BÖLÜM A

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

Kavramsal Analiz: Linux çekirdeği donanımı yönetmek için özel arayüzlere gerek olmasın diye bütün aygıtları dosya gibi sunar. Böylece aynı komutlarla hem normal dosyaları hem donanımları yönetebiliriz. Örneğin; normal bir metin dosyasını okumak için kullandığın cat komutuyla, /dev/sda yolundaki harddiski de okuyabiliriz. Bu sayede özel bir yedekleme yazılımına ihtiyaç duymadan yedekleme yapabiliriz. Kısaca Linux donanımı dosya gibi sunarak sistem yönetimini kolaylaştırır.

Tehlikeli İzinler ve SUID Biti

- 777 Tehlikesi: Bir dosyaya 777 yetkisi vermek dosyayı herkesin okuyabileceğini, yazabileceğini ve çalıştırabileceği anlamına gelir. Burdaki en önemli kısım ve tehlikeli kısım Others yani yazma iznidir. Bu yazma izni çok tehlikelidir çünkü sistemdeki en düşük yetkili kullanıcı bile dosyanın içeriğini değiştirebilir, içine kötü amaçlı kod yazabilir veya çalıştırılabilir bir dosyayı tamamen zararlı hale getirebilir. Sonuç olarak 777 bir dosyayı herkes tarafından manipüle edilebilir hale getirerek güvenlik faciası yaşanmasına neden olur.

- Hackerların Altın Anahtarı (SUID): SUID, bir programın kendi sahibinin yetkileriyle çalışmasını sağlar. Örneğin şifre değiştirme komutu (passwd) SUID bitine sahiptir. Çünkü normal bir kullanıcı, aslında sadece yöneticinin yazabildiği /etc/shadow dosyasına kendi şifresini yazmak zorundadır. SUID olmasaydı, sıradan kullanıcı şifresini değiştiremezdi. Eğer bir program kötü yazılmışsa veya SUID yanlış dosyaya verilmişse saldırgan root yetkisi elde eder. Bu olay Yetki Yükseltme (Privilege Escalation) için kullanılan en büyük açıktır.

Bash Gücü vs. GUI: 5 GB'lık bir log dosyasını Notepad veya Excel ile açmaya çalışmak bilgisayarın kitlenmesine neden olur. Ancak Linux terminalindeki araçlar dosyayı stream (akış) olarak işler. Yani dosyayı açmaz, içinden geçer. Sadece aradığın satırı bulur ve ekrana basar. Bu mühendisler için binlerce satır arasından saniyeler içinde sadece 404 hatası veren IP'leri bulup sıralamasını sağlar. böylece hem zamandan hemde jaynaktan tasarruf edilmiş olur.

2. Windows Internals: "Çarklar Nasıl Dönüyor?"

User Mode vs. Kernel Mode (Ring 0 - Ring 3): Windows ve modern işlemciler iki modda çalışır. Kernel Mode (ring 0) işletim sisteminin kalbidir ve tüm sürücüler (driver) buradadır. Tam yetkiye sahiptir. User Mode (Ring 3) ise kullandığımız Chrome, Spotify gibi programları çalıştırır. Yetkileri kısıtlıdır, doğrudan donanıma dokunamazlar. Bir hata yaparlarsa sadece o program kapanır. Eğer Ring 0 seviyesindeki bir sürücü örneğin ekran kartı sürücüsü yanlış bir işlem yaparsa, bu kritik bir hatadır. Sistem, verilerin bozulmasını veya donanımın yanmasını önlemek için tüm işlemleri durdurur ve Mavi Ekran (BSOD) verir. Ama Ring 3'teki Chrome çökseydi Windows uygulamayı kapatırdı ve kritik bir olay yaşanmazdı. Bu nedenle kritik

şeyler kernel tarafına alınır. Bu ayrım sistemin kararlılığı için zorunludur.

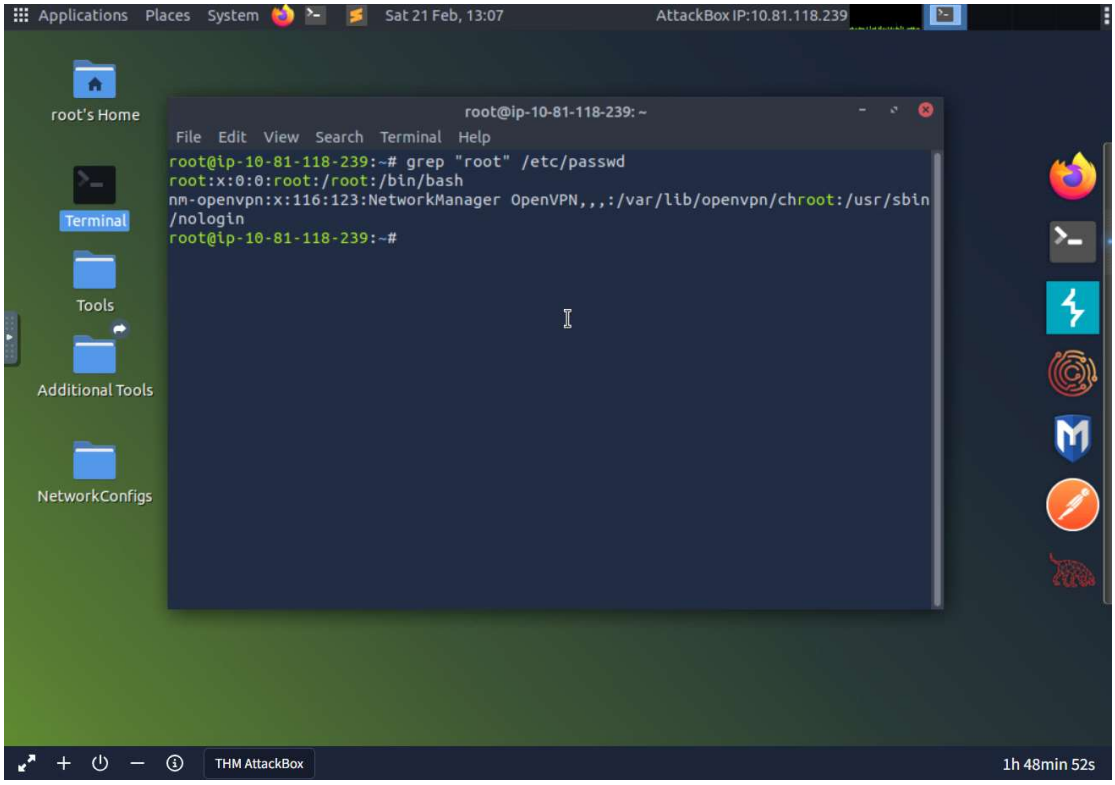
Registry (Kayıt Defteri) Anatomisi: HKLM (HKEY_LOCAL_MACHINE) bilgisayarın genel ayarlarıdır. Hangi kullanıcı girerse girsin, klavye dili veya yüklü programlar gibi ayarlar buradan okunur. HKCU (HKEY_CURRENT_USER) ise sadece o an oturan kişinin Masaüstü resmi, tarayıcı geçmişi gibi kişisel ayarlarıdır. Bir virüs bilgisayara bulaştığında, bilgisayar kapansa bile tekrar çalışmak ister. Bunun en kolay yolu Registry'deki Run anahtarlarına kendini yazmaktır. Windows her açıldığında tekrardan çalışmak için HKCU\Software \Microsoft\Windows\CurrentVersion\Run yollarını çalıştırır.

