SIBER GÜVENLIK MÜHENDISLIĞI EĞİTİMİ - 2026

HAFTA 3: İşletim Sistemleri Mimarisi (Linux & Windows Internals)

21 ŞUBAT 2026

METEHAN EROĞLU

1. Linux Mimarisi: "Her Şey Bir Dosyadır" (Everything is a File)

Kavramsal Analiz:

→Linuxta her şey bir dosyadır, sisteme dair her şey okunabilir bir dosya tutulur. Mesela cat komutu dosyaların içeriğini okumaya yarar Ödev.txt okuması gibi ve bu komut /dev/sda (Harddisk) tarzı yerleri de okuyabilir. Burdan anlıyoruz ki Linux ta her şey bir dosyadır.

Tehlikeli İzinler ve SUID Biti:

→Önce 777 nedir onunla başlayalım. İlk 7 sayısı Owner kişisine okuma(4), yazma(2), çalıştırma(1) yetkisi verir(4+2+1) ve diğer 7'ler de sırasıyla Group ve Others dır. Others kısmının bütün izinleri elinde bulundurması çok tehlikelidir, içine zararlı bir yazılım yüklenip çalıştırılabilir.

→SUID biti bir program çalıştırıldığında dosya sahibini yetkisiyle çalışmasını sağlar. Passwd komutu kullanıcı şifresi değiştirme komutudur ve bu şifreler /etc/shadow altında tutulur. /etc/shadow ise sadece root yetkisiyle çalışır. Ama normal bir kullanıcı passwd komutunu kullanarak /etc/shadow altına dosya yazabilir. Saldırganlar ise bu tarz hatalı yapılandırılmış SUID programları find / -perm -4000 komutuyla bulur ve yetki yükseltmeye çalışır.

Bash Gücü vs. GUI:

→5GB bir log dosyasını not defterinde açmaya çalışırsak ram şişer çünkü bilgisayar hepsini bi anda yüklemeye çalışır. Ama Linux ta grep awk pipe gibi komutları kullanarak açmaya çalışırsak hem log ları filtrelemiş oluruz hem de Linux sırayla dosyaları açmaya çalışacağı için ram şişmez. Bir de neden sadece 404 hatalarını ararız çünkü normal bir kullanıcı sadece önündeki linklere tıklayarak ilerler herhangi bir 404 sayfa bulunamadı hatası almaz ama saldırgan sürekli arka plana ulaşmaya çalışır bu da bir sürü 404 hatası almasına sebep olur.

2. Windows Internals: "Çarklar Nasıl Dönüyor?"

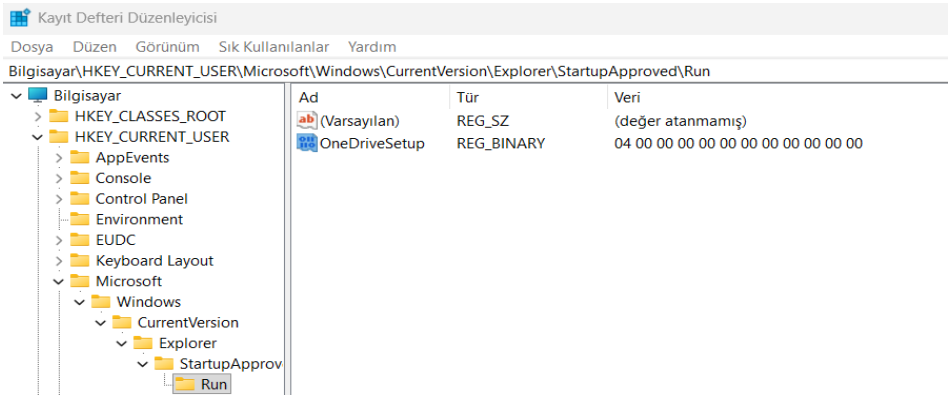
User Mode vs. Kernel Mode (Ring 0 - Ring 3):

→Ring 0 (Kernel Mode) tur sistem bileşenleri burada çalışır. Ring 3 (User Mode) ise kullanıcı uygulamalarının çalıştığı arayüzüdür. Bu yüzden Chrome.exe çökerse bilgisayar çökmez sadece Chrome.exe kapanır ama herhangi bir driver çökerse Ring 0 altında çalışacağı için mavi ekran alırız.

