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

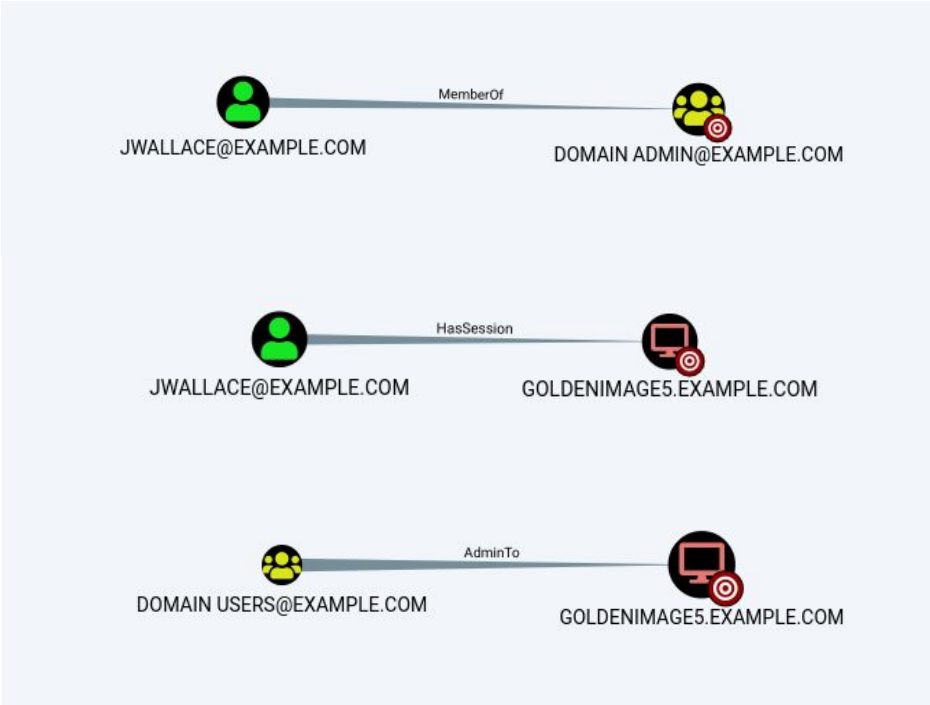
5 ROUTES TO DA

… and how to protect your administrators

PERMISSIVE GLOBAL GROUP ACCESS + MIMIKATZ

Solution: Apply the principle of least privilege

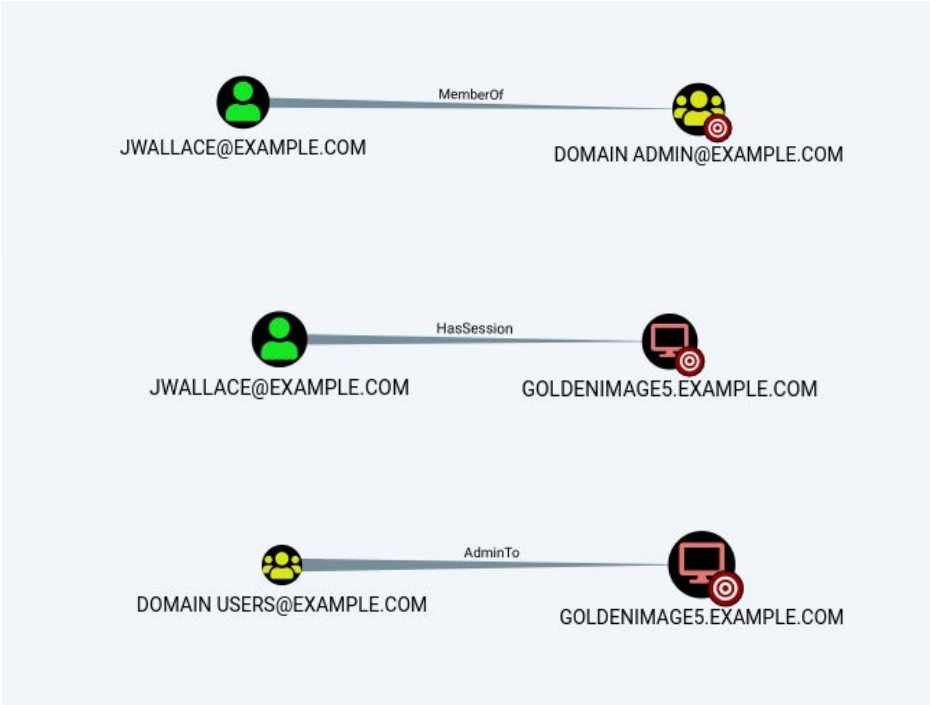
Permissive Global Group Access + MimiKatz