NTFS İzinleri ve ACL (Erişim Kontrol Listesi): Linux'taki basit izinlerden (rwx) farklı olarak, Windows çok daha detaylı bir kontrol listesi (ACL) sunar. ACL sayesinde büyük şirketlerde güvenlik yönetebilir. Örneğin; bir klasöre Stajyerler sadece içeriği görsün ama okumasın, Müdürler her şeyi yapsın, Sistem dosyaları bu klasöre dokunamasın gibi çok ince ayarlar yapılabilir. Bu büyük şirketlerde yetkisiz erişimi engelleyerek veri güvenliğinin bel kemiğini oluşturur.

BÖLÜM B

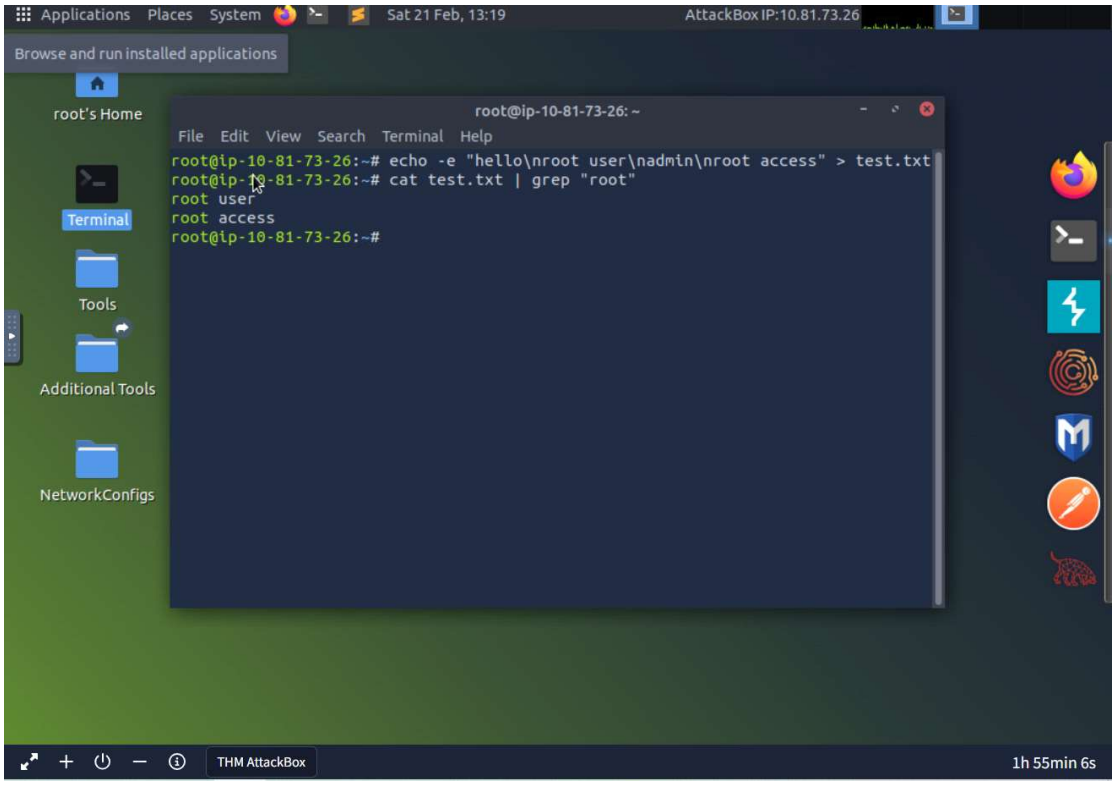
Görev 1

1) grep "root" /etc/passwd



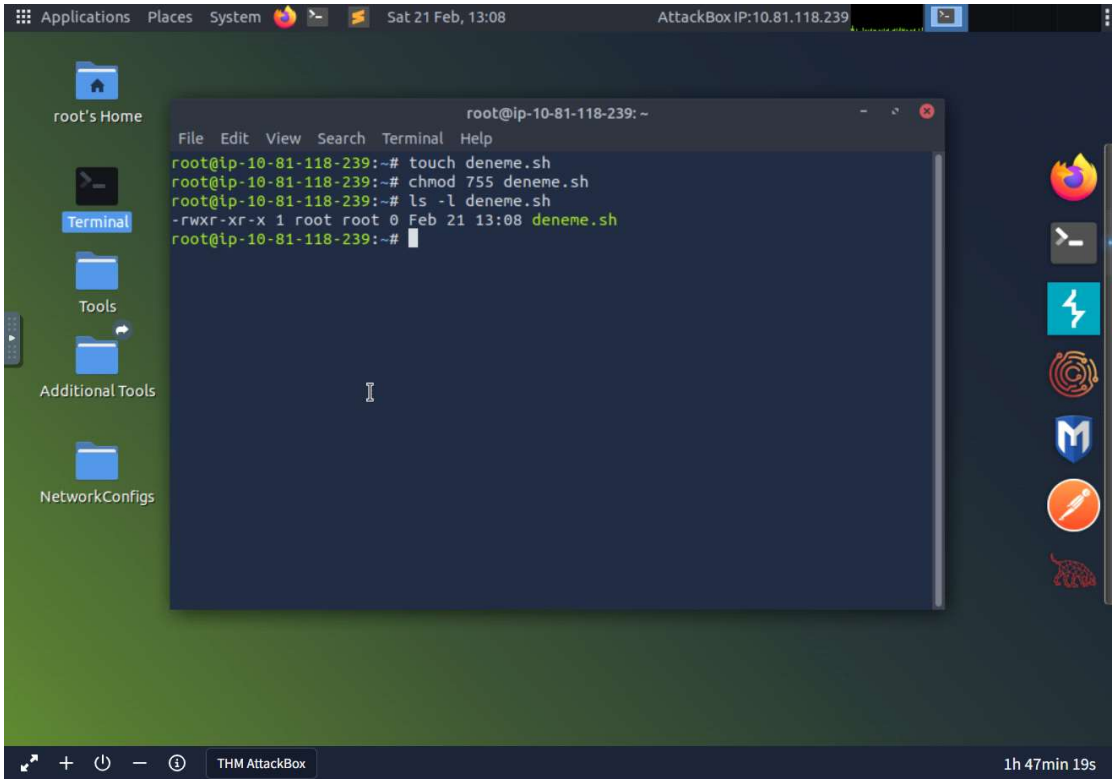
Bu komutu /etc/passwd dosyasının içinde “root” kelimesini aramak için kullandım.

2) cat test.txt | grep "root"



Burada pipe (|) kullanımını görmek için küçük bir metin dosyası oluşturdum.cat test.txt komutu dosyanın tamamını ekrana yazıyor, pipe ise bu çıktıyı grep komutuna aktarıyor. Yani bir komutun çıktısı diğer komutun girdisi oluyor.

3) chmod 755 deneme.sh



Bu komutu dosya izinlerinin nasıl değiştiğini görmek için kullandım.755 izni dosya sahibine tam yetki verirken, diğer kullanıcılar sadece okuma ve çalıştırma yetkisine sahip oluyor.

