SAR-1 CTF

Kaan Efe Öğüt

ADLİ BİLİŞİM MÜHENDİSLİĞİ

-Vulnhub üzerinde bulunan “SAR-1” zafiyetli makinesini Crontab tablosu ile sızmaya çalışacağız.

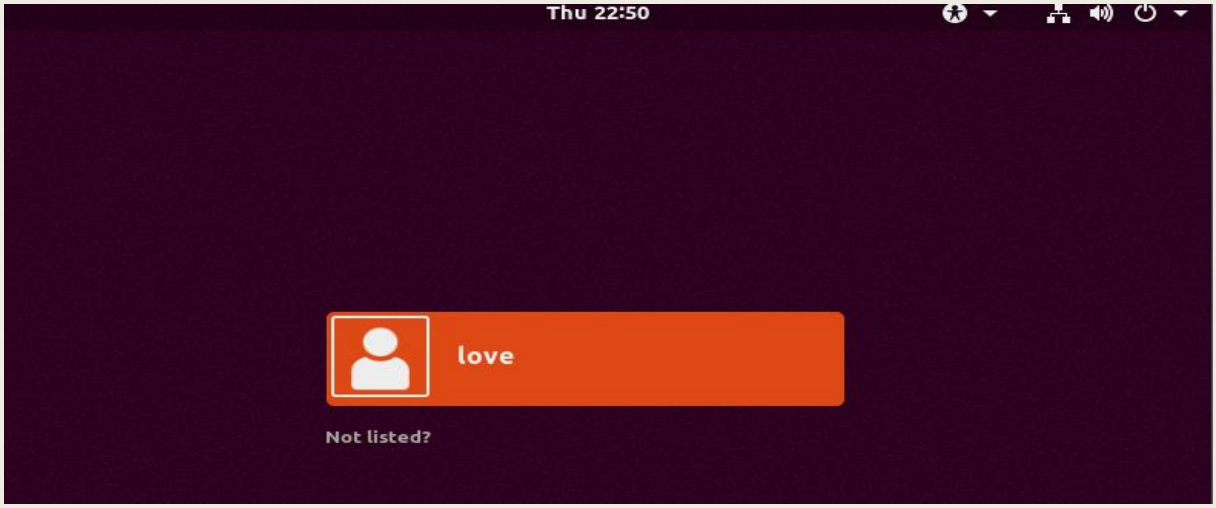
14.11.2021

Crontab ile Root Olma

-"https://www.vulnhub.com/entry/sar-1,425/" bağlantısı üzerinden zafiyetli makinemi indiriyorum.

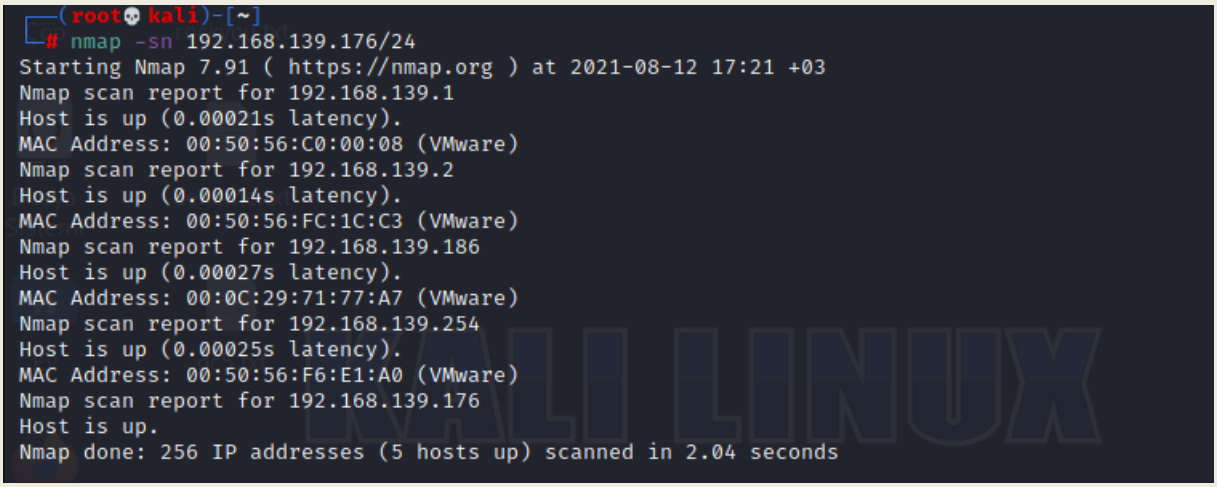
-Vmware üzerinde indirdiğim bu zafiyetli makineyi "open" komutu ile açıyorum.

