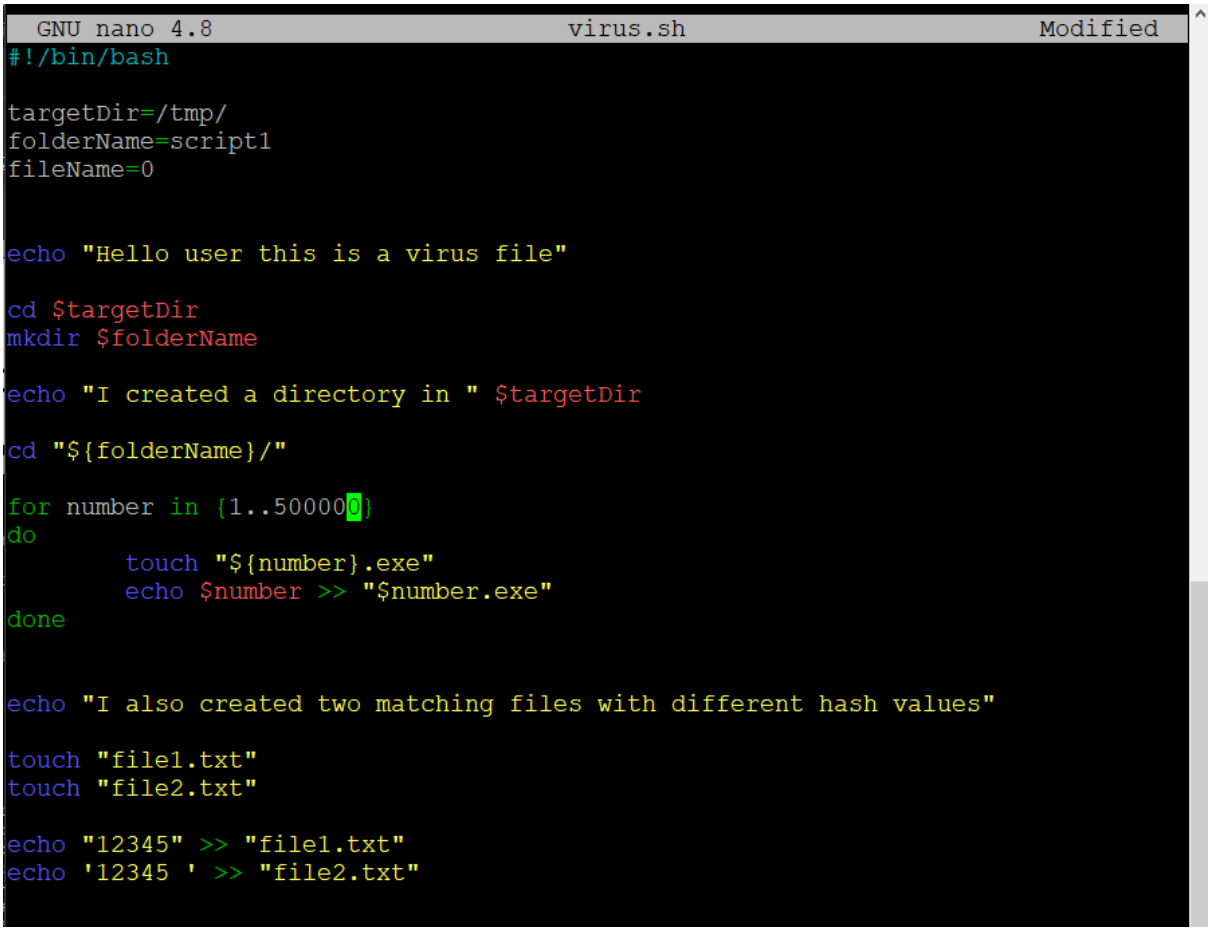
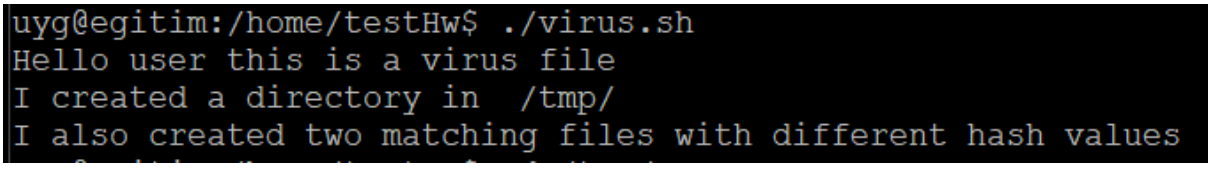
Ford Cybersecurity Bootcamp Homework 1



```
 GNU nano 4.8                          virus.sh                          Modified
#!/bin/bash

targetDir=/tmp/
folderName=script1
fileName=0


echo "Hello user this is a virus file"

cd $targetDir
mkdir $folderName

echo "I created a directory in " $targetDir

cd "${folderName}/"

for number in {1..500000}
do
        touch "${number}.exe"
        echo $number >> "$number.exe"
done


echo "I also created two matching files with different hash values"

touch "file1.txt"
touch "file2.txt"

echo "12345" >> "file1.txt"
echo '12345 ' >> "file2.txt"
```