Görev 2

System (PID 4): System işlemi Windows açılırken en önce başlayan sistem süreçlerinden biri olduğu için PID'si hep 4 oluyor. Çekirdekle bağlantılı çalıştığı için bilgisayarın en temel görevlerini o yürütüyor.

smss.exe (Session Manager): smss.exe bilgisayar açıldığında oturumu başlatan süreçtir. Temp klasörlerini hazırlar ve winlogon.exe gibi önemli bileşenleri devreye sokar.

csrss.exe (Client/Server Runtime): Bu süreç Windows'un pencere ve konsol gibi temel kısımlarını yönettiği için çok kritiktir. Kapatmaya çalışırsanız sistem bunu kaldıramayıp direkt mavi ekran verir.

lsass.exe (Local Security Authority): lsass.exe kullanıcı girişleri ve parola hashlerini tuttuğu için saldırganların en çok hedef aldığı süreçlerden biridir. Buraya erişen biri sistemde ciddi yetkiler elde edebilir.

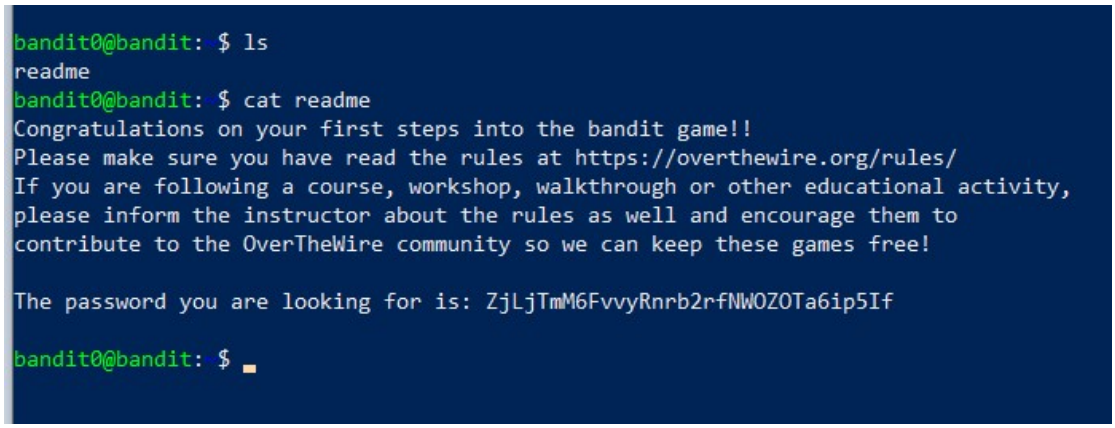
svchost.exe (Service Host): Windows'taki birçok servis ortak çalışmak için svchost'u kullanır. Servisler gruplandığı için Görev Yöneticisi'nde svchost.exe'nin onlarca tane görünmesi tamamen normal.

kanıt:

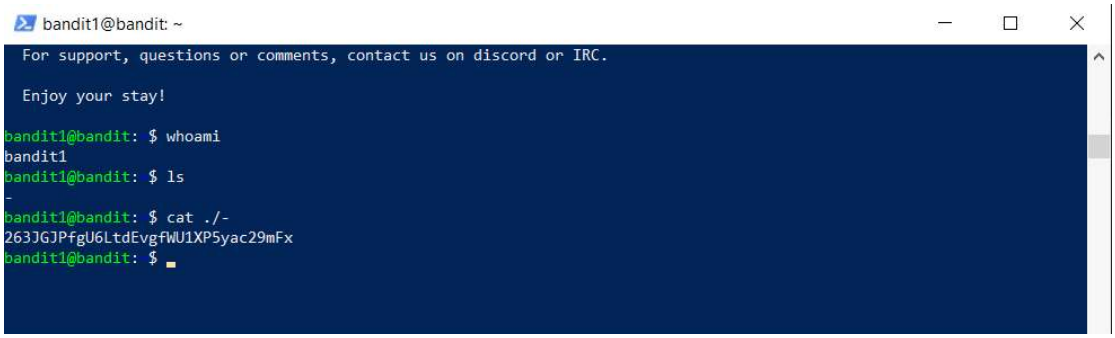
BÖLÜM C

CEPHE 1: OverTheWire – Bandit

Level 0 → 1: Oyuna SSH protokolü üzerinden bağlanarak başladım. Ana dizinde bulunan readme dosyasını cat komutuyla okuyarak bir sonraki seviyenin şifresine ulaştım.

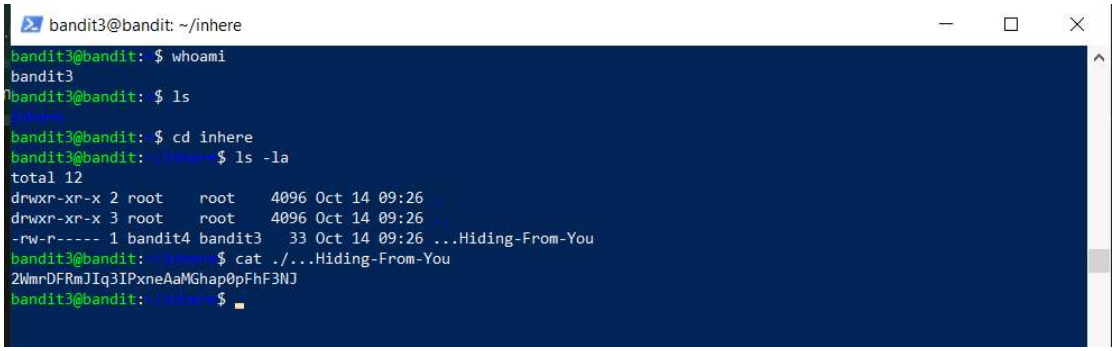


Level 1 → 2: Dosya adı sadece - karakterinden oluştuğu için cat - komutu hatalı algılanıyordu. Bu engeli aşmak için dosyanın tam yolunu belirterek komutu çalıştırdım.