-Network ayarlarını Sanal Makinem ile aynı yapıyorum.

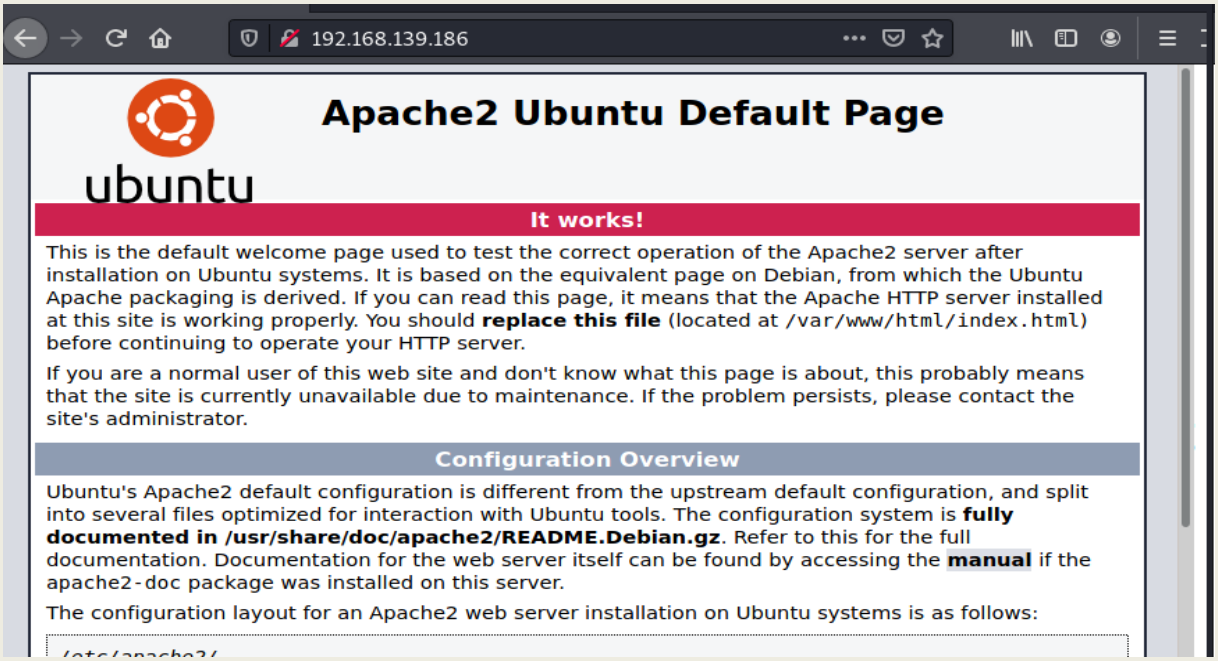


-Gerekli ayarlardan sonra sanal makinemi başlatıyorum ve arka planda bu şekilde çalışır vaziyette bırakıyorum.

-Ardından Linux makineme geçiş yapıyorum.



-Uçbirim üzerinden nmap ile port taraması gerçekleştiriyorum ve zafiyetli makinemin IP adresini öğreniyorum.



-Zafiyetli makineyi tarayıcı üzerinde görüntülediğimde bu şekildedir.

```
└─# nmap -A -sC 192.168.139.186 -o sar.txt
Starting Nmap 7.91 ( https://nmap.org ) at 2021-08-12 17:24 +03
Nmap scan report for 192.168.139.186
Host is up (0.00031s latency).
Not shown: 999 closed ports
PORT   STATE SERVICE VERSION
80/tcp open  http    Apache httpd 2.4.29 ((Ubuntu))
|_http-server-header: Apache/2.4.29 (Ubuntu)
|_http-title: Apache2 Ubuntu Default Page: It works
MAC Address: 00:0C:29:71:77:A7 (VMware)
Device type: general purpose
Running: Linux 4.X|5.X
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5
OS details: Linux 4.15 - 5.6
Network Distance: 1 hop

TRACEROUTE
HOP RTT     ADDRESS
1   0.31 ms 192.168.139.186

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 9.45 seconds
```

-Nmap aracı ile öncelikle kapsamlı bir ağ taraması gerçekleştiriyorum.

