

# Log Analiz Raporu

**Okan UZUN**

**22.09.2025**

## Table of Contents

Giriş.....	2
Alarmlar .....	3
A Member Was Added To A Security-enabled Global Group .....	3
Logon aşaması .....	3
Privilage Escalation .....	4
Path Travel Detected .....	11
Web izin sorgusu .....	11
Passwd sorgusu .....	13

Dirbuster.....	14
Root Authentication Failed.....	14
MITRE ATT&CK Analizi.....	15
Sonuç-Öneri.....	16
Kaynakça.....	17

## Giriş

Bu raporda, Graylog üzerinde tespit edilen üç güvenlik alarımının oluşum süreçleri incelenmiştir. İnceleme kapsamında **“A member was added to a security-enabled global group”**, **“Path Travel Detected”** ve **“Root Authentication Failed”** alarmlarının nasıl oluştuğu analiz edilerek ortaya konulmuştur.

## A Member Was Added To A Security-enabled Global Group

İncelenen zaman diliminde ilk tespit edilen kritik olay, Event ID 4625(Unknown user name or bad password) Başarısız giriş deneme kaydıdır. Bu kayıt Graylog üzerinde **“09.08.2025 16:44:30”** zaman damgasına denk gelirken Windows event logunda **“08.09.25 15:42:52”** zamanına denk gelmektedir.



Daha sonra kullanıcı, **philomela**, hesabı **“09.09.25 11:31:42”** zaman damgasında oluşturulmuştur(Event ID 4720). Oluşturulan hesap üzerinde parola reset girişi yapılmış(Event ID 4724). Daha sonra hesap üzerinde değişiklik yapılmış(Event ID 4738) ancak **“Changed Attributes”** alanı boş görülmektedir. Kritik değişiklik logda gözlemlenmemiştir.

```

All Messages

timestamp source

2025-09-09 11:31:43.111 127.0.0.1
["Keywords": "Audit Success", "Date and Time": "8.09.2025 15:41:17", "Source": "Microsoft-Windows-Security-Auditing", "Event ID": "4728", "Task Category": "User Account Management", "Subject": "", "Security ID": "REFORM\\philomela", "Account Name": "philomela", "Account Domain": "REFORM", "Logon ID": "b6d052", "New Account": "", "Attributes": "", "SAM Account Name": "philomela", "Display Name": "philomela", "User Principal Name": "philomela@reform.local", "Home Directory": "", "Home Drive": "", "Script Path": "", "Profile Path": "", "User Workstations": "", "Password Last Set": "8.09.2025 15:41:17", "Account Expires": "Never", "Primary Group ID": "513", "AllowedToDelegateTo": "", "Old UAC Value": "No", "New UAC Value": "Yes", "User Account Control": "", "User Parameters": "", "SID History": "", "Logon Hours": "", "Additional Information": "", "Privileges": "" ]

2025-09-09 11:31:43.111 127.0.0.1
["Keywords": "Audit Success", "Date and Time": "8.09.2025 15:41:17", "Source": "Microsoft-Windows-Security-Auditing", "Event ID": "4738", "Task Category": "User Account Management", "Subject": "", "Security ID": "REFORM\\philomela", "Account Name": "philomela", "Account Domain": "REFORM", "Logon ID": "b6c360", "Target Account": "", "Changed Attributes": "", "SAM Account Name": "", "Display Name": "", "User Principal Name": "", "Home Directory": "", "Home Drive": "", "Script Path": "", "Profile Path": "", "User Workstations": "", "Password Last Set": "", "Account Expires": "", "Primary Group ID": "", "AllowedToDelegateTo": "", "Old UAC Value": "", "New UAC Value": "", "User Account Control": "", "User Parameters": "", "SID History": "", "Logon Hours": "", "Additional Information": "", "Privileges": "" ]

2025-09-09 11:31:43.111 127.0.0.1
["Keywords": "Audit Success", "Date and Time": "8.09.2025 15:41:17", "Source": "Microsoft-Windows-Security-Auditing", "Event ID": "4724", "Task Category": "User Account Management", "Subject": "", "Security ID": "REFORM\\philomela", "Account Name": "philomela", "Account Domain": "REFORM", "Logon ID": "b62a818", "Target Account": "" ]

2025-09-09 11:31:43.111 127.0.0.1
["Keywords": "Audit Success", "Date and Time": "8.09.2025 15:41:17", "Source": "Microsoft-Windows-Security-Auditing", "Event ID": "4738", "Task Category": "User Account Management", "Subject": "", "Security ID": "REFORM\\philomela", "Account Name": "philomela", "Account Domain": "REFORM", "Logon ID": "b6d052", "Target Account": "", "Changed Attributes": "", "SAM Account Name": "", "Display Name": "", "User Principal Name": "", "Home Directory": "", "Home Drive": "", "Script Path": "", "Profile Path": "", "User Workstations": "", "Password Last Set": "", "Account Expires": "", "Primary Group ID": "", "AllowedToDelegateTo": "", "Old UAC Value": "No", "New UAC Value": "Yes", "User Account Control": "", "User Parameters": "", "SID History": "", "Logon Hours": "", "Additional Information": "", "Privileges": "" ]

2025-09-09 11:31:43.111 127.0.0.1
["Keywords": "Audit Success", "Date and Time": "8.09.2025 15:41:17", "Source": "Microsoft-Windows-Security-Auditing", "Event ID": "4738", "Task Category": "User Account Management", "Subject": "", "Security ID": "REFORM\\philomela", "Account Name": "philomela", "Account Domain": "REFORM", "Logon ID": "b6d052", "Target Account": "", "Changed Attributes": "", "SAM Account Name": "", "Display Name": "", "User Principal Name": "", "Home Directory": "", "Home Drive": "", "Script Path": "", "Profile Path": "", "User Workstations": "", "Password Last Set": "", "Account Expires": "", "Primary Group ID": "", "AllowedToDelegateTo": "", "Old UAC Value": "No", "New UAC Value": "Yes", "User Account Control": "", "User Parameters": "", "SID History": "", "Logon Hours": "", "Additional Information": "", "Privileges": "" ]