Takeaway:

SYNERCOMM

Permissive Global Group Access + MimiKatz



Takeaway:

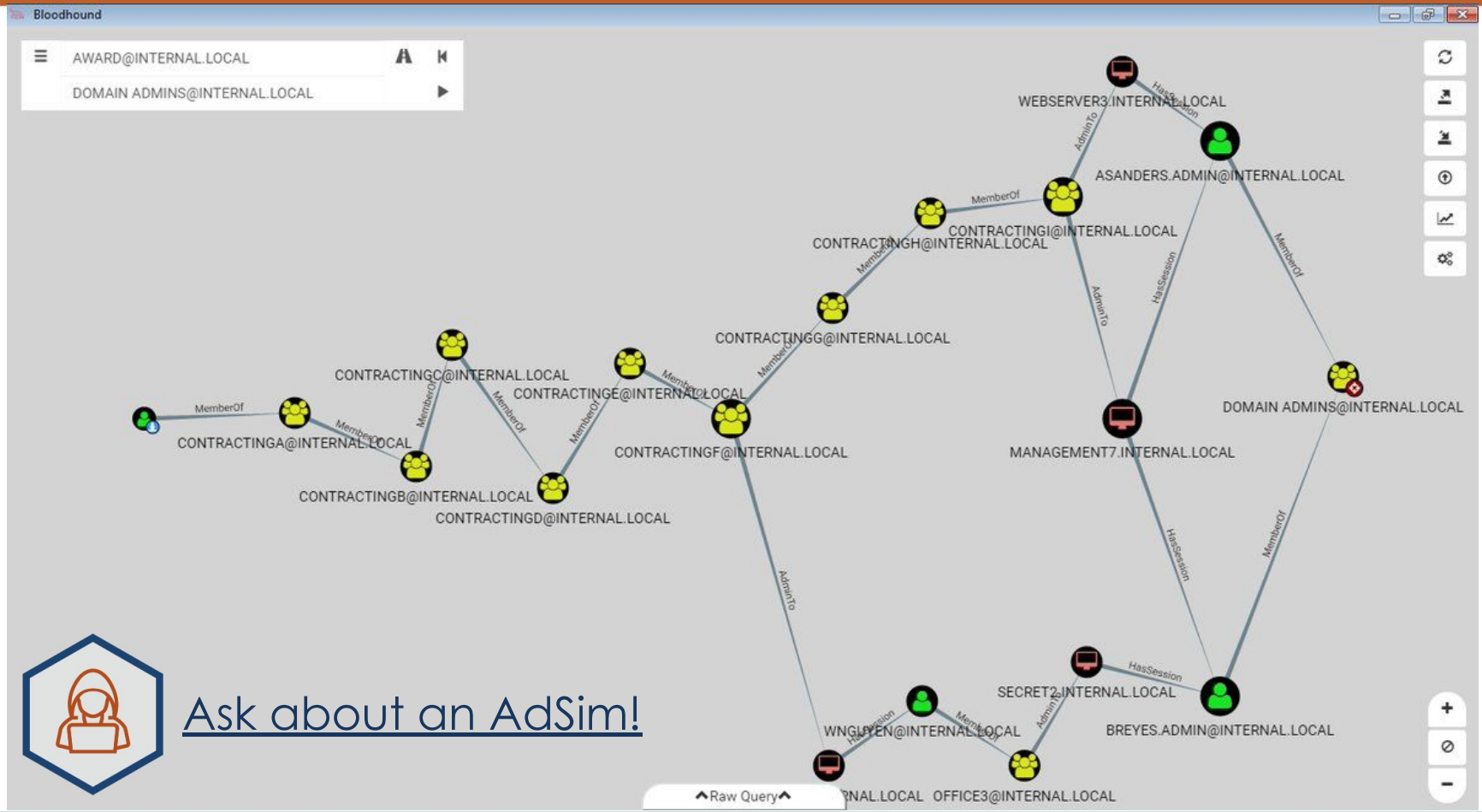
"A local admin can extract from memory the cleartext password of any authenticated user"

