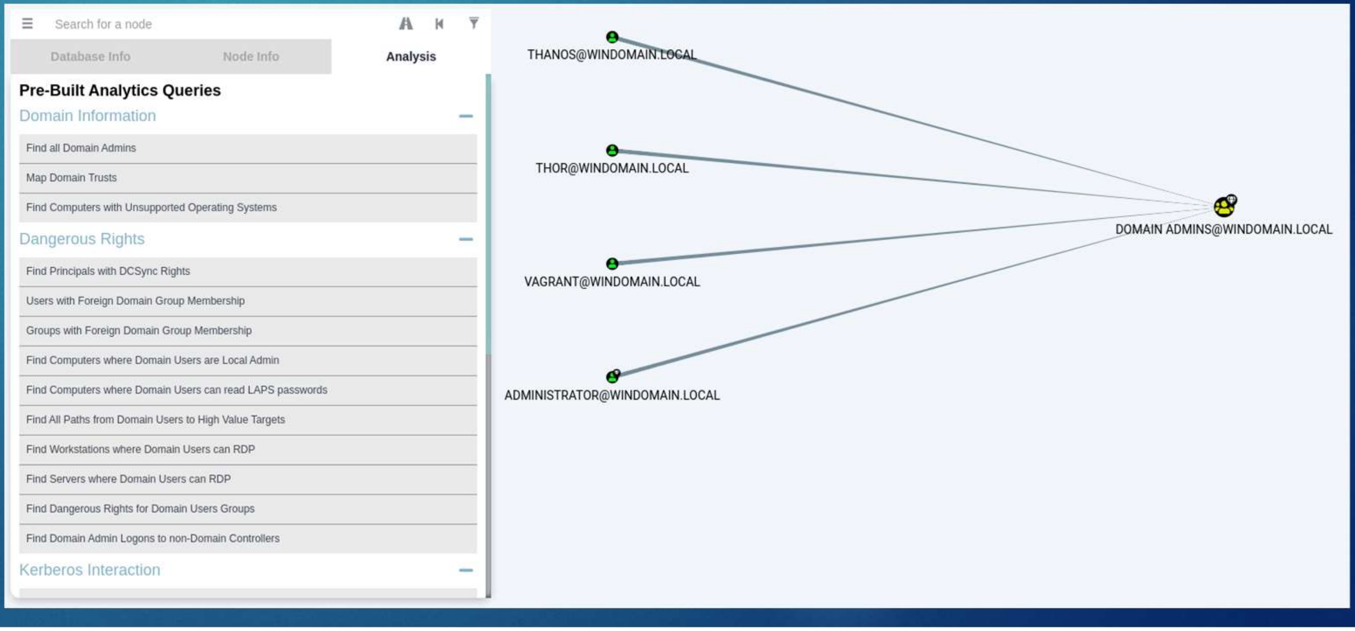
Why Would I Bother?

- Real World Example
  - Solarwinds Kerberoasting Attacks
  - https://www.cisa.gov/emergency-directive-21-01
- But I'm CIS | NIST | OWASP | SANS | TLA compliant and eliminated all the low hanging fruit
  - Did you?
  - Misconfigurations thrive in AD due:
    - Lack of expertise
    - Quick fixes to just make things work



OK, But How?

- Introduction To Bloodhound
  - Two Components
    - Collector
    - DB for Analysis
  - Quick view into common misconfigurations



Pre-Built Analytics Queries

Domain Information

- Find all Domain Admins
- Map Domain Trusts
- Find Computers with Unsupported Operating Systems

Dangerous Rights

- Find Principals with DCSync Rights
- Users with Foreign Domain Group Membership
- Groups with Foreign Domain Group Membership
- Find Computers where Domain Users are Local Admin
- Find Computers where Domain Users can read LAPS passwords
- Find All Paths from Domain Users to High Value Targets
- Find Workstations where Domain Users can RDP
- Find Servers where Domain Users can RDP
- Find Dangerous Rights for Domain Users Groups
- Find Domain Admin Logons to non-Domain Controllers

Kerberos Interaction

Audit Process

- Run Collector
- Upload data to analyze
- Perform analysis and validate
- Change Misconfigurations
- Perform Periodic Reviews

What am I looking For?

- Users with Administrative Access to Systems or Applications
  - Service Principal Names (SPNs) that are Domain Admin
  - Administrators that are daily users
- Domain Users with “Interesting” Access
  - All Access to Objects/Groups
  - Access to Modify Policy
- Machines with Unconstrained Delegation

Demo

That’s not real…

- I pulled that attack path from a real assessment
- This is far from the worst, most attack paths are way more straight forward, this was an excuse to show that sometimes you have to keep pulling on threads

LEFT
EXIT 12
Learn AD and only make approved changes
Get it done now
Busy and time constrained admins
imgflip.com

Arguments Against Open Source

- SpecterOps is a professional services organization
- They have reputational stake
- Enterprise version exists if your company requires support
- AD Explorer from Sysinternals
  - https://www.trustedsec.com/blog/adexplorer-on-engagements/

OK, Why Am I Doing This Again?

- Quick wins that will make attackers cry
- Better understanding of the effects of long term neglect
- Build up internal AD expertise

Credits

- SpecterOps - Bloodhound
- https://hausec.com/2019/09/09/bloodhound-cypher-cheatsheet/
- DetectionLab for AD
- https://github.com/jsecurity101/Import-Marvel

Questions?