Olay Müdahale Planı Nasıl Oluşturulur?

Olay tepkisi nedir?

Olay yanıtı, bir güvenlik olayı sürecini yönetmeye yönelik bir yaklaşımdır. Güvenlik olaylarına sistematik olarak yaklaşmak için bir olay müdahale planına ihtiyaç vardır. Başarılı bir olay müdahale planı aşağıdaki 6 aşamadan oluşur:

1- Hazırlık
2- Tanımlama
3- Kapsam
4- Eradikasyon
5- İyileşme
6- Alınan Dersler

1- Hazırlık

Merkezi Kayıt Sistemi Oluşturma

Büyük dosyaları yönetebilen merkezi bir log toplama sistemi ile tüm verilerin tek bir noktadan incelenebilmesi zaman tasarrufu açısından önemlidir.

Zaman Senkronizasyonu

Ağdaki tüm cihazlarda NTP'yi etkinleştirmek, toplanan günlüklerin zaman bilgilerini eşleştirmek için önemlidir.

Kullanıcı Hesabı Yönetimi

Personele ait farklı hesapların kullanıcı adlarının aynı ve diğer personelden farklı olması, herhangi bir olay durumunda kullanıcı aktivitelerinin izlenmesini kolaylaştırır.

Sistem ve Hizmet Hesaplarının Yönetimi

Kullanılan servislerin ve sistemlerin yöneticileri atanmalı ve gerektiğinde bu yöneticilere nasıl ulaşılacağına dair bir belge oluşturulmalıdır.

Varlık Yönetimi

Cihazlar, işletim sistemleri, yama sürümleri ve kritik durum gibi bilgilere anında erişim mevcut olmalıdır.

Güvenli İletişim

Gerekirse ekibin dahili ağdan bağımsız olarak iletişim kurması gerekebilir, bu gibi durumlarda cep telefonu veya ikincil e-postalar kullanılabilir.

Yasal İşlemler

Adli süreci kimin başlatacağı ve hangi durumlarda olay meydana gelmeden önce belirlenmelidir.

2- Tanımlama

Gözden Geçirme
Olası bir şüpheli olay için olayla ilgili ön bilgiler toplanmalıdır. Ardından durumun şüpheli bir olay olup olmadığına karar verilmelidir.

Görevlendirme
Olayı ilk inceleyecek kişi belirlenmelidir. Kişi inceleme hakkında notlar almalıdır.

Kontrol Listesinin Kullanılması
Olaylara tutarlı yanıtlar verilmesini sağlamak için yapılacak analiz için kontrol listeleri olmalıdır.

3- Kapsam

Olayı karakterize edin

Olayın belirlenmesi, alınacak aksiyonları belirleyeceğinden, gelen olayın türünün belirlenmesi önemlidir. ÖRNEK: DDoS, kötü amaçlı yazılım bulaşması, veri sızıntısı…

Harekete geçmek

Saldırganın yöntemine hızlı bir şekilde müdahale etmek için kullanılan tekniğe göre işlem yapılmalıdır. Ele geçirdiği bir hesap varsa hesap devre dışı bırakma, IP engelleme gibi basit önlemler hızlı bir şekilde yapılmalıdır.

Veri toplama

Güvenlik duvarı, ağ trafiği ve diğer günlüklerle birlikte geçici belleğin görüntüsü, inceleme için gerekli olacaktır.

İzolasyon

Güvenliği ihlal edilmiş sistemin fişini çekmek bir çözüm olabilir, izole etmek daha uygun bir çözümdür.

Olaydan etkilenen sistemler belirlendikten, saldırganın ağda yayılma olasılığı kesilip uçucu bilgiler toplandıktan sonra bir sonraki adıma geçilebilir.

4- Eradikasyon

Kök Nedenin Belirlenmesi

2. ve 3. aşamalarda elde edilen bilgilerle olayın kök nedeni belirlenmelidir. Saldırgan daha sonra tamamen atılmalıdır.

Rootkit Potansiyelini Belirleme

Sistemde rootkit'lerden şüpheleniliyorsa, disk temizlenmeli ve temiz bir yedek kurulmalıdır. Kurulumdan sonra mevcut uygulama ve sistemlerin en son güncellemeleri yüklenmelidir.

Savunmayı Geliştirin
İşletim sistemleri, kullanılan uygulamalar, ağ, DMZ vb. alanlarda savunma eksiklikleri belirlenmeli ve nasıl iyileştirme yapılacağı konusunda çalışmalar yapılmalıdır.

Güvenlik Açığı Taraması

Ağlar ve sistemler üzerindeki olası saldırı noktaları tespit edilmeli ve zafiyet taramaları yapılarak düzeltilmelidir.

Olayın tekrarlanmaması için gerekli düzenlemeler yapıldığında iyileşme aşamasına geçilebilir.

5- Kurtarma

Doğrulama

Günlüğe kaydetmenin, sistemlerin, uygulamaların, veritabanlarının ve diğer işlemlerin doğru çalıştığını doğrulayın.

Eski haline getirmek

Bu aşamada, geri yükleme işlemi koordine edilir.

izleme

Sistemler, tekrarlayan olaylar için izlenmelidir.

Tekrarlayan zararlı bir durum veya olağandışı bir faaliyet olmadığında bir sonraki adıma geçilir.

6- Alınan Dersler

Takip Raporu Yazma

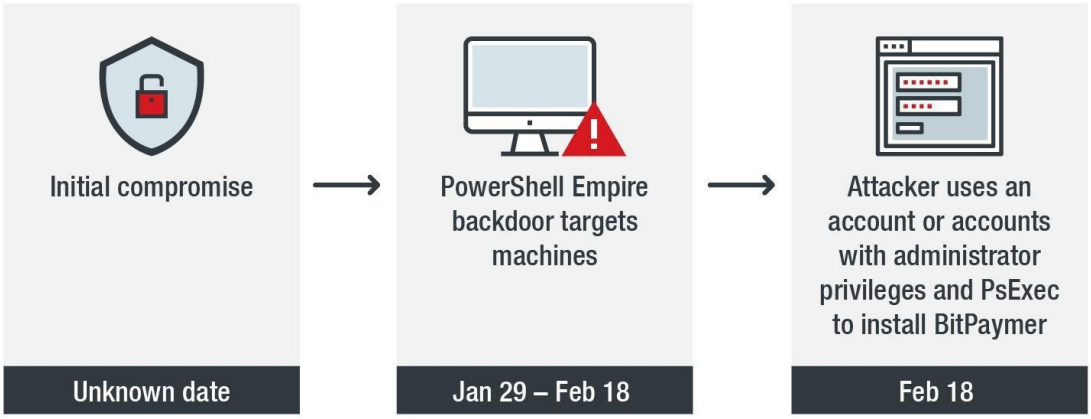
Raporda uzman ve yönetici ile yapılan incelemeler, müdahale planındaki iyi ve kötü çalışma aşamaları ve sürece ilişkin öneriler yer alır. Rapor, yöneticinin etkinliğin kapatıldığından emin olacağı şekilde yazılmalıdır.

Kullanıcılar ve Gruplar

Kullanıcılar bir işletim sisteminde olmazsa olmazdır. Sistemin güvenliğini sağlamak, verileri tanımlamak ve daha iyi bir kullanıcı deneyimi sağlamak için tüm işletim sistemlerinde kullanıcı sistemleri bulunmaktadır.

Bu yazımızda Linux işletim sistemi içerisinde yer alan kullanıcı sistemini inceleyeceğiz.

APT saldırı raporlarını incelediğimizde, siber saldırganların etki alanını tamamen tehlikeye atmak için yetkili kullanıcıyı ele geçirmeyi amaçladıklarını gözlemleyebiliriz. Günümüz dünyasında oldukça popüler hale gelen fidye yazılım saldırılarında, siber saldırganlar domain admin hesaplarını ele geçirerek domain içerisindeki tüm cihazlara fidye yazılımı indirmektedir.



Çoğu sistem yöneticisi, sorumluluğu altındaki cihazlarla ilgili periyodik olarak check-up yapmaz. Bu nedenle, bir kullanıcı devralındığında veya işletim sistemine yeni bir kullanıcı eklendiğinde, çok nadiren tanınır. Tanınma olasılığı çok düşük olduğundan, saldırganlar kalıcılığı sağlamak için sıklıkla bu yöntemi seçerler.

Ayrıca kullanıcılar için varsayılan olarak bulunan şifreler kurulum sırasında değiştirilmediği/unutulmadığı için saldırganlar işletim sistemine kolaylıkla erişebilmektedir.

Bir siber saldırının genel anatomisi incelenirse, saldırganlar internete açık bir hizmet üzerindeki zafiyetten faydalanarak sisteme erişirler ve bu hizmetler çoğunlukla yetkisiz hizmet hesapları olduğu için saldırganlar işletim sistemi üzerinde kullanıcıları tehlikeye atar. sistem üzerindeki ayrıcalıklarını artırmak için.

Olay müdahalecisi olarak, siber saldırganlar tarafından ele geçirilen, işletim sistemine eklenen veya işletim sisteminden çıkarılan kullanıcıları tespit edebilmeliyiz.

“Her şey bir dosyadır”

Her şey bir dosyadır, Unix'in tanımlayıcı özelliklerinden birini ve türevlerini tanımlar; belgeler, dizinler, sabit sürücüler, modemler, klavyeler, yazıcılar ve hatta bazı süreçler arası ve ağ iletişimleri gibi çok çeşitli giriş/çıkış kaynakları. dosya sistemi ad alanı aracılığıyla açığa çıkan basit bayt akışlarıdır. (Vikipedi)

UNIX dosya sistemi, kullanıcılar ve gruplar hakkında bilgi içeren kritik dosyalar içerir. Bir olay müdahalecisi olarak, bu dosyaların varlığını, dosya yapılarını ve bu dosyalardaki anormalliği tespit etme becerisini kazanmak gerekir.

