HF2019

Kaan Efe Öğüt

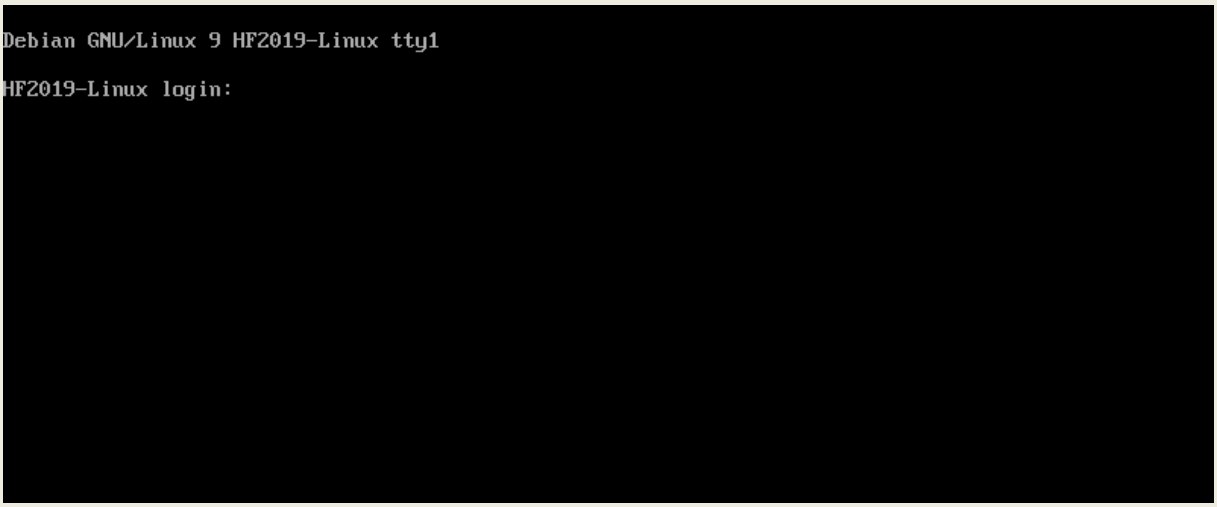
ADLİ BİLİŞİM MÜHENDİSLİĞİ

-Vulnhub üzerinde bulunan HF2019 zafiyetli makinesini birlikte çözeceğiz.