```

## Account oluşturulmuş

Bu noktada ise **“09.08.2025 15:42:07”** zaman damgasında **philomela** kullanıcısı ile başarılı bir oturum açma gerçekleşmiştir (Event ID 4624). Logon Type:3 olması sisteme ağ üzerinden erişildiği göstermektedir. Uzak masaüstü bağlantısı olan RDP protokolüyle bağlanmış olabileceğini gösterir. Oturum açma işleminde ise svchost.exe çalışmıştır. Svchost.exe bu windows içindeki hizmet işlemleri düzenleyen bir .

```

All Messages

timestamp source

2025-09-09 11:31:43.091 127.0.0.1
["Keywords": "Audit Success", "Date and Time": "8.09.2025 15:42:04", "Source": "Microsoft-Windows-Security-Auditing", "Event ID": "4624", "Task Category": "Logon", "Subject": "", "Security ID": "REFORM\\philomela", "Account Name": "philomela", "Account Domain": "REFORM", "Logon ID": "b6288023", "Logon Information": "", "Logon Type": "3", "Restricted Admin Mode": "", "Virtual Account": "No", "Elevated Token": "Yes", "Impersonation Level": "Impersonation", "New Logon": "", "Linked Logon ID": "b628803f", "Network Account Name": "", "Network Account Domain": "", "Logon GUID": "{D346C6F6-BFBC-8EDF-BA77-0B0C6889A8A4}", "Process Information": "", "Process ID": "b6fc", "Process Name": "C:\\Windows\\System32\\svchost.exe", "Network Information": "", "Workstation Name": "DCB1", "Source Network Address": "127.0.0.1", "Source Port": "0", "Detailed Authentication Information": "", "Logon Process": "User32", "Authentication Package": "Negotiate", "Transited Services": "", "Package Name (NTLM only)": "", "Key Length": "0" ]

2025-09-09 11:31:43.091 127.0.0.1
["Keywords": "Audit Success", "Date and Time": "8.09.2025 15:42:04", "Source": "Microsoft-Windows-Security-Auditing", "Event ID": "4624", "Task Category": "Logon", "Subject": "", "Security ID": "REFORM\\philomela", "Account Name": "philomela", "Account Domain": "REFORM", "Logon ID": "b628803f", "Logon Information": "", "Logon Type": "3", "Restricted Admin Mode": "", "Virtual Account": "No", "Elevated Token": "No", "Impersonation Level": "Impersonation", "New Logon": "", "Linked Logon ID": "b6288023", "Network Account Name": "", "Network Account Domain": "", "Logon GUID": "{00000000-0000-0000-0000-000000000000}", "Process Information": "", "Process ID": "b6fc", "Process Name": "C:\\Windows\\System32\\svchost.exe", "Network Information": "", "Workstation Name": "DCB1", "Source Network Address": "127.0.0.1", "Source Port": "0", "Detailed Authentication Information": "", "Logon Process": "User32", "Authentication Package": "Negotiate", "Transited Services": "", "Package Name (NTLM only)": "", "Key Length": "0" ]

2025-09-09 11:31:42.834 127.0.0.1
["Keywords": "Audit Success", "Date and Time": "8.09.2025 15:43:07", "Source": "Microsoft-Windows-Security-Auditing", "Event ID": "4624", "Task Category": "Logon", "Subject": "", "Security ID": "REFORM\\philomela", "Account Name": "philomela", "Account Domain": "REFORM", "Logon ID": "b6365354", "Logon Information": "", "Logon Type": "3", "Restricted Admin Mode": "", "Virtual Account": "No", "Elevated Token": "Yes", "Impersonation Level": "Impersonation", "New Logon": "", "Linked Logon ID": "b636537c", "Network Account Name": "", "Network Account Domain": "", "Logon GUID": "{09145898-424C-48CC-AC9E-2C26235E1380}", "Process Information": "", "Process ID": "b6fc", "Process Name": "C:\\Windows\\System32\\svchost.exe", "Network Information": "", "Workstation Name": "DCB1", "Source Network Address": "127.0.0.1", "Source Port": "0", "Detailed Authentication Information": "", "Logon Process": "User32", "Authentication Package": "Negotiate", "Transited Services": "", "Package Name (NTLM only)": "", "Key Length": "0" ]

2025-09-09 11:31:42.834 127.0.0.1
["Keywords": "Audit Success", "Date and Time": "8.09.2025 15:43:07", "Source": "Microsoft-Windows-Security-Auditing", "Event ID": "4624", "Task Category": "Logon", "Subject": "", "Security ID": "REFORM\\philomela", "Account Name": "philomela", "Account Domain": "REFORM", "Logon ID": "b636537c", "Logon Information": "", "Logon Type": "3", "Restricted Admin Mode": "", "Virtual Account": "No", "Elevated Token": "No", "Impersonation Level": "Impersonation", "New Logon": "", "Linked Logon ID": "b6365354", "Network Account Name": "", "Network Account Domain": "", "Logon GUID": "{00000000-0000-0000-0000-000000000000}", "Process Information": "", "Process ID": "b6fc", "Process Name": "C:\\Windows\\System32\\svchost.exe", "Network Information": "", "Workstation Name": "DCB1", "Source Network Address": "127.0.0.1", "Source Port": "0", "Detailed Authentication Information": "", "Logon Process": "User32", "Authentication Package": "Negotiate", "Transited Services": "", "Package Name (NTLM only)": "", "Key Length": "0" ]

```

## Logon

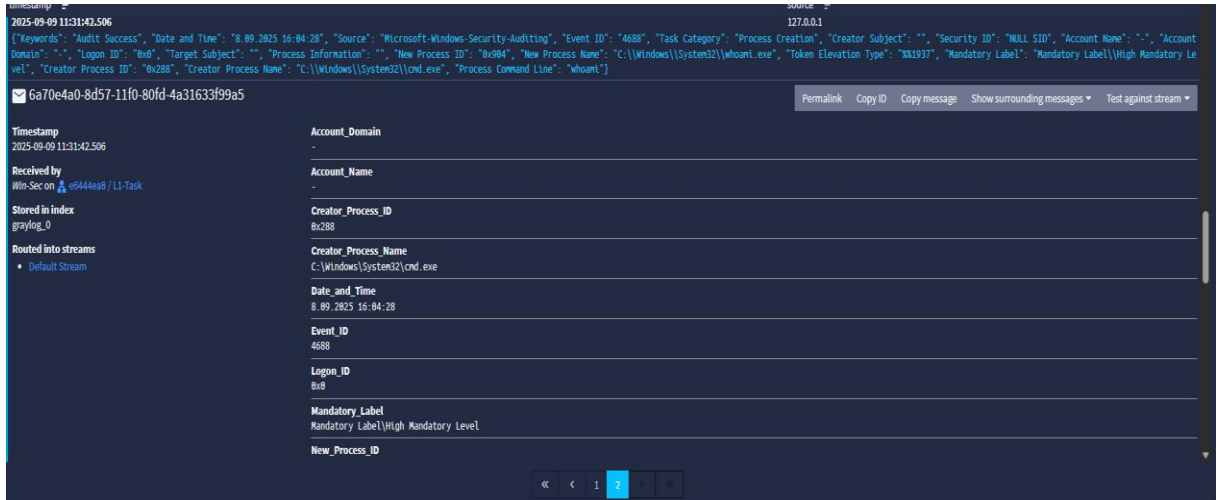
## Privilage Escalation

Bu noktada saldırgan **“2025-09-09 11:31.42”** zaman damgasına Creator Process ,svchost.exe, ardından Runtimebroker.exe çalışıyor. Bu olağan dışı davranış, saldırganın Windows servislerini istismar ederek yetkili bir RuntimeBroker işlemi oluşturduğunu



