

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 dizin 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 alarmının oluşum süreçleri incelenmiştir. İnceleme kapsamında **“A member was added to a security-enabled global group”**, **“Path Travel Detected”** ve **“Root Authentication Failed”** alarmlarının nasıl olduğu analiz edilerek ortaya konulmuştur.

Alarmlar

A Member Was Added To A Security-enabled Global Group

Logon aşaması

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.

timestamp	source	Event ID
2022-07-08 16:44:30.123	127.0.0.1	
["Keywords": "Audit Failure", "Date and Time": "8:89:2855 15:42:52", "Source": "Microsoft-Windows-Security-Auditing", "Event ID": "4625", "Task Category": "Logon", "Subject": "", "Security ID": "NULL SID", "Account Name": "philomela", "Account Domain": "R_EF00", "Logon ID": "0x3E7", "Logon Type": "2", "Account For Which Logon Failed": "", "Failure Information": "", "Failure Reason": "Unknown user name or bad password", "Status": "0x00000000", "Sub Status": "0x00000000", "Process Information": "", "Caller Process ID": "0x0fc", "Caller Process Name": "C:\Windows\System32\svchost.exe", "Network Information": "", "Workstation Name": "DC01", "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"]	127.0.0.1	
2022-08-08 16:44:30.193	127.0.0.1	
["Keywords": "Audit Failure", "Date and Time": "8:89:2855 15:42:57", "Source": "Microsoft-Windows-Security-Auditing", "Event ID": "4625", "Task Category": "Logon", "Subject": "", "Security ID": "NULL SID", "Account Name": "philomela", "Account Domain": "R_EF00", "Logon ID": "0x3E7", "Logon Type": "2", "Account For Which Logon Failed": "", "Failure Information": "", "Failure Reason": "Unknown user name or bad password", "Status": "0x00000000", "Sub Status": "0x00000000", "Process Information": "", "Caller Process ID": "0x0fc", "Caller Process Name": "C:\Windows\System32\svchost.exe", "Network Information": "", "Workstation Name": "DC01", "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"]	127.0.0.1	
2022-08-08 16:44:50.522	127.0.0.1	
["Keywords": "Audit Failure", "Date and Time": "8:89:2855 15:42:57", "Source": "Microsoft-Windows-Security-Auditing", "Event ID": "4625", "Task Category": "Logon", "Subject": "", "Security ID": "NULL SID", "Account Name": "philomela", "Account Domain": "R_EF00", "Logon ID": "0x3E7", "Logon Type": "2", "Account For Which Logon Failed": "", "Failure Information": "", "Failure Reason": "Unknown user name or bad password", "Status": "0x00000000", "Sub Status": "0x00000000", "Process Information": "", "Caller Process ID": "0x0fc", "Caller Process Name": "C:\Windows\System32\svchost.exe", "Network Information": "", "Workstation Name": "DC01", "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"]	127.0.0.1	
2022-08-08 16:44:50.572	127.0.0.1	
["Keywords": "Audit Failure", "Date and Time": "8:89:2855 15:42:57", "Source": "Microsoft-Windows-Security-Auditing", "Event ID": "4625", "Task Category": "Logon", "Subject": "", "Security ID": "NULL SID", "Account Name": "philomela", "Account Domain": "R_EF00", "Logon ID": "0x3E7", "Logon Type": "2", "Account For Which Logon Failed": "", "Failure Information": "", "Failure Reason": "Unknown user name or bad password", "Status": "0x00000000", "Sub Status": "0x00000000", "Process Information": "", "Caller Process ID": "0x0fc", "Caller Process Name": "C:\Windows\System32\svchost.exe", "Network Information": "", "Workstation Name": "DC01", "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"]	127.0.0.1	
2022-08-08 16:45:01.624	127.0.0.1	
["Keywords": "Audit Failure", "Date and Time": "8:89:2855 15:42:52", "Source": "Microsoft-Windows-Security-Auditing", "Event ID": "4625", "Task Category": "Logon", "Subject": "", "Security ID": "NULL SID", "Account Name": "philomela", "Account Domain": "R_EF00", "Logon ID": "0x3E7", "Logon Type": "2", "Account For Which Logon Failed": "", "Failure Information": "", "Failure Reason": "Unknown user name or bad password", "Status": "0x00000000", "Sub Status": "0x00000000", "Process Information": "", "Caller Process ID": "0x0fc", "Caller Process Name": "C:\Windows\System32\svchost.exe", "Network Information": "", "Workstation Name": "DC01", "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"]	127.0.0.1	