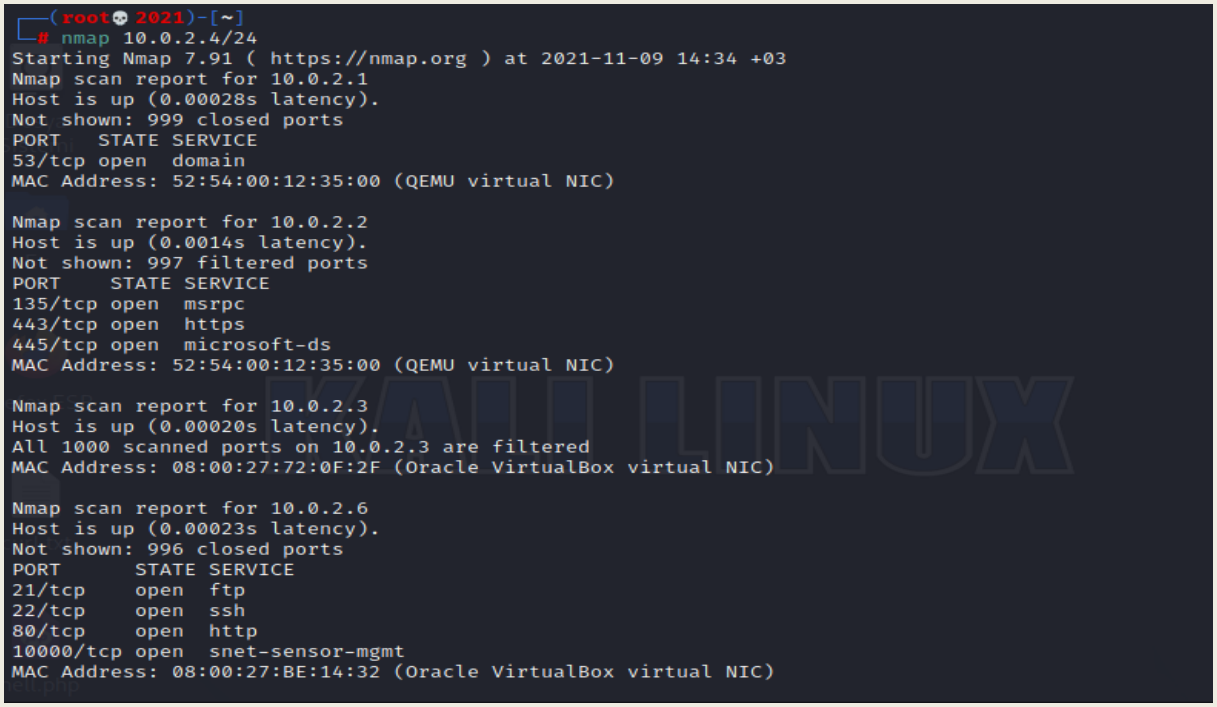
11.11.2021

-"https://www.vulnhub.com/entry/hacker-fest-2019,378/" adresinde bulunan zafiyetli makineyi öncelikle bu adresten indiriyorum.

-İndirme işleminin ardından İmport ediyorum ve Linux ile aynı ağ ayarlarına getiriyorum.



- Gerekli ayarlardan sonra makineyi başlatıp bu ekranda arka planda çalışır durumda bırakıyorum.

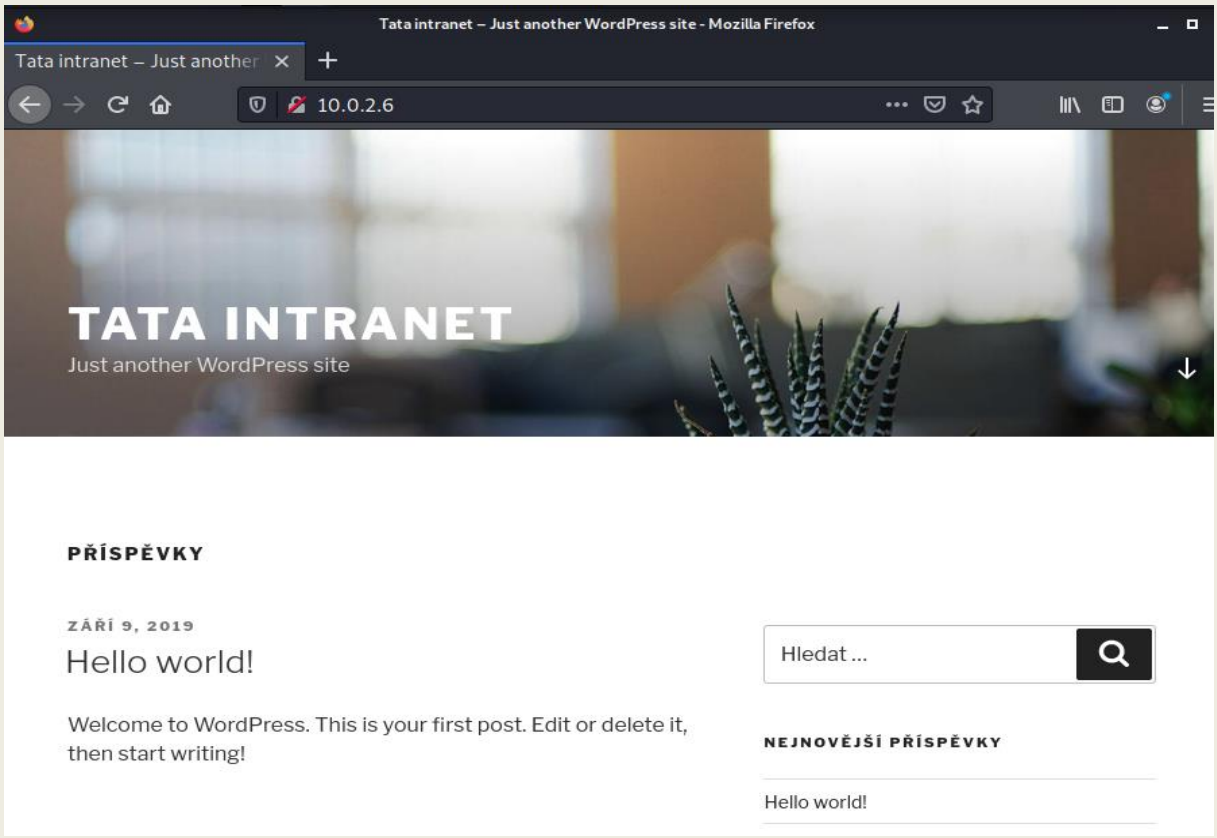


- Nmap üzerinden ağ taraması gerçekleştiriyorum ve zafiyetli makinenin IP adresine ulaşıyorum.