SYNERCOMM

BloodHound

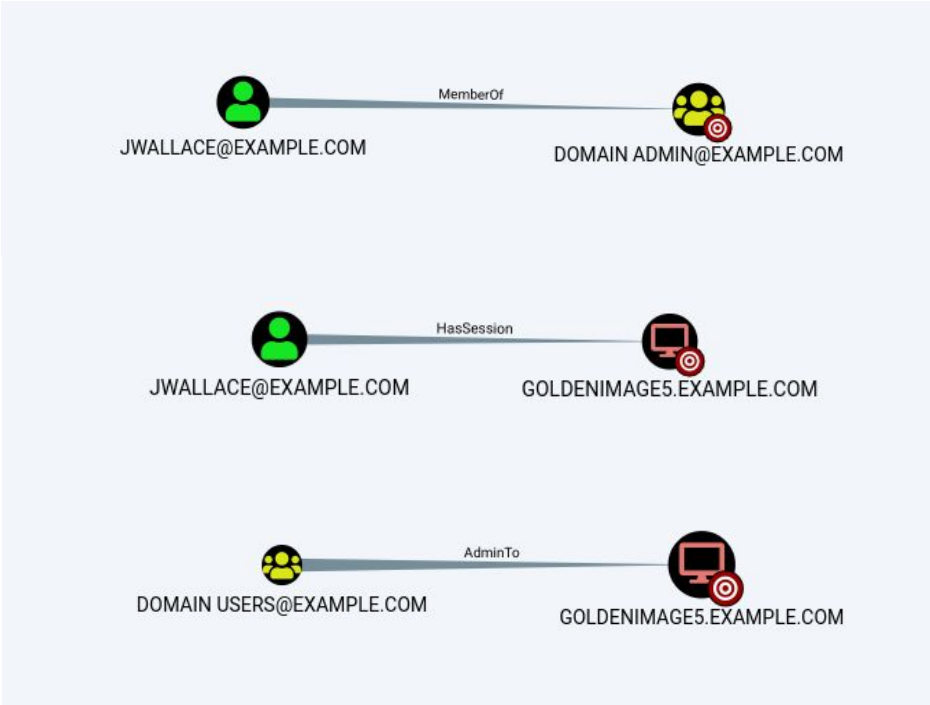
- Available on GitHub @BloodhoundAD
- 10 minute setup
- Queries DC and domain computer for session and admin information
- Creates pretty graphs … of death
- PowerShell & EXE available for information gathering

Adversary Simulation



Ask about an AdSim!