Hatalı Giriş

Daha sonra kullanıcı, **philomela**, hesabı **“09.09.25 11:31:42”** zaman damgasında oluşturulmuştur(Event ID 4720). Oluşturulan hesap üzerinde parola reset girişimi 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 127.0.0.1
2025-09-09 11:31:43.111
{"Keywords": "Audit Success", "Date and Time": "8.09.2025 15:41:17", "Source": "Microsoft-Windows-Security-Auditing", "Event ID": "4720", "Task Category": "User Account Management", "Subject": "", "Security ID": "REFORM\philomela", "Account Name": "philomela", "Account Domain": "REFORM", "Logon ID": "0x0785F", "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": "never", "Account Expires": "never", "Primary Group ID": "513", "Allowed To Delegate To": "", "Old UAC Value": "0x15", "New UAC Value": "0x15", "User Account Control": "", "User Parameters": "", "SID History": "", "Logon Hours": "", "Additional Information": ""}
127.0.0.1
2025-09-09 11:31:43.111
{"Keywords": "Audit Success", "Date and Time": "8.09.2025 15:41:17", "Source": "Microsoft-Windows-Security-Auditing", "Event ID": "4720", "Task Category": "User Account Management", "Subject": "", "Security ID": "REFORM\philomela", "Account Name": "philomela", "Account Domain": "REFORM", "Logon ID": "0x0785F", "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": "never", "Account Expires": "", "Primary Group ID": "", "AllowedToDelegateTo": "", "Old UAC Value": "", "New UAC Value": "", "User Account Control": "", "User Parameters": "", "SID History": "", "Logon Hours": "", "Additional Information": "", "Privileges": ""}
127.0.0.1
2025-09-09 11:31:43.111
{"Keywords": "Audit Success", "Date and Time": "8.09.2025 15:41:17", "Source": "Microsoft-Windows-Security-Auditing", "Event ID": "4720", "Task Category": "User Account Management", "Subject": "", "Security ID": "REFORM\philomela", "Account Name": "philomela", "Account Domain": "REFORM", "Logon ID": "0x2AF01B", "Target Account": ""}
127.0.0.1
2025-09-09 11:31:43.111
{"Keywords": "Audit Success", "Date and Time": "8.09.2025 15:41:17", "Source": "Microsoft-Windows-Security-Auditing", "Event ID": "4720", "Task Category": "User Account Management", "Subject": "", "Security ID": "REFORM\philomela", "Account Name": "philomela", "Account Domain": "REFORM", "Logon ID": "0x2AF01B", "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": "never", "Account Expires": "", "Primary Group ID": "", "AllowedToDelegateTo": "", "Old UAC Value": "0x11", "New UAC Value": "0x11", "User Account Control": "", "User Parameters": "", "SID History": "", "Logon Hours": "", "Additional Information": "", "Privileges": ""}
127.0.0.1
2025-09-09 11:31:43.111
{"Keywords": "Audit Success", "Date and Time": "8.09.2025 15:41:17", "Source": "Microsoft-Windows-Security-Auditing", "Event ID": "4720", "Task Category": "User Account Management", "Subject": "", "Security ID": "REFORM\philomela", "Account Name": "philomela", "Account Domain": "REFORM", "Logon ID": "0x2AF01B", "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": "never", "Account Expires": "", "Primary Group ID": "", "AllowedToDelegateTo": "", "Old UAC Value": "0x10", "New UAC Value": "0x10", "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 .

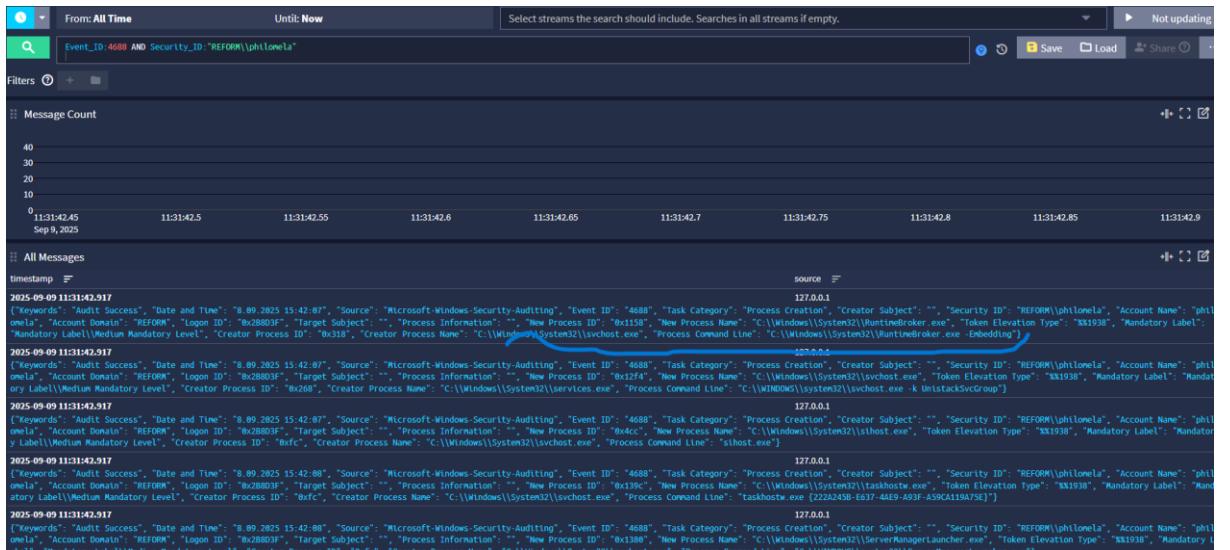
All Messages
timestamp 127.0.0.1
2025-09-09 11:31:43.091
{"Keywords": "Audit Success", "Date and Time": "8.09.2025 15:42:04", "Source": "Microsoft-Windows-Security-Auditing", "Event ID": "4624", "Task Category": "Logon", "Subject": "", "Security ID": "REFORM\philomela", "Account Name": "philomela", "Account Domain": "REFORM", "Logon ID": "0x2B8023", "Logon Information": "", "Logon Type": "2", "Restricted Admin Mode": "", "Virtual Account": "No", "Elevated Token": "Yes", "Impersonation Level": "Impersonation", "New Logon": "", "Linked Logon ID": "0x2B8023", "Network Account Name": "", "Network Account Domain": "", "Logon QUID": "{0346C6F6-B9BC-8EDF-B477-BD0C6869A8AA}", "Process Information": "", "Process ID": "0xfc", "Process Name": "C:\Windows\System32\svchost.exe", "Network Information": "", "Workstation Name": "DC01", "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": "8"}]
127.0.0.1
2025-09-09 11:31:43.091
{"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": "0x2B8023", "Logon Information": "", "Logon Type": "2", "Restricted Admin Mode": "", "Virtual Account": "No", "Elevated Token": "Yes", "Impersonation Level": "Impersonation", "New Logon": "", "Linked Logon ID": "0x2B8023", "Network Account Name": "", "Network Account Domain": "", "Logon QUID": "{0346C6F6-B9BC-8EDF-B477-BD0C6869A8AA}", "Process Information": "", "Process ID": "0xfc", "Process Name": "C:\Windows\System32\svchost.exe", "Network Information": "", "Workstation Name": "DC01", "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": "8"}]
127.0.0.1
2025-09-09 11:31:42.834
{"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": "0x36535A", "Logon Information": "", "Logon Type": "2", "Restricted Admin Mode": "", "Virtual Account": "No", "Elevated Token": "Yes", "Impersonation Level": "Impersonation", "New Logon": "", "Linked Logon ID": "0x36535C", "Network Account Name": "", "Network Account Domain": "", "Logon QUID": "{06914589B-024C-4C9E-C26225E13B0}", "Process Information": "", "Process ID": "0xfc", "Process Name": "C:\Windows\System32\svchost.exe", "Network Information": "", "Workstation Name": "DC01", "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": "8"}]
127.0.0.1
2025-09-09 11:31:42.834
{"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": "0x36535C", "Logon Information": "", "Logon Type": "2", "Restricted Admin Mode": "", "Virtual Account": "No", "Elevated Token": "Yes", "Impersonation Level": "Impersonation", "New Logon": "", "Linked Logon ID": "0x36535A", "Network Account Name": "", "Network Account Domain": "", "Logon QUID": "{06914589B-024C-4C9E-C26225E13B0}", "Process Information": "", "Process ID": "0xfc", "Process Name": "C:\Windows\System32\svchost.exe", "Network Information": "", "Workstation Name": "DC01", "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": "8"}]
127.0.0.1

