

BANDİT

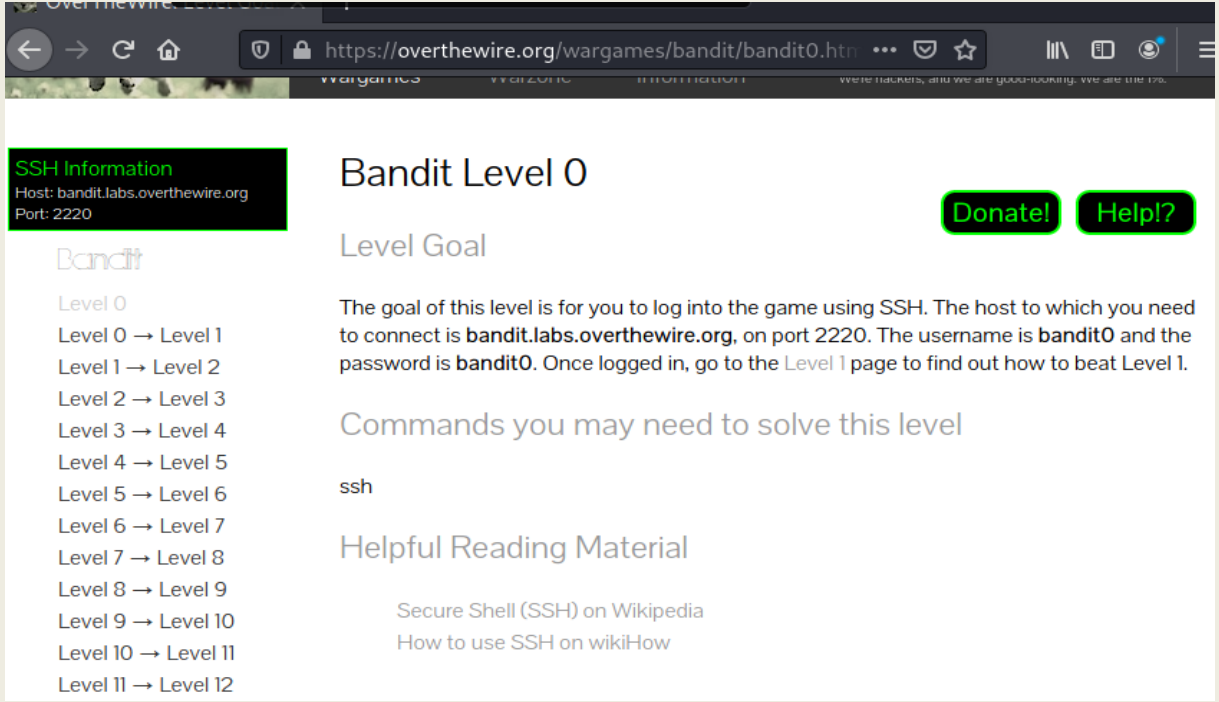
Kaan Efe Öğüt

ADLİ BİLİŞİM MÜHENDİSLİĞİ

-Vulnhub üzerinde bulunan “Bandit” zafiyetli CTF makinesinin çözümünü gerçekleştireceğiz.

14.11.2021

"Overthewire.org" bağlantısı üzerinde bulunan oyun tarzında bir ctf çözerek öncelikle linux bilgilerimizi tazelemek istiyorum. Bu CTF 34 levelden oluşmaktadır.



The screenshot shows the Overthewire.org Bandit Level 0 page. The page has a dark theme. On the left, there is a sidebar with a list of levels from 0 to 12. The main content area is titled "Bandit Level 0" and includes a "Level Goal" section, "Commands you may need to solve this level" (listing "ssh"), and "Helpful Reading Material" (linking to Wikipedia and wikiHow). There are also "Donate!" and "Help!" buttons.

SSH Information
Host: bandit.labs.overthewire.org
Port: 2220

Bandit Level 0

[Donate!](#) [Help!](#)

Level Goal

The goal of this level is for you to log into the game using SSH. The host to which you need to connect is **bandit.labs.overthewire.org**, on port 2220. The username is **bandit0** and the password is **bandit0**. Once logged in, go to the [Level 1](#) page to find out how to beat Level 1.

Commands you may need to solve this level

ssh

Helpful Reading Material

- [Secure Shell \(SSH\) on Wikipedia](#)
- [How to use SSH on wikiHow](#)

-Sitenin görüntüsü bu şekildedir. Seviye 0'dan başlıyorum.

-Burada SSH üzerinden gerekli bilgiler verilmiştir.

```
(root@kali)~# ssh bandit0@bandit.labs.overthewire.org -p 2220
The authenticity of host '[bandit.labs.overthewire.org]:2220 ([176.9.9.172]:2220)' can't be established.
ECDSA key fingerprint is SHA256:98UL0ZW85496EtCRkKLo20X30PnyPSB5tB5RPbhczc.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '[bandit.labs.overthewire.org]:2220,[176.9.9.172]:2220' (ECDSA) to the list of known hosts.
This is a OverTheWire game server. More information on http://www.overthewire.org/wargames
bandit0@bandit.labs.overthewire.org's password: 
```

Tarafıma verilen SSH bağlantısı üzerinden giriş yapıyorum.

```

* checksec.sh (http://www.trapkit.de/tools/checksec.html) in /usr/local/bin/checksec.sh

--[ More information ]--
Level 10 → Level 11
For more information regarding individual wargames, visit
http://www.overthewire.org/wargames/
Level 12 → Level 13
For support, questions or comments, contact us through IRC on
irc.overthewire.org #wargames.
Level 14 → Level 15
Level 15 → Level 16
Enjoy your stay!

bandit0@bandit:~$ pwd
/home/bandit0
bandit0@bandit:~$ ls
readme
bandit0@bandit:~$ cat readme
boJ9jbbUNNfktD7800psq0ltutMc3MY1
bandit0@bandit:~$

```

-Site üzerinde level 0>level 1 bağlantısına baktığımda seviyeler arası nasıl geçiş yapabileceğimi anlatıyor.

-Level atlamak için bulunan readme.txt dosyasının içerisinde ki Kullanıcı adı ve şifreye ulaşmam gerekmektedir.Dosyaya girdiğimde içerisinde bir sonraki levelin şifresine ulaşıyorum.

```

(root@kali)-[~]
# ssh bandit1@bandit.labs.overthewire.org -p 2220
This is a OverTheWire game server. More information on http://www.overthewire.org/wargames

bandit1@bandit.labs.overthewire.org's password:
Linux bandit.otw.local 5.4.8 x86_64 GNU/Linux

```

- Şimdi ise site üzerinden tekrardan level geçme bilgisine bakıyorum.Burada bandit1 kullanıcısı ile bulunan şifre üzerinden giriş yapmam gerektiği söyleniyor.

```

bandit1@bandit:/home$ cd bandit1
bandit1@bandit:~$ ls -la
total 24
-rw-r--r-- 1 bandit2 bandit1 33 May 7 2020 -
drwxr-xr-x 2 root root 4096 May 7 2020 .
drwxr-xr-x 41 root root 4096 May 7 2020 ..
-rw-r--r-- 1 root root 220 May 15 2017 .bash_logout
-rw-r--r-- 1 root root 3526 May 15 2017 .bashrc
-rw-r--r-- 1 root root 675 May 15 2017 .profile
bandit1@bandit:~$ cat ./-
CV1DtqXWVFXTvM2F0k09SHz0YwRINYA9
bandit1@bandit:~$

```

- Burada "-" isimli dosya içerisinde bulunan bilgileri ele geçirmem isteniyor fakat cat komutu ile doğrudan açamadığım için cat "./-" komutu ile içeriği görüntülüyorum ve şifreyi kopyalıyorum.

```
bandit2@bandit: ~  
Dosya Eylemler Düzen Görünüm Yardım  
bandit2@bandit:~$ ls  
spaces in this filename  
bandit2@bandit:~$ cat spaces\ in\ this\ filename  
UmHadQclWmgdLOKQ3YNggjWxGoRmb5lUk  
bandit2@bandit:~$
```

- Bana verdiği ipucunda boşluklu bir dosyayı okuyabilip okuyamadığımı denedi fakat cat ardından spaces komutunu yazıp taba bastığımda kod tamamlandı.

-Burada bana bir şifre verdi ve kullanıcıyı değiştirip işlemlerime devam edeceğim.