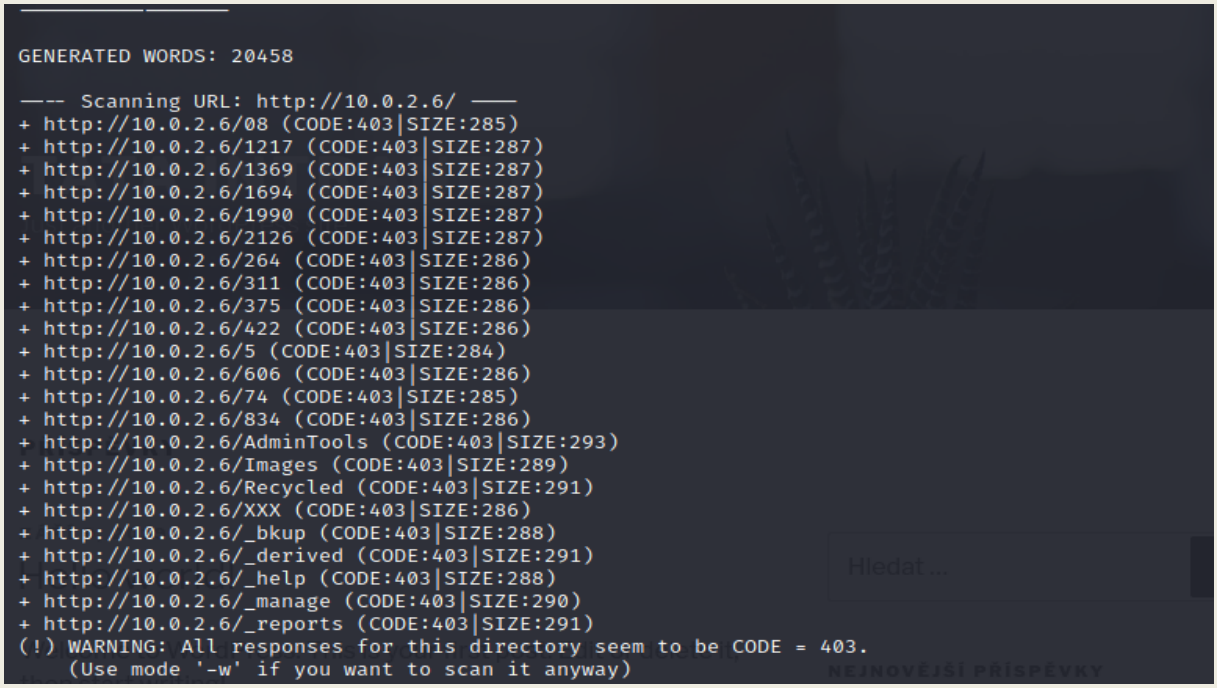
```
└─# nmap -sV -sC -p- 10.0.2.6
Starting Nmap 7.91 ( https://nmap.org ) at 2021-11-09 14:36 +03
Nmap scan report for 10.0.2.6
Host is up (0.00017s latency).
Not shown: 65531 closed ports
PORT      STATE SERVICE  VERSION
21/tcp    open  ftp      vsftpd 3.0.3
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
| -rw-rw-r--    1 ftp      ftp           420 Nov 30  2017 index.php
| -rw-rw-r--    1 ftp      ftp         19935 Sep 05  2019 license.txt
| -rw-rw-r--    1 ftp      ftp          7447 Sep 05  2019 readme.html
| -rw-rw-r--    1 ftp      ftp          6919 Jan 12  2019 wp-activate.php
| drwxrwxr-x    9 ftp      ftp          4096 Sep 05  2019 wp-admin
| -rw-rw-r--    1 ftp      ftp           369 Nov 30  2017 wp-blog-header.php
| -rw-rw-r--    1 ftp      ftp          2283 Jan 21  2019 wp-comments-post.php
| -rw-rw-r--    1 ftp      ftp          3255 Sep 27  2019 wp-config.php
| drwxrwxr-x    8 ftp      ftp          4096 Sep 29  2019 wp-content
| -rw-rw-r--    1 ftp      ftp          3847 Jan 09  2019 wp-cron.php
| drwxrwxr-x   20 ftp      ftp         12288 Sep 05  2019 wp-includes
| -rw-rw-r--    1 ftp      ftp          2502 Jan 16  2019 wp-links-opml.php
| -rw-rw-r--    1 ftp      ftp          3306 Nov 30  2017 wp-load.php
| -rw-rw-r--    1 ftp      ftp         39551 Jun 10  2019 wp-login.php
| -rw-rw-r--    1 ftp      ftp          8403 Nov 30  2017 wp-mail.php
| -rw-rw-r--    1 ftp      ftp         18962 Mar 28  2019 wp-settings.php
| -rw-rw-r--    1 ftp      ftp         31085 Jan 16  2019 wp-signup.php
| -rw-rw-r--    1 ftp      ftp          4764 Nov 30  2017 wp-trackback.php
|_-rw-rw-r--    1 ftp      ftp          3068 Aug 17  2018 xmlrpc.php
| ftp-syst:
```

