

Sample Data

Issue Uncovered: Inactive users

Client Risk: Security / Unauthorized Access

1. Assessment Summary

| Domain | |
|--------------------------------|----|
| Domain Controllers | 2 |
| Number of Organizational Units | 10 |
| Users | |
| # Enabled | 36 |
| Last Login within 30 days | 16 |
| Last Login older than 30 days | 20 |
| # Disabled | 3 |
| Last Login within 30 days | 0 |
| Last Login older than 30 days | 3 |
| Security Group | |
| Groups with Users | 46 |
| # Total Groups | 46 |

Issue Uncovered: Some computers not logged-in

Client Risk: Poor maintenance / Potential for undetected theft

| # Total Groups | 48 |
|-------------------------------|----|
| Computers in Domain | |
| Total Computers | 65 |
| Last Login within 30 days | 42 |
| Last Login older than 30 days | 23 |
| Other | 3 |

Issue Uncovered: Misalignment of IT asset organization

Client Risk: Potential for unauthorized access

2.3 Organizational Units

Active Directory is organized into basic organizational units.

- MYCO.com
 - Builtin (17 Security Groups)
 - Computers (33 Computers)
 - Domain Controllers (2 Computers)
 - ForeignSecurityPrincipals
 - Microsoft Exchange Security Groups (6 Security Groups)
 - MYCO_Users
 - Servers (19 Computers)
 - Service Accounts (1 Users)
 - Test OU (1 Computers)
 - Users (5 Contacts, 22 Security Groups, 38 Users)


Issue Uncovered: Second domain controller issue

Client Risk: Single Point of failure

2.1 Domain Controllers

There are 2 domain controllers:

| Domain Controller | Status |
|-------------------|---------|
| dc01.MYCO.com | online |
| dc02.MYCO.com | offline |



2.2 FSMO Roles

There are a set of roles needed to operate a Windows domain. These roles are called Flexible Single Master Operation (FSMO, pronounced "Fiz-mo") roles.


| Role | Domain Controller | Best Practice |
|--------------------------|-------------------|----------------|
| Schema Master | dc01.MYCO.com | ForestWide |
| Domain Naming Master | dc01.MYCO.com | ForestWide |
| PDC Emulator | dc01.MYCO.com | DomainSpecific |
| Relative ID (RID) Master | dc01.MYCO.com | DomainSpecific |
| Infrastructure Master | dc01.MYCO.com | DomainSpecific |

Issue Uncovered: Inappropriate user access

Client Risk: Security breach

2.6 Security Groups

| Group | Members |
|---|--|
| Account Operators (MYCO.com/Builtin/Account Operators) | |
| Administrators (MYCO.com/Builtin/Administrators) | David SMITH, Sam Phillips, Todd Lamons, KATHY Young, Chris Irving, Deonne William, Michelle Michels, THOMAS Linn, Steve Barlow, Brian Pierson, Keith Morris, Matthew Wendell, Pablo SANDERS, Domain Admins, Enterprise Admins, Administrator |
| Backup Operators (MYCO.com/Builtin/Backup Operators) | |



Issue Uncovered: Weak / Insecure passwords

Client Risk: Security breach

6. System Password Strength Assessment

IP Range for MBSA scan: 10.0.1.0-10.0.1.255

| Computer | IP | Assessment |
|--------------------|------------|-----------------|
| MYCO\DC01 | 10.0.1.3 | Strong Security |
| MYCO\DEVWIKI | 10.0.1.12 | Strong Security |
| MYCO\MEGATRON | 10.0.1.4 | Strong Security |
| MYCO\SHAREPOINT1 | 10.0.1.9 | Strong Security |
| MYCO\ISA1 | 10.0.1.6 | Strong Security |
| MYCO\PEACH | 10.0.1.34 | Severe Risk |
| MYCO\MYCO-ATL-CORE | 10.0.1.17 | Strong Security |
| MYCO\PABUILD | 10.0.1.35 | Strong Security |
| MYCO\SERVERS | 10.0.1.21 | Potential Risk |
| MYCO\REMOTE | 10.0.1.13 | Potential Risk |
| MYCO\HYPERV | 10.0.1.88 | Strong Security |
| MYCO\THRASH2 | 10.0.1.33 | Potential Risk |
| MYCO\ENGINEERS | 10.0.1.50 | Potential Risk |
| MYCO\DIALTONE | 10.0.1.111 | Strong Security |
| MYCO\MAINVML-DTXP | 10.0.1.132 | Severe Risk |
| MYCO\DESKTOPWORK | 10.0.1.125 | Severe Risk |
| MYCO\ERPPATCH | 10.0.1.128 | Strong Security |

Issue Uncovered: Insecure Protocols In Use

Client Risk: Security

7. Listening Ports

| Computer | FTP 21/TCP | SSH 22/TCP | Telnet 23/TCP | SMTP 25/TCP | DNS 53/TCP | HTTP 80/TCP | SQLServer 1433/TCP | MySQL 3306/TCP | RDP 3389/TCP | VNC 5900/TCP |
|---------------|---------------|---------------|------------------|----------------|---------------|----------------|-----------------------|-------------------|-----------------|-----------------|
| 10.0.1.1 | | | | | | | | | | |
| DC01 | | | | | ✓ | ✓ | | | ✓ | |
| MEGATRON | | | | | | | | | ✓ | |
| ISA1 | | | ✓ | | | ✓ | | | ✓ | |
| SHAREPOINT1 | | | | | | ✓ | ✓ | | ✓ | |
| DEVWIKI | | | | | | ✓ | | ✓ | ✓ | |
| REMOTE | | | | ✓ | ✓ | | ✓ | | ✓ | |
| MYCO-ATL-CORE | | | | | | ✓ | ✓ | | ✓ | |
| 10.0.1.20 | | ✓ | | | | ✓ | | | | |
| SERVERS | | | | ✓ | | ✓ | ✓ | | ✓ | |
| 10.0.1.25 | ✓ | | ✓ | | | ✓ | | | | |
| 10.0.1.26 | ✓ | | ✓ | ✓ | | ✓ | | | | |