- En son seviye 3 e geçmiştik ve burada gizli bir dosya bulunduğu ve bunun içerisinde şifrenin bulunduğunu bana söylüyor.

```
bandit3@bandit:~$ ls -la  
total 24  
drwxr-xr-x 3 root root 4096 May 7 2020 .  
drwxr-xr-x 41 root root 4096 May 7 2020 ..  
-rw-r--r-- 1 root root 220 May 15 2017 .bash_logout  
-rw-r--r-- 1 root root 3526 May 15 2017 .bashrc  
drwxr-xr-x 2 root root 4096 May 7 2020 inhere  
-rw-r--r-- 1 root root 675 May 15 2017 .profile  
bandit3@bandit:~$ cd inhere  
bandit3@bandit:~/inhere$ ls  
bandit3@bandit:~/inhere$ ls -la  
total 12  
drwxr-xr-x 2 root root 4096 May 7 2020 .  
drwxr-xr-x 3 root root 4096 May 7 2020 ..  
-rw-r----- 1 bandit4 bandit3 33 May 7 2020 .hidden  
bandit3@bandit:~/inhere$ cat .hidden  
pIwrPrtPN36QITSp3EQaw936yaFoFgAB
```

-Burada gizli dosyaları ls-la komutu ile görüntüleyip elde ettiğim şifre ile seviye atlıyorum.

-Elde ettiğim şifre ile bandit4 e giriş yaptım.

```
bandit4@bandit:~/inhere$ ls  
-file00 -file01 -file02 -file03 -file04 -file05 -file06 -file07 -file08 -file09  
bandit4@bandit:~/inhere$ cat ./-file00  
p2f%rL~5g  bandit4@bandit:~/inhere$ cat ./-file01  
p,k; r*  .!C  bandit4@bandit:~/inhere$ cat ./-file02  
e) 5  
pV  bandit4@bandit:~/inhere$ cat ./-file03  
h!TQ0 4"aP7ph  bandit4@bandit:~/inhere$ cat ./-file04  
?  bandit4@bandit:~/inhere$ cat ./-file05  
r?h9('!y e#x  bandit4@bandit:~/inhere$ cat ./-file06  
ly  A f  E{  bandit4@bandit:~/inhere$ cat ./-file07  
koReBOKuIDDepwhWk7jZC0RTdopnAYKh  
bandit4@bandit:~/inhere$
```

-Burada karşıma 9 adet dosya çıktı ve içlerini öğrendiğim gibi açtığımda gerekli şifreyi elde ettim.

-5.Seviyeye geçiş yaptığımda burada "human-readable,1033 bytes ve not executable" olan klasör içerisinde olduğunu belirtiyor.

```
bandit5@bandit: ~/inhere
Dosya Eylemler Düzen Görünüm Yardım
bandit5@bandit:~/inhere$ ls
maybehere00 maybehere03 maybehere06 maybehere09 maybehere12 maybehere15 maybehere18
maybehere01 maybehere04 maybehere07 maybehere10 maybehere13 maybehere16 maybehere19
maybehere02 maybehere05 maybehere08 maybehere11 maybehere14 maybehere17
bandit5@bandit:~/inhere$ ls -la
total 88
drwxr-x--- 22 root bandit5 4096 May 7 2020 .
drwxr-xr-x 3 root root 4096 May 7 2020 ..
drwxr-x--- 2 root bandit5 4096 May 7 2020 maybehere00
drwxr-x--- 2 root bandit5 4096 May 7 2020 maybehere01
drwxr-x--- 2 root bandit5 4096 May 7 2020 maybehere02
drwxr-x--- 2 root bandit5 4096 May 7 2020 maybehere03
drwxr-x--- 2 root bandit5 4096 May 7 2020 maybehere04
drwxr-x--- 2 root bandit5 4096 May 7 2020 maybehere05
drwxr-x--- 2 root bandit5 4096 May 7 2020 maybehere06
drwxr-x--- 2 root bandit5 4096 May 7 2020 maybehere07
drwxr-x--- 2 root bandit5 4096 May 7 2020 maybehere08
drwxr-x--- 2 root bandit5 4096 May 7 2020 maybehere09
drwxr-x--- 2 root bandit5 4096 May 7 2020 maybehere10
drwxr-x--- 2 root bandit5 4096 May 7 2020 maybehere11
drwxr-x--- 2 root bandit5 4096 May 7 2020 maybehere12
drwxr-x--- 2 root bandit5 4096 May 7 2020 maybehere13
drwxr-x--- 2 root bandit5 4096 May 7 2020 maybehere14
drwxr-x--- 2 root bandit5 4096 May 7 2020 maybehere15
drwxr-x--- 2 root bandit5 4096 May 7 2020 maybehere16
drwxr-x--- 2 root bandit5 4096 May 7 2020 maybehere17
drwxr-x--- 2 root bandit5 4096 May 7 2020 maybehere18
drwxr-x--- 2 root bandit5 4096 May 7 2020 maybehere19
bandit5@bandit:~/inhere$ find . -type f -size 1033c
./maybehere07/.file2
bandit5@bandit:~/inhere$ find . -type f -size 1033c -executable
bandit5@bandit:~/inhere$ find . -type f -size 1033c ! -executable
./maybehere07/.file2
bandit5@bandit:~/inhere$ cat ./maybehere07/.file2
DXJZPULLxYr17uwoI01bNLQbtFemEgo7
```

-Burada find komutunu kullanıp dosyayı bulmaya çalışacağım.

-Yaptığım arama sonucunda level atlatacak şifreye erişim sağlayabildim.

```
bandit6@bandit:~$ find / -type f -user bandit7 -group bandit6 -size 33c
find: '/root': Permission denied
find: '/home/bandit28-git': Permission denied
find: '/home/bandit30-git': Permission denied
find: '/home/bandit5/inhere': Permission denied
find: '/home/bandit27-git': Permission denied
find: '/home/bandit29-git': Permission denied
find: '/home/bandit31-git': Permission denied
find: '/lost+found': Permission denied
find: '/etc/ssl/private': Permission denied
find: '/etc/polkit-1/localauthority': Permission denied
find: '/etc/lvm/archive': Permission denied
find: '/etc/lvm/backup': Permission denied
find: '/sys/fs/pstore': Permission denied
find: '/proc/tty/driver': Permission denied
find: '/proc/10100/task/10100/fdinfo/6': No such file or directory
find: '/proc/10100/fdinfo/5': No such file or directory
find: '/cgroup2/csessions': Permission denied
find: '/boot/lost+found': Permission denied
find: '/tmp': Permission denied
find: '/run/lvm': Permission denied
```

-6.Seviyeye geçiş yaptığımda burada bir arama yapmamı istiyor.Bu sefer yaptığım aramada . komutuyla değil / komutu ile işlem yapıyorum ki sadece bulunduğum dizinde değil bütün dizinlerde arama gerçekleştiresin.

-"cat /var/lib/dpkg/info/bandit7.password " arama sonucunda burada bir şifre olduğunu görüntülüyorum ve bu şifreyle seviye atlatıyorum.

-Seviye 7'ye geçiş yapmıştık.Burada ipucuna baktığımızda millionth isimli yazıdan sonra şifrenin geldiğini belirtiyordu.

```
regulated      sxJ8HT73fvZMMiicL50nhawcwsYGUiwP
knotting      vh268WJXw10Snszed9MVaHD4rTP69Lzr
hymnals       7MqsN32lFdbPigtAX6cwFbMzCPAMUoae
Fremont       tCy02wC8xdpFqjLZ8xdBQYAHFZPHk7ls
punter's      zAfaa11OuBSamCR6eMmRoc9oNXPQ16a
junking       6Tlr5K8YZ1d2Xsduku3TTFYXWB6WOMxyT
Aymara        zSeUS0UyDBQ6a6YPwaCLRBbk1x8kFBEC
waned         gL59r6xvewh5y8t0mgiNtHtCUMG8S6Id
conceded      TWLUyXt3HbwD4qsYQ09sENOn0iNy79sC
kilned        kLjrgoJvftIyUyotu0I4cxFcXQBc6AS
Santayana     KKn1I4fuWdzKyvffp1aYrBDzQa3Tr3Pk
Antigua       dRyNieqAg00kCgrKVQFXMXS06vFarL55
heyday        UAGwMLFzylGa4fHpQZEelUQ5ZJlUpyX
praiseworthiness's      bJRBOuGXMD47h1p9hHB3mbFBMMwlnKNkq
separatism    p2167YTCJseAv4YhLZNb2fs7JivlDLUW
plan          PLz4ZXwX02fEe4oMd1I78wQXL4MIMxTf
confrontation KLHScgMgzyBQYsBXKxsjKcQ2A5erDIjL
briquet's    aHc51xHj1t3ANF7jH26dd7mHwBfd8VKz
encapsulate   STOVYQEMwtfZ54JtjJRrhdXGzCfVw8ls
wildfowls     PqcMofjmKj8NBvO9exdu7FY2NG6WUMzb
Finland       xgXsIYgqUCMriMoT7W2dSwtG1DCvbRvU
bandit7@bandit:~$ cat data.txt | grep millionth
millionth     cvX2JJJa4CFALTqS87jk27qwgHhBM9plv
```

-cat data.txt | grep millionth komutu ile burada arama gerçekleştirdiğimizde şifreye erişebiliyoruz.

