

WRITEUP Fostifest



By : ctflsMagic

!root, katana, urxry_zhqn

Table of Content

WRITEUP Fostifest	1
By : ctflsMagic	1
Bonus	3
# Sanity Check	3
Chall	3
Technical Report	3
Flag	3
# Form Feedback CTF COMPFEST 14	4
Chall	4
Technical Report	4
Flag	4
# Fosti Server Password	5
Chall	5
Technical Report	5
Flag	5
# FORENSICS	5
# The attacker	6
Chall	6
Technical Report	6
Flag	7

Bonus

Sanity Check

Chall



Challenge 21 Solves

Sanity Check

50

Flag: Fostifest{Anjazzz_Kelazzzzzzzzz}

Flag

Submit

Technical Report

Dari challnya sudah diberikan sehingga untuk penggunaan sanity check tersebut dapat digunakan copy paste kedalam kolom input flagnya

Flag

Fostifest{Anjazzz_Kelazzzzzzzzz}

Form Feedback CTF COMPFEST 14

Chall

Challenge

0 Solves

×

Feedback

50

Link: <https://forms.gle/f7umuTZr4Ue1EnuDA>

Flag

Submit

Technical Report

Dari pihan panitia fostifest diberikan form untuk review yang dimana akan mendapatkan flag gratis. Karena sudah pusing dengan soal-soal yang gahar maka dari itu kita tinggal klik linknya lalu diisi seperti dibawah

The image shows a Google Form titled "Festi Server Password". It contains four text input fields, each with a red asterisk indicating it is required. The first field is labeled "Email *" and contains the text "gricowijaya@gmail.com". The second field is labeled "Nama Team *" and contains the text "ctfisMagic". The third field is labeled "Kritik *" and contains the text "Sempat beberapa service yang down, file vm cukup besar,". The fourth field is labeled "Saran *" and contains the text "untuk lab sudah keren bagian forensiknya mungkin dapat digunakan dengan distro tanpa desktop environment, semoga taun-taun selanjutnya attempt lebih banyak :(". Below the fields are two buttons: "Berikutnya" (Next) and "Kosongkan formulir" (Clear form). At the bottom, there is a disclaimer: "Jangan pernah mengirimkan sandi melalui Google Formulir." and a link to "Konten ini tidak dibuat atau didukung oleh Google. [Laporkan Penyalahgunaan](#) - [Persyaratan Layanan](#) - [Kebijakan Privasi](#)".

Lalu klik button berikutnya sehingga akan mendapatkan

Flag

COMPFEST14{Terima kasih sudah mengisi feedback ini! Semoga mendapatkan hasil yang terbaik!!!}

Fosti Server Password

Chall

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

fostifest_d52f925a44fe265dcf678e8da09aab79

Flag chall ini: Fostifest{%s} %password

Technical Report

Diketahui Zip Fosti Server Password: fostifest_d52f925a44fe265dcf678e8da09aab79

Jadi langsung saja kita masukkan Flag chall ini yaitu Fostifest{%s} %password. Dimana password = fostifest_d52f925a44fe265dcf678e8da09aab79. Jadi flag nya yaitu Fostifest{fostifest_d52f925a44fe265dcf678e8da09aab79}.