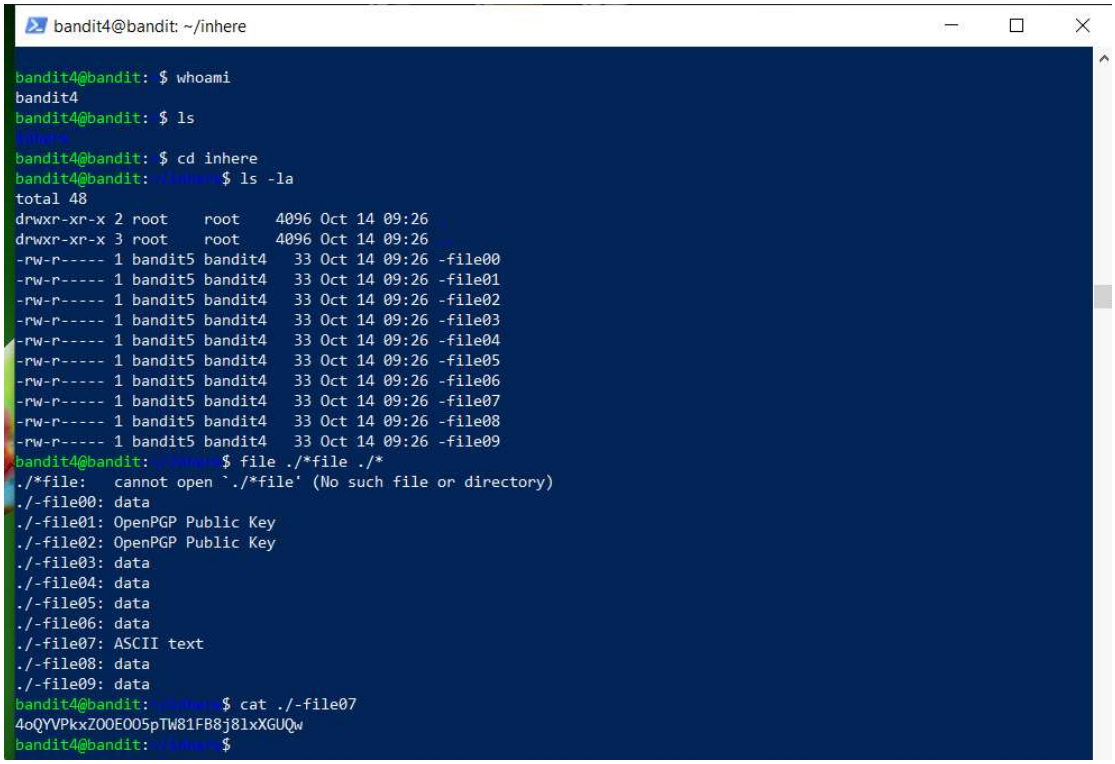


Level 2 → 3: Dizinde ismi --spaces in this filename-- olan bir dosya bulunuyordu. Dosya ismindeki boşlukların komutu bozmaması için ters eğik çizgi (\) kullanarak dosyayı okudum.

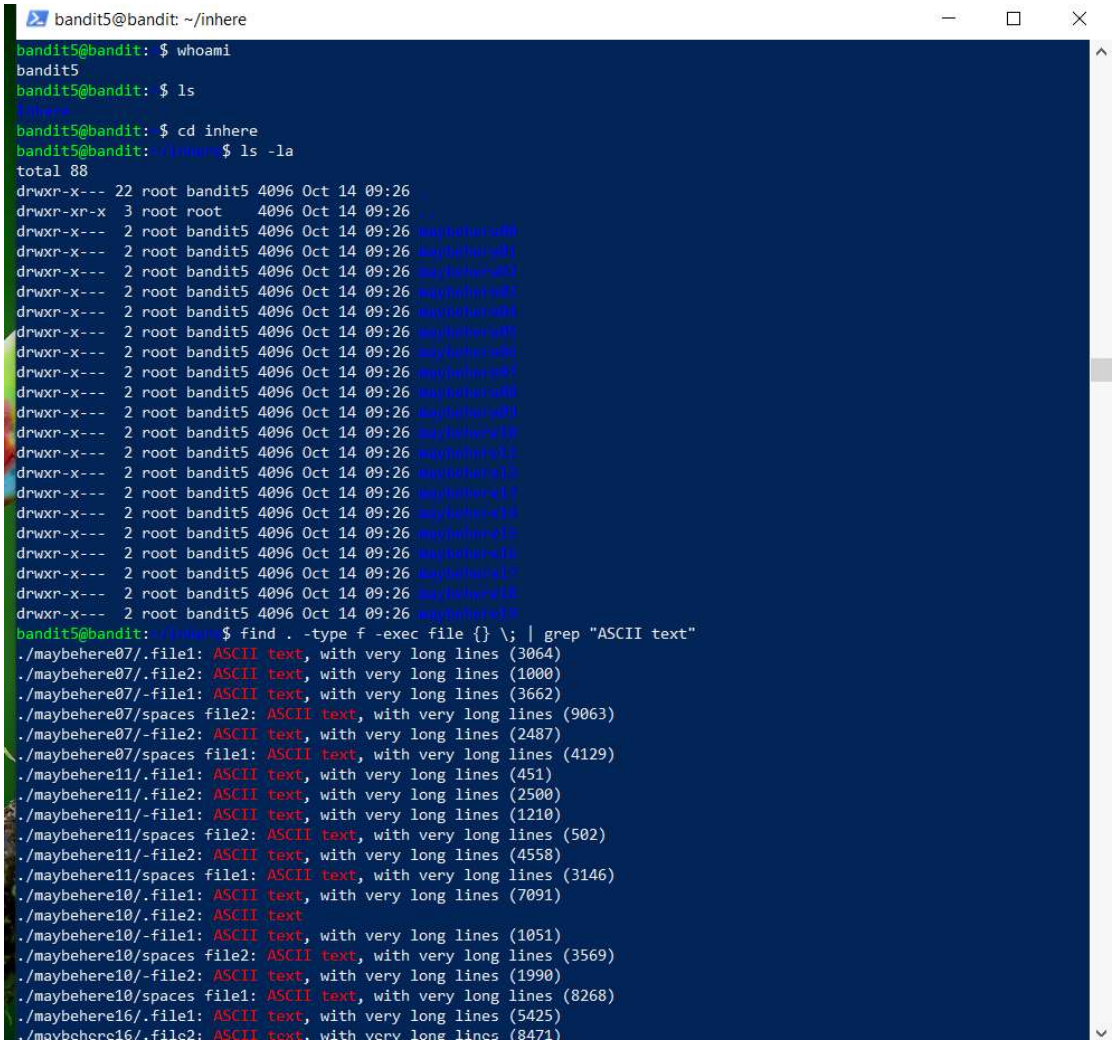
Level 3 → 4: inhere dizinine girdiğimde normal bir ls komutu içeriyi boş gösteriyordu. ls -la komutunu kullanarak gizli olan ...Hiding-From-You dosyasını ortaya çıkardım..

