

BÖLÜM A

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

Kavramsal Analiz: Linux çekirdeği donanımı yönetmek için özel arayzlere 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 yapabiliyoruz. Kisaca 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 çalıştırabileceğini anlamına gelir. Burdaki en önemli kısım ve tehlikeli kısım Others yani yazma iznidir. Bu yazma izni çok tehlikelidir çünkü sisteme 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 yazıldığı /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 kapatırırdı ve kritik bir olay yaşanmazdı. Bu nedenle kritik

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

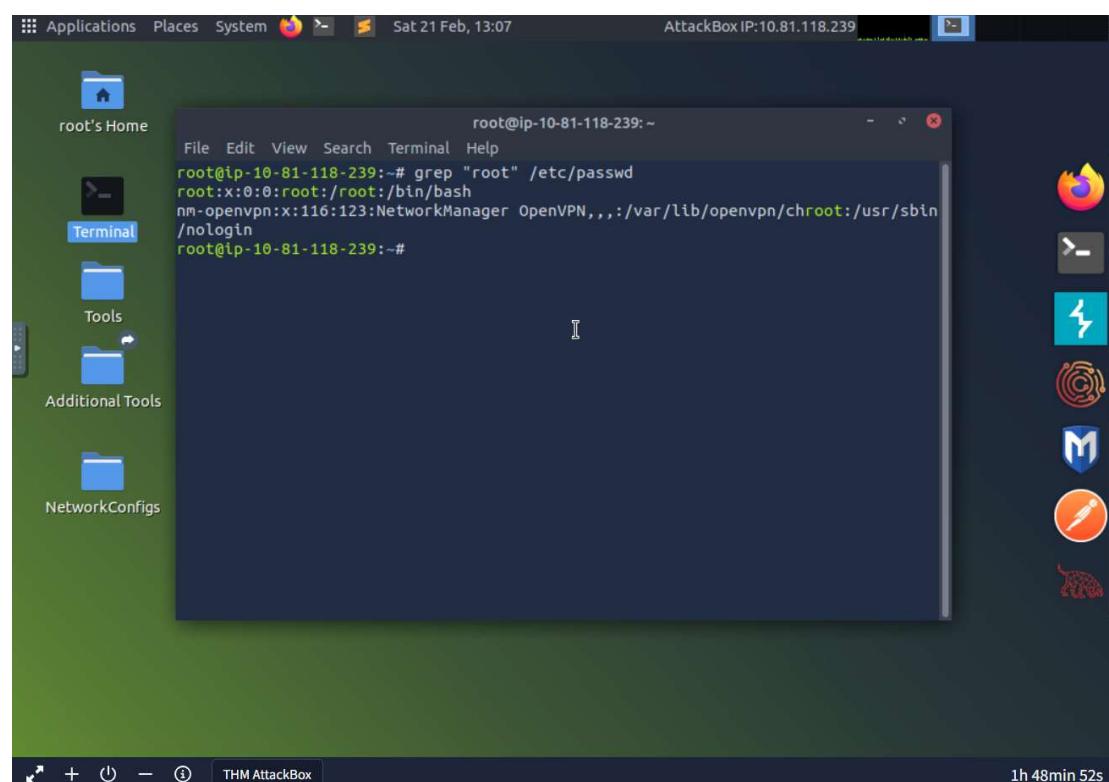
Registry (Kayıt Defteri) Anatomisi: HKLM (HKEY_LOCAL_MACHINE) bilgisayarın genel ayarlarıdır. Hangi kullanıcı girerse girsin, klavye dili veya yüklü programlar gibi ayarlar buradan okunur. HKCU (HKEY_CURRENT_USER) ise sadece o an oturan kişinin Masaüstü resmi, tarayıcı geçmiş gibi kişisel ayarlarıdır. 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 çokince ayarlar yapılabilir. Bu büyük şirketlerde yetkisiz erişimi engelleyerek veri güvenliğinin bel kemğini oluşturur.