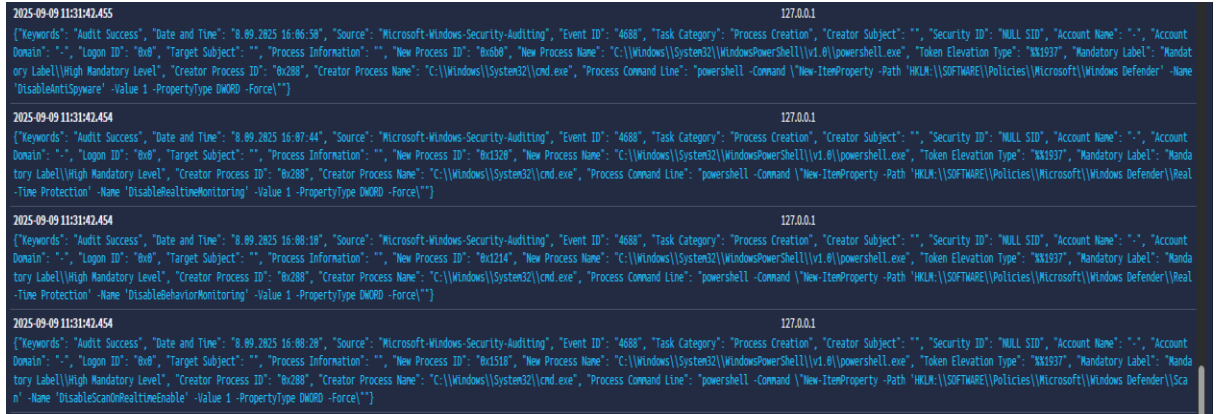
2025-09-09 11:31:47.506 127.0.0.1  
('Keywords': 'Audit Success', 'Date and Time': '8.09.2025 16:04:26', 'Source': 'Microsoft-Windows-Security-Auditing', 'Event ID': '4688', 'Task Category': 'Process Creation', 'Creator Subject': '', 'Security ID': 'BFA00000\\philowola', 'Acco





whoami

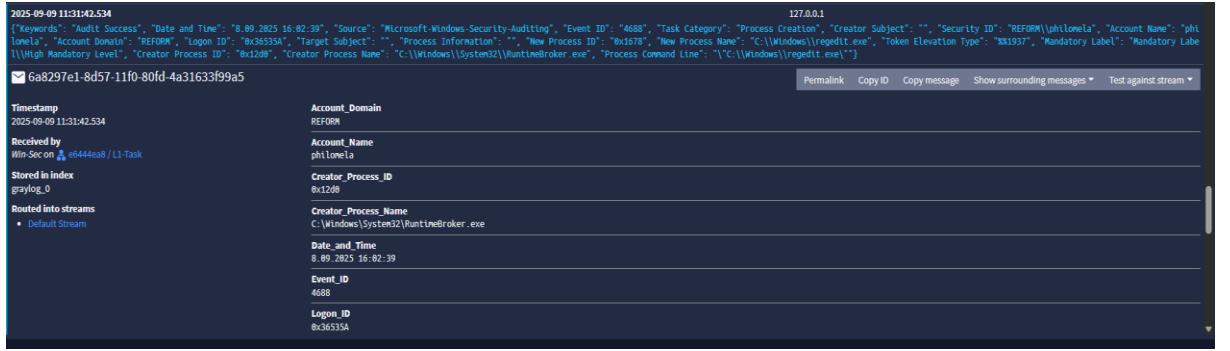
“09.09.2025 11:31:42”de powershell.exe üzerinden Windows Defender’ın registry anahtarları değiştirilerek güvenlik modülleri kapatılmıştır. Bu değişiklikler arasında antispysware modülünün, gerçek zamanlı taramanın, davranışsal analiz motorunun ve realtime tetikleyici taramalarının devre dışı bırakılması yer almaktadır. Value değerlerinin 1 olması bu araçların devre dışı bırakıldığını göstermektedir.



cmd.exe -> powershell.exe

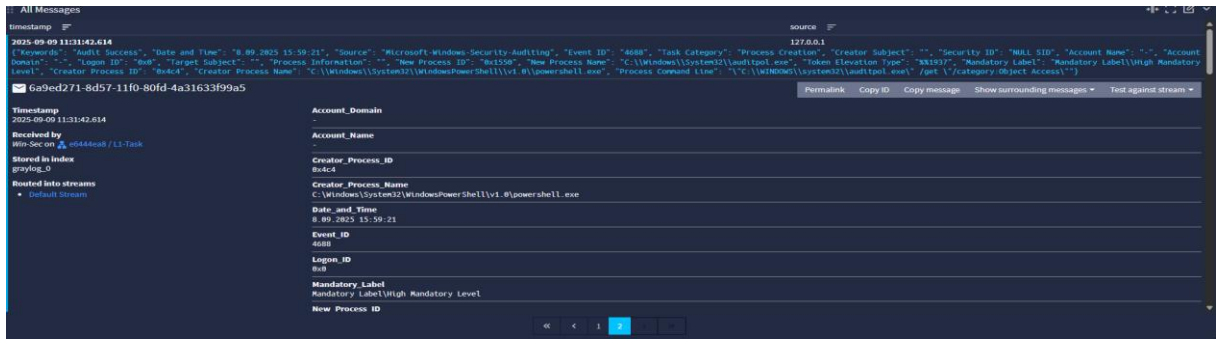
İşlem aralığı “09.09.2025 11:31:42 – 11:31:43” zaman damgalarında ise saldırının başlattığı ek süreçler de tespit edilmiştir.