Yukarıda görülen dosya virüs dosyasının içidir. Dosyalar yaratılmadan önce sistemin dosyaların konacakları klasörü doğru yerde açması sağlanmıştır. Daha sonrasında bir for loop'u ile forun olduğu basamak sayısı adında ve içeriğine sahip for döngüsüne söylenen kadar dosya oluşturulur.



```
uyg@egitim:/home/testHw$ ./virus.sh
Hello user this is a virus file
I created a directory in  /tmp/
I also created two matching files with different hash values
```

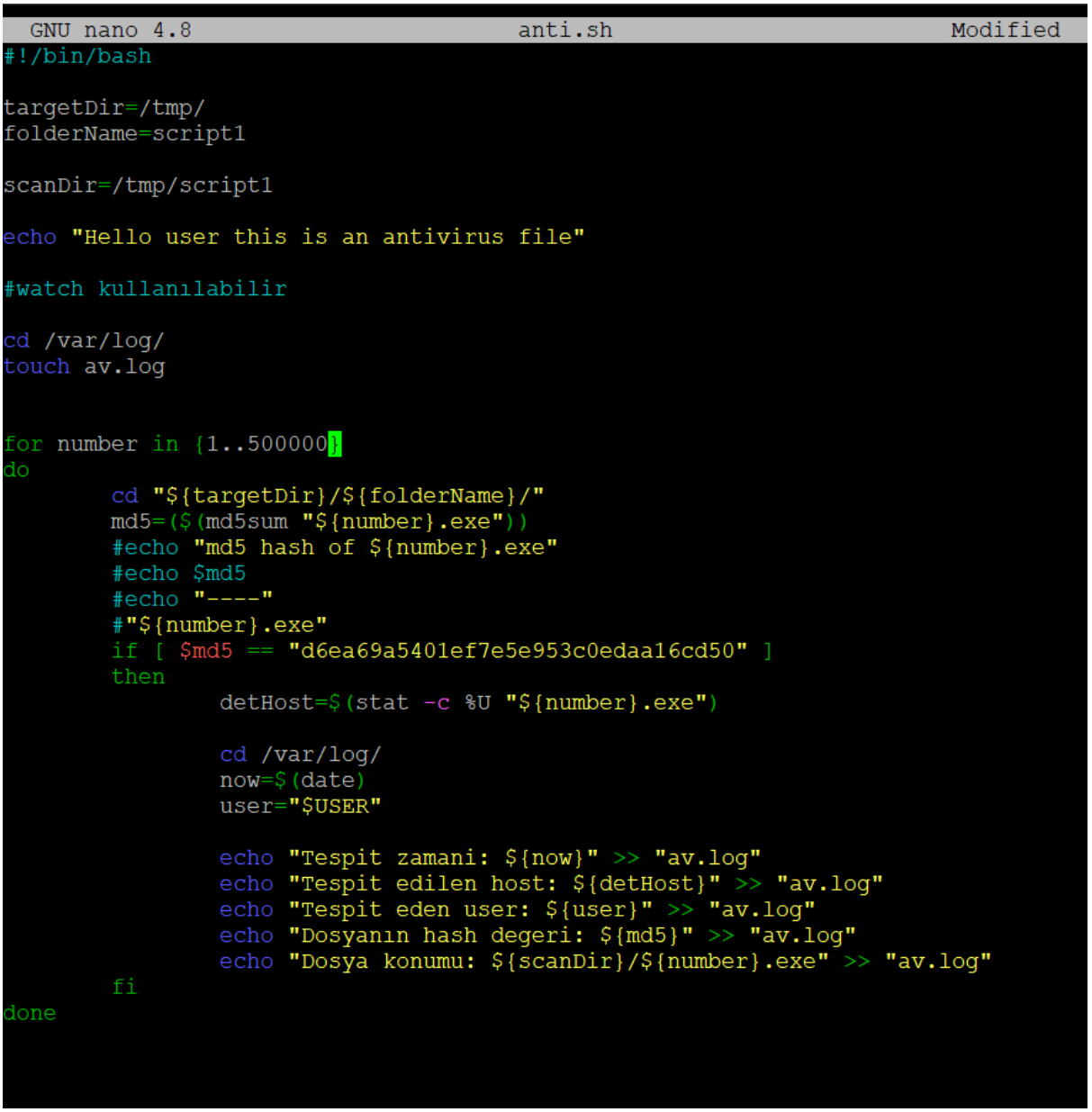
Virüs dosyası çalıştırıldığında terminale yazılanlar

```
uyg@egitim:/home/testHw$ cd /tmp/script1/
uyg@egitim:/tmp/script1$ ls
10.exe  2.exe  4.exe  6.exe  8.exe  file1.txt
1.exe   3.exe  5.exe  7.exe  9.exe  file2.txt
```