BÖLÜM B

Görev 1

1) grep "root" /etc/passwd



The screenshot shows a Linux desktop environment with a dark theme. A terminal window is open, displaying the command 'grep "root" /etc/passwd' and its output. The output includes the root user's entry in the password file. The desktop interface includes a file manager sidebar on the left and a dock with various icons at the bottom right.

```
root@ip-10-81-118-239:~# grep "root" /etc/passwd
root:x:0:0:root:/root:/bin/bash
nm-openvpn:x:116:123:NetworkManager OpenVPN,,,:/var/lib/openvpn/chroot:/usr/sbin/nologin
root@ip-10-81-118-239:~#
```

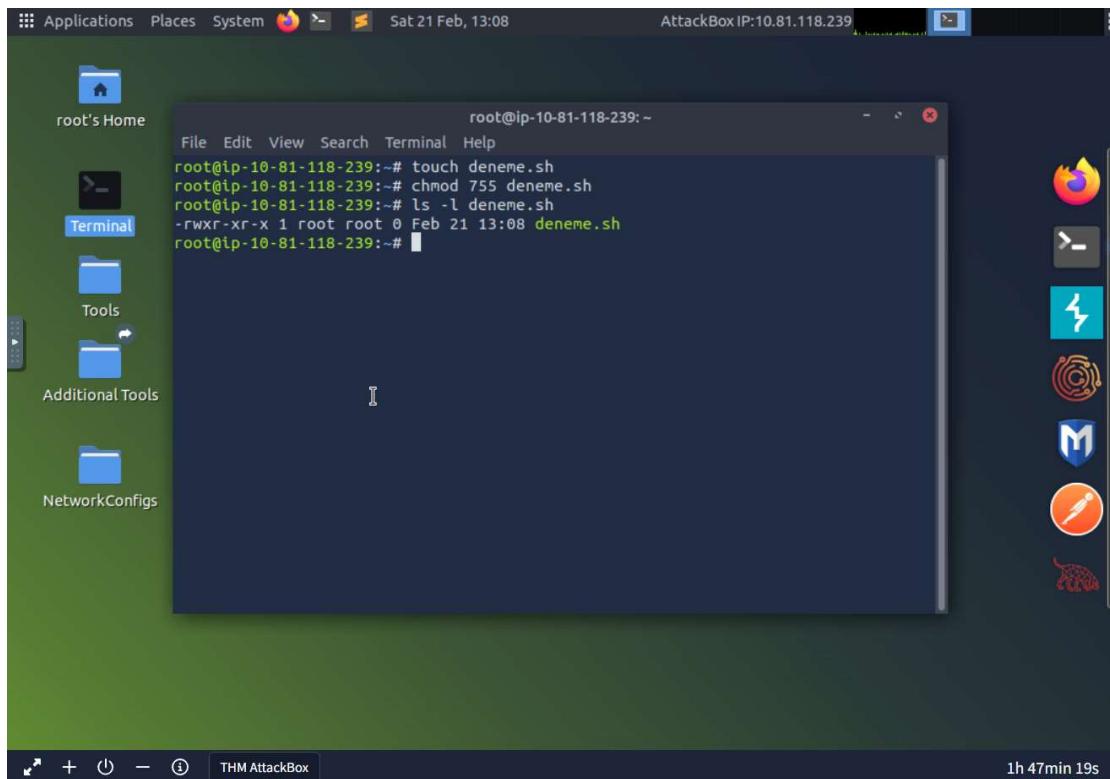
Bu komutu /etc/passwd dosyasının içinde "root" kelimesini aramak için kullandım.