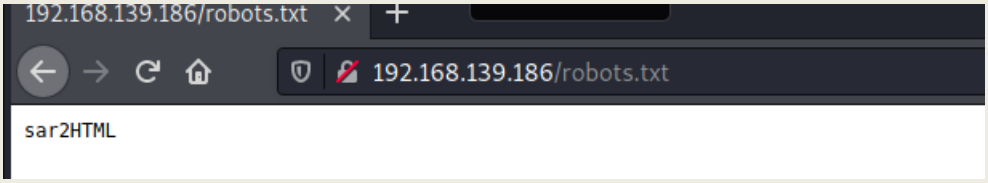
-Çok fazla bir bilgi elde edemedim.

```
gobuster dir -u http://192.168.139.186 -w /usr/share/dirb/wordlists/common.txt
===============================================================
Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://192.168.139.186
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/dirb/wordlists/common.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.1.0
[+] Timeout:                 10s
===============================================================
2021/08/12 17:23:56 Starting gobuster in directory enumeration mode
===============================================================
/.hta                 (Status: 403) [Size: 280]
/.htpasswd            (Status: 403) [Size: 280]
/.htaccess            (Status: 403) [Size: 280]
/index.html           (Status: 200) [Size: 10918]
/phpinfo.php          (Status: 200) [Size: 95431]
/robots.txt           (Status: 200) [Size: 9]
/server-status        (Status: 403) [Size: 280]

===============================================================
2021/08/12 17:24:01 Finished
===============================================================
```

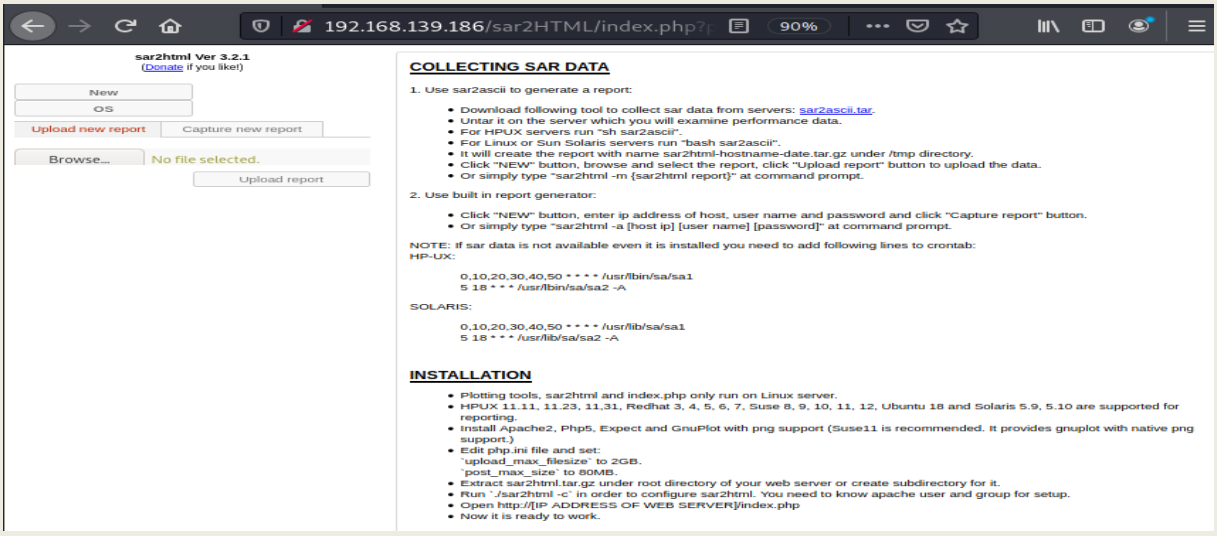
-Gobuster aracı ile dizin taraması başlatıyorum.

-Burada bulduğu dizinleri açıp içerisinden bilgi toplamaya çalışıyorum.



-Web sayfası üzerinde ilk bakmamız gereken yerlerden biri robots.txt'dir.

-Burada bir html uzantısı görüyorum ve bunu kopyalıyorum.