Logon

Privilage Escalation

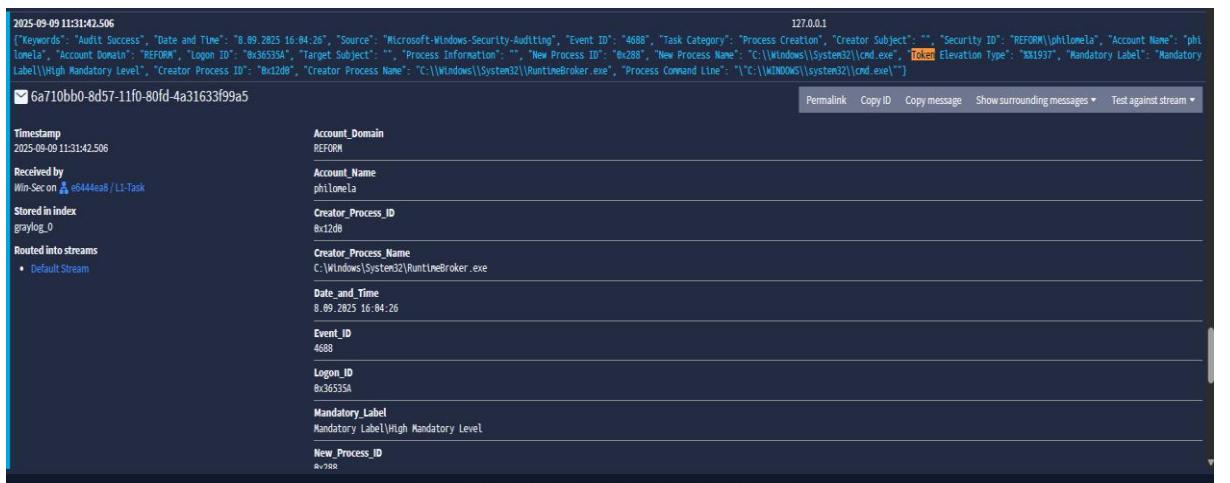
Bu noktada saldırıcı **“2025-09-09 11:31.42”** zaman damgasına Creator Process ,svchost.exe, ardından Runtimebroker.exe çalışıyor. Bu olağan dışı davranış, saldırıcının Windows servislerini istismar ederek yetkili bir RuntimeBroker işlemi oluşturduğunu

göstermektedir. Bu yöntem, privilege escalation ve defense evasion amacıyla kullanılan LOLBin (Living off the Land Binaries) tekniklerinden biridir.



Syghost.exe -> RuntimeBroker.exe

Bu noktada ise process zinciri devam etmektedir. Çalışan RuntimeBroker “**2025-09-09 11:31:42**” zaman damgasında cmd.exe’yi çalıştırmaktadır. Ayrıca olay High Mandatory Level (yükseltilmiş yetki) ile gerçekleşmiştir. Bu durum saldırganın, privilege escalation sonrasında RuntimeBroker üzerinden yönetici haklarına sahip bir komut satırı açtığını ve bunu kötüye kullandığını göstermektedir. Ayrıca bu esnada whoami sorgusu yapmıştır bu da loglarda gözlemlendi.