2) cat test.txt | grep "root"

```
root@ip-10-81-73-26:~# echo -e "hello\nroot user\nadmin\nroot access" > test.txt
root@ip-10-81-73-26:~# cat test.txt | grep "root"
root user
root access
root@ip-10-81-73-26:~#
```

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 çalışma 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 kaldırılamayıp 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 olarak 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.

```
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: ZjLjTmM6FvvyRnrb2rfNW0ZOTa6ip5If

bandit0@bandit: $
```

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

```
bandit1@bandit: ~
For support, questions or comments, contact us on discord or IRC.
Enjoy your stay!

bandit1@bandit: $ whoami
bandit1
bandit1@bandit: $ ls
-
bandit1@bandit: $ cat ./*
263JGJPfgU6LtdEvgfWU1XP5yac29mFx
bandit1@bandit: $
```

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.

```
bandit2@bandit: ~
lip Desktop App: $ ls
--spaces in this filename--
bandit2@bandit: $ cat ./--spaces\ in\ this\ filename--
MNk8KNH3Usii041PRUEoDFPqfxLP1Smx
bandit2@bandit: $
```

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..

```
bandit3@bandit: ~/inhere
bandit3@bandit: $ whoami
bandit3
bandit3@bandit: $ ls
.
..
bandit3@bandit: $ cd inhere
bandit3@bandit: ~/inhere $ ls -la
total 12
drwxr-xr-x 2 root      root    4096 Oct 14 09:26 .
drwxr-xr-x 3 root      root    4096 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
bandit3@bandit: ~/inhere $
```

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.

```
bandit4@bandit: ~/inhere
bandit4@bandit: $ whoami
bandit4
bandit4@bandit: $ ls
inhere
bandit4@bandit: $ cd inhere
bandit4@bandit: ~/inhere$ ls -la
total 48
drwxr-xr-x 2 root      root      4096 Oct 14 09:26 .
drwxr-xr-x 3 root      root      4096 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$ ./file ./*file */
./file: cannot open './file' (No such file or directory)
./file00: data
./file01: OpenPGP Public Key
./file02: OpenPGP Public Key
./file03: data
./file04: data
./file05: data
./file06: data
./file07: ASCII text
./file08: data
./file09: data
bandit4@bandit: ~/inhere$ cat ./file07
4oYVPkxZ00E005pTW81FB8j8lxXGUQw
bandit4@bandit: ~/inhere$
```

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
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)
./maybehere16/.file2: ASCII text, with very long lines (8471)
```

```
Seç bandit5@bandit: ~/inhere
./maybehere01-/file2: ASCII text
./maybehere01/spaces file1: ASCII text, with very long lines (4138)
./maybehere00-/file1: ASCII text, with very long lines (550)
./maybehere00-/file2: ASCII text, with very long lines (7835)
./maybehere00-/file1: ASCII text, with very long lines (1038)
./maybehere00/spaces file2: ASCII text, with very long lines (6849)
./maybehere00-/file2: ASCII text, with very long lines (9387)
./maybehere00/spaces file1: ASCII text, with very long lines (6117)
./maybehere05-/file1: ASCII text, with very long lines (3200)
./maybehere05/.file2: ASCII text, with very long lines (5916)
./maybehere05-/file1: ASCII text, with very long lines (2345)
./maybehere05/spaces file2: ASCII text, with very long lines (2419)
./maybehere05-/file2: ASCII text, with very long lines (5958)
./maybehere05/spaces file1: ASCII text, with very long lines (879)
./maybehere02-/file1: ASCII text, with very long lines (6350)
./maybehere02/.file2: ASCII text, with very long lines (2576)
./maybehere02-/file1: ASCII text, with very long lines (3800)
./maybehere02/spaces file2: ASCII text, with very long lines (8487)
./maybehere02/spaces file1: ASCII text, with very long lines (6745)
./maybehere03-/file1: ASCII text, with very long lines (9768)
./maybehere03/.file2: ASCII text, with very long lines (8879)
./maybehere03-/file1: ASCII text, with very long lines (314)
./maybehere03/spaces file2: ASCII text, with very long lines (3384)
./maybehere03-/file2: ASCII text, with very long lines (6594)
./maybehere03/spaces file1: ASCII text, with very long lines (2189)
./maybehere06-/file1: ASCII text, with very long lines (1270)
./maybehere06/.file2: ASCII text, with very long lines (8975)
./maybehere06-/file1: ASCII text, with very long lines (5730)
./maybehere06/spaces file2: ASCII text, with very long lines (4250)
./maybehere06-/file2: ASCII text, with very long lines (1075)
./maybehere06/spaces file1: ASCII text, with very long lines (4072)
bandit5@bandit: ~$ find . -type f -size 1033c
./maybehere07/.file2
bandit5@bandit: ~$ cat ./maybehere07/.file2
HWasnPhtq9AVKe0dmk45nxy20cvUa6EG
```

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.