[illegible]

-Ardından seviye 8'e geçiş yapıyorum ve burada bana yaklaşık 3 mb'lık bir şifre dizini veriyor.Bunun içerisinde sadece 1 tanesi tek olarak bulunmaktadır.

-Burada ilk önce sort data.txt komutunu çalıştırıp sıralama yapıyorum.

```
10 TKUtQbeYnEzzYIne7BinoBx2bHFLBXzG
10 TThRArdF2ZEXM047TIYkyPPLtvzzLcDf
10 tvW9iY1Ml0uHPK4usZnN8oZXbjRt2ATY
10 U0NYdD3wHZKpfEg9qGQOLJimaJy6qxhS
10 UASW6CQwD6MRzftu6FAfyXBK0cVvnBLP
10 UJiCNvDNfgb3fcCj8PjjnAXHqUM63Uyj
10 UjsVbcqKeJqdCZQCDMkzv6A9X7hLbNE4
1 UsvVyFSfZZWbi6wgC7dAFyFuR6jQQUHR
10 UVnZvhiVQECraz5jL8U14sMVZQhjuXia
10 V2d9umHiuPLYLIDsuHj0fr0EmreCZMaA
10 v9zaxkVA0dI0LITZY2uoCtB1fX2gmly9
10 VkBAEWyIibVkeURZV5mowiGg6i3m7Be0
10 w4zUWFGTUrAAh8lNks8gH3WK2zowBEkA
10 WBqr9xvf6mYTT5kLcTGC66jb3ex94xWr
10 wjNwumEX58RUQTTrufHMcIWz5Yx10GtTC
10 X1JHOUkrb4KgugMXIZMWWIWvRkeZleTI
10 XyeJdbrUJyGtdGx8cXLQST0pwu5cvpcA
10 yo0HbSe2GM0jJNhRQLxwoPp7ayYEmRKY
10 ySvsTwLMgnUF0n86Fgmn2TNjkS0lrV72
```

- "sort data.txt | uniq -c" komutunu kullanarak burada tek geçen şifreyi görüntülüyorum.

- Bu şifre ile seviye 9 a geçiş yapıyorum.

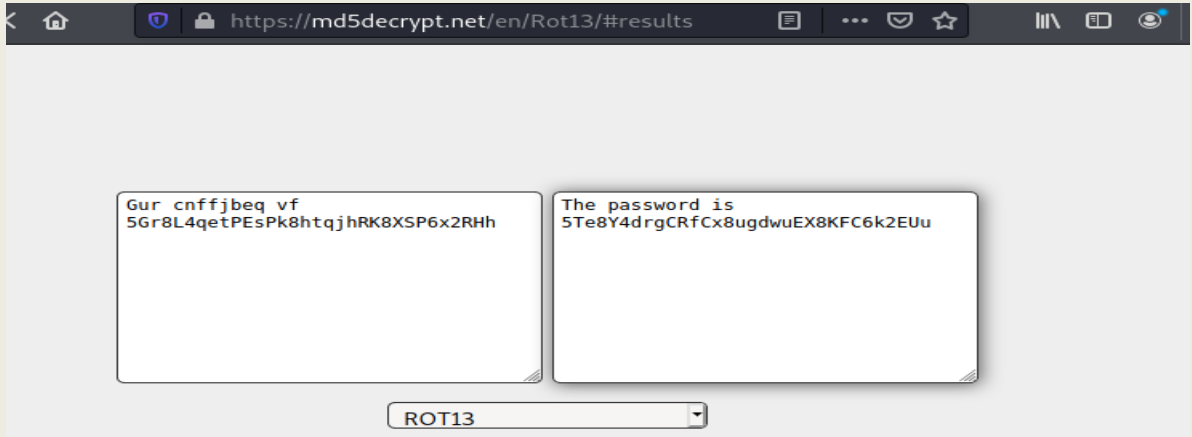
```
Dosya Eylemler Düzen Görünüm Yardım
bandit9@bandit:~$ strings data.txt | grep "="
===== the*2i"4
=:G e
===== password
<I=zsGi
Z)===== is
A= t&E
Zdb=
c^ LAh=3G
*SF=s
8===== truKldjsbJ5g7yyJ2X2R0o3a5HQJFuLk
S=A.H&^
bandit9@bandit:~$
```

- Strings komutu ile dosyayı görüntüleyip içerisinde arama gerçekleştiriyorum ve burada şifreyi görüntülüyorum.

```
bandit10@bandit:~$ ls
data.txt
bandit10@bandit:~$ cat data.txt
VGhLIHBhc3N3b3JkIGlzIElGdWt3S0dzRlc4TU9xM0lSRnFyeEUxaHhUTkViVVBSCg==
bandit10@bandit:~$
```

- Seviye 10 dan 11 e geçişte verdiği ipucunda şifrenin base64 türünde yazıldığını belirtiyor.

- Bulduğum şifreyi tarayıcı üzerine geçiş yapıp decode ediyorum ve şifreye erişiyorum.



-Decode sonucunda diğer seviyeye erişim sağladım.

-Burada tüm karakterlerin 13 birim kaydırılıp şifrelendiğini tarafıma aktarıyor. Burada tarayıcı üzerinden yapmış olduğum arama ile ROT13 ile şifrelendiğini görüntülüyorum.

-Sonrasında decode edip diğer seviyenin şifresine erişim sağlıyorum.

-Yeni geçtiğimiz seviye üzerinde bir hexdump dosyasına erişim sağlamıştık. Bu hexdump'ı dönüştürüp işlemlerimize devam edeceğiz.

Hexdump'ı hem sıkıştırmış hem de defalarca şifrelemiş bunun için bir geçici dosya oluşturup buradan bir dönüştürme işlemi yapmaya çalışacağız.

```
Dosya Eylemler Düzen Görünüm Yardım
bandit12@bandit:~$ mkdir /tmp/kaan
bandit12@bandit:~$ ls
data.txt
bandit12@bandit:~$ cp data.txt /tmp/kaan
bandit12@bandit:~$ cd /tmp/kaan
bandit12@bandit:/tmp/kaan$ ls
data.txt
bandit12@bandit:/tmp/kaan$ -
```

-Öncelikle tmp dosyasının içerisine bulduğum data.txt'yi kopyalıyorum.

-Bu kopyalama işleminin ardından hexdump'ı çözmek için "xxd" aracından yararlanacağım.

```
Dosya Eylemler Düzen Görünüm Yardım
bandit12@bandit:/tmp/kaan$ xxd -r data.txt > kaan
bandit12@bandit:/tmp/kaan$ ls
data.txt kaan
bandit12@bandit:/tmp/kaan$
```

-XXD aracı ile öncelikle decode ediyorum.


```
bandit12@bandit:/tmp/kaan$ file kaan
kaan: gzip compressed data, was "data2.bin", last modified: Thu May  7 18:14:30 2020, max compression, from Unix
bandit12@bandit:/tmp/kaan$ gzip -d kaan
gzip: kaan: unknown suffix -- ignored
bandit12@bandit:/tmp/kaan$ mv kaan kaan.gz
bandit12@bandit:/tmp/kaan$ ls
data.txt  kaan.gz
bandit12@bandit:/tmp/kaan$ gzip -d kaan.gz
bandit12@bandit:/tmp/kaan$ ls
data.txt  kaan
bandit12@bandit:/tmp/kaan$ file kaan
kaan: bzip2 compressed data, block size = 900k
```

-Ardından file komutu ile dosya türünü öğreniyorum.

-Dosya türüne baktığımda gzip olarak gözüktüyor fakat uzantısının olmadığını görüntülüyorum.