Registry (Kayıt Defteri) Anatomisi:

→ HKLM (HKEY_LOCAL_MACHINE) Sistem deki tüm kullanıcıları içinde barındırır.

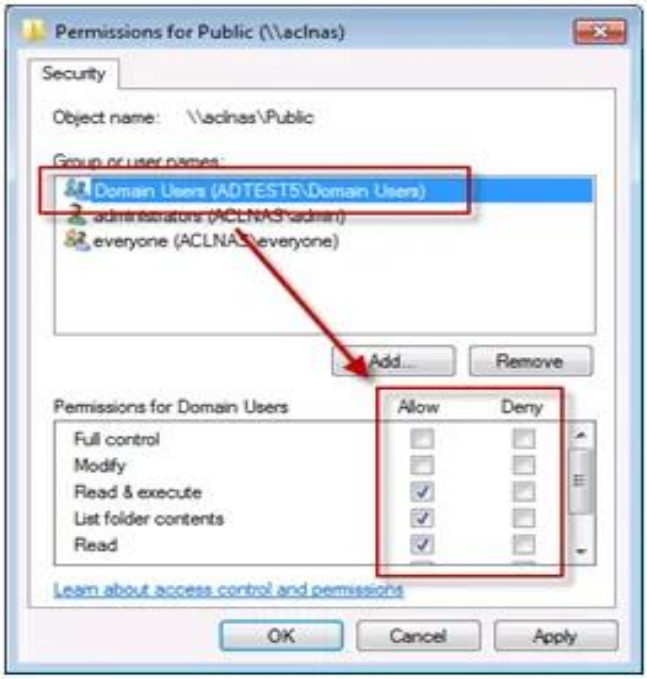
HKCU(HKEY_CURRENT_USER) Sadece o an kullanana kullanıcıyı kapsar.



HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\StartupApproved\Run Saldırgan kendilerini bu konuma kaydetmeye çalışır çünkü zararlı yazılımı bilgisayar çalıştığında çalışmasını ister.

NTFS İzinleri ve ACL (Erişim Kontrol Listesi):

→



Windows izinleri ayarlama ACL yapısı konusunda Linux tan daha detaylı davranır. Kişiye özel izinler verebilir. Bu sayede en az yetki prensibi uygulanır, iç tehditler sınırlandırılır ve kurumsal güvenlik güçlendirilir.

Görev 1: Linux Cephesi - Terminalle Tanışma

→

```
└─$ ls -lah
total 12K
drwxr-xr-x  3 kali kali 4.0K Feb 20 08:17 .
drwx------ 16 kali kali 4.0K Feb 20 08:02 ..
drwxrwxrwx  2 kali kali 4.0K Feb 20 08:17 AnkaSec
```

Bence ilk kritik komut ls-lah ile tüm gizli dosyaları, dosyanın izinlerini ve boyutunu görebilir.

```
┌──(kali㉿kali)-[~]
└─$ grep "404" access.log
grep: access.log: No such file or directory
```

İkinci kritik komut ise Grep komutu log lar arsındaki aranan bir değeri gösterebilir mesela burada 404 hatasını arıyor.

```
┌──(kali㉿kali)-[~/Desktop]
└─$ chmod 111 "AnkaSec"
```

Üçüncü kritik komut ise chmod. Chmod komutu sayesinde dosyadan gereksiz izinleri kaldırabilir.

```
d--x--x--x  2 kali kali 4.0K Feb 20 08:17 AnkaSec
```