Regedit.exe, Windows kayıt defteri üzerinde değişiklik yapılmasına izin veren güçlü bir yönetim aracıdır. Yetkisiz şekilde çalıştırılması, saldırının sistem ayarlarını değiştirme, güvenlik kontrollerini devre dışı bırakma veya kalıcılık sağlamak için başlangıç girdilerini manipüle etme amacıyla kullanılmış olabileceğini göstermektedir.



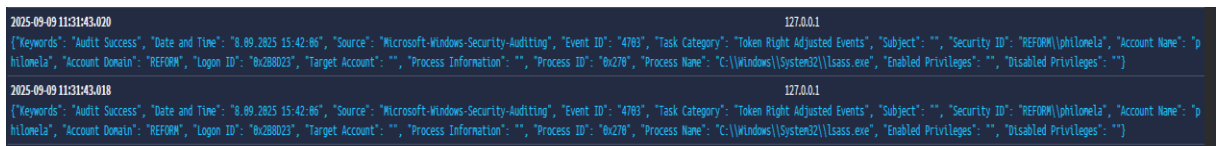
Regedit.exe

Bir diğer kayıta PowerShell.exe (PID: 0x4c4) tarafından auditpol.exe (PID: 0x1550) aracının çalıştırıldığı tespit edilmiştir. Saldırgan tespit edilmekten kaçınma ve hangi faaliyetlerin kayıt altına alındığını görmek isteyebilir.



Auditpol.exe

Kayıtlarda lsass.exe (PID: 0x270) süreci için Event ID 4703 (Token Right Adjusted Events) üretilmiştir. LSASS windows içindeki kimlik bilgileri yönetimini yapan kritik bir yapıdır. Bu noktada kimlik bilgilerini çıkarmaya çalıştığı söylenebilir.



Lsass.exe

Son olarak kayıtlarda svchost.exe (PID: 0x318) tarafından başlatılan dllhost.exe süreçleri gözlenmiştir. Normalde bu işlem meşru olabilir ama saldırı tarafından manipüle edilmeye çalışılmış olabilir.

```
2025-09-09 11:31:42.836 127.0.0.1
{"Keywords": "Audit Success", "Date and Time": "8.09.2025 15:42:24", "Source": "Microsoft-Windows-Security-Auditing", "Event ID": "4688", "Task Category": "Process Creation", "Creator Subject": "", "Security ID": "REFORM\\philomela", "Account Name": "philomela", "Account Domain": "REFORM", "Logon ID": "0x2803f", "Target Subject": "", "Process Information": "", "New Process ID": "0x4ad", "New Process Name": "C:\\Windows\\System32\\dllhost.exe", "Token Elevation Type": "XSI938", "Mandatory Label": "Mandatory Label\\Medium Mandatory Level", "Creator Process ID": "0x318", "Creator Process Name": "C:\\Windows\\System32\\svchost.exe", "Process Command Line": "C:\\WINDOWS\\system32\\dllhost.exe /processid:{DC4537C3-CA73-4AC7-9E1D-B2CE27C3A7A6}"

2025-09-09 11:31:42.815 127.0.0.1
{"Keywords": "Audit Success", "Date and Time": "8.09.2025 15:43:14", "Source": "Microsoft-Windows-Security-Auditing", "Event ID": "4688", "Task Category": "Process Creation", "Creator Subject": "", "Security ID": "REFORM\\philomela", "Account Name": "philomela", "Account Domain": "REFORM", "Logon ID": "0x36537c", "Target Subject": "", "Process Information": "", "New Process ID": "0x3b4", "New Process Name": "C:\\Windows\\System32\\dllhost.exe", "Token Elevation Type": "XSI938", "Mandatory Label": "Mandatory Label\\Medium Mandatory Level", "Creator Process ID": "0x318", "Creator Process Name": "C:\\Windows\\System32\\svchost.exe", "Process Command Line": "C:\\WINDOWS\\system32\\dllhost.exe /processid:{DC4537C3-CA73-4AC7-9E1D-B2CE27C3A7A6}"
```

*Scvdl.exe*

Zaman damgası “**2025-09-09 11:31:43**” anında log kaydı incelendiğinde, saldırganın PowerShell üzerinden klist.exe aracının ,high mandatory(%%1936), yani yönetici ayrıcalıklarıyla çalıştığı görülmektedir. Bu aracın amacı kerberos ticket bilgilerini görmek, yeniden istemek ve yönetmektir. Bundan sonra Kerberos ticket talebi veya pass-the-ticket saldırısı gerçekleşebilir.

All Messages

timestamp

2025-09-09 11:31:43.517

source

127.0.0.1

6d015382-8d57-11f0-80fd-4a31633f99a5

Permalink Copy ID Copy message Show surrounding messages Test against stream

Timestamp

2025-09-09 11:31:43.517

Account Domain

-

Received by

Win-Sec on 6444a0a8/L1-Task

Account Name

-

Stored in index

graylog\_0

Creator Process ID

0x184

Creator Process Name

C:\\Windows\\System32\\WindowsPowerShell\\v1.0\\powershell.exe

Date and Time

8.09.2025 15:37:35

Event ID

4688

Logon ID

0x0

Mandatory Label

Mandatory Label\\High Mandatory Level

New Process ID

0x7ec

New Process Name

-

*Klist.exe*

İnceleme sırasında Event ID 4771 (Kerberos authentication failure) kaydı tespit edilmiştir. Bu logda kullanıcının Kerberos kimlik doğrulama isteği gönderdiği, ancak Failure Code: 0x18 değeri ile başarısız olduğu görülmektedir. Kısa bir süre sonra ise Event ID 4768 (Kerberos Authentication Service – Success) logu oluşmuş ve aynı kullanıcı için Kerberos Ticket Granting Ticket (TGT) başarıyla alınmıştır. Log içerisinde Result Code: 0x0 ve Ticket Encryption