```
bandit6@bandit: ~
* gef (https://github.com/hugsy/gef) in /opt/gef/
* pwndbg (https://github.com/pwndbg/pwndbg) in /opt/pwndbg/
* gdbinit (https://github.com/gdbinit/Gdbinit) in /opt/gdbinit/
* pwntools (https://github.com/Gallopsled/pwntools)
* radare2 (http://www.radare.org/)

--[ More information ]--

For more information regarding individual wargames, visit
http://www.overthewire.org/wargames/

For support, questions or comments, contact us on discord or IRC.

Enjoy your stay!

bandit6@bandit: $ whoami
bandit6
bandit6@bandit: $ ls
bandit6@bandit: $ ls -la
total 20
drwxr-xr-x  2 root root 4096 Oct 14 09:25 .
drwxr-xr-x 150 root root 4096 Oct 14 09:29 ..
-rw-r--r--  1 root root  220 Mar 31 2024 .bash_logout
-rw-r--r--  1 root root 3851 Oct 14 09:19 .bashrc
-rw-r--r--  1 root root  807 Mar 31 2024 .profile
bandit6@bandit: $ find / -type f -user bandit7 -group bandit6 -size 33c 2>/dev/null
/var/lib/dpkg/info/bandit7.password
bandit6@bandit: $ cat /var/lib/dpkg/info/bandit7.password
morbNTDkSw6jIlUc0ym0dMaLn0lFVAaj
bandit6@bandit: $
```

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\Şeyma> 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\Şeyma>
```