Kullanıcı ve grupların bilgilerini içeren dosyalar aşağıda görüldüğü gibidir:

/etc/passwd

UNIX işletim sistemlerindeki en önemli dosyalardan biri şüphesiz /etc/passwd dosyasıdır. Bu dosya, kullanıcı adlarını, kullanıcının parolasını (kullanımdan kaldırılmış), UID/GID'yi, kullanıcının ana dizini ve kullanıcının kabuk bilgilerini içerir.

```
root@app:~# ls -lah /etc/passwd
-rw-r--r-- 1 root root 1.8K Oct 23 17:29 /etc/passwd
root@app:~#
```

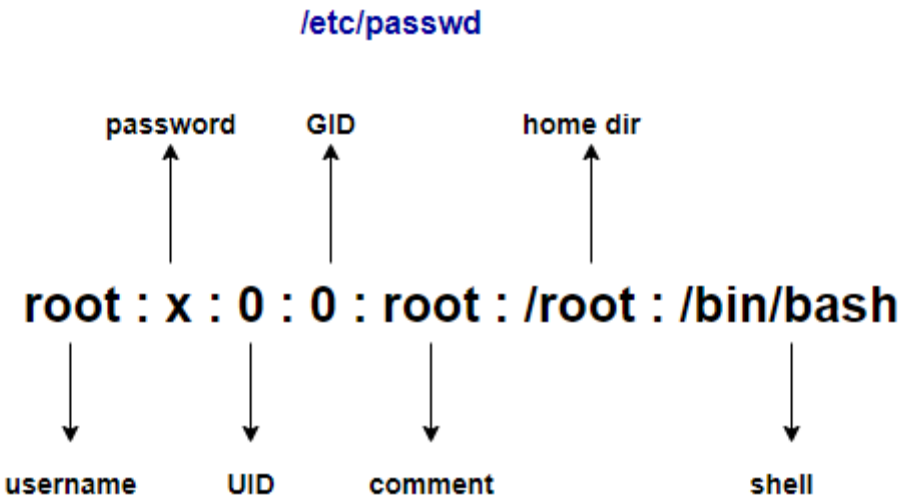
passwd isimli dosya root kullanıcısına aittir ve herkesin dosyayı okuma izni vardır. Bu nedenle saldırgan sistemdeki en düşük ayrıcalığa sahip kullanıcıyı tehlikeye atsa bile yine de cihazdaki kullanıcılar hakkında bilgi toplayabilir.

cat komutu ile *passwd* dosyasını herhangi bir dosya gibi okuyabilirsiniz .

cat /etc/passwd

```
root@app:~# cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-network:x:100:102:systemd Network Management,,,:/run/systemd:/usr/sbin/nologin
systemd-resolve:x:101:103:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin
systemd-timesync:x:102:104:systemd Time Synchronization,,,:/run/systemd:/usr/sbin/nologin
```

İlk bakışta */etc/passwd* dosyası kafa karıştırıcı görünebilir. Ancak, bu dosyadaki her satırın belirli bir biçimi vardır.



Dosya biçimini analiz ettiğimizde şunu görebiliriz:

- Kullanıcı adı, ilk iki nokta üst üste işaretinden önce her birinin başında yazılır,
- Parola, ilk iki nokta üst üste ile ikinci iki nokta arasına yazılır (bu kısım eskidir ve genellikle artık kullanılmamaktadır.)
- UID, ikinci iki nokta üst üste ile üçüncü iki nokta arasına yazılır,
- GID, üçüncü iki nokta üst üste ile dördüncü iki nokta arasına yazılır,
- Yorum, dördüncü kolon ile beşinci kolon arasında yer alır,
- Kullanıcının ana dizini beşinci kolon ile altıncı kolon arasında yazılır,
- Kullanıcı tarafından kullanılan kabuk, altıncı kolon ile yedinci kolon arasında yazılır.

Bir kullanıcının kabuğu passwd dosyasında "/usr/sbin/nologin" ise, kullanıcının işletim sistemine giriş yapamayacağı anlamına gelir.

```
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
```

Kullanıcının sisteme giriş yapamaması, kullanıcının sistemde komut çalıştıramayacağı anlamına gelmez. Örneğin, www-data kullanıcısının kabuğu "/usr/sbin/nologin"dir, ancak bir web uygulamasının güvenliği ihlal edildiğinde, saldırganlar genellikle www-data kullanıcısı ile sistemde komutlar yürütür.

/etc/shadow

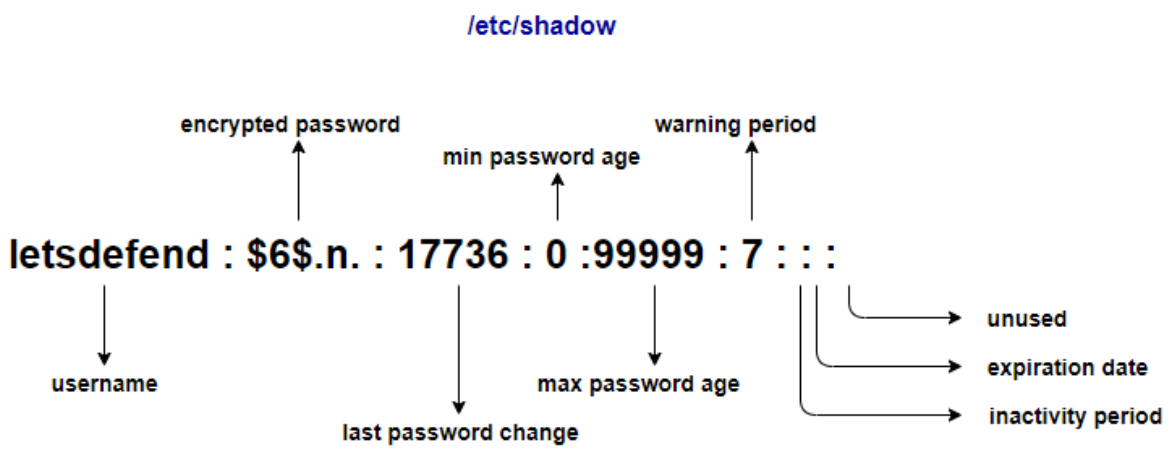
shadow dosyasında, kullanıcı parolalarının şifrelenmiş sürümleri vardır. Böylece saldırganlar tarafından en popüler dosyalardan biri haline geldi.

```
root@app:~# ls -lah /etc/shadow
-rw-r----- 1 root shadow 1021 Oct 23 17:29 /etc/shadow
root@app:~#
```

Bir dosyaya kullanıcı şifrelerinin eklenmesinin güvenlik riski oluşturabileceğini düşünebilirsiniz. Shadow dosyası yalnızca *root* kullanıcı ve *shadow* grubundaki kullanıcılar tarafından okunabilir ve parolalar şifreli tutulur. Bu dosyayı okumak tek başına bir anlam ifade etmiyor. Bir kullanıcının parolasını keşfetmek isteyen bir saldırgan, parolayı bulmak için onu kaba kuvvetle zorlamak zorundadır.

```
nagios:$6$LJBp6Hb4$RBLQ3S9cngte8yDmLr5T8QTMSvPWzleYltT4NLUVExqXv9SIOL.0KhTvqHiU5OxhUP5k4njgNAjUI1Ve6Ndjg0:18085:0:99999:7:::
```

Shadow dosya formatına bir göz atalım.



Dosya biçimini analiz ettiğimizde şunu görebiliriz:

- Kullanıcı adı, ilk iki nokta üst üste işaretinden önce yazılır,
- Şifrelenmiş parola, ilk iki nokta üst üste ile ikinci iki nokta arasına yazılır,
- İkinci iki nokta üst üste ile üçüncü iki nokta arasına son şifre değiştirme tarihi yazılır,
- Üçüncü kolon ile dördüncü kolon arasına kullanıcının şifresini değiştirmesi için gereken süre bilgisi yazılır,
- Dördüncü kolon ile beşinci kolon arasına gerekli şifre değiştirme zamanı bilgisi yazılır,
- Beşinci iki nokta ile altıncı iki nokta arasına şifrenin süresi dolmadan kullanıcıya ne zaman haber verileceği bilgisi yazılır,
- Altıncı kolon ile yedinci kolon arasına kullanıcı devre dışı bırakılmadan önce süresi dolan şifreyi değiştirmesi için kaç gün süre verileceği bilgisi yazılır,
- Hesabın ne zaman sona ereceği bilgisi yedinci ile sekiz iki nokta arasında yazılır,
- Sekizinci kolondan sonraki bölüm ileride kullanılmak üzere oluşturulmuştur ancak şu anda kullanılmadığı için boş bırakılmıştır.

/etc/group

/etc/group dosyası, grupları ve bu gruplara hangi kullanıcıların dahil edildiğine ilişkin bilgileri içerir.

Güvenliği ihlal edilmiş kullanıcıları belirlemek, bir siber güvenlik olayındaki riski anlamak için yeterli değildir. Kullanıcı grupları da kontrol edilmelidir.

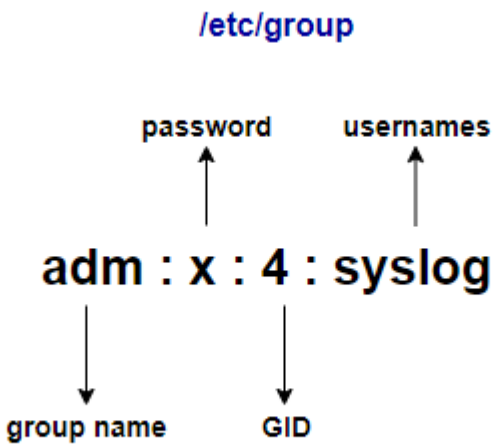
Özel bir konfigürasyon yapılmadıysa *www-data* kullanıcısı düşük yetkiye sahip bir kullanıcıdır. *Ancak bir siber olay riskini belirlerken " www-data* kullanıcısının güvenliği ihlal edilmiş ancak ayrıcalık seviyesi düşük olduğu için risk düşük " şeklinde bir bakış açısı benimsemek yanlış olacaktır . Saldırgan *www-data* kullanıcısını yüksek ayrıcalıklı bir gruba dahil ederse, www-data kullanıcısı neredeyse root kullanıcısı kadar ayrıcalığa sahip olabilir.

```
root@app:~# ls -lah /etc/group
-rw-r--r-- 1 root root 781 Oct 23 17:29 /etc/group
root@app:~#
```

Grup isimli dosya kök kullanıcıya aittir ve herkesin okuma izni vardır. Bu nedenle saldırgan sisteme en düşük ayrıcalıklara sahip kullanıcı üzerinden erişse bile yine de cihazdaki gruplar hakkında bilgi toplayabilir.

```
root@app:~# cat /etc/group
root:x:0:
daemon:x:1:
bin:x:2:
sys:x:3:
adm:x:4:syslog
tty:x:5:syslog
disk:x:6:
lp:x:7:
mail:x:8:
news:x:9:
uucp:x:10:
```

Dosya formatına bir göz atalım.



Dosya biçimini analiz ettiğimizde şunu görebiliriz:

- Grup adı, ilk iki nokta üst üste işaretinden önce her birinin başında yazılır,
- Parola, ilk iki nokta üst üste ile ikinci iki nokta arasına yazılır (bu kısım eskidir ve genellikle artık kullanılmamaktadır.)
- GID, ikinci iki nokta üst üste ile üçüncü iki nokta arasına yazılır,
- Kullanıcılar ve kullanıcı adları üçüncü iki nokta üst üste işaretinden sonra yazılır

/etc/sudoers

sudoers dosyası, sudo komutunu kimlerin hangi koşullar altında çalıştırabileceği hakkında bilgi içerir.

```
root@app:~# cat /etc/sudoers
#
# This file MUST be edited with the 'visudo' command as root.
#
# Please consider adding local content in /etc/sudoers.d/ instead of
# directly modifying this file.
#
# See the man page for details on how to write a sudoers file.
#
Defaults        env_reset
Defaults        mail_badpass
Defaults        secure_path="/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/snap/bin"

# Host alias specification

# User alias specification

# Cmnd alias specification

# User privilege specification
root    ALL=(ALL:ALL) ALL

# Members of the admin group may gain root privileges
%admin ALL=(ALL) ALL

# Allow members of group sudo to execute any command
%sudo   ALL=(ALL:ALL) ALL

# See sudoers(5) for more information on "#include" directives:

#includedir /etc/sudoers.d
root@app:~#
```

Diğer dosyalardan farklı olarak, *sudoers* dosyası varsayılan olarak dosya biçimi hakkında yorumlar içerir.