Type 0x12 değerleri görülmektedir. Bu da şifrlenmenin AES256 ile gerçekleşip doğrulamanın tamamlandığını gösterir.

```
2025-09-09 11:31:42.834 127.0.0.1
[Keywords: "Audit Failure", "Date and Time": "8.09.2025 15:42:52", "Source": "Microsoft-Windows-Security-Auditing", "Event ID": "4771", "Task Category": "Kerberos Authentication Service", "Account Information": "", "Security ID": "REFORM\\philomela", "Account Name": "philomela", "Service Information": "", "Service Name": "krbtgt/REFORM", "Network Information": "", "Client Address": "::1", "Client Port": "0", "Additional Information": "", "Ticket Options": "0x40810818", "Failure Code": "0x18", "Pre-Authentication Type": "2", "Certificate Information": "", "Certificate Issuer Name": "", "Certificate Serial Number": "", "Certificate Thumbprint": ""]

2025-09-09 11:31:42.834 127.0.0.1
[Keywords: "Audit Failure", "Date and Time": "8.09.2025 15:42:57", "Source": "Microsoft-Windows-Security-Auditing", "Event ID": "4771", "Task Category": "Kerberos Authentication Service", "Account Information": "", "Security ID": "REFORM\\philomela", "Account Name": "philomela", "Service Information": "", "Service Name": "krbtgt/REFORM", "Network Information": "", "Client Address": "::1", "Client Port": "0", "Additional Information": "", "Ticket Options": "0x40810818", "Failure Code": "0x18", "Pre-Authentication Type": "2", "Certificate Information": "", "Certificate Issuer Name": "", "Certificate Serial Number": "", "Certificate Thumbprint": ""]

2025-09-09 11:31:42.834 127.0.0.1
[Keywords: "Audit Success", "Date and Time": "8.09.2025 15:43:07", "Source": "Microsoft-Windows-Security-Auditing", "Event ID": "4768", "Task Category": "Kerberos Authentication Service", "Account Information": "", "Account Name": "philomela", "Supplied Realm Name": "REFORM", "User ID": "REFORM\\philomela", "Service Information": "", "Service Name": "krbtgt", "Service ID": "REFORM\\krbtgt", "Network Information": "", "Client Address": "::1", "Client Port": "0", "Additional Information": "", "Ticket Options": "0x40810818", "Result Code": "0x0", "Ticket Encryption Type": "0x12", "Pre-Authentication Type": "2", "Certificate Information": "", "Certificate Issuer Name": "", "Certificate Serial Number": "", "Certificate Thumbprint": ""]
```

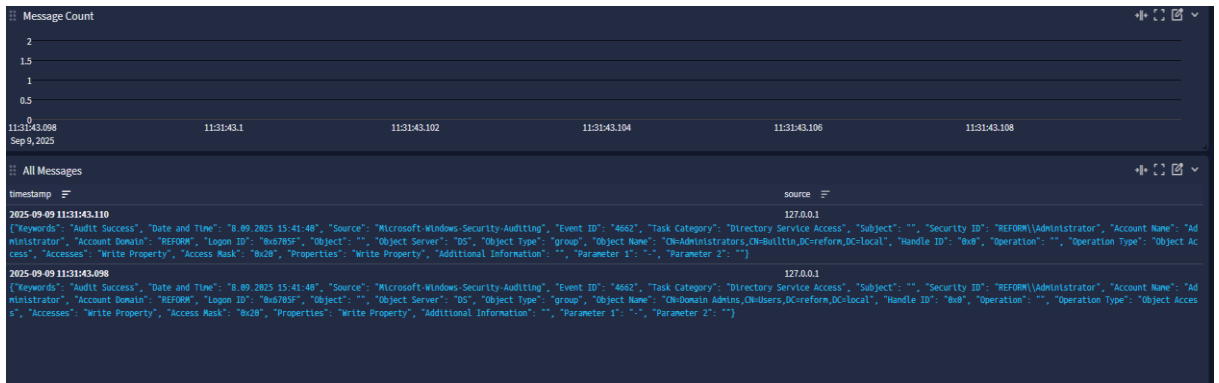
### Kerberos İşlemleri

Administrator hesabı üzerinden Active Directory’de kritik bir işlem gerçekleştirilmiş ve **“Write Property”** erişim tipi kullanılarak hem Builtin\Administrators hem de Domain Admins grupları üzerinde yazma yetkisi kullanıldığı tespit edilmiştir. Domain Admins grubu, Active Directory ortamında en yüksek yetki seviyesini temsil eder ve bu gruba üye olan kullanıcılar tüm domain üzerindeki kaynaklar üzerinde tam kontrol hakkına sahip olur. Özellikle dikkat çeken alanlardan biri Object Name kısmıdır. Burada önce CN=Administrators, CN=Builtin daha sonra da CN=Domain Admins, CN=Users gruplarında Write Property işlemleri kaydedilmiştir(Event ID 5136). Bu, philomela kullanıcısının hem local sistem yöneticisi grubuna hem de domain yöneticileri grubuna eklendiğini kanıtlamaktadır.

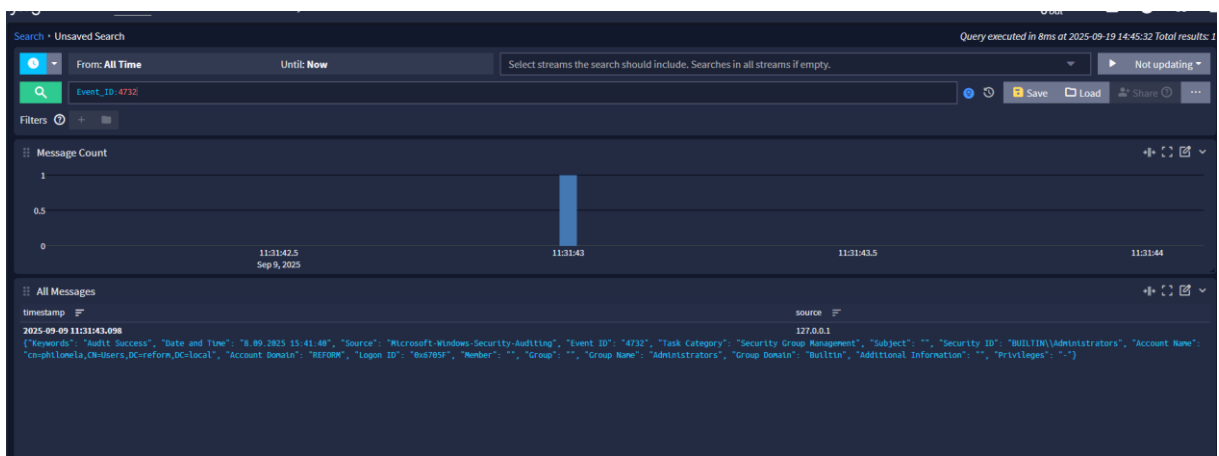
```
All Messages
Timestamp 127.0.0.1
2025-09-09 11:31:43.094
[Keywords: "Audit Success", "Date and Time": "8.09.2025 15:41:41", "Source": "Microsoft-Windows-Security-Auditing", "Event ID": "5136", "Task Category": "Directory Service Changes", "Subject": "", "Security ID": "REFORM\\Administrator", "Account Name": "Administrator", "Account Domain": "REFORM", "Logon ID": "0x6795f", "Directory Service": "", "Name": "reform.local", "Type": "Value Added", "Object": "", "DN": "CN=Administrators,CN=Builtin,DC=reform,DC=local", "Class": "group", "Attribute": "", "LDAP Display Name": "member", "Syntax (OID)": "2.5.5.1", "Value": "cn=philomela,CN=Users,DC=reform,DC=local", "Operation": "", "Correlation ID": "{86602038-08EC-4137-B195-3362DE3A2378}", "Application Correlation ID": ""]

2025-09-09 11:31:43.094 127.0.0.1
[Keywords: "Audit Success", "Date and Time": "8.09.2025 15:41:41", "Source": "Microsoft-Windows-Security-Auditing", "Event ID": "5136", "Task Category": "Directory Service Changes", "Subject": "", "Security ID": "REFORM\\Administrator", "Account Name": "Administrator", "Account Domain": "REFORM", "Logon ID": "0x6795f", "Directory Service": "", "Name": "reform.local", "Type": "Value Added", "Object": "", "DN": "CN=Domain Admins,CN=Users,DC=reform,DC=local", "Class": "group", "Attribute": "", "LDAP Display Name": "member", "Syntax (OID)": "2.5.5.1", "Value": "cn=philomela,CN=Users,DC=reform,DC=local", "Operation": "", "Correlation ID": "{80AC338-8023-4C07-872A-A58A1686883}", "Application Correlation ID": ""]
```

