Active Directory Security Audit

for Acme Co

BlackBox Auditor

January 15, 2019

BlackBox Auditor

Executive Summary

Domain Evaluated: Acme-Corp

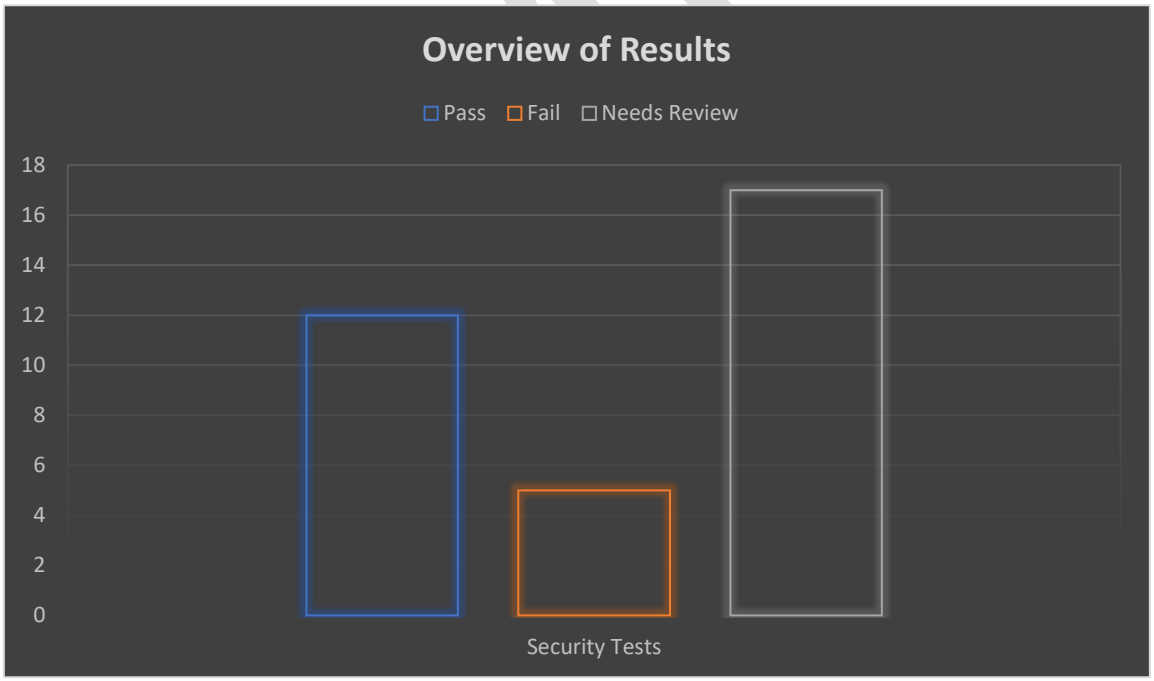
Primary Domain Controller Evaluated: DC1.acme-corp.net

Date Ran: January 15, 2019

Number of Domain Controllers: 5

Domain User Summary		Security Summary	
Total User Accounts	352	**Password Not Required**	2
Enabled	301	**Password Does Not Expire (Enabled)**	11
Disabled	51		
Locked	8		

The results of our active directory security audit resulted in the following



BlackBox Auditor

Summary Results of Testing

Security Tests	Result
1. NTLM Challenge/Response Setting (Password Transmission Encryption)	Pass
2. Allow Blank Passwords	Needs Review
3. Storing Passwords with Strong Encryption	Pass
4. Encryption of RDP Sessions (Admin Sessions)	FAIL
5. NTP Time Set	Pass
6. Permissions to Change Time Settings	Pass
7. Minimum Password Length	Pass
8. Maximum Password Age	Pass
9. Account Lockout Threshold	Pass
10. Account Lockout Reset Time	Pass
11. Password History Setting	Pass
12. LAPS in use	FAIL
13. Use of out of date operating systems	Pass
14. Fine Grained Password Policies	Needs Review
15. Use of Group Policy Passwords	FAIL
16. Windows XP Systems in Use	FAIL
17. Windows 2003 Systems in use	Pass
18. Windows 2000 Systems in use	Pass
19. SMB Signing Enabled	Pass
20. Check if UAC is enabled on Domain Controller	Pass
21. Default Local Administrator Account is Renamed	Fail
22. Local Administrator Account is disabled	Pass
23. Guest Account is disabled	Pass