Permissive Global Group Access + MimiKatz

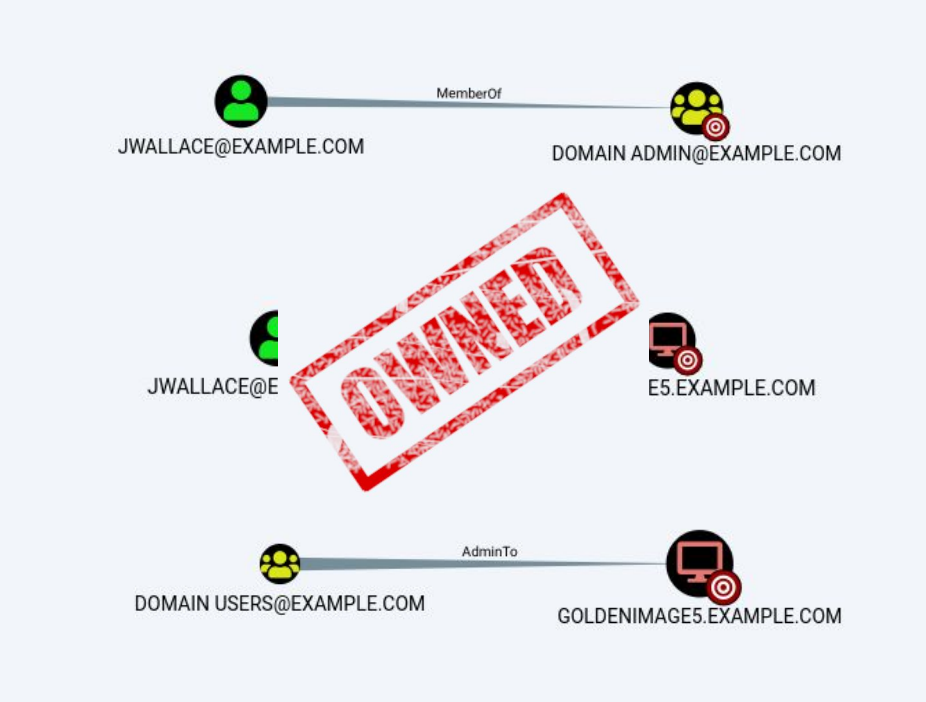


Takeaway:

"A local admin can extract from memory the cleartext password of any authenticated user."

SYNERCOMM

Permissive Global Group Access + MimiKatz



Takeaway:

"A local admin can extract from memory the cleartext password of any authenticated user."

SYNERCOMM

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

Takeaway:

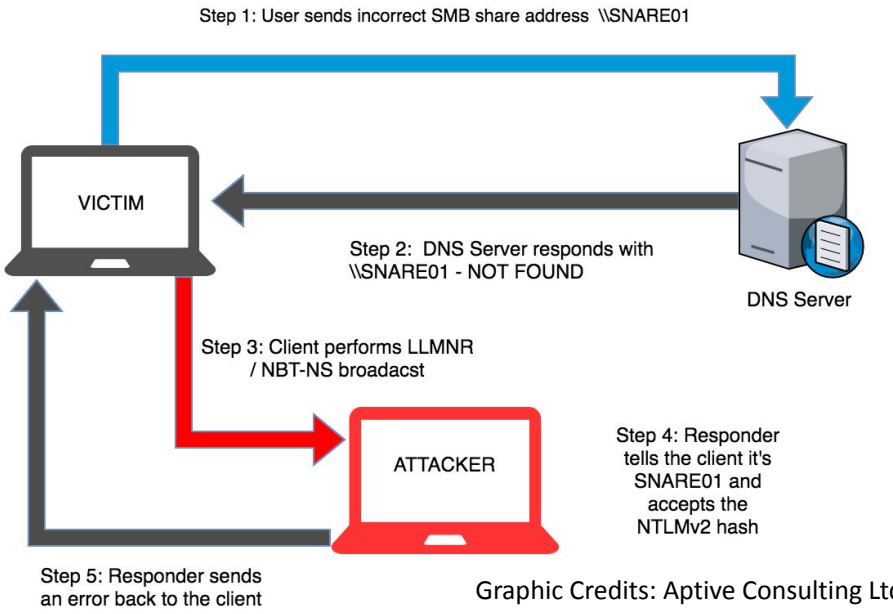
"A local admin can extract from memory the cleartext password of any authenticated user."