Flag

Fostifest{fostifest_d52f925a44fe265dcf678e8da09aab79}

FORENSICS

The attacker

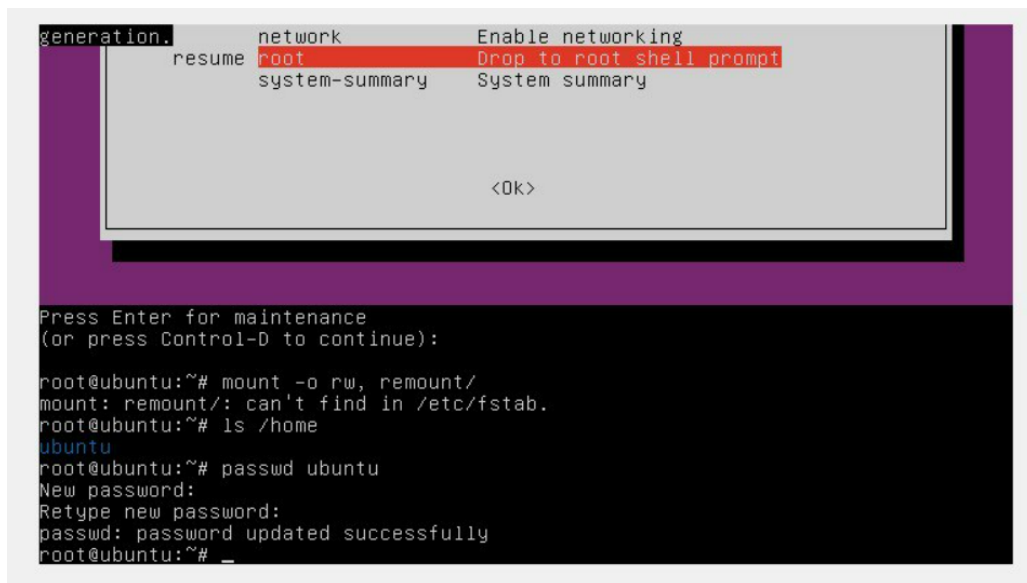
Chall

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}

Technical Report

Untuk masuk kedalam server saya harus mematikan Hyper-V Terlebih dahulu entah mengapa karena saya stuck black screen. Setelah itu saya dapat menggunakan virtual machine yang diberikan oleh panitia dan untuk akses ke sistemnya tersebut maka saya harus mengganti password terlebih dahulu. Saya melakukan reset password dan mengganti kata sandinya agak dapat login sebagai user ubuntu.



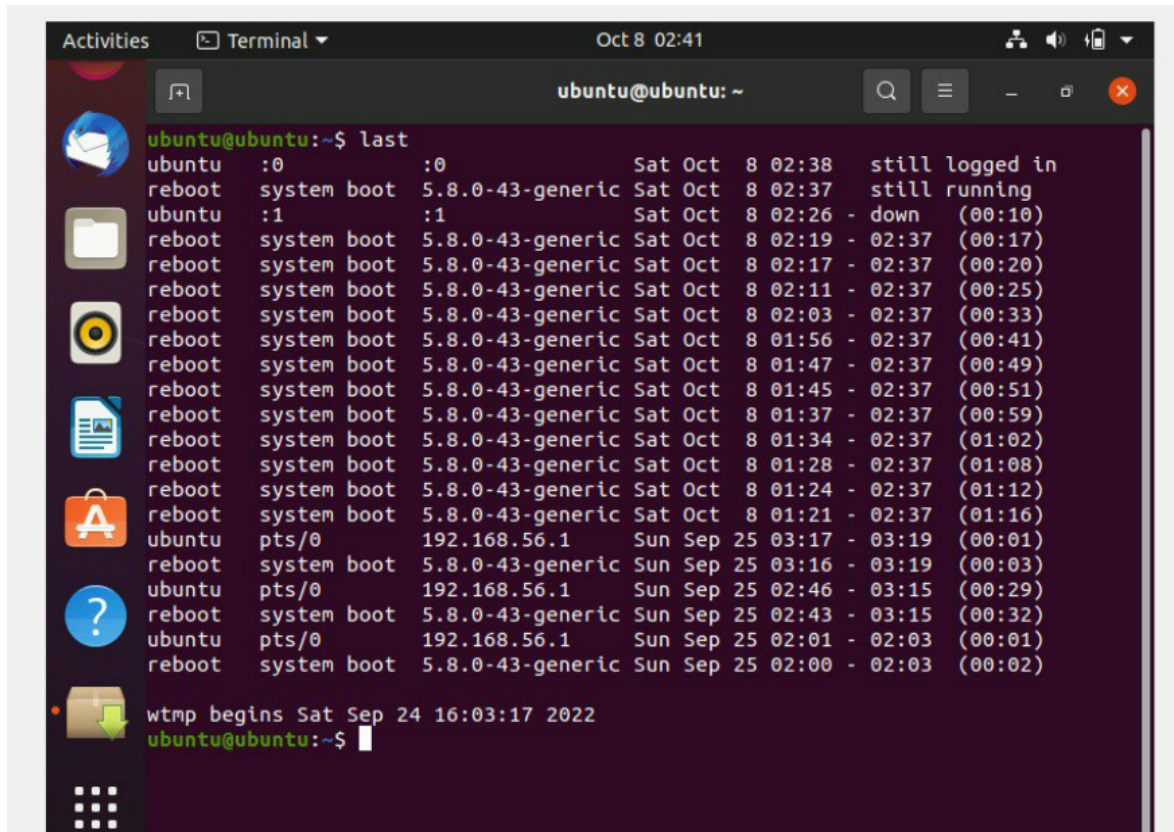
```
generation. network Enable networking
resume root Drop to root shell prompt
system-summary System summary

<Ok>

Press Enter for maintenance
(or press Control-D to continue):

root@ubuntu:~# mount -o rw, remount/
mount: remount/: can't find in /etc/fstab.
root@ubuntu:~# ls /home
ubuntu
root@ubuntu:~# passwd ubuntu
New password:
Retype new password:
passwd: password updated successfully
root@ubuntu:~# _
```