- Daha detaylı bilgi sahibi olmak Nmap üzerinden Zafiyetli makinenin taramasını gerçekleştiriyorum.

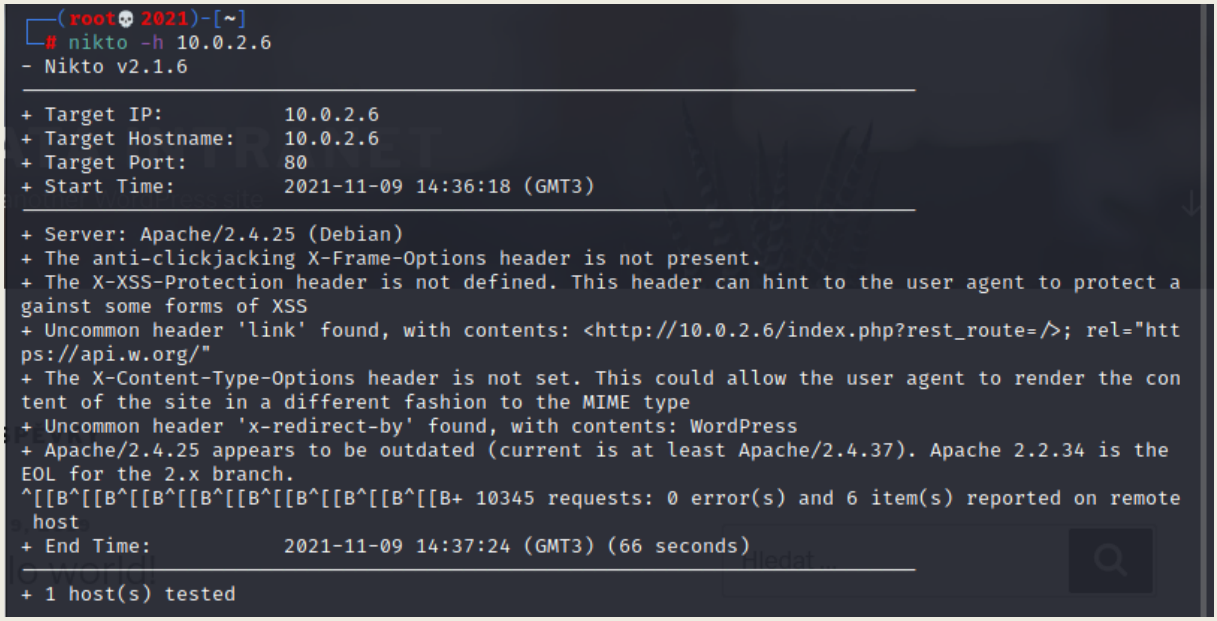
-Burada Sftpd,Worddpress,OpenSSH,Webmin gibi servisler kullanıldığını ve bu servislerin sürümlerini öğrenebildim.



- HTTP servisi aktif olduğu için web sayfasını görüntülüyorum ve karşıma böyle bir arayüz çıkıyor.