SYNERCOMM

LLMNR & NBT-NS POISONING

Solution: Turn them off.

LLMNR & NBT-NS Poisoning



Graphic Credits: Aptive Consulting Ltd.

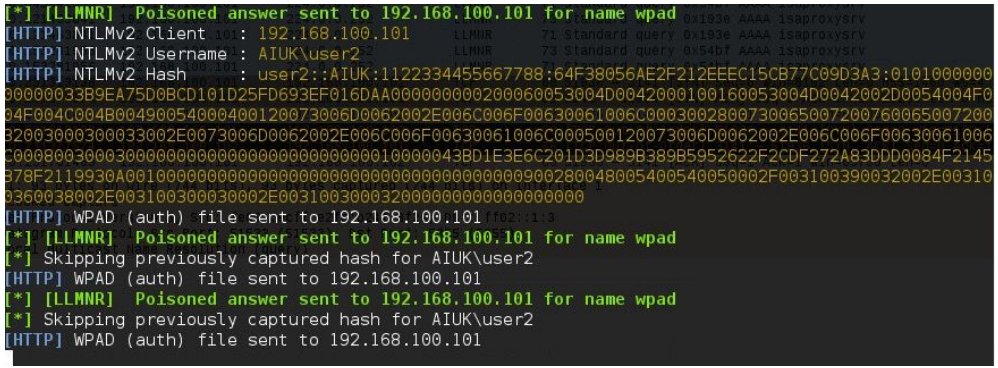
Takeaway:

"Turn off LLMNR.
Turn off NBT-NS.
Monitor for these requests."

SYNERCOMM

LLMNR & NBT-NS Poisoning

Responder.py



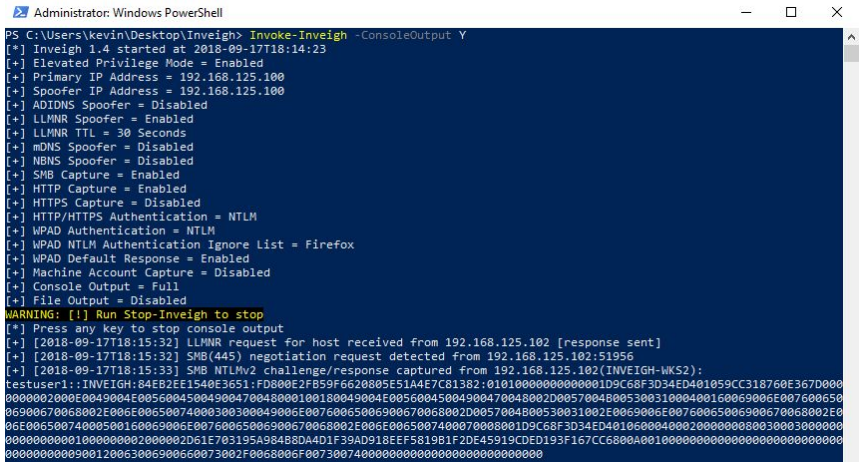
Takeaway:

"Turn off LLMNR.
Turn off NBT-NS.
Monitor for these requests."

SYNERCOMM

LLMNR & NBT-NS Poisoning

Inveigh.ps1



Takeaway:

"Turn off LLMNR.
Turn off NBT-NS.
Monitor for these requests."