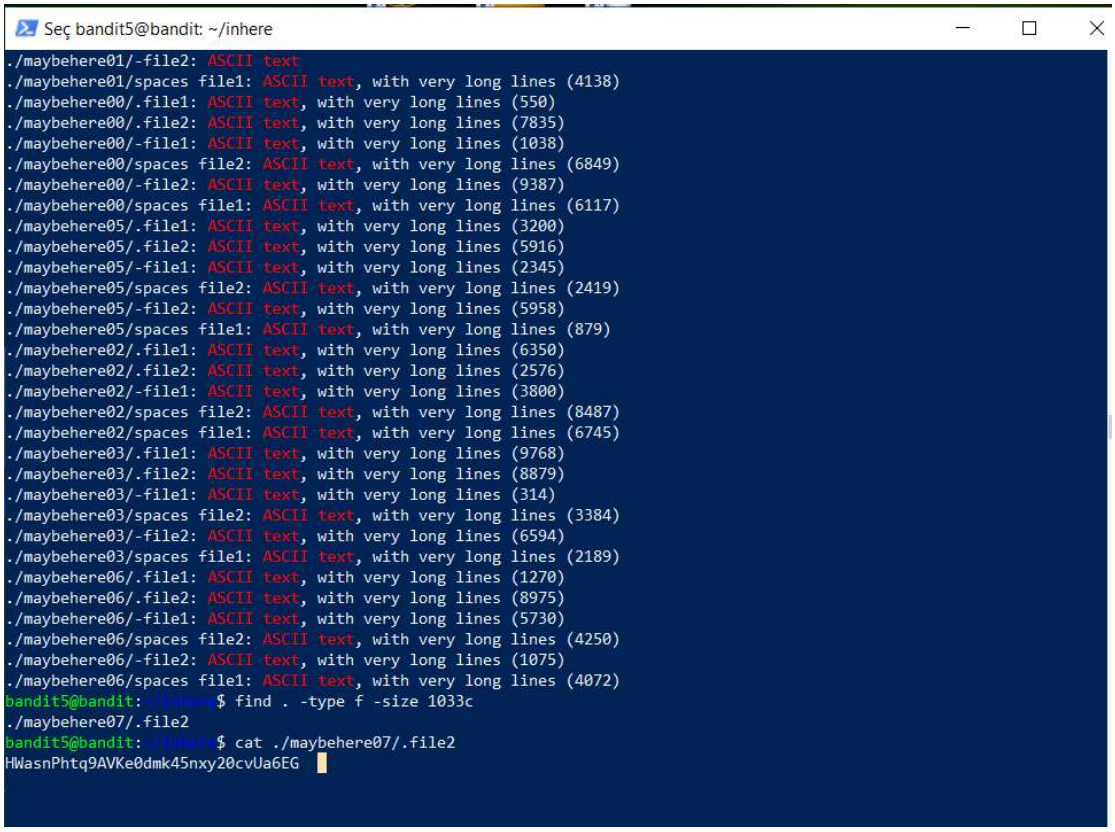


Level 4 → 5: inhere klasörü içinde bir sürü dosya vardı. file ./* komutunu kullanarak tüm dosyaların içeriğini kontrol ettim ve içlerinden sadece -file07 dosyasının "ASCII text" yani okunabilir bir metin olduğunu görüp şifreyi oradan aldım.

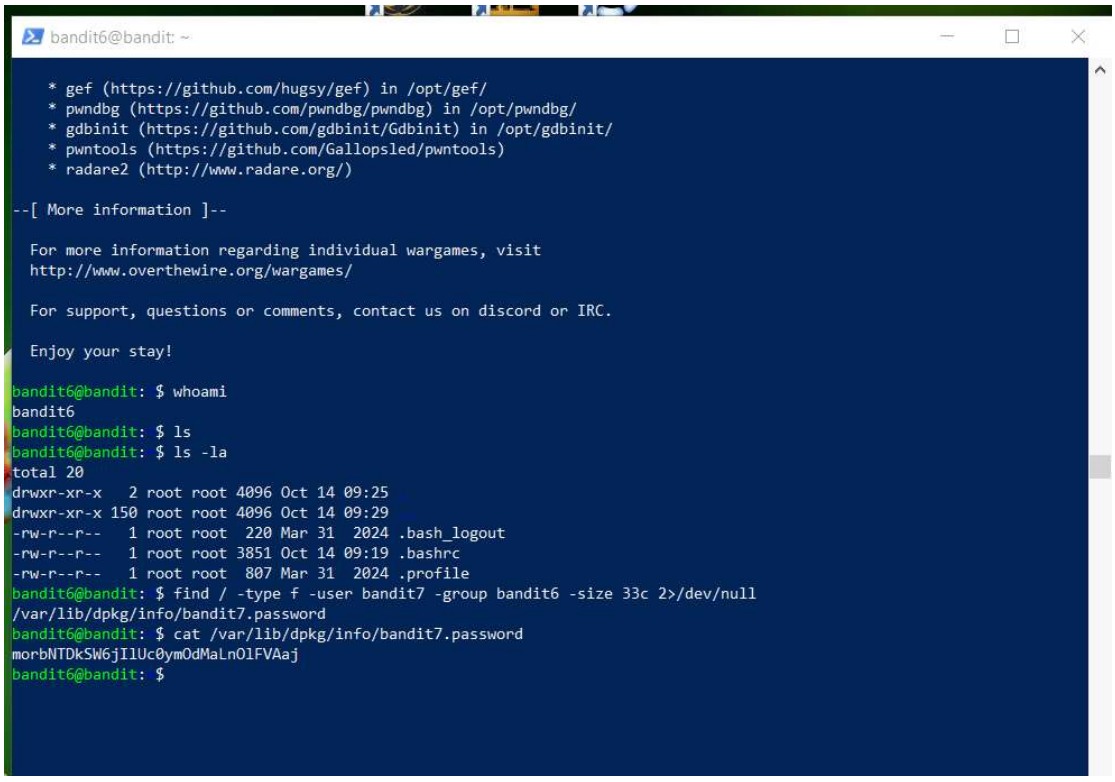


Level 5 → 6: Çok fazla alt klasör arasından belirli özelliklere sahip olan dosyayı bulmam gerekiyordu. find komutuyla tam olarak 1033c (1033 byte) boyutunda olan dosyayı arattım ve şifrenin olduğu .file2 dosyasına ulaştım.


bandit5@bandit: ~/inhere
bandit5@bandit: $ whoami
bandit5
bandit5@bandit: $ ls
inhere
bandit5@bandit: $ cd inhere
bandit5@bandit: ~/inhere$ ls -la
total 88
drwxr-x--- 22 root bandit5 4096 Oct 14 09:26 .
drwxr-xr-x 3 root root   4096 Oct 14 09:26 ..
drwxr-x--- 2 root bandit5 4096 Oct 14 09:26 maybehere00
drwxr-x--- 2 root bandit5 4096 Oct 14 09:26 maybehere01
drwxr-x--- 2 root bandit5 4096 Oct 14 09:26 maybehere02
drwxr-x--- 2 root bandit5 4096 Oct 14 09:26 maybehere03
drwxr-x--- 2 root bandit5 4096 Oct 14 09:26 maybehere04
drwxr-x--- 2 root bandit5 4096 Oct 14 09:26 maybehere05
drwxr-x--- 2 root bandit5 4096 Oct 14 09:26 maybehere06
drwxr-x--- 2 root bandit5 4096 Oct 14 09:26 maybehere07
drwxr-x--- 2 root bandit5 4096 Oct 14 09:26 maybehere08
drwxr-x--- 2 root bandit5 4096 Oct 14 09:26 maybehere09
drwxr-x--- 2 root bandit5 4096 Oct 14 09:26 maybehere10
drwxr-x--- 2 root bandit5 4096 Oct 14 09:26 maybehere11
drwxr-x--- 2 root bandit5 4096 Oct 14 09:26 maybehere12
drwxr-x--- 2 root bandit5 4096 Oct 14 09:26 maybehere13
drwxr-x--- 2 root bandit5 4096 Oct 14 09:26 maybehere14
drwxr-x--- 2 root bandit5 4096 Oct 14 09:26 maybehere15
drwxr-x--- 2 root bandit5 4096 Oct 14 09:26 maybehere16
drwxr-x--- 2 root bandit5 4096 Oct 14 09:26 maybehere17
drwxr-x--- 2 root bandit5 4096 Oct 14 09:26 maybehere18
drwxr-x--- 2 root bandit5 4096 Oct 14 09:26 maybehere19
bandit5@bandit: ~/inhere$ find . -type f -exec file {} \; | grep "ASCII text"
./maybehere07/.file1: ASCII text, with very long lines (3064)
./maybehere07/.file2: ASCII text, with very long lines (1000)
./maybehere07/-file1: ASCII text, with very long lines (3662)
./maybehere07/spaces file2: ASCII text, with very long lines (9063)
./maybehere07/-file2: ASCII text, with very long lines (2487)
./maybehere07/spaces file1: ASCII text, with very long lines (4129)
./maybehere11/.file1: ASCII text, with very long lines (451)
./maybehere11/.file2: ASCII text, with very long lines (2500)
./maybehere11/-file1: ASCII text, with very long lines (1210)
./maybehere11/spaces file2: ASCII text, with very long lines (502)
./maybehere11/-file2: ASCII text, with very long lines (4558)
./maybehere11/spaces file1: ASCII text, with very long lines (3146)
./maybehere10/.file1: ASCII text, with very long lines (7091)
./maybehere10/.file2: ASCII text
./maybehere10/-file1: ASCII text, with very long lines (1051)
./maybehere10/spaces file2: ASCII text, with very long lines (3569)
./maybehere10/-file2: ASCII text, with very long lines (1990)
./maybehere10/spaces file1: ASCII text, with very long lines (8268)
./maybehere16/.file1: ASCII text, with very long lines (5425)