RuntimeBroker.exe -> cmd.exe

Timestamp		SOURCE
2025-09-09 11:31:42.506		127.0.0.1
{"Keywords": "Audit Success", "Date and Time": "08.09.2025 16:04:28", "Source": "Microsoft-Windows-Security-Auditing", "Event ID": "4688", "Task Category": "Process Creation", "Creator Subject": "", "Security ID": "NULL SID", "Account Name": "", "Account Domain": "", "Logon ID": "0x0", "Target Subject": "", "Process Information": "", "New Process ID": "0x004", "New Process Name": "C:\Windows\System32\whoami.exe", "Token Elevation Type": "XN1937", "Mandatory Label": "Mandatory Label\\High Mandatory Level", "Creator Process ID": "0x288", "Creator Process Name": "C:\Windows\System32\cmd.exe", "Process Command Line": "whoami"}		
#6a70e4a0-8d57-11f0-80fd-a31633ff99a5		Permalink Copy ID Copy message Show surrounding messages Test against stream
Timestamp 2025-09-09 11:31:42.506		Account_Domain -
Received by Win-Sec on #6444ea8 / LI-Task		Account_Name -
Stored in index graylog_0		Creator_Process_ID 0x288
Routed into streams • Default Stream		Creator_Process_Name C:\Windows\System32\cmd.exe
Date and Time 08.09.2025 16:04:28		Date and Time 8.09.2025 16:04:28
Event_ID 4688		Event_ID 4688
Logon_ID 0x0		Logon_ID 0x0
Mandatory_Label Mandatory Label\\High Mandatory Level		Mandatory_Label Mandatory Label\\High Mandatory Level
New_Process_ID New Process ID		New_Process_ID New Process ID

whoami

“09.09.2025 11:31:42’de powershell.exe üzerinden Windows Defender’ın registry anahtarlarını değiştirilerek güvenlik modülleri kapatılmıştır. Bu değişiklikler arasında antispyware 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.

2025-09-09 11:31:42.455		127.0.0.1
{"Keywords": "Audit Success", "Date and Time": "08.09.2025 16:06:58", "Source": "Microsoft-Windows-Security-Auditing", "Event ID": "4688", "Task Category": "Process Creation", "Creator Subject": "", "Security ID": "NULL SID", "Account Name": "", "Account Domain": "", "Logon ID": "0x0", "Target Subject": "", "Process Information": "", "New Process ID": "0x006", "New Process Name": "C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe", "Token Elevation Type": "XN1937", "Mandatory Label": "Mandatory Label\\High Mandatory Level", "Creator Process ID": "0x288", "Creator Process Name": "C:\Windows\System32\cmd.exe", "Process Command Line": "powershell -Command \\"New-ItemProperty -Path 'HKLM:\SOFTWARE\ Policies\ Microsoft\ Windows Defender' -Name 'DisableBehaviorMonitoring' -Value 1 -PropertyType DWORD -Force\\""} 		
2025-09-09 11:31:42.454		127.0.0.1
{"Keywords": "Audit Success", "Date and Time": "08.09.2025 16:07:44", "Source": "Microsoft-Windows-Security-Auditing", "Event ID": "4688", "Task Category": "Process Creation", "Creator Subject": "", "Security ID": "NULL SID", "Account Name": "", "Account Domain": "", "Logon ID": "0x0", "Target Subject": "", "Process Information": "", "New Process ID": "0x132", "New Process Name": "C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe", "Token Elevation Type": "XN1937", "Mandatory Label": "Mandatory Label\\High Mandatory Level", "Creator Process ID": "0x288", "Creator Process Name": "C:\Windows\System32\cmd.exe", "Process Command Line": "powershell -Command \\"New-ItemProperty -Path 'HKLM:\SOFTWARE\ Policies\ Microsoft\ Windows Defender'\Real-Time Protection' -Name DisableBehaviorMonitoring -Value 1 -PropertyType DWORD -Force\\""} 		
2025-09-09 11:31:42.454		127.0.0.1
{"Keywords": "Audit Success", "Date and Time": "08.09.2025 16:08:18", "Source": "Microsoft-Windows-Security-Auditing", "Event ID": "4688", "Task Category": "Process Creation", "Creator Subject": "", "Security ID": "NULL SID", "Account Name": "", "Account Domain": "", "Logon ID": "0x0", "Target Subject": "", "Process Information": "", "New Process ID": "0x124", "New Process Name": "C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe", "Token Elevation Type": "XN1937", "Mandatory Label": "Mandatory Label\\High Mandatory Level", "Creator Process ID": "0x288", "Creator Process Name": "C:\Windows\System32\cmd.exe", "Process Command Line": "powershell -Command \\"New-ItemProperty -Path 'HKLM:\SOFTWARE\ Policies\ Microsoft\ Windows Defender'\Real-Time Protection' -Name DisableBehaviorMonitoring -Value 1 -PropertyType DWORD -Force\\""} 		
2025-09-09 11:31:42.454		127.0.0.1
{"Keywords": "Audit Success", "Date and Time": "08.09.2025 16:08:28", "Source": "Microsoft-Windows-Security-Auditing", "Event ID": "4688", "Task Category": "Process Creation", "Creator Subject": "", "Security ID": "NULL SID", "Account Name": "", "Account Domain": "", "Logon ID": "0x0", "Target Subject": "", "Process Information": "", "New Process ID": "0x151", "New Process Name": "C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe", "Token Elevation Type": "XN1937", "Mandatory Label": "Mandatory Label\\High Mandatory Level", "Creator Process ID": "0x288", "Creator Process Name": "C:\Windows\System32\cmd.exe", "Process Command Line": "powershell -Command \\"New-ItemProperty -Path 'HKLM:\SOFTWARE\ Policies\ Microsoft\ Windows Defender'\ScanOnRealtimeEnable' -Value 1 -PropertyType DWORD -Force\\""} 		

