ASSURE IT
ASSESS • VALIDATE • CONSULT

DA 101

Protecting your Domain Admin Account

3265 GATEWAY ROAD, SUITE 650 BROOKFIELD, WI 53045 / P: 262.373.7100 / INFO@SYNERCOMM.COM / SYNERCOMM.COM

$WHOAMI

- Penetration Tester @ SynerComm
- Bug Bounty Hunter on HackerOne
- Python enthusiast


jgardner@synercomm.com

@Rhynorater
@Rhynorater

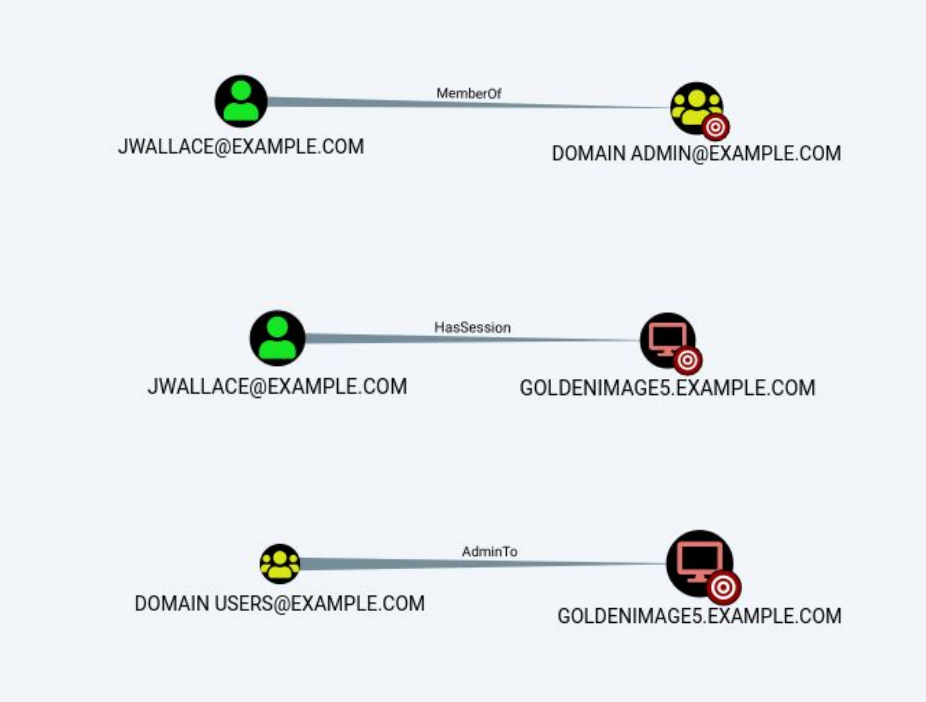
5 ROUTES TO DA

… and how to protect your administrators

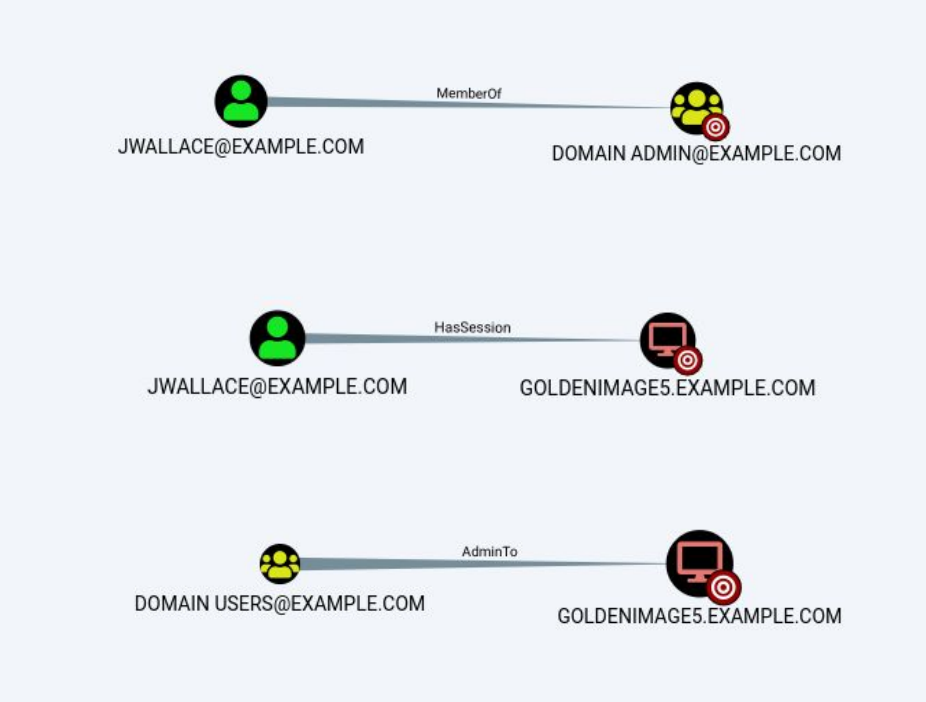
PERMISSIVE GLOBAL GROUP ACCESS + MIMIKATZ