Setelah masuk kedalam sistem maka bukalah terminal dan saya mengetikan perintah `last` sehingga akan terdapat beberapa user serta list ip yang ada.



```
ubuntu@ubuntu:~$ last
ubuntu :0 :0 Sat Oct 8 02:38 still logged in
reboot system boot 5.8.0-43-generic Sat Oct 8 02:37 still running
ubuntu :1 :1 Sat Oct 8 02:26 - down (00:10)
reboot system boot 5.8.0-43-generic Sat Oct 8 02:19 - 02:37 (00:17)
reboot system boot 5.8.0-43-generic Sat Oct 8 02:17 - 02:37 (00:20)
reboot system boot 5.8.0-43-generic Sat Oct 8 02:11 - 02:37 (00:25)
reboot system boot 5.8.0-43-generic Sat Oct 8 02:03 - 02:37 (00:33)
reboot system boot 5.8.0-43-generic Sat Oct 8 01:56 - 02:37 (00:41)
reboot system boot 5.8.0-43-generic Sat Oct 8 01:47 - 02:37 (00:49)
reboot system boot 5.8.0-43-generic Sat Oct 8 01:45 - 02:37 (00:51)
reboot system boot 5.8.0-43-generic Sat Oct 8 01:37 - 02:37 (00:59)
reboot system boot 5.8.0-43-generic Sat Oct 8 01:34 - 02:37 (01:02)
reboot system boot 5.8.0-43-generic Sat Oct 8 01:28 - 02:37 (01:08)
reboot system boot 5.8.0-43-generic Sat Oct 8 01:24 - 02:37 (01:12)
reboot system boot 5.8.0-43-generic Sat Oct 8 01:21 - 02:37 (01:16)
ubuntu pts/0 192.168.56.1 Sun Sep 25 03:17 - 03:19 (00:01)
reboot system boot 5.8.0-43-generic Sun Sep 25 03:16 - 03:19 (00:03)
ubuntu pts/0 192.168.56.1 Sun Sep 25 02:46 - 03:15 (00:29)
reboot system boot 5.8.0-43-generic Sun Sep 25 02:43 - 03:15 (00:32)
ubuntu pts/0 192.168.56.1 Sun Sep 25 02:01 - 02:03 (00:01)
reboot system boot 5.8.0-43-generic Sun Sep 25 02:00 - 02:03 (00:02)

wtmp begins Sat Sep 24 16:03:17 2022
ubuntu@ubuntu:~$
```

Dari user yang sudah login terlihat terdapat ip address yang dimana merupakan 192.168.56.1 dan login pada tanggal 25 september sehingga dari petunjuk output tersebut kita masukan sebagai flag dan berhasil.

Flag

Fostifest{192.168.56.1}