cmd.exe -> powershell.exe

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

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

2025-09-09 11:31:42.534		127.0.0.1
Keywords:	"Audit Success", "Date and Time": "8.09.2025 16:02:39", "Source": "Microsoft-Windows-Security-Auditing", "Event ID": "4688", "Task Category": "Process Creation", "Creator Subject": "", "Security ID": "REFORM\philomena", "Account Name": "philomena", "Account Domain": "REFORM", "Logon ID": "0x36535A", "Target Subject": "", "Process Information": "", "New Process ID": "0x167B", "New Process Name": "C:\Windows\System32\regedit.exe", "Token Elevation Type": "N/A", "Mandatory Label": "Mandatory Label\\High Mandatory Level", "Creator Process Name": "C:\Windows\System32\RuntimeBroker.exe", "Process Command Line": "\"C:\Windows\regedit.exe\""	
Received by	Win-Sec on A \e5444ea8 / L1-Task	Permalink Copy ID Copy message Show surrounding messages ▾ Test against stream ▾
Stored in index	graylog_0	
Routed into streams	• Default Stream	
Timestamp	2025-09-09 11:31:42.534	
Account_Domain	REFORM	
Account_Name	philomena	
Creator_Process_ID	0x120B	
Creator_Process_Name	C:\Windows\System32\RuntimeBroker.exe	
Date_and_Time	8.09.2025 16:02:39	
Event_ID	4688	
Logon_ID	0x36535A	

Regedit.exe

Bir diğer kayıttı 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.

2025-09-09 11:31:42.514		127.0.0.1
Keywords:	"Audit Success", "Date and Time": "8.09.2025 15:59:21", "Source": "Microsoft-Windows-Security-Auditing", "Event ID": "4688", "Task Category": "Process Creation", "Creator Subject": "", "Security ID": "NULL SID", "Account Name": "", "Account Domain": "", "Logon ID": "0x0", "Target Subject": "", "Process Information": "", "New Process ID": "0x5556", "New Process Name": "C:\Windows\System32\auditpol.exe", "Token Elevation Type": "N/A", "Mandatory Label": "Mandatory Label\\High Mandatory Level", "Creator Process ID": "0x4c4", "Creator Process Name": "C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe", "Process Command Line": "\"C:\Windows\System32\auditpol.exe\" /get /category Object Access"	
Received by	Win-Sec on A \e5444ea8 / L1-Task	Permalink Copy ID Copy message Show surrounding messages ▾ Test against stream ▾
Stored in index	graylog_0	
Routed into streams	• Default Stream	
Timestamp	2025-09-09 11:31:42.514	
Account_Domain	-	
Account_Name	-	
Creator_Process_ID	0x4c4	
Creator_Process_Name	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	
Date_and_Time	8.09.2025 15:59:21	
Event_ID	4688	
Logon_ID	0x0	
Mandatory_Label	Mandatory Label\\High Mandatory Level	
New_Process_ID		

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.

2025-09-09 11:31:43.020		127.0.0.1
Keywords:	"Audit Success", "Date and Time": "8.09.2025 15:42:06", "Source": "Microsoft-Windows-Security-Auditing", "Event ID": "4703", "Task Category": "Token Right Adjusted Events", "Subject": "", "Security ID": "REFORM\philomena", "Account Name": "philomena", "Account Domain": "REFORM", "Logon ID": "0x288023", "Target Account": "", "Process Information": "", "Process ID": "0x270", "Process Name": "C:\Windows\System32\lsass.exe", "Enabled Privileges": "", "Disabled Privileges": ""	
2025-09-09 11:31:43.018		127.0.0.1
Keywords:	"Audit Success", "Date and Time": "8.09.2025 15:42:06", "Source": "Microsoft-Windows-Security-Auditing", "Event ID": "4703", "Task Category": "Token Right Adjusted Events", "Subject": "", "Security ID": "REFORM\philomena", "Account Name": "philomena", "Account Domain": "REFORM", "Logon ID": "0x288023", "Target Account": "", "Process Information": "", "Process ID": "0x270", "Process Name": "C:\Windows\System32\lsass.exe", "Enabled Privileges": "", "Disabled Privileges": ""	