Solution: Apply the principle of least privilege

Permissive Global Group Access + MimiKatz



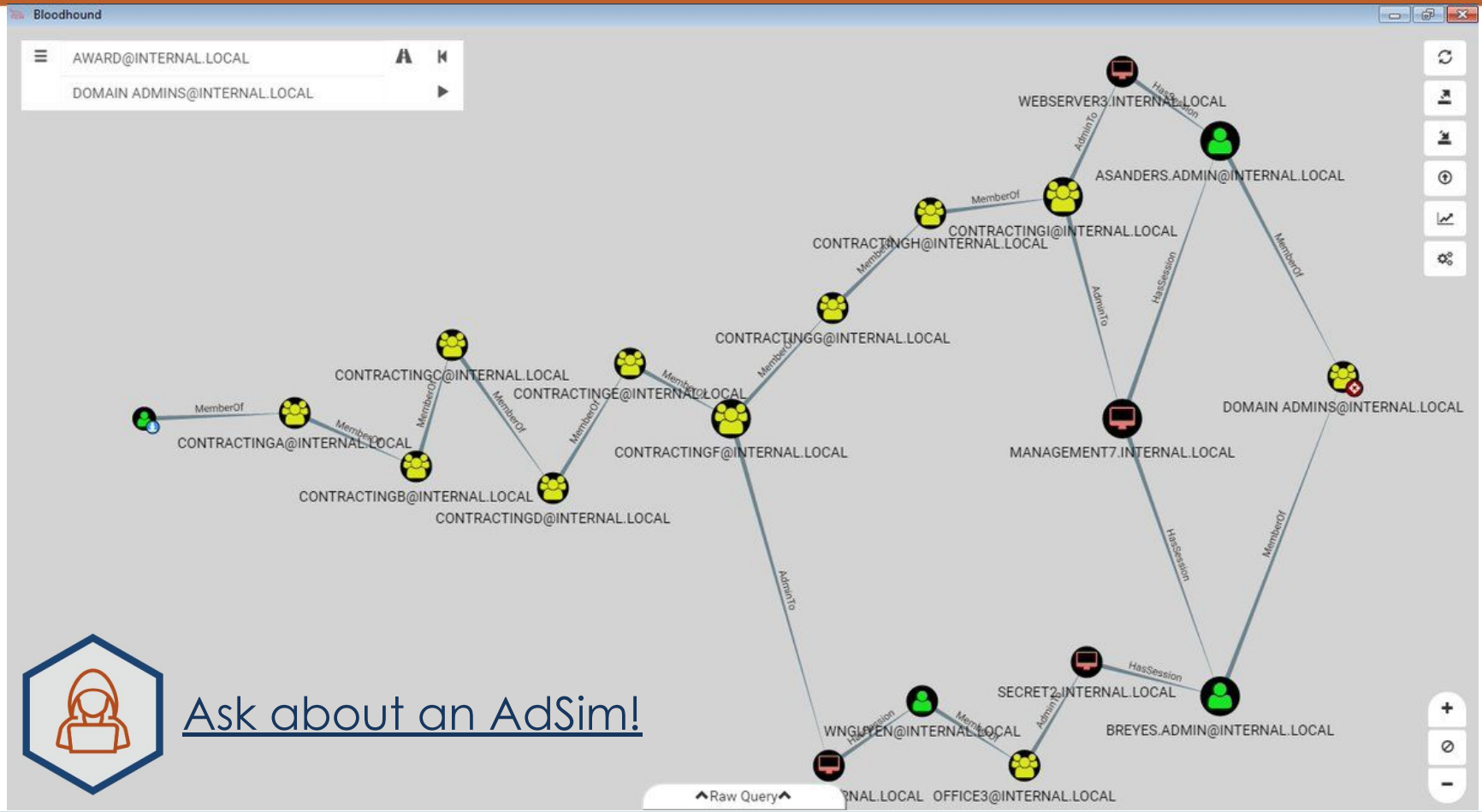
Permissive Global Group Access + MimiKatz