-Burada da mv komutunu kullanıp uzantı ekliyorum.Daha sonra "gzip -d kaan.gz" komutu ile uzantısını değiştiriyorum.

```
bandit12@bandit:/tmp/kaan$ mv kaan kaan.bz2
bandit12@bandit:/tmp/kaan$ ls
data.txt  kaan.bz2
bandit12@bandit:/tmp/kaan$ bzip2 -d kaan.bz2
bandit12@bandit:/tmp/kaan$ ls
data.txt  kaan
bandit12@bandit:/tmp/kaan$ file kaan
kaan: gzip compressed data, was "data4.bin", last modified: Thu May  7 18:14:30 2020, max compression, from Unix
```

-File komutu ile tekrardan uzantısına baktığımda bzip2 olduğunu görüyorum ve tekrar uzantısını değiştiriyorum.

-Aynı işlemleri burada da gerçekleştirdim.

```
bandit12@bandit:/tmp/kaan$ mv kaan kaan.gz
bandit12@bandit:/tmp/kaan$ ls
data.txt  kaan.gz
bandit12@bandit:/tmp/kaan$ gzip -d kaan.gz
bandit12@bandit:/tmp/kaan$ ls
data.txt  kaan
bandit12@bandit:/tmp/kaan$ file kaan
kaan: POSIX tar archive (GNU)
```

-İşlemleri gzip için tekrardan gerçekleştiriyorum.

```
bandit12@bandit:/tmp/kaan$ mv kaan.gz kaan.tar
bandit12@bandit:/tmp/kaan$ ls
data.txt  kaan.tar
bandit12@bandit:/tmp/kaan$ tar xf kaan.tar
bandit12@bandit:/tmp/kaan$ ls
data5.bin data.txt  kaan.tar
bandit12@bandit:/tmp/kaan$ file data5.bin
data5.bin: POSIX tar archive (GNU)
bandit12@bandit:/tmp/kaan$
```

-Ardından tar dosyasına erişim sağlıyorum.Burada .tar uzantısına dönüştürüyorum ve "xf" omutu ile tardan çıkarıyorum.

-Sonrasında data5.bin isimli bir dosyaya erişiyorum.Dosya uzantısına baktığımda bunundan bir tar archive olduğunu görüyorum.

```
bandit12@bandit:/tmp/kaan$ mv data5.bin kaan.tar
bandit12@bandit:/tmp/kaan$ tar xf kaan.tar
bandit12@bandit:/tmp/kaan$ ls
data6.bin data.txt  kaan.tar
bandit12@bandit:/tmp/kaan$ file data6
data6: cannot open `data6' (No such file or directory)
bandit12@bandit:/tmp/kaan$ file data6.bin
data6.bin: bzip2 compressed data, block size = 900k
bandit12@bandit:/tmp/kaan$ mv data6.bin data6.bz2
bandit12@bandit:/tmp/kaan$ ls
data6.bz2 data.txt  kaan.tar
bandit12@bandit:/tmp/kaan$ bzip2 -d data6.bz2
bandit12@bandit:/tmp/kaan$ ls
data6 data.txt  kaan.tar
bandit12@bandit:/tmp/kaan$ file data6
data6: POSIX tar archive (GNU)
bandit12@bandit:/tmp/kaan$ mv data6 data6.tar
bandit12@bandit:/tmp/kaan$ ls
data6.tar data.txt  kaan.tar
bandit12@bandit:/tmp/kaan$ tar xf data6.tar
bandit12@bandit:/tmp/kaan$ ls
data6.tar data8.bin data.txt  kaan.tar
bandit12@bandit:/tmp/kaan$ file data8.bin
data8.bin: gzip compressed data, was "data9.bin", last modified: Thu May  7 18:14:30 2020, max c
ompression, from Unix
bandit12@bandit:/tmp/kaan$ mv data8.bin data8.gz
bandit12@bandit:/tmp/kaan$ ls
data6.tar data8.gz data.txt  kaan.tar
bandit12@bandit:/tmp/kaan$ gzip -d data8.gz
bandit12@bandit:/tmp/kaan$ ls
data6.tar data8 data.txt  kaan.tar
bandit12@bandit:/tmp/kaan$ file data8
data8: ASCII text
bandit12@bandit:/tmp/kaan$ mv data8 sifre.txt
bandit12@bandit:/tmp/kaan$ ls
data6.tar data.txt  kaan.tar sifre.txt
bandit12@bandit:/tmp/kaan$ cat sifre.txt
The password is 8ZjyCRiBWFYkneahHwxCv3wb2a10RpYL
```

-Aynı işlemleri defalarca tekrar ettikten sonra şifreye ulaşabildim.

```
bandit13@bandit:~$ ssh -i sshkey.private bandit14@localhost
Could not create directory '/home/bandit13/.ssh'.
The authenticity of host 'localhost (127.0.0.1)' can't be established.
ECDSA key fingerprint is SHA256:98UL0ZWr85496EtCRkKlo20X30PnyPSB5tB5RPbhczc.
Are you sure you want to continue connecting (yes/no)? yes
Failed to add the host to the list of known hosts (/home/bandit13/.ssh/known_hosts).
This is a OverTheWire game server. More information on http://www.overthewire.org/wargames
```

-Yeni seviyede baktığımızda şifreyi bir private key üzerinden ssh bağlantısı ile kuracağımızı belirtiyor.

-Burada SSH komutu ile yeni seviyeye geçiş yapıyoruz.Aynı localhost üzerinde olduğumuz için server belirtmemize gerek kalmıyor.

```
bandit14@bandit:~$ nc localhost 30000
4wcYUJFw0k0XLShLDzztnTBHixU3b3e
Correct!
BfMYroe26WYalil77FoDi9qh59eK5xNr
```

-Yeni geçtiğimiz seviyede verdiği ipucunda 30000 portuna bağlantı kurup burada önceki seviyenin şifresini yazıp yeni seviyenin şifresine erişim sağlamamızı istiyor.

-Netcat komutu ile bu işlemi gerçekleştirip yeni seviyenin şifresine ulaşıyorum.

-Level 15 ten 16'ya geçişe baktığımda burada 30001 portundan SSL bağlantısı yapmamı istiyor.

-Bu işlemi ncat aracı kullanarak gerçekleştiriyorum

```
Invalid command '--help'; type "help" for a list.
bandit15@bandit:~$ man openssl
bandit15@bandit:~$ ncat --ssl localhost 30001
BfMYroe26WYalil77FoDi9qh59eK5xNr
Correct!
cluFn7wTiGryunymYOU4RcffSxQLuehd
```

-Gerekli işlem sonucunda sonraki seviyenin şifresine ulaşıyorum.

```
bandit16@bandit:~$ nmap localhost -p 31000-32000
Starting Nmap 7.40 ( https://nmap.org ) at 2021-10-18 13:39 CEST
Nmap scan report for localhost (127.0.0.1)
Host is up (0.00036s latency).
Not shown: 996 closed ports
PORT      STATE SERVICE
31046/tcp  open  unknown
31518/tcp  open  unknown
31691/tcp  open  unknown
31790/tcp  open  unknown
31960/tcp  open  unknown
Nmap done: 1 IP address (1 host up) scanned in 0.08 seconds
```

-Level 16'ya geçiş yaptığımda localhost üzerinde bulunan 31000-32000 arasında bulunan portlardan birine gndererek diğer porta geçiş yapacağım.