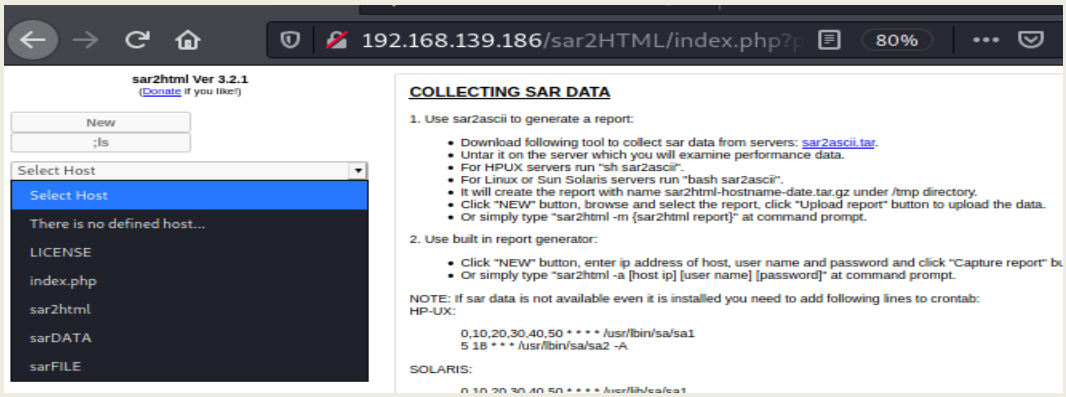
-HTML uzantılı URL'i açtığımda karşıma böyle bir sayfa geliyor.

-Burada çok önemli olarak sar versiyonunu görüntülüyorum.

```
┌──(root💀kali)-[~]
└─# searchsploit sar2html 3.2.1
 Exploit Title                                                 |  Path
---------------------------------------------------------------- ---------------------------------
sar2html 3.2.1 - 'plot' Remote Code Execution                  | php/webapps/49344.py
Sar2HTML 3.2.1 - Remote Command Execution                      | php/webapps/47204.txt
---------------------------------------------------------------- ---------------------------------
Shellcodes: No Results
```

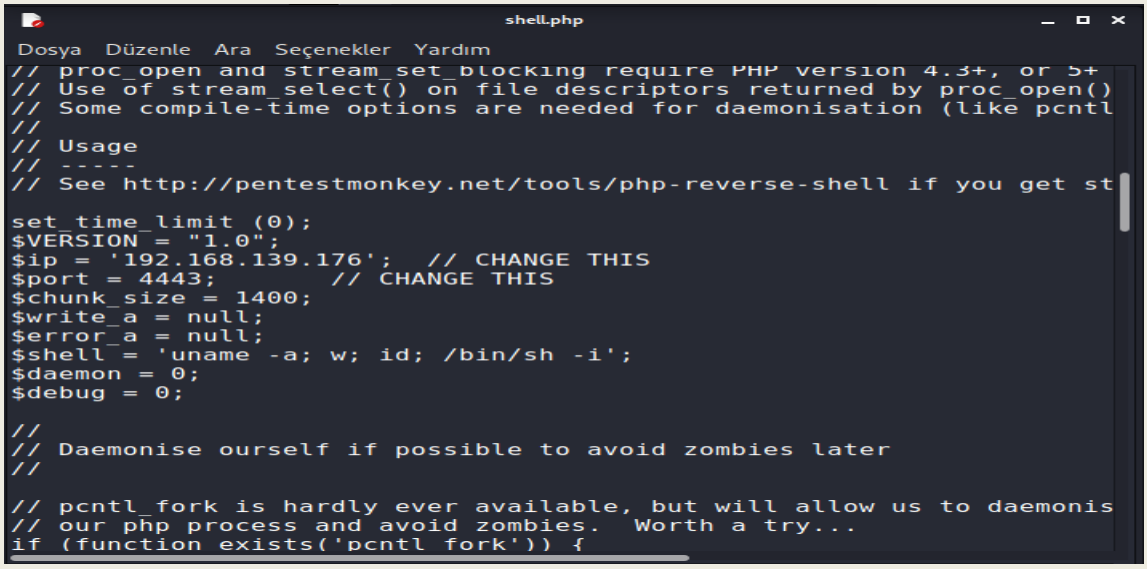
-Bu versiyonda çalışan bir exploit elde edip işlem gerçekleştirebiliriz.

-Exploit taraması gerçekleştiriyorum burada 2 adet exploit bizi karşılıyor.



-Tarayıcı üzerinden aynı exploiti arattığımda bana kullanımıyla ilgili bilgi sağlıyor.