BloodHound

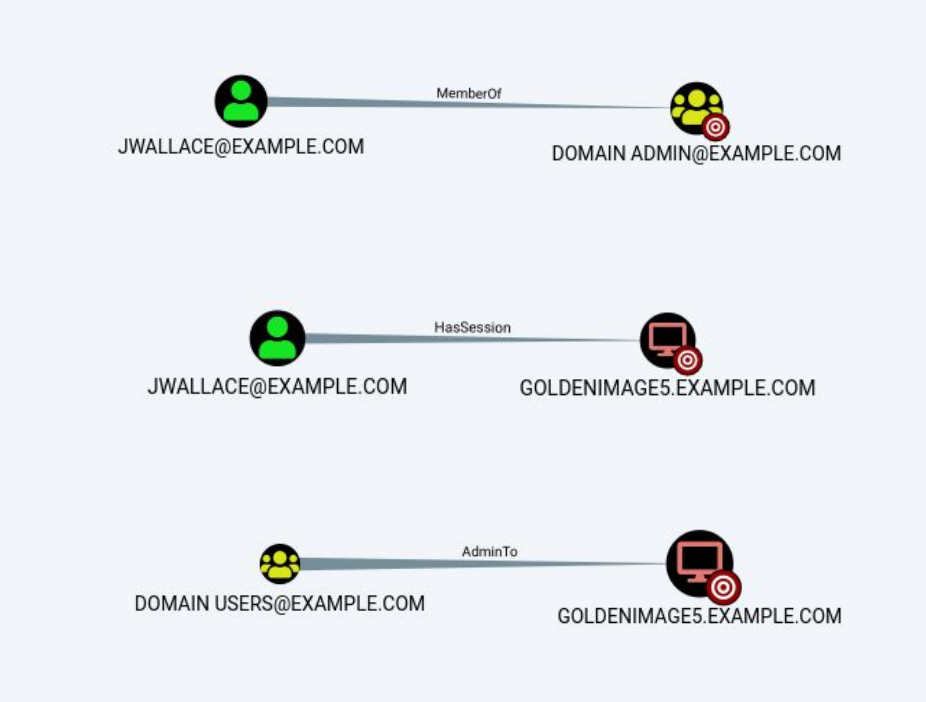
- Available on GitHub @BloodhoundAD
- 10 minute setup
- Queries DC and domain computer for session and admin information
- Creates pretty graphs … of death
- PowerShell & EXE available for information gathering