Görev 2: Windows Anatomisi - "Normal"i Tanımak

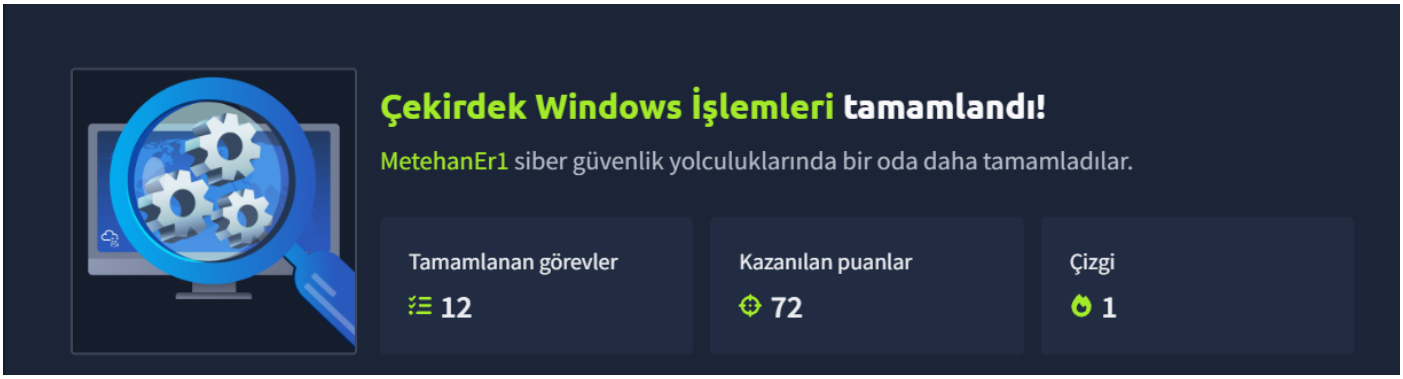
→PID 4 değeri system dir yani kernelin tüm thred leri bu süreç altında çalışır.

→smss.exe sesion 0 da csrss.exe ve wininit.exe süreçlerini başlatır bu süreç sistemin servislerini başlatır. Sesion 1 de ise csrss.exe ve winlogon.exe süreçlerini başlatır bu süreç ise kullanıcı şifre alma vb. süreçleri yönetir.

→csrss.exe yi sonlandırmak process lerin oluşmasını engeller Kernel ile iletişim kesilir bu yüzden sonlandırılması mavi ekran verdirir.

→lsass.exe kullanıc adlarını ve şifrelerinin doğrulandığı yerdir bu yüzden hackerlar için tam bir hedef noktadır.

→svchost.exe den bir sürü olmasının nedeni eğer çökerse tüm sistem çökmesin diye eğer bir tane olsaydı ve o çökseydi tüm sistem çökerdi.



Cephe 1: OverTheWire - Bandit (Linux)

LEVEL0→LEVEL1

```
Microsoft Windows [Version 10.0.26200.7840]
(c) Microsoft Corporation. Tüm hakları saklıdır.

C:\Users\Metehan>ssh bandit0@bandit.labs.overthewire.org -p 2220
                         _                     _ _ _
                        | |__   __ _ _ __   __| (_) |_
                        | '_ \ / _` | '_ \ / _` | | __|
                        | |_) | (_| | | | | (_| | | |_
                        |_.__/ \__,_|_| |_|\__,_|_|\__|


                      This is an OverTheWire game server.
            More information on http://www.overthewire.org/wargames

backend: gibson-0
bandit0@bandit.labs.overthewire.org's password:
```

Burada ssh kullanılarak makinaya ulaşıldı.

Komut: ssh bandit0@bandit.labs.overthewire.org -p 2220

Şifre: bandit0

```
bandit0@bandit:~$ ls
readme
bandit0@bandit:~$ cat readme
Congratulations on your first steps into the bandit game!!
Please make sure you have read the rules at https://overthewire.org/rules/
If you are following a course, workshop, walkthrough or other educational activity,
please inform the instructor about the rules as well and encourage them to
contribute to the OverTheWire community so we can keep these games free!

The password you are looking for is: ZjLjTmM6FvvyRnrb2rfNWOZOTa6ip5If
```

Burada ls komutu kullanılarak dosyalar listelenmiştir ve cat ile readme içeriği okunmuştur. Ve bandit 1 makinesini şifresini bulduk.

```
C:\Users\Metehan>ssh bandit1@bandit.labs.overthewire.org -p 2220
```