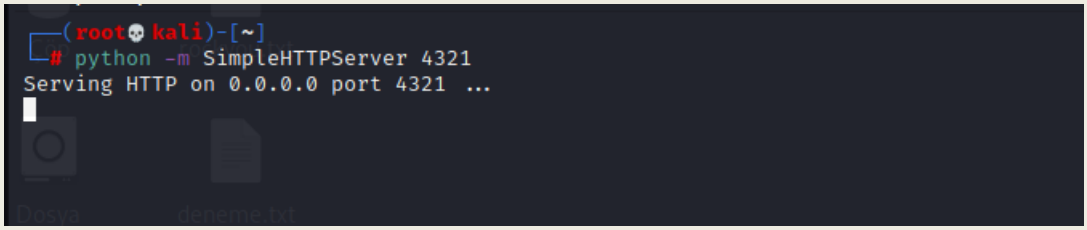
-URL sonuna ";ls" komutunu eklediğimde burada bilgi erişimi sağladığımı görüntülüyorum.



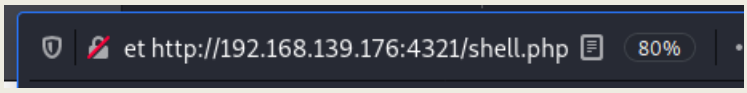
-Bu ls komutu yerine bir shell kabuğu ekleyip işlem gerçekleştirebilirim diye düşünüyorum.

-Bu sebeple önceki uygulamalarımızda kullandığım shell.php dosyasını kontrol ediyorum.

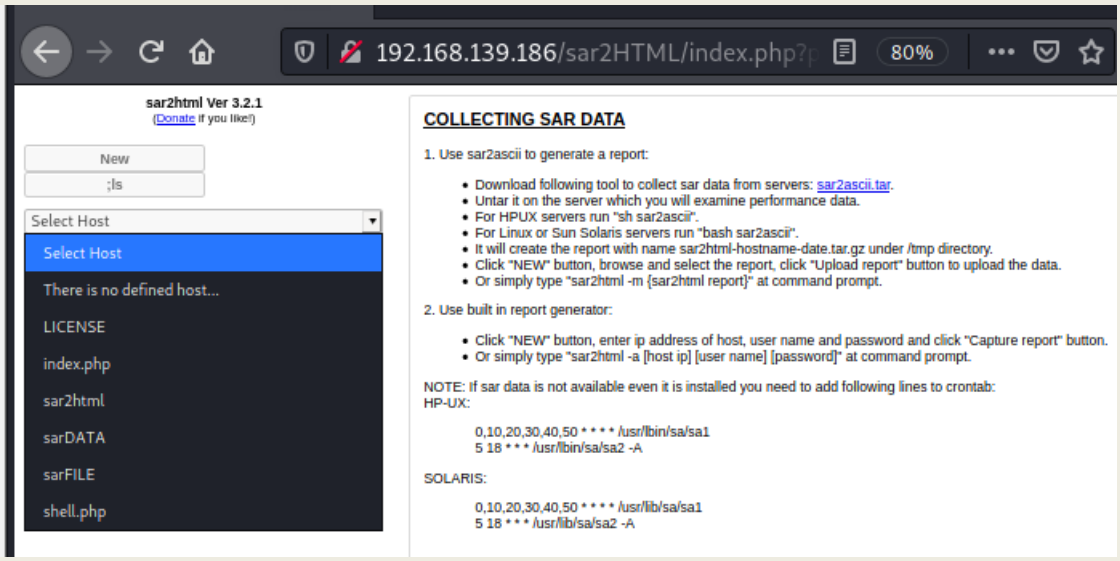
-Buraya IP adresimi ve port bilgisi ayarlarını set ediyorum.



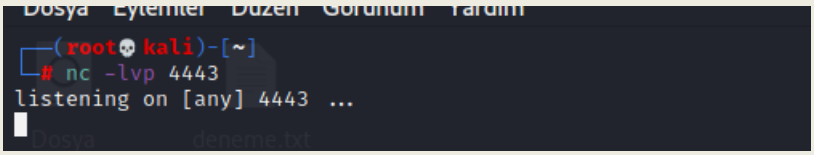
-Bu shell dosyasını sunucuya ekleyebilmem için python komutu ile HTTP server'ı başlatıyorum.