-Nmap üzerinden geçerli portlarda tarama yapıyorum ve açık portları görüntülüyorum bunlar arasından teker teker deneme gerçekleştireceğim.

```
bandit16@bandit:~$ ncat --ssl localhost 31790
cluFn7wTiGryunymY0u4RcfffSxQluehd
Correct!
-----BEGIN RSA PRIVATE KEY-----
MIIIEogIBAAKCAQEAvmOkuifmMg6HL2YPIOjon6iWfbp7c3jx34YkYWqUH57SUdyJ
imZzeyGC0gtZPGUjUSxiJSWI/oTqexh+cAMTSMLOJf7+BrJ0bArnxd9Y7YT2bRPQ
Ja6Lzb558Yw3FZL870Ri0+rW4LDCDCNd2lUvLE/GL2GwyuKN0K5iCd5TbtJzEkQTu
DSt2mcNn4rhAL+JfR56o4T6z8WWAW18BR6yGrMq7Q/kALHYW30ekePQAzL0VUYbw
JGTi65CxbCnzc/w4+mqQyvmzpWtMAzJTzAzQxNbkR2MBGySxDLrjg0LWN6sK7wNX
x0YVztz/zbIkPjfkU1jHS+9EbVNj+D1XF0JuaQIDAQABAoIBABagpxpM1aoLWfvd
KHcj10nqcoBc4oE11aFYQwik7xFW+24pRNuDE6SFth0ar69jp5RLLwD1NhPx3iBl
J9nOM80J0VToum43UOS8YxF8WwhXriYGnc1sskbwpX0UDc9uX4+UESzH22P29ovd
d8WErY0gPxun8pbJLmxkAtWNhpMvfe0050vk9TL5wqbu9AlbssgTcCXkMQnPw9nC
YNN6DDP2lbcBrvgT9YCNL6C+ZKufD52y0Q9q0kwFTEQpjtF4uNtJom+asvlpms8A
vLY9r60wYSvmZhNqBurj7lyCtXMIu1kkd4w7F77k+DjHoAXyxcUp1DGL51sOmama
+TOWWgECgYEA8JtPxP0GRJ+IQkX262jM3dEIkza8ky5moIwUqYdsx0NxHgRRhORT
8c8hAuRbb2G82s08vUHK/fur850Efc9TncnCY2crpoqsgghifKLxrLgtT+qDpfZnx
SatLdt8GfQ85yA7hnWWJ2Mx3NaesDm75Lsm+tBbAiyC9P2jGRNtMSkCgYEAypHd
HCctNi/FwjulhttFx/rHYKhLidZDFYeiE/v45bN4yFm8x7R/b0iE7KaszX+Exdvt
SghaTdcG0Knyw1bpJVyusavPzpaJMjdJ6tcFhVAbAjm7enCivGCSx+X3l5SiWg0A
R57hJglezIiVjv3aGwHwvlZvtszK6zV6oXFAu0ECgYABjo46T4hyP5tJi93V5Hdi
TtieK7xRVxUl+iu7rWkGAXFpMLFteQEsRr7PJ/lemmEY5eTDAFMLy9FL2m9oQWcg
R8VdwSk8r9FGLS+9aKcV5PI/WEKlwgXinB30hYimtiG2Cg5JCqIZFHxD6MjEG0iu
L8ktHMPvodBwNsSBULpG0QKBgBAPLTFc1HOnWiMGOU3KPwYwT006CdTKmJ0mL8Ni
blh9elyZ9FsGxsgrBXRsqXuz7wtsQAgLHxbdLq/ZJQ7Yfz0KU4ZxEnabvXnvWku
Y0djHdS0oKvDQNWu6ucyLRAWFuISeXw9a/9p7ftpxm0TSgyvmfLF2MIAEwyzRqaM
77pBAoGAMmjmIJdjp+Ez8duyn3ieo36yrttF5NSsJLABxFpdlc1gvtGCWW+9Cq0b
dxviW8+TFVEBl104f7HvM6EpTscDxU+bCXWkfjuRb7Dy9G0tt9JP8X8MBTakzh3
vBgysi/sN3RqRBCGU40f0oZyFAMT8s1m/uYv5206IgeuZ/ujbjY=
-----END RSA PRIVATE KEY-----
```

-Güncel seviyenin şifresiyle bulduğum portlar üzerinde deneme yapıyorum ve karşıma bir private key çıkmaktadır.

-Bu private_key'i kopyalıyorum ve nano komutu ile bir private key oluşturun.

-Burada bulduğum key ile SSH bağlantısı kurup bir sonraki seviyeye geçiş yapıyorum.

-Gerekli işlemler sonucunda Level17'ye erişim sağlamıştık.

```
bandit17@bandit:~$ ls -la
total 36
drwxr-xr-x  3 root    root      4096 Jul 11  2020 .
drwxr-xr-x 41 root    root      4096 May  7  2020 ..
-rw-r----- 1 bandit17 bandit17   33 Jul 11  2020 .bandit16.password
-rw-r--r--  1 root     root       220 May 15  2017 .bash_logout
-rw-r--r--  1 root     root     3526 May 15  2017 .bashrc
-rw-r----- 1 bandit18 bandit17  3300 May  7  2020 passwords.new
-rw-r----- 1 bandit18 bandit17  3300 May  7  2020 passwords.old
-rw-r--r--  1 root     root       675 May 15  2017 .profile
drwxr-xr-x  2 root    root      4096 Jul 11  2020 .ssh
bandit17@bandit:~$ diff passwords.old passwords.new
42c42
< w0YfoIrc5bwjS4qw5mq1nnQi6mF03bii
---
> kFbF3eYk5BPBRzwjqutbbfE887SVc5Yd
Ana dizinde 2 dosya vardır: pas
```

-“ls -la” komutu ile görüntülediğimde passwords.new ve passwords.old olduğunu görüyorum ve burada içeriklerinde sadece 1 tane karakter farkı vardır.

-Bunu bulmak için diff komutunu kullanıyorum ve burada şifremizi başarılı bir şekilde elde ettik.

```
--[ More information ]--

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

For support, questions or comments, contact us through IRC on
irc.overthewire.org #wargames.

Enjoy your stay!

Byebye !
Connection to bandit.labs.overthewire.org closed.
```

-Level 18'in şifresini girdiğimde beni sistemden düşürdüğünü görüntülüyorum.

```
(root@kali)~[~/Masaüstü]
# ssh -t bandit18@bandit.labs.overthewire.org -p 2220 '/bin/sh'
This is a OverTheWire game server. More information on http://www.overthewire.org/wargames

bandit18@bandit.labs.overthewire.org's password:
Permission denied, please try again.
bandit18@bandit.labs.overthewire.org's password:
$ whoami
bandit18
$ ls
readme
$ cat readme
Iueks57Ubh8G3DCwVzrTd8rAV0wq3M5x
$
```

-Bu sorunu çözmek için -t parametresinden yararlanıyorum ve /bin/zsh ile birlikte erişim sağlayıp diğer seviyenin şifresine erişiyorum.

- Seviye 19'a geçiş yaptığımda home dizininde bir script olduğunu görüntülüyorum.

```
bandit19@bandit:~$ ls -la
total 28
drwxr-xr-x  2 root    root    4096 May  7  2020 .
drwxr-xr-x 41 root    root    4096 May  7  2020 ..
-rwsr-x---  1 bandit20 bandit19 7296 May  7  2020 bandit20-do
-rw-r--r--  1 root    root     220 May 15  2017 .bash_logout
-rw-r--r--  1 root    root    3526 May 15  2017 .bashrc
-rw-r--r--  1 root    root     675 May 15  2017 .profile
bandit19@bandit:~$ ./bandit20-do
Run a command as another user.
Example: ./bandit20-do id
bandit19@bandit:~$ ./bandit20-do id
uid=11019(bandit19) gid=11019(bandit19) euid=11020(bandit20) groups=11019(bandit19)
bandit19@bandit:~$ ./bandit20-do cat /etc/bandit_pass/bandit20
GbKksEFF4yrVs6il55v6gwY5aVje5f0j
```

-Bandit seviyelerinde bir üst seviyenin key'inin bulunduğu dizine erişim yapmam engellenir.

-Bu scripti çalıştırdığımda bir sonraki seviyenin kullanıcıyıymışım gibi işlem yapabiliyorum.

-Bu şifrenini bulunduğu dizine erişim sağlayıp bir sonraki seviyenin şifresini elde ediyorum.

```
bandit20@bandit:~$ nmap -p- localhost

Starting Nmap 7.40 ( https://nmap.org ) at 2021-10-18 14:16 CEST
Nmap scan report for localhost (127.0.0.1)
Host is up (0.00025s latency).
Not shown: 65526 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
30000/tcp  open  ndmps
30001/tcp  open  pago-services1
30002/tcp  open  pago-services2
31046/tcp  open  unknown
31518/tcp  open  unknown
31691/tcp  open  unknown
31790/tcp  open  unknown
31960/tcp  open  unknown

Nmap done: 1 IP address (1 host up) scanned in 3.95 seconds
```

- Seviye 20'ye geçiş yaptığımda burada bir script bulunmakta scriptin çalışma düzenine baktığımda verdiğim port numarası üzerinden işlem yaptığını görüntülüyorum.

-Geçerli portu bulabilmek için bir nmap taraması gerçekleştiriyorum.