Bu komutla bandit 1 makinasına bağlandık ve şifreyi girdik.

```
bandit1@bandit:~$
```

LEVEL1→LEVEL2

```
bandit1@bandit:~$ ls
-
bandit1@bandit:~$ cat -


^C
bandit1@bandit:~$ cat./-
-bash: cat./-: No such file or directory
bandit1@bandit:~$ cat ./-
263JGJPfgU6LtdEvgfWU1XP5yac29mFx
bandit1@bandit:~$
```

Ls ile okuduğumuzda - dosyasını görüyoruz ama cat – yazdığımızda terminal onu okuyamıyor bu yüzde özellikle bu klasörde olduğunu belirtmemiz lazım cat ./- ile yapılır. Bu da bize bandit 2 şifresini verir.

LEVEL2→LEVEL3

Aynı şekilde bandit 2 makinesine ssh yaparak gireriz.

```
bandit2@bandit:~$ ls -lah
total 24K
drwxr-xr-x   2 root    root    4.0K Oct 14 09:26 .
drwxr-xr-x 150 root    root    4.0K Oct 14 09:29 ..
-rw-r--r--   1 root    root     220 Mar 31  2024 .bash_logout
-rw-r--r--   1 root    root    3.8K Oct 14 09:19 .bashrc
-rw-r--r--   1 root    root     807 Mar 31  2024 .profile
-rw-r-----   1 bandit3 bandit2   33 Oct 14 09:26 --spaces in this filename--
```

Bu dosyayı okumak istersek önündeki – yüzünden bir komutmuş gibi algılanır.

```
bandit2@bandit:~$ cat -- "--spaces in this filename--"
MNk8KNH3Usiio41PRUEoDFPqfxLPlSmx
```

Öndeki 2 -- işareti yazmamızın sebebi bunun bir dosya olduğunu vurgulamak bir de tırnak içine almamız gerekir.

LEVEL3→LEVEL4

```
bandit3@bandit:~/inhere$ ls -lah
total 12K
drwxr-xr-x 2 root    root    4.0K Oct 14 09:26 .
drwxr-xr-x 3 root    root    4.0K Oct 14 09:26 ..
-rw-r----- 1 bandit4 bandit3   33 Oct 14 09:26 ...Hiding-From-You
bandit3@bandit:~/inhere$ cat ...Hiding-From-You
2WmrDFRmJIq3IPxneAaMGhap0pFhF3NJ
```

Öncelikle cd inhere yazarak dosya içine girilir. Sonrada ls -lah kullanılarak gizli dosya bulunur. Son olarak cat …Hiding-From-you yazılarak dosya içeriği okunur.

LEVEL4→LEVEL5

```
bandit4@bandit:~/inhere$ ls -lah
total 48K
drwxr-xr-x 2 root    root    4.0K Oct 14 09:26 .
drwxr-xr-x 3 root    root    4.0K Oct 14 09:26 ..
-rw-r----- 1 bandit5 bandit4   33 Oct 14 09:26 -file00
-rw-r----- 1 bandit5 bandit4   33 Oct 14 09:26 -file01
-rw-r----- 1 bandit5 bandit4   33 Oct 14 09:26 -file02
-rw-r----- 1 bandit5 bandit4   33 Oct 14 09:26 -file03
-rw-r----- 1 bandit5 bandit4   33 Oct 14 09:26 -file04
-rw-r----- 1 bandit5 bandit4   33 Oct 14 09:26 -file05
-rw-r----- 1 bandit5 bandit4   33 Oct 14 09:26 -file06
-rw-r----- 1 bandit5 bandit4   33 Oct 14 09:26 -file07
-rw-r----- 1 bandit5 bandit4   33 Oct 14 09:26 -file08
-rw-r----- 1 bandit5 bandit4   33 Oct 14 09:26 -file09
bandit4@bandit:~/inhere$ cat -- "-file07"
4oQYVPkxZOOEOO5pTW81FB8j8lxXGUQw
```

Aynı şekilde – ile başladığı için dosya açılmadı bu yüzden cat –“-file07” komutunu kullandım.