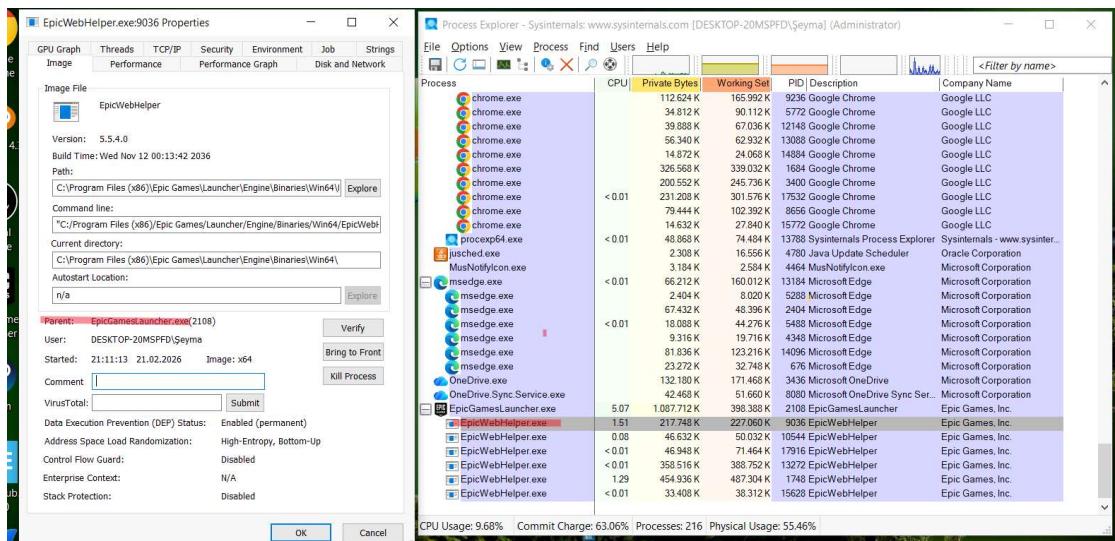
Level 9 → 10: data.txt dosyasını cat ile okumaya çalıştığımda çalışma okunamaz bir veri yiğini çıktı. İksili bir dosya içindeki insan tarafından okunabilir karakter dizilerini bulmak için strings komutunu kullandım ve şifrenin yanındaki işaretleri yakalamak için grep == ile filtreleme yaptım.

```
bandit9@bandit: $ whoami
bandit9
bandit9@bandit: $ ls
data.txt
bandit9@bandit: $ strings data.txt
Dm|H
d:Bj
pgM,
g%&N
} } Jae
: AjsC
E!ML
~>#~
+PIqZ
Zf{,
=====
the
tWIN
W9'5
UnTZ
[09xK
6dG*I>
W]C<
UW'$
6cb6:
@;IT
(p.[1
0m50
    72eW
Y8)s
Y2V:
YF_|
&g2*7
    kI`_
"Qrx
V`$^
Qj,S@h7
95<M
/b:n
GP@~
I%3gA
caK3
uN1z4
Rxvk
x++#)?W
~:xe
+5,P_a
|@[h
6hsq
```

```
{/iL
YNdA
mYc"
xk,#
Xq]D
lG&H
'0u$
8:?X
|dqA:YA:
v s\luV~4
'+Y=+
H1]7[
?Q+Z0o
)7 tf.
(%X:
bk0S
^E%g
CgAg
yLdT
/I`>
S( p
BU;_m,
45qY
XR/i
[;{.
L#in
P5*5
/HId
4JU){
>BCK
4a3M
gFh)
[ 'MN
(&\c)
P02"Td
I15:
5b0Q
b>!T
A6nOT
ICJ9
+w(Y
bandit9@bandit: $ strings data.txt | grep ==
===== the
===== password
f\Z ===== is
===== FGUW5i1LVJrxX9kMYMmlN4MgbpfMiqey
bandit9@bandit: $ exit
logout
Connection to bandit.labs.overthewire.org closed.
PS C:\Users\Seyma>
```

Cephe 2: Sysinternals Analizi (Windows)

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



Yaptığım incelemede bu sürecin ebeveyninin (Parent) EpicGamesLauncher.exe

2) Svchost Avı (Service Host):