-Gelen portları tek tek deniyorum ve buradan bir sonuç alamıyorum.

```
Dosya Eylemler Düzen Görünüm Yardım
bandit20@bandit:~$ ./suconnect 4444
GbkKsEFF4yrVs6il55v6gwY5aVje5f0j
^C
bandit20@bandit:~$ ./suconnect 4444
Read: GbkKsEFF4yrVs6il55v6gwY5aVje5f0j
Password matches, sending next password
bandit20@bandit:~$ 
Nmap done: 1 IP address (1 host up) scanned in 3.95 seconds
bandit20@bandit:~$ nc -l -localhost 4444
can't open calhost : Permission denied
bandit20@bandit:~$ nc -l localhost -p 4444
bandit20@bandit:~$ nc -l localhost -p 4444
GbkKsEFF4yrVs6il55v6gwY5aVje5f0j
gE269g2h3mw3pwgrj0Ha9Uoqen1c9DGr
bandit20@bandit:~$
```

- Ardından netcat üzerinden bir port oluşturuyorum ve tekrardan bir bağlantı kurup deneme yapıyorum.

-Aynı port üzerinde güncel şifreleri gönderdikten sonra bir sonraki seviyenin şifresini elde ediyorum.

-Seviye 21 e başarılı bir şekilde ulaştık.Burada crontab üzerinde çalışan uygulamalardan bir şifre yakalamaya çalışacağız.

```
bandit21@bandit:/etc/cron.d$ cat /usr/bin/cronjob_bandit22.sh
#!/bin/bash
chmod 644 /tmp/t706lds9S0RqQh9aMcz6ShpAoZKF7fgv
cat /etc/bandit_pass/bandit22 > /tmp/t706lds9S0RqQh9aMcz6ShpAoZKF7fgv
bandit21@bandit:/etc/cron.d$
```

-Crontab üzerinde 22.seviyeye erişim sağlıyorum.Tmp dosyası içerisine şifreyi eklediğini görüntülüyorum.

```
Dosya Eylemler Düzen Görünüm Yardım
bandit21@bandit:/etc/cron.d$ cat /tmp/t706lds9S0RqQh9aMcz6ShpAoZKF7fgv
Yk7owGAcWjwMVRwrTesJEwB7WV0iILLI
bandit21@bandit:/etc/cron.d$
```

-İçerisine eklediği dizini kontrol ettiğimde başarılı bir şekilde şifreye erişim sağlıyorum.

-22.Seviyeye geçiş yaptığımda burada da crontab üzerinden bir işlem yapacağımızı görüntülüyorum.

```
bandit22@bandit:/etc/cron.d$ cat /usr/bin/cronjob_bandit23.sh
#!/bin/bash

myname=$(whoami)
mytarget=$(echo I am user $myname | md5sum | cut -d ' ' -f 1)

echo "Copying passwordfile /etc/passwd/$myname to /tmp/$mytarget"

cat /etc/passwd/$myname > /tmp/$mytarget
bandit22@bandit:/etc/cron.d$ whoami
bandit22
bandit22@bandit:/etc/cron.d$ myname=bandit23
bandit22@bandit:/etc/cron.d$ $myname
-bash: bandit23: command not found
bandit22@bandit:/etc/cron.d$ echo I am user $myname | md5sum | cut -d ' ' -f 1
8ca319486bfbbc3663ea0fbe81326349
bandit22@bandit:/etc/cron.d$ cat /tmp/8ca319486bfbbc3663ea0fbe81326349
jc1udXuA1tiHqjIsL8yaapX5XIAI6i0n
```

-Crontab'i açtığımda 23.seviyeyle ilgili bilgilere erişmeye çalışıyorum.

-Script dosyasını görüntülediğimde burada kodu okuyorum ve gelen seviye değerini okuyup ona göre şifre oluşturduğunu görüyorum.

-Yazmış olduğum kodlar ile bir sonraki şifreyi elde ediyorum.

-Seviye 23'e geldiğimizde açıklamayı okuyorum ve burada crontab üzerinden işlem gerçekleştireceğimi biliyorum.

```
bandit23@bandit:/etc/cron.d$ cat /usr/bin/cronjob_bandit24.sh
#!/bin/bash

myname=$(whoami)

cd /var/spool/$myname
echo "Executing and deleting all scripts in /var/spool/$myname:"
for i in * .*;
do
    if [ "$i" != "." -a "$i" != ".." ];
    then
        echo "Handling $i"
        owner="$(stat --format "%U" ./$i)"
        if [ "${owner}" = "bandit23" ]; then
            timeout -s 9 60 ./$i
        fi
        rm -f ./$i
    fi
done
```

-Burada bir script yazılı olduğunu görüntülüyorum.Seviyenin açıklamasına baktığımda burada bir script yazmamın istendiğini görüyorum.

```
bandit23@bandit:/tmp/kaan123$ nano denem.txt
Unable to create directory /home/bandit23/.nano: Permission denied
It is required for saving/loading search history or cursor positions.

Press Enter to continue
```

-Bash komutunu incelediğim zaman bir şifre oluşturma scripti olduğunu görüntülüyorum burada işlem yapmak için

-Bir script yazmak istiyorum fakat bunu nano komutu ile oluşturmamı engelliyor.Bu sebeple echo ""> komutu ile yazdırarak bu işlemi gerçekleştireceğim.

```
bandit23@bandit:/tmp/kaan123$ echo "test" > myscript.sh
bandit23@bandit:/tmp/kaan123$ ls
myscript.sh
bandit23@bandit:/tmp/kaan123$ cat my.script.sh
cat: my.script.sh: No such file or directory
bandit23@bandit:/tmp/kaan123$ echo "#!/bin/bash \n " >myscript.sh
-bash: !/bin/bash: event not found
bandit23@bandit:/tmp/kaan123$ echo "cat /etc/bandit_pass/bandit24 > /tmp/kaan123/password.txt" > myscript.sh
bandit23@bandit:/tmp/kaan123$ cat myscript.sh
cat /etc/bandit_pass/bandit24 > /tmp/kaan123/password.txt
bandit23@bandit:/tmp/kaan123$ chmod +777 myscript.sh
bandit23@bandit:/tmp/kaan123$ touch password.txt
bandit23@bandit:/tmp/kaan123$ ls
myscript.sh password.txt
bandit23@bandit:/tmp/kaan123$ chmod 777 password.txt
bandit23@bandit:/tmp/kaan123$ cp myscript.sh /var/spool/bandit24
bandit23@bandit:/tmp/kaan123$ cat password.txt
UoMYTrfrBFHyQXmg6gzctqAwOmw1IohZ
```

-Script içerisinde bandit24 klasörünü çalıştırıyorum ve password.txt içerisine bir sonraki seviyenin şifresinin yazılmasını istiyorum.Sonucunda şifreyi elde edebildim.

-Seviye 24 e geldiğimizde burada 30002 potunun dinlendiğini ve buraya eğer 4 basamaklı bir pin verebilirsek bize bandit 25'in şifresini vereceğini söylüyor.

-Bunun için 10.000 kombinasyon yapmamız gerekmektedir.Bunu manuel olarak değil bruteforce kullanarak gerçekleştireceğiz.

-Bu işlemi bash dili üzerinde bir script yazıp işlemleri gerçekleştireceğim.

```
1 #!/bin/bash
2
3
4 bandit24passwd=UoMYTrfrBFHyQXmg6gzctqAwOmw1IohZ
5
6 for i in {1111..9999}; do
7     echo "$bandit24passwd $i"
8 done | nc localhost 30002
9
10
```

-Yazmış olduğum kod her defasında bandit24 passwd alıcak ve i değerini yanına ekleyip "|" sayesinde çıktığı localhost 30002'ye çıktı olarak bunları vericek.

```
Wrong! Please enter the correct pincode. Try again.  
Wrong! Please enter the correct pincode. Try again.  
Wrong! Please enter the correct pincode. Try again.  
Wrong! Please enter the correct pincode. Try again.  
Correct!  
The password of user bandit25 is uNG9058gUE7snukf3bvZ0rxhtnjzSGzG  
Exiting.
```

-Script sonucunda başarılı bir şekilde şifreyi elde ettik.

```
bandit25@bandit:~$ ssh -i bandit26.sshkey bandit26@localhost  
Could not create directory '/home/bandit25/.ssh'.  
The authenticity of host 'localhost (127.0.0.1)' can't be established.  
ECDSA key fingerprint is SHA256:98UL0ZW85496EtCRkKlo20X30PnyPSB5tB5RPbhczc.  
Are you sure you want to continue connecting (yes/no)? yes  
Failed to add the host to the list of known hosts (/home/bandit25/.ssh/known_hosts).  
This is a OverTheWire game server. More information on http://www.overthewire.org/wargame  
s  
sya Bash kuru  
Linux bandit.otw.local 5.4.8 x86_64 GNU/Linux
```

-Bu örnekte sshkey kullanarak bağlantı kurabiliyoruz fakat bizi sistemden düşürüyor.