LEVEL5→LEVEL6

```
bandit5@bandit:~/inhere$ ls -lah
total 88K
drwxr-x--- 22 root bandit5 4.0K Oct 14 09:26 .
drwxr-xr-x  3 root root    4.0K Oct 14 09:26 ..
drwxr-x---  2 root bandit5 4.0K Oct 14 09:26 maybehere00
drwxr-x---  2 root bandit5 4.0K Oct 14 09:26 maybehere01
drwxr-x---  2 root bandit5 4.0K Oct 14 09:26 maybehere02
drwxr-x---  2 root bandit5 4.0K Oct 14 09:26 maybehere03
drwxr-x---  2 root bandit5 4.0K Oct 14 09:26 maybehere04
drwxr-x---  2 root bandit5 4.0K Oct 14 09:26 maybehere05
drwxr-x---  2 root bandit5 4.0K Oct 14 09:26 maybehere06
drwxr-x---  2 root bandit5 4.0K Oct 14 09:26 maybehere07
drwxr-x---  2 root bandit5 4.0K Oct 14 09:26 maybehere08
drwxr-x---  2 root bandit5 4.0K Oct 14 09:26 maybehere09
drwxr-x---  2 root bandit5 4.0K Oct 14 09:26 maybehere10
drwxr-x---  2 root bandit5 4.0K Oct 14 09:26 maybehere11
drwxr-x---  2 root bandit5 4.0K Oct 14 09:26 maybehere12
drwxr-x---  2 root bandit5 4.0K Oct 14 09:26 maybehere13
drwxr-x---  2 root bandit5 4.0K Oct 14 09:26 maybehere14
drwxr-x---  2 root bandit5 4.0K Oct 14 09:26 maybehere15
drwxr-x---  2 root bandit5 4.0K Oct 14 09:26 maybehere16
drwxr-x---  2 root bandit5 4.0K Oct 14 09:26 maybehere17
drwxr-x---  2 root bandit5 4.0K Oct 14 09:26 maybehere18
drwxr-x---  2 root bandit5 4.0K Oct 14 09:26 maybehere19
bandit5@bandit:~/inhere$ find -size 1033c
./maybehere07/.file2
bandit5@bandit:~/inhere$ cat ./maybehere07/.file2
HWasnPhtq9AVKe0dmk45nxy20cvUa6EG
```

find -size 1033c komutuyla boyutu 1033 byte olan dosyayı buldum ve onu cat komutuyla açtım.

LEVEL6→LEVEL7

```
bandit6@bandit:~$ find / -type f -user bandit7 -group bandit6 -size 33c
/var/lib/dpkg/info/bandit7.password
bandit6@bandit:~$ cat /var/lib/dpkg/info/bandit7.password
morbNTDkSW6jIlUc0ymOdMaLnOlFVAaj
```

-type f dosyaları bul demek, -user badit, -group bandit 6 ve -size 33c olan dosyayı bulmak için bu komutu kullandım.

LEVEL7→LEVEL8

```
bandit7@bandit:~$ grep millionth data.txt
millionth       dfwvzFQi4mU0wfNbFOe9RoWskMLg7eEc
```

Eğer cat data.txt gibi bir hata yaparsanız uzunca bir dosya olduğunu anlarsınız. Bu yüzden grep millionth data.txt komutunu kullanarak o satırı rahatlıkla çağırdık.

LEVEL8→LEVEL9

```
bandit8@bandit:~$ sort data.txt | uniq -u
4CKMh1JI91bUIZZPXDqGanal4xvAg0JM
```

Burada tekrar eden tonlarca satır var bunları filtreleyip tek bir tane olanı bulmamız lazım. Bunun içinde sort data.txt | uniq -u komutunu kullanırız.