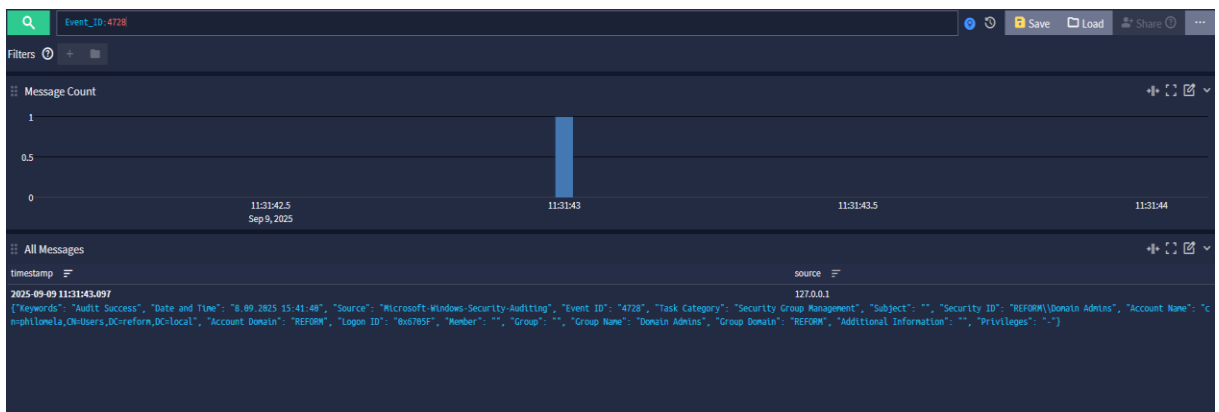
### Event ID 5136



Write property



Event ID 4732



Event ID 4728

## Path Travel Detected

Bu alarm, sistem üzerinde gerçekleştirilen dosya veya izin erişimlerinde olağan dışı bir davranış tespit edildiğinde tetiklenmektedir. Özellikle directory traversal olarak bilinen bu durum saldırganın yetkisiz klasörlere erişmeye çalışması ya da normalde izin verilmeyen dizinler arasında geçiş yapmasıyla ilişkilidir. Bu noktada web isteklerine dikkat edildi ve response kodu 200 olanlar filtrelendi ve istekler bulundu.

## Web izin sorgusu

Öncelikle /external/, /docs/ ve /config/ gibi kritik dizinlere istek gönderilmiş ve sunucu her defasında **200 OK** cevabı döndürmüştür. Bu durum, saldırganın yapılandırma ve dokümantasyon klasörlerine doğrudan erişebildiğini göstermektedir. Ardından robots.txt dosyası istenmiş bu da genellikle gizlenmek istenen dizinlerin açığa çıkmasına neden olabilmektedir. Daha kritik olarak php.ini dosyası da çağırılmış ve erişim sağlanmıştır bu dosya sistemin PHP yapılandırmasını içerdiği için veritabanı bağlantıları, hata logları veya kısıtlı fonksiyonlar gibi hassas bilgilerin sızmasına yol açabilir

Sep 8, 2025	
All Messages	
timestamp	source
2025-09-08 15:20:19.409	127.0.0.1
172.17.0.1 - - [16/Jun/2025:10:11:01 +0000] "GET /external/ HTTP/1.1" 200 1314 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"	
2025-09-08 15:20:19.409	127.0.0.1
172.17.0.1 - - [16/Jun/2025:10:11:01 +0000] "GET /docs/ HTTP/1.1" 200 1312 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"	
2025-09-08 15:20:19.409	127.0.0.1
172.17.0.1 - - [16/Jun/2025:10:11:01 +0000] "GET /config/ HTTP/1.1" 200 1124 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"	
2025-09-08 15:20:19.193	127.0.0.1
172.17.0.1 - - [16/Jun/2025:10:11:00 +0000] "GET /robots.txt HTTP/1.1" 200 254 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"	
2025-09-08 15:20:18.905	127.0.0.1
172.17.0.1 - - [16/Jun/2025:10:11:00 +0000] "GET /php.ini HTTP/1.1" 200 351 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"	
2025-09-08 15:20:18.614	127.0.0.1
172.17.0.1 - - [16/Jun/2025:10:10:59 +0000] "GET /favicon.ico HTTP/1.1" 200 1051 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"	

*Mozilla*

Ayrıca çok fazla sayıda da response 404 kodlu istek de bulunmaktadır. Burada saldırgan doğrudan **“dump”** isimli bir dosya veya dizin talep etmiş. Ancak yanıt **HTTP 404 (Not Found)** dönüyor. Yani orada dizinin bulunmadığını gösteriyor. Bu arama ,dump, çoğu zaman servis dökümü ve hata çıktılarının tutulduğu yerdir.