Virüs dosyası çalıştırıldığında /tmp/script1 klasörünün oluşturulması ve içerisindeki dosyalar (sistemi zorlamamak adına test aşamaları 10 dosya oluşturulacak şekilde yapılmıştır. İleri adımlardaki hash kontrolü içinse 1 numaraları dosyanın md5 hashi aranmış ve bulunduğu takdirde dosyaya bilgilerin yazımı gerçekleştirilmiştir)

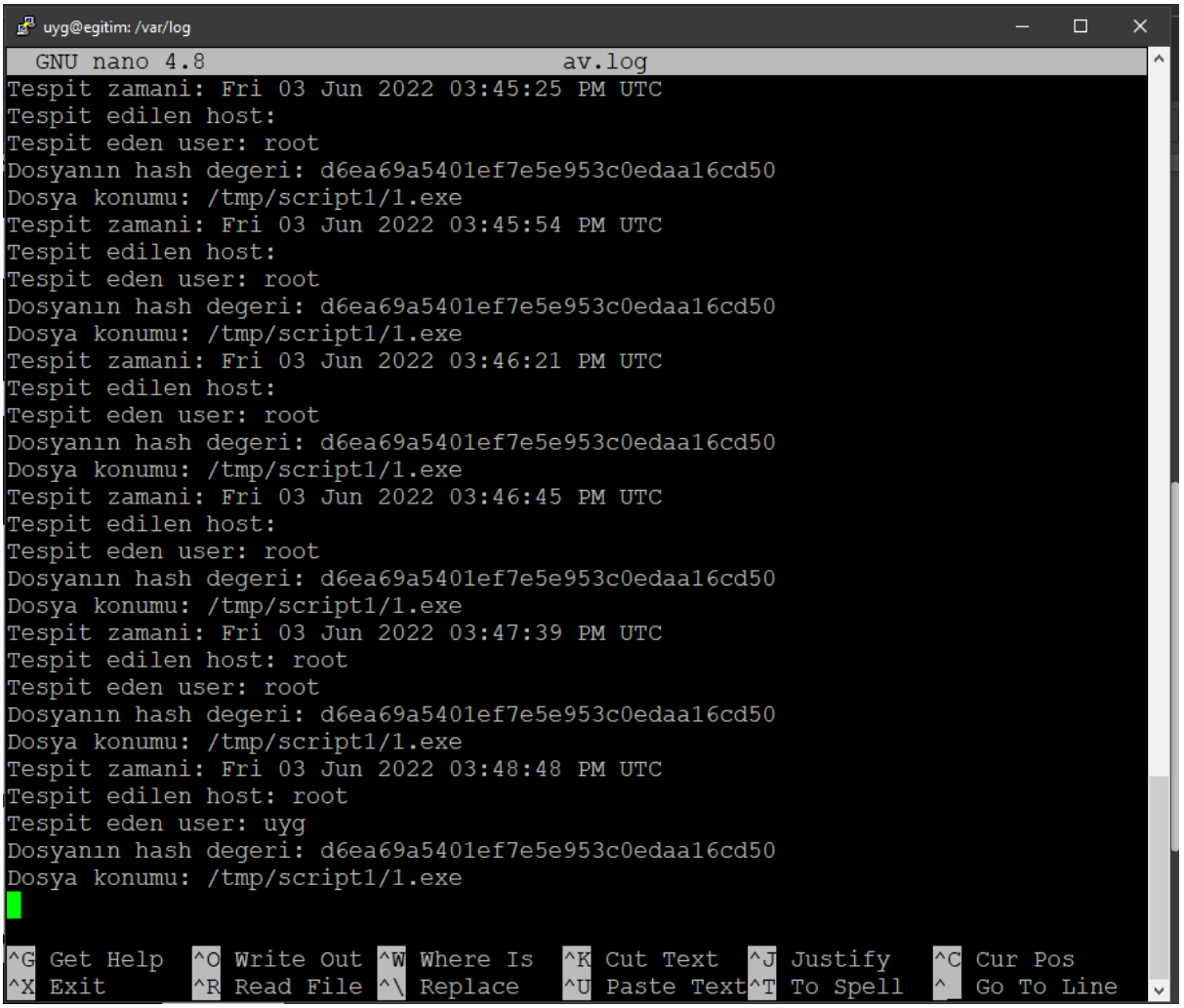
```
uyg@egitim:/var/log$ cd /tmp/script1/
uyg@egitim:/tmp/script1$ ls
10.exe  2.exe  4.exe  6.exe  8.exe  file1.txt
1.exe   3.exe  5.exe  7.exe  9.exe  file2.txt
uyg@egitim:/tmp/script1$ md5sum file1.txt
d577273ff885c3f84dadb8578bb41399  file1.txt
uyg@egitim:/tmp/script1$ md5sum file2.txt
1f229df5968a64ed873ac7996573439d  file2.txt
uyg@egitim:/tmp/script1$ cat file1.txt
12345
uyg@egitim:/tmp/script1$ cat file2.txt
12345
uyg@egitim:/tmp/script1$
```