Level 6 → 7: Şifrenin sistemde bir yerde gizlendiği bilgisi vardı. user bandit7, group bandit6 ve 33c boyut kriterlerini kullanarak tüm sistemi taradım. Hataları gizlemek için 2>/dev/null kullandım ve şifreyi /var/lib/dpkg/info/ altında buldum.



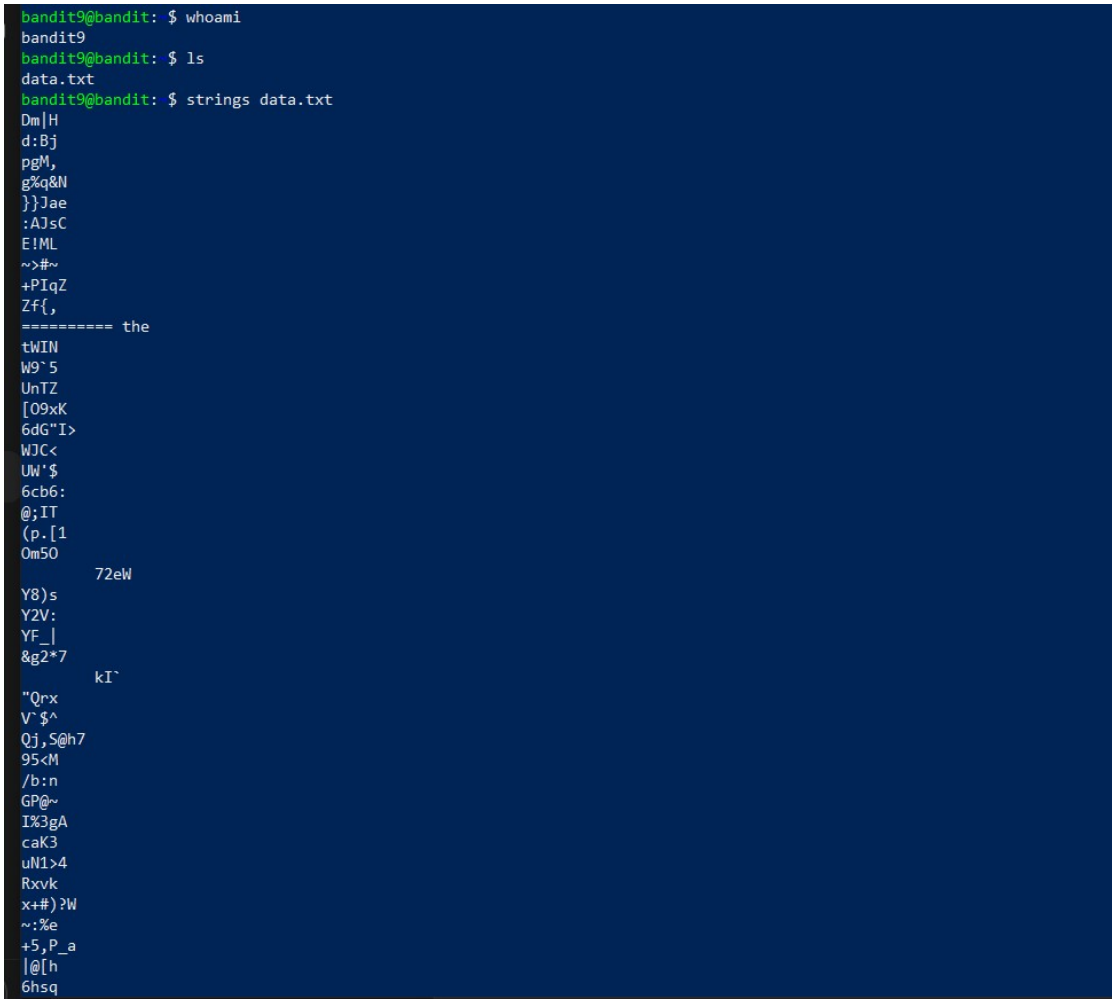
Level 7 → 8: Çok büyük boyutlu bir data.txt dosyasıyla karşılaştım. Gözle bulmanın imkansız olduğu bu dosyada grep millionth komutunu kullanarak şifreyi saniyeler içinde buldum.