Active Directory Reporting	Result
24. Listing of all Domain Admins	Needs Review
25. Listing of all Enterprise Admins	Needs Review
26. Listing of all DNSAdmins	Needs Review
27. Listing of all Account Operators	Needs Review
28. Listing of all Local Administrators	Needs Review
29. Listing of all Users Who Can Add New Users	Needs Review
30. Domain Trust Relationships	Needs Review
31. List Applied Group Policies to Domain Controller	Needs Review
32. List of Active Accounts that the password never expires	Needs Review
33. List of Active Accounts that the password is older than 180 Days	Needs Review
34. List of Active Accounts that have never been logged into	Needs Review

SAMPLE

35. List of Active Accounts that were created in the last 7 Days	**Needs Review**
36. List of All User Accounts (with details)	**Needs Review**
37. List of the high-level domain organization structure	**Needs Review**
38. List of Domain Audit Logging Settings	**Needs Review**
39. List of All Domain Groups	**Needs Review**
40. Check for Separate Admin Accounts for Domain Admins	**Needs Review**

SAMPLE

BlackBox Auditor

ACME-CORP – Detailed Results

NTLM CHALLENGE/RESPONSE SETTING | PASS

(PASSWORDS IN TRANSIT)

Overview of Test

Testing for strong encryption of passwords in transit. Microsoft has several configurable settings for how it transmits password data (hashes) over the network. Only the strongest setting (Send NTLMv2 response only/refuse LM & NTLM) should be considered secure.

Results

Active Directory Auditor evaluated the settings on the ***ACME-CORP*** Domain and determined via system generated data that the Domain Controller was configured with the following setting:

- Send NTLMv2 response only/refuse LM & NTLM

System Generated Evidence:

HKLM\System\CurrentControlSet\Control\Lsa\LmCompatibilityLevel
Lmcompatibilitylevel REG_DWORD 0x5

Remediation

None Needed

Supporting Details

Microsoft LAN Manager Authentication

SAMPLE

BlackBox Auditor

ALLOW BLANK PASSWORD | NEEDS REVIEW

Overview of Test

Windows systems can be configured to allow for the use of blank passwords on a per account basis. A check of all domain user accounts was conducted to check for this setting.

Results

Active Directory Auditor evaluated the settings on the ***ACME-CORP*** Domain and determined via system generated data that the Domain Controller **does** have user accounts that CAN have a blank password. It also means that the user could have a password shorter than the default domain password policy. It should be noted that this does not necessarily mean that the account actually has no password or shorter passwords. An export of all accounts with this setting has been provided for further review.

Remediation

After careful review, we recommend that the "Password Not Required" Setting be changed.

Supporting Details

Understanding and Remediating "PASSWD_NOTREQD"

SAMPLE

BlackBox Auditor

STORING PASSWORDS WITH STRONG ENCRYPTION | PASS

Overview of Test

Windows systems can be configured to allow for the storage of Active Directory Domain password hashes using legacy (insecure) or more modern security. This test determines if the domain stores passwords using the legacy and insecure LM Hash value. The default value for modern Windows systems is to not store passwords using LM hashes.

Results

Active Directory Auditor evaluated the settings on the ***ACME-CORP*** Domain and determined via system generated data that the Domain Controller does not store passwords using legacy insecure methods (LM Hashes). The following setting was observed:

- Do Not Store LAN Manager Hash value on next password change.

System Generated Evidence:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa
NoLmHash REG_DWORD  0x1
```

Remediation

None Needed

Supporting Details

N/A

SAMPLE

BlackBox Auditor

ENCRYPTION OF RDP (REMOTE ADMIN) SESSIONS | FAIL

Overview of Test

Windows systems can be configured to allow for various levels of encryption when using Remote Desktop Protocol (RDP). This test will check the setting on the tested domain controller. By default, Windows systems do not enforce the strongest level encryption and instead allow for the downgrading of encryption strength if the connecting system does not support strong encryption.

Results

Active Directory Auditor evaluated the settings on the tested ***ACME-CORP*** domain controller and determined via system generated data that the Domain Controller does not enforce strong encryption. The following setting was observed:

- Encryption Level: **Client Compatible**

What does this mean? The Domain Controller will accept the encryption level negotiated by the client, including using weak encryption.

System Generated Evidence:

```
HKLM\SYSTEM\CurrentControlSet\Control\TerminalServer\WinStations\RDP-Tcp
MinEncryptionLevel REG_DWORD  0x2
```

Remediation

After careful review, we recommend that the RDP encryption level setting be changed to at least "High"

Supporting Details

RDP Network Encryption Levels

SAMPLE