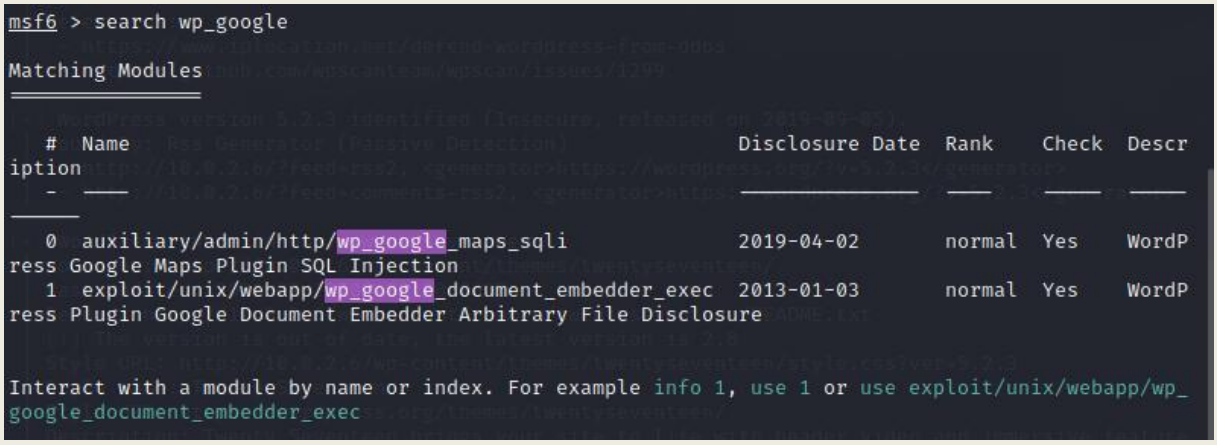


- Web servisi aktif olduğu için ilk önce Dirb ile bir tarama gerçekleştirmek istedim.



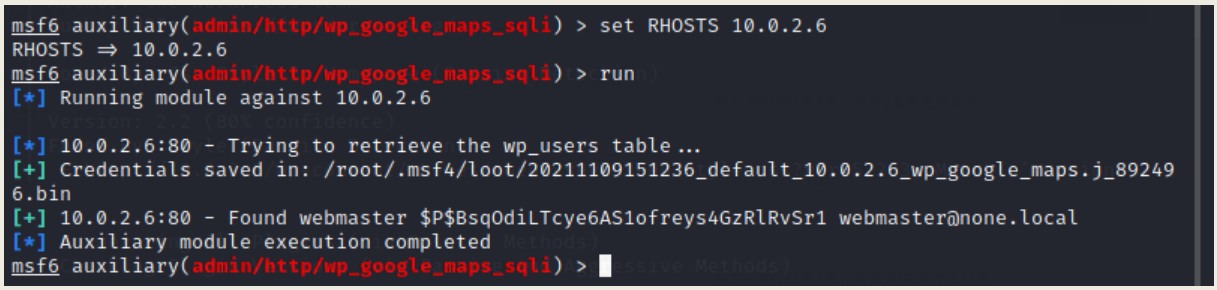
- Bu işlem arka planda yapılırken nikto aracını da çalıştırıp bilgi toplamaya çalıştım.

-Burada da Wordpress olduğunu görüntüledim.

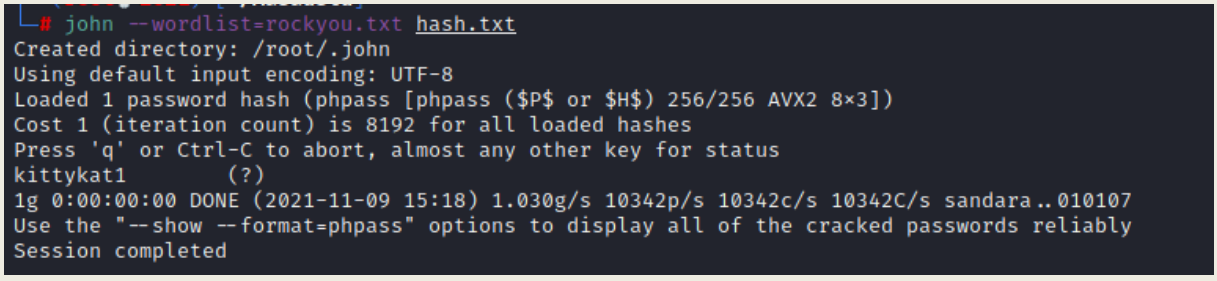


-"wp_google" kullandığını görüntülüyorum ve Metasploit başlatıp bu servis ile ilgili bir açık var mı diye tarıyorum.