<user list> <host list> = <operator list> <tag list> <command list>

- **Kullanıcı Listesi:** Hangi kullanıcıların belirli yetkilere sahip olacağını belirler.
- **Host List:** Hangi hostların belirli yetkilere sahip olacağını belirler.
- **Operatör Listesi:** <user list> içindeki kullanıcıların hangi kullanıcı adına komutları çalıştıracağını belirler.
- **Etiket Listesi:** " *PASSWD* ", " *NOPASSWD* " ve " *NOEXEC* " değerlerine sahip olabilir ve komutu çalıştırmak için parolaya ihtiyaç duyup duymadıklarını belirler.
- **Komut Listesi:** Komutları içerir

```
%admin ALL = (ALL) ALL
```

Diğer Önemli Dosyalar

Bu dosyaların dışında kullanıcı oturum açma işlemleri hakkında bilgi içeren farklı dosyalar da bulunmaktadır.

- **var/run/utmp** : sistemin mevcut durumunun, sistem önyükleme süresinin (çalışma süresi tarafından kullanılan), terminallerde, çıkışların, sistem olaylarının vb.
- **/var/log/wtmp** : tarihsel bir utmp işlevi görür
- **/var/log/btmp** : başarısız oturum açma girişimlerini kaydeder

Olay Müdahalesi

analiz et

Sistem Üzerindeki Kullanıcıların Belirlenmesi

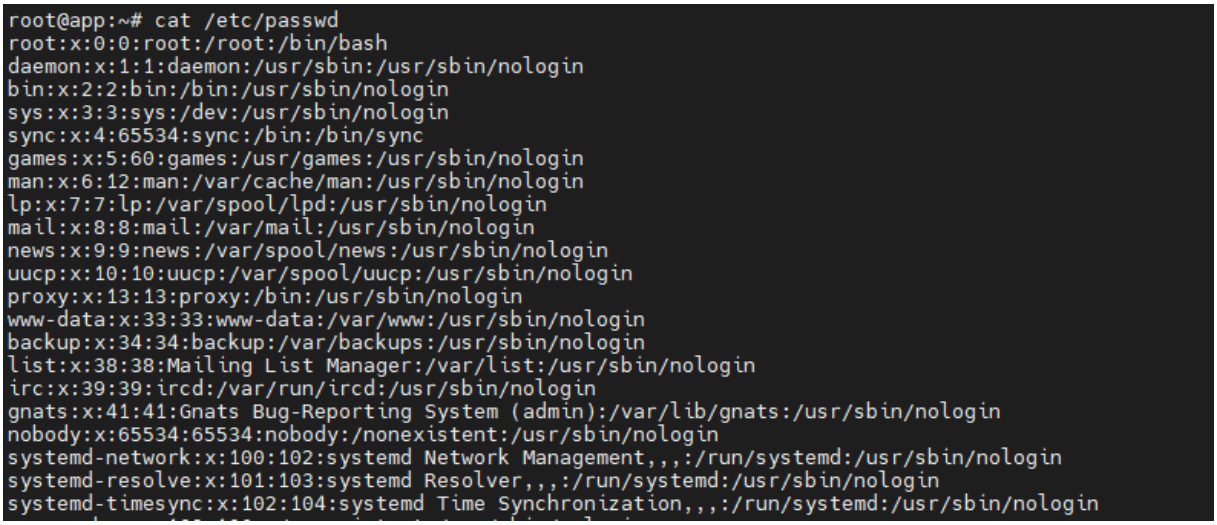
Saldırganlar, kalıcılığı sağlamak için yeni kullanıcılar ekler ve mevcut kullanıcıları değiştirir. Olay müdahalecisi olarak bu kullanıcıları tespit etmek ve bu kullanıcıları yok etme adımında risk oluşturmayacak şekilde kaldırmak/düzenlemek gerekir.

Olay müdahale sürecinde sistemdeki kullanıcıları kontrol ederken, uygulama/sunucu sahibinden cihazda olması gereken kullanıcıların listesini alarak, tehlikeye atılan sistemi temiz sistemle karşılaştırmak gerekebilir. Kullanıcı listesi alınırken siber öncesi olaydan anlık görüntülerin kullanılması daha doğru olacaktır.

Analizimizi sistemdeki kullanıcılara özel yapabilmek için öncelikle sistemdeki kullanıcıları tanımlamamız gerekmektedir.

/etc/passwd dosyası okunarak sistemde tanımlanan kullanıcılar belirlenebilir.

cat /etc/passwd



Saldırganlar , kendilerinin tespit edilmesini önlemek için oluşturdukları kullanıcılar için *destek, hizmet, dev, admin ve sysadmin gibi isimleri tercih eder.* Bu isimlere sahip kullanıcılara dikkat etmeliyiz.

passwd dosyası yanlış izinlere sahipse, passwd dosyasını düzenleyerek kullanıcılar tehlikeye girebilir. Saldırganlar, kullanıcı adlarının yanındaki "x" değerini kendi oluşturdukları şifre ile değiştirerek kullanıcıları ele geçirebilirler. *Bu nedenle olay müdahalesi sırasında passwd* dosyasındaki şifre alanındaki bilgiler dikkatli bir şekilde kontrol edilmelidir.

Ayrıca kullanıcıların kabuk bilgileri kontrol edilmelidir. Shell'e sahip olmaması gereken kullanıcıların Shell bilgileri iki kez kontrol edilmelidir.

Saldırgan auth.log dosyasını temizlemediyse, *yeni* oluşturulan kullanıcıları auth.log dosyası aracılığıyla tespit etmek mümkündür.

tail /var/log/auth.log

```
remnux@remnux:~/Desktop$ tail /var/log/auth.log
Oct 26 17:59:38 remnux sudo:   remnux : TTY=pts/1 ; PWD=/home/remnux/Desktop ; USER=root ; COMMAND=/u
sr/sbin/adduser support
Oct 26 17:59:38 remnux sudo: pam_unix(sudo:session): session opened for user root by (uid=0)
Oct 26 17:59:38 remnux groupadd[6368]: group added to /etc/group: name=support, GID=1001
Oct 26 17:59:38 remnux groupadd[6368]: group added to /etc/gshadow: name=support
Oct 26 17:59:38 remnux groupadd[6368]: new group: name=support, GID=1001
Oct 26 17:59:38 remnux useradd[6374]: new user: name=support, UID=1001, GID=1001, home=/home/support,
 shell=/bin/bash, from=/dev/pts/1
Oct 26 17:59:40 remnux passwd[6386]: pam_unix(passwd:chauthtok): password changed for support
Oct 26 17:59:40 remnux passwd[6386]: gkr-pam: couldn't update the login keyring password: no old pass
word was entered
Oct 26 17:59:47 remnux chfn[6387]: changed user 'support' information
Oct 26 17:59:48 remnux sudo: pam_unix(sudo:session): session closed for user root
remnux@remnux:~/Desktop$
```

auth.log dosyasında “useradd” kelimesini aratarak yeni oluşturulan kullanıcıları bulabilirsiniz.

grep useradd /var/log/auth.log

```
remnux@remnux:~/Desktop$ grep useradd /var/log/auth.log
Oct 26 17:59:38 remnux useradd[6374]: new user: name=support, UID=1001, GID=1001, home=/home/support,
 shell=/bin/bash, from=/dev/pts/1
remnux@remnux:~/Desktop$
```

Auth.log dosyasında “passwd” kelimesini aratarak şifresi değişen kullanıcıları belirleyebilirsiniz.

grep passwd /var/log/auth.log

```
remnux@remnux:~/Desktop$ grep passwd /var/log/auth.log
Oct 26 17:59:40 remnux passwd[6386]: pam_unix(passwd:chauthtok): password changed for support
Oct 26 17:59:40 remnux passwd[6386]: gkr-pam: couldn't update the login keyring password: no old pass
word was entered
remnux@remnux:~/Desktop$
```

Kullanıcı İzinlerinin Belirlenmesi

Daha önce yazımızda belirttiğimiz gibi, güvenliği ihlal edilmiş kullanıcıları tespit etmek, riski belirlemek için yeterli değildir. Kullanıcılar belirlendikten sonra, bu kullanıcıların dahil olduğu gruplar ve bu kullanıcılara özel tanımlanmış yetkiler de belirlenmelidir.

İyi bir başlangıç noktası, kullanıcıların ait olduğu grupları incelemek ve kullanıcının izinlerini kontrol etmektir.

/etc/group dosyası üzerinden grupları ve gruplara dahil olan kullanıcıları incelememiz gerekiyor . Grup dosyasının içeriği cat komutu kullanılarak görüntülenebilir.

```
cat /etc/group
```

```
remnux@remnux:~$ cat /etc/group
root:x:0:
daemon:x:1:
bin:x:2:
sys:x:3:
adm:x:4:syslog,remnux
tty:x:5:syslog
```

İncelemelerimizi yaparken kritik gruplara ve bu gruplarda yer alan kullanıcılara dikkat etmeliyiz. Bu gruplara dahil edilmemesi gereken kullanıcılar belirlenmelidir. Örneğin, *www-data* kullanıcısının sudo grubuna dahil olması kesinlikle şüphelidir. Kritik gruplardan bazıları aşağıda belirtildiği gibidir:

root

adm

shadow

sudo

Kullanıcı veya grupların yetkilerini anlamak için kontrol edilmesi gereken bir diğer dosya da *"/etc/sudoers" dosyasıdır.* Bu dosyada hangi kullanıcı ve grupların sudo yetkisini ne ölçüde kullanabileceğine dair bilgiler bulunmaktadır.

cat /etc/sudoers

```
remnux@remnux:~$ sudo cat /etc/sudoers
#
# This file MUST be edited with the 'visudo' command as root.
#
# Please consider adding local content in /etc/sudoers.d/ instead of
# directly modifying this file.
#
# See the man page for details on how to write a sudoers file.
#
Defaults        env_reset
Defaults        mail_badpass
Defaults        secure_path="/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:

# Host alias specification

# User alias specification
```

Sudoers dosyasında yetkisiz kullanıcılar ve sistem ihlaline neden olabilecek sudo yetkileri tanımlanmamalıdır. Ayrıca bu dosya üzerinde hatalı konfigürasyonlar tespit edilmelidir.

auth.log dosyasında *"groupadd" ve "usermod"* kelimelerini aratarak grup işlemlerini listeleyebilirsiniz. Saldırının tarih aralığındaki grup değişikliklerinin listelenmesi, saldırganın gerçekleştirdiği eylemlerin takibini kolaylaştıracaktır.