LEVEL9→LEVEL10

```
bandit9@bandit:~$ strings data.txt
```

```
5========== FGUW5ilLVJrxX9kMYMmlN4MgbpfMiqey
```

Burada strings data.txt komutu Binary içindeki ASCII metinleri ayıklar, açılan dosyada biraz aşağı inildiğinde yukarıdaki şifreyi buluruz.

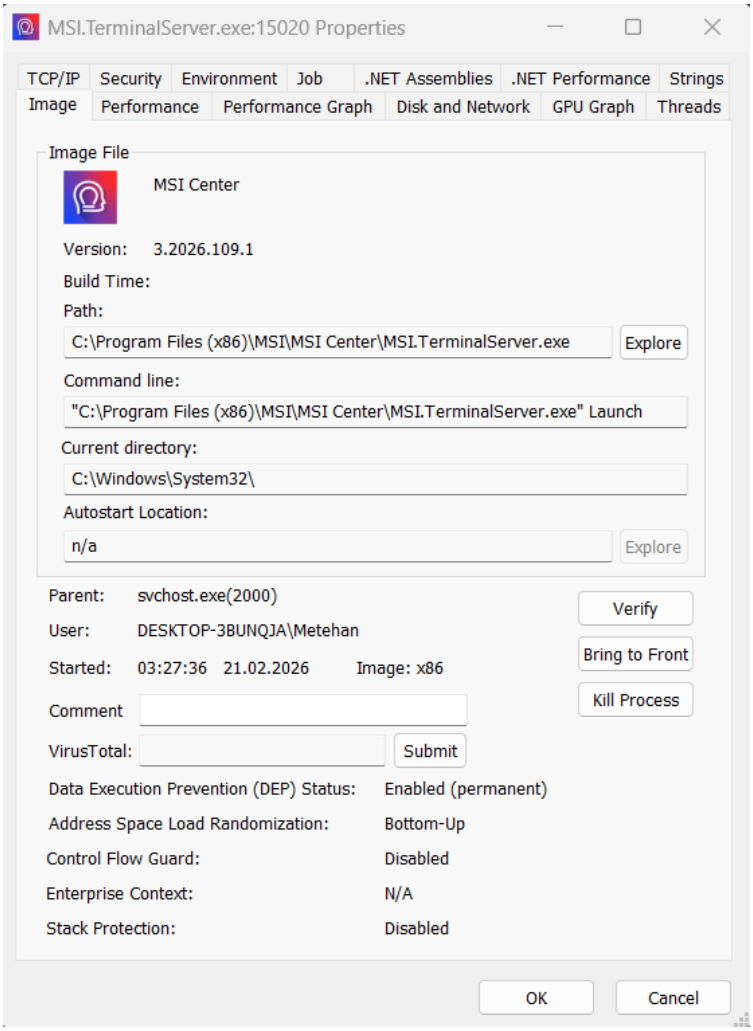
LEVEL10→LEVEL11

```
bandit10@bandit:~$ cat data.txt
VGhlIHBhc3N3b3JkIGlzIGR0UjE3M2ZaS2IwUlJzREZTR3NnMlJXbnBOVmozcVJyCg==
bandit10@bandit:~$ echo -n "VGhlIHBhc3N3b3JkIGlzIGR0UjE3M2ZaS2IwUlJzREZTR3NnMlJXbnBOVmozcVJyCg==" | base64 -d
The password is dtR173fZKb0RRsDFSGsg2RWnpNVj3qRr
```

Dosya içeriği base64 ile kodlanmış o yüzden çözmemiz gerekiyor.

echo -n "VGhlIHBhc3N3b3JkIGlzIGR0UjE3M2ZaS2IwUlJzREZTR3NnMlJXbnBOVmozcVJyCg==" | base64 -d komutunu kullanırız.