Adversary Simulation

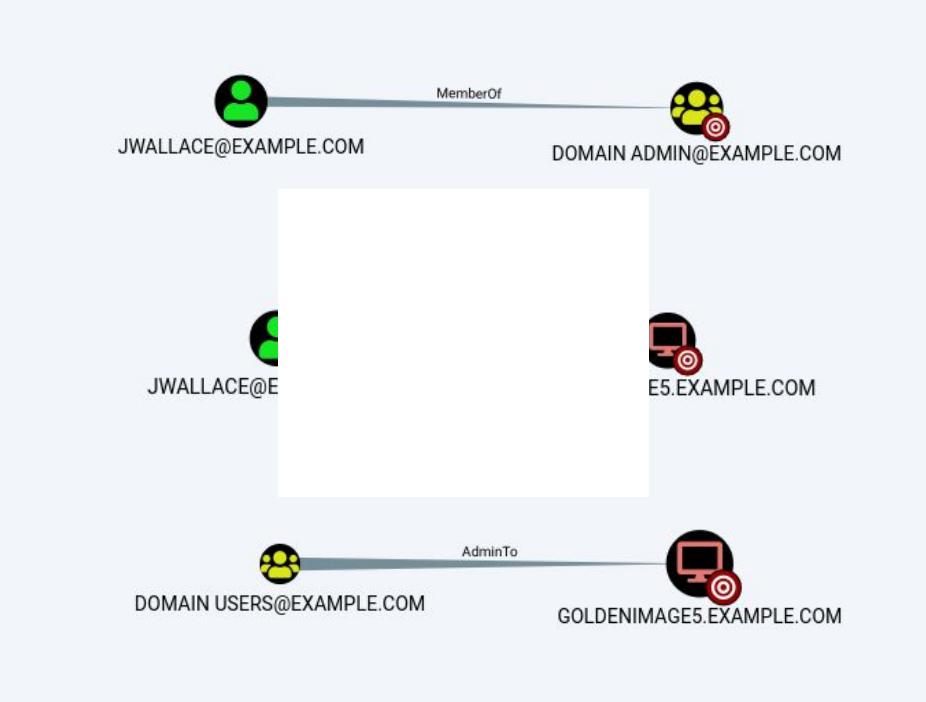


Ask about an AdSim!

Permissive Global Group Access + MimiKatz



Permissive Global Group Access + MimiKatz



Permissive Global Group Access + MimiKatz

Solution: Principle of Least Privilege

1. Determine who really needs to be a domain administrator
2. Don’t abuse Global Groups
3. Educate your DAs on when their account should be used

LLMNR & NBT-NS POISONING

Solution: Turn them off.

LLMNR & NBT-NS Poisoning

Graphic Credits: Aptive Consulting Ltd.

LLMNR & NBT-NS Poisoning

Responder.py

LLMNR & NBT-NS Poisoning

Inveigh.ps1

LLMNR & NBT-NS Poisoning

The Solution

- Turn off LLMNR in Group Policy
- Turn of NBT-NS via GPO Script
- Monitor your internal network for LLMNR & NBT-NS requests
    - Inveigh is super easy to use

LLMNR & NBT-NS Poisoning

Bonus: SMB Relay Attacks

SYSVOL PASSWORDS + LEAKED AES KEYS

Solution: Delete the XML files. Just delete them.

SYSVOL Passwords + Leaked AES Keys

Vulnerability came out in 2012, patch in 2013

We still see this ALL.THE.TIME.

SYSVOL Passwords + Leaked AES Keys

Who needs an AES key when the password is stored in cleartext?

Graphic Credit: https://adsecurity.org

SYSVOL Passwords + Leaked AES Keys

The Solution

- Educate your Sys Admins – don't put cleartext creds in files
- Apply the patch to change the AES key
- Delete old XML files with cpassword in them.

SYSVOL Passwords + Leaked AES Keys

Bonus: Run Get-GPPPassword on yourself!

https://github.com/PowerShellMafia/PowerSploit/blob/master/Exfiltration/Get-GPPPassword.ps1

KERBEROASTING

Solution: Long Service Account Passwords

KerberRoasting

Account used by service = any domain user can pull KRB5TGS hash

KerberRoasting

Audit your network with setspn.exe!

DC BACKUPS

Solution: Ensure no one but Domain Admins can access your DC backups

DC Backups

User with access to DC backup =
Domain Admin

Takeaways

1. A local admin can extract from memory the cleartext password of any authenticated user
2. Turn off LLMNR. Turn off NBT-NS. Monitor for these requests
3. SYSVOL Passwords + Leaked AES Keys
4. Domain accounts used to run services should have long and complex passwords
5. Only Domain Admins should have access to DC Backups

DA101 - Kit

https://www.SHELLNTELL.com/blog/da-101

Question or Help? Justin Gardner – jgardner@synercomm.com

Questions?