Lsass.exe

Son olarak kayıtlarda svchost.exe (PID: 0x318) tarafından başlatılan dllhost.exe süreçleri gözlenmiştir. Normalde bu işlem meşru olabilir ama saldırgan 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\philomena", "Account Name": "philomena", "Account Domain": "REFORM", "Logon ID": "0x2B03F", "Target Subject": "", "Process Information": "", "New Process ID": "0x400", "New Process Name": "C:\Windows\System32\dllhost.exe", "Token Elevation Type": "0x1938", "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:[04537C3-C473-4AC7-9E10-B2CE27C3A746]"}
2025-09-09 11:31:43.815 127.0.0.1
("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\philomena", "Account Name": "philomena", "Account Domain": "REFORM", "Logon ID": "0x3653C", "Target Subject": "", "Process Information": "", "New Process ID": "0x404", "New Process Name": "C:\Windows\System32\dllhost.exe", "Token Elevation Type": "0x1938", "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:[04537C3-C473-4AC7-9E10-B2CE27C3A746]"}

```

Scv.dll.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.

Field	Value
Event ID	4688
Date and Time	8.09.2025 15:37:35
Creator Process Name	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
Creator Process ID	0x18d4
Logon ID	0x8
Mandatory Label	High Mandatory Level
New Process ID	0x7ec
New Process Name	C:\Windows\System32\klist.exe

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 olmuş 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 şifrelenmenin AES256 ile gerçekleşip doğrulanmanın tamamlandığını gösterir.

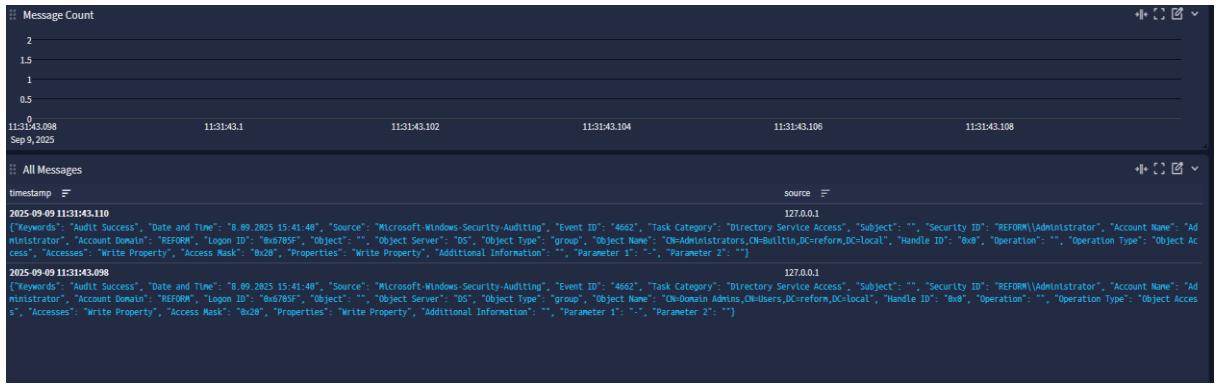
2025-09-09 11:31:42.834	127.0.0.1
("Keywords": "Audit Failure", "Date and Time": "8.09.2025 15:42:52", "Source": "Microsoft-Windows-Security-Auditing", "Event ID": "4771", "Task Category": "Kerberos Authentication Service", "Account Information": "", "Security ID": "REFORM\philomela", "Account Name": "philomela", "Service Information": "", "Service Name": "krbtgt/REFORM", "Network Information": "", "Client Address": "::1", "Client Port": "0", "Additional Information": "", "Ticket Options": "0x40010010", "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": "0x40010010", "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": "4760", "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": "0x40010010", "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 yönetici grubuna hem de domain yöneticileri grubuna eklendiğini kanıtlamaktadır.