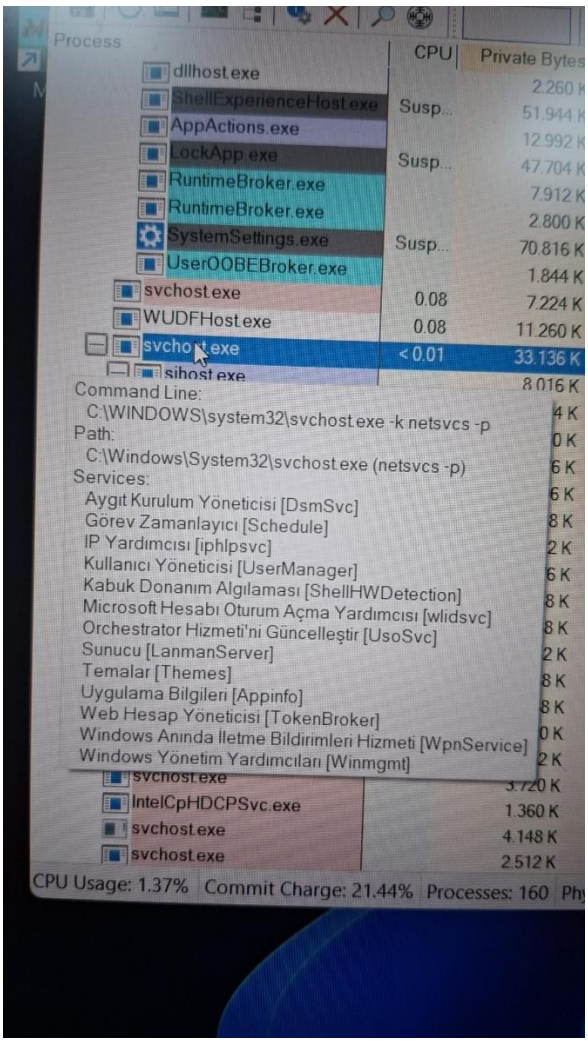
Cephe 2: Sysinternals Analizi (Windows)



Parent-Child (Ebeveyn-Çocuk) Analizi:

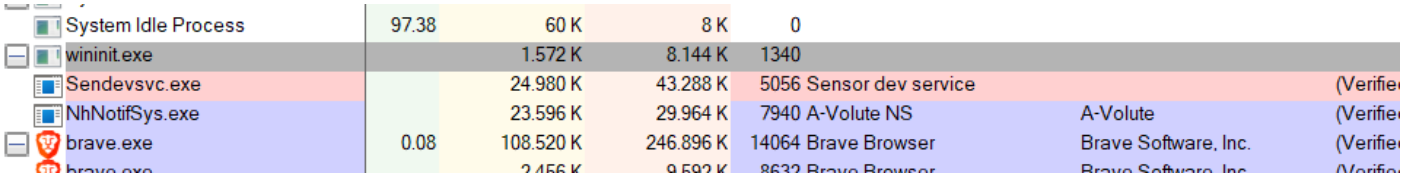
Msı Center ın parent süreci svchost.exe dir.

Svchost Avı (Service Host):



Burada svchost.exe nin çalıştırdığı servisler gözüküyor.

İmza Kontrolü (Verify Signatures):



Microsoft imzasının olmaması, ilgili sürecin işletim sistemine ait olmadığını ve dış kaynaklı ya da potansiyel olarak zararlı bir çalıştırılabilir dosya olabileceğini gösterir.

BÖLÜM D: Mühendislik Vizyonu (Reflection)

1. Yetki Yükseltme (PrivEsc) Mantığı:

→vim komutu kullanıcı tarafından kullanılan komuttur ama SUID biti sayesinde çalıştığı yer root seviyesidir. Saldırganlar bunu kullanarak root yetkisine ulaşır ve /etc/shadow üzerinde tutulan şifreyi değiştirebilir ve kendini tamamen root seviyesine çıkarabilir.

2. Zararlı Yazılım Kamuflajı (Process Injection):

→Virüsü neden oyun.exe gibi yerlere enjekte etmeyiz de svchost.exe veya explorer.exe sürecinin içine enjekte ederiz çünkü oyun.exe hemen göze batar ama svchost.exe tarzı yerler sistem yetkisiyle çalışır ve bunun kapatılması sistemin çökerticeği bilinir bu yüzden zararlı yazılımları svchost.exe tarzı yerlerin içine saklarlar.