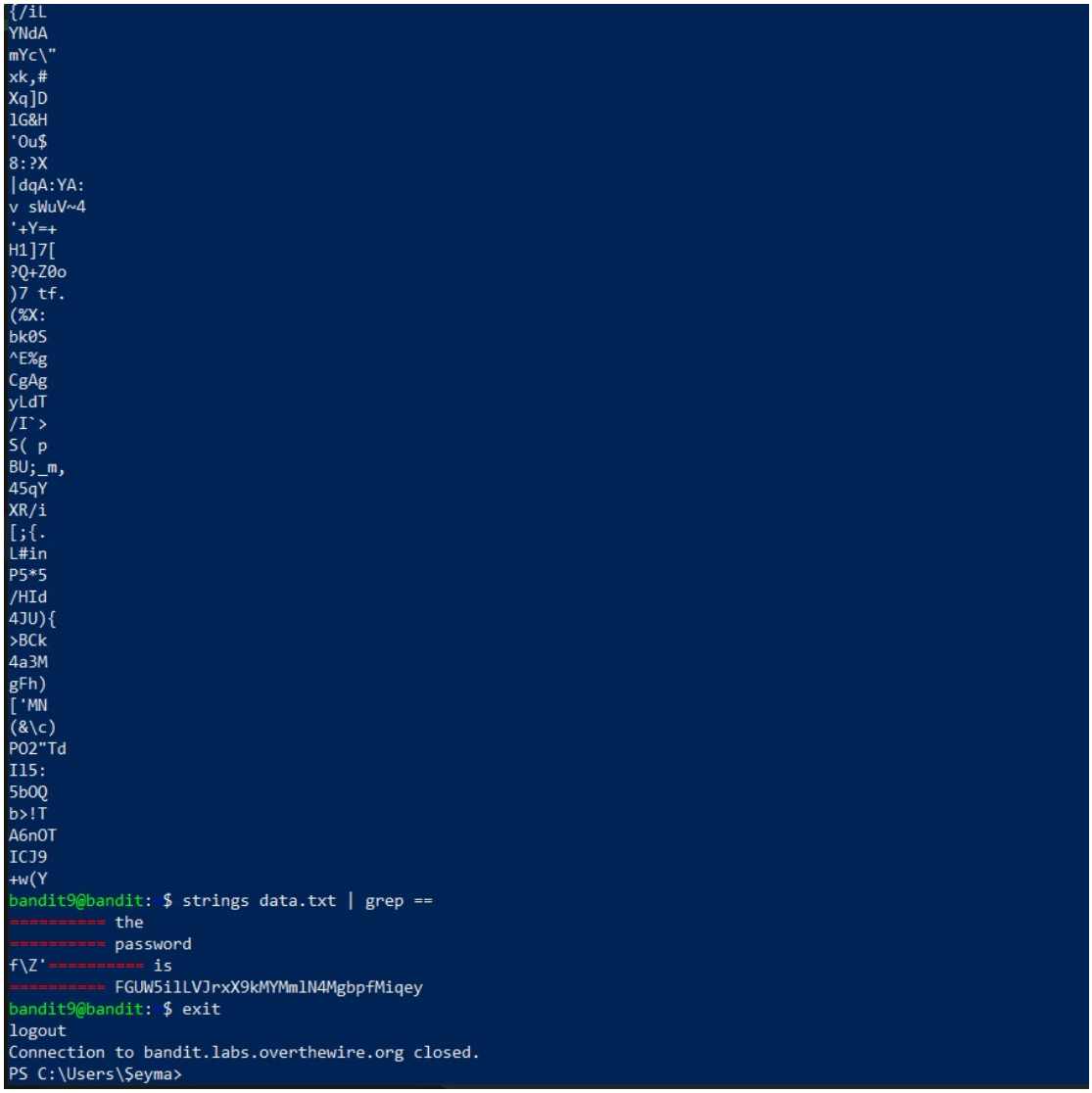
```
bandit7@bandit:~$ whoami
bandit7
bandit7@bandit:~$ ls
data.txt
bandit7@bandit:~$ grep millionth data.txt
millionth       dfwvzFQi4mU0wfNbFOe9RoWskMLg7eEc
bandit7@bandit:~$ exit
logout
Connection to bandit.labs.overthewire.org closed.
PS C:\Users\Seyma> ssh bandit8@bandit.labs.overthewire.org -p 2220
                         _                     _ _ _
                        | |__   __ _ _ __   __| (_) |_
                        | '_ \ / _` | '_ \ / _` | | __|
                        | |_) | (_| | | | | (_| | | |_
                        |_.__/ \__,_|_| |_|\__,_|_|\__|


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

backend: gibson-1
bandit8@bandit.labs.overthewire.org's password:
```

Level 8 → 9: Dosya içinde birçok satır defalarca tekrar ediyordu. Önce sort ile dosyayı alfabetik sıraya dizdim, ardından uniq -u komutuyla sadece bir kez geçen satırı (şifreyi) buldum.

```
bandit8@bandit:~$ whoami
bandit8
bandit8@bandit:~$ ls
data.txt
bandit8@bandit:~$ sort data.txt | uniq -u
4CKMh1JI91bUIZZPXDqGanal4xvAg0JM
bandit8@bandit:~$ exit
logout
Connection to bandit.labs.overthewire.org closed.
PS C:\Users\Seyma>
```

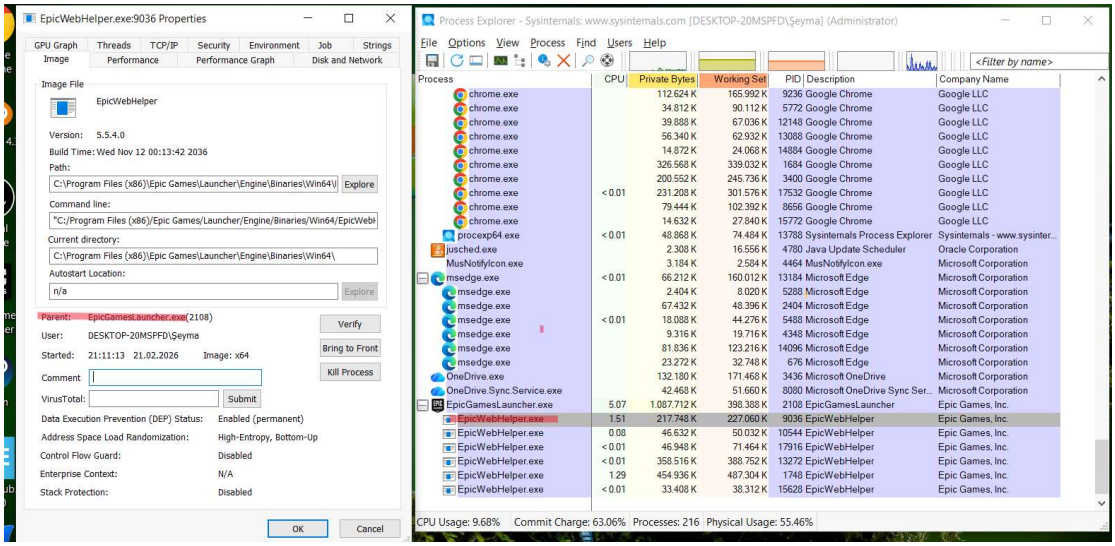
Level 9 → 10: data.txt dosyasını cat ile okumaya çalıştığımda karşıma okunamaz bir veri yığını çıktı. İksili bir dosya içindeki insan tarafından okunabilir karakter dizilerini bulmak için strings komutunu kullandım ve şifrenin yanındaki işaretleri yakalamak için grep == ile filtreleme yaptım.


bandit9@bandit:~$ whoami
bandit9
bandit9@bandit:~$ ls
data.txt
bandit9@bandit:~$ strings data.txt
Dm|H
d:Bj
pgM,
g%q&N
}}Jae
:AJsC
E!ML
~>#~
+PIqZ
Zf{,
========== the
tWIN
W9`5
UnTZ
[O9xK
6dG"I>
WJC<
UW'$
6cb6:
@;IT
(p.[1
Om5O
72eW
Y8)s
Y2V:
YF_|
&g2*7
kI`
"Qrx
V`$^
Qj,S@h7
95<M
/b:n
GP@~
I%3gA
caK3
uN1>4
Rxvk
x+#)?W
~:%e
+5,P_a
|@[h
6hsq



