



Microsoft

Active Directory

Active Directory User Account Lockout Email Alert

Güvenlik açısından active directory kullanıcı hesaplarına lockout policy uygulamak gerekiyor. En azından bence yapılmalı. Group Policy Editore gelip ilgili policyi aşağıdaki gibi düzenleyip tüm domaine uyguluyorum.

Computer Configuration → Windows Settings → Security Settings → Account Policies tıklayıp kendi ortamınıza göre policyi düzenleyebilirsiniz.

Group Policy Management Editor

File Action View Help

Computer Configuration

- Policies
- Software Settings
- Windows Settings
 - Name Resolution Policy
 - Scripts (Startup/Shutdown)
 - Security Settings
 - Account Policies
 - Account Lockout Policy

Policy	Policy Setting
Account lockout duration	30 minutes
Account lockout threshold	3 invalid logon attempts
Allow Administrator account lockout	Not Defined
Reset account lockout counter after	30 minutes

Buraya kadar her şey normal ancak bir hesap kilitletiğinde event viewer haricinde de bir uyarı almakta fayda var.

Bunun için aşağıdaki gibi bir powershell scripti mevcut. Dosyayı istediğimiz bir isimde kaydedip çalışmasını istediğimiz dizinin altına kopyalayamamız gerekiyor. Ben **AccountLocked.ps1** adını verip direkt olarak **Domain Controller**da C dizini altına kopyaladım.

AccountLocked.ps1 X

```
1 $AccountLockOutEvent = Get-EventLog -LogName "Security" -InstanceId 4740 -Newest 1
2 $LockedAccount = $($AccountLockOutEvent.ReplacementStrings[0])
3 $AccountLockedAt = $($AccountLockOutEvent.ReplacementStrings[1])
4 $AccountLockOutEventTime = $AccountLockOutEvent.TimeGenerated
5 $AccountLockOutEventMessage = $AccountLockOutEvent.Message
6
7 $From = " "
8 $To = " "
9 $SMTPServer = "smtp-mail.outlook.com"
10 $SMTPPort = "587"
11
12 $Username = " "
13 $Password = " "
14
15 $subject = "Kullanici Hesabi Kilitlendi: $LockedAccount"
16 $body = "$AccountLockOutEventTime tarihinde $LockedAccount kullanicisinin hesabi kilitlendi.`n`nOlay Detayl:`n`n$AccountLockOutEventMessage"
17
18 $smtp = New-Object System.Net.Mail.SmtpClient($SMTPServer, $SMTPPort);
19
20 $smtp.EnableSSL = $true
21 $smtp.Credentials = New-Object System.Net.NetworkCredential($Username, $Password);
22 $smtp.Send($From, $To, $subject, $body);
```

Script hesap kilitlenmesi sonucu oluřan 4740 event id sini takip ederek alert mail g nderilmesini saęlıyor.

Kırmızı alanları kendi bilgileriniz ile doldurabilirsiniz.

```
$AccountLockOutEvent = Get-EventLog -LogName "Security" -InstanceId 4740 -Newest 1
$LockedAccount = $($AccountLockOutEvent.ReplacementStrings[0])
$AccountLockedAt = $($AccountLockOutEvent.ReplacementStrings[1])
$AccountLockOutEventTime = $AccountLockOutEvent.TimeGenerated
$AccountLockOutEventMessage = $AccountLockOutEvent.Message
```

```
$From = "mail@domain.com"
$To = "mail@domain.com,mail@domain.com"
$SMTPServer = "mail.domain.com"
$SMTPPort = "Smtp Port"
```

```
$Username = "mail@domain.com"
$Password = "mailpass"
```

```
$subject = "Kullanıcı Hesabı Kilitlendi: $LockedAccount"
$body = "$AccountLockOutEventTime tarihinde $LockedAccount kullanıcı hesabı kilitlendi.`n`nOlay
Detayl:`n`n$AccountLockOutEventMessage"
```

```
$smtp = New-Object System.Net.Mail.SmtpClient($SMTPServer, $SMTPPort);
```

```
$smtp.EnableSSL = $true
$smtp.Credentials = New-Object System.Net.NetworkCredential($Username, $Password);
$smtp.Send($From, $To, $subject, $body);
```

Sonraki işlem için yine **Domain Controller** da **Task Scheduler** çalıştırıyorum ve Yeni bir task oluşturuyorum. **General** sekmesinde aşağıdaki gibi isim veriyorum. Hangi yetkili kullanıcı ile çalıştıracağımı seçiyorum. Ardından oturum açık olsada olmasada çalışmasını sağlamak için “**Run whether user is logged on or not**” işaretliyorum. OK ile kaydediyorum.