grep groupadd /var/log/auth.log

```
remnux@remnux:~/Desktop$ grep groupadd /var/log/auth.log
Oct 26 17:59:38 remnux groupadd[6368]: group added to /etc/group: name=support, GID=1001
Oct 26 17:59:38 remnux groupadd[6368]: group added to /etc/gshadow: name=support
Oct 26 17:59:38 remnux groupadd[6368]: new group: name=support, GID=1001
remnux@remnux:~/Desktop$
```

grep usermod /var/log/auth.log

```
remnux@remnux:~/Desktop$ grep usermod /var/log/auth.log
Oct 26 18:03:40 remnux sudo:   remnux : TTY=pts/1 ; PWD=/home/remnux/Desktop ; USER=root ; COMMAND=/u
sr/sbin/usermod -a -G admin support
Oct 26 18:03:48 remnux sudo:   remnux : TTY=pts/1 ; PWD=/home/remnux/Desktop ; USER=root ; COMMAND=/u
sr/sbin/usermod -a -G sudo support
Oct 26 18:03:48 remnux usermod[6408]: add 'support' to group 'sudo'
Oct 26 18:03:48 remnux usermod[6408]: add 'support' to shadow group 'sudo'
remnux@remnux:~/Desktop$ S
```

Sisteme Giriş Yapan Kullanıcıların Belirlenmesi

Çoğu linux sisteminde varsayılan olarak yüklenen bazı araçlar yardımıyla işletim sistemi üzerinde aktif bağlantısı olan kullanıcılar listelenebilmektedir. Olay müdahale prosedürü sırasında cihazın bütünlüğünü korumak için mümkün olduğunca az sayıda yeni araç kurmanızı öneririz. GNU/Linux'ta oturum açan kullanıcıları tespit etmek için kullanabileceğimiz birkaç farklı araç vardır.

w, kim, kullanıcılar ve son araçlar varsayılan olarak GNU/Linux'a dahildir. Bu araçlar yardımıyla sisteme giriş yapmış kullanıcıları tespit edebilirsiniz.

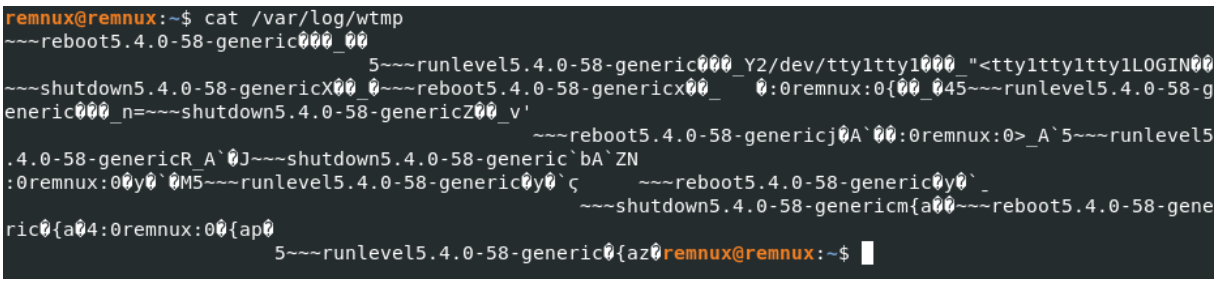
Bu araçların kendi avantajları ve dezavantajları vardır. Ancak, "last" aracı seçmek, daha fazla bilgi ve geçmiş veri sağladığı için olay müdahale sürecini hızlandıracaktır. Herhangi bir parametre verilmezse, tüm kullanıcıların giriş geçmişini verecektir.

Last

```
remnux@remnux:~$ last
remnux   :0           :0               Thu Oct 28 17:05   still logged in
reboot   system boot  5.4.0-58-generic Thu Oct 28 17:05   still running
remnux   :0           :0               Fri May  7 13:32 - down  (174+03:32)
reboot   system boot  5.4.0-58-generic Fri May  7 13:32 - 17:04 (174+03:32)
remnux   :0           :0               Thu Mar  4 17:29 - down   (00:13)
reboot   system boot  5.4.0-58-generic Thu Mar  4 20:29 - 17:42  (-2:46)
remnux   :0           :0               Thu Dec 17 19:10 - down   (00:03)
reboot   system boot  5.4.0-58-generic Thu Dec 17 19:10 - 19:14  (00:03)
remnux   tty1                          Thu Dec 17 18:20 - down   (00:49)
reboot   system boot  5.4.0-58-generic Thu Dec 17 18:20 - 19:10  (00:49)

wtmp begins Thu Dec 17 18:20:25 2020
remnux@remnux:~$
```

Son komut bu bilgiyi *"/var/log/wtmp"* dosyasından alır. Aynı bilgiyi bu dosyayı okuyarak da elde edebilirsiniz, ancak *son* komut onu daha okunaklı bir biçimde sağlar.

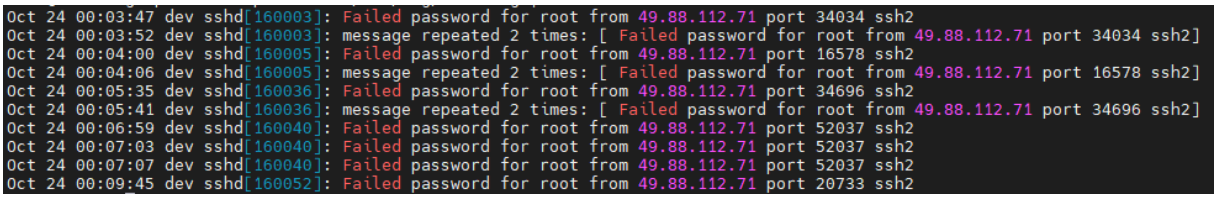
cat /var/log/wtmp



/var/log/auth.log dosyası, SSH üzerinden sisteme giriş yapan kullanıcıları tespit etmek için incelenebilir. Bu dosya, başarılı oturum açmaların yanı sıra başarısız oturum açma işlemlerini de içerir. Bu sayede auth.log dosyası içinden brute-force saldırılarını tespit edebiliyoruz.

Başarısız olan login denemelerini aşağıdaki komut ile listeleyebilirsiniz.

grep "Failed password" /var/log/auth.log



Alternatif olarak, Journalctl komutu ile başarısız SSH girişleri belirlenebilir.

journalctl _SYSTEMD_UNIT=ssh.service | egrep "Failed|Failure"

SSH Yapabilecek Kullanıcıların Belirlenmesi

Olay müdahalesi sırasında, cihaza uzaktan SSH yapabilen kullanıcıları tespit etmek gerekebilir. "Uzak Masaüstü Kullanıcıları" grubunda yer alan kullanıcıları listeleyerek Windows işletim sistemlerinde RDP yapabilen kullanıcılar hakkında bilgi edinebilirsiniz. Ancak, Linux'ta benzer bir grup yoktur. SSH yapabilen kullanıcıları tespit edebilmek için aşağıdaki adımlar izlenmelidir.

1. */etc/passwd* dosyası okunarak sistemdeki kullanıcılar tespit edilir.
2. Geçerli bir kabuğu olmayan kullanıcılar listeden çıkarılır.
3. Geçerli şifreleri olmayan kullanıcılar listeden çıkarılır.
4. *SSH izinlerine sahip kullanıcılar /etc/ssh/sshd_config* içinde algılanır . Bu dosyada "AllowUsers" belirtilmişse diğer kullanıcılar SSH hizmetini kullanamaz demektir.

eradikasyon

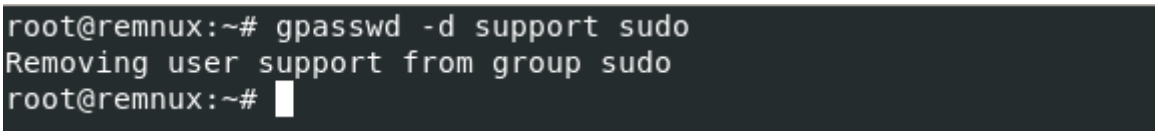
Olay müdahalesi sonunda sistem, siber saldırıdan etkilenmeyecek şekilde çalışır duruma getirilmelidir.

Saldırgan tarafından eklenen kullanıcılar sistemden silinmelidir. Aşağıdaki komut ile kullanıcıyı ve kullanıcının ana dizinini silebilirsiniz.

userdel -r **USERNAME**

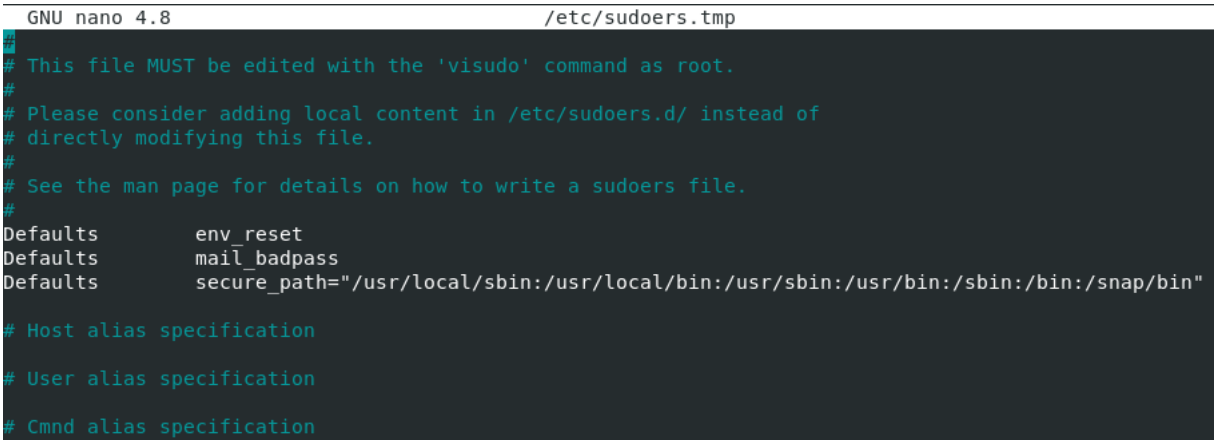
Yetkisiz kullanıcılar, yetkileri yüksek gruplardan çıkarılmalıdır. Aşağıdaki komut ile kullanıcıyı gruptan çıkarabilirsiniz.

gpasswd -d **USERNAME GROUP**



Kullanıcıya verilen sudo yetkisi kaldırılmalıdır. sudo yetkilendirmelerini visudo komutuyla düzenleyebilirsiniz.

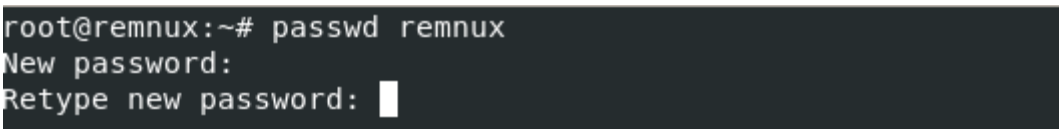
visudo



ullanıcıların silinmemesi gereken şifreleri değiştirilmeli ve SSH anahtarları yeniden oluşturulmalıdır.

Kullanıcının parolasını değiştirmek için passwd komutunu kullanabilirsiniz.

passwd **USERNAME**



Kullanıcının SSH Anahtarlarını yenilemek için önce eski anahtarların silinmesi gerekir. Ardından yeni bir SSH Anahtarı oluşturulmalıdır.