-İpuçlarına baktığımızda sistemde vi ve more komutunu kullanacağımızı söylüyor.

-More komutu cat komutundan farklı olarak belirli yüzde şeklinde gösterim yapar.

-More ile vi arasında geçiş yapabildiğimiz için burada bir işlem yapabiliriz.

-Vi'ye geçiş yaptığımızda :set shell=/bin/bash komutunu set ediyoruz.Ardından set komutunu kullandığımızda

-Seviye 26 'ya geçiş yapabiliyoruz.

```
~  
~  
~  
~  
~  
~  
~  
~/text.txt[R0] [dec= 32] [hex=20] [pos=0001:0002][16% of 6]  
:set shell=/bin/bash
```

-İlk önce shell kodunu set ediyorum ve :shell komutunu çalıştırıyorum.


```
bandit26@bandit:~$ ls
bandit27-do  text.txt
bandit26@bandit:~$ ./bandit27-do
Run a command as another user.
Example: ./bandit27-do id
bandit26@bandit:~$ ./bandit27-do cat /etc/bandit_pass/bandit27
3ba3118a22e93127a4ed485be72ef5ea
bandit26@bandit:~$
```

-Ardından 26.seviye komut satırına geçiş yaptım ve buradan level 27'ye geçiş yapıyorum.

-Seviye 27 ye geldiğimizde burada git komutu üzerinden işlem yapmamız istenmektedir.

Bandit Level 27 → Level 28

Level Goal

There is a git repository at `ssh://bandit27-git@localhost/home/bandit27-git/repo`. The password for the user `bandit27-git` is the same as for the user `bandit27`.

Clone the repository and find the password for the next level.

-Vermiş olduğu git bağlantısı üzerinden bir clonelama işlemi yapmam istenmektedir.

```
bandit27@bandit:/tmp/kaan27$ git clone ssh://bandit27-git@localhost/home/bandit27-git/repo
Cloning into 'repo' ...
Could not create directory '/home/bandit27/.ssh'.
The authenticity of host 'localhost (127.0.0.1)' can't be established.
ECDSA key fingerprint is SHA256:98UL0ZW85496EtCRkKlo20X30PnyPSB5tB5RPbhczc.
Are you sure you want to continue connecting (yes/no)? yes
Failed to add the host to the list of known hosts (/home/bandit27/.ssh/known_hosts).
This is a OverTheWire game server. More information on http://www.overthewire.org/wargames

bandit27-git@localhost's password:
remote: Counting objects: 3, done.
remote: Compressing objects: 100% (2/2), done.
remote: Total 3 (delta 0), reused 0 (delta 0)
Receiving objects: 100% (3/3), done.
```

-Tmp klasörüne bir dosya oluşturuyorum ve ardından git komutu ile verilen dosyayı oluşturduğum klasöre indiriyorum.

```
repo
bandit27@bandit:/tmp/kaan27$ cd repo
bandit27@bandit:/tmp/kaan27/repo$ ls
README
bandit27@bandit:/tmp/kaan27/repo$ cat README
The password to the next level is: 0ef186ac70e04ea33b4c1853d2526fa2
bandit27@bandit:/tmp/kaan27/repo$
```

-Klasör içine geldiğimizde burada bir sonraki seviyenin bilgi sahibi olabiliriz.

```
bandit28@bandit:~$ mkdir /tmp/kaan28
bandit28@bandit:~$ cd /tmp/kaan28
bandit28@bandit:/tmp/kaan28$ git clone ssh://bandit28-git@localhost/home/bandit28-git/repo
Cloning into 'repo' ... here is a git repository at
Could not create directory '/home/bandit28/.ssh'.
The authenticity of host 'localhost (127.0.0.1)' can't be established.
ECDSA key fingerprint is SHA256:98UL0ZW85496EtCRkKLo20X30PnyPSB5tB5RPbhczc.
Are you sure you want to continue connecting (yes/no)? yes
Failed to add the host to the list of known hosts (/home/bandit28/.ssh/known_hosts).
This is a OverTheWire game server. More information on http://www.overthewire.org/wargame
s

bandit28-git@localhost's password:
remote: Counting objects: 9, done.
remote: Compressing objects: 100% (6/6), done.
remote: Total 9 (delta 2), reused 0 (delta 0)
Receiving objects: 100% (9/9), done.
Resolving deltas: 100% (2/2), done.
```

-28.Seviyeye geldiğimizde burada da aynı işlemleri gerçekleştirip git clone üzerinden dosya indirmesi yapıyorum.

```
bandit28@bandit:/tmp/kaan28/repo$ cat README.md
# Bandit Notes
Some notes for level29 of bandit.

## credentials
There is a git repository at
- username: bandit29
- password: xxxxxxxxxxxx
The password for the user bandit28 - git is the
bandit28.

bandit28@bandit:/tmp/kaan28/repo$ git branch
* master
bandit28@bandit:/tmp/kaan28/repo$ git tag
bandit28@bandit:/tmp/kaan28/repo$ git log
commit edd935d60906b33f0619605abd1689808ccdd5ee
Author: Morla Porla <morla@overthewire.org>
Date: Thu May 7 20:14:49 2020 +0200

    fix info leak

commit c086d11a00c0648d095d04c089786efef5e01264
Author: Morla Porla <morla@overthewire.org>
Date: Thu May 7 20:14:49 2020 +0200

    add missing data

commit de2ebe2d5fd1598cd547f4d56247e053be3fdc38
Author: Ben Dover <noone@overthewire.org>
Date: Thu May 7 20:14:49 2020 +0200

    initial commit of README.md
```

-"git log" komutu ile eski versiyonlarını görüntüleyebiliyorum ve burada bir tanesinde güvenlik açığının kapatıldığını görüntülüyorum.

Burada ki commit kodunu kopyalıyorum.

```
bandit28@bandit:/tmp/kaan28/repo$ git checkout c086d11a00c0648d095d04c089786efef5e01264
Note: checking out 'c086d11a00c0648d095d04c089786efef5e01264'.

You are in 'detached HEAD' state. You can look around, make experimental
changes and commit them, and you can discard any commits you make in this
state without impacting any branches by performing another checkout.

If you want to create a new branch to retain commits you create, you may
do so (now or later) by using -b with the checkout command again. Example:

    git checkout -b <new-branch-name>

HEAD is now at c086d11... add missing data
bandit28@bandit:/tmp/kaan28/repo$ ls
README.md
bandit28@bandit:/tmp/kaan28/repo$ cat README.md
# Bandit Notes
Some notes for level29 of bandit.

## credentials

- username: bandit29
- password: bbc96594b4e001778eee9975372716b2
```

-Ardından "git checkout" komutu ile geri döndürme işlemi yapıyorum.Buradan tekrar baktığımızda passwordu ele geçirdim.

```
bandit29@bandit:/tmp/kaan29$ cd repo
bandit29@bandit:/tmp/kaan29/repo$ ls
README.md
bandit29@bandit:/tmp/kaan29/repo$ cat README.md
# Bandit Notes
Some notes for bandit30 of bandit.
[ 3 -> Level 4
## credentials

- username: bandit30
- password: <no passwords in production!>

bandit29@bandit:/tmp/kaan29/repo$ git log
commit 208f463b5b3992906eabf23c562eda3277fea912
Author: Ben Dover <noone@overthewire.org>
Date: Thu May 7 20:14:51 2020 +0200

    fix username

commit 18a6fd6d5ef7f0874bbdda2fa0d77b3b81fd63f7
Author: Ben Dover <noone@overthewire.org>
Date: Thu May 7 20:14:51 2020 +0200

    initial commit of README.md
```

-29.Seviyeye geldiğimde tekrardan git clone komutu ile indirme yapmam isteniyor.Burada indirme yapıyorum ve Readme dosyasına baktığımda şifrenin olmadığını görüntülüyorum.