Create Task

General Triggers Actions Conditions Settings

Name: AccountLockedOut

Location: \Microsoft\Windows

Author: KANSAN\prosistem

Description:

Security options

When running the task, use the following user account:

Run only when user is logged on

Run whether user is logged on or not

Do not store password. The task will only have access to local computer resources.

Run with highest privileges

Hidden

Configure for: Windows Vista™, Windows Server™ 2008

OK Cancel

Trigger sekmesine gelip **New Trigger** tıklıyorum. Ve aşağıdaki gibi **Begin the Task : On an event** seçiyorum. Log olarak **Security**, Event ID olarak **4740** belirliyorum. OK diyerek kaydediyorum.

New Trigger

Begin the task: On an event

Settings

Basic

Custom

Log: Security

Source: Security

Event ID: 4740

Advanced settings

Delay task for: 15 minutes

Repeat task every: 1 hour for a duration of: 1 day

Stop all running tasks duration

Stop task if it runs longer than: 3 days

Activate: 5.07.2024 13:57:23 Synchronize across time zones

Expire: 5.07.2025 13:57:23 Synchronize across time zones

Enabled

OK Cancel

Ardından **Action** sekmesine gelip **New Action** tıklıyorum. **Action : Start a program** seçiyorum. Program script olarak powershell.exe dosyasının yolunu gösteriyorum. **"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe"** Add argument olarak çalıştıracığım powershell dosyasının yolunu gösteriyorum. **"-file "C:\AccountLocked.ps1"** Ok ile kaydediyorum.

New Action

You must specify what action this task will perform.

Action: Start a program

Settings

Program/script: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe

Add arguments (optional): -file "C:\AccountLocked.ps1"

Start in (optional):

OK Cancel

Tekrar OK ile kaydediyorum. Görevim hazır hale geldi.

Name	Status	Triggers
AccountLockedOut	Running	On event - Log: Security, Event ID: 4740
Server Initial Configuration task	Disabled	At system startup

Şimdi test için oluşturduğum kullanıcı ile bir paylaşımaya ulaşmaya çalışacağım.

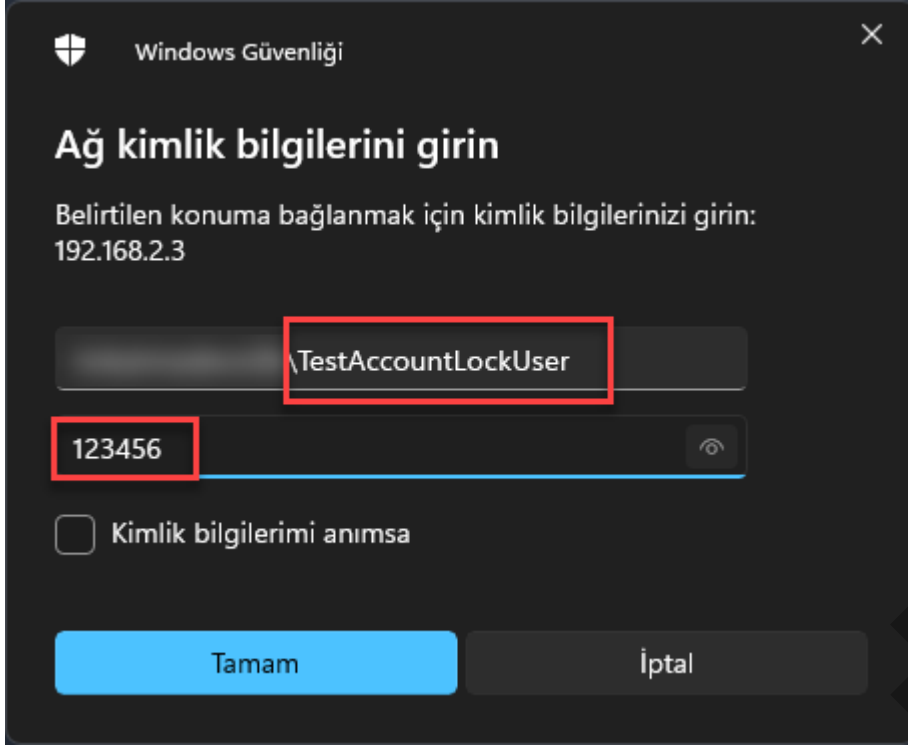
Çalıştır

Bir program, klasör, belge veya Internet kaynağının adını yazdığınızda Windows sizin için açacaktır.

Aç: \\192.168.2.3\c\$

Tamam İptal Gözet...