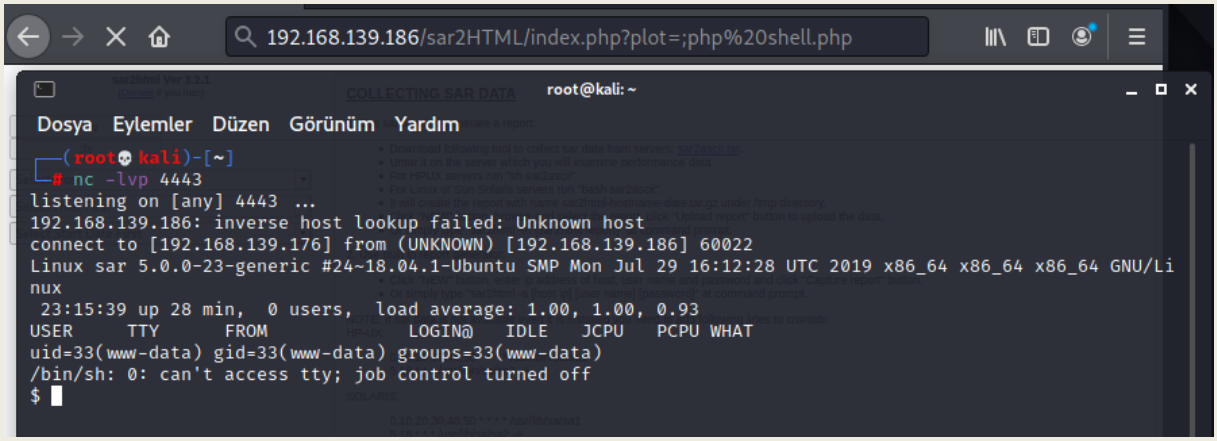
-URL Sonuna eklediğim "wget" komutu ile indirme işlemini başlatıyorum.



-URL sonuna eklediğim ";ls" komutu ile kontrol sağlıyorum ve başarılı bir şekilde aktarım olduğunu görüntülüyorum.

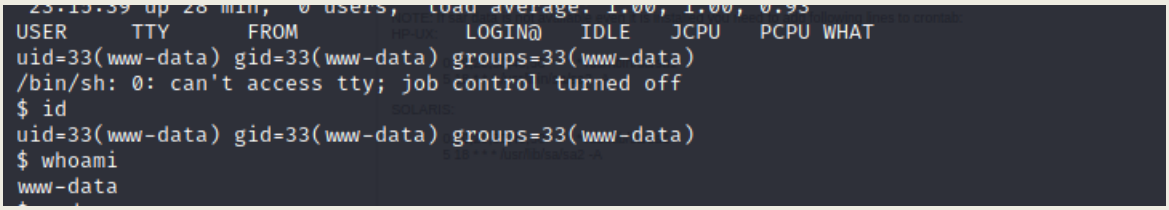


-Şimdi ise netcat üzerinden .php dosyası içerisinde belirttiğim portu dinlemeye alıyorum.



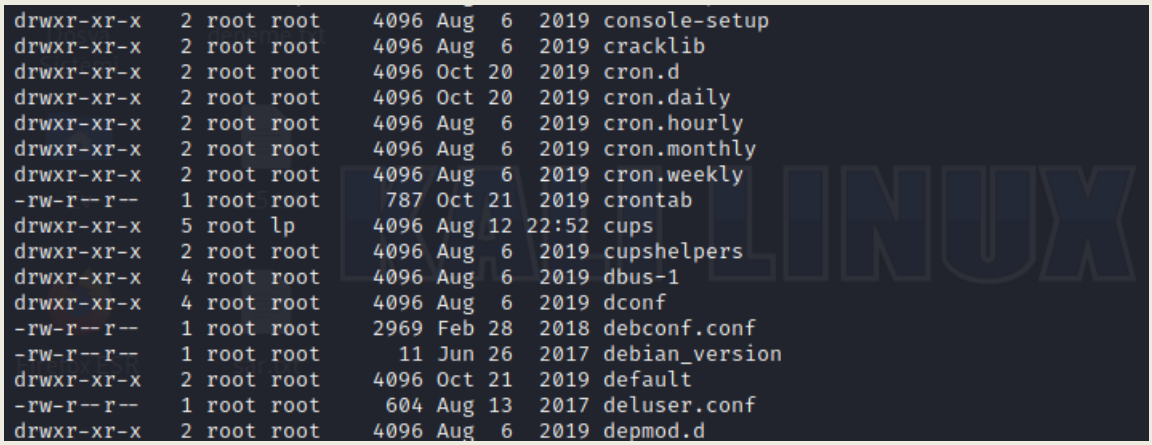
-Daha sonrasında sunucu üzerinde bu .php dosyasını çalıştırıyorum.