Process	Private Bytes	Working Set	PID	Description	Company Name	Verified Signer
RuntimeBroker.exe	3.052 K	15.196 K	5296	Runtime Broker	Microsoft Corporation	(Verified) Microsoft...
CompPkgSrv.exe	1.572 K	7.516 K	3256	Component Package Suppor...	Microsoft Corporation	(Verified) Microsoft...
XboxPcAppFT.exe	45.496 K	34.712 K	10108	Xbox App	Microsoft Corporation	(Verified) Microsoft...
dllhost.exe	4.244 K	11.604 K	10424	COM Surrogate	Microsoft Corporation	(Verified) Microsoft...
FileCoAuth.exe	9.880 K	27.112 K	13300	Microsoft OneDriveFile Co-A...	Microsoft Corporation	(Verified) Microsoft...
backgroundTaskHost.exe	12.064 K	36.356 K	11124	Background Task Host	Microsoft Corporation	(Verified) Microsoft...
backgroundTaskHost.exe	4.060 K	23.240 K	13040	Background Task Host	Microsoft Corporation	(Verified) Microsoft...
RuntimeBroker.exe	4.328 K	26.176 K	18260	Runtime Broker	Microsoft Corporation	(Verified) Microsoft...
WUDFHost.exe	2.440 K	8.600 K	1284	Windows Sürücü Yaptırı - Kull...	Microsoft Corporation	(Verified) Microsoft...
svchost.exe	12.256 K	18.484 K	1396	Windows Hizmetleri için Ana ...	Microsoft Corporation	(Verified) Microsoft...
svchost.exe	3.184 K	10.208 K	1464	Windows Hizmetleri için Ana ...	Microsoft Corporation	(Verified) Microsoft...
WUDFHost.exe	5.392 K	7.140 K	1516	Windows Sürücü Yaptırı - Kull...	Microsoft Corporation	(Verified) Microsoft...
svchost.exe	2.484 K	8.772 K	1636	Windows Hizmetleri için Ana ...	Microsoft Corporation	(Verified) Microsoft...
svchost.exe	1.912 K	7.700 K	1668	Windows Hizmetleri için Ana ...	Microsoft Corporation	(Verified) Microsoft...
svchost.exe	1.852 K	10.512 K	1676	Windows Hizmetleri için Ana ...	Microsoft Corporation	(Verified) Microsoft...
svchost.exe	2.924 K	11.000 K	1688	Windows Hizmetleri için Ana ...	Microsoft Corporation	(Verified) Microsoft...
svchost.exe	2.764 K	10.052 K	1852	Windows Hizmetleri için Ana ...	Microsoft Corporation	(Verified) Microsoft...
svchost.exe	1.928 K	8.128 K	1860	Windows Hizmetleri için Ana ...	Microsoft Corporation	(Verified) Microsoft...
svchost.exe				Command Line: C:\Windows\System32\svchost.exe -k LocalSystemNetworkRestricted -p -s NcbService	Microsoft Corporation	(Verified) Microsoft...
IntelCphID				Path: C:\Windows\System32\svchost.exe (LocalSystemNetworkRestricted -p -s NcbService)	Microsoft Corporation	(Verified) Microsoft...
svchost				Services: Ağ Bağlantısı Aracı (NcbService)	Microsoft Corporation	(Verified) Microsoft...
svchost.exe					Microsoft Corporation	(Verified) Microsoft...
svchost.exe					Microsoft Corporation	(Verified) Microsoft...
cifmon.exe	1.928 K	7.704 K	2116	Windows Hizmetleri için Ana ...	Microsoft Corporation	(Verified) Microsoft...
TabTip.exe	5.036 K	21.480 K	11744	CTF Yükleyici	Microsoft Corporation	(Verified) Microsoft...
svchost.exe	4.212 K	16.164 K	11780	Dokunmatik Klavyeyi ve El Y...	Microsoft Corporation	(Verified) Microsoft...
svchost.exe	6.016 K	6.584 K	2332	Windows Hizmetleri için Ana ...	Microsoft Corporation	(Verified) Microsoft...
svchost.exe	2.512 K	7.376 K	2408	Windows Hizmetleri için Ana ...	Microsoft Corporation	(Verified) Microsoft...
WUDFHost.exe	8.952 K	15.380 K	2448	Windows Sürücü Yaptırı - Kull...	Microsoft Corporation	(Verified) Microsoft...
svchost.exe						

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

3) İmza Kontrolü (Verify Signatures):

Process Explorer - Sysinternals: www.sysinternals.com [DESKTOP-20MSPFD\Şeyma] (Administrator)