Mounts

UNIX işletim sistemlerinde kendi cihazınıza farklı bir dosya sistemi bağlayabilirsiniz. Saldırganlar elbette bu özelliği kendi amaçları için kullanmak için yöntemler geliştirirler.

Fidye yazılımı saldırıları şu anda günümüzde önemli sayıda siber saldırı oluşturuyor. Siber tehdit aktörleri, ağda bulunan tüm cihazlara fidye yazılımı yükleyerek sistemin çalışmasını durdurur ve sahiplerinin önemli bilgilere erişimini engelleyerek mağdurları fidye ödemeye zorlar.

Kurumsal ağ topolojilerini incelediğimizde hemen hemen her şirketin bir dosya paylaşım sunucusu olduğunu görebiliriz. Fidye yazılımı saldırıları sırasında dosya paylaşım sunucuları, saldırganların ana hedefi haline geldi.

Saldırganlar, fidye yazılımı saldırıları sırasında dosya paylaşım sunucularını iki amaç için kullanır:

1. Dosya paylaşım sunucuları genellikle kritik verilere sahip olduğundan, sahiplerinin önemli bilgilere erişimini engellemek ve onları fidye ödemeye zorlamak için fidye yazılımları bu sunuculara yüklenir.
2. Fidye yazılımı kötü amaçlı yazılımları dosya paylaşım sunucularında barındırarak, saldırganın erişim sağladığı cihazlardan dosya paylaşım sunucusu aracılığıyla fidye yazılım kötü amaçlı yazılımları yüklemek.

Bir siber saldırı sırasında olay müdahale görevlisinin yapması gereken kontrollerden biri, güvenliği ihlal edilmiş cihazlar tarafından monte edilen dosya sistemlerinden herhangi birinin siber saldırıdan etkilenip etkilenmediğini kontrol etmektir.

Ne yazık ki, takma/çıkarma günlüğü yok. Bu nedenle, saldırgan bir mount prosedürü yürüttüyse ve ardından bağlantısını kestiyse, bunu tanımlayamayız. Ancak bazen, dmesg içindeki bağlamalarla ilgili günlükleri görebiliriz.

dmesg | grep mount

```
remnux@remnux:~/Desktop$ dmesg | grep mount
[    2.797615] EXT4-fs (sda5): mounted filesystem with ordered data mode. Opts: (null)
[    3.854338] systemd[1]: Set up automount Arbitrary Executable File Formats File System Automount
Point.
[    3.876185] systemd[1]: Starting Remount Root and Kernel File Systems...
[    3.904565] EXT4-fs (sda5): re-mounted. Opts: errors=remount-ro
[    3.905650] systemd[1]: Finished Remount Root and Kernel File Systems.
[    4.006036] systemd[1]: Mounting VMware vmblock fuse mount...
[    4.025270] systemd[1]: Mounted VMware vmblock fuse mount.
remnux@remnux:~/Desktop$
```

Mount prosedürleri loglanmadığı için geriye doğru arama yapamıyoruz. Ancak yine de cihaza takılı olan dosya sistemlerini belirleyerek analizlerimizi gerçekleştirebiliriz.

Mount

mount komutu ile mount edilen dosya sistemlerini listeleyebilirsiniz.

mount

```
remnux@remnux:~/Desktop$ mount
sysfs on /sys type sysfs (rw,nosuid,nodev,noexec,relatime)
proc on /proc type proc (rw,nosuid,nodev,noexec,relatime)
udev on /dev type devtmpfs (rw,nosuid,noexec,relatime,size=1972656k,nr_inodes=493164,mode=755)
devpts on /dev/pts type devpts (rw,nosuid,noexec,relatime,gid=5,mode=620,ptmxmode=000)
tmpfs on /run type tmpfs (rw,nosuid,nodev,noexec,relatime,size=400228k,mode=755)
/dev/sda5 on / type ext4 (rw,relatime,errors=remount-ro)
securityfs on /sys/kernel/security type securityfs (rw,nosuid,nodev,noexec,relatime)
tmpfs on /dev/shm type tmpfs (rw,nosuid,nodev)
tmpfs on /run/lock type tmpfs (rw,nosuid,nodev,noexec,relatime,size=5120k)
tmpfs on /sys/fs/cgroup type tmpfs (ro,nosuid,nodev,noexec,mode=755)
cgroup2 on /sys/fs/cgroup/unified type cgroup2 (rw,nosuid,nodev,noexec,relatime,nsdelegate)
cgroup on /sys/fs/cgroup/systemd type cgroup (rw,nosuid,nodev,noexec,relatime,xattr,name=systemd)
pstore on /sys/fs/pstore type pstore (rw,nosuid,nodev,noexec,relatime)
none on /sys/fs/bpf type bpf (rw,nosuid,nodev,noexec,relatime,mode=700)
cgroup on /sys/fs/cgroup/rdma type cgroup (rw,nosuid,nodev,noexec,relatime,rdma)
```

Findmnt

Findmnt, monte edilmiş dosya sistemlerini listelemek için kullanabileceğimiz başka bir araçtır. Diğer seçeneklere göre görsel olarak daha hoş bir çıktı olduğu için diğer çıktıları anlamak için vakit kaybetmek yerine findmnt komutunu kullanabiliriz.

Findmnt

```
remnux@remnux:~/Desktop$ findmnt
TARGET                                SOURCE      FSTYPE     OPTIONS
/                                     /dev/sda5   ext4       rw,relatime,errors=remount-ro
├─/sys                                sysfs       sysfs      rw,nosuid,nodev,noexec,relatime
│ ├─/sys/kernel/security              securityfs  securityf  rw,nosuid,nodev,noexec,relatime
│ ├─/sys/fs/cgroup                    tmpfs       tmpfs      ro,nosuid,nodev,noexec,mode=755
│ │ ├─/sys/fs/cgroup/unified          cgroup2     cgroup2    rw,nosuid,nodev,noexec,relatime,nsdelega
│ │ ├─/sys/fs/cgroup/systemd          cgroup      cgroup     rw,nosuid,nodev,noexec,relatime,xattr,na
│ │ ├─/sys/fs/cgroup/rdma             cgroup      cgroup     rw,nosuid,nodev,noexec,relatime,rdma
│ │ ├─/sys/fs/cgroup/cpuset           cgroup      cgroup     rw,nosuid,nodev,noexec,relatime,cpuset
│ │ ├─/sys/fs/cgroup/hugetlb          cgroup      cgroup     rw,nosuid,nodev,noexec,relatime,hugetlb
│ │ ├─/sys/fs/cgroup/devices          cgroup      cgroup     rw,nosuid,nodev,noexec,relatime,devices
│ │ ├─/sys/fs/cgroup/cpu,cpuacct      cgroup      cgroup     rw,nosuid,nodev,noexec,relatime,cpu,cpua
│ │ ├─/sys/fs/cgroup/net_cls,net_prio cgroup      cgroup     rw,nosuid,nodev,noexec,relatime,net_cls,
│ │ ├─/sys/fs/cgroup/freezer          cgroup      cgroup     rw,nosuid,nodev,noexec,relatime,freezer
│ │ ├─/sys/fs/cgroup/pids             cgroup      cgroup     rw,nosuid,nodev,noexec,relatime,pids
│ │ ├─/sys/fs/cgroup/perf_event       cgroup      cgroup     rw,nosuid,nodev,noexec,relatime,perf_eve
│ │ ├─/sys/fs/cgroup/blkio            cgroup      cgroup     rw,nosuid,nodev,noexec,relatime,blkio
│ │ └─/sys/fs/cgroup/memory           cgroup      cgroup     rw,nosuid,nodev,noexec,relatime,memory
│ ├─/sys/fs/pstore                    pstore      pstore     rw,nosuid,nodev,noexec,relatime
│ ├─/sys/fs/bpf                       none        bpf        rw,nosuid,nodev,noexec,relatime,mode=700
```

Df

Df, diskler hakkında bilgi almak için kullanabileceğimiz bir araçtır. -aTh parametresi ile mount edilmiş dosya sistemlerini listeleyebiliriz.

df -aTh

```
remnux@remnux:~/Desktop$ df -aTh
Filesystem     Type                Size  Used Avail Use% Mounted on
sysfs          sysfs                  0     0     0    - /sys
proc           proc                   0     0     0    - /proc
udev           devtmpfs             1.9G     0  1.9G   0% /dev
devpts         devpts                 0     0     0    - /dev/pts
tmpfs          tmpfs                391M  1.7M  390M   1% /run
/dev/sda5      ext4                  59G   14G   42G  25% /
securityfs     securityfs             0     0     0    - /sys/kernel/security
tmpfs          tmpfs                2.0G     0  2.0G   0% /dev/shm
tmpfs          tmpfs                5.0M     0  5.0M   0% /run/lock
tmpfs          tmpfs                2.0G     0  2.0G   0% /sys/fs/cgroup
cgroup2        cgroup2                0     0     0    - /sys/fs/cgroup/unified
cgroup         cgroup                 0     0     0    - /sys/fs/cgroup/systemd
```

/proc/mounts

Aktif olarak bağlanan dosya sistemlerini tanımlamak için /proc/mounts dosyasını okuyabiliriz.

cat /proc/mounts

```
remnux@remnux:~/Desktop$ cat /proc/mounts
sysfs /sys sysfs rw,nosuid,nodev,noexec,relatime 0 0
proc /proc proc rw,nosuid,nodev,noexec,relatime 0 0
udev /dev devtmpfs rw,nosuid,noexec,relatime,size=1972656k,nr_inodes=493164,mode=755 0 0
devpts /dev/pts devpts rw,nosuid,noexec,relatime,gid=5,mode=620,ptmxmode=000 0 0
tmpfs /run tmpfs rw,nosuid,nodev,noexec,relatime,size=400228k,mode=755 0 0
/dev/sda5 / ext4 rw,relatime,errors=remount-ro 0 0
securityfs /sys/kernel/security securityfs rw,nosuid,nodev,noexec,relatime 0 0
tmpfs /dev/shm tmpfs rw,nosuid,nodev 0 0
tmpfs /run/lock tmpfs rw,nosuid,nodev,noexec,relatime,size=5120k 0 0
tmpfs /sys/fs/cgroup tmpfs ro,nosuid,nodev,noexec,mode=755 0 0
cgroup2 /sys/fs/cgroup/unified cgroup2 rw,nosuid,nodev,noexec,relatime,nsdelegate 0 0
cgroup /sys/fs/cgroup/systemd cgroup rw,nosuid,nodev,noexec,relatime,xattr,name=systemd 0 0
pstore /sys/fs/pstore pstore rw,nosuid,nodev,noexec,relatime 0 0
none /sys/fs/bpf bpf rw,nosuid,nodev,noexec,relatime,mode=700 0 0
cgroup /sys/fs/cgroup/rdma cgroup rw,nosuid,nodev,noexec,relatime,rdma 0 0
cgroup /sys/fs/cgroup/cpuset cgroup rw,nosuid,nodev,noexec,relatime,cpuset 0 0
cgroup /sys/fs/cgroup/hugetlb cgroup rw,nosuid,nodev,noexec,relatime,hugetlb 0 0
```

Faydalı Günlük Dosyaları

Bir olay müdahale görevlisi olarak, sistemdeki hangi eylemlerin kaydedildiğini, bu eylemlerin nerede saklandığını ve olay müdahale prosedürümüz sırasında bu bilgileri nasıl kullanabileceğimizi bilmeliyiz.