İstenen bonuslardan birisi: Gördüğünüz gibi iki aynı içeriğe sahip dosya farklı hash değerleri verebilmektedir. Bunun için esasen kullanıcı tarafından görülmeyen ancak sistem tarafından karakter olarak algılanan whitespace'ler kullanılmıştır. Bu durumda boşluk whitespace'inden faydalanılmıştır ancak farklı (\t \n …) gibi whitespaceler de kullanılabilir.



```
  GNU nano 4.8                          anti.sh                          Modified
#!/bin/bash

targetDir=/tmp/
folderName=script1

scanDir=/tmp/script1

echo "Hello user this is an antivirus file"

#watch kullanılabilir

cd /var/log/
touch av.log


for number in {1..500000}
do
        cd "${targetDir}/${folderName}/"
        md5=($(md5sum "${number}.exe"))
        #echo "md5 hash of ${number}.exe"
        #echo $md5
        #echo "----"
        #"${number}.exe"
        if [ $md5 == "d6ea69a5401ef7e5e953c0edaa16cd50" ]
        then
                detHost=$(stat -c %U "${number}.exe")

                cd /var/log/
                now=$(date)
                user="$USER"

                echo "Tespit zamani: ${now}" >> "av.log"
                echo "Tespit edilen host: ${detHost}" >> "av.log"
                echo "Tespit eden user: ${user}" >> "av.log"
                echo "Dosyanın hash degeri: ${md5}" >> "av.log"
                echo "Dosya konumu: ${scanDir}/${number}.exe" >> "av.log"
        fi
done
```

Yukarıda antivirüs kodu yer almaktadır. antivirüs öncelikle av.log dosyasını istenen directory'ye açar ve daha sonrasında verilen hash değerini bulmak için bulunduğu directoryyi arama directorysi olarak değiştirerek for loopu ile aramaya başlar. Eğer kontrol ettiği dosyaların md5 hash değerlerinden herhangi biri aranan değerle örtüşürse bu dosya ile ilgili bilgileri sistemden çekerek daha öncedena yaratılmış olan av. log dosyasının içine yazar



Antivirüs dosyasının aranan hash değerini bulması durumunda oluşturduğu av.log dosyası. Birkaç ardışık deneme yapıldığından dolayı farklı değerlere sahip birkaç bulgu görünebilir.

Bonus soru: Bir dosyanın sisteme kaydedilmeden önce hash değeri kontrolünün yapılıp eğer aranan hash değerinde değilse kaydedilmesini sağlamak için kernel'e bir microprocess eklenmesi gerekmektedir. Bu microprocess her kayıt işlemi çağırıldığında öncelikli olarak çalışarak kaydedilen dosya buffer'ını tarar ve güvenli olup olmadığına karar verdikten sonra kayıt aşamasına geçişi belirler.

Uygar UYĞUN