-Karşıma çıkan açıkları denemek istiyorum.

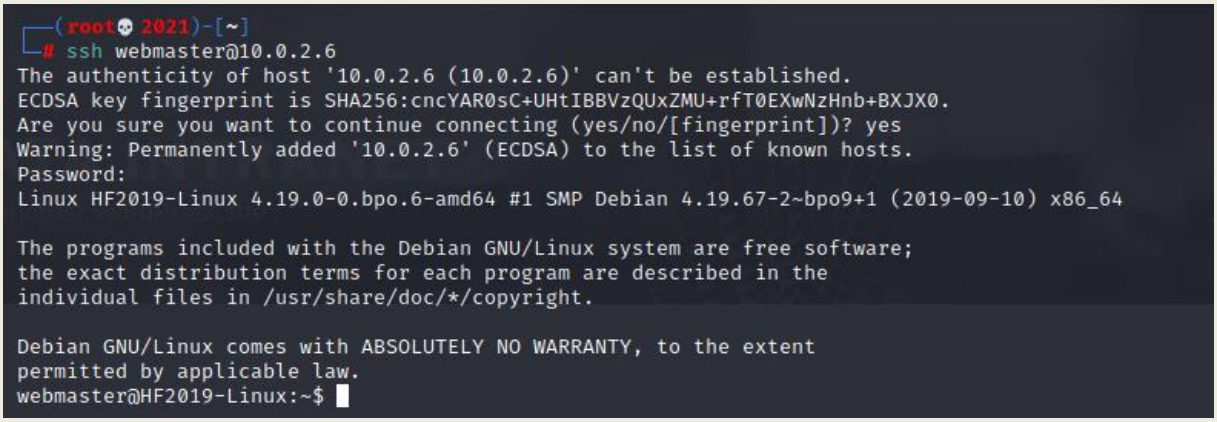


- Gerekli bilgileri set ettikten sonra aracı çalıştırıyorum ve sonucunda bana bir hash değeri döndürüyor.

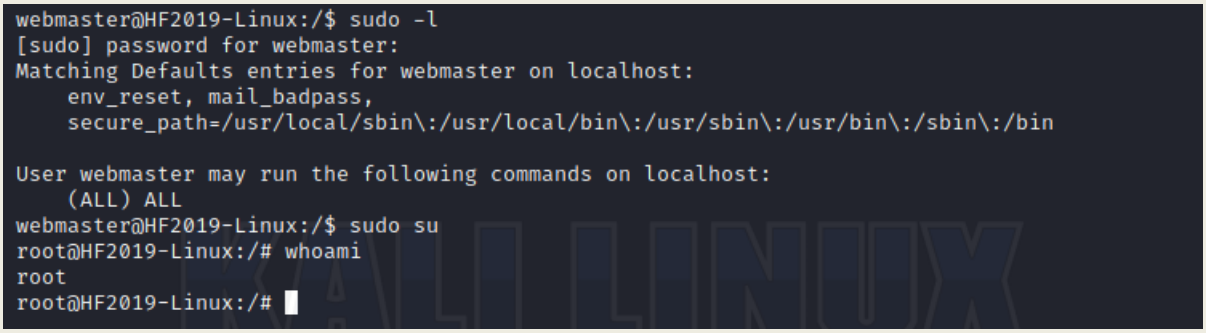


-Elde ettiğim hash değerini çözmek için Johntheripper aracını kullanacağım.

-Burada da kullanacağım Wordlist Rockyou.txt olacaktır.Sonucunda başarılı bir şekilde şifre döndü.



-Elde ettiğim şifrenin SSH bağlantı şifresi olduğunu düşünüyorum.Kullanıcı adını da metasploit üzerinde görüntüleyebilmiştim.



-Burada "sudo -l" komutunu kullanıyorum ve karşıma çıkan notta istediğim komutu çalıştırabileceğim söyleniyor.Bende "sudo su" komutunu kullanıyorum ve başarılı bir şekilde root oluyorum.

-Zafiyetten başarılı bir şekilde yararlanabildik.