Aşağıda, olay müdahale prosedürleri sırasında yaygın olarak kullanılan günlük dosyalarını ve her dosyada hangi bilgilerin saklandığını gösteren bir tablo bulabilirsiniz.

File	syslog
Location	/var/log/syslog /var/log/messages

İçindekiler cron işlerinin yürütülmesi Hizmetlerin yürütülmesi

File	access.log
Location	/var/log/apache2/access.log /var/log/nginx/access.log
İçindekiler	Web istekleri

Dosya auth.log

Konum /var/log/auth.log

/var/log/secure

İçindekiler: Oturum açma olaylarıKullanıcı oluşturma olaylarıGrup olaylarıKullanıcı değiştirme olayları

Dosya son kayıt

Konum /var/log/lastlog

İçindekiler Son oturum açma bilgileri

Dosya bash_history

Konum ~/.bash_history

İçindekiler Terminal aracılığıyla yürütülen komutlar

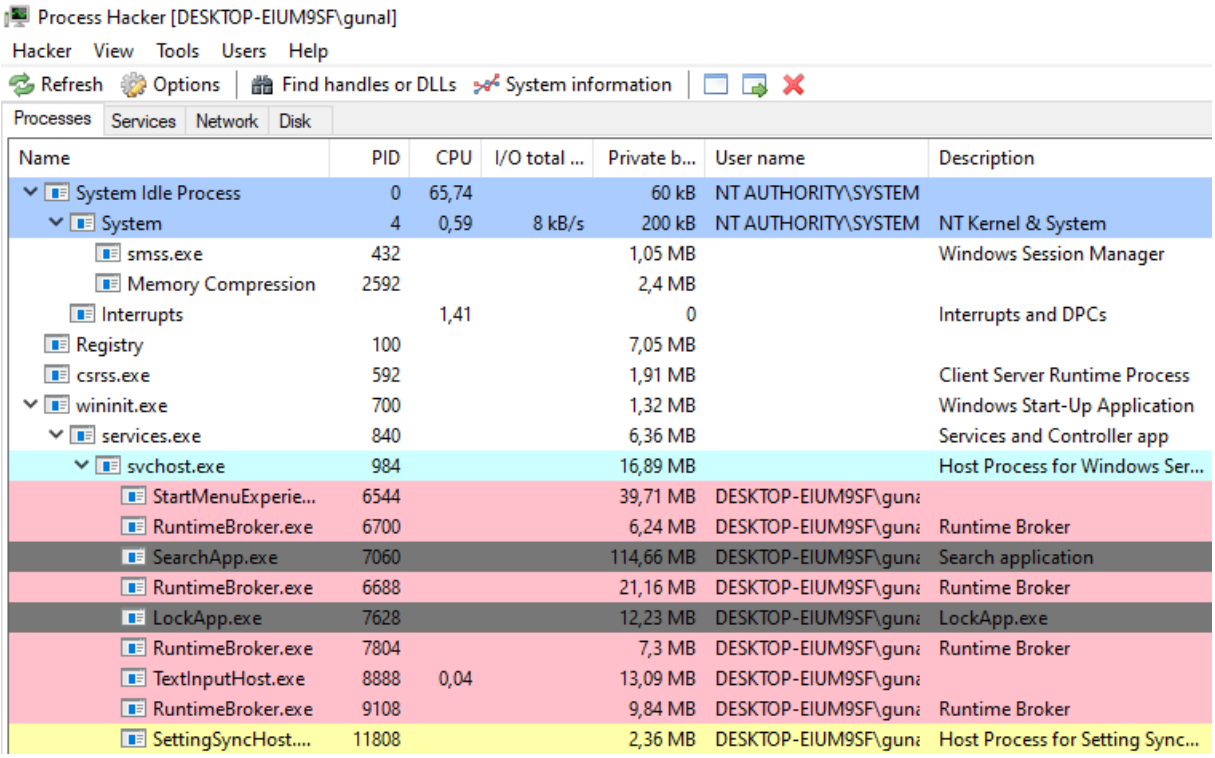
WİNDOWS

Canlı Hafıza Analizi - 1

Sistemde aktif olarak çalışmakta olan kötü niyetli bir aktiviteyi belirlemenin en iyi yolu bir hafıza analizi yapmaktır. Saldırgan(lar) o anda sisteme uzaktan erişiyorsa ve herhangi bir şekilde veri çalıyor veya etkileşim yapıyorsa buna izin veren bir süreç vardır. Buna izin veren süreci belirlemek için bir bellek analizi yapılabilir.

Bu konuyu anlatırken “Process Hacker” aracından faydalanacağız. Daha önce açıkladığımız gibi, bunun gibi farklı eşdeğer araçlar var. Önemli olan hangi aracı kullandığımız değil, neyi kontrol edeceğimizi bilmektir.

NOT: Tüm verilere erişmek için Yönetici olarak çalıştırmalısınız!



Process Hacker aracı, sistemdeki süreçlerle ilgili çok detaylı veriler sunar. Yukarıda süreç ilişkilerini, PID numaralarını ve çalışan kullanıcı bilgilerini en temel haliyle görebilirsiniz.

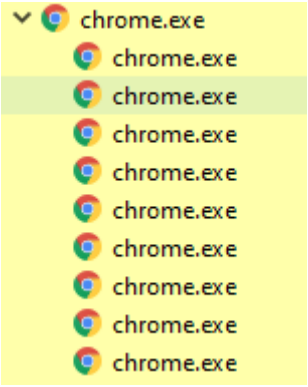
Analize dönelim. Hafıza analizi yaparken dikkat etmemiz gereken 3 kritik nokta vardır:

İşlem Ağacı

Ağ bağlantıları
İmza Durumu

İşlem Ağacı

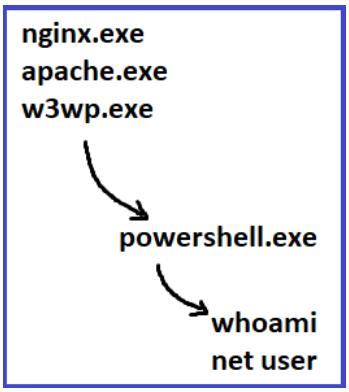
Hafıza analizi yaparken normal durumların ne olduğunu bilmek önemlidir. Örneğin, farklı sekmeler için farklı alt işlemler oluşturabileceğinden, "chrome.exe" işlemi altında alt işlem adında bir "chrome.exe" olması normaldir.



"Chrome.exe" işlemi altında oluşturulmuş bir "powershell.exe" işlemi görürsek ne olur? Bir krom işlemi altında bir PowerShell oluşturmaya normal şekilde tepki veremiyoruz. Bir istismar durumundan şüphelenmeli ve PowerShell'in ne yaptığını ve hangi komutları davet ettiğini incelemeliyiz.

Example 1 – WebShell Algılama

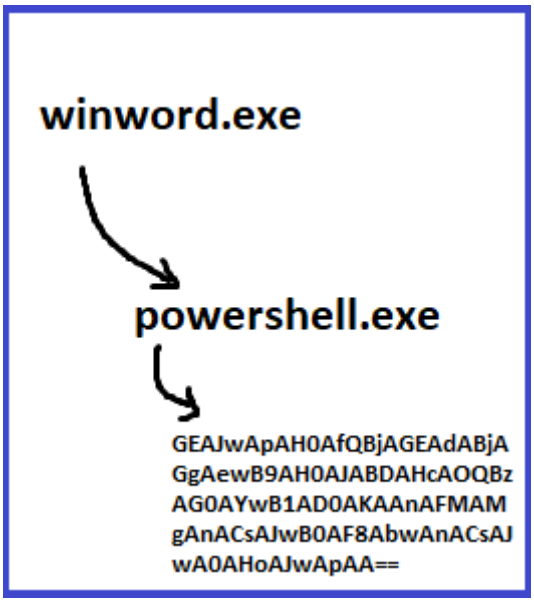
Aşağıdaki süreç ağacına bir göz atalım. Bir “powershell.exe: alt süreç, web sunucusuna ait bir süreç altında oluşturulmuştur. PowerShell yerine “cmd.exe” olabilirdi. Ardından “whoami” ve “net user” komutu çalıştırıldı. Olağanüstü durumlar dışında bir PowerShell'in bir web sunucusu işlemi altında çalışmasını bekleyemeyiz. Ayrıca, bunun üzerinde herhangi bir numaralandırma komutunun çalışmasını kesinlikle bekleyemeyiz.



Bu durumda şu sonuca varabiliriz: Bir web sunucusu işlemi altında bir cmd veya PowerShell işlemi oluşturulmuşsa, bir web kabuğundan şüphelenmeli ve araştırmalıyız.

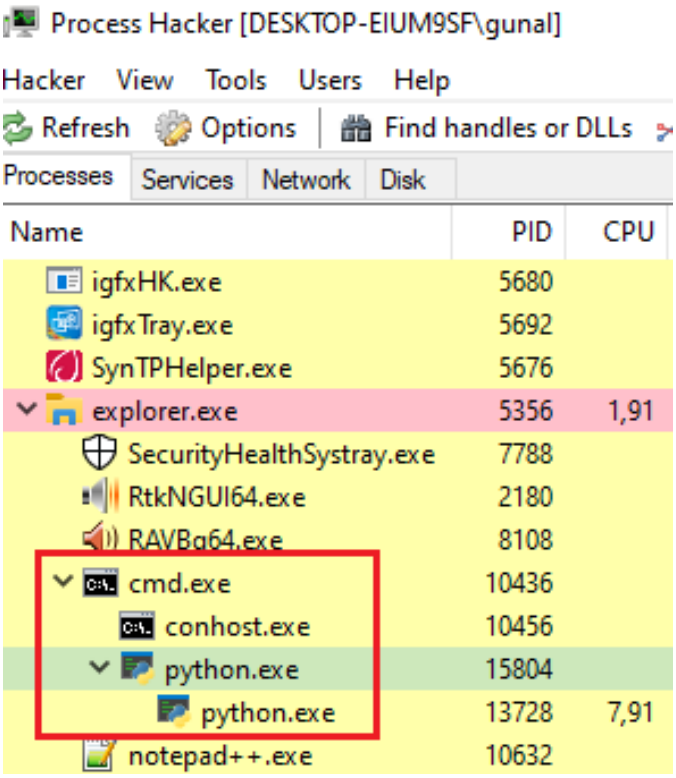
Örnek 2 – Kötü Amaçlı Makro Algılama

"Winword.exe" işlemini düşünelim. Bir word belgesi açıldığında oluşturulduğunu biliyoruz. Bir powershell.exe'nin Winword.exe işlemi altında oluşması normal midir? Ya aslında bu PowerShell, base64 ile kodlanmış bir komutla çalıştırılıyorsa. Bu durum normal değildir ve büyük olasılıkla, içinde kötü amaçlı bir makro bulunan bir dosyanın açılması nedeniyle oluşturulmuştur.