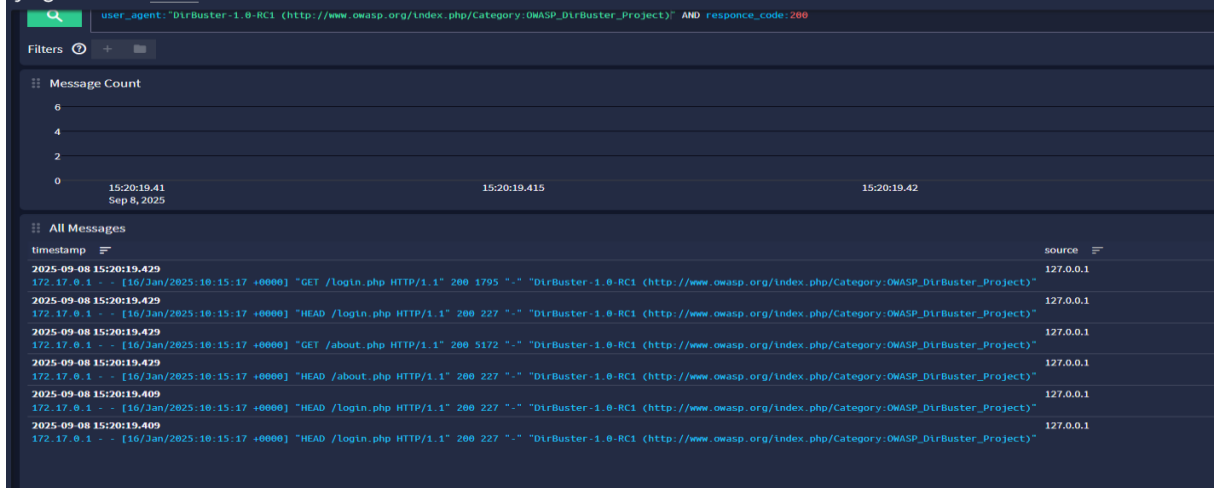
0.5	
0	
15:13	
Sep 8, 2025	
15:14	
15:15	
15:16	
15:17	
15:18	
15:19	
All Messages	
timestamp	source
2025-09-08 15:20:18.613	127.0.0.1
172.17.0.1 - - [16/Jun/2025:10:10:59 +0000] "GET /dump HTTP/1.1" 404 444 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"	
2025-09-08 15:12:52.902	127.0.0.1
172.17.0.1 - - [16/Jun/2025:10:10:59 +0000] "GET /dump HTTP/1.1" 404 444 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"	

*dump*



## Dirbuster

DirBuster logları incelendiğinde açıkça DirBuster-1.0 kullanımı var. Bu da saldırganın OWASP DirBuster aracıyla web dizin taraması yaptığını doğruluyor. Loglarda /Login.php, /about.php gibi istekler art arda geliyor ve çoğu **HTTP 200 (OK)** dönüyor.

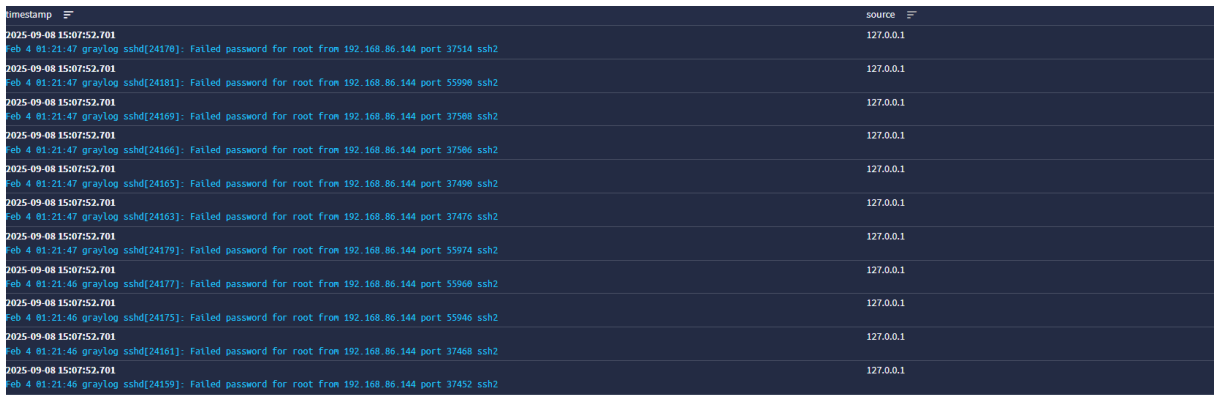


timestamp	source
2025-09-08 15:20:19.429	127.0.0.1
172.17.0.1 - - [10/Jan/2025:10:15:17 +0000] "GET /login.php HTTP/1.1" 200 1795 "-" "DirBuster-1.0-RC1 (http://www.owasp.org/index.php/Category:OWASP_DirBuster_Project)"	127.0.0.1
2025-09-08 15:20:19.429	127.0.0.1
172.17.0.1 - - [10/Jan/2025:10:15:17 +0000] "HEAD /login.php HTTP/1.1" 200 227 "-" "DirBuster-1.0-RC1 (http://www.owasp.org/index.php/Category:OWASP_DirBuster_Project)"	127.0.0.1
2025-09-08 15:20:19.429	127.0.0.1
172.17.0.1 - - [10/Jan/2025:10:15:17 +0000] "GET /about.php HTTP/1.1" 200 5172 "-" "DirBuster-1.0-RC1 (http://www.owasp.org/index.php/Category:OWASP_DirBuster_Project)"	127.0.0.1
2025-09-08 15:20:19.429	127.0.0.1
172.17.0.1 - - [10/Jan/2025:10:15:17 +0000] "HEAD /about.php HTTP/1.1" 200 227 "-" "DirBuster-1.0-RC1 (http://www.owasp.org/index.php/Category:OWASP_DirBuster_Project)"	127.0.0.1
2025-09-08 15:20:19.409	127.0.0.1
172.17.0.1 - - [10/Jan/2025:10:15:17 +0000] "HEAD /login.php HTTP/1.1" 200 227 "-" "DirBuster-1.0-RC1 (http://www.owasp.org/index.php/Category:OWASP_DirBuster_Project)"	127.0.0.1
2025-09-08 15:20:19.409	127.0.0.1
172.17.0.1 - - [10/Jan/2025:10:15:17 +0000] "HEAD /login.php HTTP/1.1" 200 227 "-" "DirBuster-1.0-RC1 (http://www.owasp.org/index.php/Category:OWASP_DirBuster_Project)"	127.0.0.1