All Messages	source
timestamp	source
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": "0x0769F", "Directory Service": "", "Name": "Reform-local", "Type": "Value Added", "Object": "", "DN": "CN=Administrators,CN=Builtin,DC=reform,DC=local", "GUID": "C9D00000-0000-0000-0000-000000000000", "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": "[86882830-08C-4137-BB5-33620E3A270]", "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": "0x0769F", "Directory Service": "", "Name": "Reform-local", "Type": "Value Added", "Object": "", "DN": "CN=Domain Admins,CN=Users,DC=reform,DC=local", "GUID": "C9D00000-0000-0000-0000-000000000000", "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": "[8DAAAC3B-8823-4C07-872A-A5BA169668B3]", "Application Correlation ID": "-")	

Event ID 5136



Write property



Event ID 4732



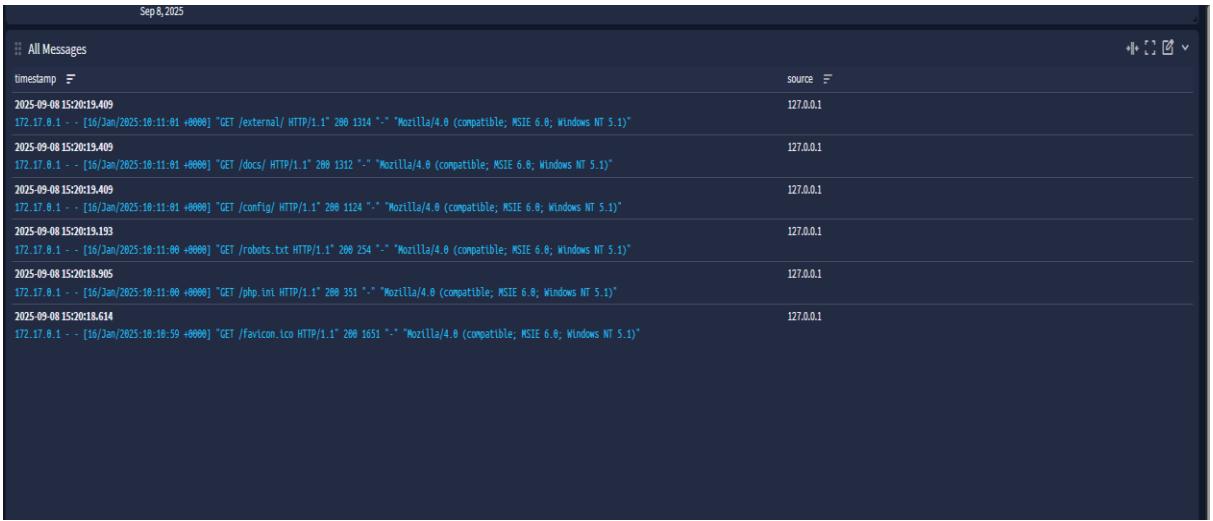
Event ID 4728

Path Travel Detected

Bu alarm, sistem üzerinde gerçekleştirilen dosya veya dizin 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 filtrelenmiş ve istekler bulundu.

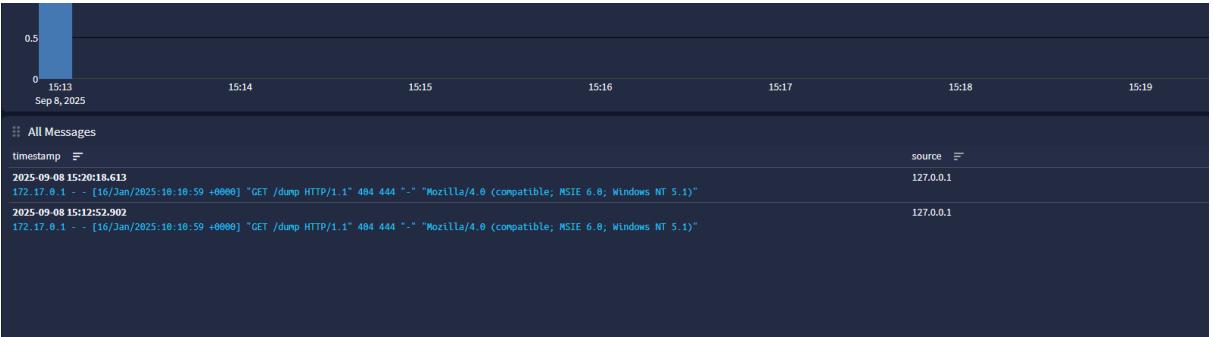
Web dizin sorgusu

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 açığamasına neden olabilmektedir. Daha kritik olarak php.ini dosyası da çağrılmış ve erişim sağlanmıştır bu dosya sistemin PHP yapılandırmasını içerdığı için veritabanı bağlantıları, hata logları veya kısıtlı fonksiyonlar gibi hassas bilgilerin sizmasına yol açabilir

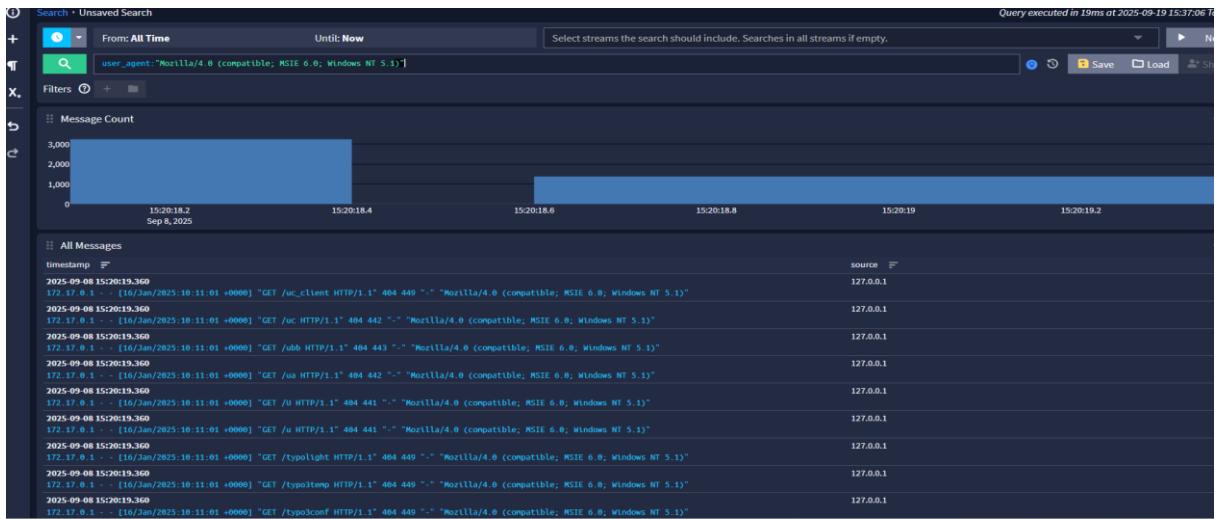


Mozilla

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.



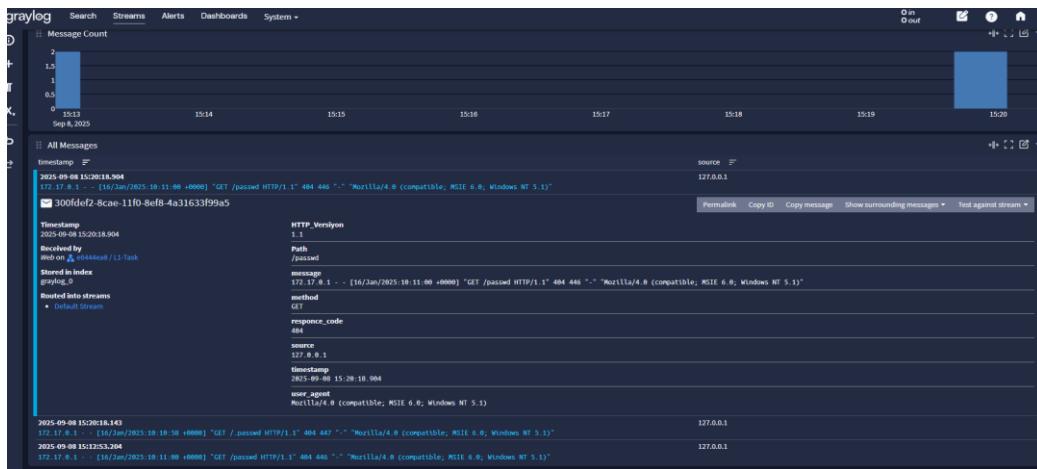
dump



Response 404

Passwd sorgusu

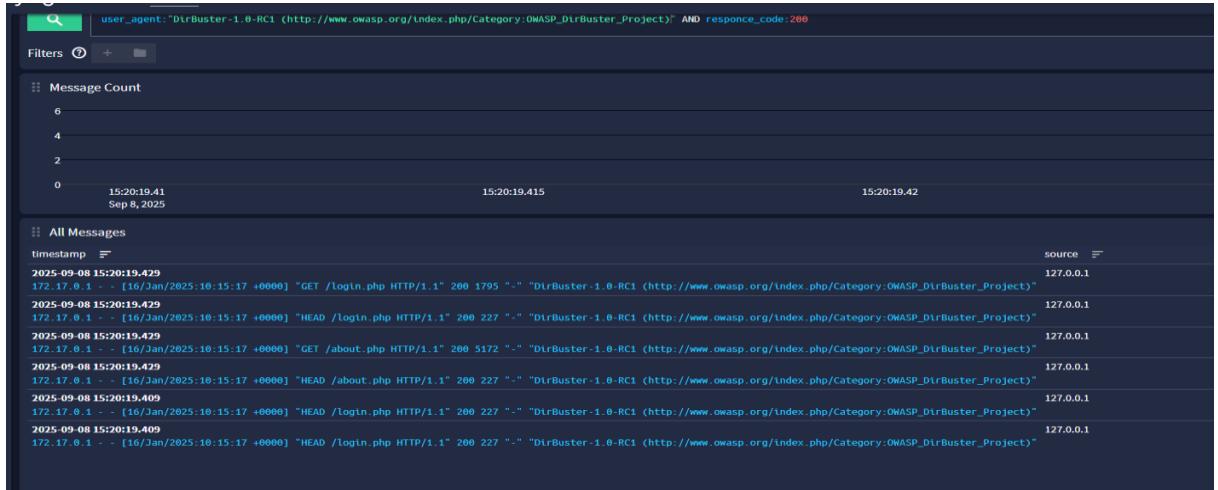
Bu esnada ise /passwd dizini ya da dosyası mevcut değil bunu response koduna(404) bakarak gözlemlenebiliriz. Saldırganın denediği path “/passwd” Unix/Linux sistemlerinde kritik şifre bilgilerini barındıran /etc/passwd dosyasına gönderme yapar. Genellikle path traversal saldırılarda saldırılar “..../..etc/passwd” ya da encode şeklinde, “%2e%2e%2f%2e%2e%2fetc%2fpasswd”, gibi denemeler yapar ama burada doğrudan /passwd olarak ilkel bir şekilde denenmiş.



Passwd

Dirbuster

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