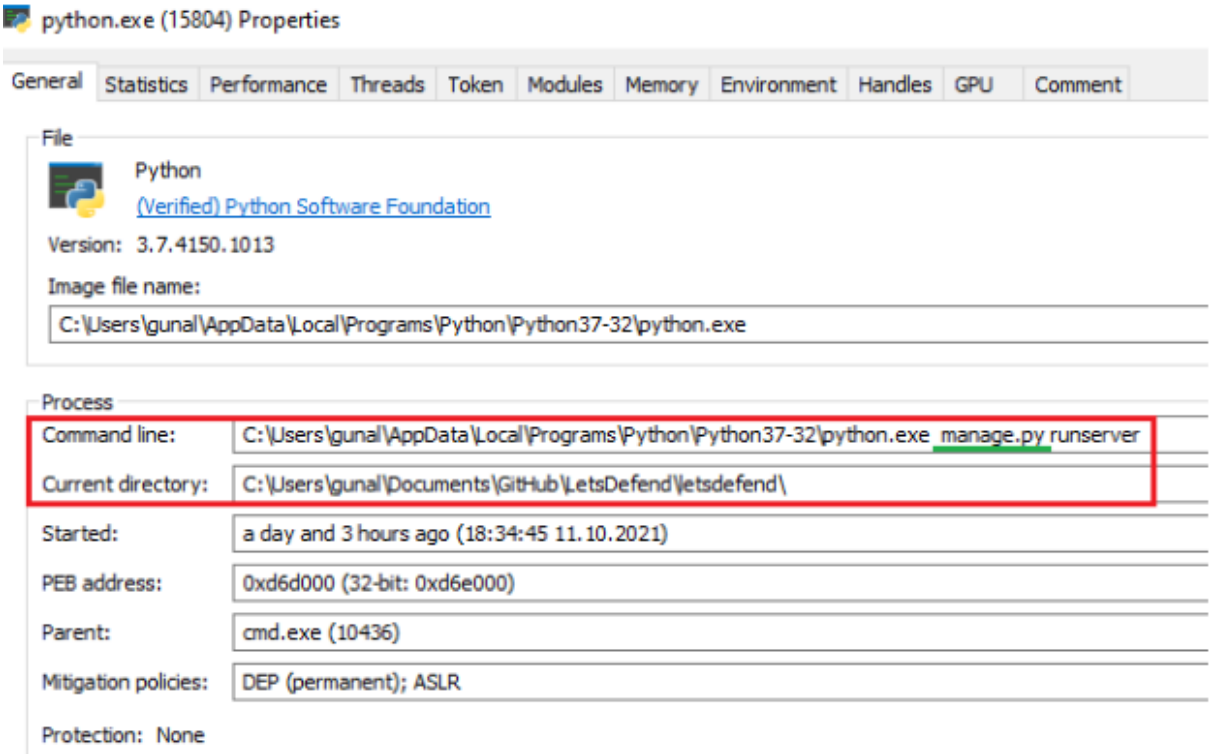


Process Hacker ile Kontrol Etme

Bir süreç ağacından türetilen şüpheli aktiviteyi nasıl tespit edebileceğimizi teorik olarak çeşitli örneklerle anlattık. Bunları gerçek bir makinede nasıl kontrol edebiliriz?



Yukarıdaki duruma baktığımızda python.exe'nin cmd.exe altında oluştuğunu görebiliriz. Bu durum yasal olabileceği gibi kötü niyetli bir python komutu da çalıştırmış olabilir. Bunu anlamak için “python.exe” üzerine çift tıklayarak hangi dosya/komutun hangi parametrelerde çalıştırıldığını kontrol etmeliyiz.



“Komut satırı” alanına baktığımızda Manage.py dosyasının “runserver” parametreleri içerisinde çalıştırıldığını ve “current directory” içerisinde işlemin nerede yapıldığını görebiliriz. Burada kesinlikle şüpheli bir durum olduğunu söyleyemeyiz. Durumun şüpheli mi yoksa kötü niyetli mi olduğunu anlamak için “manage.py” dosyasını analiz etmeliyiz. Görüldüğü gibi bu dosya “C:\Users\gunal\Documents\Github\LetsDefend\letsdefend\” konumundadır

Kullanıcılar

Kalıcılığı sağlamak için saldırganlar tarafından yaygın olarak kullanılan bir yöntem, kullanıcı oluşturmaktır. Aslında bunun yapılmasının tek nedeni kalıcılığı sağlamak değil, saldırgan(lar)ın “Yönetici” hesabının kontrolünü ele geçirdiklerinde yeni kullanıcılar oluşturduklarını gözlemliyoruz. Çünkü bu önemli bir kullanıcıdır ve etkinliği düzenli olarak izlenebilir. Böylece çok fazla dikkat çekmeyecek yeni bir kullanıcı yaratırlar ve mümkünse o kullanıcının yetkilerini arttırırlar.

Oluşturulan kullanıcılar genellikle "support", "sysadmin", "admin" gibi anahtar kelimeler içerir. Çoğu şirkette bu gibi isimlere sahip kullanıcılar fazla dikkat çekmeyecektir.

Bir olay müdahale prosedürü sırasında hızlı bir şekilde değerlendirmemiz gereken 2 şey vardır.

Şu anda sistemde olmaması gereken bir kullanıcı var mı?
Saldırı sırasında bir kullanıcı oluşturup sonrasında sildi mi?

Şüpheli Kullanıcı Tespiti

Sistemde aktif olan kullanıcıları listelemek için cmd üzerinden “net user” komutunu kullanabiliriz.

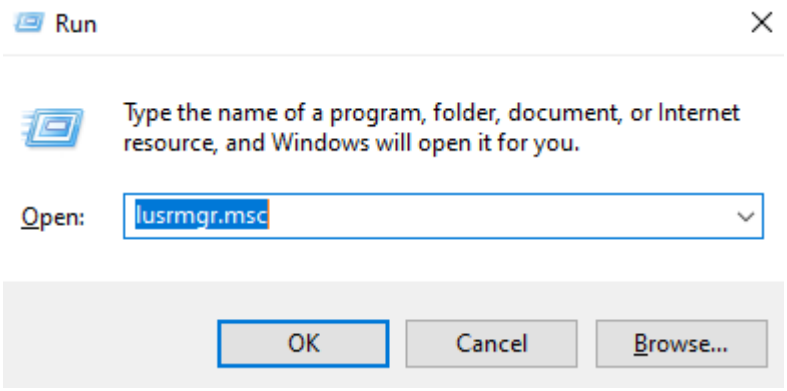
```
C:\Users\gunal>net user

User accounts for \\DESKTOP-EIUM9SF

-------------------------------------------------------------------------------
Administrator            DefaultAccount           Guest
gunal                    test                     user_name
WDAGUtilityAccount
The command completed successfully.
```

Sonuç olarak orada olmaması gereken bir kullanıcı varsa ve bu kullanıcı ile ilgili daha detaylı bilgiye ihtiyacımız varsa “net user USERNAME” yazarak arama yapabiliriz.

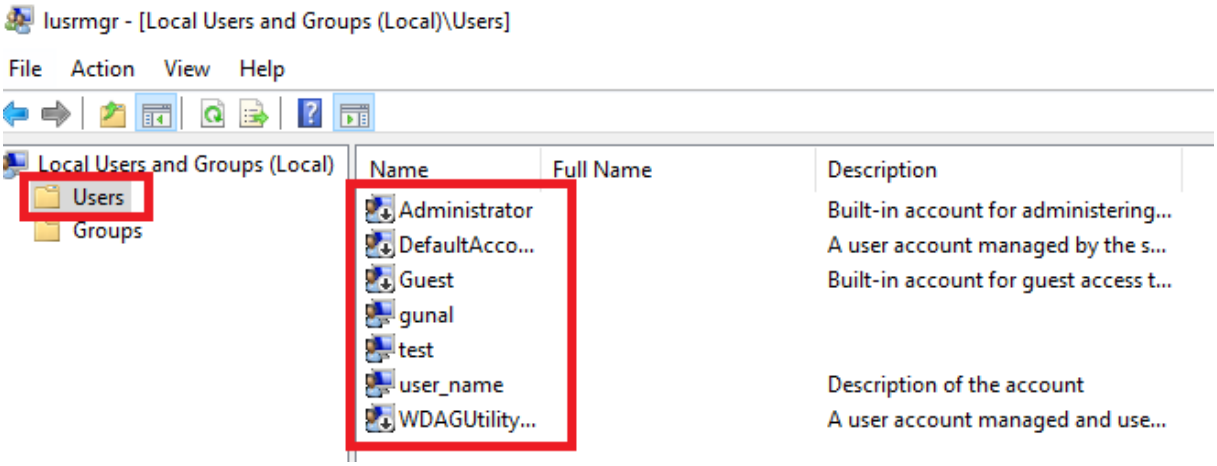
```
C:\Users\gunal>net user test
User name                    test
Full Name
Comment
User's comment
Country/region code          000 (System Default)
Account active               Yes
Account expires              Never

Password last set            31.05.2020 23:12:30
Password expires             Never
Password changeable          31.05.2020 23:12:30
Password required            No
User may change password     Yes

Workstations allowed         All
Logon script
User profile
Home directory
Last logon                   1.06.2020 09:38:43

Logon hours allowed          All

Local Group Memberships      *Users
Global Group memberships     *None
The command completed successfully.
```

Bu örnekte “Last logon” ve “Password last set” değerleri saldırı zamanı ile eşleştirilirse duruma şüpheyle yaklaşabiliriz.

Diğer bir yöntem ise kontrolü “lusrmgr” ile sürdürmektir. Bunun için “run: “Windows + R” ile etkinleştirin ve “lusrmgr.msc” yazarak Tamam'a tıklayın.



Açılan pencerede “Kullanıcılar” grubunu seçip kullanıcıları listeleyebilirsiniz.

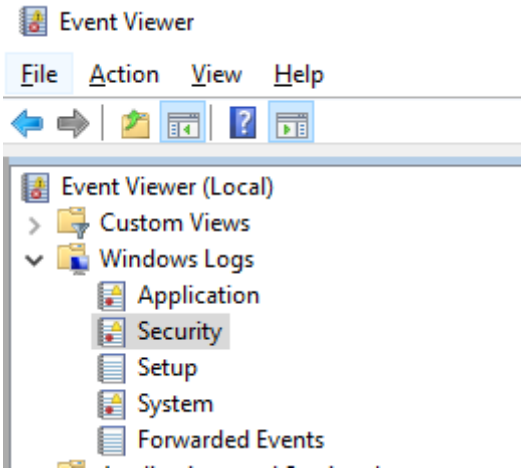


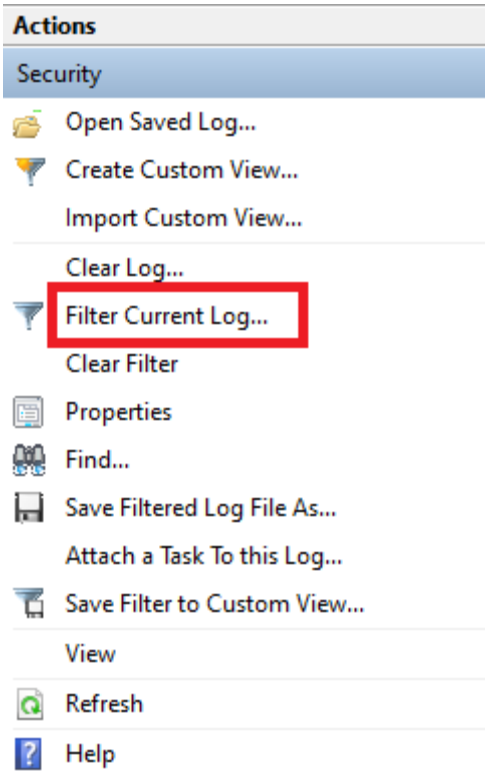
Bu denetleyiciden sonra bir kullanıcıdan şüpheleniyorsanız, sonraki analiz döneminizde o kullanıcının etkinliğine odaklanabilirsiniz.