-Burada netcat üzerinden bağlantı sağladığımı görüntülüyorum.



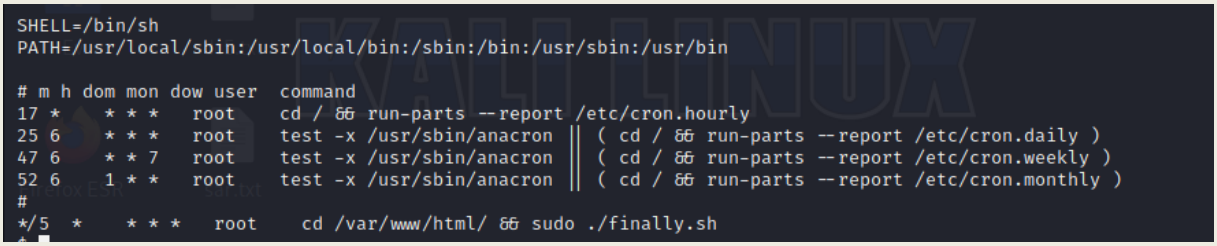
-Yetkime baktığımda yetkisiz bir kullanıcı olduğumu görüntülüyorum.

-Burada ya bir önceki uygulamamızda yaptığımız SUID işlemine bakacağım ya da config dosyası arayacağım.

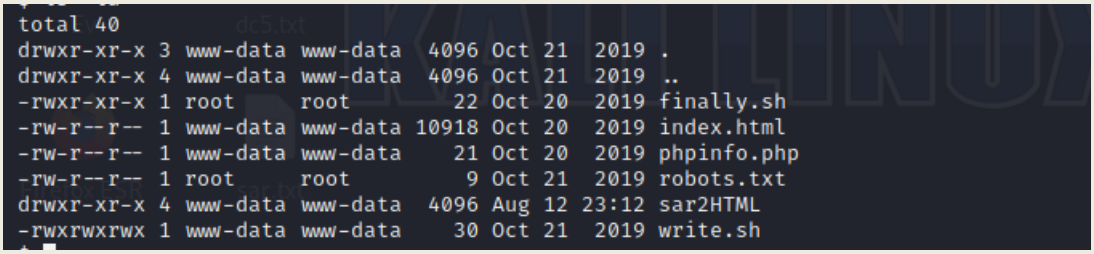


-"/Etc" dizine geçiş yapıyorum ve burada zamanlayıcı olan "crontab" dizinini kullanıp kullanamadığım yetkisine bakıyorum.

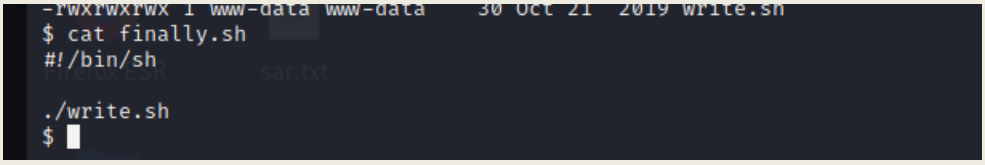
-Crontab tablosuna yetkili bir şekilde erişebiliyorum.



-Crontab dosyasını "cat" komutu ile görüntülediğim de burada bir "finally.sh" dosyası olduğunu ve 5 dakikada bir çalıştığını görüntülüyorum.



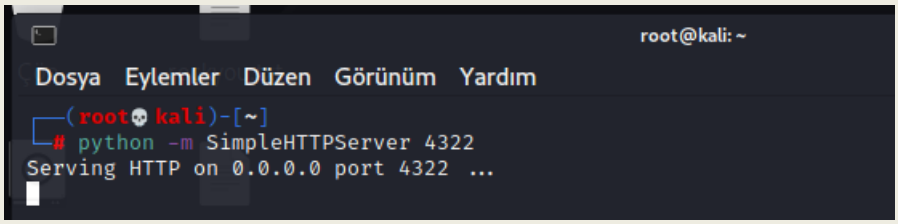
-Burada bilgisine eriştiğim "/var/www/html" dizinine geçiş yapıyorum ve "ls -la" komutu ile finally.sh dosyasını root'un çalıştırdığını görüntülüyorum.



-Burada "write.sh" dosyasını görüntülüyorum.