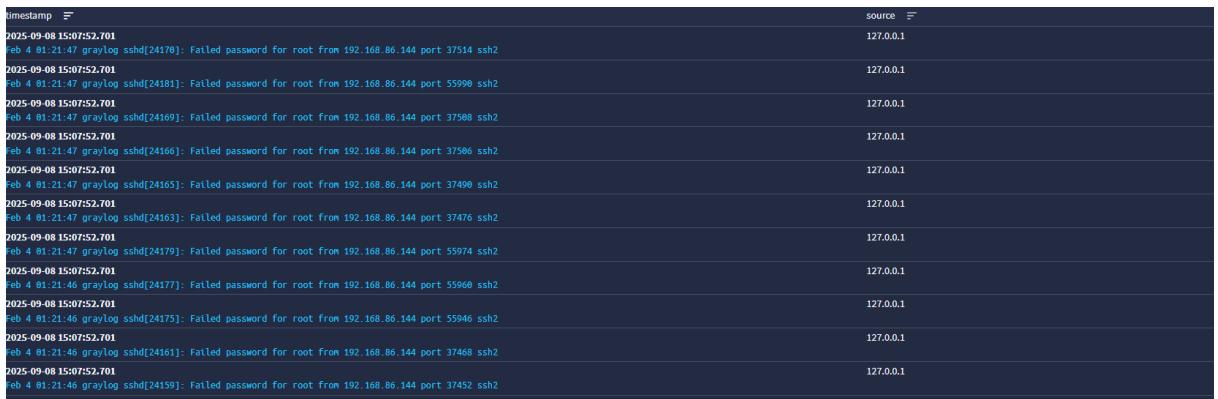
The screenshot shows a NetworkMiner capture window. At the top, there's a search bar with the query "user_agent:DirBuster-1.0-RC1 AND response_code:200". Below it, there are two sections: "Message Count" and "All Messages". The "Message Count" section shows a count of 6 messages. The "All Messages" section lists 6 log entries from 2025-09-08 at 15:20:19.415. Each entry shows a GET request to either "/Login.php" or "/about.php" with a status code of 200 and a source IP of 127.0.0.1. The timestamp for all entries is 15:20:19.415, and the date is Sep 8, 2025.

timestamp	source
2025-09-08 15:20:19.420	127.0.0.1
2025-09-08 15:20:19.420	127.0.0.1
2025-09-08 15:20:19.420	127.0.0.1
2025-09-08 15:20:19.420	127.0.0.1
2025-09-08 15:20:19.420	127.0.0.1
2025-09-08 15:20:19.409	127.0.0.1
2025-09-08 15:20:19.409	127.0.0.1
2025-09-08 15:20:19.409	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.



The screenshot shows a NetworkMiner capture window. It displays a series of log entries from 2025-09-08 at 15:07:52.701 to 2025-09-08 15:07:52.701. Each entry is a failed password attempt for the root user on port 192.168.86.144. The attempts are spread across various ports: 37514, 55990, 37508, 37476, 55974, 37490, 37476, 37468, and 37452. All attempts originate from the same source IP, 127.0.0.1.

timestamp	source
2025-09-08 15:07:52.701	127.0.0.1
Feb 4 01:21:47 graylog sshd[24170]: 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 37588 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 37586 ssh2	127.0.0.1
2025-09-08 15:07:52.701	127.0.0.1
Feb 4 01:21:47 graylog sshd[24105]: 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 girişimi
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 saldırının sistem üzerinde tam kontrol elde ettiğini işaret etmektedir. Ayrıca path traversal, DirBuster ile dizin keşfi ve SSH brute force denemeleri gibi aktiviteler, saldırının yalnızca iç ağıda değil, dışa açık servislerde de aktif keşif ve saldırı faaliyetlerinde bulunduğu 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 zayıfları nedeniyle güvenilirliğini yitirmiştir ve saldırıcılar bu zayıfları 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 zorlaştırmır.

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.)