-Ardından log kayıtlarına bakıyorum ve log kayıtlarında şifreyle ilgili bir bilgiye erişemiyorum.

```

bandit29@bandit:/tmp/kaan29/repo$ git checkout dev
Branch dev set up to track remote branch dev from origin.
Switched to a new branch 'dev'
bandit29@bandit:/tmp/kaan29/repo$ git branch
* dev
  master
bandit29@bandit:/tmp/kaan29/repo$ git log
commit bc833286fca18a3948aec989f7025e23ffc16c07
Author: Morla Porla <morla@overthewire.org>
Date: Thu May 7 20:14:52 2020 +0200
    add data needed for development

commit 8e6c203f885bd4cd77602f8b9a9ea479929ffa57
Author: Ben Dover <noone@overthewire.org>
Date: Thu May 7 20:14:51 2020 +0200
    add gif2ascii

commit 208f463b5b3992906eabf23c562eda3277fea912
Author: Ben Dover <noone@overthewire.org>
Date: Thu May 7 20:14:51 2020 +0200
    fix username

commit 18a6fd6d5ef7f0874bbdda2fa0d77b3b81fd63f7
Author: Ben Dover <noone@overthewire.org>
Date: Thu May 7 20:14:51 2020 +0200
    initial commit of README.md

```

-Burada farklı kullanıcı ismiyle işlem yapılmış olabileceğini düşünüyorum ve kullanıcıyı değiştiriyorum.

-Ardından log kayıtlarına baktığımda bir sürü log kaydı olduğunu görüntülüyorum.

```

bandit29@bandit:/tmp/kaan29/repo$ cat README.md
# Bandit Notes
Some notes for bandit30 of bandit.

## credentials

- username: bandit30
- password: 5b90576bedb2cc04c86a9e924ce42faf

```

-Readme dosyasını tekrardan okuduğumda burada sonraki seviyenin şifresine erişebiliyorum.

```

bandit30@bandit:~$ mkdir /tmp/kaan30
bandit30@bandit:~$ cd /tmp/kaan30
bandit30@bandit:/tmp/kaan30$ ls
bandit30@bandit:/tmp/kaan30$ git clone ssh://bandit30-git@localhost/home/bandit30-git/repo
Cloning into 'repo'...
Could not create directory '/home/bandit30/.ssh'.
The authenticity of host 'localhost (127.0.0.1)' can't be established.
ECDSA key fingerprint is SHA256:98UL0ZW85496EtCRkKlo20X30PnyPSB5tB5RPbhczc.
Are you sure you want to continue connecting (yes/no)? yes
Failed to add the host to the list of known hosts (/home/bandit30/.ssh/known_hosts).
This is a OverTheWire game server. More information on http://www.overthewire.org/wargame

bandit30-git@localhost's password:
remote: Counting objects: 4, done.
remote: Total 4 (delta 0), reused 0 (delta 0)
Receiving objects: 100% (4/4), done.
bandit30@bandit:/tmp/kaan30$ ls
repo
bandit30@bandit:/tmp/kaan30$ cd repo
bandit30@bandit:/tmp/kaan30/repo$ ls
README.md
bandit30@bandit:/tmp/kaan30/repo$ cat README
cat: README: No such file or directory
bandit30@bandit:/tmp/kaan30/repo$ cat README.md
just an empty file... muahaha

```

-Seviye 30 a geldiğimizde buradada aynı işlemleri yapıyorum.READ dosyasını açtığımda boş bir dosya gibi gözüküyor.

```

bandit30@bandit:/tmp/kaan30/repo$ git branch -r
origin/HEAD → origin/master
origin/master
bandit30@bandit:/tmp/kaan30/repo$ git log
commit 3aefa229469b7ba1cc08203e5d8fa299354c496b
Author: Ben Dover <noone@overthewire.org>
Date: Thu May 7 20:14:54 2020 +0200

    initial commit of README.md
bandit30@bandit:/tmp/kaan30/repo$ git tag
secret
bandit30@bandit:/tmp/kaan30/repo$ git show secret
47e603bb428404d265f59c42920d81e5

```

- Burada tag kayıtlarına baktığımızda bir adet tag kaydı olduğunu görüntülüyoruz ve içerisine baktığımızda bir sonraki seviyenin şifresine erişiyoruz.

```

bandit31@bandit:~$ mkdir /tmp/kaan31
bandit31@bandit:~$ cd /tmp/kaan31
bandit31@bandit:/tmp/kaan31$ git clone ssh://bandit31-git@localhost/home/bandit31-git/repo
Cloning into 'repo' ...
Could not create directory '/home/bandit31/.ssh'.
The authenticity of host 'localhost (127.0.0.1)' can't be established.
ECDSA key fingerprint is SHA256:98UL0ZW85496EtCRkKlo20X30PnyPSB5tB5RPbhczc.
Are you sure you want to continue connecting (yes/no)? yes
Failed to add the host to the list of known hosts (/home/bandit31/.ssh/known_hosts).
This is a OverTheWire game server. More information on http://www.overthewire.org/wargame
bandit31-git@localhost's password:
remote: Counting objects: 4, done.
remote: Compressing objects: 100% (3/3), done.
remote: Total 4 (delta 0), reused 0 (delta 0)
Receiving objects: 100% (4/4), done.
bandit31@bandit:/tmp/kaan31$ ls
repo
bandit31@bandit:/tmp/kaan31$ cd repo
bandit31@bandit:/tmp/kaan31/repo$ ls
README.md
bandit31@bandit:/tmp/kaan31/repo$ cat README.md
This time your task is to push a file to the remote repository.

Details:
File name: key.txt
Content: 'May I come in?'
Branch: master

```

- Seviye 31 içinde aynı işlemleri gerçekleştiriyorum.Ardından baktığımda bir key.txt dosyası oluşturmamı ve içerisine “may I come in” yazmam gerektiğini ve bu işlemleri master kullanıcısı olarak yapmam gerekmektedir.


```

bandit31@bandit:/tmp/kaan31/repo$ echo "May I come in?" > key.txt
bandit31@bandit:/tmp/kaan31/repo$ ls
key.txt  README.md
bandit31@bandit:/tmp/kaan31/repo$ cat key.txt
May I come in?
bandit31@bandit:/tmp/kaan31/repo$ git add key.txt
bandit31@bandit:/tmp/kaan31/repo$ git commit -m "new commit"
[master 413f6c1] new commit
 1 file changed, 1 insertion(+)
 create mode 100644 key.txt
bandit31@bandit:/tmp/kaan31/repo$ git push
Could not create directory '/home/bandit31/.ssh'.
The authenticity of host 'localhost (127.0.0.1)' can't be established.
ECDSA key fingerprint is SHA256:98UL0ZW85496EtCRkKlo20X30PnyPSB5tB5RPbhczc.
Are you sure you want to continue connecting (yes/no)? yes
Failed to add the host to the list of known hosts (/home/bandit31/.ssh/known_hosts).
This is a OverTheWire game server. More information on http://www.overthewire.org/wargame
s

bandit31-git@localhost's password:
Counting objects: 3, done.
Delta compression using up to 2 threads.
Compressing objects: 100% (2/2), done.
Writing objects: 100% (3/3), 319 bytes | 0 bytes/s, done.
Total 3 (delta 0), reused 0 (delta 0)
remote: ### Attempting to validate files... ###
remote:
remote: .oOo.oOo.oOo.oOo.oOo.oOo.oOo.oOo.oOo.oOo.
remote:
remote: Well done! Here is the password for the next level:
remote: 56a9bf19c63d650ce78e6ec0354ee45e
remote:
remote: .oOo.oOo.oOo.oOo.oOo.oOo.oOo.oOo.oOo.oOo.
remote:
To ssh://localhost/home/bandit31-git/repo
! [remote rejected] master -> master (pre-receive hook declined)
error: failed to push some refs to 'ssh://bandit31-git@localhost/home/bandit31-git/repo'

```

-Sistemin benden istediği düzenlemeleri yapıyorum ve ardından bir sonraki seviyenin şifresine erişim sağlıyorum.

```

WELCOME TO THE UPPERCASE SHELL
>> ls
sh: 1: LS: not found
>> pwd
sh: 1: PWD: not found
>> $0
$ $SHELL
WELCOME TO THE UPPERCASE SHELL
>> export SHELL=/bin/bash
sh: 1: EXPORT: not found
>> $0
$ export SHELL=/bin/bash
$ ls
uppershell 019
$ cat /etc/bandit_pass/bandit33
c9c3199ddf4121b10cf581a98d51caee

```

-32. Seviyeye geldiğimizde yazdığımız kodları büyük harfe çevirmektedir. Burada kullanım talimatlarına baktığımızda shell dilini değiştirmemiz gerektiğini görüyoruz.

Burada \$0 yazarak komut satırını düşürüyoruz ve shelli değiştirip şifreyi ediniyoruz.