SYNERCOMM

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

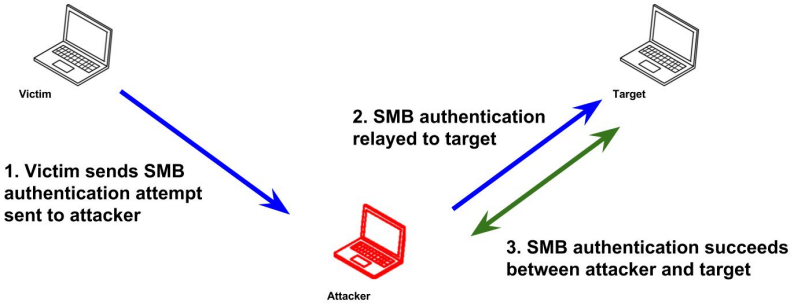
Takeaway:

"Turn off LLMNR.
Turn off NBT-NS.
Monitor for these requests."

SYNERCOMM

LLMNR & NBT-NS Poisoning

Bonus: SMB Relay Attacks



Quick Takeaway:

"Turn on SMB Signing"

SYNERCOMM

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.

```
<?xml version="1.0" encoding="utf-8" ?>
- <Groups clsid="{3125E937-EB16-4b4c-9934-544FC6D24D26}">
  - <User clsid="{DF5F1855-51E5-4d24-8B1A-D9BDE98BA1D1}" name="Administrator (built-in)" image="2" changed="2015-
      02-18 01:53:01" uid="{D5FE7352-81E1-42A2-B7DA-118402BE4C33}">
    <Properties action="U" newName="ADSAdmin" fullName="" description=""
      cpassword="RI133B2Wl2CiI0Cau1DtrtTe3wdFwzCiWB5PSAxXMDstchJt3bL0Uie0BaZ/7rdQjuqTonF3ZWAKa1iRvd4JGQ"
      changeLogon="0" noChange="0" neverExpires="0" acctDisabled="0" subAuthority="RID_ADMIN" userName="Administrator
      (built-in)" expires="2015-02-17" />
    </User>
  </Groups>
```

- 2.2.1.1 Preferences Policy File Format
  - 2.2.1.1.1 Common XML Schema
  - 2.2.1.1.2 Outer and Inner Element Names and CLSIDs
  - 2.2.1.1.3 Common XML Attributes
  - **2.2.1.1.4 Password Encryption**
  - 2.2.1.1.5 Expanding Environment Variables

2.2.1.1.4 Password Encryption

All passwords are encrypted using a derived Advanced Encryption Standard (AES) key.<3>

The 32-byte AES key is as follows:

```
4e 99 06 e8  fc b6 6c c9  fa f4 93 10  62 0f fe e8
f4 96 e8 06  cc 05 79 90  20 9b 09 a4  33 b6 6c 1b
```

Takeaway:

"Apply the patch, delete the XML files, and don't put cleartext passwords in scripts."

SYNERCOMM

SYSVOL Passwords + Leaked AES Keys

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

Changes the local Administrator password. The script should be deployed using Group Policy or through a logon script.

Visual Basic

```
Set oShell = CreateObject("WScript.Shell")
Const SUCCESS = 0

sUser = "administrator"
sPwd = "Password2"

' get the local computername with WScript.Network,
' or set sComputerName to a remote computer
Set oWshNet = CreateObject("WScript.Network")
sComputerName = oWshNet.ComputerName

Set oUser = GetObject("WinNT://" & sComputerName & "/" & sUser)

' Set the password
oUser.SetPassword sPwd
oUser.Setinfo

oShell.LogEvent SUCCESS, "Local Administrator password was changed!"
```

Graphic Credit: https://adsecurity.org

Takeaway:

"Apply the patch, delete the XML files, and don't put cleartext passwords in scripts."

SYNERCOMM

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.