Geçmişte Oluşturulmuş Kullanıcılar

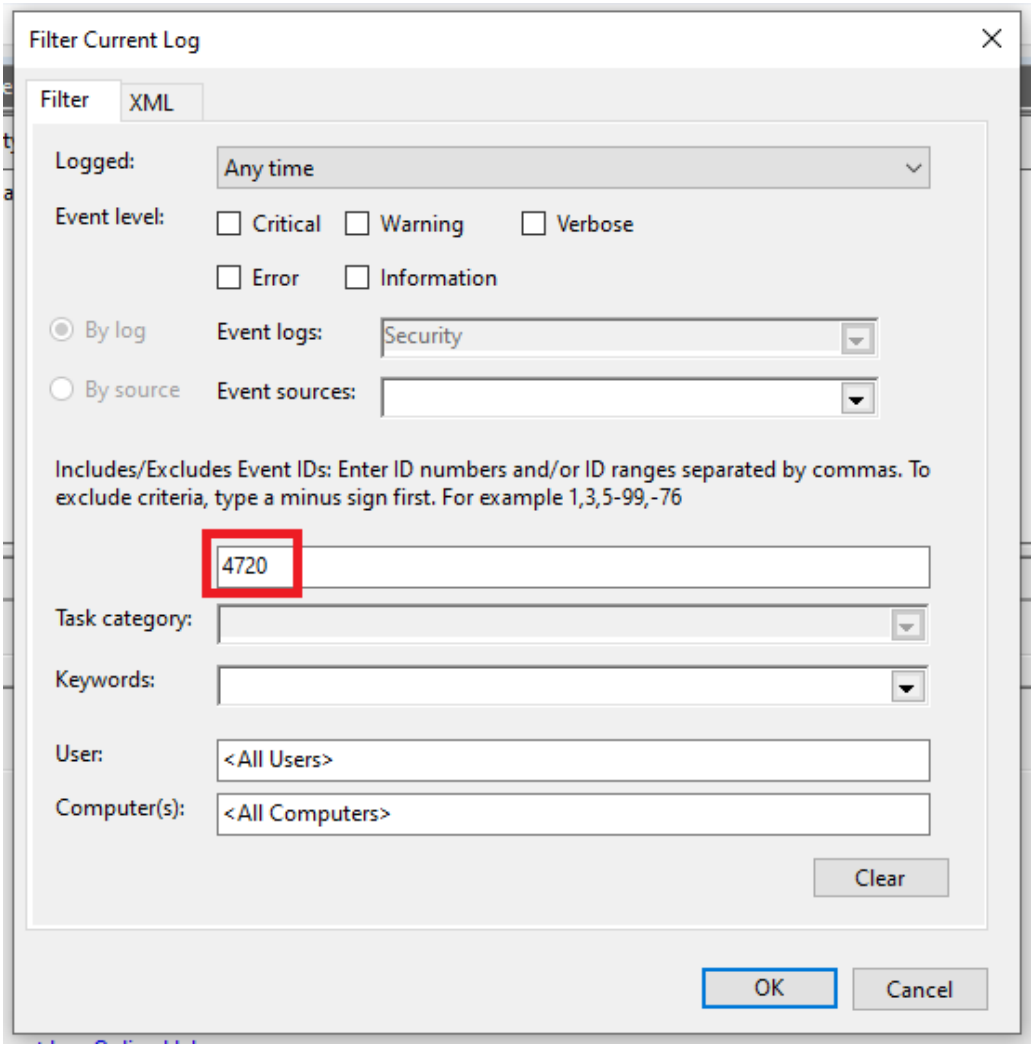
Saldırganlar, bir kullanıcı oluşturup ilgili işlemleri yaptıktan sonra, geride bıraktıkları izi en aza indirmek için işleri bittiğinde kullanıcıları silebilir. Bu durumda “net user” veya “lusrmgr” ile yaptığımız komutlarda bu kullanıcıları göremeyeceğiz. Yapmamız gereken “Güvenlik” logları içerisinden geçmişte bir kullanıcının oluşturulup oluşturulmadığını kontrol etmektir. Bunu yapmak için “Olay Kimliği 4720 – Bir kullanıcı hesabı oluşturuldu” günlüğünü kullanabiliriz.

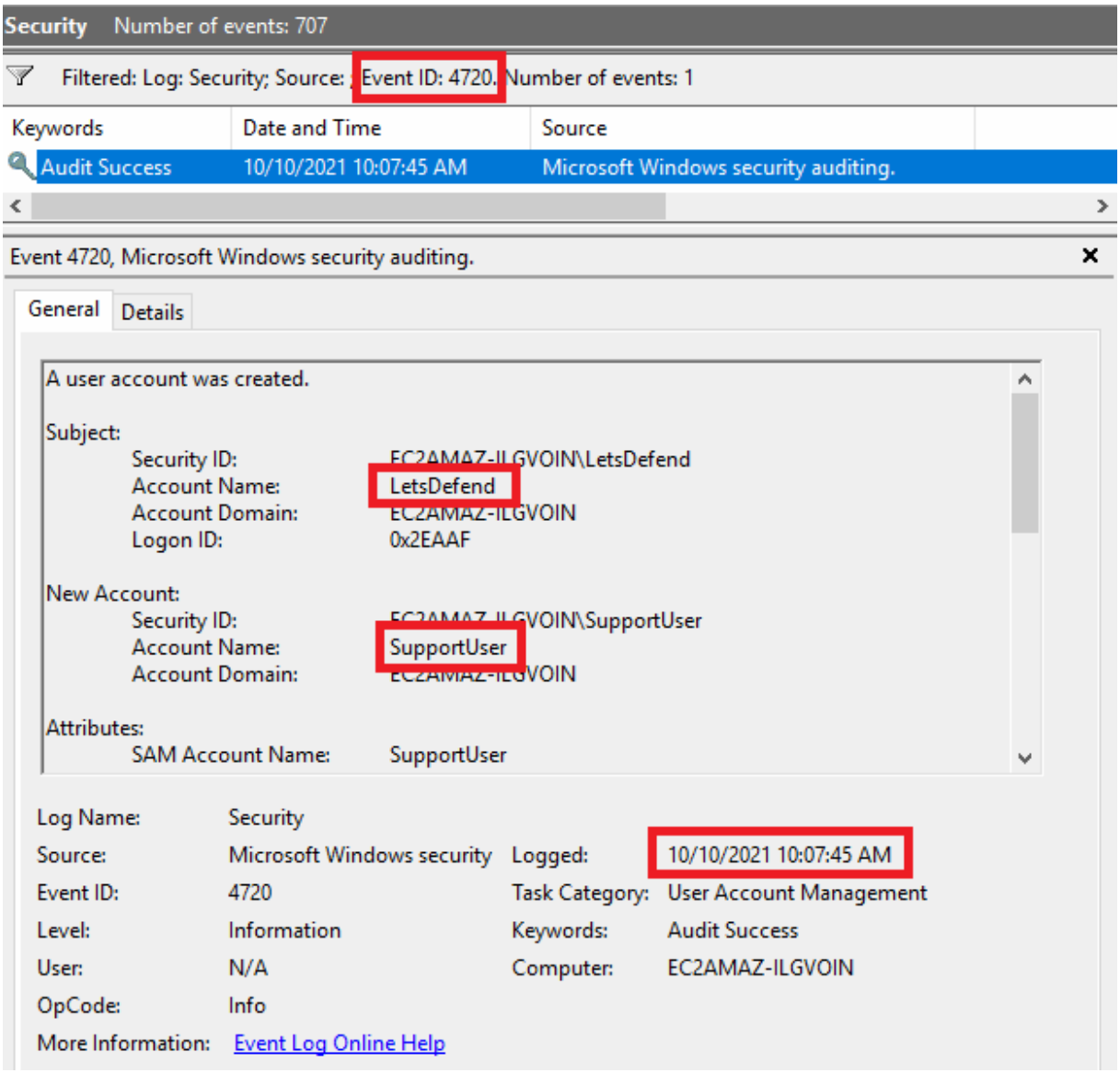
“Event Viewer” ile “Güvenlik” loglarını açtıktan sonra Event ID “4720” olan logları filtreleyebiliriz.





Açılan pencerede Event ID olarak “4720” giriyoruz.


Filter Current Log
Filter
XML
Logged:
Any time
Event level:
Critical
Warning
Verbose
Error
Information
By log
Event logs:
Security
By source
Event sources:
Includes/Excludes Event IDs: Enter ID numbers and/or ID ranges separated by commas. To exclude criteria, type a minus sign first. For example 1,3,5-99,-76
4720
Task category:
Keywords:
User:
<All Users>
Computer(s):
<All Computers>
Clear
OK
Cancel



Çıkan sonuca baktığımızda “LetsDefend” kullanıcısının “10/10/2021 10:07” tarihinde “SupportUser” isimli bir kullanıcı oluşturduğunu görüyoruz. Buradan çıkarmamız gereken çıkarım şudur; “LetsDefend” kullanıcısı devralındı veya komutların çalıştırılmasına izin verebilecek bir erişim yapıldı. Bu noktadan sonra hem “LetsDefend” hem de “SupportUser” kullanıcılarının aktiviteleri izlenmelidir.

EK OLARAK

Kullanıcılarla ilgili şüpheli durumları yakalamak için "Yöneticiler" grubuna eklenen kullanıcıları saldırının yapıldığı zaman aralığında sorgulayabilirsiniz. Böylece eklenmemesi gereken bir kullanıcıyı hemen yakalamış olacaksınız. Bunun için aşağıdaki event ID'yi kullanabilirsiniz.

Olay Kimliği 4732 – Güvenliği etkinleştirilmiş bir yerel gruba bir üye eklendi.

Ne Öğrendik?

Saldırganlar, sistemin kontrolünü ele geçirdikten sonra "destek" veya "yönetici" gibi genel adlar kullanabilir.
Yeni kullanıcının aktivitelerine ek olarak yeni kullanıcı oluşturan kullanıcının aktiviteleri de takip edilmelidir.

Önceki aktiviteleri takip ederken 4720 ve 4732 EventID logları faydalı olacaktır.