Aslında şifre farklı ancak bilerek 3 defa 123456 giriyorum.



Windows Güvenliđi

Ađ kimlik bilgilerini girin

Belirtilen konuma bağlanmak için kimlik bilgilerinizi girin:
192.168.2.3

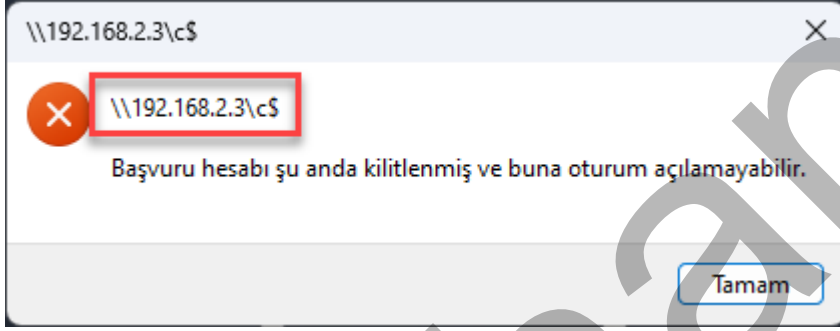
Username: \\TestAccountLockUser

Password: 123456

☐ Kimlik bilgilerimi anımsa

Tamam İptal

Aşağıdaki gibi uyarı aldım ve hesabımı kilitledim.



\\192.168.2.3\c\$


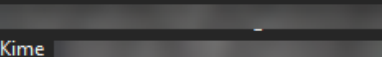
\\192.168.2.3\c\$


Başvuru hesabı şu anda kilitlenmiş ve buna oturum açılmayabilir.

Tamam

Alert Mailide geldi. Kullanıcı adı, tarih ve hangi pc üzerinden işlem yapıldığına dair bilgiler mevcut.

Kullanıcı Hesabi Kilitlendi: TestAccountLockUser

 Kime 


 İletiyi şu dile çevir: Türkçe | Şu dili hiçbir zaman çevirme: İngilizce | Çeviri tercihleri

07/05/2024 15:19:15 tarihinde TestAccountLockUser kullanıcı hesabı kilitlendi.

Olay Detayı:

A user account was locked out.

Subject:

Security ID: S-1-5-18
Account Name: -DC\$
Account Domain: 
Logon ID: 0x3e7

Account That Was Locked Out:

Security ID: S-1-5-21-401791782-913235239-411392593-2127
Account Name: TestAccountLockUser

Additional Information:

Caller Computer Name: GOKHAN-NB

Event Viewer üzerinden baktığımızda da aşağıdaki gibi olay bilgisi mevcut.

Security Number of events: 231,273 (0) New events available

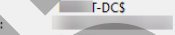
Keywords	Date and Time	Source	Event ID	Task Category
Audit Success	5.07.2024 15:19:15	Microsoft Windows security auditing.	4740	User Account Management
Audit Failure	5.07.2024 15:19:15	Microsoft Windows security auditing.	4625	Logon
Audit Success	5.07.2024 15:19:15	Microsoft Windows security auditing.	4776	Credential Validation
Audit Success	5.07.2024 15:19:15	Microsoft Windows security auditing.	4776	Credential Validation
Audit Failure	5.07.2024 15:19:14	Microsoft Windows security auditing.	4625	Logon
Audit Success	5.07.2024 15:19:11	Microsoft Windows security auditing.	4776	Credential Validation
Audit Success	5.07.2024 15:19:11	Microsoft Windows security auditing.	4776	Credential Validation
Audit Success	5.07.2024 15:19:10	Microsoft Windows security auditing.	4634	Logoff
Audit Success	5.07.2024 15:19:09	Microsoft Windows security auditing.	4624	Logon
Audit Success	5.07.2024 15:19:09	Microsoft Windows security auditing.	4672	Special Logon

Event 4740, Microsoft Windows security auditing.

General Details

A user account was locked out.

Subject:

Security ID: SYSTEM
Account Name: T-DC\$
Account Domain: 
Logon ID: 0x3E7

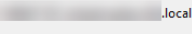
Account That Was Locked Out:

Security ID: S-1-5-21-401791782-913235239-411392593-2127
Account Name: TestAccountLockUser

Additional Information:

Caller Computer Name: GOKHAN-NB

Log Name: Security
Source: Microsoft Windows security
Event ID: **4740**
Level: Information
User: N/A
OpCode: Info
More Information: [Event Log Online Help](#)

Logged: 5.07.2024 15:19:15
Task Category: User Account Management
Keywords: Audit Success
Computer: .local