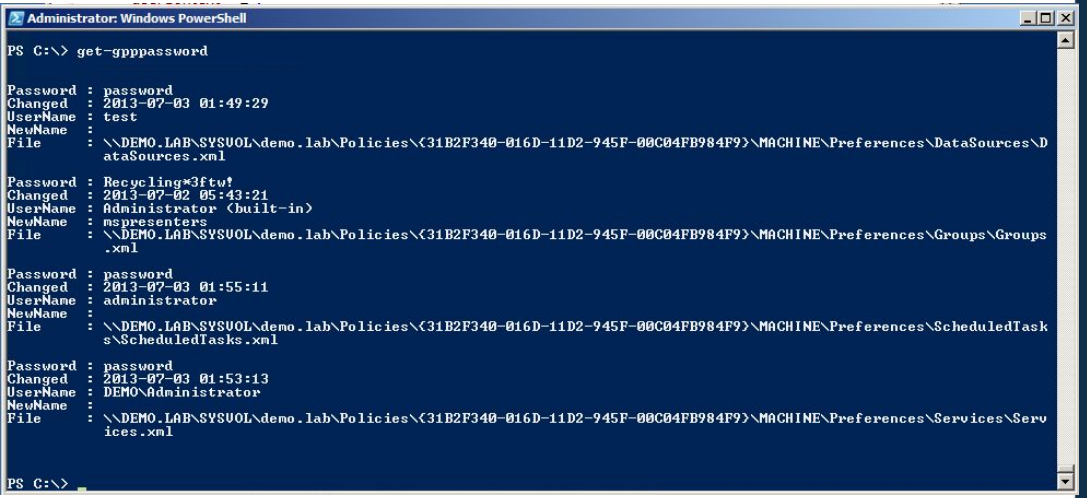
Takeaway:

"Apply the patch, delete the XML files, and don't put cleartext passwords in scripts."

SYNERCOMM

SYSVOL Passwords + Leaked AES Keys

Bonus: Run Get-GPPPassword on yourself!



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

Takeaway:

"Apply the patch, delete the XML files, and don't put cleartext passwords in scripts."

SYNERCOMM

KERBEROASTING

Solution: Long Service Account Passwords

KerberRoasting

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

```
PS C:\Users\administrator\Desktop> Invoke-Kerberoast | fl

SamAccountName       : SQLService
DistinguishedName    : CN=SQLService,CN=Users,DC=testlab,DC=local
ServicePrincipalName : MSSQLSvc/PRIMARY.testlab.local:1433
Hash                 : $krb5tgs$unknown:30FFC786BECD0E88992CBBB017155C53$0
                       343A9C8A7EB90F059CD92B5271414AB510EFE9379DE1BACD220
                       67FE4909DE3D2D860320586DED3EF4DBE25A0D73329E4E47D3F
                       D043D1BD5CCA668243186322934 76A5E741A444F0FA874C8DBF
                       8059850F14929F52DAACFD13BEEA754B27A0B190AC7AB53FC33
                       8F581E8AB76D002DF1E4619920AA4B372219DAE3256BF8D38CB
                       978ACE111ADE5ACB2F1ED9DDC85CC3E8A507E90F57ECE329A9A
                       E18F51C918DF9334BEC79C01C4DD4341BD2E1C1666BB6AAB2F0
                       39046CC4A24B71A6640A4E0C7D8C012F8864079D0844D5869F7
```

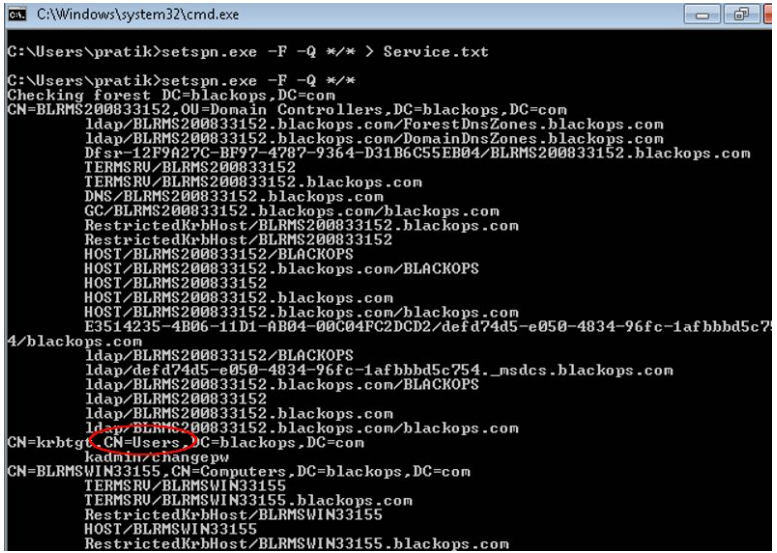
Takeaway:

"Domain accounts used to run services should have long and complex passwords"

SYNERCOMM

KerberRoasting

Audit your network with setspn.exe!



Takeaway:

"Domain accounts used to run services should have long and complex passwords"

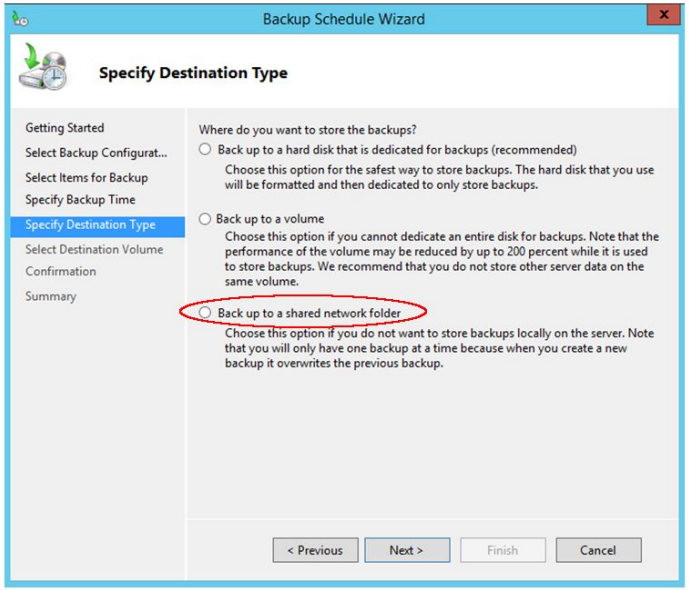
SYNERCOMM

DC BACKUPS

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

DC Backups

User with access to DC backup = Domain Admin



Takeaway:

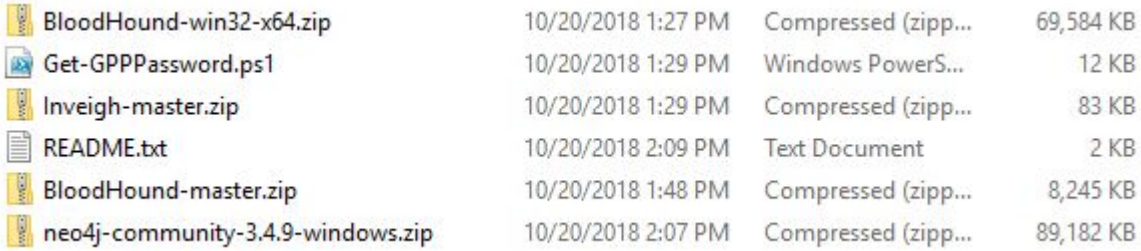
"Only Domain Admins should have access to DC Backups"

SYNERCOMM

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



BloodHound-win32-x64.zip	10/20/2018 1:27 PM	Compressed (zipp...	69,584 KB
Get-GPPPassword.ps1	10/20/2018 1:29 PM	Windows PowerS...	12 KB
Inveigh-master.zip	10/20/2018 1:29 PM	Compressed (zipp...	83 KB
README.txt	10/20/2018 2:09 PM	Text Document	2 KB
BloodHound-master.zip	10/20/2018 1:48 PM	Compressed (zipp...	8,245 KB
neo4j-community-3.4.9-windows.zip	10/20/2018 2:07 PM	Compressed (zipp...	89,182 KB

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

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

Questions?