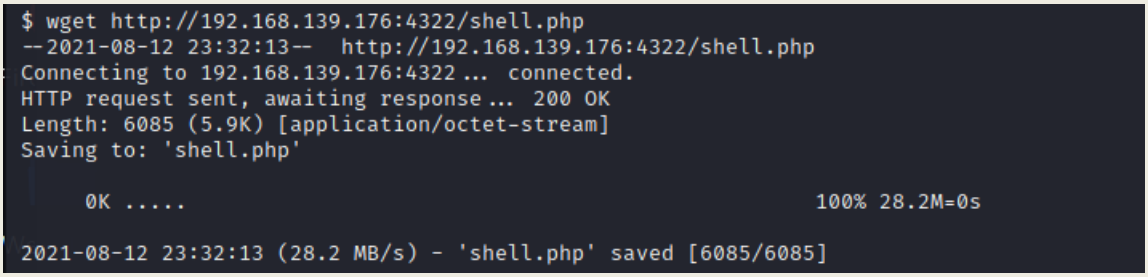
-"Finally.sh" dosyasını açtığımda "write.sh" dosyasını çalıştırdığını görüntülüyorum.

-Write.sh dosyasının içerisine bir php dosyası eklersem burada root yetkisi ile bir shell kapısı oluşturabilirim.

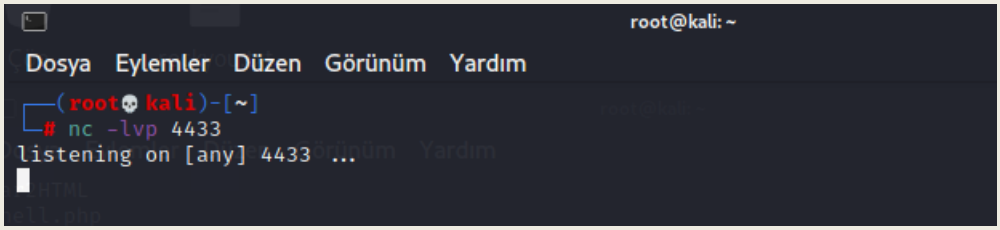


-Shell dosyamın bu sefer port numarasını değiştirip set ediyorum.

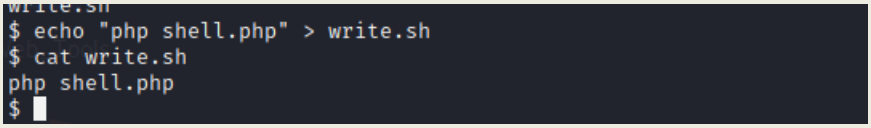
-Bu dosyayı paylaşabilmek için HTTP server'ı tekrar başlatıyorum.



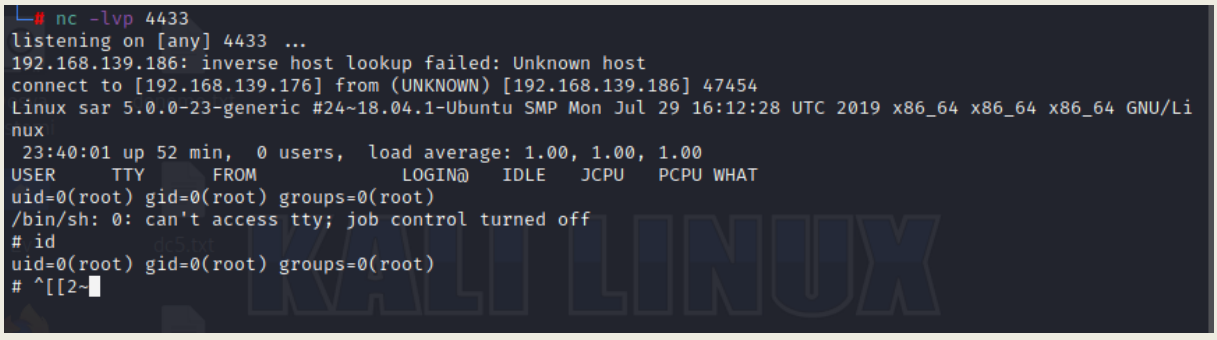
-Shell dosyamı finally.sh ile aynı dizine indiriyorum.



-Daha sonrasında shell.php içerisinde belirttiğim portu dinlemeye alıyorum.



-"Echo" komutu ile shell.php dosyasını write.sh dosyasına yazıyorum.



-Program 5 dakika da bir çalışacağı için artık tek yapacağım şey beklemek olacaktır.

-Bu bekleme işleminin ardından bağlantıyı kurabildim.

-Root yetkisine sahip bir şekilde makineye sızabildim.