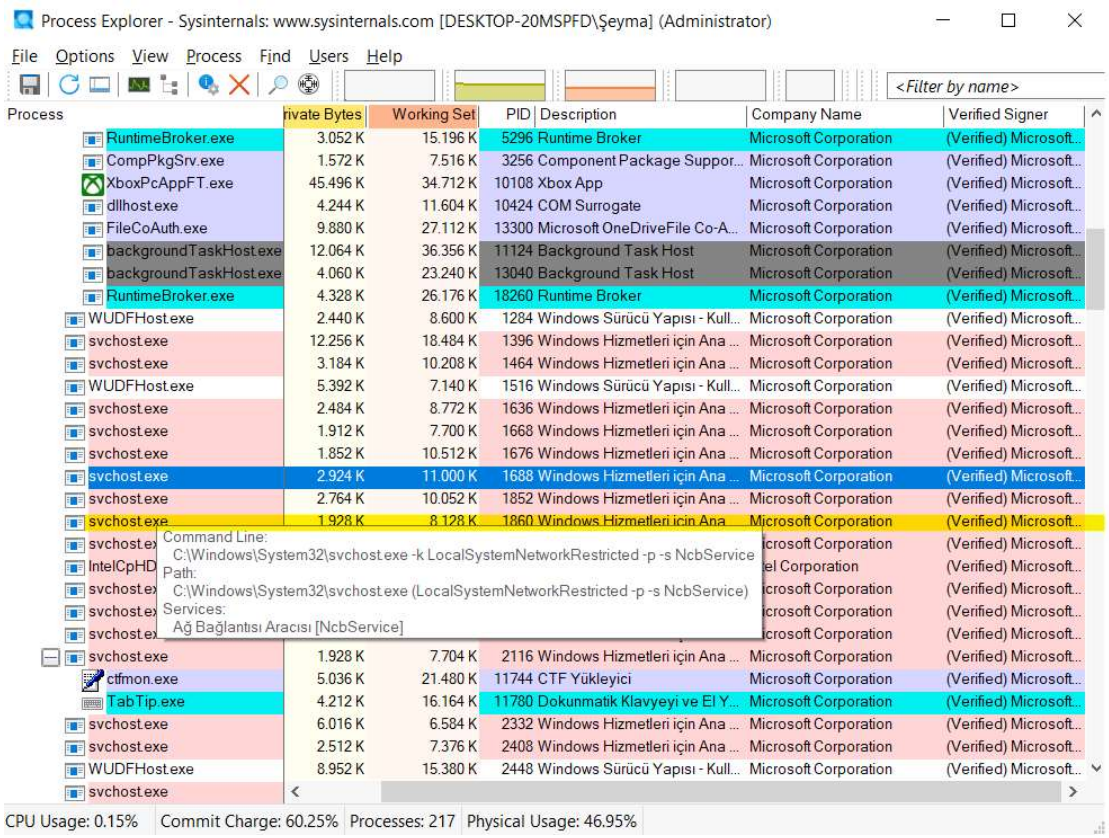
Cephe 2: Sysinternals Analizi (Windows)

1) Parent-Child (Ebeveyn-Çocuk) Analizi:



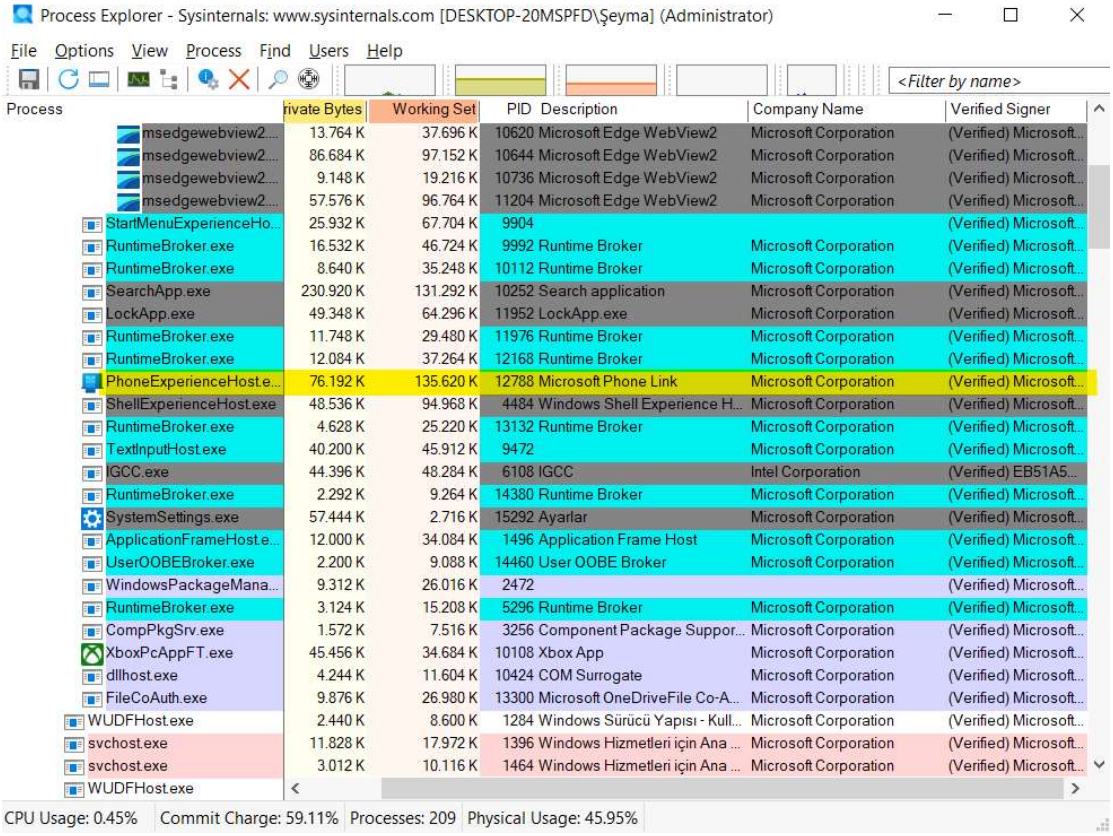
Yaptığım incelemede bu sürecin ebeveyninin (Parent) EpicGamesLauncher.exe

2) Svchost Avı (Service Host):



Fareyi sarı renkle işaretlenmiş bir svchost.exe (PID: 1860) üzerine getirdiğimde, bu sürecin tek bir iş değil, arka planda bir servis barındırdığını gördüm. Görselde de görüldüğü üzere bu süreç Ağ Bağlantısı Aracısı (NcbService) servisini taşımaktadır.

3) İmza Kontrolü (Verify Signatures):



Listeyi incelediğimde süreçlerin çoğunun yanında (Verified) Microsoft Windows yer almaktadır. Kırmızı veya mor renkle işaretlenmiş, imzası doğrulanmayan şüpheli bir süreçle karşılaşmadım. Bu özellik bir Malware Analisti için kritiktir çünkü saldırganlar dosyalarına chrome.exe veya svchost.exe gibi isimler vererek bizi kandırmaya çalışırlar. Ancak Microsoft'un veya güvenilir firmaların ıslak imzası niteliğindeki Dijital İmzayı taklit edemezler.

BÖLÜM D

1. Yetki Yükseltme (PrivEsc) Mantığı: Linux'ta bir dosyaya SUID biti atandığında, program kim çalıştırırsa çalıştırsın dosya sahibinin yetkisiyle çalışır. Vim gibi güçlü bir editöre root yetkisi verilirse, normal bir kullanıcı bile /etc/shadow veya /etc/sudoers dosyalarını okuyup değiştirebilir. Yani problem vim'in kendisi değil, ona verilen aşırı yetkidir. Bu küçük izin hatası, kullanıcıyı root seviyesinde işlem yapabilir hâle getirir.

2. Zararlı Yazılım Kamuflajı (Process Injection): Bir malware geliştirici, kodunu rastgele bir oyun.exe'ye değil, svchost.exe veya explorer.exe gibi sistem süreçlerine enjekte eder. Çünkü bu süreçler görev yöneticisinde normal görünür; kullanıcı onları zaten Windows'un temel parçaları olarak kabul eder. Böylece malware gizlenir.