*Dirbuster*

## Root Authentication Failed

Bu log çıktısına göre aynı IP adresinden (192.168.86.144) çok kısa süre içerisinde defalarca **root** kullanıcısı için başarısız oturum açma denemesi yapılmış. Her deneme farklı portlardan (37514, 55990, 37508, 37476, 55974 vs.) geliyor ama **ssh2 protokolü** üzerinden gerçekleşiyor. Log satırları “Failed password for root” şeklinde ardışık biçimde kaydedilmiş. Önleme için /etc/ssh/sshd\_config dosyasında “PermitRootLogin no” yapılarak direkt olarak root kullanıcısıyla doğrudan giriş yapılması engellenebilir.



timestamp	source
2025-09-08 15:07:52.701	127.0.0.1
Feb 4 01:21:47 graylog sshd[24178]: Failed password for root from 192.168.86.144 port 37514 ssh2	127.0.0.1
2025-09-08 15:07:52.701	127.0.0.1
Feb 4 01:21:47 graylog sshd[24181]: Failed password for root from 192.168.86.144 port 55990 ssh2	127.0.0.1
2025-09-08 15:07:52.701	127.0.0.1
Feb 4 01:21:47 graylog sshd[24169]: Failed password for root from 192.168.86.144 port 37508 ssh2	127.0.0.1
2025-09-08 15:07:52.701	127.0.0.1
Feb 4 01:21:47 graylog sshd[24166]: Failed password for root from 192.168.86.144 port 37506 ssh2	127.0.0.1
2025-09-08 15:07:52.701	127.0.0.1
Feb 4 01:21:47 graylog sshd[24165]: Failed password for root from 192.168.86.144 port 37490 ssh2	127.0.0.1
2025-09-08 15:07:52.701	127.0.0.1
Feb 4 01:21:47 graylog sshd[24163]: Failed password for root from 192.168.86.144 port 37476 ssh2	127.0.0.1
2025-09-08 15:07:52.701	127.0.0.1
Feb 4 01:21:47 graylog sshd[24179]: Failed password for root from 192.168.86.144 port 55974 ssh2	127.0.0.1
2025-09-08 15:07:52.701	127.0.0.1
Feb 4 01:21:46 graylog sshd[24177]: Failed password for root from 192.168.86.144 port 55960 ssh2	127.0.0.1
2025-09-08 15:07:52.701	127.0.0.1
Feb 4 01:21:46 graylog sshd[24175]: Failed password for root from 192.168.86.144 port 55946 ssh2	127.0.0.1
2025-09-08 15:07:52.701	127.0.0.1
Feb 4 01:21:46 graylog sshd[24161]: Failed password for root from 192.168.86.144 port 37468 ssh2	127.0.0.1
2025-09-08 15:07:52.701	127.0.0.1
Feb 4 01:21:46 graylog sshd[24159]: Failed password for root from 192.168.86.144 port 37452 ssh2	127.0.0.1

*Root Authentication Failed*

## MITRE ATT&CK Analizi

Tactic	Technique	ID	Açıklama
Defense Evasion	Impair Defenses: Disable or Modify Tools	T1562.001	PowerShell üzerinden Defender'ın kapatılması
Credential Access	OS Credential Dumping: LSASS Memory	T1003.001	lsass.exe erişimi / dump girişi
Discovery / Evasion	System Information Discovery / Modify Registry	T1082	regedit.exe çalıştırılması
Credential Access	Kerberos Tickets: TGT Abuse	T1558.001	klist.exe ile ticket'ların listelenmesi
Privilege Escalation	Create Account / Add to Group	T1136.002	Event ID 4728 / 4732 – Kullanıcıların "Domain Admins" grubuna eklenmesi
Discovery	Path Traversal	T1006	/etc/passwd, /dump gibi path traversal denemeleri
Reconnaissance	Active Scanning	T1595	DirBuster User- Agent ile Login.php, about.php taramaları
Credential Access	Brute Force: Password Guessing	T1110.001	"Failed password for root" denemeleri
System Binary Proxy Execution	Defense Evasion(LOLBIN)	T1218	RuntimeBroker- >cmd.exe- >powershell.exe

## Sonuç-Öneri

Analiz edilen log kayıtları, sistem üzerinde hem privilege escalation (yetki yükseltme) hem de defense evasion (savunma atlatma) girişimlerinin başarıyla gerçekleştirildiğini göstermektedir. Özellikle Windows Defender'ın registry üzerinden devre dışı bırakılması, LSASS sürecine erişim sağlanması, Kerberos ticket manipülasyonları ve Domain Admins grubuna kullanıcı eklenmesi saldırganın sistem üzerinde tam kontrol elde ettiğini işaret etmektedir. Ayrıca path traversal, DirBuster ile dizin keşfi ve SSH brute force denemeleri gibi aktiviteler, saldırganın yalnızca iç ağda değil, dışa açık servislerde de aktif keşif ve saldırı faaliyetlerinde bulunduğunu kanıtlamaktadır.

Active Directory ortamında en az ayrıcalık prensibi uygulanmalı, kullanıcıların erişim hakları düzenli olarak gözden geçirilmeli ve gerekli durumlarda güncellenmelidir. Güvenliği artırmak için çok faktörlü kimlik doğrulama (MFA) devreye alınmalıdır. Hizmet hesaplarının ayrıcalıkları en düşük seviyede tutulmalı ve kaba kuvvet saldırılarını zorlaştırmak amacıyla en az 25 karakter uzunluğunda, karmaşık parolalar kullanılmalıdır. RC4 şifreleme algoritması bilinen zafiyetleri nedeniyle güvenilirliğini yitirmiştir ve saldırganlar bu zafiyetleri kullanarak şifreli trafiği çözebilir. Bu nedenle devre dışı bırakılarak yerine AES gibi modern ve güçlü algoritmalar tercih edilmelidir. LSA (Yerel Güvenlik Yetkilisi) Koruması, LSASS sürecine yönelik yetkisiz erişimleri engelleyerek kimlik bilgisi hırsızlığına karşı güçlü bir savunma sağlar. Bu koruma, bellekten parola özetlerinin veya kimlik doğrulama belirteçlerinin çekilmesini zorlaştırır.



## Kaynakça

- 1- <https://www.ultimatewindowssecurity.com/> (Event loglarının detaylı olarak analiz edildiği site)
- 2- <https://www.techtarget.com/searchsecurity/definition/Kerberos> (Kerberos hakkında detaylı açıklama yapıldığı site)
- 3- <https://blog.netwrix.com/> (Genel AD yapısının açıklandığı site)
- 4- <https://www.semperis.com/blog/> (Özellikle AD güvenliği konusunda çözümleri olan bir şirketin blog sitesi)
- 5- <https://chatgpt.com/> (Loglar incelenirken anlam bütünlüğü oluşturulması adına kullanıldı.)