Process	Private Bytes	Working Set	PID	Description	Company Name	Verified Signer
msedgewebview2...	13.764 K	37.696 K	10620	Microsoft Edge WebView2	Microsoft Corporation	(Verified) Microsoft...
msedgewebview2...	86.684 K	97.152 K	10644	Microsoft Edge WebView2	Microsoft Corporation	(Verified) Microsoft...
msedgewebview2...	9.148 K	19.216 K	10736	Microsoft Edge WebView2	Microsoft Corporation	(Verified) Microsoft...
msedgewebview2...	57.576 K	96.764 K	11204	Microsoft Edge WebView2	Microsoft Corporation	(Verified) Microsoft...
StartMenuExperienceHo...	25.932 K	67.704 K	9904			(Verified) Microsoft...
RuntimeBroker.exe	16.532 K	46.724 K	9992	Runtime Broker	Microsoft Corporation	(Verified) Microsoft...
RuntimeBroker.exe	8.640 K	35.248 K	10112	Runtime Broker	Microsoft Corporation	(Verified) Microsoft...
SearchApp.exe	230.920 K	131.292 K	10252	Search application	Microsoft Corporation	(Verified) Microsoft...
LockApp.exe	49.348 K	64.296 K	11952	LockApp.exe	Microsoft Corporation	(Verified) Microsoft...
RuntimeBroker.exe	11.748 K	29.480 K	11976	Runtime Broker	Microsoft Corporation	(Verified) Microsoft...
RuntimeBroker.exe	12.084 K	37.264 K	12168	Runtime Broker	Microsoft Corporation	(Verified) Microsoft...
PhoneExperienceHoste...	76.192 K	135.620 K	12788	Microsoft Phone Link	Microsoft Corporation	(Verified) Microsoft...
ShellExperienceHostExe	48.536 K	94.968 K	4484	Windows Shell Experience H...	Microsoft Corporation	(Verified) Microsoft...
RuntimeBroker.exe	4.628 K	25.220 K	13132	Runtime Broker	Microsoft Corporation	(Verified) Microsoft...
TextInputHost.exe	40.200 K	45.912 K	9472		Microsoft Corporation	(Verified) Microsoft...
IGCC.exe	44.396 K	48.284 K	6108	IGCC	Intel Corporation	(Verified) EB51A5...
RuntimeBroker.exe	2.292 K	9.264 K	14380	Runtime Broker	Microsoft Corporation	(Verified) Microsoft...
SystemSettings.exe	57.444 K	2.716 K	15292	Ayarlar	Microsoft Corporation	(Verified) Microsoft...
ApplicationFrameHoste...	12.000 K	34.084 K	1496	Application Frame Host	Microsoft Corporation	(Verified) Microsoft...
UserOOBEBroker.exe	2.200 K	9.088 K	14460	User OOBE Broker	Microsoft Corporation	(Verified) Microsoft...
WindowsPackageManag...	9.312 K	26.016 K	2472			(Verified) Microsoft...
RuntimeBroker.exe	3.124 K	15.208 K	5296	Runtime Broker	Microsoft Corporation	(Verified) Microsoft...
CompPkgSrv.exe	1.572 K	7.516 K	3256	Component Package Suppor...	Microsoft Corporation	(Verified) Microsoft...
XboxPcAppFT.exe	45.456 K	34.684 K	10108	Xbox App	Microsoft Corporation	(Verified) Microsoft...
dllhost.exe	4.244 K	11.604 K	10424	COM Surrogate	Microsoft Corporation	(Verified) Microsoft...
FileCoAuth.exe	9.876 K	26.980 K	13300	Microsoft OneDriveFile Co-A...	Microsoft Corporation	(Verified) Microsoft...
WUDFHost.exe	2.440 K	8.600 K	1284	Windows Sürücü Yaptı - Kull...	Microsoft Corporation	(Verified) Microsoft...
svchost.exe	11.828 K	17.972 K	1396	Windows Hizmetleri için Ana ...	Microsoft Corporation	(Verified) Microsoft...
svchost.exe	3.012 K	10.116 K	1464	Windows Hizmetleri için Ana ...	Microsoft Corporation	(Verified) Microsoft...
WUDFHost.exe						

CPU Usage: 0.45% Commit Charge: 59.11% Processes: 209 Physical Usage: 45.95%

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) Mantiğı: Linux'ta bir dosyaya SUID biti atandığında, program kim çalıştırırsa çalıştırınsın 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, kullanıcayı 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.